



**BOSCH**

# **Access Management System**

AMS configuration and operation

**de**

Softwarehandbuch



# Inhaltsverzeichnis

|           |  |           |
|-----------|--|-----------|
| <b>1</b>  | <b>Verwenden der Hilfe</b>   | <b>6</b>  |
| <b>2</b>  | <b>Über diese Dokumentation</b>                                      | <b>8</b>  |
| <b>3</b>  | <b>AMS-Systemübersicht</b>   | <b>9</b>  |
| <b>4</b>  | <b>Lizenzierung des Systems</b>                                      | <b>10</b> |
| <b>5</b>  | <b>Konfigurieren des Kalenders</b>                                   | <b>11</b> |
| 5.1       | Definieren von speziellen Tagen                                      | 11        |
| 5.2       | Definieren von Tagesmodellen   | 13        |
| 5.3       | Zeitmodelle definieren   | 15        |
| <b>6</b>  | <b>Konfigurieren von Mandanten</b>                                   | <b>18</b> |
| 6.1       | Zuweisen von Mandanten zu Geräten                                    | 18        |
| 6.2       | Zuweisen von Mandanten zu Bedienern                                  | 19        |
| <b>7</b>  | <b>Konfigurieren der IP-Adressen</b>                                 | <b>20</b> |
| <b>8</b>  | <b>Verwenden des Geräteeditors</b>                                   | <b>21</b> |
| <b>9</b>  | <b>Konfigurieren von Bereichen der Zutrittskontrolle</b>             | <b>23</b> |
| 9.1       | Konfigurieren von Bereichen für Fahrzeuge                            | 24        |
| <b>10</b> | <b>Konfigurieren von Bedienern und Dialogstationen</b>               | <b>27</b> |
| 10.1      | Erstellen der Dialogstationen  | 27        |
| 10.2      | Erstellen von Dialogstationsprofilen                                 | 28        |
| 10.3      | Zuweisen von Dialogstationsprofilen                                  | 29        |
| 10.4      | Erstellen von Benutzer(Bediener-)profilen                            | 30        |
| 10.5      | Zuweisen von Benutzer(Bediener-)profilen                             | 30        |
| 10.6      | Festlegen von Passwörtern für Bediener                               | 32        |
| <b>11</b> | <b>Konfigurieren von Ausweiscodes</b>                                | <b>34</b> |
| <b>12</b> | <b>Konfigurieren der Controller</b>                                  | <b>37</b> |
| 12.1      | Konfigurieren von MACs und RMACs                                     | 37        |
| 12.1.1    | Konfigurieren eines MAC auf dem DMS-Server                           | 37        |
| 12.1.2    | Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs | 38        |
| 12.1.3    | Konfigurieren eines MAC auf seinem eigenen MAC-Server                | 39        |
| 12.1.4    | Hinzufügen von RMACs zu MACs   | 40        |
| 12.1.5    | Hinzufügen weiterer MAC/RMAC-Paare                                   | 43        |
| 12.1.6    | Verwenden des MACInstaller-Tools                                     | 44        |
| 12.2      | Konfigurieren der LACs   | 45        |
| 12.2.1    | AMC-Parameter und -Einstellungen                                     | 47        |
| <b>13</b> | <b>Konfigurieren von Durchritten</b>                                 | <b>65</b> |
| 13.1      | Durchritte – Einführung  | 65        |
| 13.2      | Erstellen von Durchritten  | 66        |
| 13.3      | Zusätzliche E/A-Prüfungen  | 69        |
| 13.4      | Konfigurieren von AMC-Signalen                                       | 70        |
| 13.5      | Vordefinierte Signale für Türmodelle                                 | 78        |
| 13.6      | Sonderdurchritte   | 84        |
| 13.6.1    | Aufzüge (DM07)   | 84        |
| 13.6.2    | Türmodelle mit Einbruchsalarmen (DM14)                               | 87        |
| 13.6.3    | DIPs und DOPs (DM15)   | 90        |
| 13.6.4    | Schleusentürmodelle  | 91        |
| 13.7      | Türen  | 93        |
| 13.8      | Leser  | 97        |
| 13.8.1    | Konfigurieren der Mitarbeiterauslösung                               | 108       |
| 13.9      | Zutritt nur durch PIN-Code   | 108       |

|           |   |            |
|-----------|---|------------|
| 13.10     | AMC-Erweiterungen   | 109        |
| <b>14</b> | <b>Benutzerdefinierte Felder für Personaldaten</b>                                | <b>114</b> |
| 14.1      | Vorschauanzeige und Bearbeiten von benutzerdefinierten Feldern                    | 114        |
| 14.2      | Regeln für Datenfelder  | 117        |
| <b>15</b> | <b>Konfigurieren von Milestone XProtect für die Verwendung von AMS</b>            | <b>118</b> |
| <b>16</b> | <b>Konfigurieren der Bedrohungsstufenverwaltung</b>                               | <b>121</b> |
| 16.1      | Konzepte der Bedrohungsstufenverwaltung   | 121        |
| 16.2      | Überblick über den Konfigurationsprozess  | 121        |
| 16.3      | Konfigurationsschritte im Geräteeditor  | 122        |
| 16.3.1    | Erstellen einer Bedrohungsstufe   | 122        |
| 16.3.2    | Erstellen eines Türsicherheitsprofils   | 123        |
| 16.3.3    | Erstellen eines Lesersicherheitsprofils   | 123        |
| 16.3.4    | Zuweisen von Tür- und Lesersicherheitsprofilen zu Eingängen                       | 124        |
| 16.3.5    | Zuweisen einer Bedrohungsstufe zu einem Hardwaresignal                            | 126        |
| 16.4      | Konfigurationsschritte in Systemdatendialogen                                     | 126        |
| 16.4.1    | Erstellen eines Personensicherheitsprofils  | 127        |
| 16.4.2    | Zuweisen eines Personensicherheitsprofils zu einem Personentyp                    | 127        |
| 16.5      | Konfigurationsschritte in Personaldatendialogen                                   | 128        |
| <b>17</b> | <b>Anlegen und Verwalten von Personaldaten</b>                                    | <b>129</b> |
| 17.1      | Personen  | 130        |
| 17.1.1    | Optionen zur Ausweis-/Gebäudekontrolle  | 131        |
| 17.1.2    | Reserve: Aufzeichnen benutzerdefinierter Informationen                            | 131        |
| 17.1.3    | Erfassen von Unterschriften   | 131        |
| 17.1.4    | Registrieren von Fingerabdruckdaten   | 132        |
| 17.2      | Firmen  | 134        |
| 17.3      | Ausweise: Erstellen und Zuweisen von Zugangsdaten und Berechtigungen              | 134        |
| 17.3.1    | Zuweisen von Ausweisen zu Personen  | 135        |
| 17.3.2    | Registerkarte "Authorizations" (Berechtigungen)                                   | 137        |
| 17.3.3    | Registerkarte "Other data" (Andere Daten): Ausnahmen und spezielle Berechtigungen | 137        |
| 17.3.4    | Autorisieren von Personen zum Festlegen des Büromodus                             | 138        |
| 17.3.5    | SmartIntego-Registerkarte   | 139        |
| 17.3.6    | Erstellen eines Alarmausweis  | 141        |
| 17.4      | Temporäre Ausweise  | 142        |
| 17.5      | PIN-Codes für Personal  | 143        |
| 17.6      | Sperrungen des Zutritts für Personal  | 145        |
| 17.7      | Setzen von Ausweisen auf die schwarze Liste                                       | 146        |
| 17.8      | Bearbeiten von mehreren Personen gleichzeitig                                     | 148        |
| <b>18</b> | <b>Definieren von Zutrittsberechtigungen und Profilen</b>                         | <b>151</b> |
| 18.1      | Erstellen von Zutrittsberechtigungen  | 151        |
| 18.2      | Erstellen von Zutrittsprofilen  | 152        |
| <b>19</b> | <b>Verwalten von Besuchern</b>  | <b>154</b> |
| 19.1      | Besucherdaten   | 154        |
| 19.2      | Besucher zu spät  | 159        |
| <b>20</b> | <b>Verwalten von Parkplätzen</b>  | <b>162</b> |
| 20.1      | Berechtigungen für mehrere Parkzonen  | 162        |
| 20.2      | Übersicht über den Parkplatz  | 163        |
| 20.3      | Erweitertes Parkplatzmanagement   | 163        |
| <b>21</b> | <b>Verwalten von Wächterrunden und Wächterkontrollgängen</b>                      | <b>165</b> |
| 21.1      | Definieren von Wächterrunden  | 165        |

---






|           |   |            |
|-----------|---|------------|
| 21.2      | Verwalten von Wächterkontrollgängen   | 166        |
| 21.3      | Überwachung von Runden (ehemals Wegekontrolle)                                  | 167        |
| <b>22</b> | <b>Zufällige Personenkontrolle</b>  | <b>169</b> |
| <b>23</b> | <b>Verwenden der Ereignisanzeige</b>  | <b>171</b> |
| 23.1      | Festlegen von Filterkriterien für die Zeit relativ zur Gegenwart                | 171        |
| 23.2      | Festlegen von Filterkriterien für ein Zeitintervall                             | 172        |
| 23.3      | Festlegen von Filterkriterien unabhängig von der Zeit                           | 172        |
| <b>24</b> | <b>Verwenden von Berichten</b>  | <b>174</b> |
| 24.1      | Berichte: Stammdaten  | 174        |
| 24.1.1    | Berichterstattung über Fahrzeuge  | 176        |
| 24.2      | Berichte: Systemdaten   | 177        |
| 24.3      | Berichte: Berechtigungen  | 178        |
| <b>25</b> | <b>Betriebs-Bedrohungsstufenverwaltung</b>                                      | <b>180</b> |
| 25.1      | Auslösen und Abbrechen eines Bedrohungsalarms über den Bedienoberflächen-Befehl | 180        |
| 25.2      | Auslösen eines Bedrohungsalarms über Hardwaresignal                             | 181        |
| 25.3      | Auslösen eines Bedrohungsalarms über den Alarmausweis                           | 181        |
| <b>26</b> | <b>Backup und Wiederherstellung</b>   | <b>183</b> |
| 26.1      | Backup-Verfahren  | 183        |
| 26.2      | Wiederherstellungsvorgang   | 184        |
|           | <b>Glossar</b>  | <b>186</b> |

---




# 1 Verwenden der Hilfe

Informationen zum Verwenden dieser Hilfedatei

## Schaltflächen der Symbolleiste

| Schaltfläche  | Funktion   | Beschreibung  |
|---|------------|---|
|    | Ausblenden | Klicken Sie auf diese Schaltfläche, um den Navigationsbereich (Registerkarten „Inhalt“, „Index“ und „Suchen“) auszublenden. Nur der Bereich „Hilfe“ bleibt sichtbar.                  |
|    | Einblenden | Die Schaltfläche „Einblenden“ wird nach dem Anklicken durch die Schaltfläche „Ausblenden“ ersetzt. Klicken Sie auf diese Schaltfläche, um den Navigationsbereich wieder einzublenden. |
|    | Zurück     | Klicken Sie auf diese Schaltfläche, um in der Reihe der zuletzt angezeigten Themen rückwärtszugehen.  |
|   | Vorwärts   | Klicken Sie auf diese Schaltfläche, um in derselben Themenreihe wieder vorwärtszugehen.   |
|  | Drucken    | Klicken Sie auf diese Schaltfläche, um das Thema zu drucken. Wählen Sie die Option „Ausgewähltes Thema drucken“ oder „Ausgewähltes Thema und alle Unterthemen drucken“.               |

## Registerkarten

- Inhalt** Auf dieser Registerkarte wird ein hierarchisches Inhaltsverzeichnis angezeigt. Klicken Sie auf ein Buchsymbol , um das Buch zu öffnen . Klicken Sie dann auf ein Themensymbol , um das Thema anzuzeigen.
- Index** Auf dieser Registerkarte wird ein Index mit Begriffen in alphabetischer Reihenfolge angezeigt. Wählen Sie in der Liste ein Thema aus, oder geben Sie ein Wort ein, um die Themen zu finden, in denen das betreffende Wort enthalten ist.
- Suchen** Verwenden Sie diese Registerkarte zur Suche nach Text. Geben Sie Text in das Feld ein, und klicken Sie dann auf die Schaltfläche

**Themen auflisten**, um die Themen anzuzeigen, die alle eingegebenen Wörter enthalten.

### **Ändern der Größe des Hilfefensters**

Ziehen Sie das Fenster an der Ecke oder am Rand auf die gewünschte Größe.

### **Weitere in dieser Dokumentation verwendete Konventionen**

- Texte (Beschriftungen) der Benutzeroberfläche sind **fett** dargestellt.  
Zum Beispiel **Extras, Datei, Speichern unter...**
- Aufeinanderfolgende Klicks sind mit dem Größer-als-Zeichen **>** dargestellt.  
Zum Beispiel **Datei > Neu > Ordner**
- Änderungen des Typs eines Steuerelements (z. B. Menü, Optionsschaltfläche, Kontrollkästchen, Registerkarte) in einer Sequenz werden unmittelbar vor der Beschriftung des Steuerelements angezeigt.  
Beispiel: Klicken Sie auf den Menüpunkt: **Extra > Optionen > Registerkarte: Ansicht**
- Tastenkombinationen sind auf zwei Weisen dargestellt:
  - „Strg+Z“ bedeutet: Sie halten die erste Taste gedrückt, während Sie die zweite Taste drücken.
  - „Alt, C“ bedeutet: Sie drücken die erste Taste, lassen sie wieder los und drücken dann die zweite Taste.
- Die Funktionen von Symbolschaltflächen sind in eckigen Klammern hinter dem Symbol selbst hinzugefügt.  
Zum Beispiel [Speichern]

## 2 Über diese Dokumentation

Dies ist das Hauptsoftwarehandbuch für den Access Management System.

Es behandelt die Verwendung des Haupt-Dialog-Manager-Programms, im Folgenden bezeichnet als AMS

- Die Konfiguration eines Zutrittskontrollsystems in AMS.
- Der Betrieb des konfigurierten Systems durch Systembedieners.

### **Dazugehörige Dokumentation**

Folgendes ist separat dokumentiert:

- Die Installation von AMS und seiner Hilfsprogramme.
- Der Betrieb von AMS - Map View.



### 3 **AMS-Systemübersicht**

Access Management System ist ein leistungsfähiges, reines Zutrittskontrollsystem, das allein oder in Verbindung mit BVMS, dem Vorseige-Videomanagementsystem von Bosch, funktioniert. Seine Stärke beruht auf der einzigartigen Kombination aus führenden und bewährten Technologien:

- Konzipiert für Benutzerfreundlichkeit: praktische Benutzeroberfläche mit Drag-and-Drop-Kartenansicht und optimierten biometrischen Registrierungsdialogen.
- Konzipiert für die Datensicherheit: Unterstützung der neuesten Standards (EU-DSGVO 2018), Betriebssysteme, Datenbanken und verschlüsselten Systemschnittstellen.
- Konzipiert für hohe Stabilität: Middle Layer-Main Access Controller bieten automatisches Failover und Wiederherstellung von lokalen Zutrittskontrollzentralen bei einem Netzwerkausfall.
- Konzipiert für die Zukunft: regelmäßige Updates und eine Pipeline voller innovativer Erweiterungen.
- Konzipiert für Skalierbarkeit: Niedrige bis hohe Einstiegslevel.
- Konzipiert für Interoperabilität: RESTful APIs mit Schnittstellen zu Bosch Videomanagement, Event-Handling und spezialisierten Partnerlösungen.
- Konzipiert für Investitionsschutz: Damit können Sie Ihre installierte Hardware für die Zutrittskontrolle weiter ausbauen und gleichzeitig die Effizienz steigern.

## 4 Lizenzierung des Systems

### Voraussetzungen

- Das System wurde erfolgreich installiert.
- Sie sind am AMS-Servercomputer angemeldet, vorzugsweise als Administrator.

### Vorgehensweise für gekaufte Lizenzen

**Voraussetzungen:** Sie haben Lizenzen basierend auf der Computersignatur dieses Computers erworben. Kontaktieren Sie Ihren Vertriebsmitarbeiter für Anweisungen.

Dialogpfad: **Configuration** (Konfiguration) > **Licenses** (Lizenzen)

1. Melden Sie sich bei AMS, dem Access Management System, an.  
**Hinweis:** Wenn AMS installiert ist und die Windows-Programme-Ordner angezeigt werden, melden Sie sich mit Windows-Administratorrechten an.
2. Navigieren Sie zu **Configuration** (Konfiguration) > **Licenses** (Lizenzen)
3. Klicken Sie auf **Start license manager** (Lizenzmanager starten)
4. Aktivieren Sie im Fenster **License Manager** (Lizenzmanager) das Kontrollkästchen des von Ihnen erworbenen Basispakets aus.
5. Führen Sie im Pop-up-Fenster **License Activation** (Lizenzaktivierung) folgende Aufgaben aus:
  - Fügen Sie die **Computersignatur** des Access Manager-Servercomputers ein,
  - Fügen Sie den **Lizenzaktivierungsschlüssel** ein, den Sie für das Basispaket erhalten haben,
  - Klicken Sie auf **Activate...** (Aktivieren...)
6. Überprüfen Sie im Fenster **License Manager** (Lizenzmanager), ob das gerade lizenzierte Basispaket den Status **Activation valid** (Aktivierung gültig) hat.
7. Klicken Sie im Fenster **License Manager** (Lizenzmanager) auf:
  - **Import Bundle Info** (Bundle-Info importieren), um alle Lizenzpakete, die Sie gekauft und als Dateien erhalten haben, zu suchen und zu aktivieren.
  - **Import License** (Lizenz importieren), um alle individuellen Lizenzen, die Sie gekauft und als Dateien erhalten haben, zu suchen und zu aktivieren.
8. Klicken Sie auf **Close** (Schließen), um den **Lizenzmanager** zu schließen.
9. Überprüfen Sie zurück im Haupt-**Lizenzen**-Dialog, ob die von Ihnen gekauften Funktionen mit der richtigen Anzahl von Einheiten aufgelistet sind.

### Vorgehensweise für den Demonstrationsmodus

Der Demonstrationsmodus lizenziert alle Systemfunktionen für einen begrenzten Zeitraum. Verwenden Sie den Demonstrationsmodus nur in Nicht-Produktionsumgebungen, um Funktionen vor dem Kauf auszuprobieren.

1. Melden Sie sich beim Access Manager an
2. Navigieren Sie zu **Configuration** (Konfiguration) > **Licenses** (Lizenzen)
3. Klicken Sie auf die Schaltfläche **Activate Demo Mode** (Demomodus aktivieren)
4. Überprüfen Sie, ob die Funktionen im Dialogfenster **Licenses** (Lizenzen) aufgelistet sind.

Der Demonstrationsmodus ist für 5 Stunden aktiviert. Beachten Sie, dass die Ablaufzeit in der Nähe des oberen Randes des Dialogs **Licenses** (Lizenzen) und in der Titelleiste der meisten Dialogfenster angezeigt.

## 5 Konfigurieren des Kalenders

Die Planung der Zutrittskontrollaktivitäten unterliegt **Zeitmodellen**.

Ein **Zeitmodell** ist eine abstrakte Sequenz von einem oder mehreren Tagen, von denen jeder durch ein **Tagesmodell** beschrieben wird.

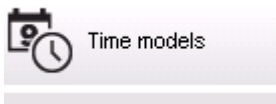
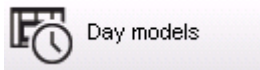
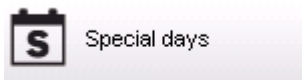
Zeitmodelle steuern Aktivitäten, wenn sie auf den zugrundeliegenden **Kalender** des Zugangskontrollsystems angewendet werden.

Der Kalender des Zutrittskontrollsystems basiert auf dem Kalender des Betriebssystems des Host-Computers, verstärkt ihn aber mit **speziellen Tagen**, die frei vom Administrator des Zutrittskontrollsystems definiert werden.

Spezielle Tage können an einem bestimmten Datum im Kalender festgelegt oder in Bezug auf ein kulturelles Ereignis, wie Ostern, definiert werden. Sie können wiederkehrend sein oder nicht.

Die Konfiguration eines effektiven Kalenders für Ihr Zutrittskontrollsystem besteht aus den folgenden Schritten.

1. Definieren Sie die **speziellen Tage** des Kalenders, der für Ihren Standort gilt.
2. Definieren Sie **Tagesmodelle**, die die aktiven und inaktiven Zeiträume jeder Art von Tag beschreiben. Zum Beispiel unterscheidet sich das Tagesmodell für einen Feiertag von dem eines normalen Arbeitstags. Schichtarbeit wirkt sich auch auf den Typ und die Anzahl der Tagesmodelle aus, die Sie benötigen.
3. Definieren Sie **Zeitmodelle** bestehend aus einem oder mehreren Tagesmodellen.
4. Weisen Sie Ausweisinhabern, Berechtigungen und Durchritten Zeitmodelle zu.



### 5.1 Definieren von speziellen Tagen

Im oberen Listenfeld dieses Dialogs befindet sich eine Liste aller definierten Feiertage. Dabei ist zu beachten, dass alle genannten Termine nur für das laufende Jahr gelten. Der Kalender wird jedoch den eingegebenen Daten entsprechend von Jahr zu Jahr fortgeführt.

Unterhalb der Liste befinden sich verschiedene Dialogfensterfelder, mit denen Sondertage erstellt, geändert oder gelöscht werden können. Mindestens drei dieser Eingabefelder müssen Daten enthalten, damit ein neuer Sondertag hinzugefügt werden kann. Zuerst müssen eine **Beschreibung** und ein **Datum** in die entsprechenden Felder eingegeben werden. Dann muss in der entsprechenden Auswahlliste die **Klasse** ausgewählt werden, der dieser Sondertag angehören soll.

Division: Common

« System data

**S** Special days

Day models

Time models

List of available special days

| Date (cur. year) | Description                | Day model    | Division |
|------------------|----------------------------|--------------|----------|
| Mi 01/01/2014    | New Year                   | DMAC-Holiday | Common   |
| Mo 01/20/2014    | Martin Luther King Jr. Day | DMAC-Holiday | Common   |
| Mo 02/17/2014    | Presidents' Day            | DMAC-Holiday | Common   |
| Mo 05/26/2014    | Memorial Day               | DMAC-Holiday | Common   |
| Fr 07/04/2014    | Independence Day           | DMAC-Holiday | Common   |
| Mo 09/01/2014    | Labor Day                  | DMAC-Holiday | Common   |
| Mo 10/13/2014    | Columbus Day               | DMAC-Holiday | Common   |
| Di 11/11/2014    | Veterans' Day              | DMAC-Holiday | Common   |
| Do 11/27/2014    | Thanksgiving Day           | DMAC-Holiday | Common   |
| Do 12/25/2014    | Christmas Day              | DMAC-Holiday | Common   |

Create, modify, or delete a special day

Description:

Day model: DMAC-Holiday : Holiday : Common

Date: 10/01/\*\*\*\* every year

Days to add: 7

Week day: Montag : after the date

Date in this year: Mo 10/13/2014

Priority: 60    Valid from:     until:

Zur Festlegung des Datums müssen mehrere Schritte ausgeführt werden. Zuerst muss in das Feld **Datum** ein Basisdatum eingegeben werden. An diesem Punkt beschreibt das Datum ein Ereignis im laufenden Jahr. Wenn der Benutzer jetzt in der Auswahlliste neben dem Datumsfeld die Häufigkeit einer periodischen Wiederkehr angibt, werden die Teile des Datums, auf die die Periodizität sich bezieht, durch Platzhalterzeichen (\*) ersetzt.

|  |            |
|--|------------|
| einmalig   | __.*.____  |
| once per year (jährlich)   | __.*.****  |
| once per month for a period of a year (monatlich für die Dauer eines Jahres) | __.**.____ |
| once per month in every year (monatlich in jedem Jahr)                       | __.**.**** |
| depending on Easter (abhängig von Ostern)                                    | **.**.**** |

Für die von Ostern abhängigen Sondertage wird kein Datum angegeben, sondern der Abstand zum Ostersonntag in Tagen. Das Datum des Ostersonntags im laufenden Jahr wird im Feld **Date within this year (Datum in diesem Jahr)** angezeigt. Die Abweichung von diesem Datum wird im Feld **Days to add (abweichende Tage)** eingegeben oder ausgewählt. Die maximale Anzahl an Tagen beträgt 188, sodass durch Addition bzw. Subtraktion jeder Tag eines Jahres festgelegt werden kann.

Die übrigen Angaben, wie z. B. der **Wochentag** des Sondertags, sind optional. Beachten Sie, dass die Liste der Wochentage von den regionalen Einstellungen des Betriebssystems gesteuert wird. Dies führt unvermeidlich zu gemischtsprachigen Anzeigen, in denen sich die Sprachen des Zugangskontrollsystems und des Betriebssystems unterscheiden.

Die Zuweisung einer **Gültigkeitsdauer** ist ebenfalls optional. Wenn keine Dauer angegeben wird, gilt aufgrund der Standardeinstellungen eine unbeschränkte Gültigkeit ab Eingabedatum. Auch eine **Priorität** kann festgesetzt werden. Die Priorität (von 1 bis 100) bestimmt, welcher Feiertag verwendet werden soll. Wenn zwei Feiertage auf das gleiche Datum fallen, rangiert der Feiertag mit der höheren Priorität an erster Stelle. Bei gleichen Prioritäten ist undefiniert, welcher Feiertag verwendet wird.

Ein Feiertag mit der Priorität „0“ wird deaktiviert und nicht verwendet.

Der Dialog **Time Models** (Zeitmodelle) zeigt nur aktive Feiertage an, also diejenigen mit einer Priorität größer als „0“.

---

**Hinweis!**

Ein Zeitmodell des Mandanten „Common“ (Allgemein) kann nur Feiertage verwenden, die dem Mandanten „Common“ (Allgemein) zugewiesen sind.

Ein Zeitmodell eines spezifischen Mandanten „A“ kann nur Feiertage verwenden, die dem Mandanten „A“ zugewiesen sind.

Es ist nicht möglich, Feiertage zwischen Mandanten zu mischen. Das bedeutet, dass jeder Mandant nur die spezifischen Feiertage verwenden kann, die ihm in dem spezifischen Zeitmodell zugewiesen sind.

---

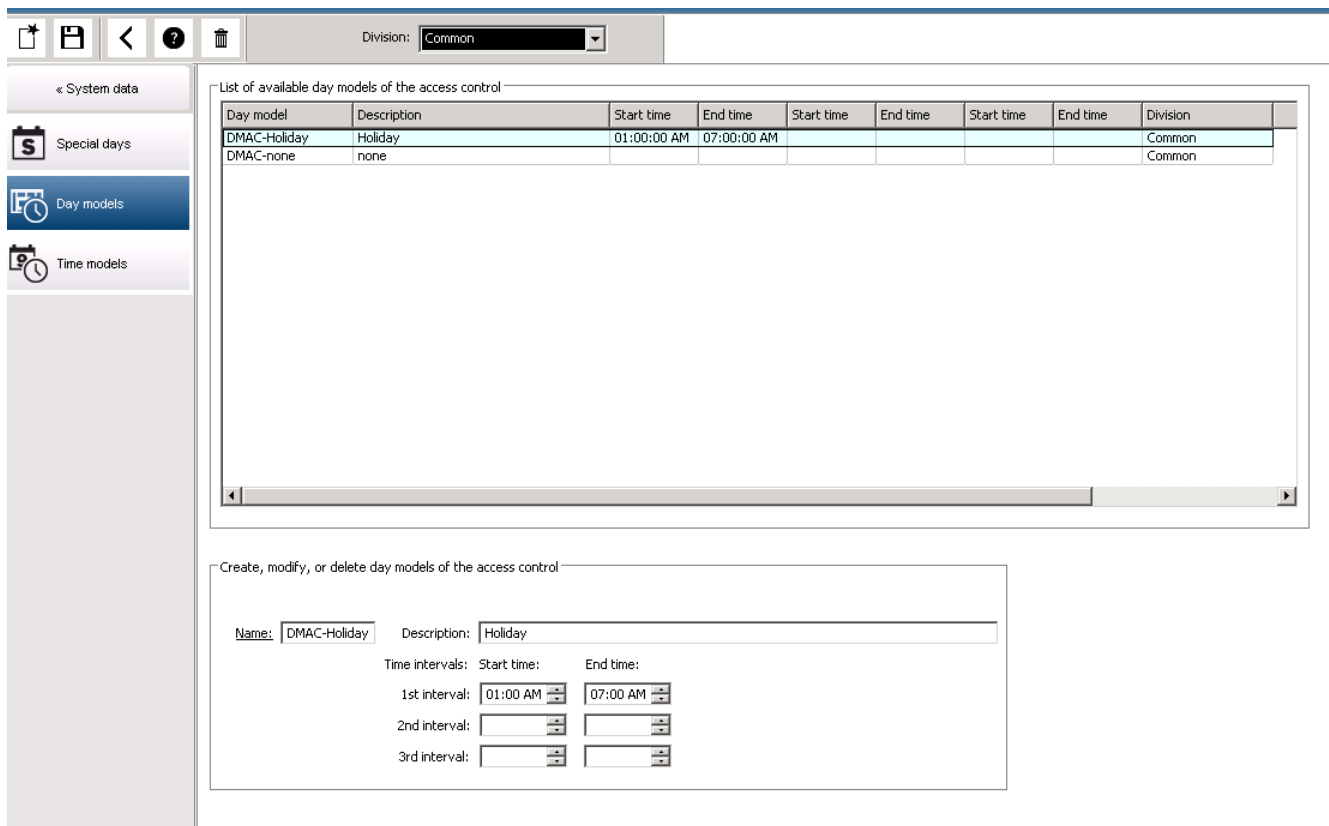


## 5.2

### Definieren von Tagesmodellen


Tagesmodelle definieren ein Schema für einen Tag. Sie können bis zu drei Zeitintervalle umfassen.

In diesem Dialog werden zunächst alle vorhandenen Tagesmodelle in einer Liste angezeigt.



Sie können in diesem Dialog Modellnamen, Beschreibungen und Intervalle eingeben oder



ändern. Klicken Sie zur Erstellung eines neuen Modells auf die Schaltfläche . Anfang und Ende eines Zeitintervalls werden in Stunden und Minuten eingegeben. Bei Erreichen der angegebenen Zeit wird das Intervall entweder aktiviert oder deaktiviert. Im Listenfeld werden auch die Sekunden angegeben (immer 00), um zu verdeutlichen, dass diese Zeiten präzise Grenzen darstellen. Beispiel: Eine Berechtigung mit einem Zeitmodell, das ein Intervall von 08:00 bis 15:30 Uhr enthält, erlaubt den Zutritt von 08:00:00 bis 15:30:00 Uhr. Um 15:30:01 Uhr wird der Zutritt verweigert. Die Start- und Endzeiten werden bei der Eingabe einer logischen Prüfung unterzogen. Beispielsweise muss die Startzeit kleiner als die zugehörige Endzeit sein. Dies hat zur Folge, dass Intervalle nicht über Mitternacht hinausgehen dürfen, sondern an diesem Punkt geteilt werden müssen:

|              |      |           |      |           |
|--------------|------|-----------|------|-----------|
| 1. Intervall | von: | ...       | bis: | 00:00 Uhr |
| 2. Intervall | von: | 00:00 Uhr | bis: | ...       |

Mit Ausnahme von Mitternacht (00:00 Uhr) dürfen sich die Intervallgrenzen eines einzelnen Tagesmodells nicht überschneiden. Es ist somit nicht möglich, die gleiche Zeit für das Ende eines Intervalls und den Anfang des nächsten Intervalls einzugeben. Die einzige Ausnahme bildet ein 24-Stunden-Intervall, das um 00:00 Uhr beginnen und enden muss.



**Hinweis!**

Tipp: Sie können Intervalle im Dialog „Zeitmodelle“ prüfen. Erstellen Sie dazu zuerst ein Tagesmodell mit diesen Intervallen („Systemdaten > Kalender > Tagesmodelle“). Weisen Sie dieses Tagesmodell dann einem Testzeitmodell mit einer Dauer von einem Tag zu („Systemdaten > Kalender > Zeitmodelle“). Die Intervalle werden dann im Balkendiagramm dargestellt.

Schließen Sie den Dialog „Zeitmodelle“, ohne die Änderungen zu speichern.

Ein Tagesmodell kann nur dann gelöscht werden, wenn es keinem Sondertag zugewiesen wurde und in keinem Zeitmodell verwendet wird.

### 5.3 Zeitmodelle definieren

| No.     | Day model    | 6:00AM | 12:00PM | 6:00PM | Description | Date (1st period) | Division |
|---------|--------------|--------|---------|--------|-------------|-------------------|----------|
| 7274568 | DMAC-Holi... | [Bar]  | [Bar]   | [Bar]  | Holiday     | Di 07/21/2015     | Commc    |
| 7274568 | DMAC-Holi... | [Bar]  | [Bar]   | [Bar]  | Holiday     | Mi 07/22/2015     | Commc    |
| 7274569 | DMAC-Holi... | [Bar]  | [Bar]   | [Bar]  | Holiday     | Do 07/23/2015     | Commc    |
| 7274570 | DMAC-Holi... | [Bar]  | [Bar]   | [Bar]  | Holiday     | Fr 07/24/2015     | Commc    |
| 7274571 | DMAC-Holi... | [Bar]  | [Bar]   | [Bar]  | Holiday     | Sa 07/25/2015     | Commc    |
| 7274572 | DMAC-none    | [Bar]  | [Bar]   | [Bar]  | none        | So 07/26/2015     | Commc    |

Über die Suchliste können vorhandene Zeitmodelle ausgewählt und die zugehörigen Details in den Dialogfensterfeldern angezeigt werden. Bei der Bearbeitung gilt das gleiche Verfahren wie beim Erstellen neuer Zeitmodelle.

Wenn die Maske leer ist, können Zeitmodelle neu angelegt werden. Hierzu müssen Sie einen **Namen** eingeben und angeben, wie viele Tage der **Zeitraum** umfassen soll. Wählen Sie außerdem ein Start- oder **Referenzdatum** aus. Nach der Bestätigung dieser Daten (**Eingabetaste**), wird im Dialogfensterfeld **Zuweisung von Tagesmodellen** eine Liste angezeigt. Die Zeilenanzahl dieser Liste entspricht der oben festgelegten Anzahl von Tagen. Die Spalten enthalten bereits eine fortlaufende Nummer und die Daten für die Periode, ausgehend vom gewählten Startdatum.

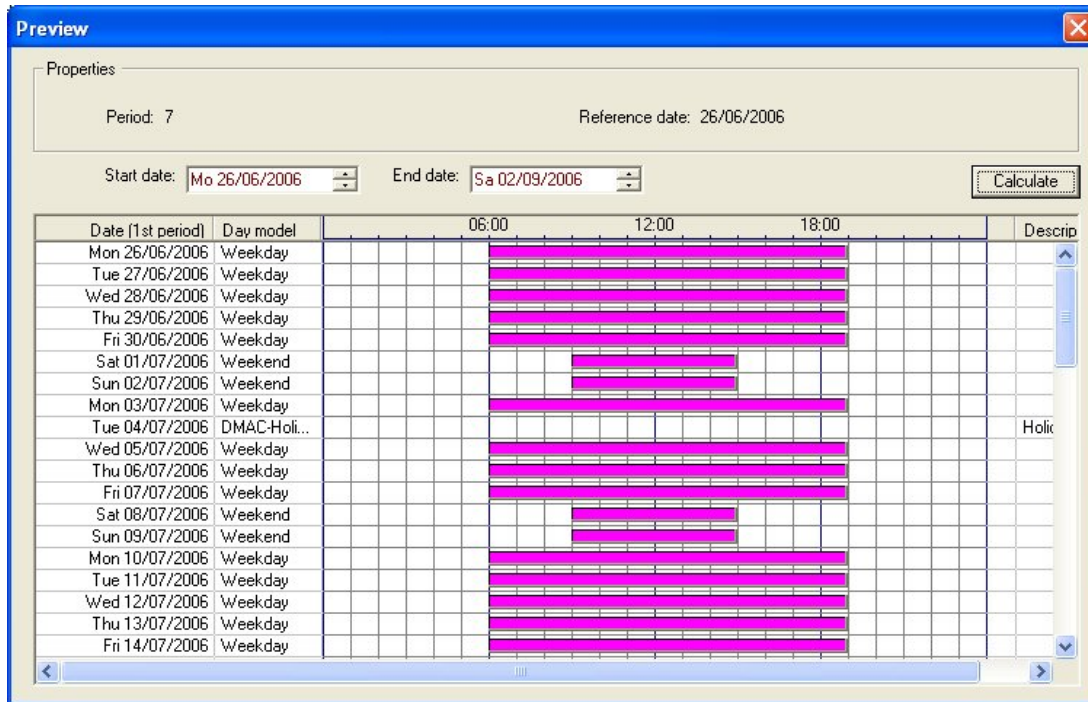
Benutzer können nur in der Spalte **Name** dieser Liste Einträge ändern oder hinzufügen. Wie bereits erwähnt, ergeben sich die Einträge in den Spalten **Nr.** und **Datum** aus den Angaben im Dialogkopf. Die Spalte **Beschreibung** wird bei der Auswahl eines Tagesmodells automatisch mit den entsprechenden Erläuterungen gefüllt.

Durch einen Doppelklick in einer Zeile der Spalte **Tagesmodell** wird ein Auswahllistenfeld aktiviert. Hier kann eines der vorhandenen Tagesmodelle ausgewählt werden. So kann jedem Tag der Periode ein bestimmtes Tagesmodell zugewiesen werden. Wenn der Benutzer zu einer anderen Zeile wechselt, wird in der Spalte **Beschreibung** eine vorhandene Erläuterung des ausgewählten Tagesmodells angezeigt.

Die vordefinierten **Sondertage** mit den entsprechenden Tagesmodellen werden im unteren Listenfeld angezeigt. Dies erleichtert die Navigation und die Kontrolle. Es ist möglich, die Tagesmodelle, die bestimmten Sondertagen zugewiesen wurden, bei dem ausgewählten oder neu erstellten Zeitmodell zu ändern. Diese Änderungen gelten allerdings nur für dieses eine Zeitmodell. Globale Änderungen, die für alle vorhandenen und künftigen Modelle gelten sollen, können ausschließlich im Dialog „Holidays“ (Sondertage) vorgenommen werden. Im Einklang mit diesen Einstellungen werden die Wochentage dann den entsprechenden Tagesmodellen zugeordnet

(es sei denn, ein Sondertag im Kalender hat Vorrang vor dem jeweiligen Tagesmodell). Damit schnell geprüft werden kann, ob Tagesmodelle insbesondere an Sondertagen richtig verwendet und zugewiesen wurden, enthält dieser Dialog eine **Vorschau**, in der die bestimmten Perioden zugewiesenen Tage angezeigt werden.

Durch einen Klick auf die Schaltfläche **Vorschau** wird ein separater Dialog geöffnet. Hier kann ein Zeitraum von bis zu 90 Tagen festgelegt werden (einschließlich etwaiger Sondertage). Über die Schaltfläche **Calculate** (Berechnen) wird ein Bericht erstellt und angezeigt (siehe nachfolgende Abbildung). Je nach der Länge des Intervalls kann dieser Vorgang ein paar Sekunden dauern.



Laut Standardeinstellung werden die Sondertage ihren Definitionen entsprechend auf die Zeitmodelle angewendet. Sollten die Sondertage nicht berücksichtigt werden, liegt dies möglicherweise daran, dass die Option **Ignore special days (Ignorieren von Sondertagen)** ausgewählt wurde. Wenn gleichzeitig die Einträge aus den beiden unteren Listen gelöscht werden, bedeutet dies, dass die Sondertage und Tagesklassen in diesem Modell keine Anwendung finden.



Division: Common

Time model of the access control

Name:  Description:

Period:  Reference date:   Ignore special days

[Preview](#)

Assignment of day models

| No.     | Day model    | 6:00AM | 12:00PM | 6:00PM | Description | Date (1st period) | Division |
|---------|--------------|--------|---------|--------|-------------|-------------------|----------|
| 7274568 | DMAC-Holl... |        |         |        | Holiday     | Di 07/21/2015     | Comm     |
| 7274568 | DMAC-Holl... |        |         |        | Holiday     | Mi 07/22/2015     | Comm     |
| 7274569 | DMAC-Holl... |        |         |        | Holiday     | Do 07/23/2015     | Comm     |
| 7274570 | DMAC-Holl... |        |         |        | Holiday     | Fr 07/24/2015     | Comm     |
| 7274571 | DMAC-Holl... |        |         |        | Holiday     | Sa 07/25/2015     | Comm     |
| 7274572 | DMAC-none    |        |         |        | none        | So 07/26/2015     | Comm     |

| Holiday | Day model | 6:00AM | 12:00PM | 6:00PM | Description | Date (1st period) | Division |
|---------|-----------|--------|---------|--------|-------------|-------------------|----------|
|         |           |        |         |        |             |                   |          |

## 6 Konfigurieren von Mandanten

### Einführung

Das System kann optional so lizenziert werden, dass es eine gemeinsame Zugriffskontrolle für eine Einrichtung bietet, die von einer beliebigen Anzahl unabhängiger Parteien gemeinsam genutzt wird. Diese werden als **Mandanten** bezeichnet.

Systembedienern können ein oder mehrere Mandanten zugewiesen sein. Die Bediener sehen dann nur noch die Personen, Geräte und Eingänge dieser Mandanten.

Wenn die **Mandanten**-Funktion nicht lizenziert ist, gehören alle vom System verwalteten Objekte zu einem einzelnen Mandanten namens **Common** (Allgemein).



### Voraussetzungen

- Die Mandanten-Funktion ist für Ihre Installation lizenziert.

### Dialogpfad

- Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Divisions** (Mandanten)

### Vorgehensweise

1. Klicken Sie in der Symbolleiste auf  .
  - Ein neuer Mandant wird mit einem Standardnamen erstellt.
2. Überschreiben Sie den Standardnamen, und geben Sie (optional) eine Beschreibung für andere Bediener ein.
3. Klicken Sie in die Spalte **Color** (Farbe), um eine Farbe zuzuweisen. Damit lassen sich die Elemente des Mandanten in der Benutzeroberfläche unterscheiden.
4. Klicken Sie zum Speichern auf  .

Access Management System: Divisions [Administrator] (Demo mode expires: 07/04/2019 11:21:08 PM)

File Edit Data Help

Division: Common

Divisions:

| Division  | Colour | Description       |
|-----------|--------|-------------------|
| Common    |        | (Common division) |
| ACME Corp |        | 1st floor tenant  |
| BCME Corp |        | 2nd floor tenant  |

« Main menu

- Device data
- Operators and Workstations
- Options
- Tools
- Licenses
- Divisions**

### 6.1 Zuweisen von Mandanten zu Geräten

Mandanten zu Geräten im Geräteeditor zuweisen


**Dialogpfad**

Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

**Voraussetzungen**

- Mandanten sind lizenziert und werden ausgeführt
- Mindestens ein Mandant wurde erzeugt.

**Vorgehensweise**

1. Wählen Sie im Gerätebaum das Gerät für die Zuweisung aus.
  - Der Geräteeditor wird im Hauptdialogfeld angezeigt.
2. Wählen Sie in der Mandantenliste den neuen Mandanten für das Gerät aus.
  - Der neue Mandant wird im Listenfeld angezeigt.
3. Klicken Sie auf  (Speichern), um zu speichern.

**Hinweis!**

Alle Komponenten eines Eingangs müssen zu einem Mandanten gehören. Das System ermöglicht es Ihnen erst, einen Eingang zu speichern, wenn alle seine Komponenten zum gleichen Mandanten gehören.

## 6.2

### Zuweisen von Mandanten zu Bedienern

Mandanten zu Bedienern im Dialogfeld **User rights** (Benutzerrechte) zuweisen


**Dialogpfad**

Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Operators and workstations (Bediener und Dialogstationen)** > **User rights** (Benutzerrechte)

**Voraussetzungen**

- Mandanten sind lizenziert und werden ausgeführt
- Mindestens ein Mandant wurde erzeugt.
- Mindestens ein Bediener wurde im System erstellt.

**Vorgehensweise**

1. Wählen Sie im Dialogfeld **User rights** (Benutzerrechte) den Personaldatensatz des Bedieners aus, der zugewiesen werden soll.
2. Verwenden Sie auf der Registerkarte **Divisions** (Mandanten) die Pfeiltasten, um Mandanten aus der Liste der **verfügbaren Mandanten** in die Liste der **zugewiesenen Mandanten** für diesen Bediener zu verschieben.
3. Klicken Sie auf  (Speichern), um zu speichern.

## 7 Konfigurieren der IP-Adressen

Die lokalen Zutrittskontrollen im Netzwerk erfordern ein einheitliches Schema von IP-Adressen, um am Zutrittskontrollsystem teilnehmen zu können. Das Tool **AccessIPConfig** lokalisiert die Controller im Netzwerk und bietet eine komfortable Schnittstelle, um ihre Adressen und andere Netzwerkooptionen zentral zu verwalten.

### Voraussetzungen

- Die lokalen Zutrittskontrollen sind eingeschaltet und mit dem Netzwerk verbunden.
- Sie haben ein Schema für die IP-Adressen der Controller und, falls erforderlich, ihre Passwörter.

### Dialogpfad

**Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Tools**

### Vorgehensweise

1. Folgen Sie dem obigen Dialogpfad und klicken Sie auf **Configuration AMC and fingerprint devices** (**Konfiguration AMC und Fingerabdruckgeräte**) Das Tool **AccessIPConfig** wird geöffnet.
2. Klicken Sie auf **Scan AMCs** (AMCs scannen).  
Die lokalen Zutrittskontrollen, die im Netzwerk verfügbar sind, werden mit den folgenden Parametern aufgelistet:
  - **MAC-Adresse:** Die Hardwareadresse des Controllers. Beachten Sie, dass dies **nicht** die Adresse seines Main Access Controllers ist, die nur zufällig MAC genannt wird.
  - **Statische IP-Adresse:**
  - **Portnummer:** Der Standardwert ist 10001
  - **DHCP:** Der Wert ist nur **Yes** (Ja), wenn der Controller so konfiguriert ist, dass er eine IP-Adresse von DHCP erhält
  - **Aktuelle IP-Adresse**
  - **Seriennummer**
  - Notizen, die vom Netzwerkkonfigurationsteam hinzugefügt wurden
3. Doppelklicken Sie auf einen AMC in der Liste, um seine Parameter in einem Popup-Fenster zu ändern. Alternativ wählen Sie die Zeile des gewünschten AMC und klicken Sie auf **Set IP...** (Statische IP-Adresse). Beachten Sie, dass eventuell ein Passwort eingegeben werden muss, falls eines für das Gerät konfiguriert wurde.  
Die geänderten Parameter werden gespeichert, sobald Sie im Popup-Fenster auf OK klicken.
4. Wenn Sie mit der Konfiguration der IP-Parameter der Controller fertig sind, klicken Sie auf **File** (Datei) > **Exit** (Beenden), um das Tool zu schließen.  
Sie kehren zur Hauptanwendung zurück.

Für detailliertere Informationen klicken Sie auf **Help** (Hilfe) im Tool **AccessIPConfig**, um seine eigene Hilfedatei anzuzeigen.

# 8 Verwenden des Geräteeditors

## Einführung

Der Geräteeditor **DevEdit** ist zum Hinzufügen und Löschen einer kleinen Zahl von Durchtritten und Geräten oder zum Hinzufügen, Ändern oder Löschen einzelner Parameter gedacht. Für den Import von großen, bestehenden Konfigurationen verwenden Sie die Funktion **Configuration Import/Export** (Konfiguration Import/Export) unter **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Tools**

Der Geräteeditor bietet Ansichten, die den folgenden bearbeitbaren Hierarchien entsprechen:

- **Gerätekonfiguration:** die elektronischen Geräte innerhalb des Zugangskontrollsystems.
- **Dialogstationen:** die Computer, die im Zugangskontrollsystem zusammenarbeiten.
- **Bereiche:** die physischen Bereiche, in die das Zutrittskontrollsystem unterteilt ist.

## Voraussetzungen










Das System ist korrekt installiert, lizenziert und im Netzwerk.





## Dialogpfad

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

## Verwenden der DevEdit-Symbolleiste

Die DevEdit-Symbolleistenschaltflächen haben die folgenden Funktionen, unabhängig davon, welche Ansicht aktiv ist, z. B. **Devices** (Geräte), **Workstations** (Dialogstationen) oder **Areas** (Bereiche).

| Schaltfläche  | Tastenkürzel  | Beschreibung   |
|---|---------------|--|
|  | Strg + N      | Erstellt ein neues Element unterhalb des gewählten Knotens. Klicken Sie alternativ mit der rechten Maustaste auf den Knoten, um dessen Kontextmenü aufzurufen. |
|  | Entf          | Löscht das gewählte Element und alle darunter befindlichen Daten.  |
|  | Strg-Bild auf | Erstes Element im Baum   |
|  | Strg -        | Vorheriges Element   |
|  | Strg +        | Nächstes Element   |
|  | Strg-Bild ab  | Letztes Element im Baum  |
|  | Strg-A        | Erweitert und reduziert den Baum.  |
|  | Strg-K        | Aktualisiert die Daten, indem sie aus der Datenbank neu geladen werden.<br><b>Alle nicht gespeicherten Änderungen werden verworfen.</b>                        |
|  | Strg-S        | Speichert die aktuelle Konfiguration   |

|   |        |   |
|---|--------|---|
|  | Strg-F | Öffnet ein Suchfenster  |
|  |        | Öffnen Sie den Baum <b>Device configuration</b> (Gerätekonfiguration) |
|  |        | Öffnen Sie den Baum <b>Workstations</b> (Dialogstationen)             |
|  |        | Öffnen Sie den Baum <b>Areas</b> (Bereiche)                           |

Beginnen Sie in allen DevEdit-Ansichten im Stammverzeichnis des Baums und fügen Sie Elemente über die Symbolleistenschaltflächen, das Menü oder das Kontextmenü der einzelnen Elemente hinzu (klicken Sie mit der rechten Maustaste, um sie aufzurufen). Um Unterelemente zum Baum hinzuzufügen, wählen Sie zuerst das Element aus, unter dem die Unterelemente angezeigt werden sollen.

Wenn Sie mit dem Hinzufügen von Elementen zum Baum fertig sind, klicken Sie auf **Save**

(Speichern)  , um die Konfiguration zu speichern.

Um DevEdit zu schließen, klicken Sie auf **File** (Datei) > **Exit** (Beenden).

## 9 Konfigurieren von Bereichen der Zutrittskontrolle

### Einführung in Bereiche

Gesicherte Anlagen können in Bereiche unterteilt werden. Bereiche können eine beliebige Größe aufweisen und beispielsweise mehrere Gebäude, einzelne Etagen oder sogar einzelne Räume umfassen.

Einige Anwendungen von Bereichen sind:

- Lokalisierung einzelner Personen in gesicherten Anlagen.
- Schätzung der Personenanzahl in einem bestimmten Bereich bei Evakuierung oder anderen Notfällen.
- Beschränkung der Anzahl von Personen oder Fahrzeugen in einem Bereich: Wenn die vorgegebene Höchstzahl erreicht ist, kann der weitere Einlass verweigert werden, bis einige Personen oder Fahrzeuge den Bereich verlassen.
- Einrichtung der Zutrittsfolge- und Zutrittswiederholkontrolle

Das System unterscheidet zwischen zwei Arten von Bereichen mit Zutrittskontrolle

- Bereiche für Personen
- Bereiche für Fahrzeuge (Parkplätze)

Jeder Bereich kann Unterbereiche für eine feinere Granularität der Kontrolle aufweisen.

Bereiche für Personen können bis zu drei Nistungsniveaus haben und Bereiche für Parkplätze nur zwei, nämlich den gesamten Parkplatz und die Parkzonen, zwischen 1 und 24.

Der Standardbereich, der in allen Installationen vorhanden ist, wird **Outside** (Außerhalb) genannt. Er dient als übergeordneter Bereich für alle benutzerdefinierten Bereiche beider Arten: Person und Parkplätze.

Ein Bereich ist nicht nutzbar, es sei denn, mindestens ein Durchtritt führt hinein.

Geräteeditor **DevEdit** kann verwendet werden, um jedem Durchtritt einen Standortbereich und einen Zielbereich zuzuordnen. Wenn eine Person einen Ausweis an einem Leser scannt, der zu einem Durchtritt gehört, wird der neue Aufenthaltsort dieser Person zum Zielbereich dieses Durchtritts.



### Hinweis!

Die Verwendung der Zutrittsfolgekontrolle und der Zutrittswiederhol Sperre setzt voraus, dass es an den Durchritten der Bereiche Durchtritt- und Ausgangsleser gibt.

Durchritte mit Drehkreuz werden dringend empfohlen, um versehentliches oder absichtliches Durchschlüpfen zu verhindern

### Vorgehensweise zum Erstellen von Bereichen

#### Voraussetzungen

Als Systembetreiber benötigen Sie eine Berechtigung von Ihrem Systemadministrator, um Bereiche anzulegen.


#### Dialogpfad (AMS)

1. Wählen Sie im AMS-Dialogmanager **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)



2. Klicken Sie auf Bereiche
3. Wählen Sie den Knoten **Outside** (Außerhalb) oder einen seiner untergeordneten Knoten



und klicken Sie auf  in der Symbolleiste. Alternativ klicken Sie mit der rechten Maustaste auf **Outside** (Außerhalb), um einen Bereich über sein Kontextmenü hinzuzufügen.

Alle ursprünglich erstellten Bereiche erhalten den eindeutigen Namen **Area** (Bereich) plus ein numerisches Suffix.

4. Wählen Sie im Popup-Fenster den Typ aus, also **Area** (Bereich) für Personen oder **Parking lot** (Parkplatz) für Fahrzeuge.

Beachten Sie das nur **Outside** (Außerhalb) untergeordnete Bereiche beider Arten haben kann. Jeder Unterbereich dieser untergeordneten Elemente erbt immer den Typ des übergeordneten Elements.

- **Bereiche** für Personen können auf drei Ebenen verschachtelt werden. Für jeden Bereich oder Unterbereich können Sie eine maximale Belegung definieren.
- **Parkplätze** sind virtuelle Einheiten, die aus mindestens einer **Parkzone** bestehen. Wenn die Belegung eines Parkplatzes nicht durch das System begrenzt werden muss, wird 0 angezeigt. Andernfalls beträgt die maximale Anzahl von Parkplätzen pro Zone 9999 und der Hauptbereich des Parkplatzes zeigt die Summe aller Räume in seinen Zonen an.

#### Vorgehensweise zum Bearbeiten von Bereichen

1. Klicken Sie auf einen Bereich in der Hierarchie, um ihn auszuwählen.
2. Überschreiben Sie eines oder mehrere der folgenden Attribute im Hauptbereich des Dialogfelds.

|   |   |
|---|---|
| <b>Name</b>                               | Der Standardname, den Sie überschreiben können.   |
| <b>Beschreibung</b>                       | Eine Freitextbeschreibung des Gebiets.  |
| <b>Maximale Anzahl von Personen/Autos</b> | Standardwert 0 (Null) für keine Begrenzung.<br>Geben Sie andernfalls eine Ganzzahl für die maximale Belegung ein. |


#### Hinweise:

- Ein Bereich kann nicht durch Ziehen und Ablegen in einen anderen Zweig der Hierarchie verschoben werden. Löschen Sie ggf. den Bereich und erstellen Sie ihn in einem anderen Zweig neu.

#### Vorgehensweise zum Löschen von Bereichen.

1. Klicken Sie auf einen Bereich in der Hierarchie, um ihn auszuwählen.



2. Klicken Sie auf **Delete** (Löschen)  oder klicken Sie mit der rechten Maustaste, um über das Kontextmenü zu löschen.

**Hinweis:** Ein Bereich kann erst gelöscht werden, wenn alle seine untergeordneten Objekte gelöscht wurden.

## 9.1

### Konfigurieren von Bereichen für Fahrzeuge



### Erstellen von Bereichen für Fahrzeuge (Parkplatz, Parkzone)

Wenn Sie den Bereichstyp **Parkplatz** auswählen, wird ein Popup-Fenster angezeigt.

| Name               | Count |
|--------------------|-------|
| Central parking_01 | 20    |
| Central parking_02 | 15    |
| Central parking_03 | 50    |
| Central parking_04 | 100   |

1. Geben Sie einen Namen in das Feld **Name starts with** (Name beginnt mit) ein, um einen Stammnamen für alle seine Unterbereiche oder **Parkzonen** zu erstellen. Bis zu 24 **Parkzonen** können über die Schaltfläche **Add** (Hinzufügen) erstellt werden und jede hat den Stammnamen plus ein zweistelliges Suffix.
2. Wenn das System die Belegung dieser Bereiche einschränken soll, geben Sie die Anzahl der Parkplätze in der Spalte **Count** (Anzahl) ein. Wenn kein Belegungslimit benötigt wird, geben Sie 0 ein.

**Hinweis:** Die maximale Belegung des gesamten Parkplatzes ist die Summe dieser Zahlen. Nur Parkzonen können Parkplätze enthalten; der **Parkplatz** ist nur eine virtuelle Einheit bestehend aus mindestens einer **Parkzone**. Die maximale Anzahl an Parkplätzen pro Parkzone beträgt 9999.

### Erstellen von Durchritten für Parkplätze

Wie bei normalen Bereichen benötigen Parkplätze einen Durchtritt. Das passende Türmodell ist **Parkplatz 05c**.

Zur Überwachung der Belegung eines Parkplatzes sind zwei Durchritte mit diesem Türmodell auf dem gleichen AMC erforderlich, eines für den Eingang und eines für den Ausgang.

#### Voraussetzung

Erstellen Sie einen Parkplatz mit mindestens einer Parkzone, wie oben beschrieben.

#### Dialogpfad

**Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)



Klicken Sie auf **LACs/Entrances/Devices** (LACs/Durchritte/Geräte)

#### Vorgehensweise

1. Erstellen Sie in der Gerätehierarchie einen AMC oder wählen Sie einen AMC aus, der keine abhängigen Durchritte hat.
2. Klicken Sie mit der rechten Maustaste auf den AMC und wählen Sie **New entrance** (Neuer Durchtritt).
3. Wählen Sie im Popup-Fenster **New entrance** (Neuer Durchtritt) das Türmodell **Parkplatz 05c** und fügen Sie einen Leser für eingehenden Verkehr hinzu, der dem Typ des am Parkplatzeingang installierten Lesers entspricht.
4. Klicken Sie auf **OK**, um das Popup-Fenster zu schließen.
5. Wählen Sie diesen neu angelegten Durchtritt in der Gerätehierarchie.

- Beachten Sie, dass das System den Leser automatisch als Eingangsleser gekennzeichnet hat.
- 6. Wählen Sie im Hauptbearbeitungsbereich auf der Registerkarte **Parking lot 05c** (Parkplatz 05c) aus dem Pull-Down-Menü **Destination** (Ziel) den Parkplatz, den Sie zuvor erstellt haben.
- 7. Klicken Sie erneut mit der rechten Maustaste auf den AMC und erstellen Sie einen weiteren Durchtritt vom Typ **Parkplatz 05c** wie oben.
  - Beachten Sie, dass Sie dieses Mal nur einen Leser für ausgehenden Verkehr auswählen können.
  - Klicken Sie auf **OK**, um das Popup-Fenster zu schließen.
- 8. Wählen Sie diesen zweiten neu angelegten Durchtritt in der Gerätehierarchie.
  - Beachten Sie, dass das System den zweiten Leser automatisch als Ausgangsleser festgelegt hat.

## 10 Konfigurieren von Bedienern und Dialogstationen

### Einführung in Administrationsrechte der Zutrittskontrolle

Administrationsrechte für das Zutrittskontrollsystem bestimmen, welche Systemdialoge geöffnet werden dürfen und welche Funktionen dort ausgeführt werden können.

Rechte können sowohl Bedienern als auch Dialogstationen zugewiesen werden.

Die Rechte einer Dialogstation können die Rechte ihres Bedieners vorübergehend einschränken, da sicherheitskritische Vorgänge nur von besonders sicheren Dialogstationen aus durchgeführt werden sollten.

Rechte werden Bedienern und Dialogstationen in Bundles zugewiesen, die **Profile** genannt werden. Jedes Profil ist auf die Aufgaben einer bestimmten Art von Bediener oder Dialogstation zugeschnitten.

Jeder Bediener oder jede Dialogstation kann mehrere Berechtigungsprofile haben.

### Gesamtverfahren und Dialogpfade

1. Erstellen Sie die Dialogstationen im Geräteeditor:

**Configuration** (Konfiguration) > **Device data** (Gerätedaten) > **Workstations**



(Dialogstationen)

2. Erstellen Sie Dialogstationsprofile im Dialog:

**Operators and workstations** (Bediener und Dialogstationen) > **Workstation profiles** (Dialogstationsprofile).

3. Weisen Sie Profile zu Dialogstationen im Dialogfeld zu:

**Operators and workstations** (Bediener und Dialogstationen) > **Workstation rights** (Dialogstationsrechte)

4. Erstellen Sie Benutzerprofile im Dialog:

**Operators and workstations** (Bediener und Dialogstationen) > **User profiles** (Benutzerprofil).

5. Weisen Sie Profile zu Bedienern im Dialog zu:

**Operators and workstations** (Bediener und Dialogstationen) > **User rights** (Benutzerrechte)

### 10.1 Erstellen der Dialogstationen

Dialogstationen sind die Computer, von denen aus das Bedienpersonal das Zugangskontrollsystem bedient.

Zuerst muss eine Dialogstation "erstellt" werden, das heißt, der Computer ist im Zutrittskontrollsystem registriert.

#### Dialogpfad

**Configuration** (Konfiguration) > **Device data** (Gerätedaten) > **Workstations** (Dialogstationen)

#### Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf **DMS** und wählen Sie **New object** (Neues Objekt) aus dem Kontextmenü oder klicken Sie auf **+** in der Symbolleiste.
2. Geben Sie Werte für die Parameter ein:
  - Der **Name** der Dialogstation muss genau mit dem Rechnernamen übereinstimmen.
  - **Beschreibung** ist optional. Sie kann beispielsweise verwendet werden, um die Funktion und den Ort der Dialogstation zu beschreiben.

- **Anmeldung über Leser** Deaktivieren Sie das Kontrollkästchen, es sei denn, Bediener müssen sich bei dieser Dialogstation mithilfe von Ausweisen bei einem Bekanntmachungsleser anmelden, der mit dieser Dialogstation verbunden ist. Einzelheiten finden Sie im Bereich 2-fach-Authentifizierung.
- **Automatische Abmeldung nach:** Die Anzahl der Sekunden, nach der eine Anmeldung über einen Bekanntmachungsleser automatisch beendet wird. Für eine unbegrenzte Zeit lassen Sie den Wert auf 0.

## 10.2 Erstellen von Dialogstationsprofilen

### Einführung in Dialogstationsprofile

Je nach physischem Standort sollte eine Dialogstation zur Zutrittskontrolle sorgfältig hinsichtlich ihrer Verwendung konfiguriert werden, zum Beispiel:

- Welche Bediener dürfen sie benutzen?
- Welche Anmeldeinformationen sind erforderlich, um sie zu verwenden?
- Welche Zutrittskontrollaufgaben können von dieser ausgeführt werden?

Ein Dialogstationsprofil ist eine Sammlung von Rechten, die Folgendes definieren:

- Menüs des Dialog-Managers und Dialoge, die an einer Dialogstation verwendet werden können
- Welche(s) Benutzerprofil(e) muss/müssen ein Bediener haben, um sich an dieser Dialogstation anzumelden?

### Hinweis!




Dialogstationsprofile überschreiben Benutzerprofile

Ein Bediener kann nur diejenigen seiner Benutzerprofilrechte verwenden, die auch im Dialogstationsprofil des Computers enthalten sind, auf dem er angemeldet ist. Wenn die Dialogstations- und Bedienerprofile keine gemeinsamen Rechte haben, fehlen dem Benutzer alle Rechte an dieser Dialogstation.

### Dialogpfad

**Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen) > **Workstation profiles** (Dialogstationsprofile)

### Erstellen eines Dialogstationsprofils

1. Wenn Sie ein neues Profil erstellen möchten, klicken Sie auf 
2. Geben Sie einen Profilnamen im Feld **Profile Name** (Profilname) (obligatorisch) ein
3. Geben Sie eine Profilbeschreibung in das Feld **Description** (Beschreibung) ein (optional, aber empfohlen)

4. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

### Vergeben von Ausführungsrechten für Systemfunktionen

1. Wählen Sie in der Liste **Functions** (Funktionen) die Funktionen aus, auf die diese Dialogstation zugreifen soll, und doppelklicken Sie auf sie, um den Wert in der Spalte **Execute** (Ausführen) auf **Yes** festzulegen.
  - Stellen Sie ebenfalls sicher, dass alle Funktionen, auf die nicht zugegriffen werden soll, auf **No** festgelegt sind.

2. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

### Vergeben von Benutzerprofilen an Dialogstationsprofile

Im Bereich **Benutzerprofil**.

Das Feld **Assigned Profiles** (Zugewiesene Profile) enthält eine Liste aller Benutzerprofile, die berechtigt sind, sich bei einem Dialogstationsprofil anzumelden.

Das Feld **Available Profiles** (Verfügbare Profile) enthält alle anderen Profile. Diese sind noch nicht berechtigt, sich mit diesem Dialogstationsprofil bei einer Dialogstation anzumelden.

1. Klicken Sie auf die Pfeilschaltflächen zwischen den Listen, um ausgewählte Profile von einer Liste in die andere zu übertragen.

2. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern



#### Hinweis!

Die Standardadministratorprofile für den Benutzer (**UP-Administrator**) und die Dialogstation (**WP-Administrator**) können nicht geändert oder gelöscht werden.

Das Profil **WP-Administrator** ist unwiderruflich an die Server-Dialogstation gebunden. Hiermit wird gewährleistet, dass mindestens ein Benutzer existiert, der sich bei dieser Server-Dialogstation anmelden kann.

## 10.3

### Zuweisen von Dialogstationsprofilen

Verwenden Sie diesen Dialog, um die Zuweisung von Dialogstationsprofilen zu Dialogstationen zu verwalten. Jede Dialogstation muss mindestens ein Dialogstationsprofil haben. Wenn es mehrere Profile hat, gelten alle Rechte in diesen Profilen gleichzeitig.

#### Dialogpfad

**Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen)  
> **Workstation rights** (Dialogstationsrechte)

#### Vorgehensweise

Die Liste **Assigned Profiles** (Zugewiesene Profile) enthält alle Dialogstationsprofile, die bereits zu dieser Dialogstation gehören.

Die Liste **Available Profiles** (Verfügbare Profile) enthält alle Dialogstationsprofile, die dieser Dialogstation noch nicht zugewiesen wurden.

1. Wählen Sie in der Liste der Dialogstationen die Dialogstation aus, die Sie konfigurieren möchten
2. Klicken Sie auf die Pfeiltasten zwischen den Listen **Assigned** (Zugewiesen) und **Available** (Verfügbar), um ausgewählte Profile von einem zum anderen zu übertragen.

3. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern



#### Hinweis!

Die Standardadministratorprofile für den Benutzer (**UP-Administrator**) und die Dialogstation (**WP-Administrator**) können nicht geändert oder gelöscht werden.

Das Profil **WP-Administrator** ist unwiderruflich an die Server-Dialogstation gebunden. Hiermit wird gewährleistet, dass mindestens ein Benutzer existiert, der sich bei dieser Server-Dialogstation anmelden kann.

## 10.4 Erstellen von Benutzer(Bediener-)profilen

### Einführung in Benutzerprofile

**Hinweis:** Der Begriff **Benutzer** ist gleichzusetzen mit **Bediener**, wenn es um Benutzerrechte geht.

Ein Benutzerprofil ist eine Sammlung von Rechten, die Folgendes definieren:



- Die Menüs des Dialog-Managers und die Dialoge, die für den Bediener sichtbar sind.
- Die Fähigkeiten des Bediener in diesen Dialogen, im Wesentlichen die Rechte zum Ausführen, Ändern, Hinzufügen und Löschen der Elemente dieser Dialoge.

Benutzerprofile sollten sorgfältig konfiguriert werden, abhängig von der Erfahrung, Sicherheitsfreigabe und den Verantwortlichkeiten der Person:

### Dialogpfad

Configuration (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen) > **User profiles** (Benutzerprofile)

### Vorgehensweise


1. Wenn Sie ein neues Profil erstellen möchten, klicken Sie auf 
2. Geben Sie einen Profilnamen im Feld **Profile Name** (Profilname) (obligatorisch) ein
3. Geben Sie eine Profilbeschreibung in das Feld **Description** (Beschreibung) ein (optional, aber empfohlen)
4. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern



### Hinweis!

Wählen Sie Profilnamen, die die Funktionen und Einschränkungen des Profils klar und genau beschreiben.

### Hinzufügen von Bearbeitungs- und Ausführungsrechten für Systemfunktionen

1. Wählen Sie im Listenbereich die Funktionen (erste Spalte) und die Funktionen innerhalb dieser Funktion (**Ausführen, Ändern, Hinzufügen, Löschen**), die für dieses Profil zugänglich sein sollen. Doppelklicken Sie auf diese, um ihre Einstellungen in **Yes** zu ändern.
  - Stellen Sie ebenfalls sicher, dass alle Funktionen, auf die nicht zugegriffen werden soll, auf **No** festgelegt sind.
2. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

## 10.5 Zuweisen von Benutzer(Bediener-)profilen

**Hinweis:** Der Begriff **Benutzer** ist gleichzusetzen mit **Bediener**, wenn es um Benutzerrechte geht.

### Voraussetzungen

- Der Bediener, der dieses Benutzerprofil erhalten soll, wurde als eine **Person** im Zutrittskontrollsystem definiert.
- Im Zutrittskontrollsystem wurde ein geeignetes Benutzerprofil definiert.

- Beachten Sie, dass das uneingeschränkte Benutzerprofil **UP-Administrator** immer zugewiesen werden kann, aber diese Vorgehensweise ist aus Sicherheitsgründen veraltet.

### Dialogpfad

**Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen)  
> **User rights** (Benutzerrechte)

### Vorgehensweise

1. Laden Sie den Personaldatensatz des vorgesehenen Benutzers in den Dialog.
2. Beschränken Sie bei Bedarf die Gültigkeit des Benutzerprofils, indem Sie Daten in die Felder **Valid from** (Gültig ab) und **Valid until** (Gültig bis) eingeben.

### Zuweisen von Benutzerprofilen zu Bedienern

Im Bereich **User Profiles** (Benutzerprofile):

Die Liste **Assigned Profiles** (Zugeordnete Profile) enthält alle Benutzerprofile, die diesem Benutzer zugewiesen wurden.

Das Feld **Available Profiles** (Verfügbare Profile) enthält alle Profile, die für die Zuweisung verfügbar sind.

1. Klicken Sie auf die Pfeilschaltflächen zwischen den Listen, um ausgewählte Profile von einer Liste in die andere zu übertragen.
2. Aktivieren Sie das Kontrollkästchen **Global administrator** (Globaler Administrator), um diesem Bediener Schreib – und Lesezugriff auf die Personaldatensätze zu geben, in denen das Attribut **administered globally** (global verwaltet) aktiviert ist. Der standardmäßige Bedienerzugriff auf solche Personalakten ist schreibgeschützt.

3. Klicken Sie zum Speichern Ihrer Änderungen auf  .

### Zuweisen von API-Nutzungsrechten zu Bedienern

Wenn er konfiguriert und lizenziert ist, kann externer Programmcode Funktionen des Zutrittskontrollsystems über eine Application Programming Interface oder API aufrufen. Das externe Programm agiert über einen Proxy-Operator innerhalb des Systems. Die Dropdown-Liste **API usage** (API-Nutzung) steuert die Funktionen des aktuellen Bediener, wenn er als Proxy-Operator von externem Code verwendet wird.

**Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen)  
> **User rights** (Benutzerrechte)

- Wählen Sie eine Einstellung aus der Liste **API usage** (API-Nutzung).

Die Auswahlmöglichkeiten sind:

**Kein Zutritt** Der Bediener kann nicht von der API zur Ausführung von Systemfunktionen verwendet werden.

**Nur Lesezugriff** Der Bediener kann von der API verwendet werden, um Systemdaten zu lesen, aber nicht, um sie hinzuzufügen, zu ändern oder zu löschen.

**Unbeschränkt** Der Bediener kann von der API zum Lesen, Hinzufügen, Ändern und Löschen von Systemdaten verwendet werden.

- Klicken Sie zum Speichern Ihrer Änderungen auf  .

## 10.6 Festlegen von Passwörtern für Bediener

Wie werden sichere Passwörter für sich selbst und andere festgelegt?

### Einführung

Das System benötigt mindestens einen Bediener. Der Standardbediener in einer neuen Installation hat den Benutzernamen **Administrator** und das Passwort **Administrator**. Der erste Schritt bei der Konfiguration des Systems sollte immer darin bestehen, sich mit diesen Zugangsdaten anzumelden und das Passwort für **Administrator** gemäß den Passwortrichtlinien Ihrer Organisation zu ändern.

Danach können Sie weitere privilegierte und nicht privilegierte Bediener hinzufügen.

### Vorgehensweise zum Ändern des eigenen Passworts.

#### Voraussetzungen

Sie sind beim Dialog-Manager angemeldet.

#### Vorgehensweise

1. Wählen Sie im Dialog-Manager-Menü: **File** (Datei) > **Change password** (Passwort ändern)
2. Geben Sie im Popup-Fenster das aktuelle Passwort, das neue Passwort und zur Bestätigung erneut das neue Passwort ein.
3. Klicken Sie auf **Change** (Ändern).

Beachten Sie, dass diese Vorgehensweise die einzige Möglichkeit ist, das Administratorpasswort zu ändern.


### Vorgehensweise zum Ändern der Passwörter anderer Bediener.

#### Voraussetzungen

Um die Passwörter anderer Benutzer zu ändern, müssen Sie im Dialog-Manager über ein Konto mit Administratorrechten angemeldet sein.

#### Vorgehensweise

1. Navigieren Sie im Hauptmenü des Dialog-Managers zu **Configuration** (Konfiguration) > **Operators and Workstations** (Bediener und Dialogstationen) > **User rights** (Benutzerrechte)
2. Verwenden Sie im Hauptdialogfeld die Symbolleiste, um den Bediener zu laden, dessen Passwort Sie ändern möchten.
3. Klicken Sie auf **Change password...** (Passwort ändern...).
4. Geben Sie im Popup-Fenster das neue Passwort und zum Bestätigen erneut das neue Passwort ein.
5. Geben Sie im Popup-Fenster den Gültigkeitszeitraum für das neue Passwort ein, entweder **Unlimited** (Unbegrenzt) oder eine Anzahl von Tagen.
  - Für Produktionsumgebungen wird dringend empfohlen, einen Gültigkeitszeitraum festzulegen.
6. Klicken Sie auf **OK**, um das Popup-Fenster zu schließen.

Klicken Sie im Hauptdialogfenster auf das Symbol , um den Benutzerdatensatz zu speichern.

Beachten Sie, dass sich die Datumsauswahl **Valid from** (Gültig ab) und **Valid until** (Gültig bis) unter der Schaltfläche **Change password...** (Passwort ändern) auf die Gültigkeit der Benutzerrechte in diesem Dialog bezieht, nicht auf das Passwort.



**Weitere Informationen**

Legen Sie Passwörter immer entsprechend der Passwortrichtlinie Ihrer Organisation fest. Eine Anleitung zum Erstellen einer solchen Richtlinie finden Sie beispielsweise in den Anleitungen von Microsoft unter:

<https://www.microsoft.com/en-us/research/publication/password-guidance/>

XREF zum Erstellen neuer Benutzer

# 11 Konfigurieren von Ausweiscodes

Die Codierung der Zutrittskontrollausweise stellt sicher, dass alle Ausweisdaten eindeutig sind.

## Dialogpfad

**Main Menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Options** (Optionen) > **Card coding configuration** (Konfiguration des Ausweiscodes)

## Eingeben von Zahlen im Dialog

Um Fehler bei der Ausweiscodierung zu vermeiden, können alle Zahlen in dezimalen oder hexadezimalen Formaten eingegeben werden. Wählen Sie die Optionsfelder **Hexadecimal** (Hexadezimal) oder **Decimal** (Dezimal) nach den Anweisungen des Ausweisherstellers aus. Bereits eingegebene Werte werden automatisch intern umgerechnet.

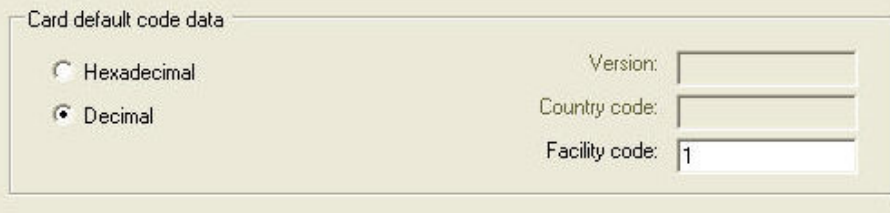

Der Hauptdialog ist in zwei Gruppen unterteilt, die im Folgenden näher beschrieben werden:

- **Ausweis-Standardcodedaten**
- **Überprüfung der Zugehörigkeit zur Anlage**

## Ausweis-Standardcodedaten

Verwenden Sie diese Felder, um Werte für **Version**, **Country code** (Ländercode) und **Facility code** (Einrichtungscodierung) einzugeben, welche der Ausweisnummer zugeordnet sind, wenn der Ausweis im System angemeldet ist.

Wenn der Ausweis manuell an einer Bediener-Dialogstation registriert wird, wird ein Dialogfeld mit den Standardwerten angezeigt, die für jeden Ausweis angepasst werden können.

|   |  |
|---|--|
| <p><b>Vollständige Codenr. (Standard)</b></p> | <p>Nur der Kundencode wird eingegeben (hexadezimal oder dezimal).</p>  <p><b>Eingeben von Codierungsdaten:</b><br/>Der Kundencode wird vom Hersteller als Dezimalwert bereitgestellt: 56720. Wählen Sie das Optionsfeld <b>Dezimal</b>, und geben Sie den Kundencode ein. Klicken Sie zum Speichern der Daten auf die Schaltfläche „Übernehmen“.</p> |
| <p><b>Aufgeteilte Codenr.</b></p>             | <p>Version, Länder- und Kundencode müssen als <b>Dezimalwert</b> eingegeben werden.</p>  <p><b>Eingeben von Codedaten:</b><br/>Die Daten werden vom Hersteller als Dezimalwerte bereitgestellt:<br/>Version: 2<br/>Ländercode: 99</p>  |

Kundencode: 56720

Geben Sie die Daten in die entsprechenden Textfelder ein.

Klicken Sie zum Speichern der Daten auf die Schaltfläche „Übernehmen“.

#### Hinweise zum Eingeben von Defaultcodedaten:

Die Standarddaten werden in der Registrierung des Betriebssystems gespeichert, und jede Ausweisnummer wird zum Codierungszeitpunkt hinzugefügt. Die Registrierung erfolgt als **8-stelliger hexadezimaler** Wert, der bei Bedarf mit führenden Nullen aufgefüllt wird.

Wenn die Codenummern vollständig übertragen werden, konvertiert das System den Wert vom dezimalen in das hexadezimale Format, füllt den Wert mit führenden Nullen auf, bis insgesamt 8 Stellen erreicht sind, und speichert den entsprechenden Systemparameter.

- Beispiel:
  - Eingabe: 56720
  - Konvertierung: DD90
  - Speicherung als: 0000DD90

Wenn die Codenummern getrennt (in geteilter Form) übertragen werden, dann nur im **dezimalen** Format. Sie werden in eine 10-stellige Dezimalzahl konvertiert, die wie folgt strukturiert ist:

- Version: 2 Stellen
- Ländercode: 2 Stellen
- Kundencode: 6 Stellen
- Sollte der 10-stellige Wert noch Leerstellen aufweisen, werden diese mit führenden Nullen aufgefüllt.
  - Beispiel: 0299056720

Dieser 10-stellige Dezimalwert wird konvertiert und als 8-stelliger Hexadezimalwert gespeichert.

- Beispiel:
  - Dezimal: 0299056720
  - Hexadezimal: 11D33E50



#### Hinweis!

Das System validiert, dass bei geteilten Codenummern Hexadezimalwerte eingegeben werden. Hiermit soll unterbunden werden, dass Benutzer ungültige Ländercodes über 63 hexadezimal oder 99 dezimal und ungültige Kundencodes über F423F hexadezimal oder 999.999 dezimal eingeben.



#### Hinweis!

Wird der Ausweis über einen angeschlossenen Dialogleser erfasst, werden die Standardwerte automatisch zugewiesen. Die Standardwerte können nicht überschrieben werden, wenn die Erfassung über einen Leser erfolgt.

Zum Überschreiben sollte der Erfassungstyp auf **Dialog** umgeschaltet werden.

Die manuelle Eingabe der Ausweisnummer erfolgt im Dezimalformat.

Beim Speichern der Daten wird ein 10-stelliger Dezimalwert (mit führenden Nullen) erstellt, der anschließend in einen 8-stelligen Hexadezimalwert konvertiert wird. Dieser Wert wird jetzt mit den Standard-Codedaten als 16-stellige Codenummer des Ausweises gespeichert.

- Beispiel:
  - Eingabe der Ausweisnummer: 415
  - 10-stellig: 0000000415
  - Konvertierung ins Hexadezimalformat: 0000019F

- Kombination mit den Standard-Codedaten (siehe oben) und Speicherung als Codenummer des Ausweises: 11D33E50000019F

### Überprüfung der Zugehörigkeit zur Anlage

Die Überprüfung der Zugehörigkeit zur Anlage bedeutet nur, dass der Ausweis nur auf die Zugehörigkeit zu einer Firma oder Organisation geprüft wird und keine Person identifiziert wird. Benutze deshalb **Membership check only** (Nur Zugehörigkeitsprüfung) nicht für Leser, die Zutritt zu Hochsicherheitsbereichen gewähren.

Mit diesem Optionsfeld können Sie bis zu vier Unternehmens- oder Kundencodes eingeben. Die Daten können als Dezimal- oder Hexadezimalzahl eingegeben werden, werden jedoch als Dezimalwerte in der Registry des Betriebssystems gespeichert.



Wählen Sie den Leser im Geräteeditor, DevEdit, und aktivieren Sie den Leserparameter **Membership check** (Zugehörigkeit zur Anlage prüfen).

Nur die Unternehmens-/Kundencodes der Ausweisdaten werden gelesen und anhand der gespeicherten Werte überprüft.



### Hinweis!

Die **Zugehörigkeitsprüfung** funktioniert nur mit vordefinierten Ausweisdefinitionen im System (grauer Hintergrund), aber nicht mit benutzerdefinierten Definitionen.

# 12 Konfigurieren der Controller

## Einführung

Die Controller im Zutrittskontrollsystem sind die virtuellen und physischen Geräte, die Befehle an die periphere Hardware an Durchritten (Leser und Türen) senden und Anfragen von den Lesern und Türen an die zentrale Entscheidungssoftware zurücksenden.

Die Controller speichern Kopien der Geräte- und Ausweisinhaberinformationen der zentralen Software und können, wenn sie so konfiguriert sind, Zutrittskontrollentscheidungen treffen, selbst wenn sie vorübergehend von der zentralen Software getrennt sind.

Die Entscheidungsfindungssoftware ist das Datenverwaltungssystem.

Controller sind von zweierlei Art:

- Main Access Controller, bekannt als die MACs und sein redundantes Backup-Gegenstück, der RMAC.
- Lokale Zutrittscontroller, bekannt als LACs oder AMCs.

Controller werden im Geräteeditor DevEdit konfiguriert

## Dialogpfad zum Geräteeditor

**Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten) >



**Device tree** (Gerätebaum)

## Verwenden des Geräteeditors DevEdit

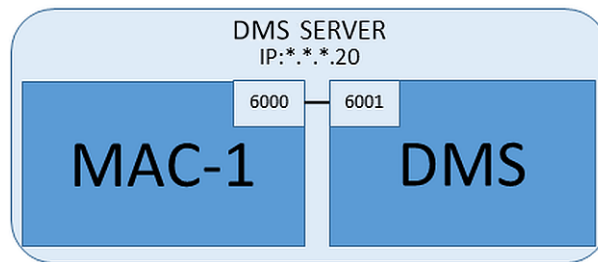
Die grundlegende Verwendung von DevEdit wird im Abschnitt **Verwenden des Geräteeditors** unter dem Link unten beschrieben.

## Siehe

- *Verwenden des Geräteeditors, Seite 21*

## 12.1 Konfigurieren von MACs und RMACs

### 12.1.1 Konfigurieren eines MAC auf dem DMS-Server



Für eine minimale Systemkonfiguration wird ein MAC benötigt. In diesem Fall kann sich der MAC auf dem DMS-Server befinden.

## Vorgehensweise

Öffnen Sie auf dem DMS-Server den Geräteeditor und erstellen Sie einen MAC im Gerätebaum, wie im Abschnitt **Verwenden des Geräteeditors** beschrieben.

Wählen Sie den MAC im Geräteeditor aus. Geben Sie auf der Registerkarte **MAC** die folgenden Parameterwerte ein:

| Parameter | Beschreibung   |
|-----------|--|
| Name      | Der Name, der im Gerätebaum angezeigt werden soll, zum Beispiel MAC-1. |

| Parameter                          | Beschreibung   |
|------------------------------------|--|
| Beschreibung                       | Optionale Beschreibung für Systembediener  |
| Mit RMAC<br>(Kontrollkästchen)     | <b>&lt;Leer lassen&gt;</b>   |
| RMAC-Port                          | <b>&lt;Leer lassen&gt;</b>   |
| Aktiv (Kontrollkästchen)           | <b>Deaktivieren</b> Sie dieses Kontrollkästchen, um die Echtzeitsynchronisierung zwischen diesem MAC und DMS vorübergehend zu unterdrücken. Dies ist nach DMS-Aktualisierungen auf größeren Systemen von Vorteil, um zu vermeiden, dass alle MACs auf einmal gespeichert werden. |
| Geräte laden<br>(Kontrollkästchen) | <b>Deaktivieren</b> Sie dieses Kontrollkästchen, um die Echtzeitsynchronisierung zwischen diesem MAC und seinen untergeordneten Geräten vorübergehend zu unterdrücken. Dadurch wird die Zeit verkürzt, die zum Öffnen eines MAC im Geräteeditor benötigt wird.                   |
| IP address (IP-Adresse)            | localhost 127.0.0.1  |
| Time zone (Zeitzone)               | <b>WICHTIG:</b> Die Zeitzone des MAC und aller untergeordneten AMCs.   |
| Mandant                            | (falls zutreffend) Der Mandant, zu dem der MAC gehört.   |

Da dieser lokale MAC keinen redundanten Failover-MAC hat, ist es nicht notwendig, das MACInstaller-Tool dafür auszuführen. Lassen Sie einfach die beiden RMAC-Parameter auf der Registerkarte **MAC** leer.

### 12.1.2

#### Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs

In diesem Abschnitt wird die Vorbereitung von Computern für die Verwendung als MAC-Server beschrieben.

Standardmäßig wird der erste MAC in einem Access Engine-System auf demselben Computer wie sein Datenverwaltungsserver (DMS) ausgeführt, doch für eine verbesserte Ausfallsicherheit wird empfohlen, den MAC auf einem separaten Computer auszuführen, der Zutrittskontrollaufgaben übernehmen kann, wenn der DMS-Computer ausfällt.

Unterschiedliche Computer, auf denen sich MACs oder RMACs befinden, werden unabhängig davon als MAC-Server bezeichnet, ob sie einen MAC oder einen RMAC hosten.

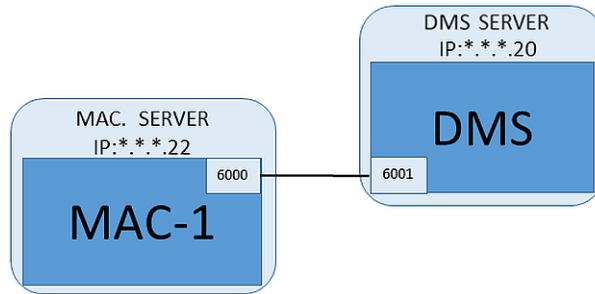
Um eine Failover-Funktion zu ermöglichen, **müssen** MACs und RMACs auf separaten MAC-Servern ausgeführt werden.

Stellen Sie sicher, dass die folgenden Bedingungen auf allen teilnehmenden MAC-Servern erfüllt sind:

1. Auf allen Servern ist dieselbe Version des Betriebssystems vom DMS-Server mit den neuesten Windows-Updates installiert.
2. Der Administrator-Benutzer auf allen Servern hat dasselbe Passwort.
3. Sie sind als Administrator angemeldet (verwenden Sie bei MSTC nur /Admin /Console-Sitzungen)
4. Deaktivieren Sie IPv6. Notieren Sie sich sorgfältig die IPv4-Adresse jedes Servers.

5. Aktivieren Sie .NET 3.5 auf allen teilnehmenden Computern.  
**Hinweis:** Unter Windows 7 ist dies mit einer Installation verbunden. Unter Windows 10- und Windows Server-Betriebssystemen wird es als Funktion aktiviert.
6. Starten Sie den Computer neu.

### 12.1.3 Konfigurieren eines MAC auf seinem eigenen MAC-Server



- Der MAC-Servercomputer wurde wie im Abschnitt Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs beschrieben vorbereitet.
1. Deaktivieren Sie den MAC auf dem DMS-Server, indem Sie die Kontrollkästchen **Activate** (Aktivieren) und **Load devices** (Geräte laden) für diesen MAC im Geräteeditor deaktivieren.
  2. Stoppen Sie den MAC-Prozess auf dem MAC-Server mit dem Windows-Programm `services.msc`.
  3. Starten Sie die `MACInstaller.exe`
    - Für ACE befindet sich diese auf den BIS-Installationsmedien `\AddOns\ACE\MultiMAC\MACInstaller` (siehe Abschnitt Verwenden des MACInstaller-Tools unten).
  4. Befolgen Sie die Schritte in den Bildschirmen des Tools und geben Sie Werte für die folgenden Parameter ein.

| Bildschirmnr. | Parameter   | Beschreibung   |
|---------------|---|--|
| 1             | <b>Destination Folder</b> (Zielordner)                        | Das lokale Verzeichnis, in dem der MAC installiert werden muss. Geben Sie nach Möglichkeit den Standardwert ein.   |
| 2             | <b>Server</b>   | Der Name oder die IP-Adresse des Servers, auf dem der DMS ausgeführt wird.   |
| 2             | <b>Port (Port to DMS)</b> (Port zu DMS)                       | Der Port auf dem DMS-Server, der zum Empfang der Kommunikation vom MAC verwendet wird. Verwenden Sie 6001 für den ersten MAC auf der DMS und steigern Sie den Wert um 1 für jeden folgenden MAC. |
| 2             | <b>Number (MAC System Number)</b> (Nummer [MAC-Systemnummer]) | Legen Sie 1 für diesen und alle MACs fest (anders als bei RMACs).  |

| Bildschirmnr. | Parameter  | Beschreibung  |
|---------------|--|---|
| 2             | <b>Twin (Name or IP address of partner MAC)</b> (Zwilling [Name oder IP-Adresse des Partner-MACs]) | Lassen Sie dieses Feld leer, solange dieser MAC keinen RMAC haben soll.   |
| 2             | <b>Configure Only</b> (Nur konfigurieren) (Optionsfeld)  | Nicht auswählen, da Sie keinen MAC auf dem Haupt-DMS-Einwahlserver konfigurieren.   |
| 2             | <b>Update Software</b> (Software aktualisieren) (Optionsfeld)                                      | Wählen Sie diese Option, da Sie einen MAC auf seinem eigenen Computer (MAC-Server) und nicht auf dem Haupt-DMS-Einwahlserver konfigurieren. |

5. Starten Sie den MAC-Server nach Beenden des Tools neu oder starten Sie alternativ den MAC-Prozess auf dem MAC-Server mit dem Windows-Programm `services.msc`.
6. Wählen Sie den MAC auf dem DMS-Server im Geräteeditor aus.
7. Geben Sie auf der Registerkarte **MAC** Werte für die folgenden Parameter ein:

| Parameter                       | Beschreibung   |
|---------------------------------|--|
| Name                            | Der Name, der im Gerätebaum angezeigt werden soll, zum Beispiel MAC-1. |
| Beschreibung                    | Optionale Beschreibung für ACE-Bediener                                |
| Mit RMAC (Kontrollkästchen)     | <b>&lt;Leer lassen&gt;</b>   |
| RMAC-Port                       | <b>&lt;Leer lassen&gt;</b>   |
| Aktiv (Kontrollkästchen)        | Kontrollkästchen jetzt aktivieren                                      |
| Geräte laden (Kontrollkästchen) | Kontrollkästchen jetzt aktivieren                                      |
| IP address (IP-Adresse)         | Die IP-Adresse des MAC-Servercomputers.                                |
| Time zone (Zeitzone)            | <b>WICHTIG:</b> Die Zeitzone des MAC und aller untergeordneten AMCs.   |
| Mandant                         | (falls zutreffend) Der ACE-Mandant, zu dem der MAC gehört.             |

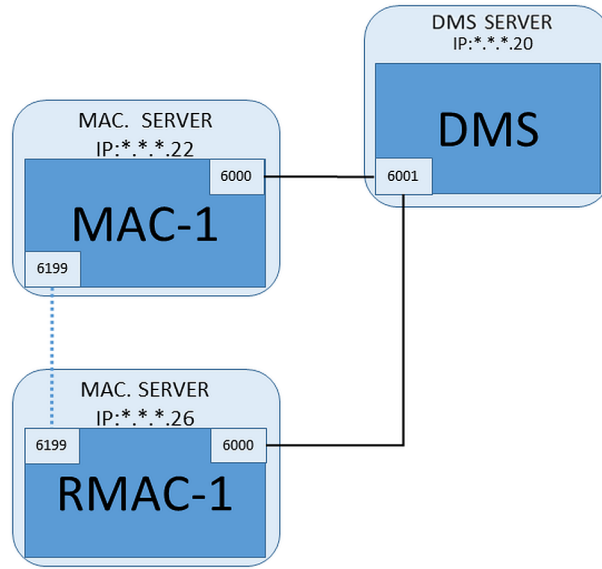
### 12.1.4 Hinzufügen von RMACs zu MACs



**Hinweis!**

Fügen Sie keine RMACs zu normalen MACs hinzu, bis die normalen MACs installiert sind und ordnungsgemäß ausgeführt werden. Andernfalls kann die Datenreplizierung verhindert oder beschädigt werden.





- Der MAC für diesen RMAC wurde wie in den vorherigen Abschnitten beschrieben installiert und wird ordnungsgemäß ausgeführt.
  - Der MAC-Servercomputer für den RMAC wurde wie im Abschnitt Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs beschrieben vorbereitet.
- MACs können mit redundanten MACs (RMACs) gekoppelt werden, um eine Failover-Funktion und damit eine belastbarere Zutrittskontrolle zu bieten. In diesem Fall werden die Zutrittskontrolldaten automatisch zwischen den beiden repliziert. Wenn eines der Paare ausfällt, übernimmt das andere die Steuerung über die lokalen Zutrittscontroller darunter.

**Auf dem DMS-Server im Configuration Browser**

1. Wählen Sie im Geräteeditor den MAC aus, zu dem der RMAC hinzugefügt werden soll.
2. Ändern Sie auf der Registerkarte **MAC** die Werte für die folgenden Parameter:

| Parameter   | Beschreibung   |
|---|--|
| <b>With RMAC</b> (Mit RMAC) (Kontrollkästchen)        | <b>Deaktivieren</b> Sie dieses Kontrollkästchen, bis Sie den entsprechenden RMAC auf dem redundanten Failover-Anschaltserver installiert haben.  |
| <b>Active</b> (Aktiv) (Kontrollkästchen)              | <b>Deaktivieren</b> Sie dieses Kontrollkästchen, um die Echtzeitsynchronisierung zwischen diesem MAC und DMS vorübergehend zu unterdrücken. Dies ist nach DMS-Aktualisierungen auf größeren Systemen von Vorteil, um zu vermeiden, dass alle MACs auf einmal gespeichert werden. |
| <b>Load devices</b> (Geräte laden) (Kontrollkästchen) | <b>Deaktivieren</b> Sie dieses Kontrollkästchen, um die Echtzeitsynchronisierung zwischen diesem MAC und seinen untergeordneten Geräten vorübergehend zu unterdrücken. Dadurch wird die Zeit verkürzt, die zum Öffnen eines MAC im Geräteeditor benötigt wird.                   |

3. Klicken Sie auf die Schaltfläche **Apply** (Übernehmen).
4. Lassen Sie den Geräteeditor geöffnet, da er später erneut benötigt wird.

**Auf dem MAC-Server für den MAC**

Gehen Sie wie folgt vor, um den MAC für die Zusammenarbeit mit einem RMAC neu zu konfigurieren.

- Führen Sie auf dem zuvor vorbereiteten MAC-Servercomputer das MACInstaller-Tool aus (siehe Verwenden des MACInstaller-Tools) und legen Sie folgende Parameter fest:
  - **Server:** Name oder IP-Adresse des DMS-Servercomputers
  - **Port:** 6001
  - **Number (Nummer):** 1 (alle MACs haben Nummer 1)
  - **Twin (Zwilling):** IP-Adresse des Computers, auf dem der RMAC ausgeführt wird.
  - **Update software** (Software aktualisieren): Wählen Sie diese Option, da Sie einen MAC-Server und nicht den DMS-Server konfigurieren.

**Auf dem MAC-Server für den RMAC**

Gehen Sie für die Konfiguration des RMAC wie folgt vor:

- Führen Sie auf dem eigenen separaten und vorbereiteten MAC-Servercomputer das MACInstaller-Tool aus (siehe Verwenden des MACInstaller-Tools) und legen Sie folgende Parameter fest:
  - **Server:** Name oder IP-Adresse des DMS-Servercomputers
  - **Port:** 6001 (wie beim MAC)
  - **Number (Nummer):** 2 (alle RMACs haben Nummer 2)
  - **Twin (Zwilling):** IP-Adresse des Computers, auf dem der Zwillings-MAC läuft.
  - **Update software** (Software aktualisieren): Wählen Sie diese Option, da Sie einen MAC-Server und nicht den DMS-Server konfigurieren.

**Rückkehr zum Geräteeditor auf dem DMS-Server**

1. **WICHTIG:** Stellen Sie sicher, dass sowohl der MAC als auch der RMAC auf ihren jeweiligen Computern ausgeführt werden und füreinander im Netzwerk sichtbar sind.
2. Ändern Sie die Parameter auf der Registerkarte **MAC** wie folgt:

| Parameter   | Beschreibung   |
|---|--|
| <b>With RMAC</b> (Mit RMAC) (Kontrollkästchen)        | <b>Selected</b> (Ausgewählt)<br>Neben der Registerkarte <b>MAC</b> erscheint die neue Registerkarte <b>RMAC</b> .                            |
| <b>RMAC Port</b>                                      | 6199 (der statische Standardwert)<br>Alle MACs und RMACs verwenden diesen Port, um zu überprüfen, ob ihre Partner aktiv und erreichbar sind. |
| <b>Active</b> (Aktiv) (Kontrollkästchen)              | <b>Selected</b> (Ausgewählt)<br>Dies ermöglicht die Synchronisierung zwischen diesem MAC und seinen untergeordneten Geräten.                 |
| <b>Load devices</b> (Geräte laden) (Kontrollkästchen) | <b>Selected</b> (Ausgewählt)<br>Dadurch wird die Zeit verkürzt, die zum Öffnen eines MAC im Geräteeditor benötigt wird.                      |

3. Geben Sie auf der Registerkarte **RMAC** Werte für die folgenden Parameter ein:

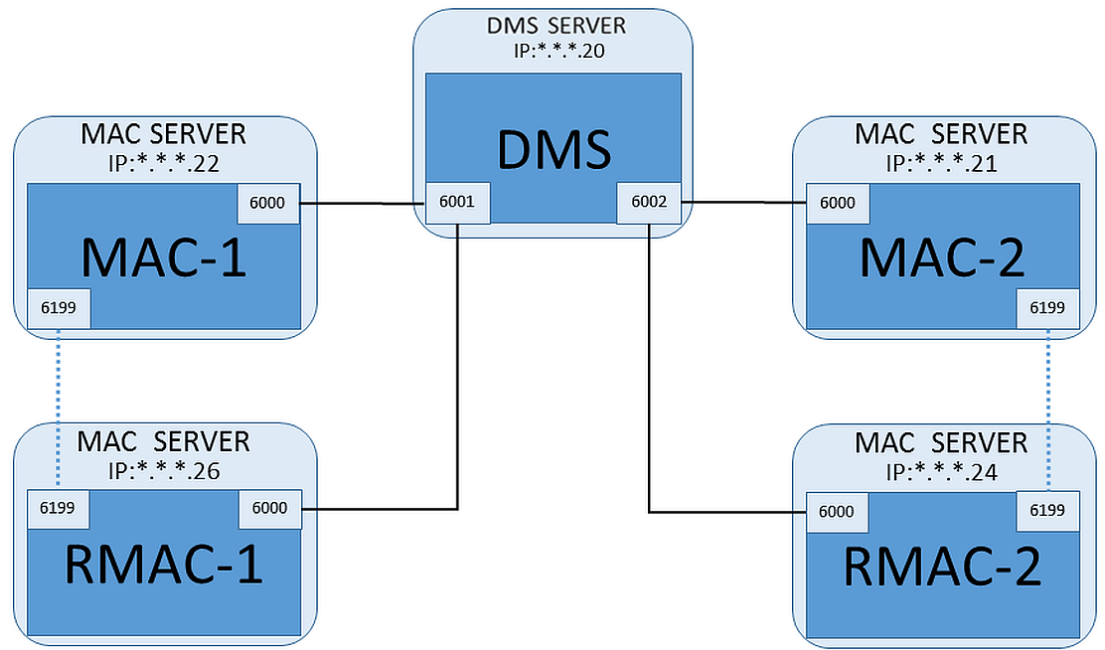
| Parameter   | Beschreibung   |
|-------------|--|
| <b>Name</b> | Der Name, der im Gerätebaum angezeigt werden soll.<br>Wenn der entsprechende MAC beispielsweise MAC-01 heißt, kann dieser RMAC RMAC-01 genannt werden. |

| Parameter                      | Beschreibung   |
|--------------------------------|--|
| <b>Beschreibung</b>            | Optionale Dokumentation für ACE-Bediener   |
| <b>IP address</b> (IP-Adresse) | Die IP-Adresse des RMAC  |
| <b>MAC Port</b>                | 6199 (der statische Standardwert)<br>Alle MACs und RMACs verwenden diesen Port, um zu überprüfen, ob ihre Partner aktiv und erreichbar sind. |

### 12.1.5

#### Hinzufügen weiterer MAC/RMAC-Paare

Abhängig von der Anzahl der zu steuernden Eingänge und dem erforderlichen Grad der Fehlertoleranz kann eine große Anzahl von MAC/RMAC-Paaren zur Systemkonfiguration hinzugefügt werden. Die genaue Anzahl, die von Ihrer Version unterstützt wird, finden Sie auf dem entsprechenden Datenblatt.



Für jedes weitere MAC/RMAC-Paar ...

1. Bereiten Sie die separaten Computer für MAC und RMAC vor, wie im Abschnitt Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs beschrieben.
2. Richten Sie den MAC wie im Abschnitt Konfigurieren eines MAC auf seinem eigenen MAC-Server beschrieben ein.
3. Richten Sie den RMAC für diesen MAC wie im Abschnitt Hinzufügen von RMACs zu MACs beschrieben ein.

Beachten Sie, dass jedes MAC/RMAC-Paar zu einem separaten Port auf dem DMS-Server überträgt. Verwenden Sie daher für den Parameter **Port (Port to DMS)** in `MACInstaller.exe`:

- 6001 für beide Computer im ersten MAC/RMAC-Paar
- 6002 für beide Computer im zweiten MAC/RMAC-Paar
- usw.

Im Geräteeditor kann der Port 6199 immer für die Parameter **MAC Port** und **RMAC Port** verwendet werden. Diese Portnummer ist für den „Handshake“ innerhalb jedes MAC/RMAC-Paars reserviert, durch den MAC bzw. RMAC wissen, ob der Partner erreichbar ist oder nicht.



**Hinweis!**

Reaktivieren von MACs nach Systemaktualisierungen  
 Nach einer Systemaktualisierung werden MACs und ihre AMCs standardmäßig deaktiviert. Denken Sie daran, sie im Configuration Browser erneut zu aktivieren, indem Sie die entsprechenden Kontrollkästchen im Geräteeditor aktivieren.

**12.1.6**

**Verwenden des MACInstaller-Tools**

MACInstaller.exe ist das Standardtool zum Konfigurieren und Neukonfigurieren von MACs und RMACs auf ihren eigenen Computern (MAC-Servern). Es sammelt Parameterwerte für einen MAC oder RMAC und nimmt die notwendigen Änderungen in der Windows-Registrierung vor.



**Hinweis!**

Vor der Neukonfiguration muss jeder laufende MAC-Prozess gestoppt werden, da das Tool Änderungen an der Windows-Registrierung vornimmt.

Das MACInstaller-Tool kann auf dem BIS-Installationsmedium unter folgendem Pfad gefunden werden:

```
\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe
```

Über eine Reihe von Bildschirmen sammelt es Werte für die folgenden Parameter.

| Bildschirmnr. | Parameter  | Beschreibung  |
|---------------|--|---|
| 1             | <b>Destination Folder</b> (Zielordner)   | Das lokale Verzeichnis, in dem der MAC installiert werden muss.   |
| 2             | <b>Server</b>  | Der Name oder die IP-Adresse des Servers, auf dem der DMS ausgeführt wird.  |
| 2             | <b>Port (Port to DMS)</b> (Port zu DMS)  | Die Portnummer auf dem DMS-Server, der für die Kommunikation zwischen dem MAC und dem DMS verwendet wird. <b>Einzelheiten finden Sie unten.</b>                     |
| 2             | <b>Number (MAC System Number)</b> (Nummer [MAC-Systemnummer])                                      | Stellen Sie 1 für alle ursprünglichen MACs ein. Stellen Sie 2 für alle redundanten Failover-MACs (RMACs) ein.   |
| 2             | <b>Twin (Name or IP address of partner MAC)</b> (Zwilling [Name oder IP-Adresse des Partner-MACs]) | Die IP-Adresse des Computers, auf dem der redundante Failover-Partner für diesen MAC-Server ausgeführt werden soll. Wenn nicht zutreffend, dieses Feld leer lassen. |
| 2             | <b>Configure Only</b> (Nur konfigurieren) (Optionsfeld)  | Wählen Sie diese Option, wenn Sie einen MAC auf dem Haupt-DMS-Einwahlservers erneut konfigurieren. <b>Einzelheiten finden Sie unten.</b>                            |

| Bildschirmnr. | Parameter   | Beschreibung   |
|---------------|---|--|
| 2             | <b>Update Software</b> (Software aktualisieren) (Optionsfeld) | Wählen Sie diese Option, wenn Sie einen MAC auf seinem eigenen Computer (MAC-Server) installieren oder erneut konfigurieren, und nicht auf dem Haupt-DMS-Einwahlserver.<br><b>Einzelheiten finden Sie unten.</b> |

Portnummern haben das folgende Nummerierungsschema:

- In einem nicht-hierarchischen System, in dem nur ein DMS-Server existiert, sendet jeder MAC und sein entsprechender RMAC von derselben Portnummer aus, normalerweise 6000. Das DMS kann mit nur einem Element von jedem MAC/RMAC-Paar gleichzeitig kommunizieren.
- Das DMS empfängt Signale vom ersten MAC oder MAC/RMAC-Paar am Port 6001, vom zweiten MAC oder MAC/RMAC-Paar am Port 6002 usw.



**Hinweis!**

DMS-Empfängerport in hierarchischen Systemen  
Beachten Sie, dass das Nummerierungsschema für DMS-Empfängerports in hierarchischen Systemen unterschiedlich ist. Weitere Informationen finden Sie unter MACs und RMACs in hierarchischen Topologien.

Durch diesen Parameter sollen die ursprünglichen MACs von den RMACs unterschieden werden:

- Alle ursprünglichen MACs haben die Nummer 1.
- Alle redundanten Failover-MACs (RMACs) haben die Nummer 2.

Wählen Sie diese Option, um die Konfiguration eines vorhandenen MAC auf dem Haupt-DMS-Server zu ändern. Insbesondere soll er dabei über einen neu installierten RMAC auf einem anderen Computer informiert werden.

Geben Sie in diesem Fall die IP-Adresse oder den Hostnamen des RMAC im Parameter **Twin** (Zwilling) an.

Wählen Sie diese Option auf einem Computer, der nicht der Haupt-DMS-Server ist, um einen RMAC zu installieren oder seine Konfiguration zu ändern.

Geben Sie in diesem Fall die IP-Adresse oder den Hostnamen des MAC-Zwillings des RMAC im Parameter **Twin** (Zwilling) an.

## 12.2 Konfigurieren der LACs

### Erstellen eines lokalen AMC-Zutrittscontrollers

Access Modular Controllers (AMCs) sind den Main Access Controllers (MACs) im Geräteeditor untergeordnet.

So erstellen Sie einen AMC:

1. Klicken Sie im Geräteeditor mit der rechten Maustaste auf einen MAC, und wählen Sie **Neues Objekt** aus dem Kontextmenü, oder
2. Klicken Sie auf die Schaltfläche **+**.

3. Wählen Sie einen der folgenden AMC-Typen aus dem angezeigten Dialog:

AMC 4W (Standard) mit vier Wiegand-Leserschnittstellen, die an maximal vier Leser angeschlossen werden können

AMC 4R4 mit vier RS485-Leserschnittstellen, die an maximal acht Leser angeschlossen werden können

**Ergebnis:** In der DevEdit-Hierarchie wird ein neuer AMC-Eintrag des ausgewählten Typs erstellt.

|                         |   |   |
|-------------------------|---|---|
| <b>AMC2 4W</b>          | <b>Access Modular Controller</b> mit vier Wiegand-Lesern.           | Maximal vier Wiegand-Leser können für den Anschluss an bis zu vier Durchtritte konfiguriert werden.<br>Der Controller unterstützt acht Eingangs- und acht Ausgangssignale. Bei Bedarf können mit Erweiterungen bis zu 48 zusätzliche Eingangs- und Ausgangssignale bereitgestellt werden. |
| <b>AMC2 4R4</b>         | <b>Access Modular Controller</b> mit vier RS485-Leserschnittstellen | Maximal acht RS485-Leser können für den Anschluss an bis zu acht Durchtritte konfiguriert werden.<br>Der Controller unterstützt acht Eingangs- und acht Ausgangssignale. Bei Bedarf können mit Erweiterungen bis zu 48 zusätzliche Eingangs- und Ausgangssignale bereitgestellt werden.   |
| <b>AMC2 8I-8O-EXT</b>   | Erweiterung für den AMC mit acht Eingangs- und Ausgangssignalen     | Zusätzliche Signale werden bereitgestellt. Bis zu drei Erweiterungen können an einen AMC angeschlossen werden.  |
| <b>AMC2 16I-16O-EXT</b> | Erweiterung für den AMC mit sechzehn Eingangs- und Ausgangssignalen |   |
| <b>AMC2 8I-8O-4W</b>    | Erweiterung für Wiegand-AMC mit acht Eingangs- und Ausgangssignalen |   |

**Aktivieren/Deaktivieren von Controllern**

Bei der ersten Erstellung hat ein neuer Controller die folgende Option (Kontrollkästchen) aktiviert: **Communication to host enabled** (Schnittstelle zum Host aktiv).

Dies öffnet die Netzwerkverbindung zwischen dem MAC und den Controllern, sodass alle geänderten oder erweiterten Konfigurationsdaten automatisch an die Controller weitergegeben werden.

Deaktivieren Sie diese Option, um Netzwerkbandbreite zu sparen und so die Leistung zu verbessern, während Sie mehrere Controller und ihre abhängigen Geräte (Durchtritte, Türen, Leser, Erweiterungskarten) erstellen. Im Geräteeditor werden Geräte dann durch grau hinterlegte Symbole gekennzeichnet.

**WICHTIG:** Stellen Sie sicher, dass Sie diese Option erneut aktivieren, wenn die Konfiguration der Geräte abgeschlossen ist. Dadurch bleiben die Controller mit Konfigurationsänderungen, die auf anderen Ebenen vorgenommen wurden, ständig auf dem neuesten Stand.

### Mischen von Controllertypen in einem System

Zutrittskontrollsysteme werden in der Regel mit nur einem Typ von Controller und Leser ausgerüstet.

Softwareupgrades sowie wachsende Systeme erfordern möglicherweise, dass vorhandene Hardwarekomponenten durch neue ergänzt werden. Selbst Konfigurationen, in denen RS485-Varianten (AMC 4R4) mit Wiegand-Varianten (AMC 4W) kombiniert werden, sind möglich, solange folgende Vorsichtsmaßnahmen beachtet werden:

- RS485-Leser übertragen ein „Telegramm“, das die gelesene Codenummer enthält.
- Wiegand-Leser übertragen ihre Daten so, dass sie mithilfe der Ausweisdefinition decodiert werden, um die Codenummer in der richtigen Form zu erhalten.
- Ein Betrieb mit gemischten Controllern kann nur funktionieren, wenn beide Codenummern identisch aufgebaut sind.

## 12.2.1






### AMC-Parameter und -Einstellungen

#### Allgemeine Parameter des AMC


The screenshot shows the configuration interface for an AMC 4-R4 controller. On the left is a tree view showing the hierarchy: DMS > MAC > AMC 4-R4-1 > DOOR1 > Door-1, OSDP V; and DOOR2 > Door-2, OSDP V;. The right pane is titled 'AMC 4-R4' and has tabs for 'Inputs', 'Outputs', and 'Terminals'. The configuration fields are as follows:

- Name: AMC 4-R4-1
- Description: AMC
- Communication to host enabled:
- Controller interface:
  - Interface type: UDP
  - PC com port: 0
  - Bus number: 1
  - IP address / host name: AMC2-DOK3
  - Port number: 10001
- Program: LCMV6221.RUN : HID, AMC-4R4
- Power supply supervision:
- No LAC accounting:
- Division: Common

**Konfiguration der AMC-Parameter**

| Parameter  | Mögliche Werte   | Beschreibung  |
|--|--|---|
| Controllername   | Alphanumerisch mit Einschränkungen:<br>1 – 16 Zeichen  | ID-Generierung (Default) gewährleistet eindeutige Namen, die jedoch einzeln überschrieben werden können. Wenn der Benutzer IDs überschreibt, liegt es in seiner Verantwortung, dafür zu sorgen, dass die IDs eindeutig sind. Es wird daher empfohlen, dass für Netzwerkverbindungen zu DHCP-Servern der Netzwerkname verwendet wird.  |
| Controller description (Controllerbeschreibung)              | Alphanumerisch:<br>0 – 255 Zeichen   | Dieser Text wird im OPC-Zweig angezeigt.  |
| Communication to host enabled (Schnittstelle zum Host aktiv) | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | <p>Standardwert = active (aktiv)</p> <p>Das Kontrollkästchen zeigt die aktuelle Einstellung an und kann auch verwendet werden, um sie zu ändern.</p> <p>Der Status der Hostverbindung wird durch folgende Symbole im Explorer-Bereich angezeigt:</p> <p>Controllervariante:<br/>active (aktiv)<br/>not active (nicht aktiv)</p> <p>AMC2 4W</p>   <p>AMC2 4R4</p>   <p>Die Deaktivierung bietet eine Möglichkeit, Geräte zu erstellen und zu parametrieren, sodass sie zu einem späteren Zeitpunkt in das Zutrittskontrollsystem aufgenommen werden können. Diese Geräte sollten nicht aktiviert und in die Datenbank des Hosts aufgenommen werden, bis sie in Betrieb genommen werden. Hierdurch werden auch sinnlose Abfragen der Geräte durch den Host verringert.</p>  |



|  |  |  |
|--|--|--|
|  |  | <p>Aus Sicherheitsgründen werden nach einem Softwareupgrade alle Controller offline geschaltet (Kontrollkästchen deaktiviert). Hierdurch wird sichergestellt, dass das System mit der alten Software weiter betrieben werden und durch die neue Software Schritt für Schritt auf den neuesten Stand gebracht werden kann. Beziehen Sie neue Controller allmählich in das System ein, indem Sie die jeweiligen Kontrollkästchen aktivieren.</p>   |
| <b>Controller Interface (Controller-Schnittstelle)</b> |  |  |
| Interface Type (Schnittstellentyp)                     | <p>COM</p> <p>UDP</p>  | <p>COM, wenn die Verbindung zum AMC über einen der MAC-COM-Ports hergestellt wird. UDP (= User Datagram Protocol), wenn die Verbindung über das Netzwerk hergestellt wird. Wenn dieser Verbindungstyp gewählt ist, können die Parameter „host name“ (Hostname) und „remote-controlled port“ (Ferngesteuerter Port) eingestellt werden.</p> <div style="text-align: center;">  </div> <p>Beim Schnittstellentyp „UDP“ <b>muss</b> DIP-Schalter „5“ am AMC eingestellt werden. Darüber hinaus wird empfohlen, Schalter „1“ auf ON (AN) zu stellen.</p> |
| PC COM-Port  | <p>Nummernbereich:<br/>COM-Ports:<br/>1-256<br/>mit UDP-Ports:<br/>1-65535</p> | <p>Nummer des COM-Ports, an dem dieser AMC an den MAC angeschlossen ist. Bei Ethernet-Verbindungen über Konverter werden virtuelle COM-Ports generiert und hier angezeigt. Wenn der Typ „UDP“ lautet, geben Sie den Port ein, über den der MAC Informationen vom AMC erhält. Wenn dieser Port unbekannt ist, braucht kein Wert in das Feld eingegeben zu werden. Ein freier Port wird dann automatisch gewählt.</p>  |
| Bus number (Busnummer)                                 | <p>Nummernbereich:<br/>1-8</p>   | <p>Wenn der Schnittstellenadapter AMC-MUX verwendet wird, können bis zu 8 Controller an einem COM-Port konfiguriert werden.</p>  |

|   |   |   |
|---|---|---|
|   |   | <p>Geben Sie in solchen Fällen die eindeutige Adresse jedes AMC ein, die durch seinen DIP-Schalter festgelegt wird.</p> <p><b>Hinweis:</b> Schalter 5 kann ignoriert werden, da nur die ersten 4 Schalter für die Adressierung verwendet werden.</p> <p>Verwenden Sie bei UDP-Verbindungen die Standardeinstellung (= 0).</p>   |
| IP Address/<br>Hostname (IP-Adresse/Hostname)                 | Netzwerkname oder IP-Adresse des AMC  | <p>In diesem Feld ist nur eine Einstellung möglich, wenn <b>UDP</b> als Porttyp festgelegt wurde.</p> <p>Wenn IP-Adressen per DHCP vergeben werden, sollte der Netzwerkname des AMC angegeben werden. Auf diese Weise kann der AMC nach einem Neustart lokalisiert werden, selbst wenn sich die IP-Adresse geändert hat. Bei Netzwerken ohne DHCP muss die IP-Adresse angegeben werden.</p>   |
| UDP-Port  | Nummernbereich:<br>1–10001 bei<br>Defaultkonfiguration  | <p>Dieses Eingabefeld ist nur aktiviert, wenn <b>UDP</b> als Porttyp festgelegt wurde.</p> <p>Dies ist der AMC-Port, der die MAC-Meldungen empfängt.</p>  |
| Weitere Parameter   |   |   |
| Program (Programm)  | Alphanumerisch  | <p>Dateiname des Programms, das in den AMC geladen wird. Die verfügbaren Programme befinden sich im BIN-Verzeichnis des MAC und können aus einer Liste ausgewählt werden. Der Einfachheit halber werden das Protokoll und die Beschreibung ebenfalls angezeigt.</p> <p>Dieser Parameter wird automatisch festgelegt, da Programme automatisch abhängig davon geladen werden, welche Leser angeschlossen sind. Der Parameter wird überschrieben, falls ein Konflikt zwischen Leser und Programm besteht.</p> |
| Power supply supervision<br>(Überwachung der Stromversorgung) | <p>0 = Deaktiviert<br/>(Kontrollkästchen ist deaktiviert)</p> <p>1 = Aktiviert<br/>(Kontrollkästchen ist aktiviert)</p> | <p>Überwachung der Stromversorgung. Wenn die Spannung abfällt, wird eine Meldung zu dem Problem generiert. Bei der Überwachungsfunktion wird eine USV (unterbrechungsfreie Stromversorgung) vorausgesetzt, sodass eine Meldung generiert werden kann.</p> <p>0 = keine Überwachung<br/>1 = Überwachung aktiviert</p>  |

|   |  |   |
|---|--|---|
| No LAC accounting<br>(Keine LAC-Berücksichtigung) | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | Markieren Sie dieses Kontrollkästchen für AMC-Geräte, die gemeinsam funktionieren, um den Zutritt zu Parkplätzen zu gewähren, wobei nur der übergeordnete MAC die Anzahl der ein- und ausgehenden Einheiten nachhält. <b>Beachten Sie</b> , dass dann, wenn diese Option ausgewählt und der AMC offline ist, der AMC den Zutritt zu überfüllten Bereichen nicht verhindern kann, da er keinen Zugriff auf die Gesamtzahlen hat. |
| Mandant   | Standardwert „Allgemein“   | Dies ist ein schreibgeschütztes Informationsfeld. „Divisions“ (Mandanten) sind ein Mittel, um ein Zutrittskontrollsystem auf mehrere autonome Parteien aufzuteilen, die in BIS Manager erstellt und verwaltet werden.   |

**Konfigurieren von AMC-Eingängen**

AMC 4-W
Inputs
Outputs
Terminals

| Name          | Serial resistor | Parallel resistor | Time model      | Messages                                 |
|---------------|-----------------|-------------------|-----------------|--|
| 01, AMC 4-W-8 | 2K2             | 1K2               | <No time model> | 03, Open, close, Line cut, short circuit |
| 02, AMC 4-W-8 | 1K5             | 1K                | <No time model> | 00,                                      |
| 03, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |
| 04, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |
| 05, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |
| 06, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |
| 07, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |
| 08, AMC 4-W-8 | none            | none              | <No time model> | 00,                                      |

Input type

Digital mode, single
  Analog mode, 4 state

Events

Time model: <No time model> ▼

Open, close

Line cut, short circuit

Resistors

serial

none

1K

1K2

1K5

1K8

2K2

2K7

3K3

3K9

4K7

5K6

6K8

8K2

parallel

none

1K

1K2

1K5

1K8

2K2

2K7

3K3

3K9

4K7

5K6

6K8

8K2

Dieser Dialog ist in vier Fenster unterteilt:

- Liste der Eingänge nach Namen
- Eingangstypen

- Die Ereignisse, die von den Eingängen signalisiert werden
- Die mit Analogmodus verwendeten Widerstandstypen

### Parameter von Eingängen

Die Parameter der AMC-Eingänge werden in der folgenden Tabelle beschrieben:

| Spaltenname                           | Beschreibung  |
|---------------------------------------|---|
| Name                                  | Nummerierung des Eingangs (von 01 bis 08) und Name des entsprechenden AMC oder AMC-EXT.   |
| Serienwiderstand                      | Anzeige des gesetzten Widerstandswerts für den Serienwiderstand<br>„Keine“ oder „---“ = Digitalmodus  |
| Parallelresistor (Parallelwiderstand) | Anzeige des gesetzten Widerstandswerts für den Parallelwiderstand<br>„Keine“ oder „---“ = Digitalmodus  |
| Time model (Zeitmodell)               | Name des gewählten Zeitmodells  |
| Messages (Meldungen)                  | Ordnungsnummer und Bezeichnung der Meldungen, die generiert werden<br>00 = keine Meldungen<br>01 = wenn die Ereignisse <b>Open</b> (Offen), <b>close</b> (Geschlossen) aktiviert wurden<br>02 = wenn die Ereignisse <b>Line cut</b> (Leitungsbruch), <b>short circuit</b> (Kurzschluss) aktiviert wurden<br>03 = wenn beide Ereignisoptionen aktiviert wurden |
| Assigned (Zugewiesen)                 | Bei Verwendung des Türmodells 15 wird der Signalname des DIP angezeigt.   |

Verwenden Sie die Strg- und die Umschalttaste beim Klicken zur gleichzeitigen Auswahl mehrerer Eingänge. Alle Werte, die Sie ändern, gelten für alle ausgewählten Eingänge.

### Ereignisse und Zeitmodelle

Abhängig vom Betriebsmodus können entweder die Türzustände **Open** (Offen), **Closed** (Geschlossen), **Line cut** (Leitungsbruch) und **Short circuit** (Kurzschluss) erkannt und gemeldet werden.

Aktivieren Sie die entsprechenden Kontrollkästchen, damit der AMC diese Status als Ereignisse an das Gesamtsystem übertragen kann.

Wählen Sie ein **Zeitmodell** aus der gleichnamigen Dropdown-Liste, um die Übertragung der Ereignisse auf die vom Modell definierten Zeiten zu beschränken. Zum Beispiel ist das Ereignis **Open** (Offen) möglicherweise nur außerhalb der normalen Geschäftszeiten von Bedeutung.

### Eingangstyp

Die Widerstände können im **Digitalmodus** oder **Analogmodus (4 Zustände)** betrieben werden. Der Standard ist **Digitalmodus**: nur die Türzustände **open** (offen) und **close** (geschlossen) werden erfasst.

Im Analogmodus werden zudem die Leitungszustände **Line cut** (Leitungsbruch) und **Short circuit (Kurzschluss)** erkannt.

|                                   |   |
|-----------------------------------|---|
| Door open<br>(Tür geöffnet)       | Summe der Serienwiderstandswerte ( $R_s$ ) und Parallelwiderstandswerte ( $R_p$ ):<br>$R_s + R_p$       |
| Door closed<br>(Tür geschlossen)  | Entspricht den Serienwiderstandswerten: $R_s$   |
| Circuit break<br>(Leistungsbruch) | Summe der Serienwiderstandswerte ( $R_s$ ) und Parallelwiderstandswerte ( $R_p$ ) geht gegen unendlich. |
| Short-Circuit<br>(Kurzschluss)    | Summe der Serienwiderstandswerte ( $R_s$ ) und Parallelwiderstandswerte ( $R_p$ ) ergibt null.          |

**Widerstände**

Die Widerstände sind im standardmäßigen **Digitalmodus** auf "none" (Keine) oder "---" eingestellt.

Im **Analogmodus** können die Werte für die seriellen und parallelen Widerstände durch Auswahl der entsprechenden Optionsfelder eingestellt werden.

**keine, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2** (in 100 Ohm)

Abhängig vom gewählten Widerstandswert sind für den entsprechenden Widerstand nur eingeschränkte Bereiche verfügbar.

In den folgenden Tabellen werden in der linken Spalte die gewählten Werte und in der rechten Spalte die verfügbaren Bereiche des anderen Widerstands angezeigt.

| Serienwiderstand          | Bereich     | Parallelwiderstand        | Bereich     |
|---------------------------|-------------|---------------------------|-------------|
| "none" (keine) oder "---" | 1K bis 8K2  | "none" (keine) oder "---" | 1K bis 8K2  |
| 1K                        | 1K bis 2K2  | 1K                        | 1K bis 1K8  |
| 1K2                       | 1K bis 2K7  | 1K2                       | 1K bis 2K7  |
| 1K5                       | 1K bis 3K9  | 1K5                       | 1K bis 3K3  |
| 1K8                       | 1K bis 6K8  | 1K8                       | 1K bis 3K9  |
| 2K2                       | 1K2 bis 8K2 | 2K2                       | 1K bis 4K7  |
| 2K7                       | 1K2 bis 8K2 | 2K7                       | 1K2 bis 5K6 |
| 3K3                       | 1K5 bis 8K2 | 3K3                       | 1K5 bis 6K8 |
| 3K9                       | 1K8 bis 8K2 | 3K9                       | 1K5 bis 8K2 |
| 4K7                       | 2K2 bis 8K2 | 4K7                       | 1K8 bis 8K2 |
| 5K6                       | 2K7 bis 8K2 | 5K6                       | 1K8 bis 8K2 |
| 6K8                       | 3K3 bis 8K2 | 6K8                       | 1K8 bis 8K2 |
| 8K2                       | 3K9 bis 8K2 | 8K2                       | 2K2 bis 8K2 |

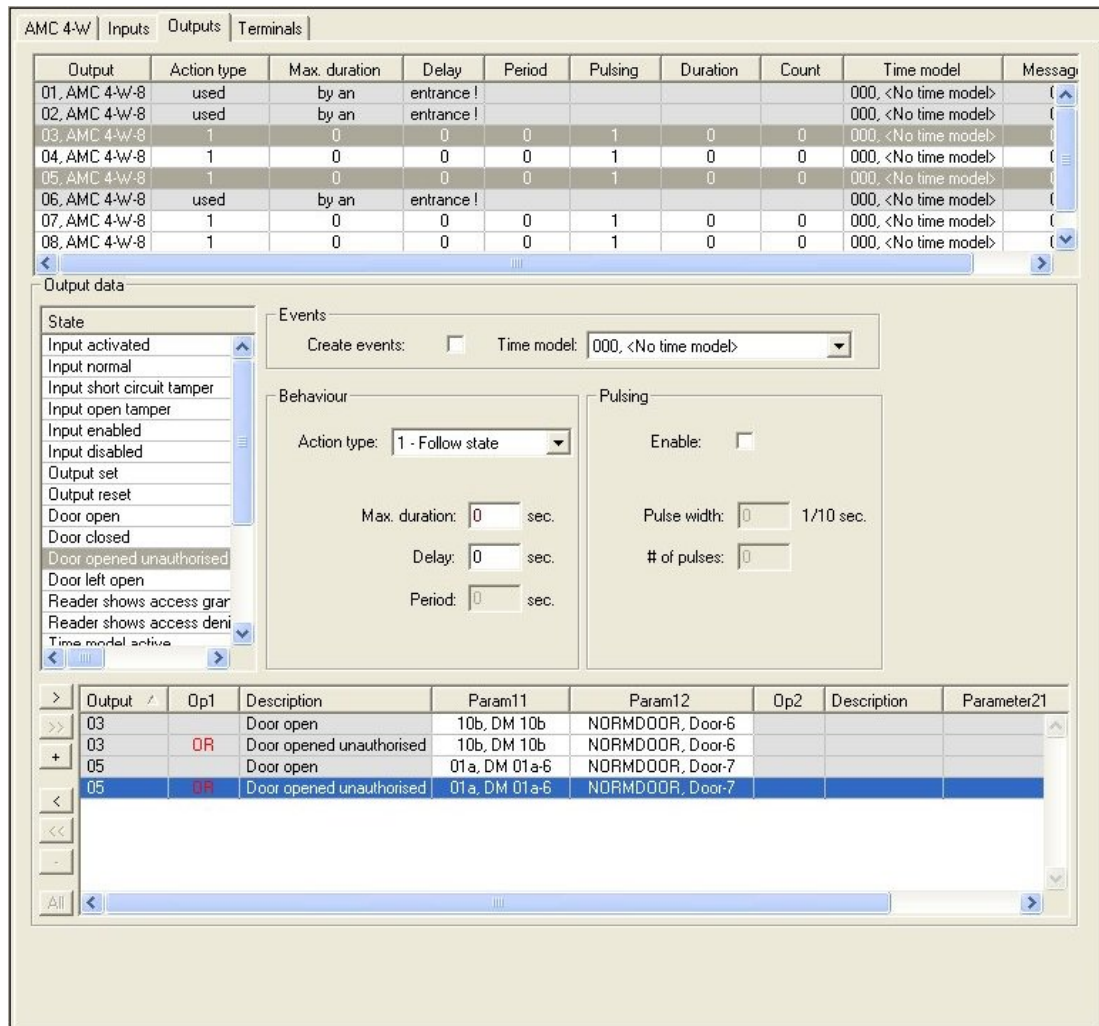
**Konfiguration der AMC-Ausgänge – Übersicht**

Auf dieser Dialogseite können Sie jeden Ausgang eines AMC oder AMC-EXT konfigurieren.

Diese Seite setzt sich aus drei Hauptbereichen zusammen:

- Listenfeld mit einer Übersicht über die für jeden Ausgang gesetzten Parameter
- Konfigurationsoptionen für die in der Liste gewählten Ausgänge

– Definition der Bedingungen für die Aktivierung der Ausgänge



**Auswahl der AMC-Ausgänge in der Tabelle**

Wählen Sie zur Konfiguration der Ausgangskontakte zuerst die entsprechende Zeile in der oberen Tabelle aus. Verwenden Sie die Strg- und die Umschalttaste zur gleichzeitigen Auswahl mehrerer Zeilen. Im unteren Teil des Fensters vorgenommene Änderungen gelten nur für die ausgewählten Ausgänge.

| 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       |

Zeilen, deren Ausgänge bereits durch ein Türmodell oder anderswo zugewiesen wurden, werden in hellgrauer Farbe mit der Information „von einem Durchtritt verwendet!“ angezeigt. Solche Ausgänge können nicht weiter konfiguriert werden.

Von Ihnen ausgewählte Zeilen werden in dunkelgrauer Farbe angezeigt.

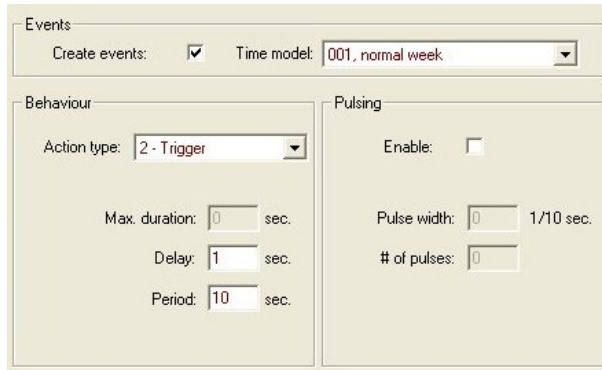
**Parameter von AMC-Ausgängen**

| Spaltenname | Beschreibung |
|-------------|--------------|
| e           |              |

|                                  |   |
|----------------------------------|---|
| Ausgang                          | Aktuelle Nummerierung der Ausgänge am jeweiligen AMC oder AMC-EXT<br>01 bis 08 bei AMC und AMC_IO08<br>01 bis 16 bei AMC_IO16               |
| Action type<br>(Aktionstyp)      | Angabe des gewählten Aktionstyps<br>1 = Follow state (Zustandsnachführung)<br>2 = Trigger (Vorübergehend)<br>3 = Alternating (Alternierend) |
| Max.<br>duration<br>(Max. Dauer) | Länge des Signals in Sekunden [1–9999; 0 = immer, falls keine widersprechende Meldung erfolgt] – nur bei Aktionstyp 1                       |
| Delay<br>(Verzögerung)           | Verzögerung in Sekunden, bis das Signal ausgegeben wird [0–9999] – nur bei Aktionstyp 1 und 2   |
| Period<br>(Zeitraum)             | Zeitraum in Sekunden, über den das Signal ausgegeben wird – nur bei Aktionstyp 2  |
| Pulsing<br>(Impuls)              | Aktivierung des Impulses – anderenfalls wird das Signal konstant ausgegeben.  |
| Duration<br>(Dauer)              | Impulslänge   |
| Count<br>(Anzahl)                | Anzahl von Impulsen pro Sekunde   |
| Zeitmodell                       | Name des gewählten Zeitmodells  |
| Messages<br>(Meldungen)          | Kennzeichnung der Meldungsaktivität<br>00 = keine Meldungen<br>03 = Ereignisse werden gemeldet  |
| Assigned<br>(Zugewiesen)         | Bei Verwendung des Türmodells 15 wird der Signalname des DOP angezeigt.   |

#### **Ausgänge: Ereignisse, Aktion, Impuls**

Alle Einträge aus der obigen Liste werden mithilfe von Kontrollkästchen und Eingabefeldern in den Bereichen **Events** (Ereignisse), **Action** (Aktion) und **Pulsing** (Impuls) des Dialogs generiert. Wenn Sie einen Listeneintrag wählen, werden die jeweiligen Einstellungen in diesen Bereichen angegeben. Dies gilt auch für die Mehrfachauswahl von Listeneinträgen unter der Voraussetzung, dass die Parameter für alle gewählten Ausgänge identisch sind. Änderungen an den Parametereinstellungen werden für alle in der Liste gewählten Einträge übernommen.



Aktivieren Sie das Kontrollkästchen **Create events** (Ereignisse erstellen), wenn für den aktivierten Ausgang eine Meldung gesendet werden soll. Wenn diese Meldungen nur in bestimmten Zeiträumen gesendet werden sollen, beispielsweise nachts oder an Wochenenden, geben Sie ein geeignetes **Zeitmodell** an.

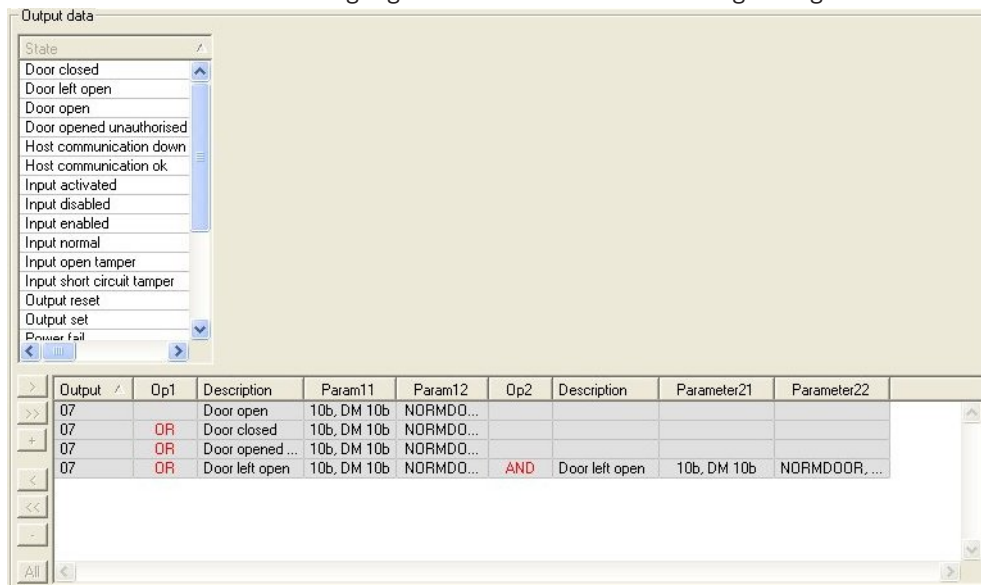
Die folgenden Parameter können für einzelne Aktionstypen gesetzt werden:

| Action type (Aktionstyp) | Max. duration (Max. Dauer) | Delay (Verzögerung) | Period (Zeitraum)                        | Impuls/ Aktivieren      | Impulsdauer | Anzahl der Impulse |
|--------------------------|----------------------------|---------------------|--|-------------------------|-------------|--------------------|
| Zustandsnachführung      | 0 = immer<br>1 - 9999      | 0 - 9999            | Nein                                     | Ja                      | 1 - 9999    | Keine              |
| Trigger                  | Nein                       | 0 - 9999            | 0-9999 wenn „Impuls“ nicht aktiviert ist | Ja deaktiviert Zeitraum | 1 - 9999    | 1 - 9999           |
| Alternierend             | Nein                       | Nein                | Nein                                     | Ja                      | 1 - 9999    | Nein               |

**AMC-Ausgabedaten**

Der untere Teil des Dialogfensters **Outputs** (Ausgänge) enthält:

- Ein Listenfeld mit den für die ausgewählten Ausgänge verfügbaren **Zuständen**.
- Eine Tabelle mit den Ausgängen und den für ihre Auslösung konfigurierten Zuständen.





### Konfiguration der Zustände zum Auslösen von Ausgängen

Sie können die oben ausgewählten Ausgänge so konfigurieren, dass sie von einzelnen Zuständen oder logischen Kombinationen von Zuständen ausgelöst werden-

- Wählen Sie im oberen Listenfeld einen oder mehrere Ausgänge aus.
- Wählen Sie einen Zustand aus der Liste **Zustand** aus.
- Wenn für einen Status mehrere Geräte oder Installationen vorhanden sind, die diesen Status übertragen können, wird die Schaltfläche neben der Schaltfläche aktiviert. Klicken Sie auf (oder doppelklicken Sie auf den Status), um für jeden ausgewählten Ausgang einen Eintrag von dessen Status mit dem ersten Gerät (zum Beispiel AMC, erster Eingang) und der Installation (zum Beispiel erstes Signal, erste Tür) zu erstellen.

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

Durch Klicken auf wird der ausgewählte Status in die Liste übertragen und zusammen mit einer ODER-Verknüpfung für jedes installierte Gerät (zum Beispiel alle AMC-Eingänge) erstellt.

| 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 |

- Mehrere Zustände können über eine OR-Verknüpfung zugewiesen werden.

| 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       | << !!! >>          |

Verknüpfungen mit AND sind ebenfalls möglich:

- Ein Status muss bereits zugewiesen sein, dem eine weitere Bedingung hinzugefügt wird, die in einer beliebigen Spalte gewählt wird.
- Ein weiterer Status wird dann gewählt und durch Klicken auf mit dem markierten Status verknüpft.

| 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 | << !!! >>   |



#### Hinweis!

Jedem Ausgang können bis zu 128 OR-Verknüpfungen zugewiesen werden. Für jede zugewiesene Bedingung kann **eine** AND-Verknüpfung erstellt werden.

Nachdem einem Gerät oder einem System ein Status zugewiesen wurde, kann er auch allen anderen vorhandenen Geräten und Systemen zugewiesen werden.

- Wählen Sie den zugewiesenen Eintrag in einer beliebigen Spalte.
- Dieser Status wird für alle vorhandenen Geräte und Systeme erstellt, indem Sie auf



klicken.

### Modifizieren der Parameter von Ausgängen

Listeneinträge können geändert werden.

Wenn der zugewiesene Status mehreren Geräten oder Systemen entspricht, werden immer die ersten Geräte und Systeme dieses Typs festgelegt.

In den Spalten **Param11** (Parameter11) und **Param21** (Parameter21) (mit AND-Verknüpfungen) werden die Geräte (beispielsweise AMC, Durchtritt) angezeigt. Die Spalten **Param12** (Parameter12) und **Param22** (Parameter22) enthalten Sondersysteme (zum Beispiel Eingangssignal, Tür, Leser).

Wenn mehrere Geräte (beispielsweise E/A-Platinen) oder Systeme (beispielsweise Zusatzsignale, Zusatzleser) vorhanden sind, ändert sich der Mauszeiger, während Sie auf diese Spalte zeigen.

| 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       | << !!! >>          |

Wenn Sie auf den Spalteneintrag doppelklicken, wird die Schaltfläche hinzugefügt, über die Sie eine Dropdownliste mit gültigen Einträgen für den Parameter öffnen können.

| 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       | <div style="border: 1px solid black; padding: 2px;"> 01, AMC 4-W-2<br/> 02, AMC 4-W-2<br/> 03, AMC 4-W-2<br/> 04, AMC 4-W-2<br/> 05, AMC 4-W-2<br/> 06, AMC 4-W-2<br/> 07, AMC 4-W-2<br/> 08, AMC 4-W-2 </div> |

Wenn Sie die Einträge in den Spalten **Param11** und **Param21** ändern, werden die Einträge in Spalte **Param12** und **Param22** aktualisiert:

| 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_10, AMC_1016_002_1 | In, 01, AMC_1016_002_1 |



**Hinweis!**

Dies ist nur für die Spalten **Param11** (Parameter11), **Param12** (Parameter12), **Param21** (Parameter21) und **Param22** (Parameter22) möglich.

Ohne weitere Optionen (weil beispielsweise nur ein Durchtritt konfiguriert wurde) ändert sich der Mauszeiger nicht, und alle Felder sind grau. Wenn Sie auf diesen Eintrag doppelklicken, wird dieser Vorgang als Löschbefehl interpretiert. Das Meldungsfeld, in dem Sie den Löschvorgang bestätigen müssen, wird angezeigt.

**Löschen der Zustände zum Auslösen von Ausgängen**

Ausgewählte Zuweisungen können Sie entfernen, indem Sie auf  '<' klicken (oder auf den Listeneintrag doppelklicken). Ein Meldungsfeld fordert Sie zur Bestätigung dieses Löschvorgangs auf.

Wenn mit einem Ausgang mehrere Zustände verbunden wurden, können diese alle wie folgt gemeinsam gelöscht werden:

- Wählen Sie den ersten Eintrag (den, der keinen Eintrag in der Spalte **Op1** hat) und klicken Sie dann auf die Schaltfläche '<<' .
- Sie können auch auf den ersten Eintrag doppelklicken.
  - Ein Popup-Fenster wird eingeblendet. Bestätigen Sie den Löschvorgang, oder brechen Sie ihn ab.
  - Wenn Sie die Löschung bestätigen, werden Sie weiter gefragt, ob Sie alle zugehörigen Einträge (Antwort **Ja**) oder nur den ausgewählten Eintrag (Antwort **Nein**) löschen möchten.

Klicken Sie zum Löschen weiterer Zustände, die den ersten Zustand durch einen UND-Operator in der Spalte **Op2** qualifizieren, an eine beliebige Stelle auf der Zeile und dann auf die „Minus“-Schaltfläche , die nur aktiv ist, wenn auf dieser Zeile ein qualifizierender UND-Zustand vorhanden ist.

**Zustandsbeschreibung**

Die folgende Tabelle bietet eine Übersicht über alle wählbaren Zustände, ihre Typnummern und Beschreibungen.

Das Listenfeld **State** (Zustand) enthält diese Parameter auch. Sie werden im rechten Bereich der Liste angezeigt. Führen Sie hierzu einen Bildlauf nach rechts durch.

| <b>State</b> (Zustand)                               | <b>Type</b> (Typ) | <b>Beschreibung</b>                                    |
|--|-------------------|--|
| Input activated (Eingang aktiviert)                  | 1                 | Lokaler Platineneingang                                |
| Input normal (Eingang normal)                        | 2                 | Lokaler Platineneingang                                |
| Input short circuit tamper (Eingang kurzgeschlossen) | 3                 | Lokaler Platineneingang, falls Widerstand konfiguriert |
| Input open tamper (Sabotage – Eingangskontakt offen) | 4                 | Lokaler Platineneingang, falls Widerstand konfiguriert |

|   |    |   |
|---|----|---|
| Input enabled (Eingang aktiv)                         | 5  | Lokaler Platineneingang durch Zeitmodell aktiviert                  |
| Input disabled (Eingang inaktiv)                      | 6  | Lokaler Platineneingang durch Zeitmodell deaktiviert                |
| Output set (Ausgang gesetzt)                          | 7  | Lokaler Platinenausgang, nicht aktueller Ausgang                    |
| Output reset (Ausgang zurückgesetzt)                  | 8  | Lokaler Platineneingang, nicht aktueller Eingang                    |
| Door open (Tür geöffnet)                              | 9  | GID des Eingangs, Türnummer   |
| Door closed (Tür geschlossen)                         | 10 | GID des Eingangs, Türnummer   |
| Door opened unauthorized (Tür unautorisiert geöffnet) | 11 | GID des Eingangs, Türnummer, ersetzt „Door open“ (Tür geöffnet) (9) |
| Door left open (Tür zu lange geöffnet)                | 12 | GID des Eingangs, Türnummer   |
| Reader shows access granted (Leser Zutritt gewährt)   | 13 | Adresse des Lesers  |
| Reader shows access denied (Leser Zutritt verwehrt)   | 14 | Adresse des Lesers  |
| Time model active (Zeitmodell aktiv)                  | 15 | Konfiguriertes Zeitmodell   |
| Tamper reader (Leser Sabotage)                        | 16 | Adresse des Lesers  |
| Tamper AMC (AMC, Sabotage Gehäuse)                    | 17 | ---   |
| Tamper I/O board (I/O Platine, Sabotage)              | 18 | ---   |
| Power fail (Batterie leer)                            | 19 | nur für AMC mit Batterie  |
| Power good (Batterie OK)                              | 20 | nur für AMC mit Batterie  |
| Host communication ok (Kommunikation ok)              | 21 | ---   |
| Host communication down (Kommunikation gestört)       | 22 | ---   |
| Reader Messages (Lesermeldungen)                      | 23 | (Details hängen von der aktuellen Softwareversion ab.)              |
| LAC Messages (LAC-Meldungen)                          | 24 | (Details hängen von der aktuellen Softwareversion ab.)              |

### Konfiguration von Ausgängen

Neben der Signalzuweisung über Türmodelle oder individuelle Zuweisung können Bedingungen für noch nicht zugeordnete Ausgänge definiert werden. Falls diese Bedingungen eintreten, wird der Ausgang nach dem gesetzten Parameter aktiviert.

Sie müssen entscheiden, was über den Ausgang geschaltet wird. Im Gegensatz zu Signalen, die mit einem speziellen Türmodell, seinen Türen und Lesern verknüpft werden können, können in diesem Fall die Signale aller an einen AMC angeschlossenen Geräte und Systeme angewendet werden.

Wenn beispielsweise ein optisches oder akustisches Signal oder eine Meldung an die UGM durch die Signale **Eingang kurzgeschlossen** und **Tür unautorisiert geöffnet** ausgelöst werden soll, werden die Eingänge oder Ausgänge, die berücksichtigt werden können, dem jeweiligen Zielausgang zugeordnet.

Beispiel, bei dem in jedem Fall nur ein Kontakt gewählt wurde:

| 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       | << !!! >>         |

Beispiel mit allen Kontakten:


| 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 |

Beispiel mit gewählten Kontakten:

Sie erstellen einen einzelnen Eintrag für jeden Kontakt, indem Sie auf klicken oder die unerwünschten Kontakte entfernen, nachdem Sie alle Kontakte zugewiesen haben:

| 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 |

Dieselben Bedingungen können für mehrere Ausgänge festgelegt werden. Wenn Sie beispielsweise neben dem optischen Signal auch noch ein akustisches Signal benötigen, könnte gleichzeitig eine Meldung an die UGM gesendet werden:

| 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       |

Liste aller vorhandenen Zustände mit den Defaultwerten für die Parameter11/21 und 12/22:

| 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     | ---                | ---                  |

### Definieren von Signalen auf der Registerkarte "Terminals" (Signale)

Auf der Registerkarte **Terminals** (Signale) werden die auf einem AMC oder AMC-EXT zugewiesenen Kontakte angezeigt. Sobald Durchtritte erstellt wurden, werden Signalzuweisungen nach dem gewählten Türmodell angegeben.

Sie können auf der Registerkarte **Terminals** (Signale) des Controllers oder der AMC Erweiterungen keine Änderungen vornehmen. Eine Bearbeitung ist nur auf der Registerkarte „terminals“ (Signale) der Seite „entrance“ (Durchtritt) möglich. Aus diesem Grund werden Signaleinstellungen grau hinterlegt angezeigt. Eingänge, die rot angezeigt werden, geben die Signalkonfigurationen der jeweiligen Ausgänge an.

AMC 4-R4 | Inputs | **Outputs** | Terminals

Signal allocation of 'AMC 4-R4' with 12 signal pairing

| 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  |          |              |          |               |



# 13 Konfigurieren von Durchritten

## 13.1 Durchritte – Einführung

Der Begriff Durchtritt bezeichnet den Zutrittskontrollmechanismus an einem Eintrittspunkt in seiner Gesamtheit:

Zu den Elementen des Durchtritts gehören:

- Kartenleser: zwischen 1 und 4
- Eine Form von Barriere, zum Beispiel eine Tür, ein Drehkreuz, eine Schleuse oder eine Schranke.
- Der Zutrittskontrollprozess wie von vordefinierten Sequenzen elektrischer Signale, die zwischen den Hardwareelementen weitergeleitet werden, definiert.

Ein Türmodell ist eine Vorlage für eine bestimmte Art von Durchtritt. Mit ihr werden die vorhandenen Türelemente (Anzahl und Typ von Lesern, Typ der Tür oder Barriere usw.) beschrieben und ein bestimmter Prozess der Zutrittskontrolle über Sequenzen oder vordefinierte Signale erzwungen.

Türmodelle erleichtern die Konfiguration eines Zutrittskontrollsystems wesentlich.

|              |  |
|--------------|--|
| Türmodell 1  | Einfache oder allgemeine Tür   |
| Türmodell 3  | Reversierbares Drehkreuz für Zugang und Ausgang                                      |
| Türmodell 5  | Parkplatzzugang oder -ausgang  |
| Türmodell 6  | Leser für eingehenden/ausgehenden Verkehr (Zeit und Anwesenheit)                     |
| Türmodell 7  | Aufzugsteuerung  |
| Türmodell 9  | Fahrzeugschranke und Rolltor   |
| Türmodell 10 | Einfache Tür mit EMA-Scharf- und -Unscharfschaltung                                  |
| Türmodell 14 | Einfache Tür mit EMA-Scharf- und -Unscharfschaltung sowie speziellen Zutrittsrechten |
| Türmodell 15 | Unabhängige Eingangs- und Ausgangssignale  |

- Bei den Türmodellen 1, 3, 5, 9 und 10 können zusätzliche Dialogleser auf der Eingangs- oder Ausgangsseite eingesetzt werden.
- Ein lokaler Zutrittscontroller, der innerhalb des Türmodells 05 (Parkplatz) oder 07 (Aufzug) verwendet wird, kann nicht mit einem anderen Türmodell geteilt werden.
- Wenn ein Durchtritt mit einem Türmodell konfiguriert und gespeichert wurde, kann das Türmodell nicht mehr gegen ein anderes ausgetauscht werden. Wenn ein anderes Türmodell erforderlich ist, muss der Durchtritt gelöscht und neu konfiguriert werden.

Einige Türmodelle haben Varianten (a, b, c, r) mit folgenden Eigenschaften:

|          |  |
|----------|--|
| <b>a</b> | Leser für eingehenden <b>und</b> ausgehenden Verkehr   |
| <b>b</b> | Leser für eingehenden Verkehr und Ausgangsdrucktaste   |
| <b>c</b> | Eingangs- <b>ODER</b> Ausgangsleser (nicht beides – dies wäre Variante <b>a</b> )  |
| <b>r</b> | (nur Türmodell 1) Ein Leser, der nur zur Registrierung von Personen an einem Sammelplatz dient, z. B. im Falle einer Evakuierung. Bei diesem Türmodell existiert keine physische Barriere. |

Die Schaltfläche **OK** zum Abschließen der Konfiguration wird nur aktiviert, wenn alle erforderlichen Werte eingegeben wurden. Türmodelle der Variante (a) erfordern beispielsweise Leser für eingehenden **und** ausgehenden Verkehr. Erst wenn ein Typ für beide Leser gewählt wurde, können Einträge gespeichert werden.

## 13.2 Erstellen von Durchtritten

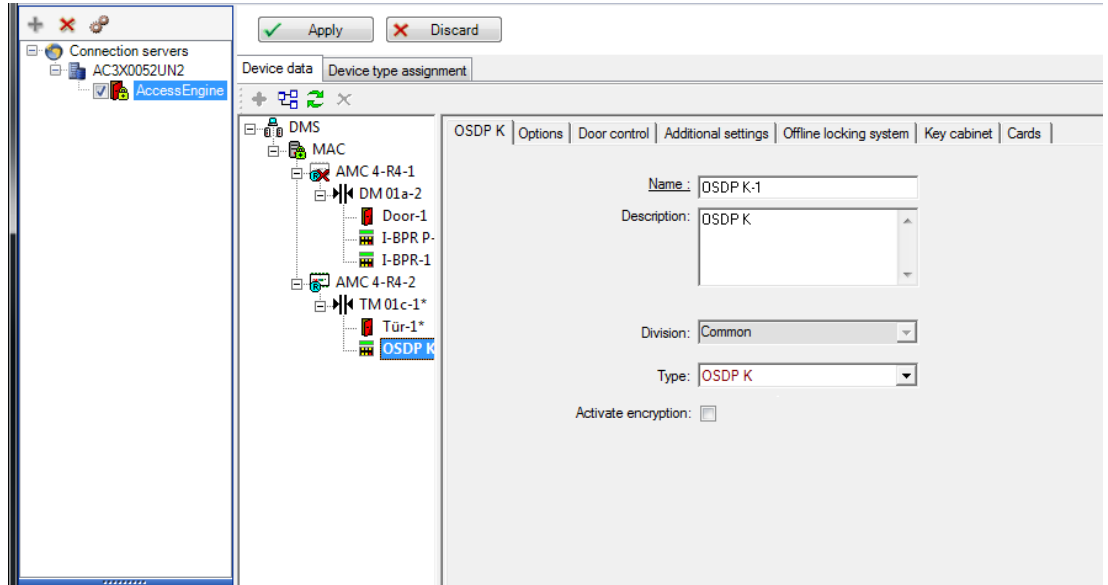
Die Liste der Leser, die zur Auswahl angezeigt werden, wird auf den ausgewählten Controllertyp zugeschnitten.

- Für **AMC 4W**-Typen sind **nur** Wiegand Leser verfügbar, sowohl mit als auch ohne Tastatur.
- Für **AMC 4R4** sind die Leser in der folgenden Tabelle verfügbar. Sie dürfen nicht verschiedene Protokolle mit demselben Controller verwenden.

| Name des Lesers             | Wiegand Protokoll | BPR-Protokoll | I-BPR-Protokoll | HID-Protokoll |
|-----------------------------|-------------------|---------------|-----------------|---------------|
| WIE1                        | X                 |               |                 |               |
| WIE1K (Keyboard)            | X                 |               |                 |               |
| BPR MF                      |                   | X             |                 |               |
| BPR MF Keyboard             |                   | X             |                 |               |
| BPR LE                      |                   | X             |                 |               |
| BPR LE Keyboard             |                   | X             |                 |               |
| BPR HI                      |                   | X             |                 |               |
| BPR HI Keyboard             |                   | X             |                 |               |
| TA40 LE                     |                   | X             |                 |               |
| TB30 LE                     |                   | X             |                 |               |
| TB15 HI1                    |                   | X             |                 |               |
| INTUS 1600                  |                   |               | X               |               |
| I-BPR                       |                   |               | X               |               |
| I-BPR K (Keyboard)          |                   |               | X               |               |
| DT 7020                     |                   |               | X               |               |
| OSDP                        |                   |               |                 | X             |
| OSDP K (Keyboard)           |                   |               |                 | X             |
| OSDP KD (Keyboard +Display) |                   |               |                 | X             |
| HADP                        |                   |               |                 | X             |
| HADP K (Keyboard)           |                   |               |                 | X             |
| HADP KD (Keyboard +Display) |                   |               |                 | X             |
| RKL 55 (Keyboard + LCD)     |                   |               |                 | X             |
| RK40 (Keyboard)             |                   |               |                 | X             |

|     |  |  |  |   |
|-----|--|--|--|---|
| R40 |  |  |  | X |
| R30 |  |  |  | X |
| R15 |  |  |  | X |

Im Falle eines **OSDP-Lesers** sieht der Dialog folgendermaßen aus:



Die folgenden Arten von OSDP-Lesern sind verfügbar:

|                |                                     |
|----------------|-------------------------------------|
| OSDP           | OSDP-Standardleser                  |
| OSDP Keyb      | OSDP-Leser mit Tastatur             |
| OSDP Keyb+Disp | OSDP-Leser mit Tastatur und Anzeige |

Folgende OSDP-Leser wurden getestet:

|  |  |
|--|--|
| OSDPv1 – unsicherer Modus              | LECTUS duo 3000 C – MIFARE classic<br>LECTUS duo 3000 CK – MIFARE classic<br>LECTUS duo 3000 E – MIFARE Desfire EV1<br>LECTUS duo 3000 EK – MIFARE Desfire EV1 |
| OSDPv2 – unsicherer und sicherer Modus | LECTUS secure 2000 RO<br>LECTUS secure 4000 RO<br>LECTUS secure 5000 RO  |



**Hinweis!**

Hinweise für OSDP

Vermischen Sie keine Produktfamilien, z. B. **LECTUS duo** und **LECTUS secure**, auf demselben OSDP-Bus.

Zur verschlüsselten Datenübertragung zum OSDP-Leser wird ein kundenspezifischer Schlüssel erstellt und verwendet. Achten Sie darauf, dass das System ordnungsgemäß gesichert ist.

Bewahren Sie die Schlüssel sicher auf. Verlorene Schlüssel können nicht wiederhergestellt werden. Bei Verlust kann der Leser nur auf die werksseitigen Standardeinstellungen zurückgesetzt werden.

Aus Sicherheitsgründen dürfen keine verschlüsselten und unverschlüsselten Modi auf demselben OSDP-Bus vermischt werden.

| Parameter   | Mögliche Werte  | Beschreibung  |
|---|---|---|
| <b>Durchtrittsname</b>                                | Alphanumerisch, zwischen 1 und 16 Zeichen             | Der Dialog erzeugt einen eindeutigen Namen für den Durchtritt, dieser Name kann jedoch auf Wunsch vom Bediener überschrieben werden, der den Durchtritt konfiguriert. |
| <b>Entrance description (Durchtrittsbeschreibung)</b> | Alphanumerisch: 0 bis 255 Zeichen                     | Ein beliebiger Beschreibungstext zur Anzeige im System.   |
| <b>Location (Standort)</b>                            | Ein beliebiger definierter Bereich (keine Parkplätze) | Der benannte Bereich (wie im System definiert), in dem sich der Leser befindet.   |

|   |   |  |
|---|---|--|
|   |   | Diese Information wird für die Zutrittsfolgekontrolle verwendet: Wenn eine Person versucht, diesen Leser zu verwenden, aber der aktuelle Standort dieser Person (wie vom System verfolgt) sich von dem des Lesers unterscheidet, verweigert der Leser dieser Person den Zutritt. |
| <b>Destination (Ziel)</b>   | Ein beliebiger definierter Bereich (keine Parkplätze) | Der benannte Bereich, wie im System definiert, zu dem der Leser Zutritt gewährt. Diese Information wird für die Zutrittsfolgekontrolle verwendet: Wenn eine Person diesen Leser verwendet, wird ihre Position auf den Wert von <b>Destination (Ziel)</b> aktualisiert.           |
| <b>Waiting time external access decision (Wartezeit für die externe Zugriffsentscheidung)</b> | Anzahl der Zehntelsekunden                            | Die Zeit, während der der Zutrittscontroller auf eine Entscheidung vom Zutrittskontrollsystem wartet, bevor er eine eigene Entscheidung trifft.  |
| <b>Division (Mandant)</b>   | Ein schreibgeschütztes Feld                           | Der definierte Mandant, zu dem der Leser gehört. Der Standard-Mandant ist immer <b>Common</b> (Allgemein).   |
| <b>Latency alarm device (Wartezeit Alarmanlage)</b><br>(nur für Türmodelle 10 und 14)         | 100 - 9999  | Die Zeitspanne, in der der Türöffner betätigt werden kann, ohne dass Alarm ausgelöst wird.<br>Dieser Leserparameter wird gesetzt und anschließend an die Leser übertragen.<br>Die Einheit dieses Parameters ist ein Zehntel (1/10) einer Sekunde.                                |
| <b>Arming Area (Scharfschaltebereich)</b><br>(nur für Türmodell 14)                           | Ein Buchstabe: A bis Z                                | Durchritte einer EMA-Gruppe werden durch die Aktivierung der Leser des Bereichs aktiviert.   |

### 13.3

### Zusätzliche E/A-Prüfungen

Zusätzliche E/A-Prüfungen können beispielsweise dabei helfen, einen Besucher basierend auf der automatischen Nummernschilderkennung (Automated Number-Plate Recognition, ANPR ) zu identifizieren.

Der AMC bekommt einen Eingang über den AMC E/A-Kontakt:

- Besucher autorisiert für Zusätzliche E/A-Prüfung

Der AMC verhindert den Zutritt, falls „nicht autorisiert“ signalisiert wird.

| T..       | entrance | Input signal     | entrance                          | Output signal    |                         |
|-----------|----------|------------------|-----------------------------------|------------------|-------------------------|
| 6482      | 01       | Parking-lot 05-1 | Door contact                      | Parking-lot 05-1 | Release door            |
| 6482      | 02       | Parking-lot 05-1 | "Request to exit" button          | Parking-lot 05-1 | Door is unlocked        |
| 6482      | 03       | Parking-lot 05-1 | Passage locked                    | Parking-lot 05-1 | Stoplight green         |
| 6482      | 04       | Parking-lot 05-1 | Passage completed                 | Parking-lot 05-1 | Alarm masking           |
| 6482      | 05       | Parking-lot 05-2 | Door contact                      | Parking-lot 05-2 | Release door            |
| 6482      | 06       | Parking-lot 05-2 | "Request to exit" button          | Parking-lot 05-2 | Door is unlocked        |
| 6482      | 07       | Parking-lot 05-2 | Passage locked                    | Parking-lot 05-2 | Stoplight green         |
| 6482      | 08       | Parking-lot 05-2 | Passage completed                 | Parking-lot 05-2 | Alarm masking           |
| 116_002_1 | 01       | Parking-lot 05-1 | External access decision accep... | Parking-lot 05-1 | External access ...     |
| 116_002_1 | 02       | Parking-lot 05-1 | External access decision denied   |                  |                         |
| 116_002_1 | 03       | Parking-lot 05-2 | External access decision accepted | Parking-lot 05-2 | External access deci... |
| 116_002_1 | 04       | Parking-lot 05-2 | External access decision denied   |                  |                         |
| 116_002_1 | 05       |                  |                                   |                  |                         |
| 116_002_1 | 06       |                  |                                   |                  |                         |
| 116_002_1 | 07       |                  |                                   |                  |                         |

| Ausweisstatus                                  | Signal = 1: ANPR autorisiert   | Signal = 0: ANPR nicht autorisiert |
|--|--------------------------------|------------------------------------|
| Ausweis autorisiert                            | Berechtigter Zutritt           | Ungültiges Fahrzeugkennzeichen.    |
| Ausweis auf Sperrliste                         | Nicht autorisiert – Sperrliste | Nicht autorisiert – Sperrliste     |
| Ausweis abgelaufen                             | Nicht autorisiert – abgelaufen | Nicht autorisiert – abgelaufen     |
| Ausweis nicht autorisiert für dieses Lesegerät | Nicht autorisiert              | Nicht autorisiert                  |

Es ist möglich, den Zugang manuell zu öffnen, selbst wenn der Besucher nicht erkannt wird.

Zu diesem Zweck gibt es einen Schalter für die E/A-Kontakte.

Der AMC gibt ein Ausgangssignal **Zusätzliche Prüfung aktiv**, bevor das Eingangssignal ausgewertet wird.

Wird ein neuer Besucher registriert, müssen die Daten des Nummernschildes in den BIS (für Berichte) und ins APNR-System (zum Scannen) eingegeben werden.

ANPR erkennt dann ein registriertes Fahrzeug aus seiner Datenbank.

## 13.4 Konfigurieren von AMC-Signalen

Was den Inhalt und die Struktur anbelangt, ist diese Registerkarte mit der AMC-Registerkarte **Terminals** (Signale) identisch.

DM 01b Terminals

Signal allocation of 'AMC 4-R4' with 8 signal pairing

| B.. | T.. | entrance      | Input signal         | entrance      | Output signal       |
|-----|-----|---------------|----------------------|---------------|---------------------|
| 0   | 01  | DM 01a        | Door contact         | DM 01a        | Release door        |
| 0   | 02  | <b>DM 01b</b> | <b>Door contact</b>  | <b>DM 01b</b> | <b>Release door</b> |
| 0   | 03  | <b>DM 01b</b> | "Request to exit"... |               |                     |
| 0   | 04  |               |                      |               |                     |
| 0   | 05  |               |                      |               |                     |
| 0   | 06  |               |                      |               |                     |
| 0   | 07  |               |                      |               |                     |
| 0   | 08  |               |                      |               |                     |

Hier können Sie jedoch die Signalzuweisung für das gewählte Türmodell ändern. Wenn Sie auf die Spalten **Ausgangssignal** oder **Eingangssignal** doppelklicken, werden Kombinationsfelder geöffnet.

DM 01b Terminals

Signal allocation of 'AMC 4-R4' with 8 signal pairing

| B.. | T.. | entrance      | Input signal             | entrance      | Output signal       |
|-----|-----|---------------|--------------------------|---------------|---------------------|
| 0   | 01  | DM 01a        | Door contact             | DM 01a        | Release door        |
| 0   | 02  | <b>DM 01b</b> | <b>Door contact</b>      | <b>DM 01b</b> | <b>Release door</b> |
| 0   | 03  | <b>DM 01b</b> | "Request to exit" ▾      |               |                     |
| 0   | 04  |               | < not assigned >         |               |                     |
| 0   | 05  |               | "Request to exit" button |               |                     |
| 0   | 06  |               | Bolt sensor              |               |                     |
| 0   | 07  |               | Passage locked           |               |                     |
| 0   | 08  |               | Sabotage                 |               |                     |

Ebenso können Sie zusätzliche Signale für den jeweiligen Durchtritt erstellen. Wenn Sie auf eine leere Zeile doppelklicken, wird das entsprechende Kombinationsfeld geöffnet:

DM 01b Terminals

Signal allocation of 'AMC 4-R4' with 8 signal pairing

| B.. | T.. | entrance      | Input signal         | entrance      | Output signal       |
|-----|-----|---------------|----------------------|---------------|---------------------|
| 0   | 01  | DM 01a        | Door contact         | DM 01a        | Release door        |
| 0   | 02  | <b>DM 01b</b> | <b>Door contact</b>  | <b>DM 01b</b> | <b>Release door</b> |
| 0   | 03  | <b>DM 01b</b> | "Request to exit"... |               |                     |
| 0   | 04  | <b>DM 01b</b> | Bolt sensor ▾        |               |                     |
| 0   | 05  |               |                      |               |                     |
| 0   | 06  |               |                      |               |                     |
| 0   | 07  |               |                      |               |                     |
| 0   | 08  |               |                      |               |                     |

Signalzuweisungen, die für den Durchtritt, den Sie bearbeiten nicht geeignet sind, sind schreibgeschützt und werden grau hinterlegt angezeigt. Diese können nur bearbeitet werden, während der entsprechende Durchtritt ausgewählt ist.

Ausgänge, die auf der AMC-Registerkarte **Ausgänge** parametrisiert wurden, sind ebenfalls grau hinterlegt und haben eine helle Vordergrundfarbe.



### Hinweis!

Die Kombinationsfelder sind nicht 100 % kontextabhängig, weswegen es möglich ist, Signale auszuwählen, die in der Praxis nicht funktionieren. Wenn Sie Signale auf der Registerkarte **Signale** hinzufügen, testen Sie diese, um sicherzustellen, dass sie logisch und physisch mit dem Durchtritt kompatibel sind.

### Signalzuweisung

Auf der Registerkarte **Signal** werden für jeden AMC und jeden Durchtritt alle 8 Signale für den AMC in 8 separaten Zeilen aufgelistet. Nicht verwendete Signale sind weiß, verwendete Signale hingegen blau markiert.

Die Liste hat die folgende Struktur:

- **Board:** Nummerierung der AMC Wiegand-Erweiterung (0) oder der E/A-Erweiterung (1 bis 3)
- **Terminal (Signal):** Anzahl der Kontakte am AMC (01 bis 08) oder der Wiegand-Erweiterung (09 bis 16).
- **Entrance (Durchtritt):** Name des Durchtritts
- **Output signal (Ausgangssignal):** Name des Ausgangssignals
- **Entrance (Durchtritt):** Name des Durchtritts
- **Input signal (Eingangssignal):** Name des Eingangssignals

| 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   |          |              |          |               |

### Ändern der Signalzuweisung

Auf den Registerkarten „Terminal (Signal)“ der Controller wird die Zuweisung der separaten Signale nur angezeigt (schreibgeschützt). Auf den Registerkarten „Terminal (Signal)“ der jeweiligen Durchtritte ist es jedoch möglich, die Signale der gewählten Durchtritte zu ändern oder umzusetzen.

Wenn Sie in der Spalte **Output signal (Ausgangssignal)** oder **Input signal (Eingangssignal)** auf den Eintrag doppelklicken, den Sie ändern möchten, wird eine Dropdown-Liste geöffnet, sodass Sie einen anderen Wert als Signal für das Türmodell wählen können. Wenn Sie **Not assigned (Nicht zugewiesen)** wählen, wird das Signal freigegeben und kann für andere Durchtritte verwendet werden.

Sie können also nicht nur Signale ändern, sondern Signale auch anderen Kontakten zuweisen, um die Nutzung der verfügbaren Spannung zu optimieren. Alle freien oder freigegebenen Kontakte können später für neue Signale oder als neue Positionen für vorhandene Signale verwendet werden.





**Hinweis!**

Im Prinzip können alle Eingangs- und Ausgangssignale frei gewählt werden. Allerdings ist nicht jede Auswahl für alle Türmodelle sinnvoll. Beispiel: Es wäre nicht sinnvoll, einem Türmodell (z. B. 01 oder 03) EMA-Signale zuzuweisen, wenn es keine EMA unterstützt. Weitere Einzelheiten finden Sie in der Tabelle im Abschnitt "Zuweisen von Signalen zu Türmodellen".

**Zuweisen von Signalen zu Türmodellen**

Um eine fehlerhafte Parametrierung zu vermeiden, enthalten die Pulldown-Menüs, über die Sie Türmodellen Signale zuweisen können, nur die Signale, die mit dem gewählten Türmodell kompatibel sind.

**Tabelle der Eingangssignale**

| <b>Eingangssignale</b>  | <b>Beschreibung</b>   |
|---|---|
| Door sensor (Türsensor)   |   |
| Request to exit button (Türtaster)  | Türöffnungsknopf  |
| Bolt sensor (Riegelkontakt)   | Wird nur für Meldungen verwendet. Es ist keine Steuerungsfunktion vorhanden.  |
| Entrance locked (Durchtritt verriegelt)                                   | Wird verwendet, um die gegenüberliegende Tür in Schleusen vorübergehend zu verriegeln. Kann jedoch auch zum permanenten Verriegeln verwendet werden.  |
| Sabotage  | Sabotagesignal eines externen Controllers.  |
| Turnstile in normal Position (Drehkreuz in normaler Position)             | Drehkreuz ist geschlossen.  |
| Passage completed (Durchtritt beendet)                                    | Ein Durchtritt wurde erfolgreich abgeschlossen. Hierbei handelt es sich um einen Impuls eines externen Controllers.   |
| IDS: ready to arm (EMA: bereit zum Scharfschalten)                        | Wird von der EMA gesetzt, wenn sich alle Melder in Ruhestellung befinden und die EMA scharfgeschaltet werden kann.  |
| IDS: is armed (EMA: ist scharfgeschaltet)                                 | Die EMA ist scharfgeschaltet.   |
| IDS: request to arm button (EMA: Taste zum Anfordern der Scharfschaltung) | Taste zum Scharfschalten der EMA.   |
| Local open enable (Lokale Öffnung aktivieren)                             | Wird verwendet, wenn die Tür aufgrund einer bestimmten Regelung ohne Beteiligung des AMC geöffnet wird. Der AMC sendet keine Einbruchsmeldung, aber die Meldung, dass die Tür lokal geöffnet wurde. |

|  |  |
|--|--|
| Externe Zutrittsentscheidung akzeptiert. | Signal wird gesetzt, wenn eine externe Zutrittsentscheidung akzeptiert wird. |
| Externe Zutrittsentscheidung abgelehnt.  | Signal wird gesetzt, wenn eine externe Zutrittsentscheidung akzeptiert wird. |

**Tabelle der Ausgangssignale**

| Ausgangssignale  | Beschreibung  |
|--|---|
| Door opener (Türöffner)  |   |
| Sluice: lock opposite direction (Schleuse: Gegenrichtung verriegeln) | Verriegelt die andere Seite der Schleuse. Dieses Signal wird gesendet, wenn sich die Tür öffnet.                              |
| Alarm suppression (Alarmunterdrückung)                               | ... gegenüber EMA. Wird gesetzt, solange die Tür geöffnet ist, um zu vermeiden, dass die EMA eine Einbruchsmeldung generiert. |
| Indicator green (Anzeige grün)                                       | Anzeigelampe – wird verwendet, solange die Tür geöffnet ist.  |
| Door open too long (Tür zu lange geöffnet)                           | Impulse von drei Sekunden. Wenn die Tür zu lange geöffnet ist.  |
| Camera activation (Kameraaktivierung)                                | Die Kamera wird zu Beginn eines Durchtritts aktiviert.  |
| Open turnstile inbound (Drehkreuz nach innen öffnen)                 |   |
| Open turnstile outbound (Drehkreuz nach außen öffnen)                |   |
| Door is permanent open (Tür ist dauerhaft geöffnet)                  | Signal zum Entsperren einer Tür für eine längere Zeit.  |
| IDS: arm (EMA: scharfschalten)                                       | Signal zum Scharfschalten der EMA.  |
| IDS: disarm (EMA: unscharfschalten)                                  | Signal zum Unscharfschalten der EMA.  |
| Externe Zutrittsentscheidung aktiviert.                              | Signal muss gesetzt werden, um das System für externe Zutrittsentscheidung zu aktivieren.                                     |

**Mapping-Tabelle von Türmodellen zu Ein- und Ausgangssignalen**

Die folgende Tabelle listet sinnvolle Zuordnungen von Signalen und Türmodellen auf.

| Türmodell | Beschreibung | Eingangssignale | Ausgangssignale |
|-----------|--------------|-----------------|-----------------|
|-----------|--------------|-----------------|-----------------|

|    |  |   |   |
|----|--|---|---|
| 01 | Einfache Tür mit Eingangs- und Ausgangsleser Leser für Zeit und Anwesenheit Externe Zutrittsentscheidung verfügbar.          | <ul style="list-style-type: none"> <li>- Door sensor (Türsensor)</li> <li>- "Request to exit" button (Türtaster)</li> <li>- Riegelkontakt</li> <li>- Entrance locked (Durchtritt verriegelt)</li> <li>- Sabotage</li> <li>- Local open enable (Lokale Öffnung aktivieren)</li> <li>- External access decision accepted (Externe Zutrittsentscheidung akzeptiert)</li> <li>- External access decision denied (Externe Zutrittsentscheidung abgelehnt)</li> </ul> | <ul style="list-style-type: none"> <li>- Door opener (Türöffner)</li> <li>- Sluice. lock opposite direction (Schleuse: Gegenrichtung verriegeln)</li> <li>- Alarm suppression (Alarmunterdrückung)</li> <li>- Indicator green (Anzeige grün)</li> <li>- Camera activation (Kameraaktivierung)</li> <li>- Door open too long (Tür zu lange geöffnet)</li> <li>- External access decision activated (Externe Zutrittsentscheidung aktiviert)</li> </ul>   |
| 03 | Drehtür mit Eingangs- und Ausgangsleser Leser für Zeit und Anwesenheit Externe Zutrittsentscheidung verfügbar.               | <ul style="list-style-type: none"> <li>- Turnstile in rest position (Drehkreuz in Ruhelage)</li> <li>- "Request to exit" button (Türtaster)</li> <li>- Entrance locked (Durchtritt verriegelt)</li> <li>- Sabotage</li> <li>- External access decision accepted (Externe Zutrittsentscheidung akzeptiert)</li> <li>- External access decision denied (Externe Zutrittsentscheidung abgelehnt)</li> </ul>  | <ul style="list-style-type: none"> <li>- Sluice. lock opposite direction (Schleuse: Gegenrichtung verriegeln)</li> <li>- Open turnstile inbound (Drehkreuz nach innen öffnen)</li> <li>- Open turnstile outbound (Drehkreuz nach außen öffnen)</li> <li>- Alarm suppression (Alarmunterdrückung)</li> <li>- Camera activation (Kameraaktivierung)</li> <li>- Door open too long (Tür zu lange geöffnet)</li> <li>- External access decision activated (Externe Zutrittsentscheidung aktiviert)</li> </ul> |
| 05 | Parkplatzeingang oder -ausgang – maximal 24 Parkzonen Leser für Zeit und Anwesenheit Externe Zutrittsentscheidung verfügbar. | <ul style="list-style-type: none"> <li>- Door sensor (Türsensor)</li> <li>- "Request to exit" button (Türtaster)</li> <li>- Entrance locked (Durchtritt verriegelt)</li> <li>- Passage completed (Durchtritt beendet)</li> <li>- External access decision accepted (Externe Zutrittsentscheidung akzeptiert)</li> </ul>   | <ul style="list-style-type: none"> <li>- Door opener (Türöffner)</li> <li>- Alarm suppression (Alarmunterdrückung)</li> <li>- Indicator green (Anzeige grün)</li> <li>- Door open too long (Tür zu lange geöffnet)</li> <li>- Door is permanent open (Tür ist dauerhaft geöffnet)</li> </ul>  |

|    |  |   |   |
|----|--|---|---|
|    |  | - External access decision denied (Externe Zutrittsentscheidung abgelehnt)  | - External access decision activated (Externe Zutrittsentscheidung aktiviert)   |
| 06 | Leser für Zeit und Anwesenheit   |   |   |
| 07 | Aufzug – maximal 56 Stockwerke   |   |   |
| 09 | Leser und Drucktaste<br>Fahrzeugeingang- oder -ausgang<br>Leser für Zeit und Anwesenheit<br>Externe Zutrittsentscheidung verfügbar.                                      | - Door sensor (Türsensor)<br>- "Request to exit" button (Türtaster)<br>- Entrance locked (Durchtritt verriegelt)<br>- Passage completed (Durchtritt beendet)<br>- External access decision accepted (Externe Zutrittsentscheidung akzeptiert)<br>- External access decision denied (Externe Zutrittsentscheidung abgelehnt)   | - Door opener (Türöffner)<br>- Alarm suppression (Alarmunterdrückung)<br>- Indicator green (Anzeige grün)<br>- Door open too long (Tür zu lange geöffnet)<br>- Door is permanent open (Tür ist dauerhaft geöffnet)<br>- External access decision activated (Externe Zutrittsentscheidung aktiviert) |
| 10 | Einfache Tür mit Eingangs- und Ausgangsleser und Scharfschaltung/ Unscharfschaltung der EMA<br>Leser für Zeit und Anwesenheit<br>Externe Zutrittsentscheidung verfügbar. | - Door sensor (Türsensor)<br>- "Request to exit" button (Türtaster)<br>- IDS: ready to arm (EMA: bereit zum Scharfschalten)<br>- IDS: is armed (EMA: ist scharfgeschaltet)<br>- Sabotage<br>- IDS: request to arm (EMA: Scharfschaltung anfordern)<br>- External access decision accepted (Externe Zutrittsentscheidung akzeptiert)<br>- External access decision denied (Externe Zutrittsentscheidung abgelehnt) | - Door opener (Türöffner)<br>- Camera activation (Kameraaktivierung)<br>- IDS: arm (EMA: scharfschalten)<br>- IDS: disarm (EMA: unscharfschalten)<br>- Door open too long (Tür zu lange geöffnet)<br>- External access decision activated (Externe Zutrittsentscheidung aktiviert)                  |
| 14 | Einfache Tür mit Eingangs- und Ausgangsleser und Scharfschaltung/ Unscharfschaltung der EMA  | - Door sensor (Türsensor)<br>- "Request to exit" button (Türtaster)<br>- IDS: ready to arm (EMA: bereit zum Scharfschalten)   | - Door opener (Türöffner)<br>- Camera activation (Kameraaktivierung)<br>- IDS: arm (EMA: scharfschalten)  |

|    |                                |   |  |
|----|--------------------------------|---|--|
|    | Leser für Zeit und Anwesenheit | - IDS: is armed (EMA: ist scharfgeschaltet)<br>- Sabotage<br>- IDS: request to arm (EMA: Scharfschaltung anfordern) | - Door open too long (Tür zu lange geöffnet) |
| 15 | Digitalkontakte                |   |  |

**Zuweisen von Signalen zu Lesern**

Serielle Leser (d. h. Leser an einem AMC2 4R4) und OSDP-Leser können mit lokalen E/A-Signalen optimiert werden. Auf diese Weise können zusätzliche Signale zur Verfügung gestellt und elektrische Pfade zu den Türkontakten verkürzt werden.

Wenn Sie einen seriellen Leser erstellen, werden auf der Registerkarte **Terminals (Signale)** des entsprechenden Durchtritts zwei Eingangs- und zwei Ausgangssignale für jeden Leser unter den Signalen des Controllers und (sofern vorhanden) der AMC Erweiterung angezeigt.



**Hinweis!**

Diese Listeneinträge werden für jeden seriellen Leser unabhängig davon erstellt, ob lokale E/A vorhanden sind oder nicht.

Diese lokalen Signale des Lesers können Funktionen nicht zugewiesen werden, und sie können auch nicht wie die Signale von Controllern und Platinen parametrisiert werden. Sie werden ebenfalls nicht auf den Registerkarten **Input signal** (Eingangssignal) und **Output signal** (Ausgangssignal) angezeigt, und sie können auch nicht für Aufzüge verwendet werden (um beispielsweise den Grenzwert 56 Stockwerke außer Kraft zu setzen). Aus diesem Grund sind sie am besten für die direkte Steuerung von Türen geeignet (z. B. Türöffnung deaktivieren oder Tür freigeben). Hierdurch werden Controllersignale freigegeben, die dann für komplexere parametrisierte Funktionen zur Verfügung stehen.

**Bearbeiten von Signalen**

Wenn Sie einen Durchtritt erstellen, werden auf der Registerkarte **Terminals (Signale)** des entsprechenden Durchtritts zwei Eingangs- und zwei Ausgangssignale für jeden Leser unter den Controllersignalen angezeigt. In der Spalte „Board“ wird der Name des Lesers angezeigt.

Die Standardsignale für den Durchtritt werden per Default den ersten freien Signalen des Controllers zugewiesen. Um diese auf die eigenen Signale des Lesers zu verlagern, müssen Sie sie zunächst an ihrer ursprünglichen Position löschen. Wählen Sie hierzu den Listeneintrag **<Not assigned> (Nicht zugewiesen)**.

Doppelklicken Sie auf die Spalte **Input signal (Eingangssignal)** oder **Output signal (Ausgangssignal)** des Lesers, um eine Liste möglicher Signale für das gewählte Türmodell anzuzeigen und das Signal zu verlagern. Wie alle Signale können sie auf der Registerkarte **Terminals (Signale)** des Controllers angezeigt, aber dort nicht bearbeitet werden.

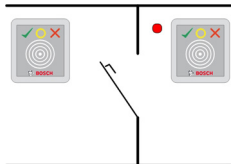


**Hinweis!**

Der Status der Lesersignale kann nicht überwacht werden. Sie können nur für die Tür verwendet werden, der der Leser zugeordnet ist.

## 13.5 Vordefinierte Signale für Türmodelle

### Türmodell 01



Modellvarianten:

|            |   |
|------------|---|
| <b>01a</b> | Normale Tür mit Eingangs- <b>und</b> Ausgangsleser  |
| <b>01b</b> | Einfache Tür mit Eingangsleser und Türöffnungsknopf |
| <b>01c</b> | Normale Tür mit Eingangs- <b>oder</b> Ausgangsleser |

### Mögliche Signale:

| Eingangssignale                               | Ausgangssignale  |
|---|--|
| Door sensor (Türsensor)                       | Door opener (Türöffner)  |
| „Request to exit” button (Türtaster)          | Sluice: lock opposite direction (Schleuse: Gegenrichtung verriegeln) |
| Sabotage                                      | Indicator green (Anzeige grün)                                       |
| Local open enable (Lokale Öffnung aktivieren) | Camera activation (Kameraaktivierung)                                |
|   | Door open too long (Tür zu lange geöffnet)                           |



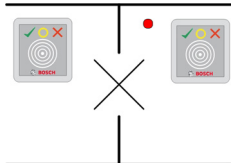
### Hinweis!

Die Vereinzelungsfunktion, insbesondere die Verriegelung der Gegenseite, kann nur bei TM 03 parametrierbar werden.

Die Alarmunterdrückung wird nur aktiviert, wenn die Alarmunterdrückungszeit vor der Türöffnung größer als 0 ist.

Dieses Türmodell kann auch für Fahrzeugdurchritte vorteilhaft sein. In diesem Fall wird ein Sekundärleser für Lkw und Pkw empfohlen.

### Türmodell 03



Modellvarianten:

|            |  |
|------------|--|
| <b>03a</b> | Umschaltbares Drehkreuz mit Eingangs- <b>und</b> Ausgangsleser |
| <b>03b</b> | Umschaltbares Drehkreuz mit Eingangsleser und Türöffnungsknopf |

|            |   |
|------------|---|
| <b>03c</b> | Drehkreuz mit Eingangs- <b>oder</b> Ausgangsleser |
|------------|---|

Mögliche Signale:

| <b>Eingangssignal</b>  | <b>Ausgangssignale</b>   |
|--|--|
| Turnstile in normal Position (Drehkreuz in normaler Position)            | Open turnstile inbound (Drehkreuz nach innen öffnen)                 |
| „Request to exit” button (Türtaster)                                     | Open turnstile outbound (Drehkreuz nach außen öffnen)                |
| Sabotage   | Entrance locked (Durchtritt verriegelt)                              |
|  | Camera activation (Kameraaktivierung)                                |
|  | Door open too long (Tür zu lange geöffnet)                           |
| Zusätzliche Signale, die die Option <b>mantrap</b> (Schleuse) verwenden: |  |
| Entrance locked (Durchtritt verriegelt)                                  | Sluice: lock opposite direction (Schleuse: Gegenrichtung verriegeln) |
|  | Alarm suppression (Alarmunterdrückung)                               |

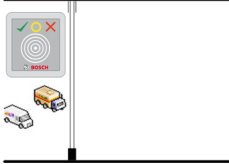
Konfigurationshinweise für Schleusen:

Wenn sich das Drehkreuz in der normalen Position befindet, wird das erste Eingangssignal aller angeschlossenen Leser eingeschaltet. Wenn ein Ausweis eingelesen wird, der Inhaber Zutrittsrechte für diesen Durchtritt hat:

- und der Inhaber sich am Eingangsleser befindet, wird das erste Ausgangssignal am Eingangsleser für die Dauer der Aktivierungszeit gesetzt.
- und der Inhaber sich am Ausgangsleser befindet, wird das zweite Ausgangssignal am Ausgangsleser für die Dauer der Aktivierungszeit gesetzt.

Wenn der Türtaster (REX) gedrückt wird, werden das zweite Eingangssignal und das zweite Ausgangssignal gesetzt. Während dieses Zeitraums kann die Drehtür in der aktivierten Richtung verwendet werden.

**Türmodell 05c**



Modellvariante:

|            |   |
|------------|---|
| <b>05c</b> | Eingangs- <b>oder</b> Ausgangsleser für Parkplatzzugang |
|------------|---|

Mögliche Signale für dieses Türmodell:

| <b>Eingangssignale</b>  | <b>Ausgangssignale</b>  |
|-------------------------|-------------------------|
| Door sensor (Türsensor) | Door opener (Türöffner) |

|   |   |
|---|---|
| „Request to exit” button (Türtaster)    | Door is permanent open (Tür ist dauerhaft geöffnet) |
| Entrance locked (Durchtritt verriegelt) | Indicator green (Anzeige grün)                      |
| Passage completed (Durchtritt beendet)  | Alarm suppression (Alarmunterdrückung)              |
|   | Door open too long (Tür zu lange geöffnet)          |

Sowohl Eingang als auch Ausgang des Parkplatzes müssen auf demselben Controller konfiguriert werden. Wenn einem Controller Parkplatzzugang zugewiesen wurde, kann dieser Controller keine anderen Türmodelle regeln. Für den Zugang zum Parkplatz kann nur ein Eingangsleser (kein Ausgangsleser) zugewiesen werden. Sobald der Eingang zugewiesen wurde, können Sie bei erneutem Wählen des Türmodells nur den Ausgangsleser definieren. Sie können für jeden Parkplatz maximal 24 Unterbereiche definieren, und einer dieser Unterbereiche muss in den Ausweisberechtigungen enthalten sein, damit der Ausweis funktioniert.

**Türmodell 06**



Modellvarianten:

|            |  |
|------------|--|
| <b>06a</b> | Eingangs- <b>und</b> Ausgangsleser für Zeit und Anwesenheit  |
| <b>06c</b> | Eingangs- <b>oder</b> Ausgangsleser für Zeit und Anwesenheit |

Leser, die mit diesem Türmodell erstellt werden, steuern nicht den Zutritt, sondern werden ausschließlich zum Erfassen von Zeit und Anwesenheit eingesetzt. Sie steuern nicht die Türen, sondern leiten die Ausweisdaten an das Zeit- und Anwesenheitssystem weiter. Folglich werden keine Signale definiert. Diese Leser werden in der Regel innerhalb eines bereits kontrollierten Bereichs montiert.



**Hinweis!**

Damit gültige Buchungspaare (Eingangs- und Ausgangszeit) im Zeit- und Anwesenheitssystem erstellt werden können, müssen zwei getrennte Leser mit Türmodell 06 parametrisiert werden: einer für die zeitliche Erfassung des eingehenden Verkehrs und einer für die Erfassung des ausgehenden Verkehrs.

Verwenden Sie Variante **a**, wenn Eingang und Ausgang nicht getrennt sind. Verwenden Sie Variante **c**, wenn Eingang und Ausgang räumlich getrennt sind oder Sie die Leser nicht an denselben Controller anschließen können. Stellen Sie sicher, dass Sie einen der Leser als Leser für eingehenden Verkehr und einen als Leser für ausgehenden Verkehr definieren. Wie bei jedem Durchtritt müssen Sie Berechtigungen erstellen und zuweisen. In Access Engine werden auf der Registerkarte **Time Management** (Zeitwirtschaft) der Dialoge **Access Authorizations** (Zutrittsberechtigungen) und **Area/time authorizations** (Raum-Zeit-Berechtigung) alle definierten Leser für Zeit und Anwesenheit aufgelistet. Aktivieren Sie mindestens einen Leser in eingehender Richtung und einen Leser in ausgehender Richtung. Berechtigungen der Leser für Zeit und Anwesenheit können zusammen mit anderen Zutrittsberechtigungen oder als separate Berechtigungen zugewiesen werden.



Wenn mehr als ein Leser für Zeit und Anwesenheit für eine gegebene Richtung vorhanden ist, können bestimmte Ausweisinhaber bestimmten Lesern zugeordnet werden. Nur die Anwesenheitszeiten zugewiesener und berechtigter Benutzer werden vom Leser registriert und gespeichert.



**Hinweis!**

Andere Zutrittskontrollfunktionen wirken sich auch auf das Verhalten der Leser für Zeit und Anwesenheit aus. Schwarze Listen, Zeitmodelle oder Ablaufdaten können auch verhindern, dass ein Leser für Zeit und Anwesenheit Zutrittszeiten registriert.

Die registrierten Eingangs- und Ausgangszeiten werden im Verzeichnis: C:\MgtS\AccessEngine\AC\TAEExchange unter dem Namen TAccExc\_EXP.txt in einer Textdatei gespeichert und so lange vorgehalten, bis sie in ein Zeit- und Anwesenheitssystem exportiert werden.

Die Buchungsdaten werden in folgendem Format übertragen:

ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.

T=Tag, M=Monat, J=Jahr, h=Stunde, m=Minute, s=Sommerzeit, 0=ausgehend, 1=eingehend  
Die Exportdatei wird nicht nach Personen sortiert, sondern enthält alle Buchungen in der chronologischen Reihenfolge, in der sie vom Administrationsmodul eingegangen sind. Das Feldtrennzeichen in der Datei ist das Semikolon.

**Türmodell 07 – Varianten**



Modellvarianten:

|            |                                   |
|------------|-----------------------------------|
| <b>07a</b> | Aufzug mit maximal 56 Stockwerken |
| <b>07b</b> | Aufzug mit maximal 56 Stockwerken |

**Türmodell 07a**

**Signale:**

| Eingangssignal | Ausgangssignale  |
|----------------|--|
|                | Release <name of the floor> (Freigabe <Name des Stockwerks>) |
|                | Ein Ausgangssignal pro definiertem Stockwerk (maximal 56).   |

Bei Rufen des Aufzugs kann der Ausweisinhaber nur die Stockwerke wählen, für die sein Ausweis berechtigt ist.

Die Aufzugtürmodelle können nicht mit anderen Türmodellen auf demselben Controller gemischt werden. Mithilfe von AMC Erweiterungen können für jeden Aufzug auf einem AMC bis zu 56 Stockwerke definiert werden. Die Ausweisberechtigungen müssen den Aufzug selbst und mindestens ein Stockwerk umfassen.

**Türmodell 07c**

**Signale:**

| Eingangssignal | Ausgangssignal |
|----------------|----------------|
|----------------|----------------|

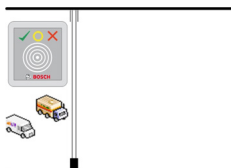
|   |  |
|---|--|
| Input key <name of the floor> (Eingabetaste <Name des Stockwerks>)                      | Release <name of the floor> (Freigabe <Name des Stockwerks>) |
| Für jedes definierte Stockwerk existiert ein Ausgangs- und Eingangseintrag – bis zu 56. |  |

Wenn Sie den Aufzug rufen und eine Taste zum Wählen eines Stockwerks drücken (dies ist der Grund, warum Eingangssignale erforderlich sind), werden die Ausweisberechtigungen überprüft, um festzustellen, ob sie das gewählte Stockwerk enthalten.

Zudem ist es bei diesem Türmodell möglich, beliebige Stockwerke für den **öffentlichen Zugang** zu definieren, für die also keine Berechtigungsprüfung durchgeführt werden muss und die jedermann mit dem Aufzug erreichen kann. Dennoch kann der öffentliche Zugang selbst durch ein **Zeitmodell** geregelt werden, das den Zugang auf bestimmte Stunden an bestimmten Tagen beschränkt. Außerhalb dieser Stunden wird die übliche Berechtigungsprüfung durchgeführt.

Die Aufzugtürmodelle können nicht mit anderen Türmodellen auf demselben Controller gemischt werden. Mithilfe von AMC Erweiterungen können für jeden Aufzug auf einem AMC bis zu 56 Stockwerke definiert werden. Die Ausweisberechtigungen müssen den Aufzug selbst und mindestens ein Stockwerk umfassen.

### Türmodell 09

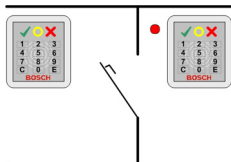


Mögliche Signale:

| Eingangssignale                         | Ausgangssignale                            |
|---|--|
| Door sensor (Türsensor)                 | Door opener (Türöffner)                    |
| „Request to exit” button (Türtaster)    | Tür ist dauerhaft offen                    |
| Entrance locked (Durchtritt verriegelt) | Ampel ist grün                             |
| Passage completed (Durchtritt beendet)  | Alarm suppression (Alarmunterdrückung)     |
|   | Door open too long (Tür zu lange geöffnet) |

Für die Barrieresteuerung wird eine zugrunde liegende Steuerung (SPS) vorausgesetzt. Anders als bei **Türmodell 5c** können Sie diesen Eingang und Ausgang auf verschiedenen AMCs konfigurieren. Des Weiteren gibt es keine Unterbereiche, sondern nur eine allgemeine Berechtigung für den Parkbereich.

### Türmodell 10



**Modellvarianten:**

|            |   |
|------------|---|
| <b>10a</b> | Normale Tür mit Eingangs- <b>und</b> Ausgangsleser <b>und</b> Scharfschaltung/<br>Unscharfschaltung der EMA (Einbruchmeldeanlage) |
| <b>10b</b> | Normale Tür mit Eingang, Türtaster und Scharfschaltung/Unscharfschaltung der<br>EMA   |
| <b>10e</b> | Normale Tür mit Eingang, Türtaster und dezentraler Scharfschaltung/<br>Unscharfschaltung der EMA                                  |

Mögliche Signale:

| <b>Eingangssignale</b>   | <b>Ausgangssignale</b>  |
|--|---|
| Door sensor (Türsensor)  | Door opener (Türöffner)   |
| IDS: is armed (EMA: ist scharfgeschaltet)                                    | IDS: arm (EMA: scharfschalten)                                    |
| IDS: ready to arm (EMA: bereit zum<br>Scharfschalten)                        | IDS: disarm [only DM 10e] (EMA:<br>unscharfschalten [nur TM 10e]) |
| „Request to exit” button (Türtaster)   | Camera activation (Kameraaktivierung)                             |
| Bolt sensor (Riegelkontakt)  | Door open too long (Tür zu lange geöffnet)                        |
| Sabotage   |   |
| IDS: request to arm button (EMA: Taste zum<br>Anfordern der Scharfschaltung) |   |



**Hinweis!**

Für dieses Türmodell sind Leser mit Tastatur erforderlich. Ausweisinhaber müssen **PIN-Codes** eingeben, um die EMA scharf- oder unscharfzuschalten.

Abhängig von den montierten Lesern müssen unterschiedliche Verfahren durchgeführt werden.

**I-BPR-Leser:** (z. B. DELTA 1010, INTUS 1600)

Drücken Sie zum Scharfschalten die Taste **7**, und bestätigen Sie mit der Eingabetaste (#).  
Lesen Sie den Ausweis ein, geben Sie den PIN-Code ein, und bestätigen Sie erneut mit der  
Eingabetaste (#).

Lesen Sie zum Unscharfschalten den Ausweis ein, geben Sie den PIN-Code ein, und bestätigen  
Sie mit der Eingabetaste (#).

**BPR-Leser:** (einschließlich Wiegand)

Drücken Sie zum Scharfschalten die Taste 7, lesen Sie den Ausweis ein, und geben Sie den  
PIN-Code ein. Eine Bestätigung des Vorgangs durch Drücken der Eingabetaste ist nicht  
erforderlich.

Lesen Sie zum Unscharfschalten den Ausweis ein, und geben Sie den PIN-Code ein.  
Unscharfschaltung und Türfreigabe erfolgen gleichzeitig.

**Sondermerkmale des TM 10e:**

Bei den Türmodellen 10a und 10b bildet jeder Durchtritt den eigenen Sicherheitsbereich, während beim Türmodell 10e mehrere Durchtritte zu Einheiten gruppiert werden können. Jeder einzelne Leser in dieser Gruppe kann die gesamte Einheit scharf- oder unscharfschalten. Das Ausgangssignal **EMA unscharfschalten** ist erforderlich, um den Status zurückzusetzen, der von einem Leser in der Gruppe festgelegt wurde.

Signale:

- Türmodell 10a und 10b:
  - Scharfschaltung wird durch ein konstantes Signal ausgelöst.
  - Unscharfschaltung wird durch die Aussetzung des konstanten Signals ausgelöst.
- Türmodell 10e:
  - Scharfschaltung und Unscharfschaltung werden durch einen Signalimpuls mit einer Dauer von 1 Sekunde ausgelöst.

[Mit einem bistabilen Relais kann die EMA von mehreren Türen gesteuert werden. Dazu ist für die Signale aller Türen eine OR-Verknüpfung am Relais erforderlich. Die Signale **IDS armed** (EMA scharfgeschaltet) und **IDS ready to arm** (EMA bereit zum Scharfschalten) müssen an allen beteiligten Türen repliziert werden.]

## 13.6

### Sonderdurchtritte

#### 13.6.1

#### Aufzüge (DM07)

##### Allgemeine Hinweise zu Aufzügen (Türmodell 07)

Aufzüge können nicht mit anderen Türmodellen auf dem gleichen AMC-Controller kombiniert werden.

Aufzüge können nicht mit den Leseroptionen **Group access** (Gruppenbegehung) oder **Attendant required** (Begleiter erforderlich) verwendet werden.

Bis zu acht Stockwerke können auf einem AMC definiert werden. Eine AMC-Erweiterung bietet je Erweiterung acht oder 16 zusätzliche Ausgänge.

Daher ist es bei Nutzung der maximalen Anzahl der größten Erweiterungsplatinen möglich, bis zu 56 Etagen mit RS485-Lesern zu konfigurieren, sowie 64 Etagen mit Wiegand-Lesern, wenn zusätzlich eine spezielle Wiegand-Erweiterungsplatine verwendet wird.

##### Unterschiede zwischen Türmodell 07a und 07c

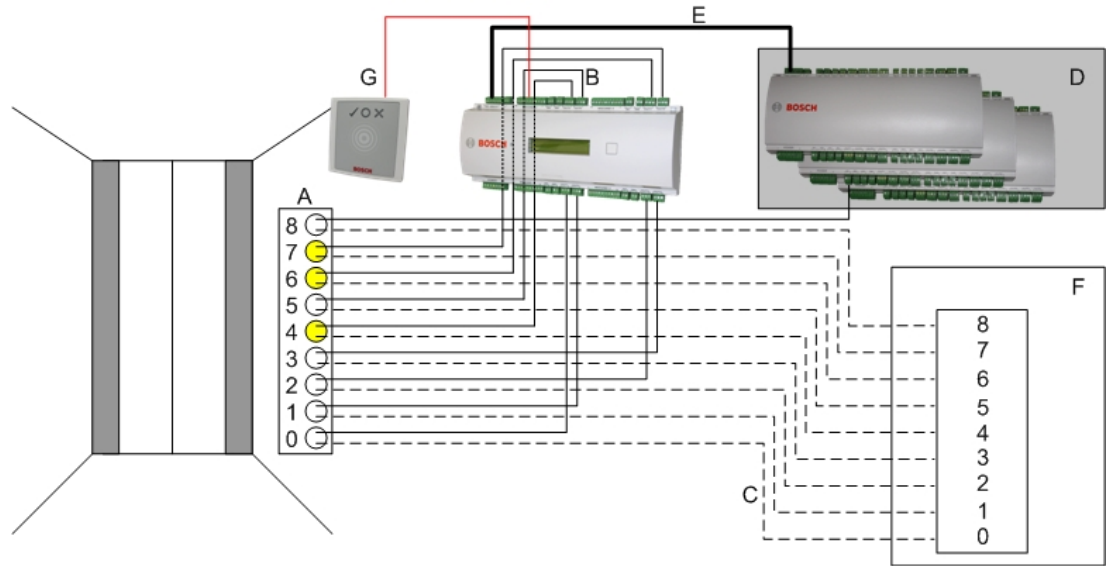
In den Zutrittsberechtigungsdialogen des Access Engine Systems können Sie bestimmte Etagen der Berechtigung einer Person zuweisen.

Wenn der Aufzug mithilfe des Türmodells **07a** erstellt wurde, liest die Person ihren Ausweis ein und die Etagen, zu denen sie Zugang hat, sind dann verfügbar.

Beim Türmodell **07c** überprüft das System die Berechtigung für die gewählte Etage, nachdem die Person sie gewählt hat. Die als **öffentlich** gekennzeichneten Stockwerke sind für jedermann unabhängig von der Berechtigung zugänglich. Zusammen mit einem Zeitmodell kann der öffentliche Zugang eingeschränkt werden. Außerhalb dieses Zeitraums wird die Berechtigung für das gewählte Stockwerk überprüft.

##### Verkabelungsschema für Aufzüge:

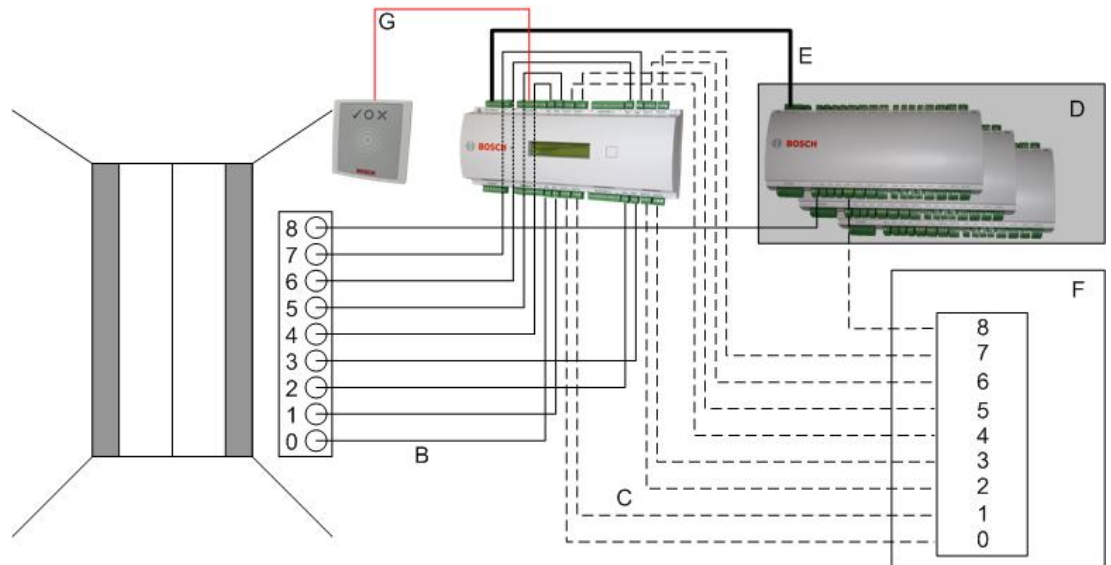
In der folgenden Abbildung wird das Anschlussschema eines Aufzugs mithilfe des Türmodells 07a veranschaulicht.



Legende:

- A = Tastenfeld des Aufzugs
- B = (durchgezogene Linie) AMC-Ausgangssignale
- C = (gestrichelte Linie) Anschluss an die Aufzugsteuerung
- D = Maximal drei E/A-Erweiterungen können an einen AMC angeschlossen werden, sofern dessen eigene acht Ein- und Ausgänge nicht ausreichend sind.
- E = Daten und Stromversorgung vom AMC zu den E/A-Erweiterungen
- F = Etagenauswahl des Aufzugs
- G = Leser. Zwei Leser können für jeden Aufzug konfiguriert werden.

In der folgenden Abbildung ist das Anschlussschema eines Aufzugs mithilfe des Türmodells 07c dargestellt.



Legende:

- B = (durchgezogene Linie) AMC-Ausgangssignale
- C = (gestrichelte Linie) Anschluss an die Aufzugsteuerung
- D = Maximal drei E/A-Erweiterungen können an einen AMC angeschlossen werden, sofern dessen eigene acht Ein- und Ausgänge nicht ausreichend sind.
- E = Daten und Stromversorgung vom AMC zu den E/A-Erweiterungen
- F = Etagenauswahl des Aufzugs

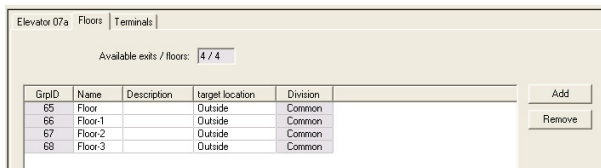
- G = Leser. Zwei Leser können für jeden Aufzug konfiguriert werden.

Wie Parkplätze haben Aufzüge den Parameter **Öffentlich**. Dieser Parameter kann für jedes Stockwerk individuell gesetzt werden. Wenn der Parameter **Öffentlich** aktiviert ist, werden Zutrittsberechtigungen nicht überprüft – so kann jeder Ausweisinhaber im Aufzug das Stockwerk auswählen.

Legen Sie auf Wunsch ein Zeitmodell für das Eintrittsmodell fest: Außerhalb der definierten Zeitzonen werden Berechtigungen geprüft.

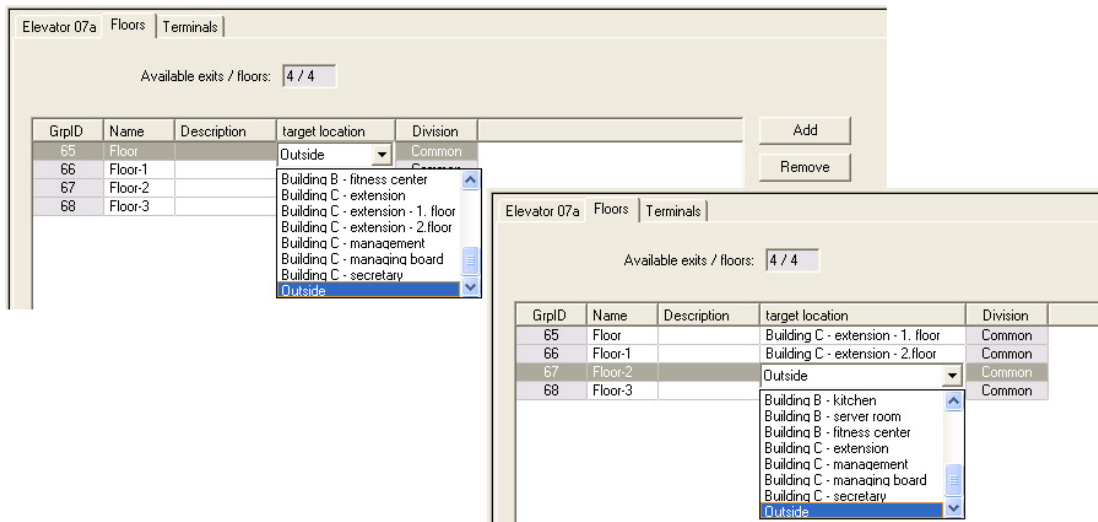
**Stockwerke für Türmodell 07**

Verwenden Sie die Registerkarte **Floors** (Stockwerke) zum Hinzufügen und Entfernen von Stockwerken für den Aufzug mit den Schaltflächen **Add** (Hinzufügen) und **Remove** (Entfernen).

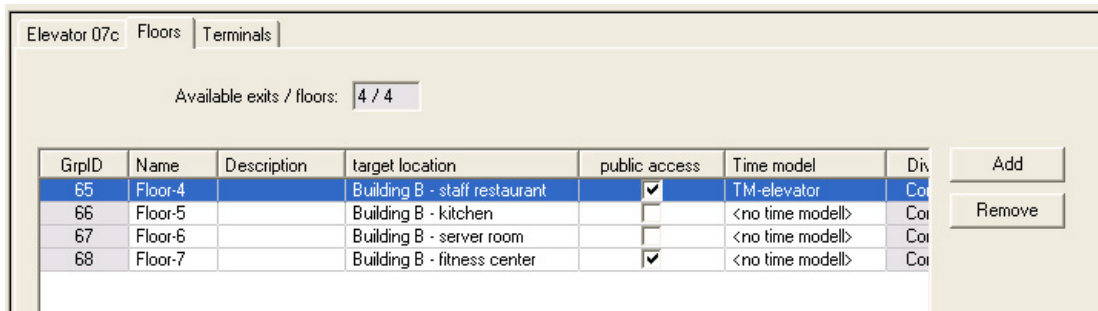


Zielorte für ein Stockwerk können alle **Bereiche** mit Ausnahme von Parkplätzen und Parkzonen sein.

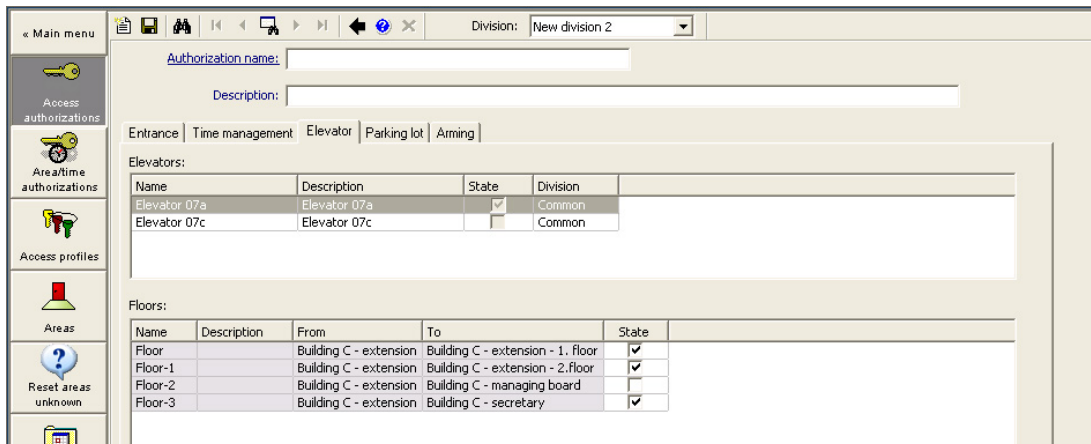
Einem Stockwerk kann nur ein Bereich zugewiesen werden. Aus diesem Grund wird nach jeder Zuweisung die Auswahl in den Kombinationsfeldern verringert, um unbeabsichtigte Doppelzuweisungen zu verhindern.



Wenn Sie das Türmodell 07a verwenden, können Sie einzelne Stockwerke öffentlich zugänglich machen, indem Sie das Kontrollkästchen **public access** (öffentlicher Zugang) aktivieren. In diesem Fall werden keine Berechtigungen überprüft. Durch die zusätzliche Zuweisung eines **Zeitmodells** kann der Zugang auf vordefinierte Zeiträume begrenzt werden.



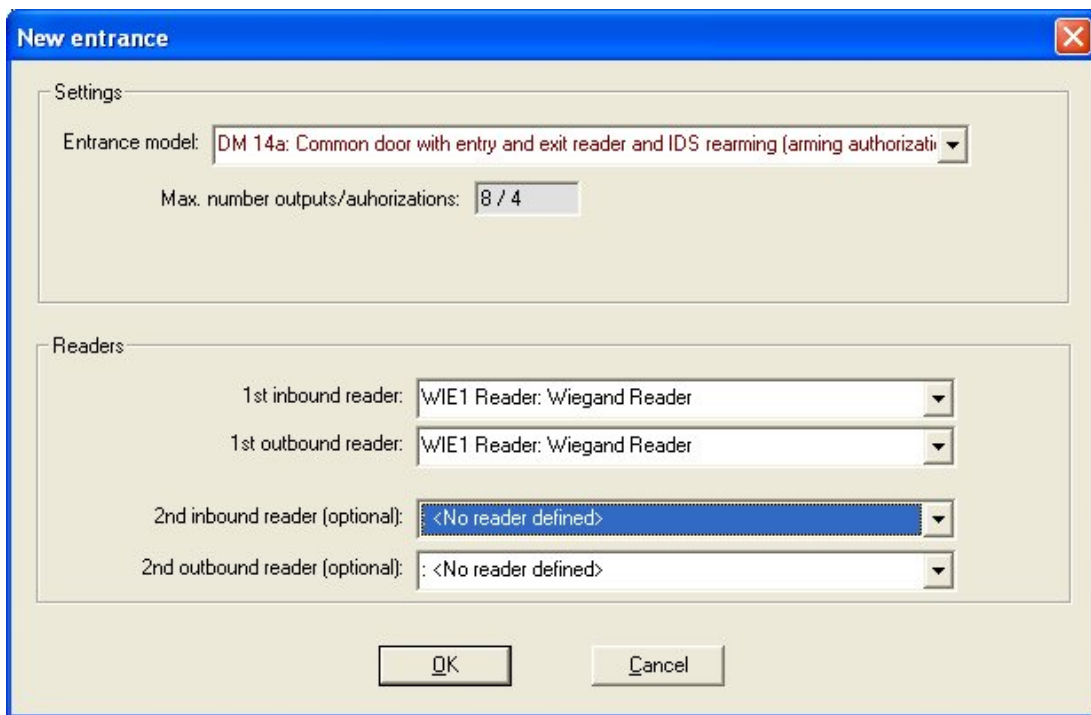
Wählen Sie auf der Registerkarte **Elevator** (Aufzüge) über dem oberen Listenfeld in den Access Engine-Dialogen **Access authorizations** (Zutrittsberechtigungen) und **Area/time authorization** (Raum-Zeit-Berechtigung) zunächst den gewünschten Aufzug und anschließend darunter die Etagen, zu denen dem Ausweisinhaber Zugang gewährt werden soll.



### 13.6.2 Türmodelle mit Einbruchsalarmen (DM14)

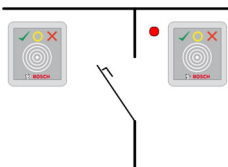
#### Scharf- und Unscharfschalten von Einbruchmeldeanlagen – DM 14

Anders als das Türmodell 10 kann DM 14 scharfgeschaltet/unscharfgeschaltet werden.



Ein Scharfschaltebereich wird durch einen Großbuchstaben auf der ersten Seite des Durchtritts gekennzeichnet. Wenn Sie einem Scharfschaltebereich einen Durchtritt zuweisen, gilt die Scharfschaltung an einem Leser für alle Durchritte in diesem Bereich.

**Türmodell 14**



Modellvarianten:

|            |   |
|------------|---|
| <b>14a</b> | Einfache Tür mit Eingangs- und Ausgangsleser und EMA-Scharfschaltung/ Unscharfschaltung |
| <b>14b</b> | Normale Tür mit Eingang, Türöffnungsknopf und Scharfschaltung/Unscharfschaltung der EMA |

Mögliche Signale:

| Eingangssignale   | Ausgangssignale                            |
|---|--|
| Door sensor (Türsensor)   | Door opener (Türöffner)                    |
| IDS: is armed (EMA: ist scharfgeschaltet)                                 | IDS: arm (EMA: scharfschalten)             |
| IDS: ready to arm (EMA: bereit zum Scharfschalten)                        | Camera activation (Kameraaktivierung)      |
| „Request to exit” button (Türtaster)                                      | Door open too long (Tür zu lange geöffnet) |
| Bolt sensor (Riegelkontakt)   |  |
| Sabotage  |  |
| IDS: request to arm button (EMA: Taste zum Anfordern der Scharfschaltung) |  |

Bei Türmodell 14 können gesicherte Bereiche gebildet werden. Die EMA (Einbruchmeldeanlage) kann von jedem Leser im Bereich scharfgeschaltet werden. In diesem Fall müssen die Signale **EMA scharfgeschaltet** und **EMA bereit zum Scharfschalten** an jedem Durchtritt repliziert werden.

Im Gegensatz zu Modell 10 können für das Türmodell 14 Leser mit oder ohne Tastenfeld verwendet werden. Ein weiterer Unterschied ist die Zuweisung von Berechtigungen für Scharfschaltung/Unscharfschaltung. Nur Ausweisinhaber mit korrekter Berechtigung dürfen scharfschalten/unscharfschalten.

Bei Lesern mit Tastenfeld wird die Scharf- und Unscharfschaltung wie bei Türmodell 10 durchgeführt.

Bei Lesern ohne Tastenfeld erfolgt die Scharfschaltung nicht durch Eingeben des PIN-Codes. Stattdessen wird ein Schalter in der Nähe des Lesers verwendet, der dieselbe Funktion wie die Taste 7 der Leser mit Tastenfeld hat. Nach Betätigen dieses Schalters wird der Status des Alarmgeräts durch die farbigen LEDs des Lesers angezeigt:

- unscharf = Grün und Rot leuchten abwechselnd
- scharf = Rot leuchtet konstant

Scharfschaltung durch Einlesen eines Ausweises mit geeigneter Berechtigung.

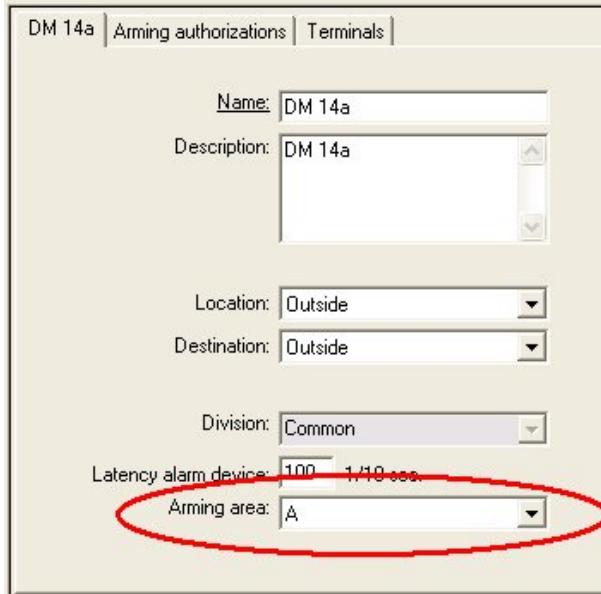
Unscharfschaltung durch Betätigen des Schalters und Einlesen eines Ausweises mit geeigneter Berechtigung.

Die Tür wird bei Unscharfschaltung nicht automatisch freigegeben. Hierzu muss der Ausweis erneut eingelesen werden.



### Scharfschalteberechtigungen für Türmodell 14

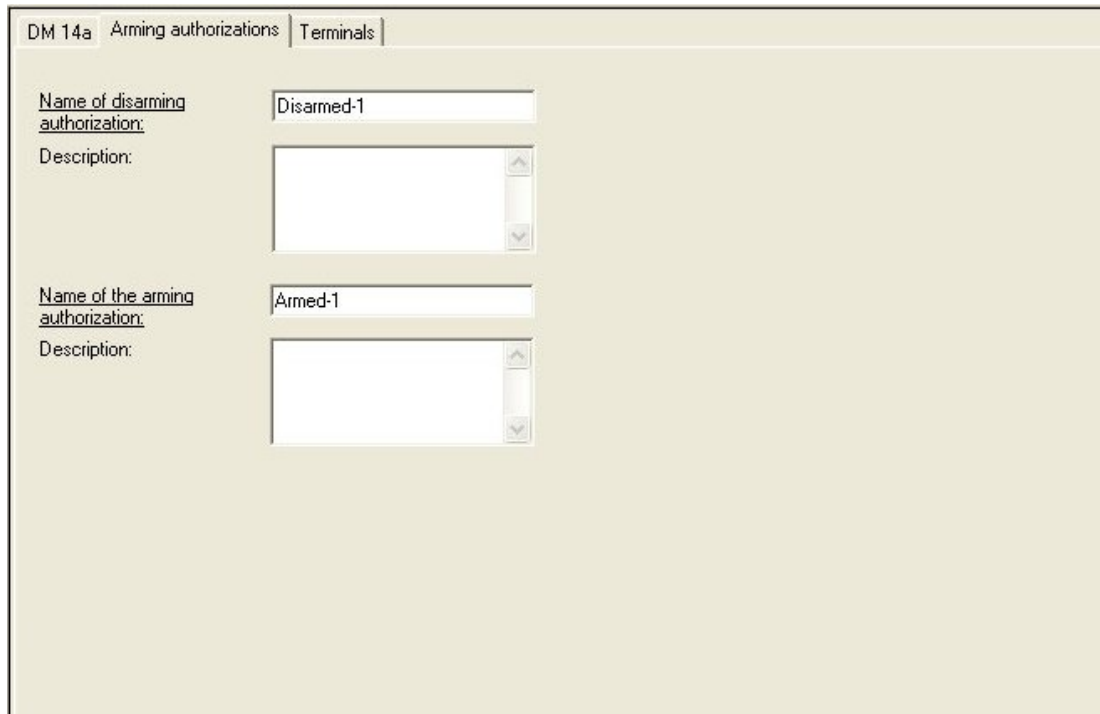
Die erste Registerkarte des Dialogs für Türmodell 14 enthält einen zusätzlichen Parameter zum Erstellen von Scharfschaltebereichen. Mehrere Durchtritte, die mit dem Türmodell 14 konfiguriert wurden, können denselben Scharfschaltebereich referenzieren, sodass jeder Leser in diesem Bereich die EMA (Einbruchmeldeanlage) scharf- oder unscharfschalten kann.



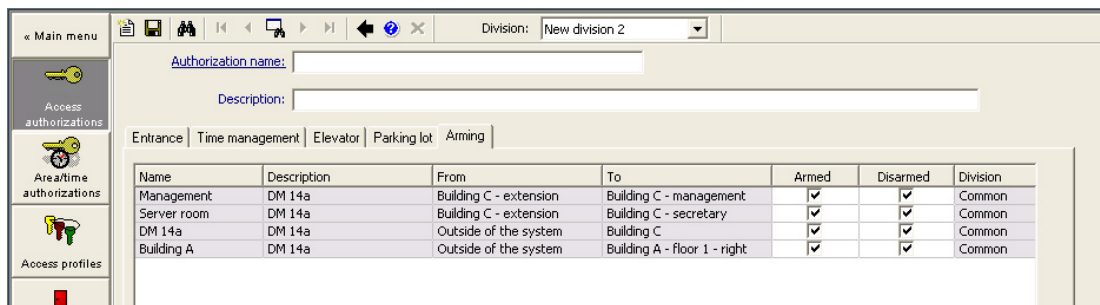
In diesem Fall müssen die Signale **EMA scharfgeschaltet** und **EMA bereit zum Scharfschalten** an den Eingängen der anderen Durchtritte repliziert werden. Wenn ein zweites Türmodell für denselben Scharfschaltebereich erstellt wird, übernimmt der Geräteeditor die Replikation für Sie. Die Beschreibung des Signals der zweiten Tür wird um die Signalnummer des entsprechenden Signals des ersten Türmodells erweitert, beispielsweise 1:04 [= das vierte Signal auf der Erweiterung 1].

| Board    | T... | entrance | Input signal         | entrance | Output signal |
|----------|------|----------|----------------------|----------|---------------|
| AMC 4-R4 | 01   | DM 14b   | Door contact         | DM 14b   | Release do    |
| AMC 4-R4 | 02   | DM 14b   | 1:04:IDS armed       | DM 14b   | Arming IDS    |
| AMC 4-R4 | 03   | DM 14b   | 1:05:IDS ready t...  |          |               |
| AMC 4-R4 | 04   | DM 14b   | Arm IDS              |          |               |
| AMC 4-R4 | 05   | DM 14b   | "Request to exit"... |          |               |
| AMC 4-R4 | 06   | DM 14b.1 | Door contact         | DM 14b.1 | Release door  |

Nachdem Sie ein Türmodell 14 erstellt haben, werden auf der zusätzlichen Registerkarte **Scharfschalteberechtigungen** die erstellten Berechtigungen aufgelistet. Der Benutzer kann Namen für die Scharf-/Unscharfschalteberechtigungen frei wählen.



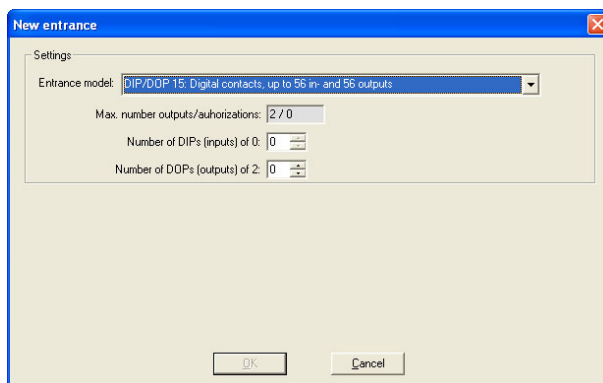
Wenn Sie die Berechtigungen zusammenstellen, werden alle erstellten Instanzen des Türmodells 14 auf der Registerkarte **Arming** (Scharfschalten) der Dialoge **Access authorizations** (Zutrittsberechtigungen) und **Area/time authorizations** (Raum-Zeit-Berechtigung) aufgelistet. Die Berechtigungen für Scharfschaltung und Unscharfschaltung können separat zugewiesen werden.



### 13.6.3 DIPs und DOPs (DM15)

#### Erstellen des Türmodells 15:

Dieses Türmodell bietet unabhängige Eingangs- und Ausgangssignale.



Wenn alle Leserschnittstellen belegt sind, ist nur dieses Türmodell verfügbar. Sie können dieses Türmodell definieren, solange mindestens zwei Signale frei sind. AMCs mit Aufzügen (Modell 07) oder Parkplätzen (Modell 05c) kann dieses Türmodell nicht zugewiesen werden.

**Türmodell 15**

Mögliche Signale: Diese Standardnamen können überschrieben werden.

| Eingangssignal | Ausgangssignal |
|----------------|----------------|
| DIP            | DOP            |
| DIP-1          | DOP-1          |
| ...            | ...            |
| DIP-63         | DOP-63         |

Im Gegensatz zu anderen Türmodellen verwaltet Türmodell 15 die nicht belegten Eingänge und Ausgänge eines Controllers und stellt sie dem gesamten System als allgemeine Eingänge und spannungsfreie Ausgänge zur Verfügung.

Anders als die Ausgangskontakte anderer Türmodelle können die Ausgangskontakte des Türmodells 15 auf der grafischen BIS Benutzeroberfläche einzeln durchsucht werden.

**Wiederherstellen von DOPs nach Neustarts**

Wenn ein MAC oder AMC neu gestartet wird, setzt er normalerweise die Statuswerte seiner untergeordneten DOPs auf den Standardwert 0 (Null) zurück.

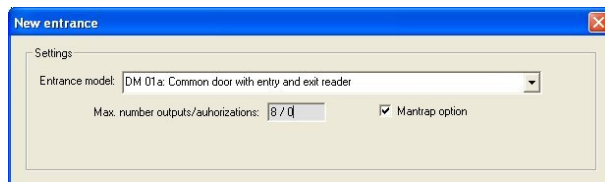
Um einen Neustart sicherzustellen, wird ein DOP immer auf den letzten Status zurückgesetzt, der ihm manuell zugewiesen wurde. Wählen Sie das DOP im Gerätebaum aus und aktivieren Sie das Kontrollkästchen **Keep state** (Status beibehalten) im Hauptfenster.

**13.6.4**

**Schleusentürmodelle**

**Erstellen einer Schleuse**

Die Türmodelle 01 und 03 können als "Schleusen" zum Vereinzeln der Zutritte von Ausweisinhabern verwendet werden. Aktivieren Sie das Kontrollkästchen **Mantrap option** (optionale Schleuse), um die zusätzlich erforderlichen Signale zur Verfügung zu stellen.



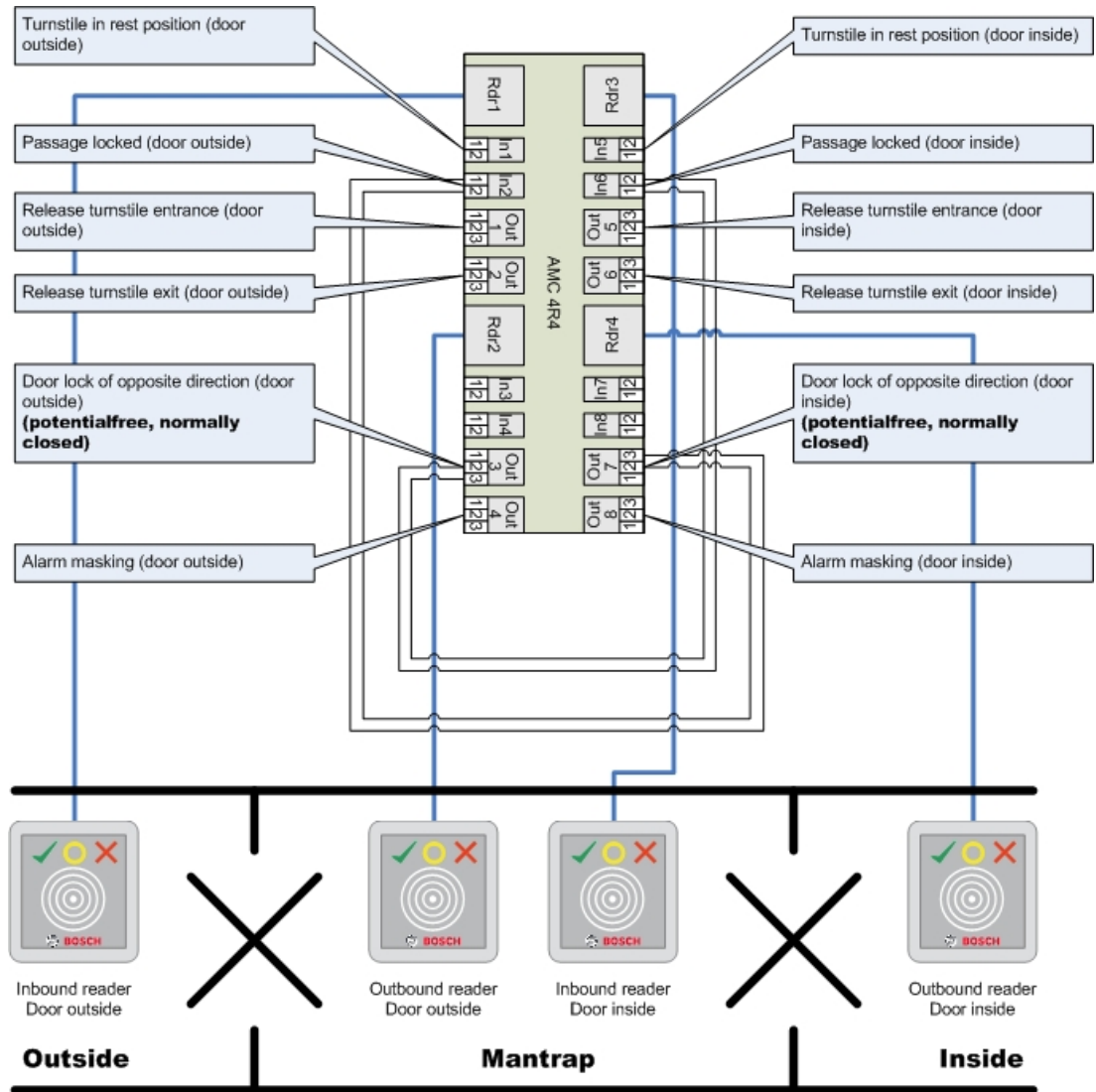
Sie können alle Modelle des Typs 01 und 03 kombinieren, müssen aber diese Option an beiden Durchritten festlegen, die zur Schleuse gehören.

Neben den üblichen Signalzuweisungen für das Türmodell sind für die Option "Mantrap option" (Schleusenoption) weitere eigene Signalzuweisungen erforderlich.

**Beispiel: Schleuse auf einem Controller**

Drehkreuze sind das gängigste Mittel, um den Zugang von Ausweisinhabern zu vereinzeln. In den folgenden Beispielen wurde daher das Türmodell 3a verwendet (Drehkreuz mit Eingangs- und Ausgangsleser).

Schleusenkonfiguration mit zwei Drehkreuzen (TM 03a):



Verbindungen zu den Türverriegelungen für die Gegenrichtung gewährleisten, dass jeweils nur eines der Drehkreuze geöffnet werden kann.

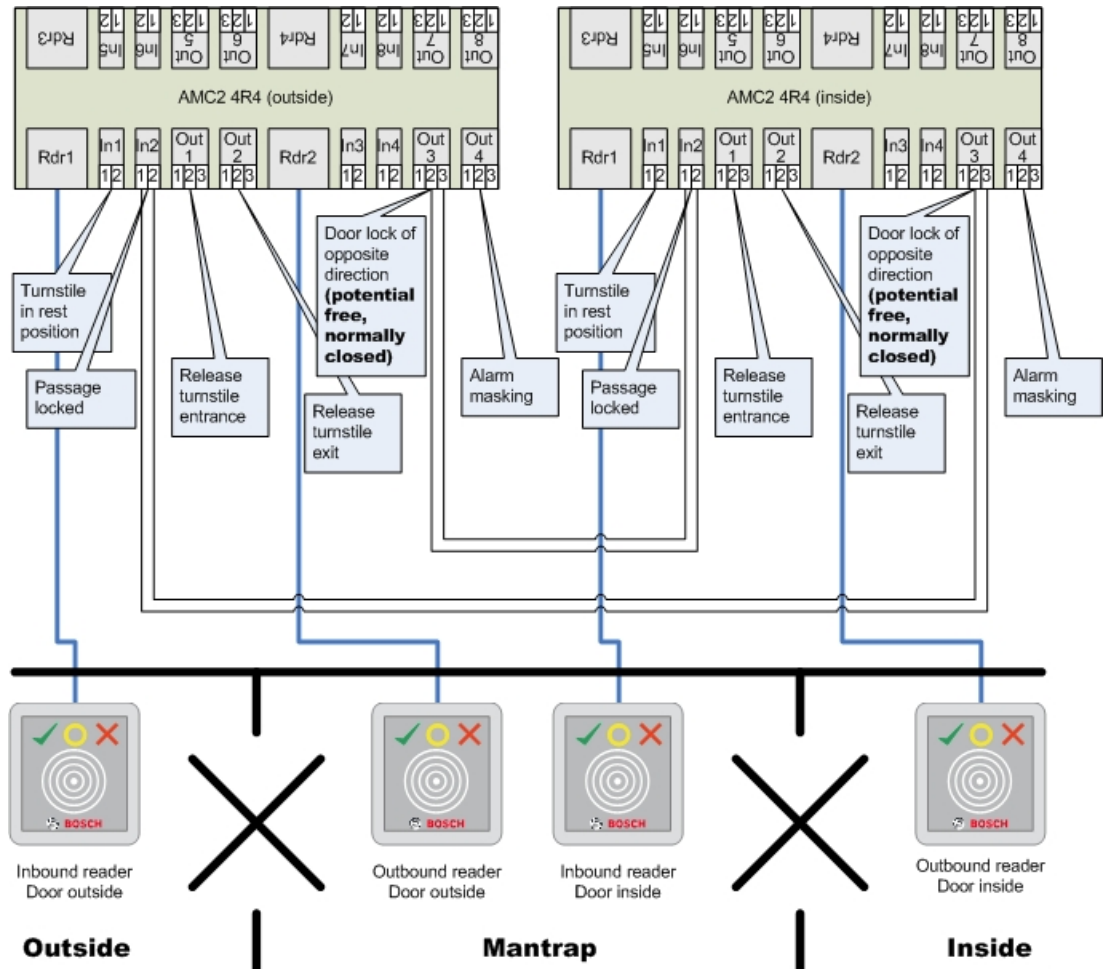


**Hinweis!**

Die Ausgangssignale (Out) 3 und 7 müssen potenzialfrei geschaltet werden (spannungsloser Modus).  
 Das Signal "Türsperre für Gegenrichtung" ist auf der 0 aktiv. Es muss für die Ausgänge 3 und 7 "Öffner" verwendet werden.

**Beispiel: Schleuse auf zwei Controllern**

Schleusenkonfiguration mit zwei Drehkreuzen (TM 03a), die auf zwei Controller verteilt sind:



Verbindungen zu den Türverriegelungen für die Gegenrichtung gewährleisten, dass jeweils nur eines der Drehkreuze geöffnet werden kann.



**Hinweis!**

Das Ausgangssignal (Out) 3 muss potenzialfrei geschaltet werden (spannungsloser Modus). Das Signal "Türsperre für Gegenrichtung" ist auf der 0 aktiv. Es muss für Ausgang 3 "Öffner" verwendet werden.

**13.7**

**Türen**

**Konfigurieren einer Tür: Allgemeine Parameter**

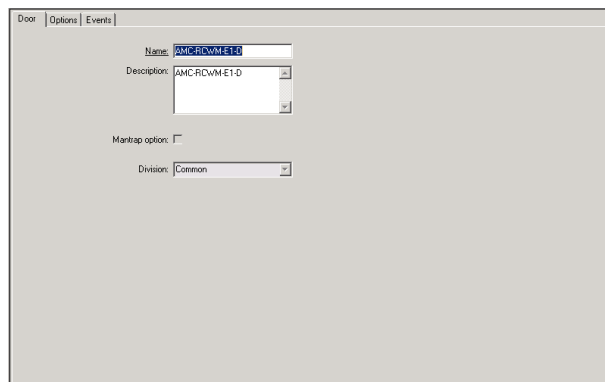
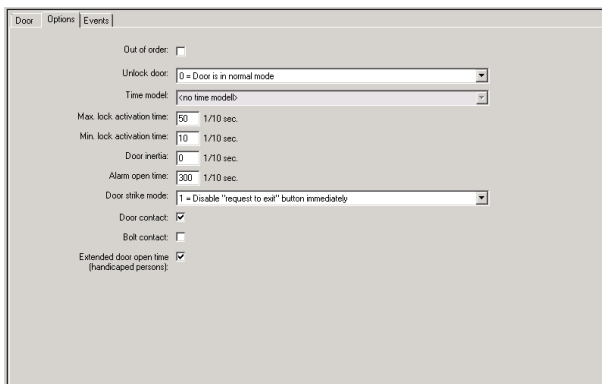


Abbildung 13.1:

| Parameter  | Mögliche Werte   | Beschreibung  |
|--|--|---|
| Name   | Alphanumerisch, bis zu 16 Zeichen  | Der generierte Standardwert kann wahlweise durch einen eindeutigen Namen ersetzt werden.  |
| Beschreibung   | Alphanumerisch, bis zu 255 Zeichen   |   |
| Mandant  | Der Standard-Mandant ist immer "Common" (Allgemein).   | Dies ist ein schreibgeschütztes Feld. Zu jeder Tür in der Gerätehierarchie werden Zuweisungen zu Mandanten im Geräteeditor DevEdit durchgeführt   |
| Nur für Türmodelle 01 und 03 bei Konfiguration einer Schleuse: |  |   |
| Schleusenoption  | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Eine Schleuse existiert, wenn für zwei kombinierte Türen das Türmodell 01 oder 03 verwendet wird. Aktivieren Sie die Schleusenoption für <b>beide</b> Türen. Für die Türen ist ebenfalls eine spezielle physische Verdrahtung erforderlich. |

**Konfigurieren einer Tür: Optionen**

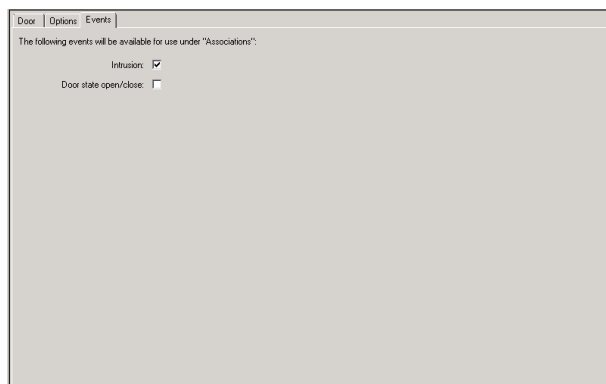


| Parameter                             | Mögliche Werte   | Bemerkung   |
|---------------------------------------|--|---|
| Manual operation (Manuelle Bedienung) | 0 = Kontrollkästchen ist deaktiviert<br>1 = Kontrollkästchen ist aktiviert | 0 = Die Tür befindet sich im Normalmodus (Standard), d. h. sie unterliegt der Zutrittskontrolle durch das Gesamtsystem. 1 = Tür ist vom Zutrittskontrollsystem ausgeschlossen. Die Tür wird nicht gesteuert und generiert keine Meldungen. Sie kann nur manuell gesperrt oder entsperrt werden. Alle anderen Parameter für diese Tür sind ausgeschaltet. Dieser Parameter muss für Tür und Leser getrennt gesetzt werden. |
| Unlock door (Tür entsperren)          | 0 = Tür ist im Normalmodus   | 0 = Normalmodus (Standard) – die Tür wird abhängig von den Zutrittsrechten der Anmeldedaten gesperrt oder entsperrt.  |

|   |   |  |
|---|---|--|
|   | <p>1 = Tür ist entsperrt<br/> 2 = Tür ist zeitmodellabhängig entsperrt<br/> 3 = Tür ist zeitmodellabhängig geöffnet nach erster Begehung<br/> 5 = Tür ist dauerhaft gesperrt<br/> 6 = Tür ist zeitmodellabhängig gesperrt</p> | <p>1 = Für längere Zeit entsperren – Zutrittskontrolle ist für den Zeitraum aufgehoben.<br/> 2 = Für einen Zeitraum entsperren, der vom Zeitmodell definiert ist. Während dieser Zeit ist die Zutrittskontrolle aufgehoben.<br/> 3 = gesperrt, solange das Zeitmodell aktiv ist, bis der ersten Person Zutritt gewährt wird. Anschließend ist sie so lange geöffnet, wie das Zeitmodell aktiv ist.<br/> 5 = blockiert, bis sie manuell entsperrt wird.<br/> 6 = gesperrt, solange das Zeitmodell aktiv ist. Die Tür wird nicht kontrolliert und die Tür kann nicht verwendet werden, wenn das Zeitmodell gültig ist.</p> |
| Time model (Zeitmodell)                               | Eines der verfügbaren Zeitmodelle   | Zeitmodell für Türöffnungszeiten. Wenn Sie die Türmodi 2, 3, 4, 6 und 7 wählen, ist das Listenfeld für die Zeitmodelle verfügbar. Die Auswahl eines Zeitmodells ist erforderlich.  |
| Max. lock activation time (Maximale Aktivierungszeit) | 0 - 9999  | Zeitspanne für die Aktivierung des Türöffners in Zehntelsekunden – Standard: 50 für Türen, 10 für Drehtüren (03) und 200 für Barrieren (05c oder 09c).   |
| Min. lock activation time (Minimale Aktivierungszeit) | 0 - 9999  | Mindestzeitspanne für die Aktivierung des Türöffners in Zehntelsekunden. Elektromagnetische Verriegelungen benötigen eine gewisse Zeit zum Entmagnetisieren. Standard: 10.   |
| Door inertia (Türträgheit)                            | 0 - 9999  | Nachdem die Aktivierungszeit verstrichen ist, kann die Tür in dieser Zeitspanne geöffnet werden, ohne dass Alarm ausgelöst wird. Wert in Zehntelsekunden. Hydrauliktüren benötigen eine gewisse Zeit, um Druck aufzubauen. Standard: 0.  |
| Alarm open time (Alarm-Öffnungszeit)                  | 0 - 9999  | Wenn die Tür nach dieser Zeitspanne geöffnet bleibt, wird eine Meldung ausgegeben (Tür zu lange geöffnet). Wert in Zehntelsekunden. Standard: 300.<br>0 = kein Zeitlimit, keine Meldung  |
| Türöffnermodus  | Listenfeldeintrag   | 0 = Türtaster ist nach der Aktivierungszeit deaktiviert<br>1 = Türtaster ist sofort deaktiviert (= Standard)   |

|  |  |   |
|--|--|---|
| Door contact<br>(Türöffnungskontakt)                                       | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Tür hat keinen Rahmenkontakt<br><br>1 = Tür hat Rahmenkontakt. Ein geschlossener Kontakt bedeutet in der Regel, dass die Tür geschlossen ist (= Standard).  |
| Bolt contact<br>(Türriegelkontakt)   | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Tür hat keinen Riegelkontakt (= Standard)<br><br>1 = Tür hat Riegelkontakt. Eine Meldung wird ausgegeben, wenn die Tür geöffnet oder geschlossen wird.  |
| Extended door open time (Erweiterte Türöffnungszeit) (behinderte Personen) | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Die Aktivierungszeit ist normal.<br>1 = Die Aktivierungszeit wird um den im systemweiten Parameter EXTIMFAC eingestellten Faktor verlängert. Dies gibt behinderten Personen mehr Zeit, um die Tür zu passieren. (= Standard). |

**Konfigurieren einer Tür: Ereignisse**



| Parameter                       | Mögliche Werte   | Bemerkung  |
|---------------------------------|--|--|
| Einbruch                        | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Keine Einbruchmeldung. Dies ist nützlich, wenn eine Tür von der Innenseite frei geöffnet werden kann.<br>1 = Bei unzulässiger Öffnung wird eine Meldung ausgelöst. Eine weitere Meldung gibt die nachfolgende Schließung an (Standard) |
| Türstatus Offen/<br>Geschlossen | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Meldung, dass keine Tür geöffnet ist, wird gesendet (Standard)<br>1 = Eine Meldung wird beim Öffnen oder Schließen gesendet.   |



# 13.8 Leser

## Konfigurieren eines Lesers: Allgemeine Parameter

I-BPR K | Options | Door control | **Additional settings** | Cards

Name : I-BPR K

Description: I-BPR K

Division: Common

Type: I-BPR K

Activate encryption:  Supported only by OSDP v2 readers.

| Parameter                  | Mögliche Werte                                       | Beschreibung  |
|----------------------------|--|---|
| Name des Lesers            | Alphanumerisch, begrenzt auf 1 bis 16 Zeichen        | Der Standardwert kann durch einen eindeutigen Namen ersetzt werden. |
| Description (Beschreibung) | Alphanumerisch: 0 bis 255 Zeichen                    | Eine Freitextbeschreibung.  |
| Mandant                    | Der Standard-Mandant ist immer "Common" (Allgemein). | Nur relevant, wenn Mandanten lizenziert und in Verwendung sind.     |
| Type (Typ)                 | Alphanumerisch, begrenzt auf 1 bis 16 Zeichen        | Typ des Lesers oder einer Leserguppe                                |

### Konfigurieren eines Lesers: Optionen

I-BPR K | Options | Door control | Additional settings | Offline locking system | Key cabinet | Cards

PIN code required:

Time model for PIN codes:

Access also by PIN code alone:

Reader terminal / bus address:

Attendant required:

Membership check:

Membership time model:

Group access:

Deactivate reader beep if access granted:


Deactivate reader beep if access denied:

VDS - Mode:

Max. time for arming:  1/10 Sec.

| Parameter                       | Mögliche Werte  | Beschreibung   |
|---------------------------------|---|--|
| PIN-Code erforderlich           | 0 = PIN-Code deaktiviert – keine Eingabe erforderlich (= Standard)<br>1 = PIN-Code aktiviert – Eingabe immer erforderlich<br>2 = PIN-Code durch Zeitmodell gesteuert – Eingabe nur außerhalb des Zeitmodells erforderlich | Dieses Feld wird nur aktiviert, wenn der Leser über ein Eingabegerät verfügt.<br><br>Beachten Sie, dass die Prüfungen auf dem Ausweis, wie beispielsweise die Berechtigungen und die Zutrittsfolge (falls aktiviert), Vorrang vor der Korrektheit der PIN haben. |
| Zeitmodell für PIN-Codes        | Eines der verfügbaren Zeitmodelle   | Die Auswahl eines Zeitmodells ist hier erforderlich, wenn der Parameter <b>PIN code required</b> (PIN-Code erforderlich) auf 2 gesetzt ist.  |
| Zutritt auch nur durch PIN-Code | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)  | Legt fest, ob dieser Leser den Zutritt auch nur auf der Grundlage eines PIN-Codes gewähren kann, d. h. ohne Ausweis, wenn das Zutrittskontrollsystem so konfiguriert ist. Siehe Zutritt nur durch PIN-Code   |

|                                 |  |  |
|---------------------------------|--|--|
|                                 | 1 = Aktiviert<br>(Kontrollkästchen ist aktiviert)  |  |
| Leserterminal/<br>Busadresse    | 1 - 4  | AMC 4W: nummeriert nach den Wiegand-Schnittstellen<br>AMC 4R4: nummeriert nach der gebrückten Adresse des Lesers   |
| Begleiter erforderlich          | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Besuch braucht keinen Begleiter (= Standard)<br><br>1 = Begleiter muss den Leser ebenfalls verwenden   |
| Zugehörigkeit zur Anlage prüfen | Listeneintrag  | Die Zugehörigkeitsprüfung wird normalerweise in der Anfangsphase verwendet, bevor ein Zutrittskontrollsystem in Betrieb genommen wird. Hier wird der Zutritt basierend auf der generischen Firmen-ID des Ausweises anstatt der eindeutigen Personen-ID gewährt.<br><b>WICHTIG</b> Die Zugehörigkeitsprüfung funktioniert nur mit physischen Ausweisen, bei denen die Ausweisdefinitionen im System vordefiniert sind (grauer Hintergrund) und <b>nicht</b> mit benutzerdefinierten Definitionen oder biometrischen Nachweisen.<br><b>0 – keine Überprüfung</b><br>Die Zugehörigkeitsprüfung ist deaktiviert, aber der Ausweis wird wie üblich auf Autorisierungen geprüft (= Standard).<br><b>1 – Prüfung</b><br>Der Ausweis wird nur auf Firmen-ID geprüft, d. h. auf Zugehörigkeit im System.<br><b>2 – abhängig vom Zeitmodell</b><br>Der Ausweis wird auf Firmen-ID (Zugehörigkeit) geprüft, jedoch nur während des im Zeitmodell „Zugehörigkeit“ definierten Zeitraums. |
| Zeitmodell Zugehörigkeit        | Eines der verfügbaren Zeitmodelle  | Das Zeitmodell aktiviert/deaktiviert die Kontrolle auf Zugehörigkeit.<br>Die Auswahl eines Zeitmodells ist für <b>Zugehörigkeitsprüfung</b> Option 2 obligatorisch.  |
| Gruppenbegehung                 | 1 - 10   | <b>Für Leser mit Tastenfeld:</b><br>Mindestanzahl gültiger Ausweise, die am Dialogleser eingelesen werden müssen, bevor die Tür geöffnet wird. Diese Anzahl kann   |

|  |  |   |
|--|--|---|
|  |  | <p>kleiner als die Anzahl der zur Gruppe gehörenden Ausweise sein. In diesem Fall muss die Eingabetaste/Taste # gedrückt werden, um zu signalisieren, dass die Gruppe vollständig ist. Anschließend wird die Tür geöffnet.</p> <p><b>Für Leser ohne Tastenfeld:</b><br/>                 Genaue Anzahl gültiger Ausweise, die am Ausweisleser eingelesen werden müssen, bevor die Tür geöffnet wird.<br/>                 Der Standardwert ist 1.</p> |
| Lesersignalton deaktivieren, wenn Zutritt gewährt wird   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Bei Aktivierung (1) bleibt der Leser still, wenn ein autorisierter Benutzer Zutritt erhält.   |
| Lesersignalton deaktivieren, wenn Zutritt nicht gewährt wird   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Bei Aktivierung (1) bleibt der Leser still, wenn einem nicht autorisierten Benutzer der Zutritt verweigert wird.  |
|  <p>Die Funktionen für „(Lesersignalton deaktivieren“ hängen von der entsprechenden Firmware des Lesers ab.<br/>                 Die Firmware einiger Leser unterstützen diese Funktion möglicherweise nicht.</p> |  |   |
| VDS-Modus  | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Bei Aktivierung (1) ist die Signalisierung des Lesers ausgeschaltet.  |
| Max. Zeit für Scharfschaltung  | 1 – 100 [1/Sek]  | Maximale Zeit für Rückmeldung vom Einbruchmeldesystem, dass die Scharfschaltung abgeschlossen ist.  |

**Netzwerk- und Betriebsmodi**

Diese Registerkarte wird nur für vernetzte biometrische Leser angezeigt.

**Vorlagen** sind gespeicherte Muster. Dabei kann es sich um Ausweisdaten oder biometrische Daten handeln.

Vorlagen können sowohl auf Geräten über dem Leser im Gerätebaum als auch auf dem Leser selbst gespeichert werden. Daten auf dem Leser werden regelmäßig von den darüber liegenden Geräten aktualisiert.

Der Leser kann so konfiguriert werden, dass er seine eigenen Vorlagen verwendet, wenn er Zutrittsentscheidungen trifft, oder so, dass nur die Vorlagen von den darüber liegenden Geräten verwendet werden.

| Parameter   | Beschreibung   |
|---|--|
| IP-Adresse:   | Die IP-Adresse dieses vernetzten Lesers  |
| Port:   | Der Standardport ist 51211.  |
| <b>Vorlagen auf Server</b>                                    |  |
| Card only (Nur Ausweis)                                       | Der Leser liest nur Ausweisdaten.<br>Er authentifiziert sie gegen Daten aus dem Gesamtsystem.  |
| Card and fingerprint (Ausweis und Fingerabdruck)              | Der Leser liest sowohl Ausweisdaten als auch Fingerabdruckdaten.<br>Er authentifiziert sie gegen Daten aus dem Gesamtsystem.   |
| <b>Vorlagen auf Gerät</b>                                     |  |
| Person dependent verification (Personenabhängige Überprüfung) | Der Leser erlaubt Einstellungen des einzelnen Ausweisinhabers, um festzustellen, welchen <b>Identifikationsmodus</b> er verwendet. Die Personaldaten bieten folgende Möglichkeiten: <ul style="list-style-type: none"> <li>– Fingerprint only (Nur Fingerabdruck)</li> <li>– Card only (Nur Ausweis)</li> <li>– Card and fingerprint (Ausweis und Fingerabdruck)</li> </ul> Diese werden später in dieser Tabelle beschrieben. |
| Fingerprint only (Nur Fingerabdruck)                          | Der Leser liest nur Fingerabdruckdaten.<br>Er authentifiziert sie gegen seine eigenen gespeicherten Daten.   |
| Card only (Nur Ausweis)                                       | Der Leser liest nur Ausweisdaten.<br>Er authentifiziert sie gegen seine eigenen gespeicherten Daten.   |
| Card and fingerprint (Ausweis und Fingerabdruck)              | Der Leser liest sowohl Ausweisdaten als auch Fingerabdruckdaten.<br>Er authentifiziert sie gegen seine eigenen gespeicherten Daten.  |
| Card or fingerprint (Ausweis oder Fingerabdruck)              | Der Leser liest entweder Ausweisdaten oder Fingerabdruckdaten, je nachdem, was der Ausweisinhaber zuerst anbietet.<br>Er authentifiziert sie gegen seine eigenen gespeicherten Daten.  |

### Konfigurieren eines Lesers: Türsteuerung

I-BPR K Options Door control Additional settings Cards

Reader blocking: 0 = Reader is in normal mode

Time model to block reader: <no time model>

Office mode:

Manual operation:

Check time model upon access:

Additional verification:

Host request timeout: 330 1/10 sec.

Open door if no answer from host:

| Parameter   | Mögliche Werte   | Bemerkung   |
|---|--|---|
| Reader blocking (Leser sperren)                         | Listenfeldeintrag  | 0 = Reader in normal mode (0 = Leser ist im Normalbetrieb) – keine Sperrung (= Default)<br>1 = Reader is permanently blocked (1 = Leser ist dauerhaft gesperrt) – dauerhafte Sperrung<br>2 = Leser ist zeitmodellabhängig gesperrt – Sperrung nach Zeitmodell, die mit <i>Time model to block reader</i> (Zeitmodell für Lesersperre) festgelegt wird |
| Time model to block reader (Zeitmodell für Lesersperre) | eines der im System definierten Zeitmodelle.   | Sperrt den Leser gemäß dem ausgewählten Zeitmodell.   |
| Office mode (Büromodus)                                 | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Ermöglicht die Verwendung dieses Lesers im Büromodus,   |
| Manual operation (Manuelle Bedienung)                   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | 0 = Leser ist im Normalbetrieb (= Standard)<br>1 = Leser wird effektiv aus dem Zutrittskontrollsystem entfernt, das heißt, er ist "außer Betrieb".<br>Es werden keine Befehle empfangen. Alle anderen Parameter für diesen Leser sind ausgeschaltet.<br>Der Parameter muss für Leser und Tür unabhängig gesetzt werden.                               |

|   |  |  |
|---|--|--|
| Check time models upon access<br>(Zeitmodelle bei Begehung prüfen)          | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Zeitmodelle werden nicht kontrolliert. Es besteht keine Zeitbeschränkung für den Zutritt.<br>1 = Wenn dem Ausweisinhaber ein Zeitmodell zugewiesen wurde, entweder direkt oder als Raum-Zeit-Berechtigung, wird das Zeitmodell überprüft.<br>(= Standard)  |
| Zusätzliche Überprüfung   | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | 0 = Verifikation durch Host ist nicht erforderlich<br>1 = Verifikation durch Host ist erforderlich (= Standard)<br><b>(WICHTIG:</b> Die Aktivierung dieser Option ist für eine zusätzliche Videoverifikation durch den Bediener eines BVMS- oder BIS-Systems erforderlich.)  |
|   |  |  |
| Wartezeit auf Antwort   | 0 = Ausgeschaltet  | 0 = AMC funktioniert ohne Verifikation durch Host (funktioniert nicht mit <i>Bereichsänderung</i> oder <i>Personenzählungen</i> ). Dieses Kontrollkästchen ist nur aktiv, wenn Verifikation durch Host deaktiviert ist (0) und wenn <i>Open door if no answer from host</i> (Tür öffnen, wenn Host nicht antwortet) aktiviert ist (1).<br>1 bis 9999 = Zum Verwenden des Lesers ist eine BIS Anfrage erforderlich. Diese Anfrage muss innerhalb der festgelegten Zeitspanne beantwortet werden. Wenn die Zeit abläuft, kontrolliert der AMC den Parameter <b>Open door if no answer from host</b> (Tür öffnen, wenn Host nicht antwortet) und trifft die Entscheidung eigenständig. Werte werden in Zehntelsekunden angegeben (Standard = 30). |
| Open door if no answer from host<br>(Tür öffnen, wenn Host nicht antwortet) | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | Dieses Kontrollkästchen ist nur aktiv, wenn der Parameter <b>Host verification</b> (Verifikation durch Host) gesetzt ist.<br>0 = Tür wird nicht geöffnet, wenn eine Hostentscheidung erforderlich ist, aber nicht abgerufen werden kann (Offlinebetrieb).<br>1 = Tür wird nach abgelaufenem Zeitlimit geöffnet, wenn sie vom AMC freigegeben werden kann. (= Standard).  |
| Check parking ticket credits (Parkticket-Guthaben prüfen)                   | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)  | Bei Aktivierung (1) werden die Parkticket-Guthaben geprüft.  |

|   |  |   |
|---|--|---|
|   | 1 = Aktiviert<br>(Kontrollkästchen ist aktiviert)  |   |
| Check overstayed parking (Parkdauerüberschreitung prüfen) | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | Bei Aktivierung (1) wird geprüft, ob die Parkdauer zu lang war. |

**Konfigurieren eines Lesers: Zusätzliche Einstellungen**

I-BPR K Options Door control Additional settings Cards

Access sequence check: 0 - Deactivated

Time management:

Double access control

Enable:

Door group ID: ..

Anti-Pass-Back timeout: 5 minutes

Random screening

Random screening:

Screening rate:


Timeout random screening: Minutes

REX button active when IDS armed:

Read permanently:

| Parameter              | Mögliche Werte  | Bemerkung  |
|------------------------|---|--|
| Zutrittsfolgekontrolle | 0 – Deactivated (0 – Ausgeschaltet)<br>1 – Activated; deactivate upon LAC malfunction (1 – Eingeschaltet, bei LAC Störung ausschalten)<br>2 – Activated; leave active upon LAC malfunction (2 – | 0 = Leser nimmt an der Zutrittsfolgekontrolle nicht teil (= Default).<br>Mit aktivierter Folgekontrolle können UNBEKANNTE Personen wie folgt behandelt werden:<br>1 = Das erste Einlesen des Ausweises erfolgt ohne Kontrolle des Standorts. Alle Controller müssen online geschaltet sein.<br>2 = Das erste Einlesen des Ausweises erfolgt ohne Kontrolle des Standorts.<br>3 = Der Standort wird bei jedem Einlesen des Ausweises während der LAC Störung geprüft. |



|  |   |  |
|--|---|--|
|  | Eingeschaltet, bleibt bei LAC Störung aktiv)<br>3 – Activated; use strict sequence checking even when LAC malfunctions (3 – Eingeschaltet, bleibt aktiv, strikte Prüfung erfordert manuelle Korrektur des Aufenthaltsortes) |  |
|  <p>Auf der BIS Plattform gibt es einen MAC-Befehl, um die Zutrittsfolgekontrolle generell zu aktivieren oder zu deaktivieren.</p> <p>Um die Zutrittsfolgekontrolle für einen bestimmten Zeitraum zu deaktivieren, wird ein Wert in Minuten angegeben, der maximal 2880 (= 48 Stunden) betragen darf. Wenn Sie den Wert „0“ festlegen, wird die Zutrittsfolgekontrolle vollständig deaktiviert.</p> <p><b>Hinweis:</b> Mit diesem Befehl können Sie die Zutrittsfolgekontrolle nur für die Leser ändern, bei denen der Parameter <b>Enable access sequence (Zutrittsfolge aktivieren)</b> gesetzt ist. Die Zutrittsfolgekontrolle wird nicht für <i>alle</i> Leser deaktiviert/aktiviert.</p> |   |  |
| Time Management (Zeitwirtschaft)   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert)  | Bei Aktivierung (1) sammelt der ACE Prozess Daten vom Zeitanwesenheitssystem.  |
| <p><b>Double access control (anti-passback control) (Doppelzutrittskontrolle [Zutrittswiederholkontrolle])</b></p>   |   |  |
| Enable (Aktivieren)  | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert)  | 0 = ohne Doppelzutrittskontrolle (= Standard)<br>1 = mit Doppelzutrittskontrolle<br>Innerhalb der Zeitspanne, die mithilfe des Parameters <b>Duration (Dauer)</b> festgelegt wird, können dieser und andere Leser nicht mit demselben Ausweis verwendet werden. Wenn dieser Parameter aktiviert ist, muss eine Türgruppenkennung verwendet werden, selbst wenn nur ein Leser verwendet wird. |
| Door group ID (Türgruppenkennung)  | Buchstaben A – Z und a – z und „-“  | Leser können mit einer Türgruppenkennung gruppiert werden. Wenn ein Ausweis an einem Leser eingelesen wird, werden   |

|  |  |  |
|--|--|--|
|  | 2 Zeichen  | nachfolgende Registrierungen an allen Lesern in der Türgruppe (Standard = --) gesperrt, bis das Zeitlimit verstrichen ist.   |
| Anti-passback time out (Zeitlimit für Zutrittswiederholspere)                  | 1 - 120  | Der Leser kann mit demselben Ausweis erneut verwendet werden, wenn diese Zeitspanne abgelaufen ist. Sobald der Ausweis an einem Leser außerhalb der Gruppe verwendet wird, wird die Sperre sofort aufgehoben.<br>Werte in Minuten. Standard = 5.   |
| Random screening (Mitarbeiterauslösung)  | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | 0 = keine Mitarbeiterauslösung<br>1 = Faktorabhängige Mitarbeiterauslösung erhält erst Zutritt, wenn Entsperrung durch den Dialog <b>Blocking</b> (Sperrung) erfolgt.  |
| Screening rate (Auslösungsfaktor)  | 1 - 100  | Prozentsatz der Mitarbeiterauslösung zur erweiterten Kontrolle. Verfügbar, wenn „random screening“ (Mitarbeiterauslösung) aktiviert ist.   |
| Timeout random screening (Timeout-Mitarbeiterauslösung)                        | 1 - 120  | Innerhalb der Zeitspanne wird die Mitarbeiterauslösung auf den Benutzer angewendet. Werte in Minuten.<br>Standard = 5.   |
| REX button active when IDS armed (REX-Taste aktiv bei Scharfschaltung der EMA) | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Nur bei <b>TM10</b> und <b>TM14</b> : Türtaster sind standardmäßig deaktiviert, wenn die EMA scharfgeschaltet ist. Hierdurch wäre es nicht möglich, den überwachten Bereich zu verlassen. Mit dem neuen Leserparameter wird der Türtaster aktiviert, selbst wenn die EMA scharfgeschaltet ist.<br>Dieser Parameter muss auch gesetzt werden, wenn ein Leser statt eines Türtasters verwendet wird. |
| Read permanently (Permanent lesen)   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Der Leser liest permanent, wenn er mit der entsprechenden Firmware des Herstellers ausgestattet ist.   |

### Konfigurieren eines Lesers: Ausweise

WIE1K Reader | Options | Door control | Additional settings | Offline locking system | Biometrics | Key cabinet | Cards

---

Card validation

Motorized card reader:

Withdraw card:

Triggering criteria:

Blocked card

Visitor card

Card is blacklisted

Invalid time model

Invalid area/time model

No authorization

Always collect

Collect visitor cards on collecting date

Collect visitor cards on last day of validity

Collect other cards (no visitor cards) on collecting date

Collect other cards (no visitor cards) on last day of validity

Time model defined and invalid, independent of access and reader parameters

Area/Time model defined and invalid, independent of access and reader parameters

| Parameter                                    | Mögliche Werte   | Bemerkung  |
|--|--|--|
| Motorized card reader (Motorisierter Einzug) | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Aktivieren Sie dieses Kontrollkästchen, wenn ein motorisierter Ausweisleser verwendet wird.  |
| Withdraw card (Ausweis entziehen)            | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Im Fall eines motorisierten Ausweislesers bedeutet „Entziehen“, dass der Ausweis physisch entzogen wird.<br>Im Fall von anderen Ausweislesern bedeutet „Entziehen“, dass der Ausweis vom System ungültig gemacht wird. |
| Triggering criteria (Auslösende Kriterien)   | 0 = Deaktiviert (Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert (Kontrollkästchen ist aktiviert) | Wählen Sie aus dieser Liste alle Kriterien, die die Aktion <b>Withdraw card</b> (Ausweis entziehen) auslösen sollen.   |



**Hinweis!**

Motorisierte Ausweisleser können nur mit IBPR-Lesern verwendet werden.

## 13.8.1 Konfigurieren der Mitarbeiterauslosung

Mitarbeiterauslosung ist eine gängige Methode zur Verbesserung der Sicherheit von Websites durch zufällige Auswahl von Mitarbeitern für zusätzliche Sicherheitsprüfungen.

### Voraussetzungen:

- Der Durchtritt sollte als Schleuse oder Drehkreuz eingerichtet werden, um zu verhindern, dass eine Person zusammen mit einer anderen Person "durchschlüpft", ohne den eigenen Ausweis einzulesen.
- Ein Ausweisleser muss für mindestens eine der Durchgangsrichtungen vorhanden sein.
- Die Leser müssen für die normale Zutrittskontrolle konfiguriert sein.
- Der Zufallsgenerator kann für jeden Leser separat konfiguriert werden.
- Eine Dialogstation sollte sich in unmittelbarer Nähe befinden, um Sperren freizugeben, die vom System festgelegt wurden.

### Vorgehensweise

1. Suchen Sie den gewünschten Leser im Geräteeditor DevEdit
2. Aktivieren Sie auf der Registerkarte **Settings** das Kontrollkästchen **Random screening** (Mitarbeiterauslosung).
3. Geben Sie den Prozentsatz der auszulosenden Personen in das Feld **Screening percentage** (Auslosungsfaktor) ein.
4. Speichern Sie Ihre Einstellungen.

## 13.9 Zutritt nur durch PIN-Code

### Hintergrund

Leser mit Tastenfeld können so konfiguriert werden, dass der Zutritt mit dem PIN-Code allein möglich ist.

Wenn Leser so konfiguriert sind, kann der BIS-Bediener ausgewählten Personen individuelle PIN-Codes zuweisen. Tatsächlich erhalten diese Personen einen „virtueller Ausweis“, der nur aus einer PIN besteht. Dies wird als Identifikations-PIN bezeichnet. Demgegenüber ist eine Verifikations-PIN eine PIN, die in Kombination mit einem Ausweis verwendet wird, um die Sicherheit zu erhöhen.


Der Bediener kann PINs für Personen manuell eingeben oder ihnen die vom System generierten PINs zuweisen.

Beachten Sie, dass diese Personen weiterhin auch mit den ihnen zugewiesenen physischen Ausweisen Zutritt haben.

### Erforderliche Berechtigung für Bediener

Die Berechtigung für einen Ausweisinhaber zum Zutritt nur mit der PIN kann nur von Bedienern gewährt werden, die über die besondere Berechtigung zur Zuweisung virtueller Ausweise verfügen. Gehen Sie wie folgt vor, um einem Bediener diese Berechtigung zu erteilen:

1. Navigieren Sie zu Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen) > **User profiles** (Benutzerprofile)
2. Wählen Sie das Benutzerprofil, das die Berechtigung erhalten soll:  
Geben Sie es entweder in das Textfeld **Profile name** (Profilname) ein, oder verwenden Sie die Suchfunktion, um das gewünschte Profil zu finden.





3. Klicken Sie in der Dialogliste auf die Zelle, die **Cards (Ausweise) enthält**. Ein Popup-Fenster mit der Bezeichnung **Special functions** (Besondere Funktionen) erscheint im unteren Bereich des Hauptfensters.
4. Aktivieren Sie im Bereich "Special functions" (Besondere Funktionen) das Kontrollkästchen **Assign virtual cards (PIN)** (Virtuelle Ausweise zuweisen (PIN)).
5. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

### Einstellen der Länge der Identifikations-PIN für unterstützte Lesertypen

Die Länge der manuell eingegebenen oder systemgenerierten PINs richtet sich nach dem in der Systemkonfiguration eingestellten Parameter.

- Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Options** (Optionen) > **PIN codes** (PIN-Codes) > **PIN code length** (PIN-Code-Länge)

### Konfigurieren eines Lesers zum Zutritt nur per PIN

1. Navigieren Sie zum Baum Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten) > **Workstations** (Dialogstationen) 
2. Wählen Sie im Fenster **Workstation** (Dialogstation) die Dialogstation aus, mit dem der Leser physisch verbunden ist.
3. Klicken Sie mit der rechten Maustaste auf den Bedienplatz und fügen Sie einen Leser des Typs **Dialog PIN-Eingabe** oder **Dialog PIN-Erstellung** hinzu.
4. Wählen Sie den Leser im Fenster **Bedienplätze** aus.  
Rechts vom Fenster **Bedienplätze** wird ein Fenster für die individuelle Leserkonfiguration angezeigt.
5. Prüfen Sie, ob die Dropdown-Liste **Card usage default** (Standard-Ausweisverwendung) den Standardwert **Virtual card. Use PIN as card** (Virtueller Ausweis. PIN als Ausweis verwenden) enthält.
6. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern
7. Navigieren Sie im Geräteeditor DevEdit zum Baum **Device configuration** (Gerätekonfiguration) 
8. Wählen Sie den Leser an dem Eingang, an dem Sie den Zutritt nur per PIN konfigurieren möchten.
9. Aktivieren Sie auf der Registerkarte **Options** (Optionen) das Kontrollkästchen **Access also by PIN code alone** (Zutritt auch nur durch PIN-Code).
10. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

## 13.10 AMC-Erweiterungen


### Erstellen einer AMC-E/A-EXT (E/A-AMC Erweiterung)

AMC Erweiterungen bieten zusätzliche Eingangs- und Ausgangssignale, wenn die acht Kontakte des AMC für den Anschluss der erforderlichen Kontakte (beispielsweise bei Aufzügen) nicht ausreichen.

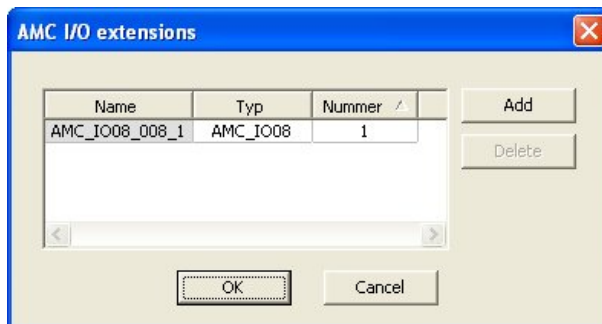
Diese Erweiterungen werden physisch an den zugeordneten AMC angeschlossen und können im Geräteeditor nur unterhalb der jeweiligen AMCs installiert werden. Der entsprechende AMC Eintrag zum Erstellen einer AMC-EXT wird im Explorer und der Eintrag **New Extension Board (Neues Erweiterungsboard)** im Kontextmenü **New Object (Neues Objekt)** gewählt.



### Hinweis!

Wenn Sie in der Symbolleiste des Geräteeditors auf die Schaltfläche  klicken, werden nur neue Durchritte erstellt. Erweiterungen können im Kontextmenü gewählt werden.

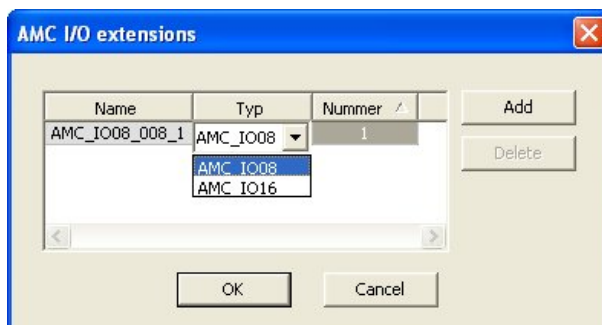
Ein Auswahldialog zum Erstellen der Erweiterungen wird angezeigt.



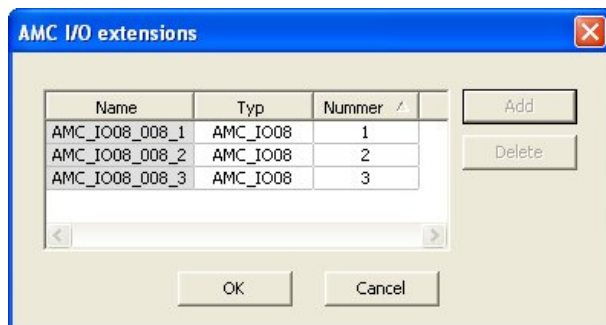
AMC-EXT ist in zwei Varianten verfügbar:

- AMC\_IO08: mit 8 Eingängen und 8 Ausgängen
- AMC\_IO16: mit 16 Eingängen und 16 Ausgängen
- AMC\_4W Erweiterung: mit 8 Eingängen und 8 Ausgängen

Der Auswahldialog enthält einen Eintrag mit einer AMC\_IO08. Wenn Sie im Listenfeld auf die Spalte **Type (Typ)** doppelklicken, können Sie auch eine AMC\_IO16 einfügen.



Sie können bis zu drei Erweiterungen an einen AMC anschließen. Beide Varianten können auch gemischt werden. Klicken Sie auf **Add (Hinzufügen)**, um weitere Listeneinträge zu erstellen. Sie können alle Spalteneinträge anpassen.



Die AMC Erweiterungen werden je nach Erstellung mit 1, 2 oder 3 nummeriert. Die Nummerierung der Signale beginnt bei jeder Erweiterung mit 01. Die Signalnummer und die Erweiterungsnummer bilden zusammen eine eindeutige ID. Die Signale der AMC Erweiterungen werden auf der Registerkarte des AMC angezeigt, zu dem sie gehören. Zusammen mit den Eingangs- und Ausgangssignalen des AMC können auf diese Weise maximal 56 Signalpaare bereitgestellt werden.

AMC Erweiterungen können nach Bedarf einzeln oder zu einem späteren Zeitpunkt bis zur maximalen Anzahl (3 pro AMC) hinzugefügt werden.

#### Erstellen einer AMC2 4W-EXT

Es ist möglich, spezielle AMC Erweiterungen (AMC2 4W-EXT) für Controller mit Wiegand-Leserschnittstellen (AMC2 4W) zu konfigurieren. Diese Module bieten 4 zusätzliche Wiegand-Leseranschlüsse sowie jeweils 8 Eingangs- und 8 Ausgangskontakte. Somit kann die maximale Anzahl der Leser und Türen, die pro AMC2 4W anschließbar sind, auf 8 verdoppelt werden.



#### Hinweis!

Die AMC2 4W-EXT kann nicht als eigenständiger Controller, sondern lediglich als Erweiterung eines AMC2 4W verwendet werden. Der AMC2 4W steuert die Türen und trifft die Zutrittskontrollentscheidungen.

Die AMC2 4W-EXT kann nur zusammen mit einem AMC2 4W verwendet werden. Da sie lediglich mit Wiegand-Leserschnittstellen ausgestattet ist, kann sie nicht zusammen mit der AMC Variante AMC2 4R4 eingesetzt werden.

Wie die E/A-Erweiterungen (AMC2 8I-8O-EXT und AMC2 16I-16O-EXT) wird die AMC2 4W-EXT über die Erweiterungsschnittstelle des AMC2 4W angeschlossen. Die AMC Erweiterung verfügt weder über einen eigenen Speicher noch ein eigenes Display, sondern wird vollständig durch den AMC2 4W gesteuert.

Eine AMC2 4W-EXT und maximal drei E/A-Erweiterungen können an jeden AMC2-4W angeschlossen werden.

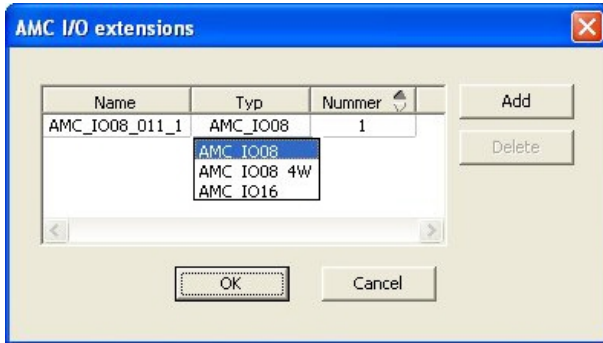
Um im System eine AMC2 4W-EXT zu erstellen, klicken Sie im Explorer mit der rechten Maustaste auf den gewünschten übergeordneten AMC2 4W, und klicken Sie im Kontextmenü auf **New object (Neues Objekt) > New extension board (Neues Erweiterungsboard)**.



#### Hinweis!

Die Schaltfläche **+** auf der Symbolleiste des Geräteeditors kann nur verwendet werden, um Durchritte hinzuzufügen. AMC Erweiterungen können nur über das Kontextmenü hinzugefügt werden.

Es wird derselbe Auswahldialog wie beim Erstellen von E/A-Erweiterungen angezeigt. Der einzige Unterschied besteht darin, dass die Liste für einen AMC2 4W das zusätzliche Element AMC\_IO08\_4W enthält.



Der Listeneintrag „AMC2 4W“ kann nur einmal hinzugefügt werden. Hingegen können maximal drei E/A-Erweiterungen hinzugefügt werden.

Mit der Schaltfläche **Add (Hinzufügen)** fügen Sie neue Listeneinträge hinzu. Bei einem AMC2 4W beträgt die maximale Anzahl 4, wobei der vierte Eintrag als AMC2 4W-EXT erstellt wird. AMC Erweiterungen werden nach der Reihenfolge ihrer Erstellung mit 1, 2 oder 3 nummeriert. Die AMC2 4W-EXT erhält die Nummer 0 (Null). Die Nummerierung der Signale für die AMC2 4W-EXT wird von der Nummerierung des Controllers, also 09 bis 16 fortgesetzt, während die Nummerierung für jede E/A-Erweiterung mit 01 beginnt. Die Signale für alle AMC Erweiterungen werden auch auf der Registerkarte für den relevanten AMC2 4W angezeigt. Zusammen mit den Eingangs- und Ausgangssignalen des AMC2 4W können bis zu 64 Signalpaare bereitgestellt werden.

**Ändern und Löschen von AMC Erweiterungen**

Die erste Registerkarte enthält die folgenden Steuerelemente zum Konfigurieren von AMC Erweiterungen.

| Parameter                           | Mögliche Werte   | Beschreibung  |
|-------------------------------------|--|---|
| Board name<br>(Erweiterungsname)    | Alphanumerisch mit Einschränkungen:<br>1 – 16 Zeichen  | Mit der Default-ID wird ein eindeutiger Name sichergestellt, der jedoch manuell überschrieben werden kann. Achten Sie unbedingt darauf, dass die ID eindeutig ist. Bei Netzwerkanschlüssen mit DHCP-Servern sollte der Netzwerkname verwendet werden. |
| Board description<br>(Beschreibung) | Alphanumerisch:<br>0 – 255 Zeichen   | Dieser Text wird im OPC-Zweig angezeigt.  |
| Board number<br>(Platinennummer)    | 1 - 3  | Nummer der an den AMC angeschlossenen Erweiterung.<br>Schreibgeschütztes Feld.  |
| Power supply<br>(Stromversorgung)   | 0 = Deaktiviert<br>(Kontrollkästchen ist deaktiviert)<br>1 = Aktiviert<br>(Kontrollkästchen ist aktiviert) | Überwachung der Stromversorgung.<br>Bei Spannungsausfällen wird eine Meldung nach Ablauf einer Verzögerung generiert.<br>Bei der Überwachungsfunktion wird die Verwendung einer USV vorausgesetzt, sodass eine Meldung generiert werden kann.         |




|         |  |   |
|---------|--|---|
|         |  | 0 = keine Überwachung<br>1 = Überwachung aktiviert  |
| Mandant | Standardwert<br>"Common" (Allgemein<br>) | Dieses schreibgeschützte Feld ist nur anwendbar, wenn die Funktion "Divisions" (Mandanten) lizenziert und verwendet wird. |

Die Registerkarten "Inputs" (Eingänge), "Outputs" (Ausgänge) und "Signal Settings" (Signaleinstellungen) haben dasselbe Layout und dieselbe Funktion wie die entsprechenden Registerkarten für die Controller.

### Löschen von AMC Erweiterungen

Eine AMC Erweiterung kann nur gelöscht werden, wenn keine ihrer Schnittstellen belegt ist. Die zugehörigen Signale müssen zuerst für eine andere Erweiterung konfiguriert werden, bevor

die Schaltfläche „Löschen“  und die Option **Delete object (Objekt löschen)** des Kontextmenüs verfügbar sind.

### AMC2 4W-EXT

Da Leser, die Erweiterungen belegen, nicht einzeln entfernt oder neu konfiguriert werden können, müssen sie zusammen mit den zugehörigen Durchritten gelöscht werden. Erst dann kann die AMC2 4W-EXT ebenfalls entfernt werden.

## 14 Benutzerdefinierte Felder für Personaldaten

### Einführung

Datenfelder für Personal sind auf verschiedene Arten anpassbar:

- ob sie **sichtbar** sind, d. h. ob sie im ACE-Client überhaupt angezeigt werden
- ob sie **erforderlich** sind, d. h. ob ein Datensatz ohne gültige Daten in diesem Feld gespeichert werden kann
- ob die enthaltenen Werte im System **eindeutig** bleiben müssen
- welchen Datentyp sie enthalten (Text, Datum und Uhrzeit, Ganzzahl etc.)
- wo (in welcher Registerkarte, Spalte und Zeile) sie im ACE-Client angezeigt werden
- wie groß sie erscheinen
- ob und wo die Daten in Standardberichten verwendet werden

Es ist natürlich nach wie vor möglich, komplett neue Datenfelder mit allen hier aufgelisteten Attributen zu definieren.

### 14.1 Vorschauanzeige und Bearbeiten von benutzerdefinierten Feldern

#### Dialogpfad

- Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Options** (Optionen) > **Custom fields** (Benutzerdefinierte Felder)

Das Hauptfenster ist in zwei Registerkarten unterteilt:

**Overview** (Übersicht) Diese Registerkarte und ihre Unterregisterkarten **Address, Contact, Additional person data, Additional Company data, Remarks, Card Control** und **Extra Info** (Adresse, Kontaktinformationen, Zusätzliche Personendaten, Zusätzliche Firmendaten, Anmerkungen, Ausweiskontrolle und Reserve) sind schreibgeschützt und enthalten eine ungefähre WYSIWYG-Übersicht dazu, welche Daten auf welchen Registerkarten im ACE-Client erscheinen werden.


**Details** Diese Registerkarte enthält eine Liste der Editoren; einer für jedes vordefinierte oder benutzerdefinierte Datenfeld.

#### Bearbeiten von vorhandenen Datenfeldern

Unter **Custom fields** (Benutzerdefinierte Felder) > **Details** verfügt jedes Datenfeld, sowohl vordefiniert als auch benutzerdefiniert, über ein eigenes Editorfenster, in dem die entsprechenden Attribute bearbeitet werden können.

Klicken Sie im Editor auf das Feld, das Sie bearbeiten möchten. Der aktive Editor wird hervorgehoben.

Die editierbaren Attribute von benutzerdefinierten Feldern werden in der folgenden Tabelle erklärt.

| <b>Beschriftungst ext</b>   | <b>Beschreibung</b>  |
|---|--|
| <p><b>Label</b><br/>(Beschriftung)</p>  | <p><b>Label</b> (Beschriftung) ist die Beschriftung des Datenfelds, wie es im Client erscheint. Es kann nach Belieben verändert werden, um der Terminologie Ihres Standorts zu entsprechen.</p>  |
| <p><b>Field type</b><br/>(Feldtyp)</p>  | <p><b>Field type</b> (Feldtyp) beschreibt den Datentyp und bestimmt, wie der Bediener bei diesem Dialog vorgehen muss, um Eingaben im Client zu tätigen. Jeder Feldtyp bietet Konsistenzprüfungen für seine speziellen Eingabewerte, um gültige Daten, Zeiten, Textlängen und numerische Grenzen sicherzustellen.</p> <ul style="list-style-type: none"> <li>- <b>Text field</b> (Textfeld) <ul style="list-style-type: none"> <li>- Klicken Sie auf die daneben liegende Schaltfläche mit den Auslassungspunkten, um die Anzahl der zulässigen Zeichen festzulegen.</li> </ul> </li> <li>- <b>Check box</b> (Kontrollkästchen)</li> <li>- <b>Date field</b> (Datumsfeld)</li> <li>- <b>Time</b> (Uhrzeit)</li> <li>- <b>Date-time field</b> (Datum-Zeit-Feld)</li> <li>- <b>Combo box</b> (Auswahllistenfeld) <ul style="list-style-type: none"> <li>- Geben Sie die gültigen Werte für das Auswahllistenfeld in das entsprechende Textfeld ein. Trennen Sie sie durch Kommas oder Zeilenumbrüche.</li> </ul> </li> <li>- <b>Numerical input</b> (Numerische Eingabe) <ul style="list-style-type: none"> <li>- Geben Sie in den dafür vorgesehenen Drehfeldern Ihren minimalen und maximalen Wert für die numerische Eingabe ein.</li> </ul> </li> <li>- <b>Building control 1</b> und <b>Building control 2</b> (Gebäudesteuerung) <ul style="list-style-type: none"> <li>- Dies sind spezielle Steuerelemente, die hier umbenannt werden können (im Feld <b>Label</b>; Beschriftung) und mit Befehlen in der Client-Bedienoberfläche verknüpft sind. So können Sie bestimmten Benutzern die Erlaubnis geben, mit ihren Ausweisen bestimmte Bedienvorgänge innerhalb der Seite auszuführen. Beispiele für solche Bedienvorgänge sind das Einschalten von Scheinwerfern oder die Steuerung von Spezialgeräten.</li> </ul> </li> </ul> |
| <p><b>Visible</b><br/>(Sichtbar)</p>  | <p>Deaktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass das Datenfeld im Client angezeigt wird.</p>  |
| <p><b>Unique</b><br/>(Eindeutig)</p>  | <p>Aktivieren Sie dieses Kontrollkästchen, damit Datenfeldinhalte zurückgewiesen werden, die nicht eindeutig sind. Beispiel: Jeder Angestellte sollte eine eindeutige Personalnummer haben.</p>  |
|  | <p>Das grüne Licht bedeutet, dass dieses Datenfeld in der Datenbank derzeit <b>nicht</b> verwendet wird.<br/>Das rote Licht bedeutet, dass dieses Datenfeld momentan in der Datenbank verwendet wird.</p>  |
| <p><b>Display in</b><br/>(Angezeigt in)</p>   | <p>Verwenden Sie diese Dropdown-Liste, um die Registerkarte im Client auszuwählen, in der das Datenfeld angezeigt werden soll.</p>   |

| <b>Beschriftungstext</b>                 | <b>Beschreibung</b>   |
|--|---|
| <p><b>Required</b><br/>(Pflichtfeld)</p> | <p>Aktivieren Sie dieses Kontrollkästchen, um das Ausfüllen des Datenfelds obligatorisch zu machen. Beispiel: Bei jedem Personendatensatz ist ein Nachname erforderlich. Ohne einen Nachnamen kann der Datensatz nicht gespeichert werden.</p> <p>Beachten Sie, dass erforderliche Datenfelder nicht mit dem Kontrollkästchen <b>Visible</b> (Sichtbar) unsichtbar gemacht werden können. Für mehr Benutzerfreundlichkeit im Client wird empfohlen, alle erforderlichen Felder auf der ersten Registerkarte zu platzieren.</p>  |
| <p><b>Position</b></p>                   | <p>Verwenden Sie die Drehfelder <b>Column</b> (Spalte) und <b>Row</b> (Zeile), um die Datenfelder auf der in der Dropdown-Liste <b>Display in</b> (Angezeigt in) festgelegten Registerkarte zu positionieren.</p> <p>Beachten Sie, dass der Editor Ihnen nicht erlaubt, eine bereits verwendete Position auszuwählen oder vorhandene Datenfelder zu überlagern. Verwenden Sie das Drehfeld <b>Width (percent)</b> (Breite [Prozent]), um die Größe bestimmter anpassbarer Steuerungen festzulegen, z. B. von Textfeldern. 100 % bedeutet, dass die Steuerung den gesamten Platz einnehmen wird, der nicht bereits von der Datenfeldbeschriftung eingenommen wird.</p> |
| <p><b>Dimension</b><br/>(Abmessung)</p>  | <p>Verwenden Sie die Drehfelder für <b>Column</b> (Spalte) und <b>Row</b> (Zeile), um die Anzahl der Spalten und Zeilen anzugeben, die auf der in der Dropdown-Liste angegebenen Registerkarte <b>Display in</b> (Angezeigt in) belegt werden sollen. Beachten Sie, dass Sie mit dem Editor keine vorhandenen Datenfelder überlagern können.</p>  |

**Erstellen und Bearbeiten von neuen Datenfeldern**

Unter **Custom fields** (Benutzerdefinierte Felder) > **Details** verfügt jedes Datenfeld, sowohl vordefiniert als auch benutzerdefiniert, über ein eigenes Editorfenster, in dem die entsprechenden Attribute bearbeitet werden können.

Klicken Sie auf die Schaltfläche **New field** (Neues Feld), um ein neues benutzerdefiniertes Feld mit seinem eigenen Editor zu erstellen. Das aktive Editorfenster wird hervorgehoben. Der Editor verfügt über dieselben Dialogsteuerungen zum Bearbeiten vorhandener Datenfelder (siehe Tabelle oben) und zwei zusätzliche Steuerungen:

|   |   |
|---|---|
| <p><b>Use in reports</b> (In Berichten nutzen)<br/>(Kontrollkästchen)</p> | <p>Aktivieren Sie dieses Kontrollkästchen, damit das neue Datenfeld in den Standardberichten erscheint.</p> |
| <p><b>Sequence number</b><br/>(Sequenznummer)<br/>(Drehfeld)</p>          | <p>Die Sequenznummer bestimmt die Spalte, die das Datenfeld in den Standardberichten belegen wird.</p>      |



**Hinweis!**

Aktuell können nur die Sequenznummern 1 bis 10 von **Badge Designer** (Ausweisdesigner) und **Reports** (Berichten) adressiert werden.

## 14.2 Regeln für Datenfelder

- Position von Datenfeldern
  - Jedes Feld kann nur auf einer Registerkarte angezeigt werden.
  - Jedes benutzerdefinierte Feld kann auf jeder beliebigen wählbaren Registerkarte angezeigt werden.
  - Felder können auf andere Registerkarten verschoben werden. Hierzu muss der Eintrag in der Pulldown-Liste **Display in** (Angezeigt in) geändert werden.
- Die Beschriftung kann einen beliebigen Text enthalten: max. 20 Zeichen.
- Die benutzerdefinierten Textfelder können einen beliebigen Text enthalten: max. 2000 Zeichen.
- Jedes Feld kann als erforderlich markiert werden, aber dafür muss das Kontrollkästchen **Visible** (Sichtbar) aktiviert werden.



### Hinweis!

Dringende Empfehlungen vor dem produktiven Einsatz

Bestimmen und finalisieren Sie die Feldtypen und ihre Verwendung, bevor Sie diese zum Speichern von Personendatensätzen nutzen:

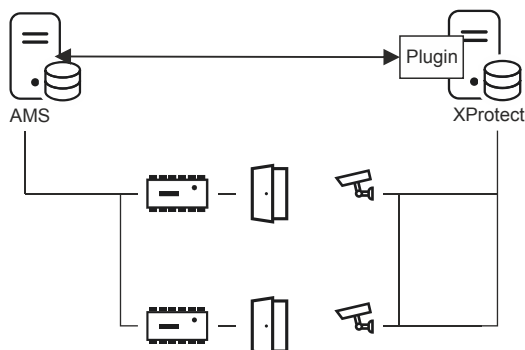
Jedes Dateneingabefeld ist einem bestimmten Datenbankfeld zugewiesen, damit die Daten sowohl manuell als auch durch Berichtsfunktionen gefunden werden können. Sobald Datensätze für benutzerdefinierte Felder in der Datenbank gespeichert worden sind, können diese Felder nicht mehr verschoben oder geändert werden, ohne Datenverluste zu riskieren.

## 15 Konfigurieren von Milestone XProtect für die Verwendung von AMS

### Einführung

In diesem Kapitel wird beschrieben, wie Milestone XProtect so konfiguriert wird, dass die Zutrittskontrollfunktionen von AMS verwendet werden.

Ein Plug, das von AMS bereitgestellt, aber auf dem XProtect-Server installiert ist, überträgt Ereignisse und Befehle an AMS und sendet die Ergebnisse an XProtect zurück.



Die Konfiguration besteht aus drei Stufen, die in den folgenden Abschnitten beschrieben werden:

- Installieren des öffentlichen AMS-Zertifikats auf dem XProtect-Server
- Installieren des AMS-Plugins auf dem XProtect-Server
- Konfigurieren von AMS in der XProtect-Anwendung

### Voraussetzungen

- AMS ist installiert und lizenziert.
- XProtect ist auf demselben Computer oder auf seinem eigenen Computer installiert und lizenziert.
- Zwischen beiden Systemen besteht eine Netzwerkverbindung.

### Installieren des öffentlichen AMS-Zertifikats auf dem XProtect-Server

Beachten Sie, dass dieses Verfahren nur erforderlich ist, wenn AMS auf einem anderen Computer ausgeführt wird.

1. Kopieren Sie die Zertifikatsdatei vom AMS-Server  
`C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`  
 auf den XProtect-Server.
2. Doppelklicken Sie auf dem XProtect-Server auf die Zertifikatsdatei.  
 Der Zertifikats-Assistent wird angezeigt.
3. Klicken Sie auf **Install Certificate...** (Zertifikat installieren)  
 Der Zertifikats-Importassistent wird angezeigt.
4. Wählen Sie **Local Machine** (Lokaler Rechner) als den **Speicherort**, und klicken Sie auf **Next** (Weiter).
5. Wählen Sie **Place all certificates...** (Alle Zertifikate platzieren).
6. Klicken Sie auf **Browse...** (Durchsuchen...).
7. Wählen Sie **Trusted Root Certification Authorities** (Vertrauenswürdige Root-Zertifizierungsstellen), und klicken Sie auf **OK**.

8. Klicken Sie auf **Next** (Weiter).
9. Überprüfen Sie die Zusammenfassung der Einstellungen, und klicken Sie auf **Finish** (Fertigstellen).

### Installieren des AMS-Plugins auf dem XProtect-Server

1. Kopieren Sie die Setup-Datei  
`AMS XProtect Plugin Setup.exe`  
vom AMS-Installationsmedium auf den XProtect-Server.
2. Führen Sie die Datei auf dem XProtect-Server aus.  
Der Setup-Assistent wird angezeigt.
3. Stellen Sie im Setup-Assistenten sicher, dass das AMS XProtect-Plugin für die Installation markiert ist, und klicken Sie auf **Next** (Weiter).  
Der Endbenutzer-Lizenzvertrag wird angezeigt. Klicken Sie auf **Accept** (Akzeptieren), um die Vereinbarung zu akzeptieren, wenn Sie fortfahren möchten.
4. Der Assistent zeigt den Standardinstallationspfad für das Plugin an. Klicken Sie auf **Next** (Weiter), um den Standardpfad zu akzeptieren, oder **Browsen** Sie, um ihn zu ändern, bevor Sie auf **Next** (Weiter) klicken.  
Der Assistent bestätigt, dass er im Begriff ist, das AMS XProtect-Plugin zu installieren.
5. Klicken Sie auf **Install** (Installieren).
6. Warten Sie auf die Bestätigung, dass die Installation abgeschlossen ist, und klicken Sie auf **Finish** (Fertigstellen).
7. Starten Sie den Windows-Dienst mit dem Namen **Milestone XProtect Event Server** neu.

### Konfigurieren von AMS in der XProtect-Anwendung

1. Navigieren Sie in der XProtect-Management-Anwendung zu **Advanced Configuration** (Erweiterte Konfiguration) > **Access Control** (Zutrittskontrolle).
2. Klicken Sie mit der rechten Maustaste auf **Access Control** (Zutrittskontrolle), und wählen Sie **Create new... (Neu erstellen...)**. Der Plugin-Assistent wird angezeigt.
3. Geben Sie die folgenden Informationen in den Plugin-Assistenten ein:
  - **Name:** Eine Beschreibung dieser AMS-XProtect-Integration, um sie von anderen Integrationen auf demselben XProtect-System zu unterscheiden
  - **Integrations-Plug-in:** `AMS - XProtect Plugin` (Dieser Name ist in der Dropdown-Liste nach erfolgreicher Installation des Plugins verfügbar)
  - **AMS-API-Erkennungsendpunkt:** `https://<hostname of the AMS system>:44347/`  
, wobei 44347 der Standardport bei der Installation der AMS-API ist.
  - **Bedienername:** Der Benutzername eines AMS-Bedieners mit mindestens Berechtigungen zur Bedienung der Türen, denen XProtect-Kameras zugeordnet werden.
  - **Bedienerpasswort:** das AMS-Passwort dieses Bedieners.
4. Klicken Sie auf **Next** (Weiter).  
Das AMS-Plugin stellt eine Verbindung mit dem von Ihnen angegebenen AMS-Server her und listet die gefundenen Zutrittskontrollelemente auf (Türen, Einheiten, Server, Ereignisbefehle und Zustände).
5. Wenn der Fortschrittsbalken vollständig durchgelaufen ist, klicken Sie auf **Next (Weiter)**. Die Assistentenseite **Associate cameras** (Kameras verknüpfen) wird angezeigt.

6. Um Kameras mit Türen zu verknüpfen, ziehen Sie Kameras aus der Liste **Cameras** (Kameras) auf die Zutrittspunkte in der Liste **Doors** (Türen).
7. Wenn Sie fertig sind, klicken Sie auf **Next** (Weiter).  
XProtect speichert die Konfiguration und bestätigt, wenn sie erfolgreich gespeichert wurde.



## 16 Konfigurieren der Bedrohungsstufenverwaltung

### Einführung

Das Ziel der Bedrohungsstufenverwaltung besteht darin, effektiv auf Notfallsituationen zu reagieren, indem das Verhalten von Eingängen im gesamten betroffenen Bereich sofort geändert wird.

### 16.1 Konzepte der Bedrohungsstufenverwaltung

- Eine **Bedrohung** ist eine kritische Situation, die eine sofortige und gleichzeitige Reaktion von einigen oder allen Durchtritten in einem Zutrittskontrollsystem erfordert.
- Eine **Bedrohungsstufe** ist die Reaktion des Systems auf eine vorhergesehene Situation. Jede Bedrohungsstufe muss sorgfältig konfiguriert werden, damit jeder der MAC-Eingänge weiß, wie er reagieren muss.  
Bedrohungsstufen sind vollständig anpassbar, z. B. können typische hohe Bedrohungsstufen wie folgt konfiguriert werden:
  - **Lockout** (Sperrung): Nur Ersthelfer mit hohen Sicherheitsstufen können eintreten.
  - **Lockdown** (Vollständige Sperrung): Alle Türen sind verschlossen. Sowohl das Ein- als auch das Austreten wird für alle Ausweisinhaber unterhalb einer konfigurierten Sicherheitsstufe verweigert.
  - **Evacuation** (Evakuierung): Alle Ausgangstüren sind entriegelt.
- Typische niedrige Bedrohungsstufen können wie folgt konfiguriert werden:
  - **Sports event** (Sportveranstaltung): Türen zu Sportbereichen sind entsperrt, alle anderen Bereiche sind gesichert.
  - **Parents' evening** (Elternabend): Nur ausgewählte Klassenzimmer und der Haupteingang sind zugänglich.
- Ein **Bedrohungsalarm** ist ein Alarm, der eine Bedrohungsstufe auslöst. Entsprechend autorisierte Personen können einen Bedrohungsalarm mit einer momentanen Aktion auslösen, z. B. über die Benutzeroberfläche des Bedieners, über ein Hardwaresignal (z. B. Drucktaste) oder durch Vorzeigen eines speziellen Bedrohungsalarmausweises an einem beliebigen Ausweisleser.
- Eine **Sicherheitsstufe** ist ein Attribut der **Sicherheitsprofile** von Ausweisinhabern und Lesern, ausgedrückt als Ganzzahl von 0 bis 100. Jede Bedrohungsstufe setzt die Leser des Main Access Controllers (MAC) auf die eingerichteten Sicherheitsstufen. Dann gewähren diese Leser nur Personen mit einer gleichen oder höheren Sicherheitsstufe in ihren Sicherheitsprofilen Zutritt.
- Ein **Sicherheitsprofil** ist eine Sammlung von Attributen, die mit einem **Personentyp** (**Personensicherheitsprofil**), einer Tür (**Türsicherheitsprofil**) oder einem Leser (**Lesersicherheitsprofil**) verknüpft werden können. Sicherheitsprofile regeln das folgende Zutrittskontrollverhalten:
  - **Sicherheitsstufe**, wie oben definiert, für Personentyp, Tür oder Lesegerät
  - **Auslosungsfaktor**. Die prozentuale Wahrscheinlichkeit, dass die Mitarbeiterauslösung von diesem Personentyp oder Lesegerät ausgelöst wird.

### 16.2 Überblick über den Konfigurationsprozess

Die Bedrohungsstufenverwaltung erfordert die folgenden Konfigurationsschritte, die nach dieser Übersicht ausführlich erläutert werden.

1. Im Geräteeditor
  - Definieren von Bedrohungsstufen
  - Definieren von Türsicherheitsprofilen
  - Definieren von Lesersicherheitsprofilen

- Zuweisen von Türsicherheitsprofilen zu Eingängen
- 2. In den Systemdatendialogen
  - Definieren von Personensicherheitsprofilen
  - Zuweisen von Personensicherheitsprofilen zu Personentypen
- 3. In den Systemdatendialogen
  - Zuweisen von Personentypen zu Personen
  - Zuweisen von Personentypen zu Personengruppen

Wenn die Bedrohungsstufenverwaltung erfolgreich konfiguriert wurde, können Alarme und die Gerätezustände des MAC über die Anwendung „Kartenansicht“ überwacht und gesteuert werden. Weitere Informationen finden Sie in der Online-Hilfe zur Kartenansicht.

## 16.3 Konfigurationsschritte im Geräteeditor

In diesem Abschnitt werden die Konfigurationsschritte beschrieben, die im Geräteeditor durchgeführt werden müssen.



### Hinweis!

Gerätedaten können nicht im Geräteeditor geändert werden, wenn eine Bedrohungsstufe in Betrieb ist.

### 16.3.1 Erstellen einer Bedrohungsstufe

In diesem Abschnitt wird beschrieben, wie Bedrohungsstufen für die Verwendung an Ihrem Standort erstellt werden. Es können bis zu 15 erstellt werden.

#### Dialogpfad

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

#### Vorgehensweise

1. Wählen Sie die Unterregisterkarte **Threat levels** (Bedrohungsstufen).
  - Die Tabelle „Bedrohungsstufen“ wird angezeigt. Sie kann bis zu 15 Bedrohungsstufen enthalten, jede mit einem Namen, einer Beschreibung und einem Kontrollkästchen, mit dem die Bedrohungsstufe aktiviert werden kann, nachdem sie konfiguriert wurde.
2. Klicken Sie auf die Zeile **Please enter a name for the threat level** (Bitte geben Sie einen Namen für die Bedrohungsstufe ein).
3. Wählen Sie einen Namen, der für die Systembediener aussagekräftig ist.
4. (optional) Geben Sie in der Spalte **Description** (Beschreibung) eine ausführlichere Beschreibung des Verhaltens der Eingänge ein, wenn diese Bedrohungsstufe in Betrieb ist.
5. Aktivieren Sie zu diesem Zeitpunkt **nicht** das Kontrollkästchen **Active** (Aktiv). Führen Sie zunächst alle anderen Konfigurationsschritte für diese Bedrohungsstufe aus, wie in den folgenden Abschnitten beschrieben.
6. Klicken Sie auf (Speichern), um die neue Bedrohungsstufe zu speichern.

### 16.3.2 Erstellen eines Türsicherheitsprofils

In diesem Abschnitt wird beschrieben, wie Sicherheitsprofile für verschiedene Türtypen erstellt und der Status definiert wird, in den alle Türen dieses Profils wechseln, wenn eine Bedrohungsstufe in Betrieb genommen wird.


#### Dialogpfad

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

#### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.

#### Vorgehensweise

1. Wählen Sie die Unterregisterkarte **Door security profiles** (Türsicherheitsprofile).
  - Das Hauptdialogfenster gliedert sich zwei Bereiche: **Selection** (Auswahl) und **Door security profile** (Türsicherheitsprofil) (Standardname).
2. Klicken Sie auf **New** (Neu).
  - Ein neues Türsicherheitsprofil wird mit einem Standardnamen erstellt.
  - Die Tabelle **Threat level** (Bedrohungsstufe) im Bereich **Door security profile** (Türsicherheitsprofil) wird mit den bereits erstellten Bedrohungsstufen sowie dem Wert **undefined** (undefiniert) für jede in der Spalte **State** (Status) gefüllt.
3. Geben Sie im Bereich **Door security profile** (Türsicherheitsprofil) einen Namen für den Türtyp ein, dem dieses Profil zugewiesen wird.
  - Der neue Profilname wird im **Auswahlbereich** angezeigt. Falls gewünscht, kann es aus der Konfiguration gelöscht werden, indem Sie in diesem Bereich auf **Delete** (Löschen) klicken.
4. (Optional) Geben Sie eine Beschreibung des Profils ein, damit die Bediener das Profil korrekt zuweisen können.
5. Wenn dieses Profil einem Drehkreuz zugewiesen werden soll, aktivieren Sie das Kontrollkästchen **Turnstile** (Drehkreuz).
  - Dies bietet zusätzliche Optionen für den Zielzustand der Tür bei verschiedenen Bedrohungsstufen, z. B. die Möglichkeiten, das Ein- oder Austreten allein oder beides zusammen zuzulassen.
6. Wählen Sie in der Spalte **State** (Status) der Tabelle **Threat level** (Bedrohungsstufe) für jede Bedrohungsstufe einen geeigneten Zielzustand für alle Türen dieses Profils, wenn diese Bedrohungsstufe ausgelöst wird.
7. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

Wiederholen Sie den Vorgang, um so viele Türsicherheitsprofile zu erstellen, wie in Ihrer Konfiguration Türtypen vorhanden sind. Typische Türtypen können Folgende sein:

- Öffentliche Haupttür
- Evakuierungszutritt nach draußen
- Zutritt zu Klassenzimmern
- Öffentlicher Zutritt zur Sportarena

### 16.3.3 Erstellen eines Lesersicherheitsprofils

In diesem Abschnitt wird beschrieben, wie Sicherheitsprofile für verschiedene Lesertypen erstellt werden. Lesersicherheitsprofile definieren die folgenden Leserattribute **für jede Bedrohungsstufe:**

- Die Mindestsicherheitsstufe, die für einen Ausweis erforderlich ist, um Zutritt am Leser zu erhalten.
- Der Auslosungsfaktor, d. h. der Prozentsatz der Ausweisinhaber, die nach dem Zufallsprinzip für zusätzliche Sicherheitsüberprüfungen ausgewählt werden.
  - **Hinweis:** Ein Auslosungsfaktor, der in einem Lesersicherheitsprofil festgelegt ist, setzt einen Auslosungsfaktor außer Kraft, der auf dem Leser selbst festgelegt ist.


#### Dialogpfad

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

#### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.

#### Vorgehensweise

1. Wählen Sie die Unterregisterkarte **Reader security profiles** (Lesersicherheitsprofile).
  - Das Hauptdialogfenster gliedert sich zwei Bereiche: **Selection** (Auswahl) und **Reader security profile** (Lesersicherheitsprofil) (Standardname).
2. Klicken Sie auf **New** (Neu).
  - Ein neues Lesersicherheitsprofil wird mit einem Standardnamen erstellt.
  - Die Tabelle **Threat level** (Bedrohungsstufe) im Bereich **Reader security profile** (Lesersicherheitsprofil) wird mit den bereits erstellten Bedrohungsstufen sowie dem Standardwert **0** für jede in den Spalten **Security level** (Sicherheitsstufe) und **Screening rate** (Auslosungsfaktor) erstellt.
3. Geben Sie im Bereich **Reader security profile** (Lesersicherheitsprofil) einen Namen für den Lesertyp ein, dem dieses Profil zugewiesen wird.
  - Der neue Profilname wird im **Auswahlbereich** angezeigt. Falls gewünscht, kann es aus der Konfiguration gelöscht werden, indem Sie in diesem Bereich auf **Delete** (Löschen) klicken.
4. (Optional) Geben Sie eine Beschreibung des Profils ein, damit die Bediener das Profil korrekt zuweisen können.
5. Wählen in der Spalte **Security level** (Sicherheitsstufe) der Tabelle **Threat level** (Bedrohungsstufe) für jede Bedrohungsstufe eine Mindestsicherheitsstufe (Ganzzahl von 0..100) aus, die ein Bediener haben muss, um einen Leser dieses Profils zu bedienen, wenn diese Bedrohungsstufe ausgelöst wird.
6. Wählen Sie in der Spalte **Screening rate** (Auslosungsfaktor) der Tabelle **Threat level** (Bedrohungsstufe) für jede Bedrohungsstufe den Prozentsatz der Ausweisinhaber aus, die vom Leser nach dem Zufallsprinzip für zusätzliche Sicherheitsüberprüfungen ausgewählt werden, wenn diese Bedrohungsstufe ausgelöst wird.
7. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

## 16.3.4

### Zuweisen von Tür- und Lesersicherheitsprofilen zu Eingängen

In diesem Abschnitt wird beschrieben, wie die Tür- und Lesersicherheitsprofile den Türen und Lesern an bestimmten Eingängen zugewiesen werden.

Im ersten untergeordneten Verfahren wird die Gruppe von Eingängen, die Sie zuweisen möchten, identifiziert und herausgefiltert. Im zweiten untergeordneten Verfahren werden die Zuordnungen vorgenommen.

Darüber hinaus können Sie eine Vorschau der Zustände, Sicherheitsstufen und Auslosungsfaktoren der ausgewählten Eingänge anzeigen. Sie sehen, wie Sie von den verschiedenen von Ihnen definierten Bedrohungsstufen festgelegt würden.

**Dialogpfad**

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

**Voraussetzungen**

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.

**Vorgehensweise**

1. Wählen Sie im Gerätebaum das **DMS** (den Stamm des Gerätebaums).
2. Wählen Sie im Hauptdialogbereich die Registerkarte **Threat level management** (Bedrohungsstufenverwaltung).
  - Der Hauptdialogbereich erhält mehrere Unterregisterkarten.

**Untergeordnetes Verfahren 1: Auswahl von Eingängen für die Zuweisung**

1. Wählen Sie die Unterregisterkarte **Entrances** (Eingänge).
  - Das Hauptdialogfenster gliedert sich zwei Bereiche: **Filter conditions** (Filterbedingungen) und eine Tabelle aller Eingänge, die bisher im System erstellt wurden.
2. (Optional) Geben Sie im Bereich **Filter conditions** (Filterbedingungen) Kriterien ein, um die Gruppe von Eingängen einzuschränken, die in der Tabelle in der unteren Hälfte des Dialogfelds angezeigt werden. Beispiel:
  - Aktivieren oder deaktivieren Sie die Kontrollkästchen, die bestimmen, ob **Leser für eingehenden Verkehr, Leser für ausgehenden Verkehr** und/oder **Türen** in der Tabelle angezeigt werden sollen.
  - Geben Sie Zeichenfolgen ein, die in den Namen der Eingänge, Bereiche, Profilnamen oder Lesernamen aller in der Tabelle aufgeführten Eingänge angezeigt werden müssen.
  - Aktivieren oder deaktivieren Sie das Kontrollkästchen, über das festgelegt wird, ob Türen und Leser, die noch nicht konfiguriert sind, auch in der Tabelle angezeigt werden sollen.
3. Klicken Sie auf **Apply filter** (Filter übernehmen), um die Liste „Eingänge“ zu filtern, oder auf **Reset filter** (Filter zurücksetzen), um die Filtersteuerelemente wieder auf ihre Standardwerte festzulegen.

**Untergeordnetes Verfahren 2: Zuweisen von Sicherheitsprofilen zu den ausgewählten Eingängen**

Voraussetzung: Die zuzuweisenden Eingänge wurden identifiziert und erscheinen in der Tabelle in der unteren Hälfte des Dialogs.

Beachten Sie, dass jeder Eingang in der Regel aus einer Tür oder Barriere plus einem oder mehreren Kartenlesern besteht. Einige spezielle Eingangstypen wie **Sammelplätze** haben dies jedoch möglicherweise nicht.

1. Klicken Sie in der Spalte **Door or reader security profile** (Tür- oder Lesersicherheitsprofil) auf die Zelle, die der Tür oder dem Leser entspricht, die bzw. den Sie zuweisen möchten.
2. Wählen Sie ein Tür- oder Lesersicherheitsprofil aus der Dropdown-Liste der Zelle aus.

**(Optional) Vorschau des Verhaltens von Türen und Lesern bei Bedrohungsstufen**

Die Spalten auf der rechten Seite der Tabelle sind schreibgeschützt. Sie zeigen, was der Sperrstatus (**Modus**), die **Sicherheitsstufe** und **Auslösungsfaktor** der Türen und Leser in der Tabelle wären, wenn die in der Liste **Select threat level for details** (Bedrohungsstufe auswählen, um Details anzuzeigen) ausgewählte Bedrohungsstufe in Betrieb wäre.

Voraussetzung: Die Eingänge, die Sie in der Vorschau anzeigen möchten, wurden identifiziert und werden in der Tabelle in der unteren Hälfte des Dialogs angezeigt.

- ▶ Wählen Sie in der Liste **Select threat level for details** (Bedrohungsstufe auswählen, um Details anzuzeigen) die Bedrohungsstufe aus, die Sie in der Vorschau anzeigen möchten.
- ✓ In der Tabelle werden der Sperrstatus (**Mode**) der Türen und die **Sicherheitsstufe** und der **Auslösungsfaktor** der Leser angezeigt, wie sie wären, wenn die ausgewählte Bedrohungsstufe in Betrieb wäre.

### 16.3.5

#### Zuweisen einer Bedrohungsstufe zu einem Hardware signal

In diesem Abschnitt wird beschrieben, wie Sie ein Hardwareeingangssignal zuweisen, um einen Bedrohungsalarm auszulösen oder abzubrechen.


##### Dialogpfad

- **Main menu** (Hauptmenü) > **Configuration** (Konfiguration) > **Device data** (Gerätedaten)

##### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.

##### Vorgehensweise

1. Wählen Sie im Gerätebaum einen **Eingang** unterhalb des AMC-Controllers aus, dessen Eingangssignale Sie zuweisen möchten.
2. Wählen Sie im Hauptdialogfenster die Registerkarte **Terminals** (Signale) aus.
  - Die Tabelle der Eingänge und Signale wird angezeigt.
3. Klicken Sie in der Zeile des Signals, das Sie zuweisen möchten, auf die Zelle für **Input signal** (Eingangssignal).
  - Die Dropdown-Liste enthält einen Befehl **Threat level: Deactivate** plus eine **Bedrohungsstufe: <name>** für jede Bedrohungsstufe, die Sie zuvor definiert haben.
  - Der Befehl **Threat level: Deactivate** bricht alle Bedrohungsstufen ab, die derzeit in Betrieb sind.
4. Weisen Sie die Befehle den gewünschten Eingangssignalen zu.
5. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.



##### Hinweis!

Beschränkung für DM 15

Türmodell 15 (DIP/DOP) kann derzeit nicht verwendet werden, um eine Bedrohungsstufe auszulösen.

## 16.4

### Konfigurationsschritte in Systemdatendialogen

In diesem Abschnitt wird beschrieben, wie **Personensicherheitsprofile** erstellt und **Personentypen** zugewiesen werden.

## 16.4.1 Erstellen eines Personensicherheitsprofils



### Dialogpfad

- **Main menu** (Hauptmenü) > **System data** (Systemdaten) > **Person security profile** (Personensicherheitsprofil)

### Voraussetzungen

Personensicherheitsprofile erfordern eine sorgfältige Planung und Spezifikation im Voraus, da sie erhebliche Auswirkungen auf das Funktionieren des Systems in kritischen Situationen haben werden.

### Vorgehensweise

1. Wenn das Dialogfeld bereits Daten enthält, klicken Sie auf  (Neu), um sie zu löschen.
2. Geben Sie im Textfeld für den Sicherheitsprofilnamen einen Namen für das neue Profil ein:
3. (Optional) Geben Sie eine Beschreibung des Profils ein, damit die Bediener das Profil korrekt zuweisen können.
4. Geben Sie eine Ganzzahl zwischen 0 und 100 im Feld **Security level** (Sicherheitsstufe) ein.
  - Da der Ausweisinhaber berechtigt ist, einen Eingang zu benutzen, reicht 100 aus, um bei jedem Leser Zutritt zu erhalten, auch wenn seine Sicherheitsstufe derzeit ebenfalls auf 100 festgelegt ist.
  - Andernfalls muss die Sicherheitsstufe im Personensicherheitsprofil eines Ausweisinhabers gleich oder größer als die aktuelle Sicherheitsstufe des Lesers sein.
5. Geben Sie eine Ganzzahl zwischen 0 und 100 in das Feld **Screening rate** (Auslosungsfaktor) ein.
  - **Hinweis:** Der Auslosungsfaktor des Personenprofils ist sekundär zu dem des Leserprofils. Die folgende Tabelle beschreibt das Zusammenspiel der beiden Auslosungsfaktoren des Profils.
6. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

### Zusammenspiel von Auslosungsfaktoren für Personen- und Lesersicherheitsprofile

| Auslosungsfaktor (%) im Lesersicherheitsprofil<br><b>R</b> | Auslosungsfaktor (%) im Personensicherheitsprofil<br><b>P</b> | Person für zusätzliche Sicherheitsüberprüfungen ausgewählt? |
|--|---|---|
| 0  | Beliebig  | <b>Nein</b>   |
| 100  | Beliebig  | <b>Ja</b>   |
| 1..99  | 0   | <b>Nein</b>   |
| 1..99  | 100   | <b>Ja</b>   |
| 1..99  | 1..99   | <b>Mögliche</b><br>Wahrscheinlichkeit = MAX(R,P)            |


## 16.4.2 Zuweisen eines Personensicherheitsprofils zu einem Personentyp

### Dialogpfad

- **Main menu** (Hauptmenü) > **System data** (Systemdaten) > **Person Type** (Personentyp)
- **ACE client** (ACE-Client) > **System data** (Systemdaten) > **Person Type** (Personentyp)

### Vorgehensweise

**Hinweis:** Aus historischen Gründen ist **Mitarbeiter-ID** hier ein Synonym für **Person type** (Personentyp).

1. Wählen Sie in der Tabelle **Predefined employee IDs** (Vordefinierte Mitarbeiter-IDs) oder **User-defined employee IDs** (Benutzerdefinierte Mitarbeiter-IDs) die Zelle in der Spalte **Security profile name** (Sicherheitsprofilname) aus, die dem gewünschten Personentyp entspricht.
2. Wählen Sie ein Personensicherheitsprofil aus der Dropdown-Liste aus.
  - Wiederholen Sie diesen Vorgang für alle Personentypen, für die ein Personensicherheitsprofil erforderlich ist.
3. Klicken Sie auf  (Speichern), um Ihre Zuordnungen zu speichern.

## 16.5

### Konfigurationsschritte in Personaldatendialogen

In diesem Abschnitt wird beschrieben, wie neue **Personendatensätze**, die im System erstellt werden, ein **Personensicherheitsprofil** über ihren **Personentyp** erhalten.

#### Dialogpfade

- **Main menu** (Hauptmenü) > **Personnel data** (Personaldaten) > **Persons** (Personen)
- **Main menu** (Hauptmenü) > **Personnel data** (Personaldaten) > **Group of Persons** (Personengruppen)

**Hinweis:** Aus historischen Gründen ist **Mitarbeiter-ID** hier ein Synonym für **Person type** (Personentyp).

#### Vorgehensweise

Alle im System erstellten **Personendatensätze** müssen über einen **Personentyp** verfügen.

1. Stellen Sie sicher, dass Systembediener nur **Personentypen** zuweisen, die im Dialog **Main menu** (Hauptmenü) > **System data** (Systemdaten) > **Person Type** (Personentyp) mit einem **Personensicherheitsprofil** verknüpft wurden.
2. Klicken Sie auf die folgenden Links, um Details zur Verknüpfung von **Personensicherheitsprofilen** und zur Erstellung von **Personendatensätzen** zu erhalten.

#### Siehe

- *Zuweisen eines Personensicherheitsprofils zu einem Personentyp, Seite 127*
- *Anlegen und Verwalten von Personaldaten, Seite 129*



# 17

## Anlegen und Verwalten von Personaldaten

### Dialogpfad

Main menu (Hauptmenü) > **Personnel data** (Personaldaten) > <sub-dialogs>

### Gesamtverfahren

1. Geben Sie im Unterdialog **Persons** (Personen) die ID-Daten der Person ein.
2. Im Unterdialog **Cards** (Ausweise) haben Sie folgende Möglichkeiten:
  - Zuweisen von Zutrittsprofilen oder individuellen Zutrittsberechtigungen
  - Zuweisen eines Zeitmodells, falls erforderlich
  - Zuweisen des Ausweises
3. Im Unterdialog **PIN-Code** : Weisen Sie bei Bedarf einen PIN-Code zu.
4. Im Unterdialog **Print Badges** (Ausweise drucken) drucken Sie den Ausweis.

Gehen Sie bei **Besuchern** wie folgt vor:

- Geben Sie im Dialog **Visitors** (Besucher) des Menüs **Visitors** (Besucher) die personenbezogenen Daten ein, und weisen Sie gegebenenfalls einen Begleiter zu.



### Hinweis!

Ausweise und Zutrittsberechtigungen müssen nicht gleichzeitig zugewiesen werden. Es ist also möglich, Personen nur Ausweise oder nur Zutrittsberechtigungen zuzuweisen. Allerdings wird diesen Personen in beiden Fällen jeglicher Zutritt verwehrt.

### Der Vorgang des Scannens von Ausweisen.

Wenn Ausweise an Lesern gescannt werden, führt der Leser eine Reihe von Überprüfungen durch:

- Ist der Ausweis gültig und im System registriert?
- Ist der Ausweisinhabers aktuell gesperrt (im System deaktiviert)?
- Verfügt der Ausweisinhaber über die Berechtigung zum Zutritt in dieser Richtung?
- Handelt es sich bei der Zutrittsberechtigung um eine Raum-Zeit-Berechtigung? Wenn ja, liegt die Scanzeit innerhalb des vom Zeitmodell vorgegebenen Zeitfensters?
- Ist die Zutrittsberechtigung aktiv, d. h. weder **abgelaufen** noch **gesperrt** (deaktiviert)?
- Unterliegt der Ausweisinhaber einem Zeitmodell? Wenn ja, liegt die Scanzeit innerhalb der definierten Intervalle?

**Voraussetzung:** Die Zeitmodellprüfungen müssen beim betreffenden Leser aktiviert sein.

- Befindet sich der Ausweisinhaber laut Zutrittssequenzüberwachung am richtigen Ort?  
**Voraussetzung:** Die Zutrittssequenzüberwachung ist am betreffenden Leser aktiviert.
- Wurde für den Zielbereich dieses Lesers eine Höchstanzahl an Personen definiert und wurde diese Anzahl bereits erreicht?
- Im Falle der Zutrittssequenzüberwachung, einschließlich Zutrittswiederholkontrolle: Wird dieser Ausweis an einem Leser gescannt, bevor die durch die Zutrittswiederholkontrolle eingestellte Sperrzeit abgelaufen ist?
- Ist ein zusätzlicher PIN-Code erforderlich? **Voraussetzung:** Der Leser verfügt über eine Tastatur.
- Wenn eine Bedrohungsstufe in Betrieb ist, hat das **Personensicherheitsprofil** des Ausweisinhabers eine **Sicherheitsstufe**, die mindestens der Sicherheitsstufe des Lesers auf dieser Bedrohungsstufe entspricht?

## 17.1 Personen

Die Daten von Personen, für die das Kontrollkästchen **Administered globally** (Global administriert) ausgewählt wurde, können nur von Bedienern mit der zusätzlichen Berechtigung **Global Administrator** (Globaler Administrator) bearbeitet werden. Diese Berechtigung wird im BIS Configuration Browser im Bedienerdialog festgelegt.

Zu den geschützten Daten gehören:

- alle Daten des Dialogs **Persons** (Personen) außer denen auf der Registerkarte **Remarks** (Anmerkungen) und speziell definierten zusätzlichen Informationsfeldern auf der Registerkarte **Extra Info** (Reserve)
- alle Daten des Dialogs **Cards** (Ausweise)
- alle Daten des Dialogs **PIN-Code**

Alle anderen Daten dieser Personen können von einem beliebigen Bediener bearbeitet werden.

Die folgende Tabelle führt die wichtigsten Datentypen auf, die aufgezeichnet werden können. Fast alle Felder sind optional. Pflichtfelder sind auf der Bedieneroberfläche deutlich mit unterstrichenen Beschriftungen markiert.

| Registerkarte                  | Feldname   |
|--------------------------------|--|
| Dialogkopf                     | Name   |
|                                | First name (Vorname)   |
|                                | Birth name (Geburtsname) (Geburtsname oder auch Mädchenname)   |
|                                | Personnel no. (Personalnr.)                                    |
|                                | Date of birth (Geburtsdatum)                                   |
|                                | Employee ID (Mitarbeiter-ID) (auch als Personentyp bezeichnet) |
|                                | Gender (Geschlecht)  |
|                                | Company (Unternehmen)  |
|                                | Title (Titel)  |
|                                | ID card no. (Ausweis-Nr)                                       |
|                                | Car license no. (Kfz.-Kennzeichen)                             |
| Address (Adresse)              | Zip code (PLZ)   |
|                                | Street, no. (Straße, Nr.)                                      |
|                                | Country, state (Land, Staat)                                   |
|                                | Nationality (Staatsangehörigkeit)                              |
| Contact (Kontaktinformationen) | Phone other (Telefon Privat)                                   |
|                                | Company phone (Telefon Firma)                                  |
|                                | Company fax (Fax Firma)  |
|                                | Mobile phone (Telefon Mobil)                                   |
|                                | Phone (Telefon)  |

|   |  |
|---|--|
|   | E-Mail   |
|   | Web page address (Homepage)  |
| Additional Person Data<br>(Weitere Personendaten) | Patronymic (Vatername, zusätzlicher Name, der in vielen Kulturen verwendet wird)   |
|   | Birthplace (Geburtsort)  |
|   | Marital status (Familienstand)   |
|   | Official identity card (Amtl. Ausweis)   |
|   | Identity card no. (Ausweis Nr.)  |
|   | Valid until (Gültig bis)   |
|   | Height (Größe)   |
| Additional Company Data<br>(Firmendaten)          | Department (Abteilung)   |
|   | Location (Standort)  |
|   | Cost center (Kostenstelle)   |
|   | Job title (Tätigkeitsbezeichnung)  |
|   | Attendant (Escort) (Betreuer für betriebsfremde Personen)  |
|   | Reason for visit (Aufenthaltsgrund)  |
|   | Anmerkungen  |
| Anmerkungen                                       | (Bietet ein frei definierbares Textfeld für Notizen und Hinweise zur Person.)  |
| Extra Info (Reserve)                              | 10 benutzerdefinierbare Felder   |
| Unterschrift                                      | Unterschriften erfassen, neu erfassen und löschen  |
| Fingerabdrücke                                    | Fingerabdrücke als biometrische Nachweise erfassen, neu erfassen, löschen und testen.<br>Bestimmte Fingerabdrücke als Zeichen bei Bedrohung festlegen. |

### 17.1.1 Optionen zur Ausweis-/Gebäudekontrolle

#### 17.1.2 Reserve: Aufzeichnen benutzerdefinierter Informationen

Auf der Registerkarte **Extra info** (Reserve) können Sie [zusätzliche Felder](#) definieren, die auf anderen Registerkarten nicht zur Verfügung stehen. Falls keine zusätzlichen Felder definiert werden, bleibt die Registerkarte leer.

#### 17.1.3 Erfassen von Unterschriften

Um Unterschriften zu erfassen, muss eine Unterlage von Signotec zum Erfassen von Unterschriften angeschlossen und im System konfiguriert sein. Wenden Sie sich bei Fragen an Ihren Systemmanager.

1. Klicken Sie auf die Registerkarte **Signature** (Unterschrift).
2. Klicken Sie zum Erfassen einer neuen Unterschrift auf die Schaltfläche **Capture Signature** (Unterschrift erfassen).
3. Unterzeichnen Sie mit dem besonderen Stift direkt auf der Unterlage.

- Klicken Sie zur Bestätigung auf die Häkchen-Schaltfläche.  
Die neue Unterschrift wird nun auf dem Bildschirm angezeigt. (Zur Vergrößerung der Ansicht auf die Unterschrift klicken.)

#### Verwandte Verfahren:

- Klicken Sie auf die Schaltfläche **Capture Signature** (Unterschrift erfassen), wenn Sie eine vorhandene Unterschrift überschreiben möchten.
- Klicken Sie auf die Schaltfläche **Delete Signatur** (Unterschrift löschen), um eine vorhandene Unterschrift zu löschen.

## 17.1.4


### Registrieren von Fingerabdruckdaten

#### Voraussetzungen

- Ein oder mehrere Fingerabdruckleser müssen an den Durchritten konfiguriert werden, um eine biometrische Zutrittskontrolle durchzuführen.
- WICHTIG: Diese Leser empfangen und speichern regelmäßig Ausweis- und Fingerabdruckdaten von den Servern. Die Einstellungen am einzelnen Leser entscheiden letztendlich, welche Zugangsdaten akzeptiert werden. Sie überschreiben alle hier für die Person vorgenommenen Einstellungen.
- Um Fingerabdrücke als Verifizierung für (oder alternativ zu) ausweisbasierter Berechtigung zu verwenden, müssen alle Ausweisinhaber ihre Fingerabdrücke scannen lassen.
- Der Registrierende befindet sich vor einem Fingerabdruckleser, der mit Ihrer Dialogstation verbunden und für diese konfiguriert ist.
- Als Bediener kommunizieren Sie direkt mit dem Registrierenden, also mit der Person, deren Fingerabdrücke als biometrischer Nachweis für den Zutritt erfasst werden.
- Sie sind mit dem Vorgang vertraut, wie der Finger wiederholt vor dem verwendeten Leser gezeigt werden muss, damit die Fingerabdrücke effektiv erfasst werden.

#### Registrieren eines Fingerabdrucks für den Zutritt

- Navigieren Sie zum Fingerabdruckdialog: **Personnel data** (Personaldaten) > **Persons** (Personen) > Registerkarte: **Fingerprints** (Fingerabdrücke) und erstellen oder suchen Sie den Registrierenden in der Datenbank.

2. Fragen Sie den Registrierenden, welcher Finger für den regelmäßigen Zutritt über den Fingerabdruckleser verwendet werden soll.
3. Wählen Sie den entsprechenden Finger im Schaubild aus.  
Ergebnis: Die Fingerspitze wird mit einem Fragezeichen markiert.
4. Klicken Sie auf die Schaltfläche **Enroll fingerprint** (Fingerabdruck registrieren).
5. Erläutern Sie dem Registrierenden, wie der Finger an den Leser gehalten werden soll. Beispielanweisungen befinden sich im Dialogbereich unterhalb des Handschaubilds. Für die einzelnen Lesertypen können jedoch auch leicht unterschiedliche Vorgehensweisen gelten.
6. Wenn der Fingerabdruck erfolgreich registriert wurde, wird ein Bestätigungsfenster angezeigt.
7. Wählen Sie einen **Identifikationsmodus** aus. Dieser bestimmt, welche Zugangsdaten ein Fingerabdruckleser vom Registrierenden verlangt, wenn dieser Zugriff anfordert. Beachten Sie, dass der hier eingestellte Modus nur wirksam wird, wenn der Leserparameter **Personenabhängige Überprüfung** ausgewählt wurde.  
Die Optionen sind:
  - **Nur Fingerabdruck:** Es wird nur der Fingerabdruckscanner im Leser verwendet.
  - **Nur Karte:** Es wird nur der Kartenscanner im Leser verwendet.
  - **Karte und Fingerabdruck:** Beide Scanner im Leser werden verwendet. Der Registrierende muss sowohl die Karte als auch den ausgewählten Finger am Leser präsentieren, um Zutritt zu erhalten.
8. Klicken Sie auf  (Speichern), um den Fingerabdruck und den Identifikationsmodus für den Registrierenden zu speichern.



#### Hinweis!

Lesereinstellungen überschreiben Personeneinstellungen

Beachten Sie, dass der im Fingerabdruckdialog ausgewählte Identifikationsmodus nur funktioniert, wenn der Fingerabdruckleser selbst mit der Option **Personenabhängige Überprüfung** im Geräteeditor konfiguriert ist. Wenden Sie sich bei Fragen an Ihren Systemadministrator.

#### Registrieren eines Fingerabdrucks als Zeichen für Bedrohung

##### Voraussetzungen:

- Mindestens ein Fingerabdruck des Registrierenden wurde bereits registriert und gespeichert.
  - Der Fingerabdruckleser ist online. Im Offline-Modus kann der Leser natürlich kein Zeichen für Bedrohung an das System senden.
1. Bitten Sie den Registrierenden, einen Finger auszuwählen, den er bei Bedrohung verwenden möchte, falls er von einer nicht autorisierten Person gezwungen wird, den Fingerabdruckleser zu verwenden.
  2. Wiederholen Sie für diesen Finger die oben beschriebene Vorgehensweise zum Registrieren eines Fingerabdrucks.
  3. Nachdem der zweite Fingerabdruck registriert wurde, wählen Sie ihn im Schaubild aus. Klicken Sie auf die Schaltfläche **Duress finger** (Finger bei Bedrohung). Der gewählte Finger als Zeichen für Bedrohung wird mit einem Ausrufezeichen im Schaubild markiert.

Wenn der Registrierende dann den „Bedrohungsfinger“ an einem Fingerabdruckleser verwendet und der Leser nicht offline ist, signalisiert das System dem Bediener unter Verwendung eines Popup-Fensters eine Bedrohung.

#### Testen gespeicherter Fingerabdrücke

1. Wählen Sie im Schaubild den Fingerabdruck aus, den Sie testen möchten.
2. Bitten Sie den Registrierenden, den Finger auf dem Leser zu platzieren.
3. Klicken Sie auf die Schaltfläche **Match fingerprint** (Fingerabdruck abgleichen).  
Ergebnis: In einem Popup-Fenster wird bestätigt, ob der gespeicherte Fingerabdruck dem auf dem Lesegerät entspricht oder nicht. Dieser Vorgang sollte wiederholt werden, um die Wahrscheinlichkeit eines Falschalarms zu reduzieren.

#### Löschen gespeicherter Fingerabdrücke

1. Wählen Sie im Schaubild den Fingerabdruck aus, den Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche **Delete fingerprint** (Fingerabdruck löschen).
3. Warten Sie auf die Bestätigung der Löschung.

## 17.2

### Firmen

- In diesem Dialog können neue Firmen erstellt und vorhandene Firmendaten geändert oder gelöscht werden.
- Der Name und Kurzname der Firma müssen eingegeben werden. Der Kurzname muss eindeutig sein.
- Wenn die Eintragung einer Firma im Dialog **Persons** (Personen) obligatorisch ist, erstellen Sie in diesem Dialog die Firma, bevor Sie Personaldatensätze für diese Firma anlegen.
- Firmen können nicht aus dem System gelöscht werden, wenn ihnen noch Personaldatensätze zugeordnet sind.

## 17.3

### Ausweise: Erstellen und Zuweisen von Zugangsdaten und Berechtigungen

Der Zweck dieses Dialogs ist die Zuweisung von **Ausweisen, Zutrittsberechtigungen** oder Bundles an Zutrittsberechtigungen (**Zutrittsprofile**) zu Personaldatensätzen.

Zutrittsberechtigungen und Profile werden Personen, nicht Ausweisen, zugewiesen.

Neue Ausweise, die einer Person zugeordnet sind, erhalten die Zutrittsberechtigungen, die dieser Person bereits zugewiesen sind.

#### Hinweis: Verwenden von Zugriffsprofilen zum Bündeln von Berechtigungen

Aus Gründen der Einheitlichkeit und Bequemlichkeit werden Zutrittsberechtigungen nicht einzeln zugewiesen, sondern typischerweise gebündelt in **Zugriffsprofile** und als solche zugewiesen.

- Hauptmenü: > **System data (Systemdaten)** > **Access profiles** (Zugriffsprofile)

#### Die Ausweisliste

Im Dialog "Cards" (Ausweise) wird eine Liste der Ausweise angezeigt, die die ausgewählte Person besitzt. Unter anderem werden folgende Attribute in der Liste aufgeführt:

- Verwendungstyp.
- Ein Kennzeichen dafür, ob der Ausweis für ein konfiguriertes Offline-Sperrsystem verwendet werden kann.

- Ob der Ausweis aufgrund wiederholter Verwendung ungültiger PINs gesperrt ist. Dieser Zustand wird besonders hervorgehoben.
- Erstellungsdatum des Ausweises.
- Ablaufdatum des Ausweises (Einzugsdatum).  
**Hinweis:** Ein motorisierter Ausweisleser kann einen abgelaufenen Ausweis einziehen. Andere Ausweisleser entwerfen den Ausweis einfach.
- Das Datum des letzten Drucks des Ausweises und die Anzahl der gedruckten Ausweise.
- Details der Code-Daten.

Option **Administered globally** (Global administriert)

Die Daten von Personen, für die die Einstellung **Administered globally** (Global administriert) (Kontrollkästchen neben dem Fotorahmen) ausgewählt wurde, können nur von Bedienern mit der zusätzlichen Berechtigung **Global Administrator** (Globaler Administrator) bearbeitet werden.

Die folgenden Daten sind schreibgeschützt für Bediener, die dieses Recht nicht haben:

- alle Daten im Dialog **Persons** (Personen) außer auf den Registerkarten **Remarks, Extra info** (Bemerkung, Reserve) und in den Reservefeldern
- alle Daten des Dialogs **Cards** (Ausweise)
- alle Daten des Dialogs **PIN Code** (PIN-Code)

Dieses **Globaler Administrator**-Recht kann im folgenden Kontrollkästchen zugewiesen werden:

- Hauptmenü: **Configuration** (Konfiguration) > **Operators and workstations** (Bediener und Dialogstationen) > **User rights** (Benutzerrechte) > Kontrollkästchen: **Global Administrator** (Globaler Administrator).

## 17.3.1

### Zuweisen von Ausweisen zu Personen

#### Einführung

Eine Person, die der Zutrittskontrolle unterliegt, benötigt einen Ausweis oder einen anderen elektronischen Nachweis, der in dem Ausweis-Dialog dem Inhaber zugewiesen ist. Ausweisnummern können manuell oder automatisch über einen Bekanntmachungsleser zugewiesen werden.

#### Dialogpfad

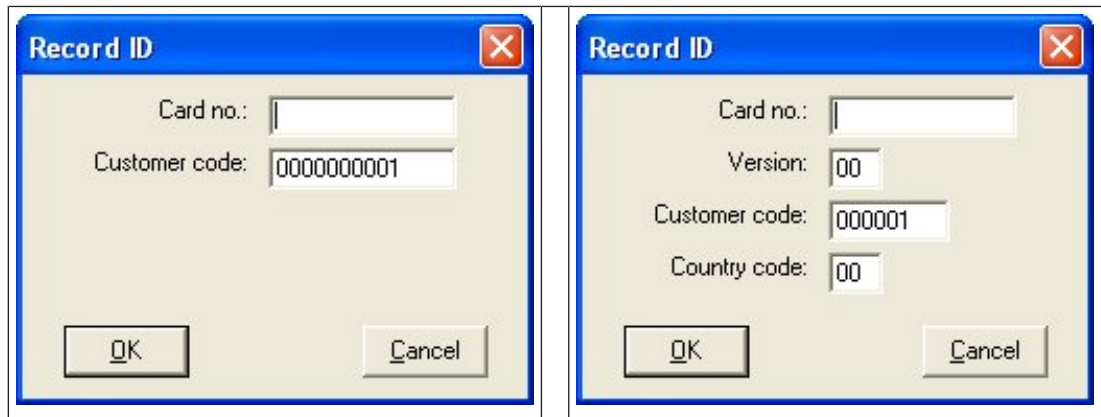
Main menu (Hauptmenü) > **Personnel data** (Personaldaten) > **Cards** (Ausweise)

#### Voraussetzung

Sie haben den Personaldatensatz, der den Ausweis erhalten soll, in die Kopfzeile des Dialogs **Cards** (Ausweise) geladen.

#### Manuelle Eingabe von Ausweisdaten

Über die Schaltfläche **Record card** (Ausweis erfassen) wird einer Person ein Ausweis zugewiesen. Der Dialog **Record ID** (Ausweiskarte erfassen) wird angezeigt. Je nachdem, welcher Ausweistyp ausgewählt wurde und welche Controller und Leser verwendet werden, wird einer der beiden folgenden Eingabedialoge eingeblendet.



Geben Sie die auf dem Ausweis gedruckte Nummer manuell ein. Ausweisnummern werden automatisch mit führenden Nullen aufgefüllt, damit sie zwölfstellig gespeichert werden können. In einigen Systemen werden keine neuen Ausweisnummern zugewiesen, wenn ein Ausweis verloren geht. Vielmehr wird die gleiche Ausweisnummer mit einer höheren Versionsnummer ausgegeben. Der Ländercode und der Kundencode werden vom Hersteller bereitgestellt und müssen in die Registrierungsdatei des Systems eingegeben werden. Wenn sie nicht bereits vom System verwendet wird, wird die Ausweisnummer der Person zugewiesen. Die erfolgreiche Zuweisung wird in einem Popup-Fenster bestätigt.

### Verwenden eines Bekanntmachungslesers

#### Voraussetzung

Ein Bekanntmachungsleser wurde mit der Dialogstation verbunden, an der Sie arbeiten.

#### Vorgehensweise für die Registrierung

1. Klicken Sie auf die Schaltfläche  auf der rechten Seite der Schaltfläche **Record card** (Ausweis erfassen), um einen konfigurierten Bekanntmachungsleser auszuwählen.
2. Klicken Sie auf die Schaltfläche **Record card** (Ausweis erfassen) und folgen Sie den Anweisungen auf dem Bildschirm.
3. Je nach Lesertyp können Sie jetzt die Ausweisdetails in ein Dialogfeld eingeben oder die Daten aus dem Ausweis über den Leser auslesen lassen.

#### Vorgehensweise zum Wechseln von Ausweisen

1. Wähle einen Ausweis aus der Liste aus.
2. Klicken Sie auf die Schaltfläche **Change card** (Ausweis wechseln).
3. Bearbeiten Sie die Ausweisdaten im Popup-Fenster und klicken Sie zum Speichern auf OK.

#### Löschen von Ausweisen

1. Wähle einen Ausweis aus der Liste aus.
2. Klicken Sie auf die Schaltfläche **Delete card** (Ausweis löschen), um die Zuweisung eines Ausweises zu einer Person zu entfernen.

**Hinweis:** Wenn Sie den letzten Ausweis eines Ausweisinhabers löschen, wird der Status der Person zu **unregistered** (unbekannt) geändert (rote Beschriftung in der Statusleiste neben **Registered** (Bekannt)). Diese Person unterliegt dann länger der Zutrittskontrolle.



### 17.3.2

## Registerkarte "Authorizations" (Berechtigungen)

### Zuweisen von Berechtigungen, die als Zutrittsprofile gebündelt sind

Die bequemste und flexibelste Möglichkeit, Ausweisinhabern Berechtigungen zuzuweisen, besteht darin, sie zuerst in Zutrittsprofile zu bündeln und dann das Profil zuzuordnen.

- Informationen zum Erstellen von Zutrittsprofilen finden Sie im Abschnitt *Erstellen von Zutrittsprofilen*, Seite 152
- Um diesem Ausweisinhaber ein Zutrittsprofil zuzuweisen, wählen Sie ein definiertes Profil aus der Liste **Access profile:** (Zutrittsprofil:)

### Direktes Zuweisen von Zutrittsberechtigungen

Auf der Registerkarte **Authorizations** (Berechtigungen):

Alle Zutrittsberechtigungen, die der Person bereits zugewiesen wurden, erscheinen in der linken Liste.

Alle Zutrittsberechtigungen, die für die Zuweisung zur Verfügung stehen, erscheinen in der rechten Liste.

Wählen Sie Elemente aus und klicken Sie dann auf die Schaltflächen zwischen den Listen, um Elemente von einer Liste in die andere zu verschieben.



weist das ausgewählte Element zu.



hebt die Zuweisung des ausgewählten Elements auf.



weist alle verfügbaren Elemente zu.



hebt die Zuweisung aller zugewiesenen Elemente auf.

### Möglichkeit: **Berechtigungen zugewiesen lassen**

Die Auswirkung der Zuweisung eines Zutrittsprofils zu einer Person hängt vom Status des Kontrollkästchens **Keep authorizations assigned** (vergebene Rechte beibehalten) ab:

- Ist das Kontrollkästchen deaktiviert, werden alle zuvor getroffenen Auswahlen und alle bereits zugewiesenen Zutrittsberechtigungen **ersetzt**, sobald das Profil zugewiesen wird.
- Ist das Kontrollkästchen aktiviert, werden die im Profil enthaltenen Berechtigungen den zugewiesenen Berechtigungen **hinzugefügt**.

### Begrenzung der Zeitspanne von Berechtigungen

Verwenden Sie die Datumsfelder **Valid from:** (Gültig ab:) und **until:** (bis:), um die Start- und Endzeiten der Berechtigungen und Profile zu begrenzen. Wenn keine Werte festgelegt sind, ist die Berechtigung sofort gültig und zeitlich unbegrenzt.



Klicken Sie auf , um einen Dialog zu öffnen, um die Dauer für einzelne Berechtigungen festzulegen.

### Anzeigen der Durchtritte einer Berechtigung

Klicken Sie mit der rechten Maustaste auf eine Berechtigung in einer der beiden Listen, um eine Liste der zugehörigen Durchtritte anzuzeigen.

### 17.3.3

## Registerkarte "Other data" (Andere Daten): Ausnahmen und spezielle Berechtigungen

### Zuweisen eines Zeitmodells:

Geben Sie im Listenfeld **Time model** (Zeitmodell) an, zu welchen Zeiten dem Ausweisinhaber täglich der Zutritt gewährt wird. Das sind die Zeiträume, in denen die Zugangsdaten des Karteninhabers Zugang gewähren.

#### **Ausschließen von Personen von der Mitarbeiterauslosung**

Aktivieren Sie das Kontrollkästchen **Excluded from random screening** (von MA-Auslosung ausgeschlossen), um Personen davon auszuschließen, zufällig für die Überprüfungen an den Ein- und Ausgängen ausgewählt zu werden.

#### **Ausschließen von Personen von PIN-Code Prüfungen**

Aktivieren Sie das Kontrollkästchen **Disable PIN code check** (PIN-Code Prüfung deaktivieren), um Personen davon auszuschließen, außerhalb der normalen Arbeitszeiten ihre PIN-Codes an den PIN-Code-Lesern einzugeben.



#### **Hinweis!**

Der Ausschluss von PIN-Code Prüfungen wirkt sich auf das gesamte System aus. Beispiel: Da die PIN-Codes dieser Personen nicht überprüft werden, können sie auch nicht in Türmodell 10 das Alarmsystem an den Eingängen scharf oder unscharf stellen.

#### **Verlängern der Türöffnungszeit**

Aktivieren Sie das Kontrollkästchen **Extended door opening time** (Verlängerte Türöffnungszeit), um Personen mit Behinderung die dreifache Zeit für den Durchtritt zu geben, bevor der Zustand **Door open too long** (Tür zu lange geöffnet) generiert wird.

#### **Wegekontrolle**

Ein **Weg** oder ein **Rundgang** beschreibt eine strenge Abfolge von Lesern, die im Client-Menü festgelegt wird: Dialog **Tour monitoring** (Wegekontrolle) > **Define routes** (Wege definieren). Um einem Ausweisinhaber einen Weg zuzuweisen, aktivieren Sie das Kontrollkästchen **Tour monitoring** (Wegekontrolle) und wählen Sie aus der Dropdown-Liste eine definierte Runde aus. Falls keine Runden definiert wurden, bleibt das Kontrollkästchen deaktiviert. Nach dem Zuweisen zu einem Ausweisinhaber wird ein **Weg** aktiviert, sobald der Ausweisinhaber seinen Ausweis am ersten Leser der Abfolge scannt. Anschließend müssen alle Leser in der vorgeschriebenen Reihenfolge aufgesucht werden, bis die Runde abgeschlossen ist. Diese Funktion kommt in der Regel zum Einsatz, wenn strenge Zutrittsabfolgen erzwungen werden sollen, wie in industrielle Reinräumen, hygienisch kontrollierten oder Hochsicherheitsbereichen.

#### **Erlaubnis zum Öffnen von Türen**

Aktivieren Sie das Kontrollkästchen, damit der Ausweisinhaber Türen für längere Zeit entsperren kann (siehe **Büromodus**).

## 17.3.4

### **Autorisieren von Personen zum Festlegen des Büromodus**

#### **Einführung**

Der Begriff Büromodus beschreibt die Aufhebung der Zutrittskontrolle an einem Durchtritt während der Büro- oder Geschäftszeiten. Während dieser Zeiten bleibt der Durchtritt entsperrt, um einen ungehinderten öffentlichen Zutritt zu ermöglichen. Außerhalb dieser Zeiten gilt der Normale Modus, d. h. dass der Zutritt nur Personen gewährt wird, die einen gültigen Ausweis am Leser vorzeigen.

Der Büromodus ist eine typische Anforderung von Einzelhandels-, Bildungs- und medizinischen Einrichtungen.

### Voraussetzungen

Damit der Büromodus funktioniert, müssen die folgenden Voraussetzungen erfüllt sein:

#### In der Konfiguration (Gerätebaum)

- Ein oder mehrere Durchtritte müssen so konfiguriert werden, dass lange entspernte Zeiträume zulässig sind.
- Am Durchtritt muss mindestens ein Leser mit Tastenfeld verwendet werden.

#### Im Client (Personen-Dialoge)

- Ein oder mehrere Ausweisinhaber müssen berechtigt sein, den Büromodus für den Durchtritt zu aktivieren und zu deaktivieren.
- Ihre Ausweise müssen gültig sein und den Zutritt beim Durchtritt außerhalb der Büromodus-Zeiten erlauben.

### Autorisieren von Personen zum Festlegen des Büromodus

#### Vorgehensweise für einzelne Ausweisinhaber

1. Navigieren Sie zu: **Personaldaten** > **Karten** > Registerkarte: **Weitere Daten** und erstellen oder suchen Sie den ausgewählten Ausweisinhaber in der Datenbank.
2. Aktivieren Sie das Kontrollkästchen **Erlaubnis zum Öffnen von Türen**.



3. Klicken Sie auf das Diskettensymbol, um die Daten des Ausweisinhabers zu speichern.

#### Vorgehensweise für Gruppen von Ausweisinhabern

1. Navigieren Sie zu: **Personaldaten** > **Groups of persons** (Gruppen von Personen) und verwenden Sie die Filterkriterien, um eine Liste von Ausweisinhabern im Listenfenster zusammenzustellen.
2. Wählen Sie aus der Dropdown-Liste **Field to change** (Zu änderndes Feld) die Option **Unlock doors** (Türen öffnen) aus.
3. Aktivieren Sie das Kontrollkästchen **Unlock doors** (Türen öffnen).
4. Klicken Sie auf die Schaltfläche **Änderungen ausführen**, um die Daten des Ausweisinhabers zu speichern.

### Anweisen des Ausweisinhabers für das Starten und Stoppen des Büromodus

Um den Büromodus am Durchtritt zu starten oder zu stoppen, drückt der Ausweisinhaber die Nummer 3 auf der Tastatur und zeigt dann seine speziell autorisierte Karte am Leser vor.

Der Durchtritt bleibt solange frei, bis ein berechtigter Ausweisinhaber 3 drückt und die Karte erneut vorzeigt.

Beachten Sie, dass Wachleute mit Wächterausweisen den Büromodus auf die gleiche Weise ohne besondere Erlaubnis stoppen können.

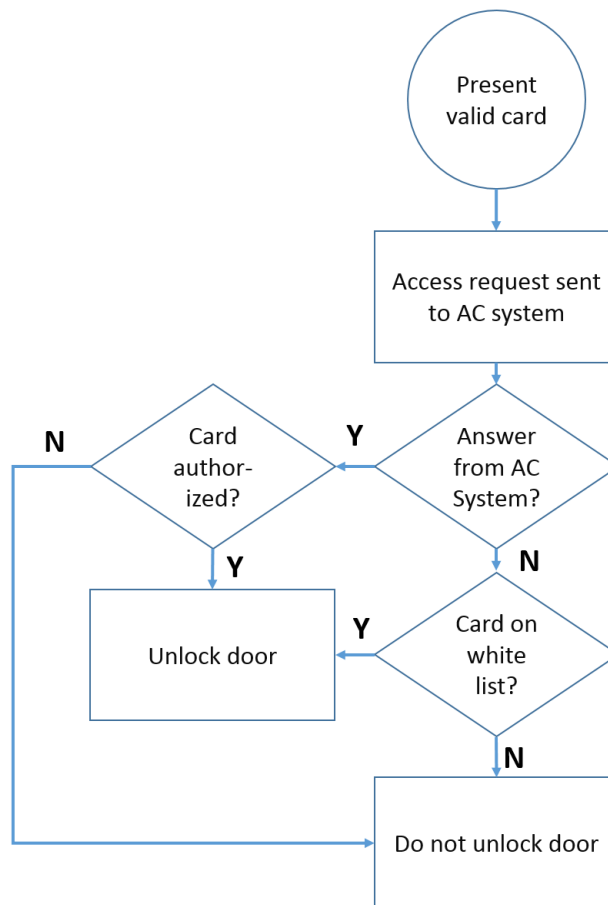
## 17.3.5

### SmartIntego-Registerkarte

#### SmartIntego-Schließsysteme

#### Einführung

Der SmartIntego-Ausweisleser versucht zunächst, den Zutritt über das Hauptzutrittskontrollsystem zu autorisieren. Wenn die Verbindung fehlschlägt, sucht er auf der Whitelist nach der Ausweisnummer.



Zutrittsberechtigungen für das SmartIntego-Schließsystem wurden auf dieselbe Weise wie andere Zutrittsberechtigungen vergeben.

#### Voraussetzungen

- Ein SimonsVoss SmartIntego-Schließsystem wurde in Ihrem Zutrittskontrollsystem konfiguriert. Anweisungen finden Sie in der Konfigurationsanleitung.
- Die Ausweisinhaber verwenden MIFARE classic- oder MIFARE Desfire-Karten. SmartIntego verwendet die Kartenseriennummer (Card Serial Number, CSN).

#### Das Zuweisungsverfahren

Im Folgenden wird beschrieben, wie Sie zusätzlich zu sämtlichen Berechtigungen, die bereits über das Hauptzutrittskontrollsystem vergeben wurden, eine Kartennummer zu einer SmartIntego-Whitelist hinzufügen.

Whitelists werden lokal auf den SmartIntego-Türen gespeichert, sodass ein Leser Zutritt zu den Whitelist-Kartennummern gewähren kann, selbst wenn die Verbindung zu seinem MAC unterbrochen ist.

Ergänzungen zu und Löschungen aus den Whitelists werden an die SmartIntego-Leser übertragen, sobald die Ausweisinhaberdaten gespeichert sind und eine Verbindung verfügbar ist.

1. Wählen Sie im AMS-Client-Hauptmenü **Personnel data** (Personaldaten) > **Cards** (Ausweise) aus.

2. Wählen Sie die Person aus, die SmartIntego-Berechtigungen erhalten soll.
3. Wählen Sie die Registerkarte **SmartIntego**.
4. Nehmen Sie die Zuweisungen vor:
  - Alle Zutrittsberechtigungen, die der Person bereits zugewiesen wurden, erscheinen in der linken Liste.
  - Alle Zutrittsberechtigungen, die für die Zuweisung zur Verfügung stehen, erscheinen in der rechten Liste.

Wählen Sie Elemente aus und klicken Sie dann auf die Schaltflächen zwischen den Listen, um Elemente von einer Liste in die andere zu verschieben.



weist das ausgewählte Element zu.



hebt die Zuweisung des ausgewählten Elements auf.



weist alle verfügbaren Elemente zu.



hebt die Zuweisung aller zugewiesenen Elemente auf.

### 17.3.6

#### Erstellen eines Alarmausweis

In diesem Abschnitt wird beschrieben, wie Sie eine Alarmausweis erstellen, die verwendet werden kann, um eine Bedrohungsstufe auszulösen.

##### Einführung

Ein Alarmausweis ist eine Karte, die eine bestimmte Bedrohungsstufe auslöst, wenn sie an einem Leser eingelesen wird. Eine Bedrohungsstufe kann nicht durch einen Alarmausweis, sondern nur über die Zutrittskontrollsoftware aufgehoben werden.

##### Voraussetzungen

- Auf Ihrem System ist ein Dialogleser zum Schreiben von Daten auf den Ausweis installiert.
- Mindestens eine Bedrohungsstufe wurde im System definiert.

##### Dialogpfad

Main menu (Hauptmenü) > **Personnel data** (Personaldaten) > **Cards** (Ausweise) > **Alert card** (Alarmausweise)

##### Vorgehensweise

1. Laden Sie den Personendatensatz der Person, der der Alarmausweis zugewiesen wird.
2. Klicken Sie auf der Registerkarte „Alert card“ (Alarmausweis) auf „Record card“ (Ausweis erfassen).
  - Ein Popup-Fenster wird angezeigt: **Select threat level** (Bedrohungsstufe auswählen).
3. Wählen Sie im Popup-Fenster die gewünschte Bedrohungsstufe aus, und klicken Sie auf **OK**.
  - Ein Popup-Fenster wird angezeigt: **Recording badge ID** (Badge-ID wird erfasst).
4. Geben Sie die üblichen Ausweisdaten ein, die Ihrer Standortinstallation entsprechen, und klicken Sie auf **OK**.
  - Der erfasste Alarmausweis wird in der Liste auf der Registerkarte **Alert card** (Alarmausweis) angezeigt.

## 17.4 Temporäre Ausweise

Ein temporärer Ausweis ist ein vorübergehender Ersatz für einen Ausweis, die von einem normalen Ausweisinhaber verlegt wurde. Es ist ein Duplikat, das alle Berechtigungen und Einschränkungen des Originals enthält, einschließlich der Rechte für Offline-Türen.



Um Missbrauch vorzubeugen, kann das System wahlweise eine oder alle anderen Karten des Ausweisinhabers für einen begrenzten Zeitraum oder bis zum manuellen Entsperren sperren. Temporäre Ausweise sind daher als Besucherkarten **nicht geeignet**.

### Voraussetzungen

- Der Bediener hat Zugriff auf einen Bekanntmachungsleser, der auf seiner Dialogstation konfiguriert ist.
- Ein geeigneter physischer Ausweis ist für die Registrierung im System als temporärer Ausweis verfügbar.
- Der Empfänger des temporären Ausweises hat bereits mindestens einen weiteren Ausweis.

**Main menu** (Hauptmenü) > **Personnel data** (Personaldaten) > **Cards** (Ausweise)

### Vorgehensweise: Zuweisen von temporären Ausweisen

1. Laden Sie den erforderlichen Personaldatensatz in den Dialog **Cards** (Ausweise).
2. Wählen Sie in der Ausweisliste den Ausweis oder die Ausweise aus, für die ein vorübergehender Ersatz erforderlich ist.
3. Klicken Sie auf **Change card** (Ausweis ändern).
4. Wählen Sie im Popup-Fenster **Change card** (Ausweis wechseln) **Temporary card** (Temporärer Ausweis) aus.
5. Wählen Sie in der Liste **Period** (Zeitraum) eine der folgenden Optionen aus:
  - **Today** (Heute)
  - **Today and tomorrow** (Heute und morgen)
  - **Enter number of days** (Anzahl der Tage eingeben)
6. Geben Sie bei der letzten Option eine Ganzzahl für die Anzahl der Tage in das Feld ein. Beachten Sie, dass der **Zeitraum** in allen drei Fällen immer um Mitternacht des betreffenden Tages abläuft.
7. Aktivieren Sie ggf. das Kontrollkästchen **Deactivate all cards now** (Alle Ausweise jetzt deaktivieren).
  - Wenn ausgewählt, werden alle Ausweise dieses Ausweisinhabers gesperrt.
  - Wenn diese Option deaktiviert ist, wird nur der oben ausgewählte Ausweis gesperrt.
8. Aktivieren Sie ggf. das Kontrollkästchen **Activate card(s) automatically after period** (Ausweis(e) nach Zeitraum automatisch aktivieren).
  - Die gesperrten Ausweise werden automatisch entsperrt, wenn der oben definierte **Zeitraum** abläuft.
9. Platzieren Sie den temporären Ausweis auf dem Bekanntmachungsleser
10. Klicken Sie auf **OK**  
Die Ausweis-ID wird vom Bekanntmachungsleser erfasst.
  - Der temporäre Ausweis wird als aktiv  in der Liste der Ausweise angezeigt, zusammen mit seiner Gültigkeitsdauer und Codedaten.
  - Der andere Ausweis oder die anderen Ausweise werden als gesperrt angezeigt , abhängig von der oben vorgenommenen Einstellung: **Deactivate all cards now** (Alle Ausweise jetzt deaktivieren).

11. (Optional) Klicken Sie in der Ausweisliste auf die Spalte **Collecting date**(Einzugsdatum) für den temporären Ausweis und legen Sie ein Datum fest, um ihn vom Ausweisinhaber abzurufen.  
Der Standardwert ist **Never** (Nie).

#### **Vorgehensweise: Löschen von temporären Ausweisen**

Wenn der verlegte Originalausweis gefunden wurde, löschen Sie den temporären Ausweis wie folgt:

1. Laden Sie den erforderlichen Personaldatensatz in den Dialog **Cards** (Ausweise).
2. Wählen Sie in der Liste der Ausweise den temporären Ausweis aus.
3. Klicken Sie auf **Delete card**  
**(Ausweis löschen)**Der temporäre Ausweis wird aus der Liste gelöscht und der Ausweis oder die Ausweise, die ersetzt wurden, werden sofort entsperrt

#### **Vorgehensweise: Entfernen von temporären Sperren auf Ausweisen**

Wenn die Sperrung des ursprünglichen Ausweises nicht mehr erforderlich ist, löschen Sie die Sperre wie folgt:

1. Navigieren Sie zum Dialog **Blocking** (Sperrung): **Personnel data** (Personaldaten) > **Blocking** (Sperrung).
2. Wählen Sie in der Liste der Ausweise den persönlichen Ausweis aus, die in der Spalte **Lock(s)** (Sperre(n)) als gesperrt angezeigt werden.
3. Klicken Sie auf **Release temporary lock**  
**(Temporäre Sperre aufheben)**Beachten Sie, dass der Datensatz in der Liste **Blocking** (Sperrung) bleibt. Die Liste enthält nur einen Verlauf aller Sperren für den aktuellen Personaldatensatz, gegenwärtig und vergangen.

#### **Hinweise zu temporären Ausweisen**

- Das System erlaubt nicht, dass temporäre Ausweise selbst durch temporäre Ausweise ersetzt werden.
- Das System erlaubt nicht, dass ein persönlicher Ausweis mehr als einen temporären Ausweis hat.
- Um eine schnelle Zusammenfassung aller Ausweise eines Ausweisinhabers anzuzeigen, bewegen Sie die Maus über das linke kleine Feld mit der Beschriftung **Registered**, (Bekannt,) in der Statusleiste des Hauptdialogfensters.

## 17.5

### **PIN-Codes für Personal**

#### **Dialog: PIN-Code**

Für den Zutritt zu Zonen mit höheren Sicherheitsanforderungen sind Zutrittsberechtigungen möglicherweise nicht ausreichend. Hier muss auch ein PIN-Code eingegeben werden. Jede Person bzw. jeder Ausweis kann einen PIN-Code haben, der für alle Bereiche gilt. Die Verwendung allzu simpler Codes (z. B. 123456 oder Palindromen wie 127721) wird vom System verhindert. Die Gültigkeit kann beschränkt werden und wird für jede Person im Dialog festgelegt.

Wenn ein PIN-Code gesperrt oder abgelaufen ist, wird der Zutritt zu dem Bereich, für den der Code erforderlich ist, verweigert. Dies gilt auch, wenn der Ausweis für alle anderen Bereiche weiterhin gültig ist.

**Wird dreimal hintereinander der falsche Code eingegeben (Standardeinstellung; möglich sind Werte von 1 bis 99), so wird der Ausweis gesperrt, d. h. ihm wird der Zutritt zu allen Bereichen verweigert. Eine derartige Ausweissperre kann nur über den Dialog Blocking (Sperrung) aufgehoben werden.**

The screenshot shows a user profile form with the following fields and values:

- Name:** Mustermann
- First name:** Max
- Birth name:** (empty)
- Personnel no.:** 5c999000
- Date of birth:** Tu 08/09/1988
- Employee ID:** Employee
- Gender:** Male
- Company:** Test\_Firma
- Title:** Dr
- Car license No.:** Car000998
- Card no.:** (empty) with a 'Reader..' button
- PIN code:** (masked with red dots)
- Confirm:** (masked with red dots)
- Valid until:** Mo 01/21/2013

Additional information: Division: Common, 10/20/2014, Administered globally.

Geben Sie einen neuen PIN-Code im Eingabefeld **PIN-Code** ein und bestätigen Sie ihn durch die erneute Eingabe. Die Länge des PIN-Codes (vier bis acht Stellen, Standardwert: sechs) wird vom Systemadministrator vorgegeben.

### Hinweis!



Je nach den im System konfigurierten Ausweislesern gibt es für Ausweisinhaber unterschiedliche Methoden, ihre ID-PINs einzugeben. Beispiele:

An den RS485-Ausweislesern geben Ausweisinhaber Folgendes ein: **4 # <the PIN>**

An Wiegand und anderen Ausweislesern geben Ausweisinhaber Folgendes ein: **<the PIN> #**  
Stellen Sie sicher, dass die Ausweisinhaber über die Eingabemethode für ihre PINs informiert sind. Wenden Sie sich bei Fragen an Ihren Systemadministrator.

### PIN-Code zum Scharfschalten von Meldeanlagen

Geben Sie eine vier- bis achtstellige PIN ein (Standard: sechs Stellen, wie bei Verifikations-PIN). Diese PIN wird zur Scharfschaltung der EMA (Einbruchmeldeanlage) verwendet. Die Anzeige dieser Felder kann parametrierbar sein. Nur wenn die **separate EMA-PIN** der Kontrolle aktiviert ist, ist die Kontrolle verfügbar.

- Main menu (Hauptmenü) > **Configuration** (Konfiguration) > **Options** (Optionen) > **PIN codes** (PIN-Codes)

Wählen Sie ggf. ein Ablaufdatum.

Sind die Eingabefelder für die Eingabe der EMA-PIN nicht verfügbar, kann die Scharf- und Unscharfschaltung der EMA auch über die Verifikations-PIN erfolgen. Werden die Eingabefelder hingegen in diesem Dialog angezeigt, kann nur die Scharfschaltungs-PIN für die EMA verwendet werden.

Standardeinstellung: Die Eingabefelder für den Scharfschaltungs-PIN-Code werden nicht angezeigt.



**PINs bei Alarm (Bedrohung)**

Bedrohte Personen können über einen speziellen PIN-Code einen stillen Alarm auslösen. Da der stille Alarm von dem Bedroher unbemerkt bleiben soll, wird der Zutritt zwar gewährt, aber die Systembediener erhalten einen Hinweis auf die Bedrohung.

Es stehen zwei Varianten zur Verfügung, die gleichzeitig aktiviert sind und zwischen denen die bedrohte Person wählen kann:

- Eingabe des PIN-Codes in umgekehrter Reihenfolge (321321 statt 123123).
- Erhöhung der PIN um eine Ziffer (Beispiel: 123124 anstelle von 123123). In diesem Fall wird die PIN auch erhöht, wenn die letzte Ziffer 9 lautet, sodass für eine PIN mit den Ziffern 123129 die Bedrohungs-PIN 123130 lauten würde.

**17.6 Sperren des Zutritts für Personal**

**Dialog: Blocking (Sperrung)**

Es kann vorkommen, dass einer Person der Zutritt zeitweise verwehrt werden muss oder eine Sperre, die vom MAC beispielsweise wegen dreimaliger Falscheingabe des PIN-Codes oder einer Mitarbeiterauslösung verhängt wurde, aufgehoben werden muss.

Sperren bedeutet, dass der Zutritt für diese Person unabhängig von den verwendeten Zugangsdaten verweigert wird.

The screenshot shows the 'Blocking' dialog for a person named Anita. The interface includes a sidebar with navigation options like 'Persons', 'Companies', 'Print badges', 'Cards', 'PIN code', 'Blocking', 'Blacklist', 'Group of persons', 'Group authorizations', and 'Areas'. The main area shows personal data, a photo, and a table of card information.

Personal Data:

- Name: Musterfrau
- First name: Anita
- Birth name: [Empty]
- Personnel no.: SC41156
- Date of birth: Th 12/14/1995
- Employee ID: Employee
- Gender: Female
- Company: Test\_Firma
- Title: [Empty]
- Car license No.: Car2515132
- Card no.: 000000101234

Card Information Table:

| Card no.     | Application type | PIN lock | Created on             | Last printed on | No. of prints | Code data   |
|--------------|------------------|----------|------------------------|-----------------|---------------|---|
| 000000101234 | Personal card    |          | 10/21/2014 02:57:22 PM |                 | 0             | Customer code:150, Badge no.:101234, Version:4, Country d |

Blocking Table:

| Blocked from | Blocked until | Blocking reason | Last edited by |
|--------------|---------------|-----------------|----------------|
| [Empty]      |               |                 |                |

Buttons: Release PIN lock, New, Change, Delete

1. Wählen Sie die Person wie gewohnt aus.

2. Klicken Sie im Blockierbereich auf **New** (Neu) oder um eine Sperrung für die aktuell ausgewählte Person zu erstellen.
  3. Geben Sie zusätzliche Informationen im Popup-Dialog ein:
    - **Blocked from / until** (Gesperrt von/bis): (Wenn kein Endzeitraum angegeben ist, wird die Person gesperrt, bis die Sperrung manuell aufgehoben wird.)
    - **Block type** (Sperrtyp):
    - **Blocking reason** (Sperrgrund): (Für den Datensatz der Person, wenn der Sperrtyp `Manual` lautet)
  4. Klicken Sie auf **Save** (Speichern) im Popup, um die Sperrung zu speichern.
- Wählen Sie bei Bedarf eine Sperrung aus der Liste und klicken Sie auf **Change** (Ändern) oder **Delete** (Löschen), um sie zu ändern oder zu löschen.

Wenn **Manual lock** (Manuelle Sperrung) als Sperrtyp ausgewählt ist, geben Sie ein **Sperrgrund** für den Datensatz der Person ein.

**Hinweis!**

Die Sperrung gilt für die Person, nicht für bestimmte Zugangsdaten. Es ist daher nicht möglich, die Sperre durch die Zuweisung eines neuen Ausweises aufzuheben oder zu umgehen.

## 17.7

### Setzen von Ausweisen auf die schwarze Liste

**Dialog: Blacklist (Schwarze Liste)**

Alle Ausweise, die nie wieder verwendet werden dürfen (z. B. gestohlene oder verlorene Ausweise), werden in die schwarze Liste eingetragen.

Beachten Sie, dass der Ausweis auf der schwarzen Liste steht und nicht die Person.

**Hinweis!**

Dieser Vorgang kann nicht rückgängig gemacht werden. Ausweise, die auf der schwarzen Liste stehen, sind unwiderruflich gesperrt, sie können jedoch ersetzt werden.

Ausweise, die auf der schwarzen Liste stehen, gewähren keinen Zutritt. Die versuchte Verwendung wird sogar in der Protokolldatei aufgezeichnet, und es wird ein Alarm generiert.

Division: **Common**

Name:  First name:

Birth name:

Personnel no.:  Date of birth:

Employee ID:  Gender:

Company:  Title:

Car license No.:

Card no.:

| Card no. | Application type | PIN lock | Created on | Last printed on | No. of prints | Code data |
|----------|------------------|----------|------------|-----------------|---------------|-----------|
|          |                  |          |            |                 |               |           |

Reason:

Main menu (Hauptmenü) > **Personnel data** (Personaldaten) > **Blacklist** (Schwarze Liste)

1. Wählen Sie die Person aus, deren Ausweis in die schwarze Liste aufgenommen werden soll.
2. Wenn diesem Ausweisinhaber mehrere Ausweise zugewiesen sind, wählen Sie den Ausweis aus der Liste **Ausweisnummer** aus.
3. Geben Sie im Eingabefeld **Reason** (Grund) den Grund für die Sperre an.
4. Klicken Sie auf die Schaltfläche **Blacklist this card** (Diesen Ausweis in "Schwarze Liste" aufnehmen).
5. Bestätigen Sie den Vorgang im Popup-Fenster.

Der Ausweis wird zur schwarzen Liste hinzugefügt, und die Sperre tritt sofort in Kraft.



#### Hinweis!

Die schwarze Liste gilt für Ausweise und **nicht** für die Ausweisinhaber.

Ausweise desselben Inhabers, die sich nicht auf der schwarzen Liste befinden, werden nicht gesperrt.

## 17.8 Bearbeiten von mehreren Personen gleichzeitig

### Personengruppe

☰
🔍
⏪
?

< Main menu

Persons

Companies

Print badges

Cards

PIN code

Blocking

Blacklist

Group of persons

Group authorizations

Areas

Change division

PegaSys Stoppage card

Keys

Employee ID:

Name:

First name:

Personnel number:

Company:

Card:

Valid on:

Gender:

Department:

Cost center:

until starting with:

until starting with:

until starting with:

until starting with:

until starting with:

Number of records found: 2  Show all

| Name       | First name | Gender | Pers. number | Location | Cost unit | Job title           | Company    | Department | Card number | Time model | Valid from | Valid until |
|------------|------------|--------|--------------|----------|-----------|---------------------|------------|------------|-------------|------------|------------|-------------|
| Musterfrau | Anja       | Female | SC41156      |          |           |                     | Test_Firma |            |             |            |            |             |
| Mustermann | Max        | Male   | Sc999000     |          |           | Software-Entwickler | Test_Firma |            |             |            |            |             |

Wanted field to change:

Wanted action:

In einem weiteren Dialog wird eine Personengruppe ausgewählt, für die Gruppenänderungen definiert werden können. Zur besseren Administration der ausgewählten Personengruppe werden die ersten zehn Personen namentlich aufgeführt. Die Datenbank setzt sich zudem aus Echtdaten zusammen. (Echtdaten: Bei Auswahl von „ST-AC“ als Abteilung werden „ST-ACS“ und „ST-ACX“ angezeigt.) Darüber hinaus wird angezeigt, wie viele Personen die ausgewählte Gruppe umfasst.

Nachdem die Personengruppe ausgewählt wurde, können Sie die folgenden Einträge auswählen:

- Employee ID (Personalkennung)
- Name
- First name (Vorname)
- Personnel number (Personalnummer)
- Company (Unternehmen)
- Card (Ausweis)
- Valid on (Gültig am)
- Gender (Geschlecht)
- Department (Abteilung)
- Kostenstelle
- Reservefelder, sofern definiert

Dann kann die Änderungsoption ausgewählt werden:

- Feld, welches geändert werden soll
- Gewünschte Aktion

- Alter Wert
- New value (Neuer Wert)

In die Felder **Old value** (Alter Wert) und **New value** (Neuer Wert) können die gewünschten Werte eingegeben werden. Die Aktion wird durch Klicken auf die Schaltfläche **Apply changes** (Änderungen ausführen) und Bestätigen des Sicherheitshinweises **apply changes for all selected persons?** (Änderungen für alle ausgewählten Personen ausführen?) abgeschlossen. Der Dialog kann während der Ausführung der Aktion nicht anderweitig verwendet werden. Die über die Felder \*1 bis \*4 ausgelösten Aktionen sind wahrscheinlich zeitaufwendiger als Aktionen, die über die anderen Felder (ohne Stern) ausgelöst werden. Im Übrigen sind nicht alle Änderungen zulässig. Beispielsweise kann **Desired action** (Gewünschte Aktion) nicht mit **New value** (Neuer Wert) kombiniert werden, da diese Eingaben vom Standardprodukt nicht abgedeckt werden. Die Felder **Old value** (Alter Wert) und **New value** (Neuer Wert) können auch entsprechend variieren.

### Gruppenberechtigungen

The screenshot shows the 'Group Authorizations' configuration page. On the left is a navigation menu with icons for 'Persons', 'Companies', 'Print badges', 'Cards', 'PIN code', 'Blocking', 'Blacklist', 'Group of persons', 'Group authorizations', and 'Areas'. The main content area has a search bar with 'Employee ID' set to 'Employee'. Below are various search criteria: Name, First name, Personnel number, Company, Card, Valid on, Gender, Department, and Cost center. Each criterion has a corresponding 'until starting with' field. At the bottom, there are two tables. The first table, 'Group authorizations', shows 2 selected persons: Musterfrau Anja (Personnel no. SC41156) and Mustermann Max (Personnel no. Sc999000). The second table, 'Authorizations', has columns for Assign, Withdraw, Name, MAC, Time model, and Division, with a filter set to '1'.

Im Menüelement **[Group Authorization]** (Gruppenberechtigungen) werden die folgenden Suchkriterien unterstützt:

- Employee ID (Personalkennung)
- Name
- First name (Vorname)
- Personnel number (Personalnummer)
- Company (Unternehmen)
- Card (Ausweis)
- Valid on (Gültig am)
- Gender (Geschlecht)
- Department (Abteilung)
- Kostenstelle
- Reservfelder, sofern definiert

Im unteren Bereich des Dialogs wird dann eine Liste aller ausgewählten Personen (mit Name, Vorname und Personalnummer) angezeigt. Unten rechts wird eine Liste aller Berechtigungen angezeigt. Die Liste enthält für jede Berechtigung eine Beschreibung, das Zeitmodell sowie die Spalten **[Assign]** (Erteilen) und **[Withdraw]** (Entziehen). Wenn die Berechtigungsliste geöffnet wird, werden keine der aktuellen Berechtigungen angezeigt. Die Spalten **[Assign]** (Erteilen) und **[Withdraw]** (Entziehen) enthalten jeweils den Standardeintrag "Nein". Die einzelnen Berechtigungen können nun zugewiesen werden. Durch einen Doppelklick in einer der Spalten wird der entsprechende Eintrag „No“ (Nein) in den Eintrag „Yes“ (Ja) verwandelt oder umgekehrt. Durch das Klicken auf „Execute changes“ (Änderungen ausführen) werden alle Berechtigungen mit dem Eintrag „Yes“ (Ja) allen ausgewählten Personen erteilt bzw. entzogen. Alle anderen Berechtigungen der Personen bleiben unverändert, denn die ausgewählten Personen haben in der Regel nicht vollkommen identische Berechtigungen.

# 18 Definieren von Zutrittsberechtigungen und Profilen

## 18.1 Erstellen von Zutrittsberechtigungen


### Dialogpfad

Main menu (Hauptmenü) > **System data** (Systemdaten) > **Authorizations** (Berechtigungen)

### Vorgehensweise

1. Klicken Sie in der Symbolleiste auf **New** (Neu) , um den Inhalt der Eingabefelder zu löschen.

Alternativ klicken Sie auf **Copy** (Kopieren) , um eine neue Berechtigung basierend auf einer bestehenden zu erstellen.

2. Geben Sie einen eindeutigen Namen für die Berechtigung ein.
3. (Optional) Geben Sie eine Beschreibung ein
4. (Optional) Wählen Sie ein Zeitmodell, um diese Berechtigung zu regeln
5. (Optional) Wählen Sie ein **Inactivity limit** (Inaktivitätslimit) aus der Liste.  
Dies ist eine Zeitperiode zwischen 14 und 365 Tagen. Wenn eine Person, die diese Berechtigung zuweist, dies nicht innerhalb der festgelegten Frist tut, verliert sie diese. Jedes Mal, wenn die zuweisende Person die Berechtigung verwendet, wird die Zeitschaltuhr von Null an neu gestartet.
6. (Obligatorisch) Weisen Sie mindestens einen **Durchtritt** zu.  
Die vorhandenen Durchtritte sind je nach Türmodell auf verschiedenen Registerkarten aufgeführt.  
(Generisch) **Entrance** (Durchtritt), **Time management** (Zeitwirtschaft), **Elevator** (Aufzug), **Parking lot** (Parkplatz), **Arming Intrusion detection** (Einbruchmeldeanlage scharfschalten).  
Wählen Sie einzelne Durchtritte aus den Listen auf den verschiedenen Registerkarten aus, wie nachfolgend beschrieben.  
Verwenden Sie alternativ die Schaltflächen **Assign all** (Alle zuweisen) und **Remove all** (Alle entfernen) auf jeder Registerkarte.
  - Wählen Sie auf der Registerkarte **Entrance** (Durchtritt) einen Durchtritt aus, indem Sie eines oder beide Kontrollkästchen für **In** (Hinein) oder **Out** (Hinaus) auswählen.
  - Wählen Sie auf der Registerkarte **Time management** (Zeitwirtschaft) (für Zeit- und Anwesenheitsleser) eines oder beide Kontrollkästchen für **In** (Hinein) oder **Out** (Hinaus) aus.
  - Wählen Sie auf der Registerkarte **Elevator** (Aufzug) die verschiedenen Stockwerke aus.
  - auf der Registerkarte **Parking lot** (Parkplatz) durch Auswählen eines Parkplatzes und einer Parkzone
  - auf der Registerkarte **Arming Intrusion detection** (Einbruchmeldeanlage scharfschalten) durch Auswählen von **Armed** (Scharf) oder **Disarmed** (Unscharf).
7. Wählen Sie den gewünschten MAC in der Liste aus.
8. Klicken Sie auf "Save" (Speichern) , um die Berechtigung zu speichern.



### Hinweis!

Nachfolgende Änderungen an Berechtigungen wirken sich auf vorhandene zuweisende Personen aus, es sei denn, das verantwortliche Profil ist gesperrt.

**Beispiel:** Wenn ein Inaktivitätslimit von 60 Tagen auf 14 Tage reduziert wird, geht die Berechtigung für alle Personen verloren, die diese in den letzten 14 Tagen nicht genutzt haben.

**Ausnahme:** Wenn eine Berechtigung Teil eines Zugriffsprofils ist, das für eine Mitarbeiter-ID (Personentyp) **gesperrt** ist, sind Personen dieses Typs von Inaktivitätslimits für die Berechtigung nicht betroffen. Profilsperren können mit dem folgenden Kontrollkästchen gesetzt werden.

Main menu (Hauptmenü) > **System data** (Systemdaten) > **Person Types** (Personentypen) > Tabelle: **Predefined Employee IDs** (Vordefinierte Personalkennungen) > Kontrollkästchen: **Profile locked** (Gesperrtes Profil)

## 18.2

### Erstellen von Zutrittsprofilen

#### Hinweis: Verwenden von Zugriffsprofilen zum Bündeln von Berechtigungen





Aus Gründen der Einheitlichkeit und Bequemlichkeit werden Zutrittsberechtigungen nicht einzeln zugewiesen, sondern typischerweise gebündelt in **Zugriffsprofile** und als solche zugewiesen.

- Hauptmenü: > **System data (Systemdaten)** > **Access profiles** (Zugriffsprofile)


#### Voraussetzungen

Zutrittsberechtigungen wurden bereits im System definiert.

#### Vorgehensweise

1. Klicken Sie in der Symbolleiste auf **New** (Neu) , um den Inhalt der Eingabefelder zu löschen.  
  
Alternativ klicken Sie auf **Copy** (Kopieren) , um ein neues Profil basierend auf einem bestehenden zu erstellen.
2. Geben Sie einen eindeutigen Namen für das Profil ein.
3. (Optional) Geben Sie eine Beschreibung ein
4. (Optional) Aktivieren Sie das Kontrollkästchen **Visitor profile** (Besucherprofil), um dieses Profil auf Besucher zu beschränken.
5. (Optional) Legen Sie einen Wert für **Standard duration of validity** (Standardgültigkeitsdauer) fest.
  - Wenn kein Wert festgelegt ist, wird das Profil unbegrenzt zugewiesen.
  - Wenn ein Wert festgelegt ist, wird damit das Ablaufdatum einer späteren Zuweisung des Profils berechnet.
6. (Obligatorisch) Weisen Sie mindestens eine **Berechtigung** zu:  
Berechtigungen, die für die Zuweisung verfügbar sind, sind auf der rechten Seite aufgeführt.  
Berechtigungen, die bereits vergeben sind, sind auf der linken Seite aufgelistet.  
Wählen Sie Elemente aus und klicken Sie dann auf die Schaltflächen zwischen den Listen, um Elemente von einer Liste in die andere zu verschieben.
  -  weist das ausgewählte Element zu.
  -  hebt die Zuweisung des ausgewählten Elements auf.



7. Klicken Sie auf "Save" (Speichern)  , um das Profil zu speichern.

## 19 Verwalten von Besuchern

Besucher haben im Zutrittskontrollsystem einen besonderen Status und werden von anderen Personaldaten getrennt aufbewahrt. Aus diesem Grund werden Besucherdaten in separaten Dialogen erstellt und gepflegt.

### 19.1 Besucherdaten

#### Einführung

Das System unterstützt eine schnelle und einfache Administration von Besucherdaten. Somit ist es möglich, die Daten für bereits bekannte Besucher schon im Vorfeld einzugeben und auch die Zutrittsberechtigungen festzulegen. Wenn der Besucher ankommt, muss nur der Ausweis zugewiesen werden. Wenn der Ausweis am Ende des Besuchs zurückgegeben wird, wird die Verbindung zwischen Ausweis und Person wieder gelöscht, und die Berechtigungen werden automatisch entzogen.

Sollten die Besucherdaten nicht vom Benutzer gelöscht werden, werden sie nach Ablauf des konfigurierten Zeitraums (Standardwert: 6 Monate) nach der letzten Ausweiserückgabe vom System gelöscht.

Für die Administration externer Besucher gibt es zwei Dialoge.

- Der Dialog **Visitors** (Besucher) dient zur Eingabe der Daten und Zutrittsberechtigungen der Besucher.
- Im Dialog **Visitor cards** (Besucherausweise) werden die Registrierung und die Löschung von Besucherausweisen geregelt.

#### Dialog: Visitors (Besucher)

Besucher haben einen von den übrigen Personen streng getrennten Status und werden deshalb auch in einem separaten Dialog bearbeitet. Es ist im Dialog **Personen** nicht möglich, Personen mit der Kennung **Besucher** zu erstellen oder für diese Besucher Ausweise zu erfassen.

Im Dialog **Visitors** (Besucher) fehlt unter anderem das Eingabefeld **Personalkennung**. Da es eine separate Datenbanktabelle für Besucher gibt, erhalten die im hier beschriebenen Dialog erstellten Personen automatisch die Kennung „Besucher“. Dies bedeutet, dass hier ausschließlich Besucher erstellt werden können. Eine in diesem Dialog vorgenommene Auswahl ist daher auf die entsprechende Datenbanktabelle beschränkt. Alle im System registrierten Personen können hingegen in den anderen Personaldatendialogen zwar ausgewählt, aber gegebenenfalls nicht für Besucher verwendet werden (Dialog **Ausweise**). Sofern bekannt, können Besucherdaten vor der Ankunft des Besuchers ganz oder zum Teil im System eingegeben werden. Hierdurch verkürzt sich die Wartezeit für Besucher, deren Daten bereits erfasst wurden, auf ein Minimum.

Division: Common

Last name:  First name:

Birth name:  Date of birth:

Street, no.:  Zip code / City:

Phone:

Car license No.:

Employee ID: Visitor Company:

Official pass

Passport

Driver's licence

Identity card

Other:

Number:

Card no.:  Reader.. ▶

Additional data

Authorizations
Form/Photo
Signature

Attendant:  ... Reason:

Remark:

Expected arrival:  Expected departure:

Date of arrival:  Date of departure:

Visited person:  ...  Extended door opening time

Location:

| Card no. | Application type | PIN lock | Collecting date | Code data |
|----------|------------------|----------|-----------------|-----------|
|          |                  |          |                 |           |

Read card ... ▶  
Withdraw card

Der **Reason** (Grund) des Besuches, der besuchte **Location** (Ort) und eine **Remark** (Bemerkung) können in die unten stehenden Eingabefelder eingegeben werden. Wenn Sie Daten in die Felder **Erwartete Ankunft** und **Erwartete Abreise** eingeben, werden die Daten in die Felder **Gültig von** und **bis** übertragen. In die Felder **Ankunftsdatum** und **Tag der Abreise** werden vom System die entsprechenden Daten eingetragen, wenn Besucherdaten einem Besucherausweis zugewiesen bzw. davon getrennt werden. Wie auch im Dialog **Cards** (Ausweise) ist es möglich, eine verlängerte Türöffnungszeit zuzuweisen, um z. B. behinderten Personen den Zutritt zu erleichtern.

Im Dialog **Assign authorization** (Berechtigung zuweisen) kann ein vorhandenes Benutzerprofil in der Profilliste ausgewählt werden. Es können auch einzelne Zutrittsberechtigungen in der Liste **Available access authorization** (Verfügbare Zutrittsberechtigungen) markiert und in die links stehende Liste **Assigned access authorization** (Zugewiesene Zutrittsberechtigung) übertragen werden, wo sie dann ausgewählt werden können.

Nur Zutrittsprofile, die als Besucherprofile markiert sind, können in diesem Dialog ausgewählt werden. Damit soll verhindert werden, dass Besucher durch die Zuweisung allgemeiner Berechtigungen Zutritt zu Sonderbereichen erhalten.

Die Prüfung der Zutrittsberechtigungen kann auch für jede Berechtigung einzeln erfolgen. Wenn beim Lesen des Ausweises ein Fehler auftritt, kann die Ausweisnummer auch manuell angegeben werden. Gleichzeitig wird das aktuelle Datum als Tag der Ankunft gespeichert. Am Ende des Besuchs gibt der Besucher seinen Ausweis ab. Beim Lesen des Ausweises im Ausweisleser bzw. bei der manuellen Eingabe der Ausweisnummer wird die entsprechende Person ausgewählt, und ihre Daten werden auf dem Bildschirm angezeigt.

Der Bediener bestätigt die Rückgabe des Ausweises. Die Verknüpfung zwischen Ausweis und Besucher wird durch Klicken auf die Schaltfläche **Confiscate card** (Ausweis einziehen) entfernt. Gleichzeitig werden das Datum und die Uhrzeit dieser Aktion als Tag der Abreise gespeichert.

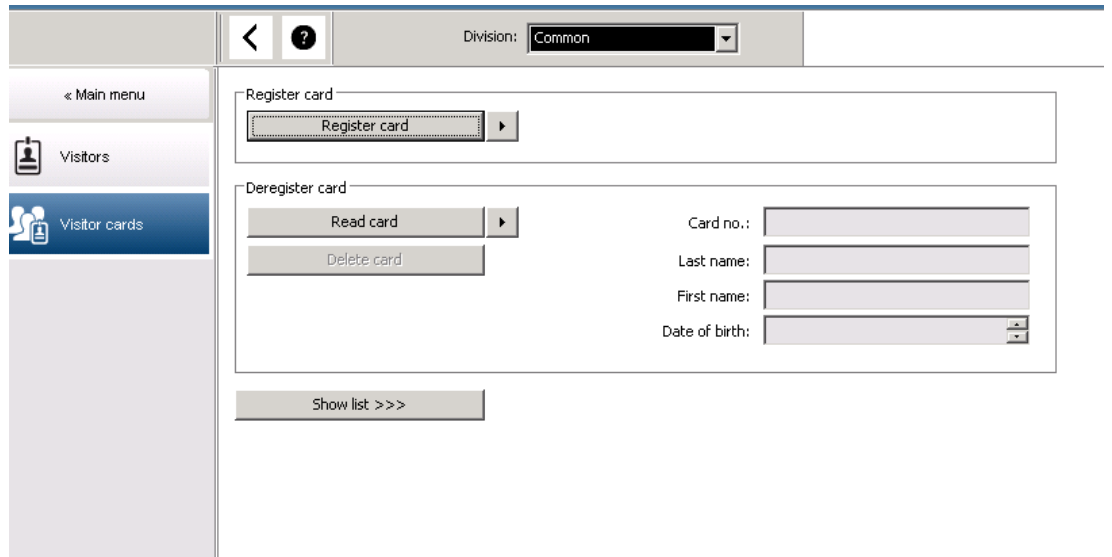
#### Dialog: Visitor Cards (Besucherausweise)

Einige Ausweise im System werden als Besucherausweise reserviert. Normalerweise wird einem ankommenden Besucher ein Besucherausweis zugewiesen. Er wird wieder zurückgegeben, wenn der Besucher das Gelände verlässt. Der Ausweis kann anschließend wiederverwendet werden. Einige Ausweise können in diesem Dialog als Besucherausweise registriert werden, bevor sie Besuchern zugewiesen werden können:



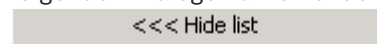
#### Hinweis!

Im Allgemeinen werden Besucherausweise ohne Namen oder Foto erstellt, damit sie wiederverwendet werden können.



Klicken Sie auf die Schaltfläche **Register ID card** (Ausweis registrieren), um die Registrierung durchzuführen.

Anhand des bereits beschriebenen Eingabeverfahrens (siehe Kapitel **Personaldaten**, Abschnitte **Personen** und **Ausweise**) und der Ausweisnummer wird der Ausweis ermittelt. Dies gestattet es dem System, den Ausweis als Besucherausweis zu erkennen und in den folgenden Dialogen anzuwenden.



| Card no. | In use | Name | First name | Usage type | Division |  |
|----------|--------|------|------------|------------|----------|--|
|          |        |      |            |            |          |  |

Um die Zuweisung von Besucherausweisen zu beschleunigen, empfiehlt es sich, alle vorhandenen Ausweise zu scannen, damit diese Ausweise den gewünschten Besuchern im nächsten Dialog zugewiesen werden können.

Am Ende des Besuchs gibt der Besucher seinen Ausweis zurück. Durch Scannen des Ausweises an einem Dialogleser oder durch die manuelle Eingabe der Ausweisnummer wird die dem Ausweis zugewiesene Person ausgewählt, und die Daten dieser Person werden auf dem Bildschirm angezeigt. [Weitere Informationen zur manuellen Eingabe der Ausweisnummer und zum Umschalten zu Lesern siehe **Dialog: Ausweise** und **Dialog: Visitors (Besucher)**.] Der

Benutzer bestätigt die Rückgabe des Ausweises. Die Verbindung zwischen Ausweis und Personaldaten des Besuchers wird über die Schaltfläche entfernt. Das aktuelle Datum wird als Tag der Abreise gespeichert.

#### **Drucken eines Besucherformulars**



Die Symbolleiste im Dialog **Visitors** (Besucher) enthält eine zusätzliche Schaltfläche zum Drucken eines Besucherzertifikats. Die Person, die den Besucher empfängt, kann anhand des Besucherzertifikats beispielsweise bestätigen, wann der Besucher ankam und wieder ging.

### Visitor pass

|  |   |
|--|---|
| Entry  | Exit  |
| First- and lastname<br>Steven Visitor  |   |
| Company<br>_____   |   |
| <input type="checkbox"/> Proof of authority for plant area   | Registration plate<br>_____   |
| Passed card  |   |
| Contact person   | Phone   |
| Department   |   |
| Reason of visit  | Visit appointment<br><input type="checkbox"/> Yes <input type="checkbox"/> No   |
| Type of official<br>Passport   | Number of official document   |
| I accept the terms and conditions overleaf<br><br><div style="display: flex; justify-content: space-between;"> <span>_____ Location, date</span> <span>_____ Sign of visitor</span> </div> |   |
| Identity card with photo seen ?<br><input type="checkbox"/> Yes <input type="checkbox"/> No<br><br>_____<br>Sign of plant protective force   | To complete from visited person<br><br>Arrival at _____<br>Departure at _____<br><br>_____<br>To sign on visited person |

## 19.2 Besucher zu spät

Die Anzeige **Besucher zu spät** (Visitor too late) ermöglicht dem Kunden die Überprüfung, wo sich Besucher aufhalten und ob sie möglicherweise die Aufenthaltszeit überschritten haben. Autorisierte BIS-Benutzer benötigen einen konfigurierten Link auf ihrem Startbildschirm, um die Webseite anzeigen zu können.

Zusätzlich ein Trigger kann im BIS zum DMS-Gerät konfiguriert werden, über den im Falle einer Verspätung ein Alarm aktiviert wird, der die Webseite öffnet und die betreffende Person mit ihren letzten Aufenthaltsorten anzeigt.

[Siehe Bild der Webseite]

#### **Ereignisse, die zur Meldung "Visitor too late" (Besucher zu spät) führen:**

Wenn einem Besucher ein Ausweis zugewiesen wird, muss die voraussichtliche Abreisezeit vom Bediener eingetragen werden. Am Ende des Besuchs gibt der Besucher den Ausweis am Empfang zurück, wo er von einem Bediener gelöscht wird.

Alternativ kann ein motorisierter Einzug als Ausgangsleser für Besucher verwendet und so konfiguriert werden, dass die Besucher den Ausweis behalten können, wenn sie das Gelände verlassen.

Wenn ein Besucher den Ausweis nicht vor der vereinbarten Abreisezeit zurückgibt, wird die Meldung **Visitor too late** (Besucher zu spät) vom System erstellt, unabhängig davon, ob sich der Besucher noch auf dem Gelände befindet.

Diese Prüfung nach überfälligen Ausweiserückgaben wird in regelmäßigen Intervallen (z. B. jede Minute) durchgeführt. Die Meldung **Visitor too late** (Besucher zu spät) wird bei jeder Prüfung erstellt, bis der Ausweis zurückgegeben wird. Das Zeitintervall kann im Registry des Servers unter `HKLM\Software\Micos\SPS\Default\VLDP\Interval` konfiguriert werden.



#### **Hinweis!**

Das Erstellen dieser Meldung kann im Registry des Servers unter `HKLM\Software\Micos\SPS\Default\VLDP\Active` deaktiviert werden.

Durch diese Funktion kann jede Person, die den angegebenen Ansprechpartner nicht kontaktiert oder sich an der Rezeption bzw. am Ausgang nicht im festgelegten Zeitrahmen zurückgemeldet hat, ermittelt werden.

Dabei wird Folgendes kontrolliert:

- Was war der letzte betretene Bereich für die Gebäudezutrittskennzeichnung eines Besuchers.
- Hat der Besucher die Gebäudezutrittskennzeichnung zurückgegeben.
- Hat der Besucher die Fahrzeugzutrittskennzeichnung zurückgegeben (falls zutreffend).

Eine **Visitor too late (Besucher zu spät)** und **Vehicle too late (Fahrzeug zu spät)**-Meldung wird ausgelöst.

Der aktuelle Aufenthaltsort der Kennzeichnung kann in die Meldung aufgenommen werden. Der Status des Besuchers wird auf der Webseite mit farblichen Kennzeichnungen wie folgt versehen:

- **Grün:** Besucher hat alle Ausweise zurückgegeben.
- **Gelb:** Besuch noch nicht beendet, Zeit noch nicht abgelaufen..
- **Rot:** Besuch noch nicht beendet, aber Zeit abgelaufen. Das bedeutet **Besucher zu spät**.



|              |                                  |      |                         |      |               |           |            |
|--------------|----------------------------------|------|-------------------------|------|---------------|-----------|------------|
| Fritz        | Mustermann                       | Arr. | 15.07.2014 08:21:00'000 | Dep. | 10:22:00 exp. | Vehicle   |            |
|              | over 1 d/23h 58'31               | Dur. | 1 d/23h 59'31           |      |               | Last area | Zone A     |
| Test Visitor | Test Visitor                     | Arr. | 16.07.2014 14:55:00'000 | Dep. | 09:04:54      | Vehicle   |            |
|              | departed 15h 04'54<br>16.07.2014 | Dur. | 16h 09'54               |      |               | Last area | AUSSEN     |
| Malmendier   | Walter                           | Arr. | 16.07.2014 14:52:00'000 | Dep. | 00:00:00 exp. | Vehicle   | AC-WM-1234 |
|              | over 10h 20'31                   | Dur. | 17h 28'31               |      |               | Last area |            |
| Cibis        | Roman                            | Arr. | 16.07.2014 14:53:00'000 | Dep. | 02:00:00 exp. | Vehicle   | AC-CC-1010 |
|              | over 8h 20'31                    | Dur. | 17h 27'31               |      |               | Last area |            |
| Nettelbeck   | Ulrike                           | Arr. | 17.07.2014 07:39:00'000 | Dep. | 00:00:00 exp. | Vehicle   | AC-UN-4646 |
|              | still 13h 39'28                  | Dur. | 41'31                   |      |               | Last area |            |

Die Seite wird automatisch alle 30 Sekunden aktualisiert. Diese Aktualisierungszeit kann auf der Webseite konfiguriert werden. Zusätzlich kann der Bediener filtern auf **Show returned** (Alle zurückgegebenen), **Too late only** (Nur verspätete) sowie **Vehicle search** (Fahrzeugsuche).

## 20

### 20.1

## Verwalten von Parkplätzen

### Berechtigungen für mehrere Parkzonen

Auf einigen Parkplätzen gibt es Zonen für behinderte und solche für nicht behinderte Fahrer. In diesem Fall gelten folgende Regeln:

- Inhaber von Dauertickets dürfen nur einfahren, solange noch Parkplätze für nicht behinderte Personen frei sind.
- Behinderte Personen dürfen einfahren, solange noch Parkplätze für behinderte oder nicht behinderte Personen frei sind.



#### Hinweis!

Dies setzt voraus, dass sich die Ticketinhaber an die Regeln halten. Dies bedeutet insbesondere:

Nicht behinderte Personen parken nicht auf einem Behindertenparkplatz.

Behinderte Personen benutzen Behindertenparkplätze, solange solche frei sind.

Eine Person, die mehrere Berechtigungen besitzt, hat Zutritt in beide Zonen, ob behindert oder nicht. Der AMC versucht, die Person entsprechend der konfigurierten Reihenfolge der Parkzonen einzubuchen. Falls eine Zone voll ist, wird die Suche bei der nächsten autorisierten und freien Parkzone fortgesetzt.

Zählerberechnung in MAC und AMC:

1) Ein AMC steuert alle Ein- und Ausfahrten des Parkplatzes:

=> Der AMC zählt selbst und kann bei Online-Verbindung durch den MAC korrigiert werden.

2) Ein- und Ausfahrten eines Parkplatzes sind auf verschiedene AMCs aufgeteilt:

=> Der MAC zählt bei Online-Betrieb für den AMC. Bei Offline-Betrieb gewähren die AMCs den Zutritt (bei entsprechender Konfiguration), führen aber keine Zählung durch.

Wenn mehrere AMCs einen Parkplatz kontrollieren, aktivieren Sie das Kontrollkästchen **No AMC accounting** (Keine Zählung durch den AMC) in der AMC-Konfiguration.

AMC 4-W | Inputs | Outputs | Terminals

Name: AMC 4-W-1

Description: AMC

Communication to host enabled:

Controller interface

Interface type: UDP

PC com port: 0

Bus number: 1

IP address / host name:

Port number: 10001

Program: LCMV3732.RUN : WIE, AMC-4W

Power supply supervision:

No LAC accounting:

Division: Common

## 20.2 Übersicht über den Parkplatz

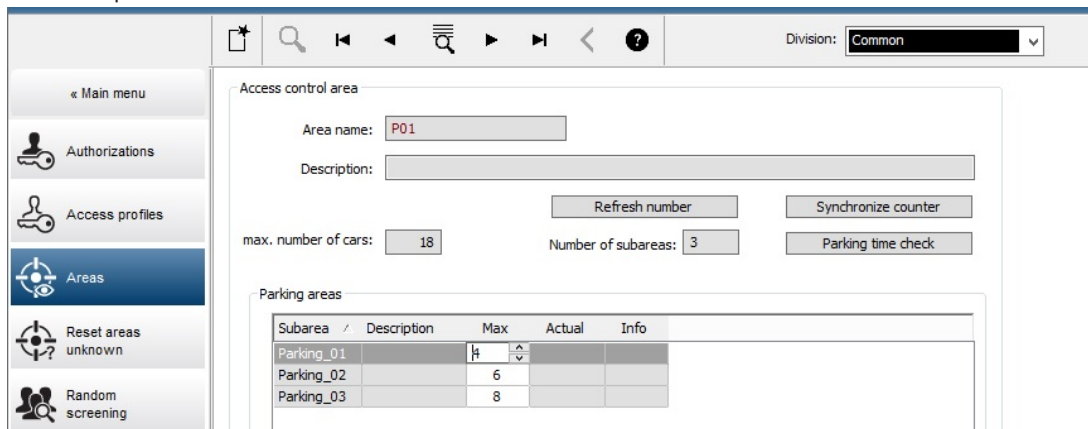
| Parking lot list  |        |               |       |
|-------------------|--------|---------------|-------|
| Parking area      | Zone   | Vehicle count | State |
| <b>Main Park</b>  |        | 51            |       |
|                   | Zone A | 30            | full  |
|                   | Zone B | 9             | --    |
|                   | Zone C | 12            | --    |
| <b>Building A</b> |        | 39            |       |
|                   | Zone A | 30            | full  |
|                   | Zone B | 9             | --    |
| <b>Building B</b> |        | 39            |       |
|                   | Zone A | 30            | full  |
|                   | Zone B | 9             | --    |

## 20.3 Erweitertes Parkplatzmanagement

Der Bediener kann die Anzahl der Parkplätze in einem Parkbereich anpassen, um einen Ausgleich für Fahrzeuge von nicht standardmäßiger Größe zu schaffen, zum Beispiel:

- LKW
- Behindertengerechter Zugang

- Motorräder
- 1. Wählen Sie einen Parkplatz aus.
- 2. Passen Sie im Bereich **Parkbereiche** den Wert in Spalte **Max** auf die neue Anzahl von Parkplätzen für diesen Bereich an.



Hauptmenü > Systemdaten > Bereiche

## 21

# Verwalten von Wächterrunden und Wächterkontrollgängen

### Einführung in Wächterrunden

Eine **Wächterrunde** ist eine von Ausweislesern vorgegebene Route auf dem Gelände. Personen vom Mitarbeitertyp **Guard** (Wächter) müssen einen speziellen Wächterausweis vorlegen, um nachzuweisen, dass sie persönlich am Leser waren.

Mit Wächterausweisen werden keine Eingänge geöffnet, sie dienen lediglich der Kontrolle. Für das Öffnen von Eingängen benötigt der Wächter zusätzlich einen Zutrittsausweis.

Die Wächterrunde besteht aus einer Reihe von Lesern mit einer ungefähren Zeitangabe für die Dauer zwischen den Lesern. Ebenso werden der Wächterrunde Toleranzgrenzen für Verspätungen zwischen den einzelnen Lesern und für Abweichungen (+/-) ab der Startzeit zugewiesen. Abweichungen außerhalb dieser definierten Toleranzen können potenziell einen Alarm auslösen und werden unter **Patrols** (Wächterkontrollgänge) aufgezeichnet.

### Einführung in Wächterkontrollgänge

Ein **Patrol** (Wächterkontrollgang) ist das Durchkreuzen einer Wächterrunde an einem bestimmten Datum zu einem bestimmten Zeitpunkt. Jeder Wächterkontrollgang wird im System für forensische Zwecke als einzigartige Entität angelegt und aufgezeichnet.

## 21.1

### Definieren von Wächterrunden

Wählen Sie **Guard tours** (Wächterrunden) > **Define guard tours** (Wächterrunden definieren)

The screenshot shows the 'Define guard tour' interface. The 'Name' field contains 'Building 1 perimeter' and the 'Description' field contains 'A route around the perimeter of Building 1'. Below the form is a table with the following data:

| No. | Description of reader | Time on the way | Total time | Max. delay | Startzeit +/- |
|-----|-----------------------|-----------------|------------|------------|---------------|
| 1   | BPR HI-1: BPR HI      | 00:00:00        | 00:00:00   | 00:00:00   | 3 min         |
| 2   | BPR HI-2: BPR HI      | 00:10:00        | 00:10:00   | 00:02:00   |               |
| 3   | BPR HI-1: BPR HI      | 00:10:00        | 00:20:00   | 00:05:00   |               |

Buttons for 'Add reader' and 'Delete reader' are visible below the table.

- Geben Sie im Textfeld **Name** einen Namen für die Wächterrunde ein.
- Geben Sie im Textfeld **Description** (Beschreibung) eine detailliertere Beschreibung der Route ein (optional).

### Hinzufügen von Lesern zur Wächterrunde:

1. Klicken Sie auf die Schaltfläche **Add reader** (Leser hinzufügen). In der Tabelle wird eine Linie erstellt.
2. Wählen Sie in der Spalte **Description of reader** (Leser-Bezeichnung) aus der Dropdown-Liste einen Leser aus.
3. Geben Sie Werte für tolerierbare Abweichungen ein:
  - Handelt es sich um den ersten Leser in der Abfolge, geben Sie unter **Start time +/-** (Startzeit +/-) die Anzahl der Minuten ein, in deren Rahmen ein verspäteter oder verfrühter Start eines Wächterkontrollgangs bei dieser Wächterrunde tolerierbar wäre.

- Handelt es sich **nicht** um den ersten Leser in der Abfolge, geben Sie unter **Time on the way** (Zeit unterwegs) die erforderliche Zeit (hh:mm:ss) für den Gang des Wächters vom vorherigen zu diesem Leser ein.  
Die Gesamtzeit der Runde – ohne Verzögerungen – wird in der Spalte **Total time** (Gesamtzeit) zusammengefasst.
- 4. Geben Sie unter **Max. delay** (Max. Verzögerung) die maximale zusätzliche **Time on the way** (Zeit unterwegs) ein, die toleriert wird, ohne dass ein Wächterkontrollgang als **Delayed** (Verspätet) gekennzeichnet wird.
- 5. Fügen Sie die erforderliche Anzahl an Lesern hinzu. Mehrfachnennungen desselben Lesers sind möglich, wenn die Wächterrunde mehrmals an einem Leser vorbeiführt oder zu ihm zurückkehrt.
- Um einen Leser aus der Abfolge zu löschen, wählen Sie die Zeile aus, und klicken Sie auf die Schaltfläche **Delete reader** (Leser löschen).
- Um die Reihenfolge zu ändern, klicken Sie auf die Zeile eines bestimmten Lesers und verschieben Sie ihn mithilfe der  
 und  per Klick nach oben oder unten.

## 21.2

### Verwalten von Wächterkontrollgängen

Wählen Sie **Guard tours** (Wächtertouren) > **Manage guard tours** (Wächtertouren verwalten)

#### Planen eines neuen Wächterkontrollgangs

Gehen Sie folgendermaßen vor, um einen Wächterkontrollgang für eine bestimmte Wächterrunde festzulegen:


1. Stellen Sie sicher, dass Sie den gewünschten Wächterausweis für den Kontrollgang besitzen. Zudem müssen Sie Zugriff auf einen konfigurierten Zutrittsausweisleser oder einem direkt verbundenen Bekanntmachungsleser haben.
2. Wählen Sie in der Spalte **Guard tours** (Wächterrunden) eine der definierten Wächterrunden aus.
3. Klicken Sie auf die Schaltfläche **New patrol...** (Neuer Wächterkontrollgang...). Ein Popup-Fenster wird geöffnet.
4. Ändern Sie in diesem Fenster bei Bedarf in der Dropdown-Liste die Wächterrunde.
5. Falls es für den Wächterkontrollgang eine vorab festgelegte Startzeit geben soll, aktivieren Sie das Kontrollkästchen **Set start time** (Startzeit einstellen):
  - Geben Sie das Startdatum und die Startuhrzeit ein.
  - Klicken Sie bei Bedarf auf das Drehfeld **Start time +/-** (Startzeitbereich +/-), um die Toleranzgrenze für verspätete oder verfrühte Starts festzulegen.
6. Klicken Sie auf den rechten Pfeil, und wählen Sie den Leser aus, der für die Registrierung des Wächterausweises verwendet werden soll. Der Leser muss bereits im System konfiguriert sein, bevor er hier ausgewählt werden kann.
7. Klicken Sie auf die Schaltfläche mit dem grünen Pluszeichen, um das Lesen des Wächterausweises zu starten. Zeigen Sie den Ausweis am Leser, und befolgen Sie die angezeigten Anweisungen.  
Dadurch wird der Wächterausweis für die Verwendung im Wächterkontrollgang erfasst.
8. Wiederholen Sie den vorherigen Schritt, um weitere Wächterausweise für diesen Wächterkontrollgang zu erfassen. Es ist jedoch unbedingt erforderlich, dass der erste Ausweis, der auf einem Kontrollgang eingelesen wird, mit dem identisch ist, der an allen weiteren Lesern dieses Kontrollgangs verwendet wird.


9. Klicken Sie auf **OK**. Die ausgewählte Wächterrunde wird in der Liste als **planned** (Geplant) markiert.


### Verfolgen eines Wächterkontrollgangs

Alle geplanten und aktiven Wächterkontrollgänge werden in den oberen Bereich der Liste verschoben. Falls mehrere Kontrollgänge geplant oder aktiv sind, ist der ausgewählte Kontrollgang rot markiert. Klicken Sie auf den Rahmen, um weitere Informationen zu erhalten. Der Beginn eines Wächterkontrollgangs wird durch das Vorlegen des Wächterausweises am ersten Leser der Wächterrunde gekennzeichnet. Dieser Ausweis muss für den Rest des Kontrollgangs verwendet werden, selbst wenn weitere Ausweise für den Kontrollgang definiert wurden.

Der **State** (Status) des Wächterkontrollgangs ändert sich in **Active** (Aktiv).

Jeder Leser, der im festgelegten Zeitrahmen erreicht wird, erhält ein grünes Häkchen: . Die geplante und die tatsächliche Dauer zwischen den Lesern des aktuell ausgewählten Wächterkontrollgangs werden in der unteren Hälfte des Dialogfensters angezeigt.

Jeder Leser, der später als die festgelegte Zeit plus **Max. delay** (Max. Verzögerung) erreicht wird, wird rot mit  gekennzeichnet. Der Wächterkontrollgang ist als **Delayed** (Verspätet) markiert.

In diesem Fall ruft der Wächter den Bediener an, um die Bestätigung zu erhalten, dass kein Problem vorliegt. Der Bediener klickt dann auf die Schaltfläche **Resume patrol** (Wächterkontrollgang fortsetzen). Der Leser wird mit einem grünen Häkchen und dem Buchstaben "c"  markiert. Der Wächter kann den Wächterkontrollgang jetzt am nächsten Leser fortsetzen.

Sollte es bei einem aktiven Wächterkontrollgang eine unvorhergesehene, aber harmlose Verspätung geben, kann der Wächter den Bediener anrufen, um den Zeitplan anzupassen. Geben Sie im Drehfeld **Delay (min)** (Verzögerung (Min.)) ein, um wie viele Minuten eine Verspätung vorliegt, und klicken Sie auf die Schaltfläche **Apply** (Übernehmen).

Sollte ein Wächterkontrollgang nicht innerhalb des Zeitplans abgeschlossen werden können, kann der Bediener ihn abbrechen, indem er auf die Schaltfläche **Interrupt** (Unterbrechen) klickt. Der **State** (Status) des Wächterkontrollgangs ändert sich in **Aborted** (Abgebrochen) und wird unter die geplanten und aktiven Wächterrunden in der Liste verschoben.

## 21.3

## Überwachung von Runden (ehemals Wegekontrolle)

### Einführung

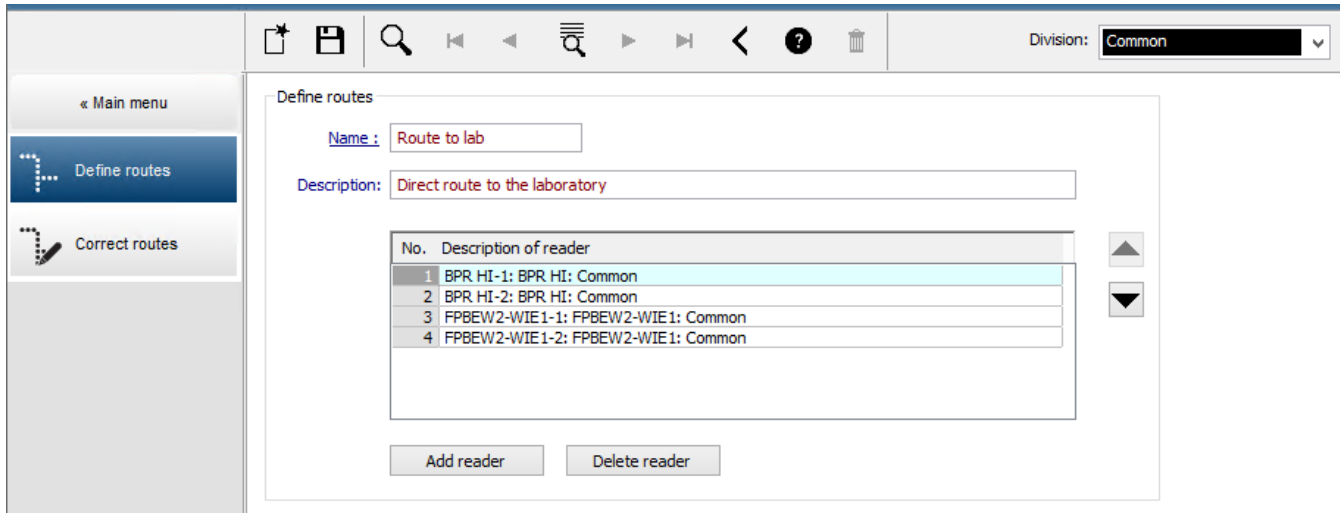
Ein Weg (oder eine Runde) beschreibt eine vorab definierte Abfolge von Lesern, die für bestimmte Personen im Zutrittskontrollsystem festgelegt werden kann. Auf diese Weise werden ihre Bewegungen unabhängig von den jeweiligen Berechtigungen auf dem Gelände gesteuert.

Diese Funktion kommt in der Regel zum Einsatz, wenn strenge Zutrittsabfolgen erzwungen werden sollen, wie in industrielle Reinräumen, hygienisch kontrollierten oder Hochsicherheitsbereichen.

### Definieren von Wegen

1. Wählen Sie im Hauptmenü **Tour monitoring** (Wegekontrolle) > **Define routes** (Wege definieren).
2. Geben Sie einen Namen für den Weg ein (bis zu 16 Zeichen).
3. Geben Sie eine detailliertere Beschreibung ein (optional).

- Klicken Sie wie bei den Wächterrunden auf die Schaltfläche **Add reader** (Leser hinzufügen), um eine Abfolge von Lesern zu erstellen. Verändern Sie mithilfe der Pfeilschaltflächen die Position eines Lesers in der Abfolge. Um einen Leser zu entfernen, verwenden Sie die Schaltfläche **Delete reader** (Leser löschen).



### Zuweisen einer Route zu einer Person

Gehen Sie folgendermaßen vor, um einer Person eine Route zuzuweisen:

- Klicken Sie im Hauptmenü auf **Personnel data** (Personaldaten) > **Cards** (Ausweise)
- Laden Sie den Personendatensatz der zuzuweisenden Person
- Aktivieren Sie auf der Registerkarte **Other data** (Weitere Daten) das Kontrollkästchen **Tour monitoring** (Wegekontrolle).
- Wählen Sie in der Dropdown-Liste daneben einen definierten Weg aus (siehe vorherigen Abschnitt zum Definieren von Wächterrunden).
- Speichern Sie den neuen Personendatensatz.

Ein Weg wird aktiviert, wenn die zugewiesene Person ihren Ausweis an dem ersten Leser des Weges vorlegt. Die anderen Leser auf dem Weg müssen jetzt in der vorgegebenen Reihenfolge besucht werden. Nur der festgelegte nächste Leser gewährt Zutritt. Nachdem der Weg vollständig abgegangen wurde, kann sich die Person an einem beliebigen anderen Leser aus ihrem Berechtigungsbereich anmelden.

### Korrigieren und Überwachen von Wegen

- Wählen Sie im Hauptmenü **Tour monitoring** (Wegekontrolle) > **Correct routes** (Wege korrigieren).
- Laden Sie den Personaldatensatz der Person, die der Route zugeordnet ist.
- Um diese Person auf der Route zu finden, klicken Sie auf die Schaltfläche **Determine location** (Position ermitteln).
- Leser, die bereits angelaufen wurden, erhalten in der Liste ein grünes Häkchen ✓.
- Um den Standort einer Person auf der Route zurückzusetzen oder zu korrigieren, klicken Sie auf die Schaltfläche **Set location** (Position setzen).



## 22 Zufällige Personenkontrolle

### Der Prozess der Mitarbeiterauslösung

1. Ein Ausweisinhaber liest seinen Ausweis an einem Leser ein, der für die Mitarbeiterauslösung konfiguriert ist.

#### Hinweis

Nur Personen, die berechtigt sind, den Durchtritt in der definierten Richtung zu passieren, können zufällig ausgewählt werden. Da Berechtigungen vor der Mitarbeiterauslösung kontrolliert werden, werden nicht zutrittsberechtigte Personen sofort abgewiesen und nicht in den Auswahlprozess einbezogen.

2. Wenn der Zufallsgenerator diese Person zur Mitarbeiterauslösung wählt, wird ihr Ausweis für das gesamte System gesperrt.
  - Das Ereignis wird im Systemlogbuch aufgezeichnet.
  - An den Dialog **Sperrung** wird ein Eintrag mit unbegrenzter Dauer gesendet, der durch **Mitarbeiterauslösung** gekennzeichnet ist [Abbildung 1 unten].
  - In der Statusleiste des Dialogs „personnel data“ (Personal Daten) von Access Engine werden die „LEDs“ „Blocked“ (Gesperrt) (rot) mit dem (violett blinkenden) Hinweis „Random screening“ (Mitarbeiterauslösung) angezeigt



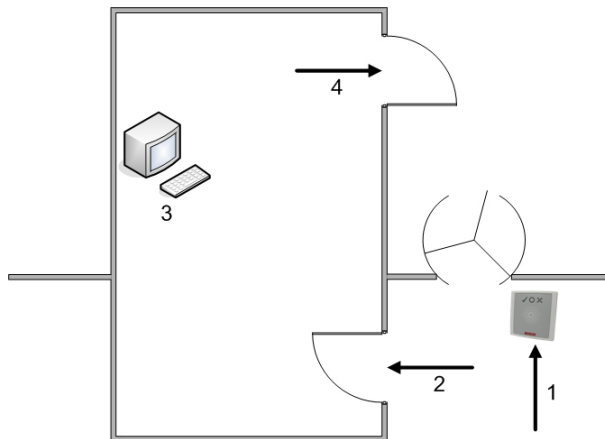
#### Hinweis!

Personen, für die der Parameter **Excluded from random screening** (Von MA-Auslösung ausgeschlossen) im Dialog **Cards** (Ausweise), Registerkarte **Other data** (Weitere Daten) gesetzt wurde, werden in den Auslösungsprozess nicht einbezogen.

3. Die zufällig ausgewählte Person wird zu weiteren Kontrollen in eine separate Sicherheitskabine gebeten.
4. Nachdem diese Kontrollen ausgeführt wurden, setzt der Wachmann die Sperre im Dialog **Blocking** (Sperrung) wie folgt zurück:
  - Wählen Sie die entsprechende Sperre in der Liste „control“ (Steuerung) der Liste **Blocking** (Sperrung) aus.
  - Klicken Sie auf die Schaltfläche **Delete** (Löschen).
  - Bestätigen Sie den Löschvorgang, indem Sie auf **Yes** (Ja) klicken.

Die ausgeloste Person kann jetzt ihren Ausweis wieder an allen Lesern verwenden, für die sie über Berechtigungen verfügt.

### Beispiel Raumgrundriss für Mitarbeiterauslösung



1 = Ausweis einlesen – Auslösung – systemweite Sperre

2 = Ausweisinhaber betritt Sicherheitskabine.

3 = Ausweisinhaber wird durchsucht, und die Sperre wird anschließend über den Dialog aus seinem Ausweis entfernt.

4 = Ausweisinhaber verlässt die Sicherheitskabine, ohne den Ausweis erneut beim Leser einzulesen.

**Hinweis!**


Der Auslosungsfaktor wird über die Zeit kumulativ erreicht. Zum Beispiel gibt es bei einer Mitarbeiterauslosung von 10 % immer noch die Möglichkeit (1 in 100, also  $1/10 \times 1/10$ ), dass zwei aufeinanderfolgende Personen ausgewählt werden.

## 23 Verwenden der Ereignisanzeige

### Einführung

Mit der Ereignisanzeige können entsprechend autorisierte Bediener Ereignisse überprüfen, die vom System aufgezeichnet wurden, und Berichte erstellen, die gedruckt oder auf dem Bildschirm angezeigt werden.

Um die gewünschten Datensätze aus der Logbuch-Datenbank abzurufen und anzuzeigen, legen

Sie Filterkriterien fest und klicken Sie auf **Refresh** (Aktualisieren) .

Filterkriterien können auf verschiedene Arten festgelegt werden:

**Relativ** Um Ereignisse relativ zur aktuellen Zeit auszuwählen

**Intervall** Um Ereignisse innerhalb eines frei definierbaren Zeitintervalls auszuwählen

**Insgesamt** Um Ereignisse unabhängig vom Zeitpunkt ihres Auftretens auszuwählen





### Voraussetzungen

Sie sind beim Dialog-Manager angemeldet.





### Dialogpfad

Dialog-Manager-Hauptmenü > **Reports** (Berichte) > **Event viewer** (Ereignisanzeige)


### 23.1 Festlegen von Filterkriterien für die Zeit relativ zur Gegenwart




1. Wählen Sie unter **Time period** (Zeitraum) das Optionsfeld **Relative** (Relativ)
2. Legen Sie im Feld **Search within the last** (Suche innerhalb der letzten) die Anzahl der zu durchsuchenden Zeiteinheiten fest und wählen Sie die zu verwendenden Einheiten aus, z. B. Wochen, Tage, Stunden, Minuten und Sekunden.
3. Wählen Sie im Menü **Event types** (Ereignistypen) die Kategorie der zu durchsuchenden Ereignisse und dann die Ereignistypen, die Sie interessieren.
4. Begrenzen Sie im Menü **Maximum number** (Maximale Anzahl) die Anzahl der Ereignisse, die die Ereignisanzeige zu empfangen versucht. Aus Leistungsgründen ist es **nichtempfohlen**, den Wert **(unlimited)** (unbegrenzt) zu lassen.
5. Geben Sie andere Filterkriterien an, die Sie interessieren:
  - Nachname
  - First name (Vorname)
  - Personalnummer
  - Ausweisnummer
  - Benutzer (d. h. der Systembetreiber)
  - Codedaten
  - Gerätename
  - Bereichsname.
- Klicken Sie auf **Refresh** (Aktualisieren) , um mit dem Sammeln von Ereignissen zu beginnen, und auf **Cancel** (Abbrechen), um dies zu stoppen.
- Klicken Sie auf , um die Ergebnisse zu speichern, oder auf , um sie zu drucken.
- Klicken Sie auf , um die Ergebnisse für eine weitere Suche zu löschen.

## 23.2 Festlegen von Filterkriterien für ein Zeitintervall

1. Wählen Sie unter **Time period** (Zeitraum) das Optionsfeld **Interval** (Intervall)
  2. Definieren Sie in der Datumsauswahl **Time from, Time until** (Zeit von, Zeit bis) den Beginn und das Ende des Zeitraums, in dem nach Ereignissen gesucht werden soll.
  3. Wählen Sie im Menü **Event types** (Ereignistypen) die Kategorie der zu durchsuchenden Ereignisse und dann die Ereignistypen, die Sie interessieren.
  4. Begrenzen Sie im Menü **Maximum number** (Maximale Anzahl) die Anzahl der Ereignisse, die die Ereignisanzeige zu empfangen versucht. Aus Leistungsgründen ist es **nichtempfohlen**, den Wert **(unlimited)** (unbegrenzt) zu lassen.
  5. Geben Sie andere Filterkriterien an, die Sie interessieren:
    - Nachname
    - First name (Vorname)
    - Personalnummer
    - Ausweisnummer
    - Benutzer (d. h. der Systembetreiber)
    - Codedaten
    - Gerätename
    - Bereichsname.
- Klicken Sie auf **Refresh** (Aktualisieren) , um mit dem Sammeln von Ereignissen zu beginnen, und auf **Cancel** (Abbrechen), um dies zu stoppen.
- Klicken Sie auf , um die Ergebnisse zu speichern, oder auf , um sie zu drucken.
- Klicken Sie auf , um die Ergebnisse für eine weitere Suche zu löschen.

## 23.3 Festlegen von Filterkriterien unabhängig von der Zeit

1. Wählen Sie unter **Time period** (Zeitraum) das Optionsfeld: **Total** (Insgesamt)
  2. Wählen Sie im Menü **Event types** (Ereignistypen) die Kategorie der zu durchsuchenden Ereignisse und dann die Ereignistypen, die Sie interessieren.
  3. Begrenzen Sie im Menü **Maximum number** (Maximale Anzahl) die Anzahl der Ereignisse, die die Ereignisanzeige zu empfangen versucht. Aus Leistungsgründen ist es **nichtempfohlen**, den Wert **(unlimited)** (unbegrenzt) zu lassen.
  4. Geben Sie andere Filterkriterien an, die Sie interessieren:
    - Nachname
    - First name (Vorname)
    - Personalnummer
    - Ausweisnummer
    - Benutzer (d. h. der Systembetreiber)
    - Codedaten
    - Gerätename
    - Bereichsname.
- Klicken Sie auf **Refresh** (Aktualisieren) , um mit dem Sammeln von Ereignissen zu beginnen, und auf **Cancel** (Abbrechen), um dies zu stoppen.

- Klicken Sie auf  , um die Ergebnisse zu speichern, oder auf  , um sie zu drucken.
- Klicken Sie auf  , um die Ergebnisse für eine weitere Suche zu löschen.


## 24 Verwenden von Berichten

Dieser Abschnitt beschreibt eine Sammlung von Berichtsfunktionen, mit denen System- und Logbuchdaten gefiltert und in übersichtlichen Formaten dargestellt werden können.

### Dialogpfad







Main menu (Hauptmenü) > **Reports** (Berichte).

### Verwenden der Berichte-Symbolleiste

Klicken Sie auf , um vor dem Drucken eine Vorschau anzuzeigen.

Die Vorschau hat eine eigene Symbolleiste:

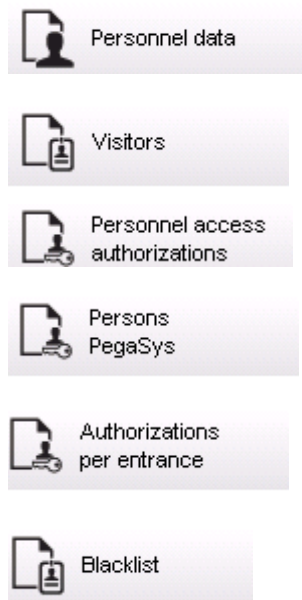


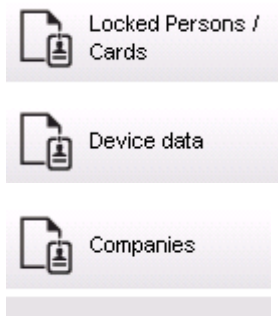
- Klicken Sie auf , um die Vorschau ohne Drucken zu verlassen.
- Benutze die Pfeiltasten   in der Vorschau-Symbolleiste, um zwischen den Seiten hin- und herzublätern oder einzelne Seiten nach Seitenzahl auszuwählen.
- Klicken Sie auf , um mit Ihrem Standarddrucker sofort zu drucken
- Klicken Sie auf , um über einen Druckereinstellungen-Dialog zu drucken, der weitere Druckoptionen ermöglicht.
- Klicken Sie auf , um den Bericht in eine Auswahl von Dateiformaten zu exportieren, einschließlich PDF, RTF und Excel.
- Die Zahlen auf der rechten Seite der Symbolleiste repräsentieren:
  - Die Gesamtzahl der vorhandenen Datenbankeinträge, die den Filterkriterien entsprechen.
  - Der Prozentsatz der Datenbankeinträge, die in der Vorschau angezeigt werden.

### 24.1 Berichte: Stammdaten

#### Berichteübersicht – Stammdaten

Die Stammdatenberichte enthalten alle Berichte zu Personen, Besuchern, Ausweisen und ihrem Zutritt. Darüber hinaus können die Geräte- und Unternehmensdaten angezeigt werden.



**Bericht: Personnel Data (Personaldaten)**

Beim Erstellen der Berichte können zwei Filter angewendet werden.

Personenfilter: Hier basiert der Bedienerfilter auf den üblichen Personaldatenfeldern.

Zutrittsausweisfilter: Hier kann der Bediener anhand der Ausweisnummern, Nummernbereiche, des Status und des Sperrstatus filtern.

**Bericht: Visitors (Besucher)**

Hier können ähnlich wie bei den Personaldaten Besucherberichte erstellt werden. Dabei kann dennoch auf alle erstellten Besucherdaten zugegriffen werden. Das bedeutet, dass selbst Besucher, deren Ankunft noch bevorsteht, die aber bereits registriert sind, ausgewählt werden können.

**Bericht: Personnel Access Authorizations (Personalzutrittsberechtigungen)**

Dieser Bericht gibt einen Überblick über die im System registrierten Zutrittsberechtigungen.

Zudem führt er die Personen auf, denen diese Berechtigungen zugewiesen wurden.

Als Filter können personenbezogene Daten und bestimmte Berechtigungen verwendet werden:

- Personaldaten: Nachname, Vorname, Personalnummer
- Gültigkeit aller Berechtigungen
- Name der Berechtigung, die für den Durchtritt gilt
- Name des Zeitmodells (sofern vorhanden)
- Begehungsrichtung am Durchtritt
- Gültigkeit der Sonderberechtigung

**Bericht: Blacklist (Schwarze Liste)**

In diesem Dialog kann eine Liste aller oder nur bestimmter Ausweise, die aus verschiedenen Gründen auf die schwarze Liste gesetzt wurden, gedruckt werden.

**Bericht: Blocked Persons/Cards (Gesperrte Personen/Ausweise)**

Mit diesem Dialog können Berichte erstellt werden, die Daten zu allen gesperrten Personen enthalten.

Verwenden Sie Datumsangaben, um Sperrungen innerhalb bestimmter Zeiträume zu finden.

**Bericht: Device Data (Gerätedaten)**

Der Dialog kann verwendet werden, um Berichte basierend auf Gerätedaten zu erstellen, z. B. Geräte- oder Gerätetyp.

**Bericht: Companies (Firmen)**

Mit dem Berichtdialog "Companies" (Firmen) können Sie Firmendaten in einer Liste zusammenstellen.

Verwenden Sie beispielsweise Sternchen, um Firmen zu finden, die mit einem bestimmten Buchstaben beginnen.

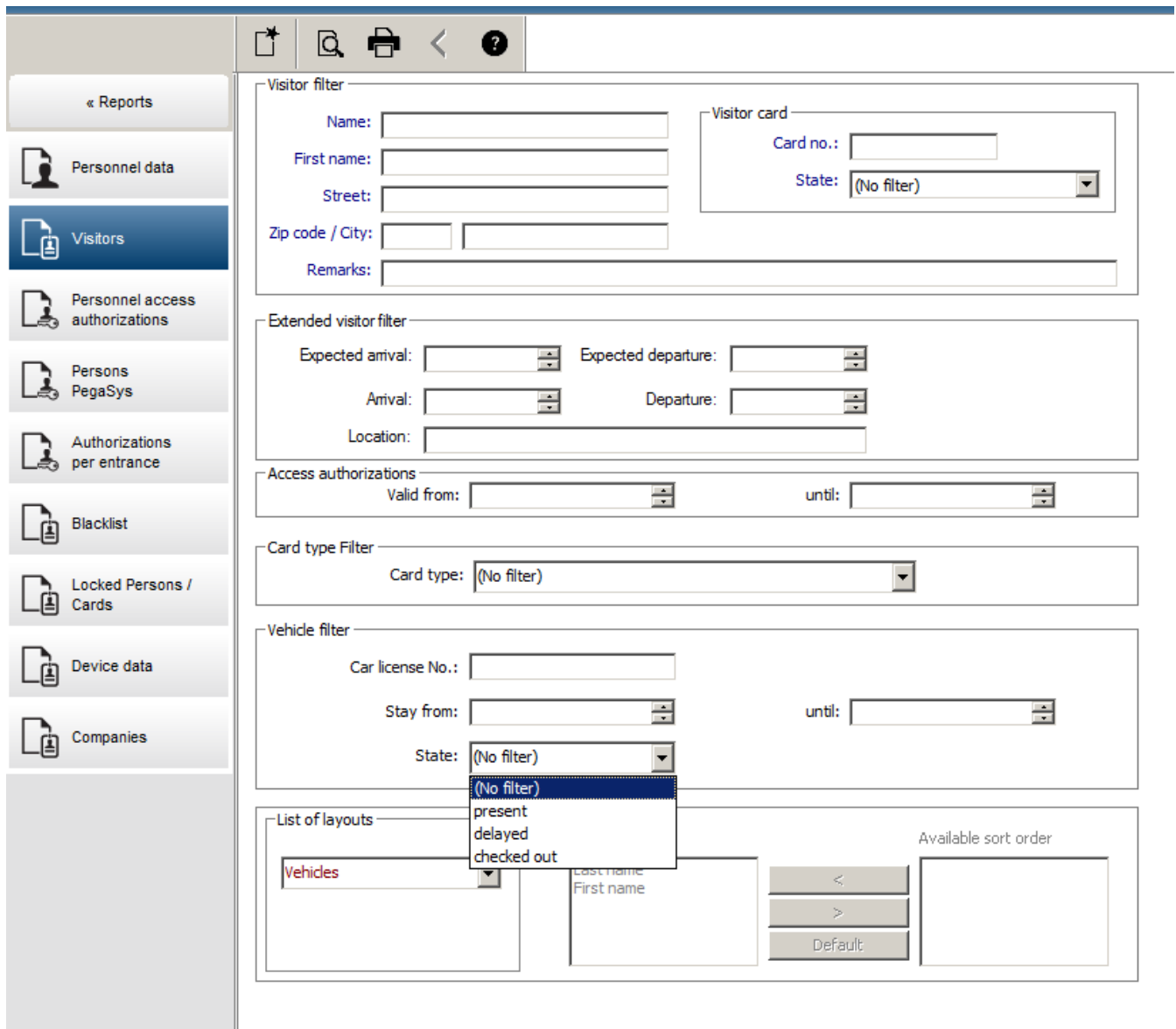
**24.1.1**

**Berichterstattung über Fahrzeuge**

Im Dialog **Reports (Berichte) > Visitors (Besucher)** kann **Vehicles (Fahrzeuge)** von der Liste gewählt werden. Sobald **Vehicles (Fahrzeuge)** ausgewählt wurde, ist der **Vehicle filter (Fahrzeugfilter)** aktiviert und kann zum Filtern von Fahrzeugen und deren Status verwendet werden.

Die Statusinformationen sind wie folgt aufgebaut:

- Present (Anwesend): Besuch noch nicht beendet, Zeit noch nicht abgelaufen.
- Delayed (Verspätet): Besuch noch nicht beendet, aber Zeit ist abgelaufen.
- Checked out (Abgemeldet): Besucher hat alle Ausweise zurückgegeben.





Der **Report for vehicles (Fahrzeugbericht)** kann nur für Besucher erstellt werden, da voraussichtliches Ankunfts- und Abreisedatum sowie tatsächliches Ankunfts- und Abreisedatum in der Datenbank nur für Besucher in der Tabelle **Visitors (Besucher)** verfügbar ist.

Der Bericht listet nur die Fahrzeugnummern, die in der Datenbanktabelle **Persons (Personen)** gespeichert sind. Wenn sich also einmal eine Fahrzeugnummer ändert, wird der Bericht andere Ergebnisse ausweisen.

Die Aufenthaltsdauer wird wie folgt berechnet:

- Falls der Besucher bereits abgemeldet ist, wird der Unterschied zwischen Ankunft und Abfahrt in Minuten angezeigt.
- Falls der Besucher noch nicht abgemeldet ist, wird der Unterschied zwischen Ankunft und dem jetzigen Zeitpunkt in Minuten angezeigt.

### Access Engine




Datum 02.07.2014 , 14:26:14  
Seite 1

| Lastname                              | Firstname                             | Arrival<br>Departure<br>Duration                | Vehicle<br>Last area       | Person<br>Last area |
|---------------------------------------|---------------------------------------|---|----------------------------|---------------------|
| Neuer Besucher mit<br>Langem Namen    | Vorname                               | 02.07.2014 14:21<br>02.07.2014 14:30<br>0h 5'   | AC BB 5678<br>parkplatz_01 | ASB                 |
|                                       | present                               |   |                            |                     |
| Test                                  | Visitor                               | 01.07.2014 09:10<br>02.07.2014 12:00<br>29h 16' | AC AA 1234<br>parkplatz_01 | ISB                 |
|                                       | too late                              |   |                            |                     |
| Testbesucher mit sehr<br>langem Namen | Besucher mit gaaaaanz<br>langem namen | 01.07.2014 07:30<br>01.07.2014 12:00<br>4h 30'  | AC AA 2345<br>AUSSEN       | AUSSEN              |
|                                       | departed                              |   |                            |                     |


## 24.2 Berichte: Systemdaten

### Berichte – Systemdaten

Im Gegensatz zu den Stammdaten handelt es sich bei den Systemdaten um Informationen, die dem System zugewiesen werden und nicht auf Personen, Ausweise oder Firmen bezogen sind. Diese Berichte werden im Folgenden näher erläutert.

-  Areas
-  Area configuration
-  Area muster list

---

-  Muster list total

**Bericht: Areas (Bereiche)**

Mit diesem Dialog können die verschiedenen Standorte in einem Bericht gesammelt werden. Der Dialog enthält nur einen Bereichsfilter, über den die verschiedenen Gebäude und anderen Zonen ausgewählt werden können.

Der betreffende Bereich wird über einen Klick mit der linken Maustaste ausgewählt. Der Benutzer kann den Bericht über die Schaltfläche **Preview** (Vorschau) auf dem Bildschirm anzeigen, bevor er den Druckvorgang mit **Print** (Drucken) startet.

Es sind zwei Layouts verfügbar.

|  |                   |   |
|--|-------------------|---|
|  | Standard          | Personen, die sich am Standort aufhalten – keine Parkplätze |
|  | Parkplatzbelegung | Personen, die sich am Standort aufhalten – nur Parkplätze   |

Damit kontrolliert werden kann, ob die angezeigten Datensätze auf dem aktuellen Stand sind, werden auch die letzten Ausweisscans für die Bereiche angezeigt.

Somit können für verschiedene Anlässe zuverlässige Informationen über den Aufenthaltsort von Personen bereitgestellt werden.

**Bericht: Areas Configuration (Bereiche Konfiguration)**

Definierte Bereiche und deren Unterbereiche mit einer Kennung für Parkplätze sowie Angabe der maximal erlaubten Anzahl von Personen oder Fahrzeugen in diesem Bereich.

**Bericht: Area Muster List (Feuerwehrliste)**

Die Personen in einem Bereich können nicht nur rein zahlenmäßig, sondern auch namentlich erfasst werden.

Neben den Scanzeiten der einzelnen Bereiche enthalten diese Bereiche auch die Zeiten der einzelnen Personen.

**Bericht: Muster List Total (Feuerwehrliste Summe)**

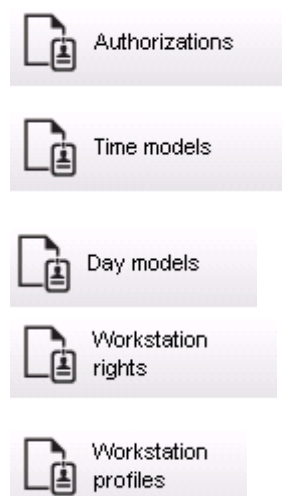
Im Prinzip entsprechen die Feuerwehrlisten dem Berichtdialog **Areas** (Bereiche). Allerdings bieten sie für die einzelnen Zonen Listen mit Informationen über die Anzahl der Personen, die sich laut Zutrittskontrolle gegenwärtig in diesem Bereich aufhalten.

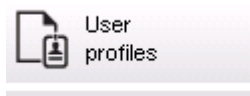
## 24.3

### Berichte: Berechtigungen

**Übersicht**

In diesem Menüelement sind die verschiedenen Berechtigungen zusammengefasst, die in den entsprechenden Dialogen erteilt wurden:



**Bericht: Authorizations (Berechtigungen)**

Mit diesem Dialog können die im System definierten Zutrittsberechtigungen angezeigt werden. Die den einzelnen Zutrittsberechtigungen zugeordneten Durchtritte werden aufgeführt. Der Name des ausgewählten Zeitmodells wird angezeigt. Darüber hinaus wird in dem Bericht angegeben, wie vielen Personen die Berechtigung zugewiesen wurde.

**Bericht: Time Models (Zeitmodelle)**

In diesem Bericht können die im System definierten und ausgewählten Zeitmodelle angezeigt werden. Dieser Bericht enthält alle Daten zu einem Modell und gibt an, wie vielen Personen das Modell zugewiesen wurde.

**Bericht: Day Models (Tagesmodelle)**

In diesem Bericht werden alle definierten Tagesmodelle mit Namen, Beschreibungen und Intervallen aufgeführt.

**Bericht: Workstation Rights (Dialogstationsrechte)**

Mit diesem Dialog können die Dialogstationsrechte angezeigt werden, die den im System definierten Dialogstationen zugewiesen wurden.

**Bericht: Workstation Profiles (Dialogstationsprofile)**

Mit diesem Dialog können die im System definierten Dialogstationsprofile angezeigt werden. Die Systemabläufe, die an den einzelnen Dialogstationen möglich sind, können somit in einem klaren Format präsentiert werden.

**Bericht: User Rights (Benutzerrechte)**

Mit diesem Dialog können die Benutzerprofile angezeigt werden, die den im System definierten Benutzern zugewiesen wurden.

**Bericht: User Profiles (Benutzerprofile)**

Mit diesem Dialog können die Dialoge und Dialogrechte angezeigt werden, die den im System definierten Benutzerprofilen zugewiesen wurden.

## 25 Betriebs-Bedrohungsstufenverwaltung

In diesem Abschnitt werden die verschiedenen Möglichkeiten beschrieben, um eine Bedrohungsstufe auszulösen und abzurechnen. Hintergrundinformationen finden Sie im Abschnitt *Konfigurieren der Bedrohungsstufenverwaltung, Seite 121*

### Einführung

Eine Bedrohungsstufe wird durch einen Bedrohungsalarm aktiviert. Ein Bedrohungsalarm kann auf folgende Weise ausgelöst werden:

- Durch einen Befehl in der Software-Benutzeroberfläche
- Durch ein Eingangssignal, das auf einer lokalen Zutrittskontrollzentrale definiert ist, z. B. eine Drucktaste.
- Durch Einlesen eines Alarmausweises an einem Leser

Beachten Sie, dass Bedrohungswarnungen durch den Bedienoberflächen-Befehl oder das Hardware-Signal, jedoch nicht durch einen Alarmausweis abgebrochen werden können.


### Siehe

- *Konfigurieren der Bedrohungsstufenverwaltung, Seite 121*

### 25.1 Auslösen und Abbrechen eines Bedrohungsalarms über den Bedienoberflächen-Befehl

In diesem Abschnitt wird beschrieben, wie Sie einen Bedrohungsalarm in der AMS Kartenansicht auslösen.

#### Dialogpfad

- AMS Kartenansicht >  (Gerätebaum)

#### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens eine Bedrohungsstufe wurde im Geräteeditor mit „Aktiv“ markiert.
- Sie als Map View und AMS-Bediener verfügen über die erforderlichen Berechtigungen:
  - zum Betrieb von Bedrohungsstufen
  - zum Anzeigen des MAC oder der MACs im Mandanten, in dem die Bedrohungsalarm ausgelöst werden soll.

#### Verfahren zum Auslösen eines Bedrohungsalarms

1. Klicken Sie im Gerätebaum in der AMS Kartenansicht mit der rechten Maustaste auf das MAC-Gerät, auf dem der Bedrohungsalarm ausgelöst werden soll.
  - Es wird ein Kontextmenü mit den Befehlen angezeigt, die Sie auf diesem MAC ausführen dürfen.
  - Wenn noch keine Bedrohungsstufe in Betrieb ist, enthält das Menü ein oder mehrere Elemente mit der Bezeichnung **Activate Threat level** (Bedrohungsstufe aktivieren) „<name>“, wobei der Name der Bedrohungsstufe im Geräteeditor definiert ist.
2. Wählen Sie die Bedrohungsstufe aus, die Sie auslösen möchten.
  - Die Bedrohungsstufe geht in Betrieb.

#### Verfahren zum Abbrechen eines Bedrohungsalarms

Voraussetzung: Eine Bedrohungsstufe ist bereits in Betrieb.

1. Klicken Sie im Gerätebaum in der AMS Kartenansicht mit der rechten Maustaste auf das MAC-Gerät, auf dem der Bedrohungsalarm abgebrochen werden soll.
  - Es wird ein Kontextmenü mit den Befehlen angezeigt, die Sie auf diesem MAC ausführen dürfen.
2. Wählen Sie **Deactivate Threat level** (Bedrohungsstufe deaktivieren). Aus dem Kontextmenü.
  - Die aktuelle Bedrohungsstufe ist deaktiviert.

## 25.2 Auslösen eines Bedrohungsalarms über Hardware signal

In diesem Abschnitt wird beschrieben, wie Sie ein Hardwareeingangssignal senden, um einen Bedrohungsalarm auszulösen.

### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.
- Hardware signale wurden auf einem AMC definiert, und ein Gerät wurde an das richtige Terminal an diesem AMC angeschlossen, das ihm ein Signal liefert. Klicken Sie bei Bedarf auf den Link am Ende dieses Abschnitts, um Anweisungen zum Konfigurieren des Eingangssignals zu erhalten, oder wenden Sie sich an den Systemadministrator.

### Vorgehensweise

Aktivieren Sie das Gerät, in der Regel eine Drucktaste oder ein Hardware schalter, das mit dem AMC verbunden ist.

Um den Bedrohungsalarm abzubrechen, aktivieren Sie das Gerät, das die als

**Threat level: Deactivate** definierte Eingangssignale sendet.

### Siehe

- *Zuweisen einer Bedrohungsstufe zu einem Hardware signal, Seite 126*

## 25.3 Auslösen eines Bedrohungsalarms über den Alarmausweis

In diesem Abschnitt wird beschrieben, wie Sie einen Bedrohungsalarm über einen Alarmausweis auslösen.

### Voraussetzungen

- Mindestens eine Bedrohungsstufe wurde definiert.
- Mindestens ein Eingang wurde im Gerätebaum konfiguriert.
- Für einen bestimmten Ausweisinhaber wurde ein Alarmausweis erstellt. Klicken Sie bei Bedarf auf den Link am Ende dieses Abschnitts, um Anweisungen zum Erstellen eines Alarmausweises zu erhalten, oder wenden Sie sich an den Systemadministrator.

### Vorgehensweise

1. Der Ausweisinhaber liest seinen speziellen Alarmausweis an einem beliebigen **Nicht-Fingerabdruckleser** am Standort ein.
  - Die für diesen Ausweis definierte Bedrohungsstufe wird aktiviert.
2. Wenn die Bedrohung vorbei ist, brechen Sie die Bedrohungsstufe über den Bedienoberflächen-Befehl oder den Hardware schalter ab. Grundsätzlich ist es nicht möglich, eine Bedrohungsstufe über einen Alarmausweis abzubrechen.

**Siehe**

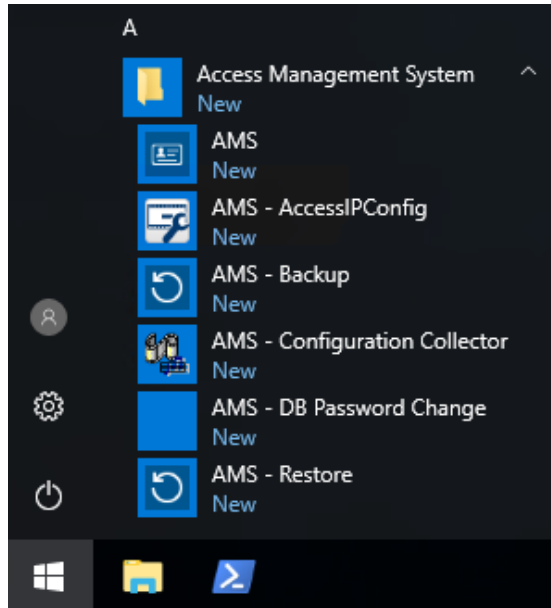
- *Erstellen eines Alarmausweis, Seite 141*

## 26 Backup und Wiederherstellung

Die Funktion **Backup & Restore** (Backup & Wiederherstellung) ermöglicht es Ihnen, Ihre Installation auf einem anderen Computer zu rekonstruieren, wenn der ursprüngliche Computer ausfällt.

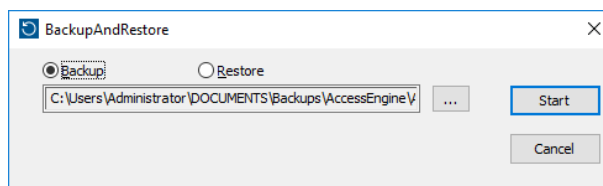
**Backup and Restore** (Backup und Wiederherstellung) kann nur auf dem Rechner gestartet werden, auf dem der AMS-Server installiert ist. Zur Vereinfachung werden zwei Verknüpfungen erstellt:

- **AMS - Backup** zum Erstellen eines Backups
- **AMS - Restore** (AMS - Wiederherstellung) zum Wiederherstellen eines Backups:

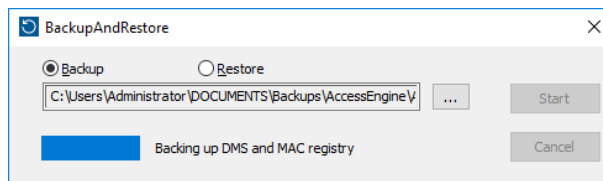


### 26.1 Backup-Verfahren

1. Klicken Sie auf die Verknüpfung **AMS - Backup**.  
Dadurch wird das Tool **Backup and Restore** (Backup und Wiederherstellung) gestartet:

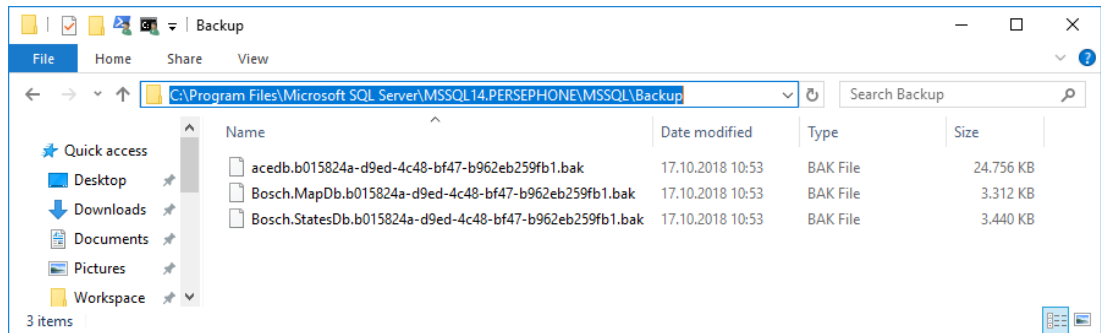


2. Geben Sie einen Pfad ein, in dem die GZIP-Datei gespeichert werden soll.
3. Klicken Sie auf **Start** (Starten), um das Backup zu starten.  
Ein Fortschrittsbalken wird angezeigt.  
Sobald dieser vollständig ist, wird die GZIP-Datei erstellt.



Der Speicherort des Backups der Datenbank hängt von der Version von SQL Server und dem Namen der Datenbankinstanz ab.

Wenn der AMS SQL Server-Instanzname beispielsweise "PERSEPHONE" lautet, befindet sich das Backup im folgenden Verzeichnis:



**WICHTIG:** Zur Datensicherheit empfiehlt Bosch dringend, diesen Ordner und die GZIP-Datei an einen sicheren, entfernten Ort zu kopieren. Lassen Sie nicht die einzige Sicherungskopie auf dem DMS-Servercomputer.



### Hinweis!

Das Logbuch wird unter dem folgenden Standardpfad gespeichert (Ihr Installationsprogramm hat möglicherweise einen anderen Pfad ausgewählt):

C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\

## 26.2

## Wiederherstellungsvorgang

### Voraussetzungen

- Die GZIP-Datei, die vom Tool **Backup and Restore** (Backup und Wiederherstellung) erstellt wurde
- Die Backup-Daten, die von SQL Server im SQL Server-Backup-Ordner erstellt werden.
- Ein SQL-Konto mit **sysadmin**-Rechten, wie **sa**.

### Hinweise zum Zielcomputer

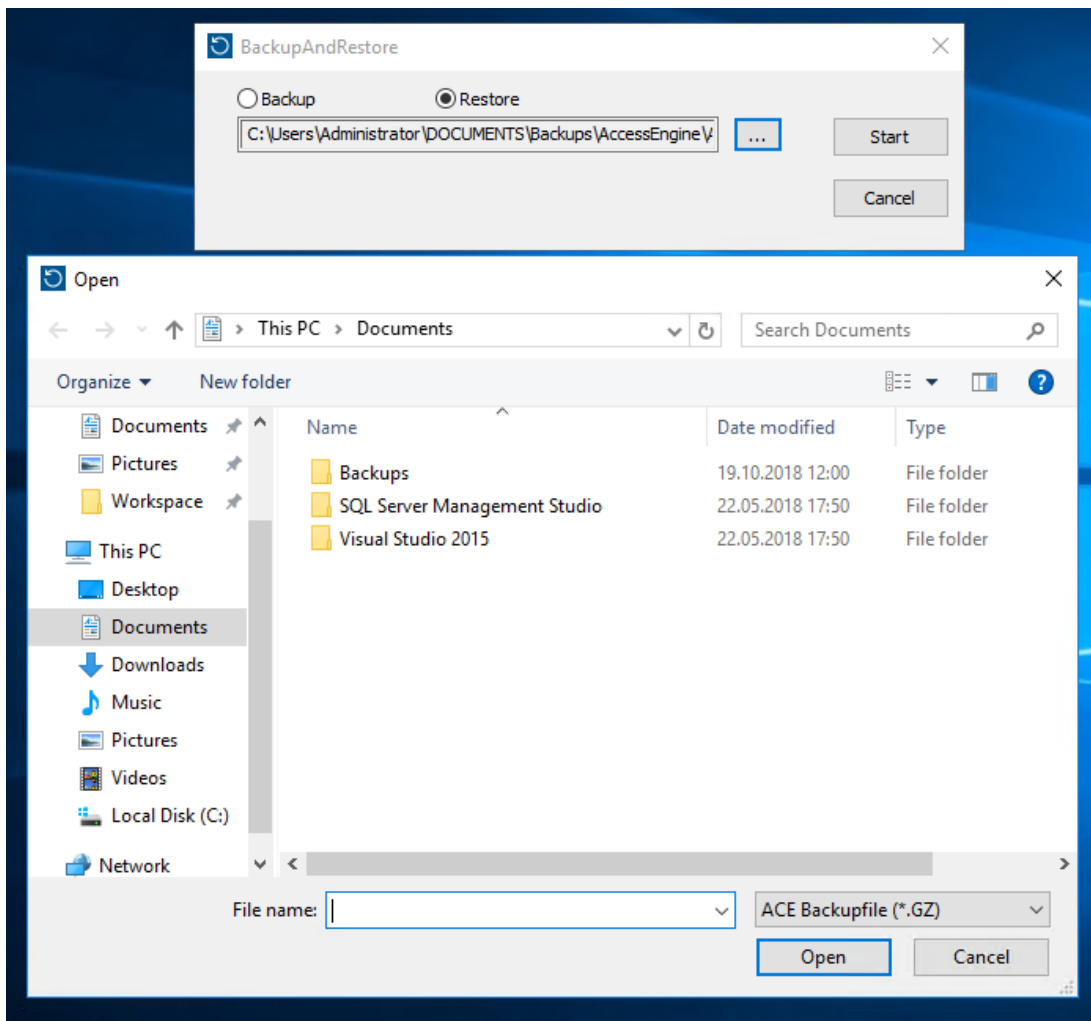
- Um die wiederhergestellte Konfiguration auszuführen, benötigt der Zielcomputer (auf dem Sie das Backup wiederherstellen) mindestens gleichwertige Lizenzen wie auf dem Computer, auf dem das Backup erstellt wurde.
- Alle Clients des Zielcomputers benötigen die Zertifikate, die von der Installation auf dem Zielcomputer generiert werden, nicht die von der Installation auf dem ursprünglichen Computer generierten Zertifikate.

Informationen zur Installation von Clientzertifikaten finden Sie im Installationshandbuch.

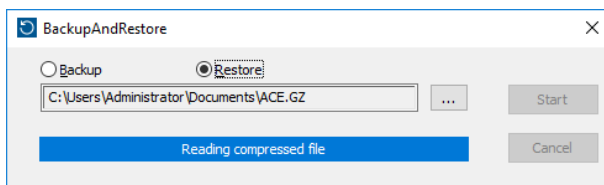
### Vorgehensweise

1. Klicken Sie im AMS-Programm auf **File** (Datei) > **Exit** (Beenden), um alle laufenden Dienste zu stoppen.
2. Wenn das Programm beendet wurde, führen Sie die Windows **Services**-Anwendung aus und überprüfen Sie, ob alle **Access Engine**- und **Access Management System**-Dienste gestoppt wurden.
3. Klicken Sie auf Windows Start > **AMS - Restore** (AMS – Wiederherstellung)
4. Klicken Sie auf die Schaltfläche **[...]**, um die GZIP-Backup-Datei zu suchen und auszuwählen.





5. Klicken Sie auf **Start** (Starten), um den Wiederherstellungsprozess zu starten.
6. Geben Sie die **SQL sysadmin**-Anmeldedaten ein.  
Der Wiederherstellungsvorgang beginnt



7. Wenn der Wiederherstellungsvorgang abgeschlossen ist, führen Sie die Windows **Services**-Anwendung aus und überprüfen Sie, ob alle `Access Engine`- und `Access Management System`-Dienste neu gestartet wurden.  
Wenn nicht, starten Sie sie manuell neu.
8. Starten Sie **AMS Kartenansicht** vom Desktop aus.
9. Suchen Sie den MAC in der Kartenansicht und klicken Sie mit der rechten Maustaste darauf.
10. Wählen Sie **Cold start MAC** (MAC kaltstarten), um die Daten aus dem Backup mit den aktuellen Systemdaten erneut zu synchronisieren.

# Glossar

## 1. MAC (erster MAC)

Der primäre MAC (Master Access Controller) in einem BIS Access Engine(ACE)- oder Access Manager(AMS)-System. Er kann sich auf demselben Computer wie das DMS befinden, aber er kann sich auch wie ein untergeordneter MAC auf einem separaten Computer befinden, der als MAC-Server bezeichnet wird.

## Automatische Nummernschilderkennung (Automated Number-Plate Recognition, ANPR)

Videotechnologie zum Lesen und Verarbeiten von Nummernschildern, in der Regel von Straßenfahrzeugen.

## Bedrohungsalarm

ein Alarm, der eine Bedrohungsstufe auslöst. Entsprechend autorisierte Personen können einen Bedrohungsalarm mit einer momentanen Aktion auslösen, z. B. über die Benutzeroberfläche des Bedieners, über ein Hardware-Signal (z. B. Drucktaste) oder durch Vorzeigen eines speziellen Bedrohungsalarmausweises an einem beliebigen Ausweisleser.

## Büromodus

Die Aufhebung der Zutrittskontrolle an einem Durchtritt während der Büro- oder Geschäftszeiten.

## Datenverwaltungssystem (DMS)

Ein Prozess auf der obersten Ebene zum Verwalten von Zutrittskontrolldaten in Access Engine. Der DMS liefert Daten an MACs (Main Access Controller), die wiederum Daten an lokale Zutrittskontrollzentralen (i. d. R. AMC) liefern.

## Datenverwaltungssystem (DMS)

Ein Prozess auf der obersten Ebene zum Verwalten von Zutrittskontrolldaten in Access Engine. Das DMS liefert Daten an MACs, die wiederum Daten an AMCs liefern.

## Durchschlüpfen

Umgehung der Zutrittskontrolle, indem einem autorisierten Ausweisinhabers durch einen Durchtritt nah gefolgt wird, ohne dass eigene Zugangsdaten vorgelegt werden.

## Durchtritt

Der Begriff Durchtritt bezeichnet den Zutrittskontrollmechanismus an einem Eintrittspunkt in seiner Gesamtheit: Er enthält die Leser, eine Art von abschließbarer Sperre und ein Zutrittsverfahren, definiert durch Sequenzen elektrischer Signale, die zwischen den Hardwareelementen weitergegeben werden.

## EMA

Einbruchmeldesystem, auch bekannt als Einbruchmeldeanlage.

## Identifikations-PIN

Eine persönliche Identifikationsnummer (PIN), die allein für den Zutritt ausreicht.

## Lokale Zutrittssteuerung (Local Access Controller, LAC)

Ein Hardwaregerät, das Zutrittsbefehle an die periphere Zutrittskontrollhardware, wie z. B. Leser und Schösser, sendet und Anforderungen von dieser Hardware für das gesamte Zutrittskontrollsystem verarbeitet. Der häufigste LAC ist ein Access Modular Controller oder AMC.

## MAC (Main Access Controller)

In Zutrittskontrollsystemen ein Serverprogramm, das die Local Access Controller, meist AMCs (Access Modular Controller), koordiniert und steuert

## MAC-Server

Hardware: Ein Computer (außer dem DMS-Server) in einem Access Engine-(ACE-) oder Access Management-(AMS-)System, auf dem ein MAC oder ein RMAC ausgeführt wird.

## Normalmodus

Im Gegensatz zum Büromodus gewährt der Normalmodus nur den Zutritt für Personen, die einen gültigen Ausweis am Leser vorzeigen.

## RMAC

Ein redundanter Main Access Controller (MAC), bei dem es sich um einen synchronisierten Zwilling eines vorhandenen MAC handelt. Dieser übernimmt die Verwaltung seiner Daten, wenn der erste MAC fehlschlägt oder nicht mehr verbunden ist.

---

**Sammelplatz**

Ein ausgewiesener Ort, an dem Menschen nach der Evakuierung eines Gebäudes warten sollen.

---

**SmartIntego**

Ein digitales Schließsystem von SimonsVoss Technologies. SmartIntego ist in einige Bosch Zutrittskontrollsysteme integriert.

---

**Türmodell**

Eine gespeicherte Softwarevorlage für einen bestimmten Durchtrittstyp. Türmodelle erleichtern die Definition von Durchritten in Zutrittskontrollsystemen.

---

**Verifikations-PIN**

Eine persönliche Identifikationsnummer (PIN), die in Kombination mit einem physischen Ausweis verwendet wird, um mehr Sicherheit zu gewährleisten.

---

**Whitelist (SmartIntego)**

Eine Whitelist ist eine Liste mit Ausweisnummern, die lokal auf den Ausweislesern eines SmartIntego-Schließsystems gespeichert ist. Wenn der MAC des Lesers offline ist, gewährt der Leser Zutritt für Ausweise, deren Nummern in der lokalen Whitelist enthalten sind.

---

**Zutrittssequenzüberwachung**

Die Verfolgung einer Person oder eines Fahrzeugs von einem definierten Bereich in einen anderen, indem jeder Scan der ID-Karte aufgezeichnet wird und nur Zutritt aus Bereichen gewährt wird, in denen die Karte bereits gescannt wurde.

---

**Zutrittswiederhol Sperre**

Eine einfache Form der Zutrittssequenzüberwachung, bei der ein Ausweisinhaber innerhalb einer definierten Zeitspanne daran gehindert wird, zweimal in einen Bereich einzutreten, es sei denn, der Ausweis wurde in der Zwischenzeit zum Verlassen dieses Bereichs gescannt. Die Zutrittswiederhol Sperre verhindert, dass Personen Zugangsdaten durch einen Eingang zurück an eine nicht autorisierte zweite Person geben, damit diese sie verwenden kann.







**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

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

© Bosch Security Systems B.V., 2020