Access Management System

AMS Configuration and Operation

de Software manual

Inhaltsverzeichnis

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 Vorzeige-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** > **Licenses** (Konfiguration > Lizenzen)

1. Melden Sie sich bei AMS (Access Management System) an.
2. Klicken Sie in der Registerkarte **License** (Lizenz) auf die Schaltfläche **Start License Manager** (Lizenzmanager starten).
   – **Ergebnis:** Das Dialogfenster „License Manager“ (Lizenzmanager) wird angezeigt.
3. Wählen Sie die Kontrollkästchen für das Softwarepaket, die Funktionen und Erweiterungen aus, die Sie bestellt haben. Geben Sie für die Erweiterungen auch die Anzahl der benötigten Einheiten an.
4. Klicken Sie auf die Schaltfläche **Activate...** (Aktivieren...).
   – **Ergebnis:** Das Dialogfenster **Lizenzaktivierung** mit Ihrer Computersignatur wird angezeigt.
5. Notieren Sie sich die Computersignatur, oder fügen Sie sie per Copy & Paste in eine Textdatei ein.
6. Geben Sie auf einem Rechner mit Internetzugang folgende URL im Browser ein: https://activation.boschsecurity.com
   Wenn Sie nicht über ein Konto für den Zugriff auf das Bosch License Activation Center verfügen, erstellen Sie entweder ein neues Konto (empfohlen) und melden Sie sich an oder klicken Sie auf den Link, um eine neue Lizenz ohne Anmeldung zu aktivieren. Bitte beachten Sie, dass für SMA-Lizenzen (Softwarewartungsvertrag) immer ein Konto erforderlich ist. Ein Konto hat weiter den Vorteil, das Sie für künftige Angaben einen Überblick über sämtliche Aktivierungen haben.

   Folgen Sie den Angaben auf der Website, um den Lizenzaktivierungsschlüssel zu erhalten.

7. Kehren Sie zur Software zurück. Tippen Sie im Dialogfenster **License Activation** (Lizenzaktivierung) den vom Bosch License Activation Center erhaltenen Lizenzaktivierungsschlüssel (oder fügen Sie ihn per Copy & Paste ein) und klicken Sie auf die Schaltfläche **Activate** (Aktivieren).
   – **Ergebnis:** Die Softwarepakete werden für den Rechner aktiviert.

Hinweis!
Auswirkungen von Hardware- und Softwareänderungen
Änderungen an der Hardware Ihres Servers können dazu führen, dass die Lizenz ungültig wird und die Software nicht mehr funktioniert. Wenden Sie sich an den technischen Support, bevor Sie Änderungen am Server vornehmen.

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

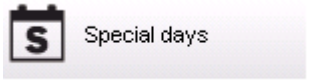
2. Navigieren Sie zu **Configuration** (Konfiguration) > **Licenses** (Lizenzen)
3. Klicken Sie auf die Schaltfläche **Activate Demo Mode** (Demomodus aktivieren)
4. Überprüfen Sie, ob die Funktionen im Dialogfenster **Licenses** (Lizenzen) aufgelistet sind.

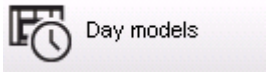
Der Demonstrationsmodus ist für 5 Stunden aktiviert. Beachten Sie, dass die Ablaufzeit in der Nähe des oberen Randes des Dialogs **Licenses** (Lizenzen) und in der Titelleiste der meisten Dialogfenster angezeigt.

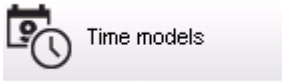
5 Konfigurieren des Kalenders

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 Durchtritten Zeitmodelle zu.

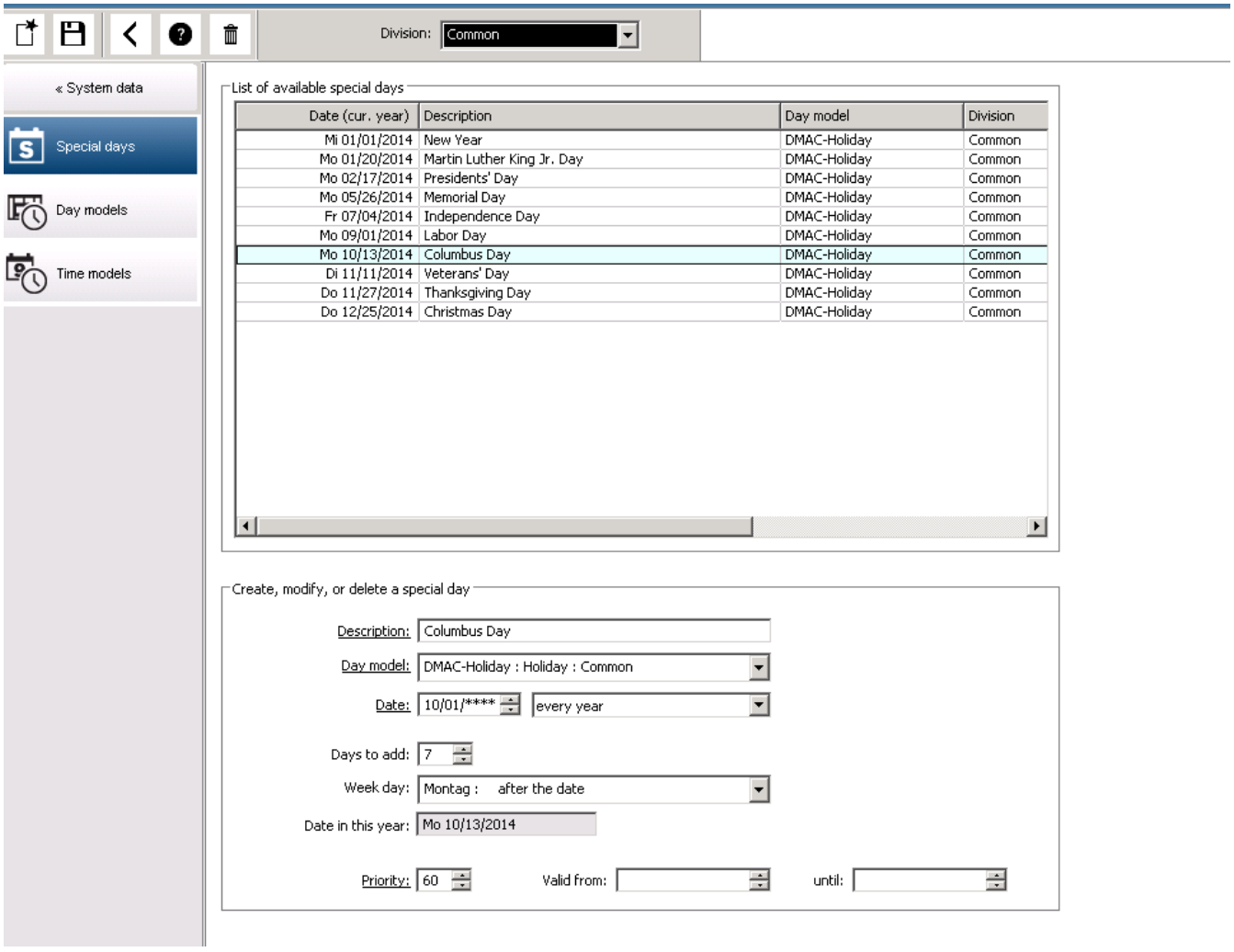






5.1 Definieren von speziellen Tagen

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.



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)	**.**.****

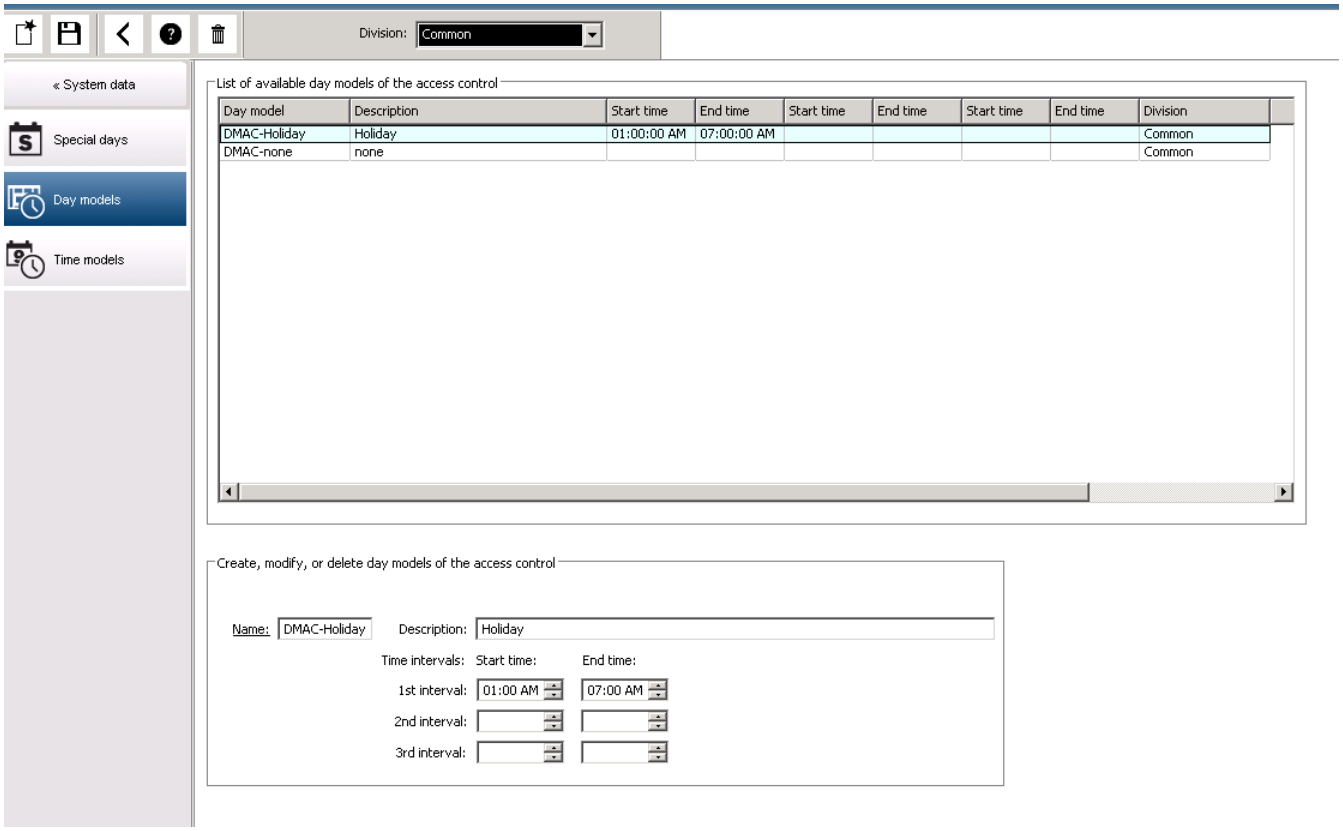
Für die von Ostern abhängigen Sondertage wird kein Datum angegeben, sondern der Abstand zum Ostersonntag in Tagen. Das Datum des Ostersonntags im laufenden Jahr wird im Feld **Date within this year (Datum in diesem Jahr)** angezeigt. Die Abweichung von diesem Datum wird im Feld **Days to add (abweichende 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:

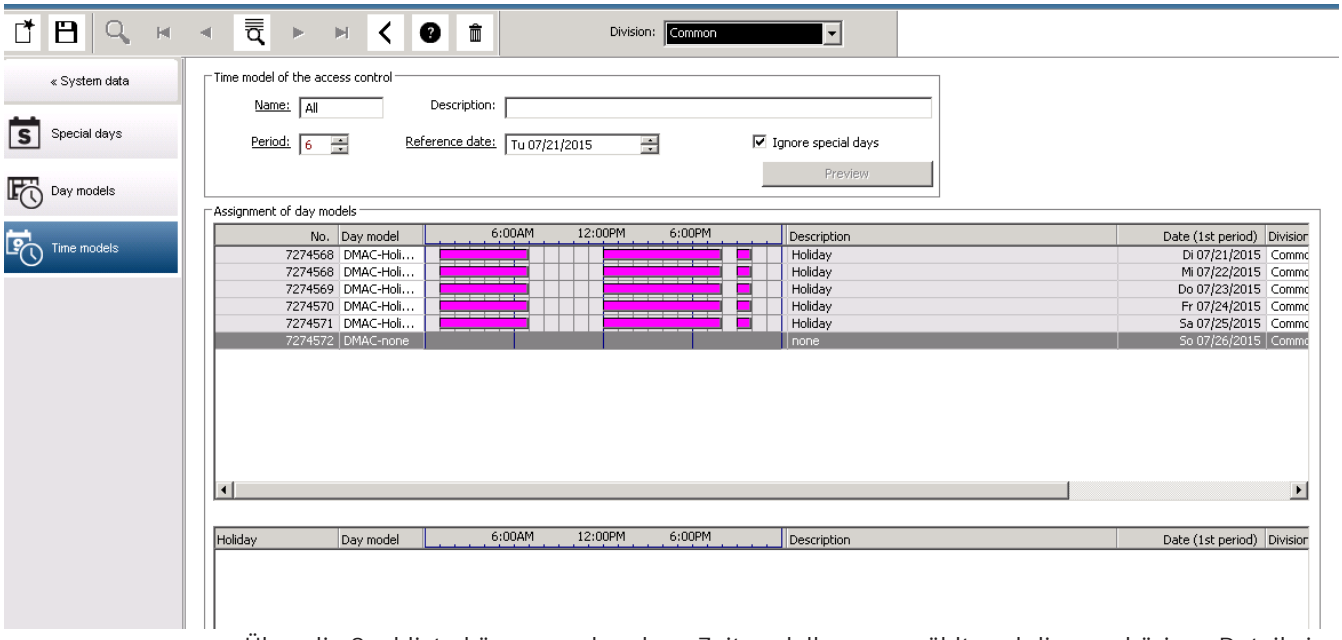
1. Intervall	von:	...	bis:	00:00 Uhr
2. Intervall	von:	00:00 Uhr	bis:	...

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.

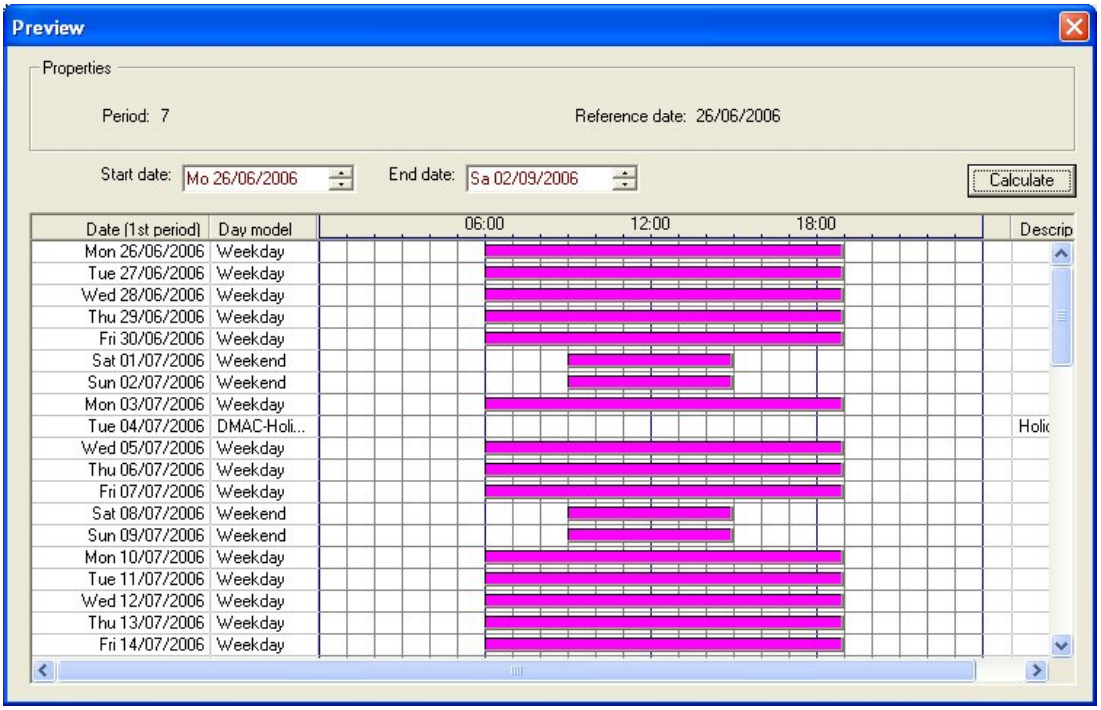
Ein Tagesmodell kann nur dann gelöscht werden, wenn es keinem Sondertag zugewiesen wurde und in keinem Zeitmodell verwendet wird.

5.3 Zeitmodelle definieren

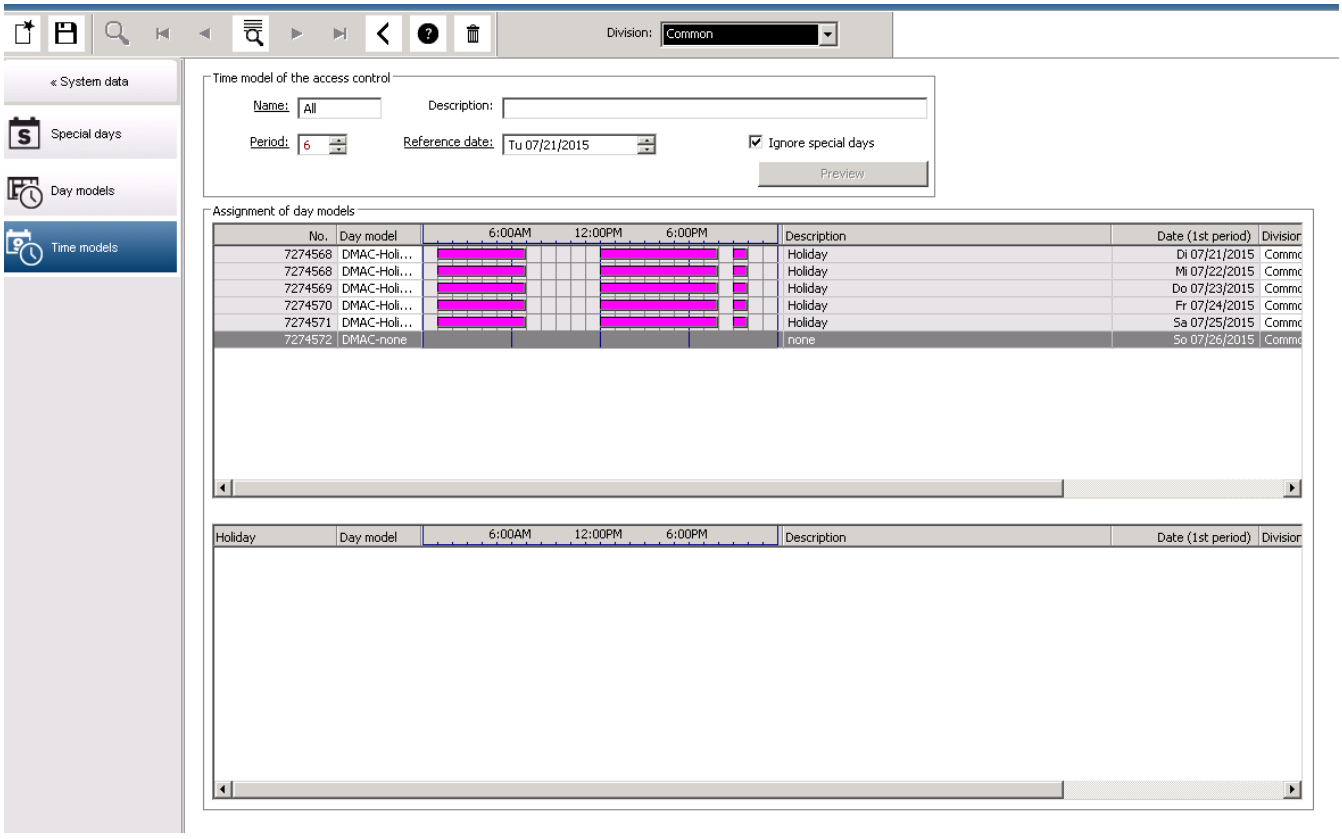


Über die Suchliste können vorhandene Zeitmodelle ausgewählt und die zugehörigen Details in den Dialogfensterfeldern angezeigt werden. Bei der Bearbeitung gilt das gleiche Verfahren wie beim Erstellen neuer Zeitmodelle.
Wenn die Maske leer ist, können Zeitmodelle neu angelegt werden. Hierzu müssen Sie 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
« System data
Special days
Day models
Time models
Time model of the access control
Name:
All
Description:
Period:
6
Reference date:
Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No.
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
Division
7274568 DMAC-Holi... Holiday Di 07/21/2015 Commc
7274568 DMAC-Holi... Holiday Mi 07/22/2015 Commc
7274569 DMAC-Holi... Holiday Do 07/23/2015 Commc
7274570 DMAC-Holi... Holiday Fr 07/24/2015 Commc
7274571 DMAC-Holi... Holiday Sa 07/25/2015 Commc
7274572 DMAC-none none So 07/26/2015 Commc
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

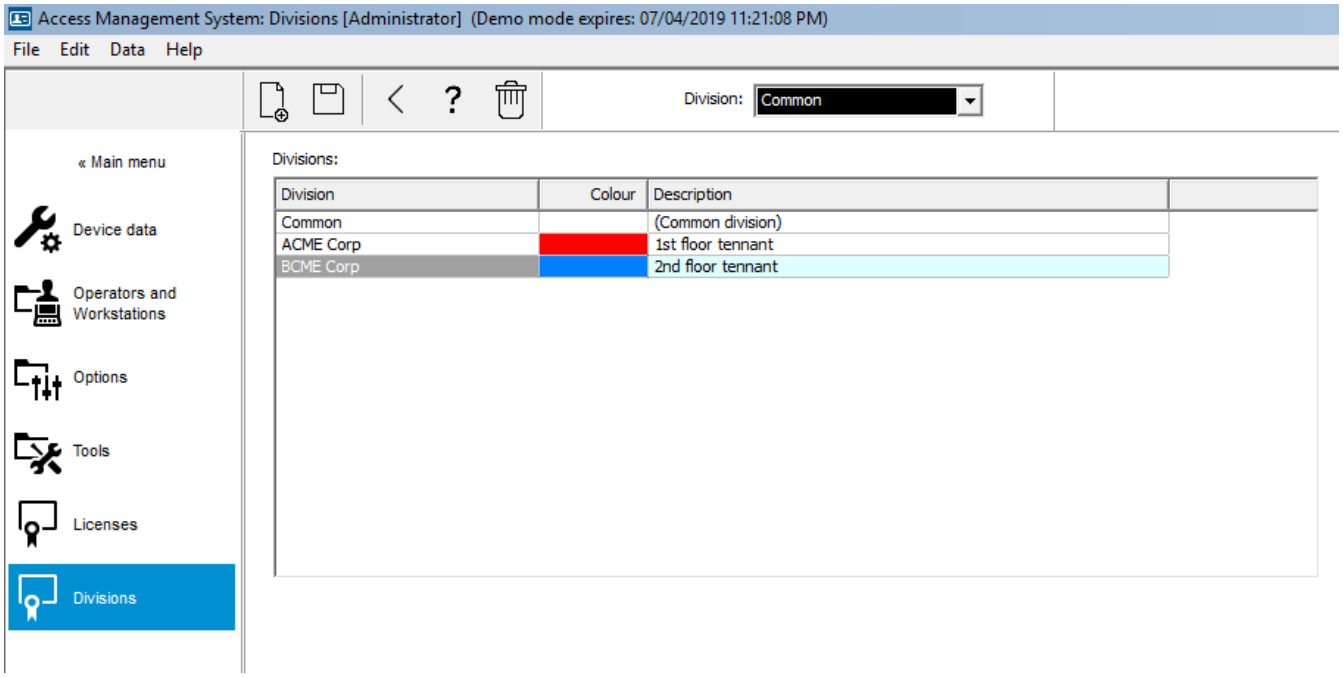
– Die Mandanten-Funktion ist für Ihre Installation lizenziert.

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  .



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 Netzwerkoptionen 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, das 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 ist ein Tool zum Hinzufügen, Löschen oder Ändern von Durchtritten und Geräten.

Der Geräteeditor bietet Ansichten für die folgenden bearbeitbaren Hierarchien:

- **Device configuration** (Gerätekonfiguration): die elektronischen Geräte innerhalb des Zutrittskontrollsystems.
- **Workstations** (Bedienstationen): die Computer, die im Zugangskontrollsystem zusammenarbeiten.
- **Areas** (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 Geräteeditor-Symbolleiste

Die Symbolleiste des Geräteeditors bietet die folgenden Funktionen, unabhängig davon, welche Ansicht aktiv ist: **Devices** (Geräte), **Workstations** (Bedienstationen) 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. **Alle nicht gespeicherten Änderungen werden verworfen.**
	Strg-S	Speichert die aktuelle Konfiguration

	Strg-F	Öffnet ein Suchfenster
		Öffnet den Baum **Device configuration** (Gerätekonfiguration)
		Öffnet den Baum **Workstations** (Bedienstationen)
		Öffnet den Baum **Areas** (Bereiche)

Beginnen Sie in allen Geräteeditor-Ansichten im Stammverzeichnis des Baums und fügen Sie Elemente über die Symbolleistenschaltflächen, das Menü oder das Kontextmenü der einzelnen Elemente hinzu (klicken Sie zum Aufrufen mit der rechten Maustaste). Um Unterelemente zu einem Gerät hinzuzufügen, wählen Sie zuerst das übergeordnete Gerät aus, unter dem die Unterelemente angezeigt werden sollen.

Kopieren und Einfügen von AMC-Geräten

So kopieren Sie AMC-Geräte von einem Teil des Baums in einen anderen:

1. Klicken Sie mit der rechten Maustaste auf das AMC-Gerät und wählen Sie im Kontextmenü die Option **Copy** (Kopieren) aus.
2. Klicken Sie mit der rechten Maustaste auf ein geeignetes übergeordnetes Gerät an einer anderen Stelle im Baum und wählen Sie im Kontextmenü die Option **Paste** (Einfügen) aus.
   - Das Gerät wird mit seinen Untergeräten und Einstellungen zur neuen Position kopiert.
   - Geräteparameter wie **IP-Adresse** und **Name**, die eindeutig sein müssen, werden **nicht** kopiert.
3. Geben Sie eindeutige Werte für die erforderlichen Geräteparameter ein. Erst nach der Eingabe kann der Gerätebaum gespeichert werden.

Speichern der Konfiguration

Wenn Sie mit dem Hinzufügen und Bearbeiten von Elementen im Baum fertig sind, klicken Sie auf **Save** (Speichern)  , um die Konfiguration zu speichern.

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

8.1 Konfigurationsmodi und Überschreibungen

Der Konfigurationsmodus ist der Standardzustand der Zutrittskontrollgeräte im Geräteeditor. Im Konfigurationsmodus können autorisierte Benutzer von AMS oder BIS ACE Änderungen für Geräte im Geräteeditor ausführen. ACS gibt diese Änderungen sofort an untergeordnete Geräte weiter.

Ein Bediener kann den Konfigurationsmodus **überschreiben**, indem er von außerhalb des Geräteeditors Befehle direkt an die Zutrittskontrollgeräte sendet. Dies ist beispielsweise häufig der Fall, wenn ein Bediener eingehende Meldungen und Alarme verarbeitet. Bis der Bediener den Befehl **Restore Configuration** (Konfiguration wiederherstellen) sendet, bleibt das Gerät im Betriebsmodus.

Wenn ein Konfigurationsbenutzer ein Gerät im Geräteeditor auswählt, während es sich im Betriebsmodus befindet, wird auf der Haupteigenschaftenseite des Geräts folgende Benachrichtigung angezeigt:

Dieses Gerät befindet sich nicht im Konfigurationsmodus.

Sie können Konfigurationsänderungen ausführen und speichern. Die Änderungen werden jedoch zwischengespeichert und erst dann wirksam, wenn der Alarmbetriebsmodus beendet und der Konfigurationsmodus wiederhergestellt wird.

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 Evakulierung 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 Zutrittswiederholsperre setzt voraus, dass es an den Durchtritten der Bereiche Durchtritt- und Ausgangsleser gibt.

Durchtritte 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.

Name	Der Standardname, den Sie überschreiben können.
Beschreibung	Eine Freitextbeschreibung des Gebiets.
Maximale Anzahl von Personen/Autos	Standardwert 0 (Null) für keine Begrenzung. 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.

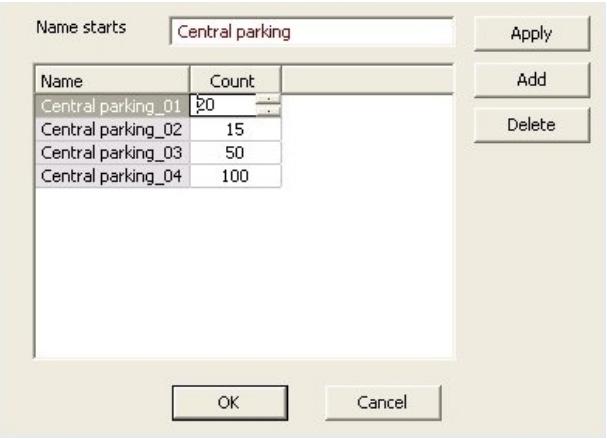
1. Klicken Sie auf einen Bereich in der Hierarchie, um ihn auszuwählen.
2. Klicken Sie auf **Delete** (Löschen)  oder klicken Sie mit der rechten Maustaste, um über das Kontextmenü zu löschen.

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.



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 Durchtritten für Parkplätze

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

Zur Überwachung der Belegung eines Parkplatzes sind zwei Durchtritte 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/Durchtritte/Geräte) 

Vorgehensweise

1. Erstellen Sie in der Gerätehierarchie einen AMC oder wählen Sie einen AMC aus, der keine abhängigen Durchtritte 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 Konfiguration von Einbruchmeldezentralen und -bereichen

Einführung

Das Zutrittskontrollsystem unterstützt die Verwaltung und Bedienung von Bosch Einbruchmeldezentralen. Weitere Informationen zu den unterstützten Modellen finden Sie im Datenblatt des Zutrittskontrollsystems. Durch das Zutrittskontrollsystem wird die Verwaltung von **Benutzern**der Einbruchmeldezentrale verbessert. Diese Benutzer sind eine Teilmenge der Ausweisinhaber des gesamten Zutrittskontrollsystems. Administratoren des Zutrittskontrollsystems erteilen diesen Ausweisinhabern über den AMS Dialog-Manager spezielle Berechtigungen für die Verwaltung und Bedienung der Einbruchmeldezentralen.
Die Einbruchmeldezentralen selbst werden wie zuvor über die Remote Programming Software (RPS) konfiguriert und aktualisiert. AMS liest kontinuierlich Daten aus der RPS-Datenbank und zeigt die enthaltenen Zentralen an.
AMS enthält Dialoge zum Erstellen von Zentralenbenutzern und ihren Berechtigungsprofilen und zur Verwaltung der Bereiche.

Voraussetzungen

- Die RPS der unterstützten Bosch Einbruchmeldezentralen wird auf einem separaten Computer im AMS-System installiert, **nicht** auf dem AMS-Server. Installationsanweisungen hierzu finden Sie im RPS-Installationshandbuch.
- RPS wurde mit den Einbruchmeldezentralen konfiguriert, die zum AMS Zutrittskontrollsystem gehören. Anweisungen hierzu finden Sie im RPS-Benutzerhandbuch oder in der Online-Hilfe.
- Die Uhren in den Zentralen befinden sich innerhalb von 100 Tagen der Uhr auf dem AMS-Server, um die automatische Synchronisierung zu unterstützen.
- Für alle angeschlossenen Zentralen ist das Modus-2-Protokoll festgelegt.
- Ausweise mit einer der folgenden Standardausweisdefinitionen:
  - HID 37 BIT -> Intrusion 37 BIT mit dem Einrichtungs-/Standortcode 32767 oder niedriger.
  - HID 26 BIT- > Intrusion 26 BIT
  - EM 26 BIT- > Intrusion 26 BIT

Übersicht

Der Konfigurationsprozess besteht aus den folgenden Phasen, die in den folgenden Abschnitten dieses Kapitels beschrieben werden:

1. Verbinden des Zutrittskontrollsystems mit den Einbruchmeldezentralen
   - Verbinden mit der RPS-API
   - Konfigurieren der Zentralenverbindungen
2. Erstellen von Zentralen-Berechtigungsprofilen, die regeln, welche Funktionen der angeschlossenen Zentralen verwendet werden können
3. Zuweisen von Zentralen-Berechtigungsprofilen zu Ausweisinhabern
   - Diese Ausweisinhaber werden somit Bediener für die Einbruchmeldezentralen.

10.1 Verbinden des Zutrittskontrollsystems mit den Einbruchmeldezentralen

Einführung

In diesem Abschnitt wird beschrieben, wie die Einbruchmeldezentralen angezeigt und für die Steuerung mit dem Map View verfügbar gemacht werden. Das Zutrittskontrollsystem stellt eine Verbindung mit einer RPS im Netzwerk her und verwaltet darüber eine aktuelle interne Liste der verfügbaren kompatiblen Einbruchmeldezentralen.

Dialogpfad

Hauptmenü > **Configuration** > **Panels** (Konfiguration > Zentralen) und Unterdialoge

10.1.1 Schritt 1: Verbinden mit der RPS-API

Die RPS-API ist eine Schnittstelle zu RPS, die auf einem separaten Computer ausgeführt wird. Schritt 1 dient zur Angabe der Adresse des Computers und der Anmeldeinformationen des Administrators für das Zutrittskontrollsystem.

Dialogpfad

Hauptmenü > **Configuration** > **Panels > RPS API configuration** (Konfiguration > Zentralen > RPS-API-Konfiguration)

Vorgehensweise

1. Geben Sie die folgenden Informationen ein:

Information	Beschreibung
Host name/IP address (Hostname/IP-Adresse)	Die HTTPS-Adresse des Computers, auf dem die RPS ausgeführt wird, und die Portnummer, über die die RPS kommuniziert. Die Standard-Portnummer ist *9000*.
User name (Benutzername)	Der Benutzername eines RPS-Administratorbenutzers für die API.
Password (Passwort)	Das Passwort des RPS-Administratorbenutzers.

2. Klicken Sie auf die Schaltfläche **Test the connection** (Verbindung testen), um sicherzustellen, dass die RPS ausgeführt wird und Benutzername und Passwort gültig sind.

10.1.2 Schritt 2: Konfigurieren der Zentralenverbindungen

In Schritt 2 wird festgelegt, wie viel Kontrolle das Zutrittskontrollsystem über einzelne Bereiche im Netzwerk hat.

Dialogpfad

Hauptmenü > **Configuration** > **Panels > Panel administration** (Konfiguration > Zentralen > Zentralenverwaltung)

Der Dialog zeigt eine Liste der kompatiblen Einbruchmeldezentralen, die die RPS-API für AMS bereitgestellt hat.

Die Liste wird regelmäßig im Hintergrund aktualisiert. Klicken Sie nach dem Öffnen des Dialogs gelegentlich auf  , um eine sofortige Aktualisierung manuell zu erzwingen.

Die Liste ist schreibgeschützt, mit Ausnahme der im folgenden Abschnitt beschriebenen Steuerelemente.

Vorgehensweise

Mithilfe der folgenden Steuerelemente können Sie die Steuerung einzelner Einbruchmeldezentralen durch das Zutrittskontrollsystem ermöglichen.

Spalte **User administration** (Benutzerverwaltung)	Aktivieren Sie das Kontrollkästchen, um sicherzustellen, dass die Benutzer der Einbruchmeldezentrale in dieser Zeile im Zutrittskontrollsystem und **nicht** in der Zentrale selbst verwaltet werden. **WICHTIG**: Diese Einstellung führt dazu, dass alle lokal in RPS erstellten Zentralenbenutzer überschrieben werden.
Spalte **Map View**	Aktivieren Sie das Kontrollkästchen, damit diese Zentrale für Steuerung und Kontrolle durch die Map View zur Verfügung steht.
 Einstellungen (Zahnrad-Symbol) in Spalte **Access Data** (Zutrittsdaten)	Wenn Sie das Kontrollkästchen in der Spalte **Map View** aktiviert haben, klicken Sie auf dieses Symbol, um einen Hostnamen oder eine IP-Adresse, einen Port und das Passwort für die jeweilige Zentrale einzugeben.
Schaltfläche **Delete selected panel** (Ausgewählte Zentrale löschen)	Wenn eine Zentrale in RPS gelöscht wurde, wird sie in der Liste mit dem Status **Removed** (Entfernt) angezeigt. Wählen Sie die Zentrale aus und klicken Sie auf diese Schaltfläche, um sie vollständig aus der Datenbank zu löschen.

10.2 Erstellen von Zentralen-Berechtigungsprofilen

Einführung

In diesem Abschnitt wird das Erstellen von Zentralen-Berechtigungsprofilen beschrieben. Ein Zentralen-Berechtigungsprofil ist ein benutzerdefinierter Satz von Berechtigungen für die Bedienung eines benutzerdefinierten Satzes von Einbruchmeldezentralen. Ein AMS-Administrator kann für die verschiedenen Verantwortlichkeiten verschiedener Gruppen von Ausweisinhabern mehrere Zentralen-Berechtigungsprofile erstellen.

Dialogpfad

Hauptmenü > **System data** > **Authorization profiles for intrusion panels** (Systemdaten > Berechtigungsprofile für Einbruchmeldezentralen)

Vorgehensweise

1. Klicken Sie auf  , um ein neues Profil zu erstellen.
2. (Obligatorisch) Geben Sie einen eindeutigen Namen für das Profil ein.
3. (Optional) Geben Sie eine Freitextbeschreibung für die Zentrale ein.
4. Klicken Sie unterhalb der Liste **Assigned panels** (Zugewiesene Zentralen) auf **Add...** (Hinzufügen...), um eine oder mehrere Zentralen aus einer Popup-Liste der im Netzwerk verfügbaren Zentralen hinzuzufügen.
   Wählen Sie umgekehrt eine oder mehrere Zentralen aus und klicken Sie auf **Remove** (Entfernen), um sie aus der Liste zu entfernen.
5. Klicken Sie auf eine Zentrale in der Liste **Assigned panels** (Zugewiesene Zentralen), um sie auszuwählen.
   – Im Bereich **Authorizations** (Berechtigungen) wird eine Liste mit allen Einbruchmeldebereichen angezeigt, die zur ausgewählten Zentrale gehören.

6. Wählen Sie in der Liste **Authorizations** (Berechtigungen) in der Spalte **Authority level** (Berechtigungsstufe) eine Berechtigungsstufe für jeden Einbruchmeldebereich der Zentrale aus, der in diesem Profil enthalten sein soll.
   – Die Berechtigungsstufen werden in RPS definiert und verwaltet. Sie können auch dort angepasst werden. Stellen Sie sicher, dass Sie die Definition der Berechtigungsstufe in RPS kennen, bevor Sie sie einem Profil zuweisen.
   – Standardmäßig ist **L1** die höchste Berechtigungsstufe. Die Stufen **L2**, **L3** usw. sind zunehmend eingeschränkt.
   – Wenn Sie ein Feld leer lassen, hat der Empfänger dieses Profils **keine** Berechtigung für den ausgewählten Einbruchmeldebereich der ausgewählten Zentrale.
7. Wiederholen Sie diesen Vorgang für alle Einbruchmeldebereiche aller Zentralen, die in dieses Profil aufgenommen werden sollen.
8. (Optional) Wählen Sie in der Liste **User group** (Benutzergruppe) eine Benutzergruppe der Zentrale aus, um die Berechtigungen auf bestimmte Zeiträume zu beschränken.
   – Die Benutzergruppen werden in RPS definiert und verwaltet. Sie können auch dort angepasst werden. Stellen Sie sicher, dass Sie die Definition der Benutzergruppe in RPS kennen, bevor Sie die Benutzergruppe einem Profil zuweisen.
9. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

10.3 Zuweisen von Zentralen-Berechtigungsprofilen zu Ausweisinhabern

Einführung

In diesem Abschnitt wird beschrieben, wie Sie unterschiedlichen Typen oder Gruppen von Ausweisinhabern verschiedene Berechtigungsprofile zuweisen.

Voraussetzung

Sie haben ein oder mehrere Zentralen-Berechtigungsprofile im Zutrittskontrollsystem definiert.

Dialogpfad

Hauptmenü > **Persons** > **Cards** (Personen > Ausweise)

Vorgehensweise

1. Suchen Sie in gewohnter Weise den gewünschten Ausweisinhaber in der Datenbank und wählen Sie ihn aus.
2. Klicken Sie auf die Registerkarte **Intrusion** (Einbruchmeldung).
3. Aktivieren Sie auf der Registerkarte **Intrusion** (Einbruchmeldung) das Kontrollkästchen **Panel user** (Zentralenbenutzer).
4. (Obligatorisch) Geben Sie im Feld **Passcode** (Passwort) ein Passwort ein, mit dem dieser Ausweisinhaber die Einbruchmeldezentrale bedienen wird.
   – Verwenden Sie ggf. die Schaltfläche, um ein nicht verwendetes neues Passwort zu generieren.
5. Wählen Sie in der Liste **ID card** (Ausweis) einen der Zutrittskontrollausweise aus, die diesem Ausweisinhaber zugewiesen sind.
6. (Optional) Geben Sie im Feld **Number of remote** (Remote-Anzahl) die Zahl ein, die auf dem Fernsteuerungsgerät des Ausweisinhabers für Einbruchmeldezentralen aufgedruckt ist.
7. Wählen Sie in der Liste **Language** (Sprache) die bevorzugte Sprache des Ausweisinhabers zum Lesen der Zentralendialoge aus.

8. Wenn der Ausweisinhaber die Bosch Smartphone-App für Einbruchmeldezentralen verwenden soll, aktivieren Sie das Kontrollkästchen **Remote access** (Fernzugriff).
9. Wählen Sie in der Liste **Authorization profile** (Berechtigungsprofil) ein geeignetes Zentralen-Berechtigungsprofil für den Ausweisinhaber aus.
10. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.
    – Dieses Zentralen-Berechtigungsprofil wird dem Ausweisinhaber mit allen zugehörigen Zentralen und Berechtigungen zugewiesen. Der Ausweisinhaber wird somit ein Bediener für die Einbruchmeldezentralen.

Beachten Sie, dass Sie die Datenfelder in diesem Dialog auch mit der Schaltfläche  verwenden können, um Ausweisinhaber in der Datenbank zu finden.

11 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)

11.1 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.

11.2 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.

11.3 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 **Assígned** (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.

11.4 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 Bedieners 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

11.5 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 Bedieners, 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	DerBediener 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 

11.6 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. Navigieren Sie im Menü des Dialog-Managers zu **File** > **Change password** (Datei > 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.
Bei der ersten Anmeldung nach einer Installation fordert Sie das System dazu auf, 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/

12 Konfigurieren von Ausweisen

12.1 Ausweisdefinition

Mit diesem Dialog können Sie die Ausweisdefinitionen aktivieren, deaktivieren, ändern oder hinzufügen, die von Ihrem Zutrittskontrollsystem verwendet werden sollen.

Dialogpfad

– AMS-Hauptmenü > **Configuration** > **Options** > **Card definition** (Konfiguration > Optionen > Ausweisdefinition)

Die folgenden Typen sind vom System vordefiniert und nicht modifizierbar:

– 32 Bit CSN - Standard MIFARE (32 bit)
– HID 26 - Standard Wiegand 26 bit code = active (**default**)
– HID 35 - HID corporate 1000
– HID 37 - HID 37 bit code - CN-H10304
– EM 26 - EM 26 Bit code
– Serial readers (AMC 4R4/LACi) - 64 bit
– HID 48 - HID corporate 1000
– 56 Bit CSN - Standard MIFARE Desfire

HID 26 ist der Standardausweistyp und erscheint in der Liste **Active card types** (Aktive Ausweistypen).

12.1.1 Erstellen und Ändern

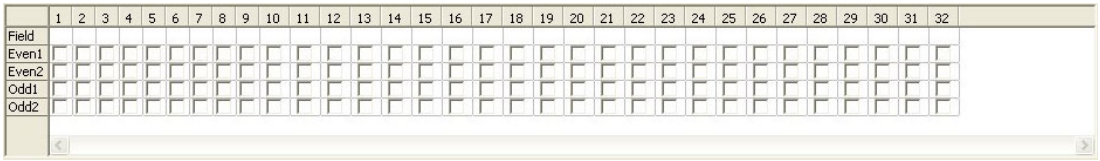
Klicken Sie über dem rechten Listenfeld auf die Schaltfläche ✚ (grünes +), um einen neuen Listeneintrag zu erstellen. Im Gegensatz zu vordefinierten Ausweistypen können die Daten neu erstellter Typen frei bearbeitet werden. Doppelklicken Sie auf die Felder **Name**, **Description** (Beschreibung) und **Number of Bits** (Anzahl Bits), um sie zu bearbeiten.
Der Name darf maximal aus 80 Zeichen und die Beschreibung aus maximal 255 Zeichen bestehen. Die Anzahl der Bits ist auf 64 begrenzt. (Wenn Sie eine größere Zahl eingeben, wird sie bei Verlassen des Felds auf den Maximalwert zurückgesetzt.)

Hinweis!
Mit den Bitlängen wird zwischen Wiegand Definitionen unterschieden. Aus diesem Grund muss jeder neuen Definition eine eindeutige Bitlänge zugeordnet werden, die von keiner anderen bestehenden Definition verwendet wird.

- Um ein Datenbit zu ändern, doppelklicken Sie auf das betreffende Feld. Wenn Sie ein Datenbit löschen möchten, markieren Sie es zunächst und klicken Sie anschließend auf die Schaltfläche ✕ (rotes X).

Hinweis!
Nur Ausweistypen, die vom Benutzer erstellt wurden, können geändert oder gelöscht werden.

Wenn Sie einen einzelnen Ausweistypen (in der linken oder rechten Liste) wählen, wird dessen Codierung im unteren Bereich des Dialogs angezeigt. Die Datenbits werden in 5 Zeilen und in der Anzahl von Spalten angezeigt, die der Anzahl der Bits in der Definition entspricht.



Jeder Spalte der Zeile **Field** (Field) kann eine Bezeichnung zugewiesen werden, die angibt, wie dieser Teil des Codes interpretiert werden muss. Die Bezeichnungen lauten wie folgt:

F	Kunde: Kennzeichnet den Codeteil für die Kundenzugehörigkeit	
C	Codenummer: Codeteil mit der individuellen Ausweisnummer	
E1	Gerade 1: Bit zum Ergänzen der ersten Maske mit gerader Parität	Mit der Auswahl dieser Werte wird das Kontrollkästchen für die entsprechende Zeile aktiviert.
E2	Gerade 2: Bit zum Ergänzen der zweiten Maske mit gerader Parität	
O1	Ungerade 1: Bit zum Ergänzen der ersten Maske mit ungerader Parität	
O2	Ungerade 2: Bit zum Ergänzen der zweiten Maske mit ungerader Parität	
1	Im Code enthaltene feste Bitwerte	
0		

Bei den Bezeichnungen E1, E2, O1 und O2 reicht es, das Kontrollkästchen der entsprechenden Zeile zu aktivieren. Das Kästchen in der Zeile **Field** (Feld) wird automatisch entsprechend aktiviert.

Erläuterung:

Das Signal, das ein Leser überträgt, wenn ein Ausweis eingelesen wird, setzt sich aus einer Reihe von Nullen und Einsen zusammen. Für jeden Ausweistyp ist die Länge dieses Signals (d. h. die Anzahl der Bits) genau definiert.

Neben den eigentlichen Benutzerdaten, die als Codedaten gespeichert sind, enthält das Signal auch Steuerungsdaten, um a) das Signal als Ausweissignal zu kennzeichnen und b) die fehlerfreie Übertragung zu überprüfen.

Im Allgemeinen sind die festen Nullen und Einsen nützlich, um den Signaltyp zu kennzeichnen. Die Paritätsbits, die als Prüfsumme ausgewählter Bits des Signals entweder null (gerade Parität) oder eins (ungerade Parität) ergeben müssen, werden zum Überprüfen der fehlerfreien Übertragung verwendet. Die Controller können so konfiguriert werden, dass eine oder zwei Prüfsummen für gerade Paritäten und eine oder zwei Prüfsummen für ungerade Paritäten berechnet werden.

In der Liste „control“ (Steuerung) können diese Bits in den jeweiligen Zeilen für die Paritätsprüfsummen (Even1, Even2, Odd1 und Odd2) gekennzeichnet werden, die in die Prüfsumme einbezogen werden sollen. In der obersten Zeile „Field“ (Feld) wird für jede verwendete Prüfsumme ein Bit definiert, um die Prüfsumme für den Paritätstyp zu ergänzen. Wenn eine Paritätsoption nicht verwendet wird, bleibt die entsprechende Zeile einfach leer.

12.1.2 Aktivieren/Deaktivieren von Ausweisdefinitionen

Bis zu 8 Ausweisdefinitionen können gleichzeitig aktiv sein. Die Definitionen, die aktiviert werden sollen, müssen in die linke Liste **Active Card Types** (Aktive Ausweistypen) verschoben werden. Markieren Sie hierzu auf der rechten Seite eine oder mehrere Definitionen, und klicken Sie auf die Schaltfläche mit dem Pfeil nach links (**<**).
Sie können höchstens vier Definitionen gleichzeitig verschieben. Sobald vier Definitionen zum Verschieben markiert worden sind, wird jede weitere Markierung vom Verschieben ausgeschlossen. Um der Liste **Active Card Types** (Aktive Ausweistypen) weitere Definitionen hinzuzufügen, müssen Sie eine oder mehrere Definitionen markieren und mithilfe der Schaltfläche mit dem Pfeil nach rechts (**>**) in die rechte Liste verschieben, sodass sie auf diese Weise deaktiviert werden.

Hinweis!
Um Leser mit L-Bus- oder BG900-Protokollen zu verwenden, aktivieren Sie den Ausweistyp **Serial Reader** (Serieller Leser). Dadurch wird der manuelle Eingabedialog **Dialog Bosch** für den Dialog-Manager des Zutrittskontrollsystems verfügbar.

12.1.3 Erstellen von Ausweisdaten im Dialog-Manager

Manuelle Dateneingabe
Für Wiegand und Bosch Ausweise werden verschiedene Eingabemethoden verwendet.
Für alle Wiegand Definitionen (HID 26, HID 35, HID 37 und 32 Bit CSN) können Sie im Dialogfeld **Dialog (Wiegand)** den **Customer code** (Kundencode) und die **Card no.** (Ausweisnummer) eingeben.
Für serielle Leser enthält das Dialogfeld **Dialog Bosch** zusätzliche Felder für **Version** und **Country code** (Ländercode).

Dateneingabe durch Bekanntmachungsleser
Neben der manuellen Dateneingabe kann jede Bedienstation mit einem Dialogleser zum Erfassen von Ausweisdaten ausgerüstet werden. Verwenden Sie einen Leser aus der Liste im folgenden Dialog:

– AMS-Hauptmenü > **Configuration** > **Options** > **Card reader** (Konfiguration > Optionen > Ausweisleser)

Wenn es sich bei dem ausgewählten Leser um einen Eingabeleser für Wiegand Ausweise handelt, werden alle aktiven Wiegand Ausweistypen zusammen mit dem Leser aufgeführt.

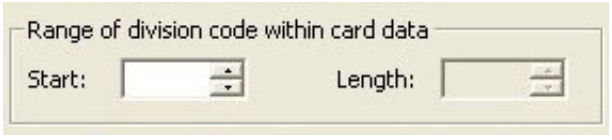
– AMS-Hauptmenü > **Personnel data** > **Cards** > Reader button > ▶ (right arrow) (Personaldaten > Ausweise > Leserschaltfläche > ▶ / Pfeil nach rechts).

Einer dieser Ausweistypen muss gewählt werden, um zu gewährleisten, dass die Ausweiscodierung richtig gespeichert wird. Dies bedeutet, dass der Leser selbst nicht direkt, sondern nur indirekt über die Auswahl der Wiegand Definition gewählt werden kann.
Wenn der erforderliche Ausweistyp nicht in der Pulldown-Liste angezeigt wird, müssen Sie ihn im Dialog für die Ausweisdefinition aktivieren.

– AMS-Hauptmenü > **Configuration** > **Options** > **Card definition** (Konfiguration > Optionen > Ausweisdefinition)

HITAG, LEGIC und MIFARE Bekanntmachungsleser können direkt aus der Liste ausgewählt werden.

Ausweisdefinition für Mandanten (Mandantenfähigkeit)
Wenn Sie die Mandantenfunktion für die Verwaltung mehrerer Parteien (auch „Mandanten“ genannt) in den zutrittskontrollierten Bereichen lizenziert haben, können Sie einen Codebereich auf dem Ausweis konfigurieren, mit dem der Bediener die Ausweise verschiedener Mandanten unterscheiden kann. Verwenden Sie die optionalen Felder (nur wählbar, wenn die Mandantenfunktion lizenziert wurde), um die Position des **Start**bits und die **Länge** der Mandantencodierung auf den Ausweisen zu definieren.



12.2 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
Eingeben von Zahlen im Dialog
Zur Vereinfachung können Sie Zahlen im Dezimal- oder Hexadezimalformat eingeben. Wählen Sie die Optionsfelder **Hexadecimal** (Hexadezimal) oder **Decimal** (Dezimal) entsprechend dem vom Ausweishersteller festgelegten Format aus.
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 Texteingabefelder, um Werte für **Version**, **Country code** (Ländercode) und **Facility code** (Kundencode) einzugeben, die der Ausweisnummer zugeordnet sind, wenn der Ausweis im System registriert ist. Wenn die Felder nicht ausgefüllt werden können, sind sie für keine der aktiven Ausweisdefinitionen relevant. Beim Bosch Code können alle Felder ausgefüllt werden.

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

Eingeben von Codedaten

Wenn die Daten vom Hersteller als Dezimalwerte bereitgestellt werden, wählen Sie das Optionsfeld „Decimal“ (Dezimal) aus und geben Sie die angegebenen Werte ein, z. B.:

Version: *2*

Country code (Ländercode): *99*

Facility code (Kundencode): *56720*

Klicken Sie auf **Apply** (Übernehmen), um die Daten zu speichern.

Hinweise zum Eingeben von Standard-Codedaten

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.

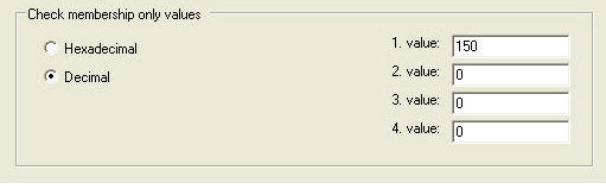
Hinweis!
Wird der Ausweis über einen angeschlossenen Dialogleser erfasst, werden die Standardwerte automatisch zugewiesen. Die Standardwerte können nicht überschrieben werden, wenn die Erfassung über einen Leser erfolgt.
Zum Überschreiben sollte der Erfassungstyp auf **Dialog** umgeschaltet werden.

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: 11D33E500000019F

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.

13 Konfigurieren der Controller

Einführung

Die Controller im Zutrittskontrollsystem sind die virtuellen und physischen Geräte, die Befehle an die periphere Hardware an Durchtritten (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

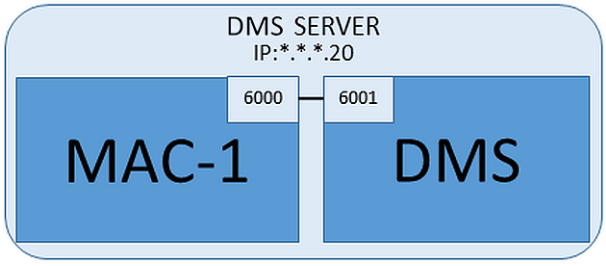
Die grundlegende Verwendung von DevEdit wird im Abschnitt **Verwenden des Geräteeditors** unter dem Link unten beschrieben.

Siehe

- *Verwenden des Geräteeditors, Seite 23*

13.1 Konfigurieren von MACs und RMACs

13.1.1 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 (Kontrollkästchen)	**<Leer lassen>**
RMAC-Port	**<Leer lassen>**
Aktiv (Kontrollkästchen)	**Deaktivieren** 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 (Kontrollkästchen)	**Deaktivieren** 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)	**WICHTIG:** 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.

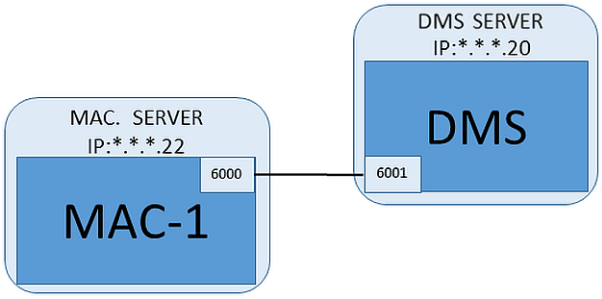
13.1.2 Vorbereiten von MAC-Servercomputern zum Ausführen von MACs und RMACs

In diesem Abschnitt wird die Vorbereitung von Computern für die Verwendung als MAC-Server beschrieben.
Standardmäßig wird der erste MAC in einem Zutrittskontrollsystem 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.
Damit ein Failover möglich ist, **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. Die Betriebssysteme aller MAC-Server müssen aktuell von Microsoft unterstützt werden. Außerdem müssen auf ihnen die jeweils aktuellen Updates installiert sein.
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: Auf den Betriebssystemen Windows 10 und Windows Server ist dies als Funktion aktiviert.
6. Starten Sie den Computer neu.

13.1.3 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. Klicken Sie auf dem DMS-Servercomputer im Geräteeditor
   – mit der rechten Maustaste auf den MAC und wählen Sie **Disable all LACs** (Alle LACs deaktivieren).
   – Deaktivieren Sie den MAC, indem Sie die Kontrollkästchen **Activate** (Aktivieren) und **Load devices** (Geräte laden) für diesen MAC deaktivieren.
2. Verwenden Sie auf dem MAC-Servercomputer das Windows-Programm *services.msc*.
   – Beenden Sie den MAC-Dienst **AUTO_MAC2**.
   – Legen Sie beim **Startup type** (Starttyp) dieses MAC-Diensts **Manual** (Manuell) fest.
3. Starten Sie die *MACInstaller.exe*
   – Für AMS befindet sich diese auf den AMS-Installationsmedien *\AddOns\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
3	**Destination Folder** (Zielordner)	Das lokale Verzeichnis, in dem der MAC installiert werden muss. Geben Sie nach Möglichkeit den Standardwert ein.
4	**Server**	Der Name oder die IP-Adresse des Servers, auf dem der DMS ausgeführt wird.
4	**Port (Port to DMS)** (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.

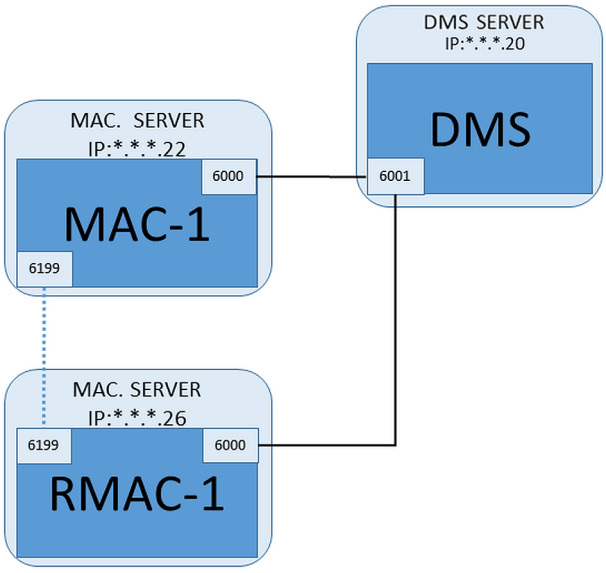
Bildschirmnr.	Parameter	Beschreibung
4	**Number (MAC System Number)** (Nummer [MAC-Systemnummer])	Legen Sie 1 für diesen und alle MACs fest (anders als bei RMACs).
4	**Twin (Name or IP address of partner MAC)** (Zwilling [Name oder IP-Adresse des Partner-MACs])	Lassen Sie dieses Feld leer, solange dieser MAC keinen RMAC haben soll.

5. Wählen Sie den MAC auf dem DMS-Server im Geräteeditor aus.
6. 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 Systembediener
With RMAC (Mit RMAC) (Kontrollkästchen)	**<Leer lassen>**
RMAC-Port	**<Leer lassen>**
Active (Aktiv) (Kontrollkästchen)	Kontrollkästchen jetzt aktivieren
Load devices (Geräte laden) (Kontrollkästchen)	Kontrollkästchen jetzt aktivieren
IP address (IP-Adresse)	Die IP-Adresse des MAC-Servercomputers.
Time zone (Zeitzone)	**WICHTIG:** Die Zeitzone des MAC und aller untergeordneten AMCs.
Division (Mandant)	(falls zutreffend) Der **Mandant**, zu dem der MAC gehört.

13.1.4 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
With RMAC (Mit RMAC) (Kontrollkästchen)	**Deaktivieren** Sie dieses Kontrollkästchen, bis Sie den entsprechenden RMAC auf dem redundanten Failover-Anschalteserver installiert haben.
Active (Aktiv) (Kontrollkästchen)	**Deaktivieren** 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.
Load devices (Geräte laden) (Kontrollkästchen)	**Deaktivieren** 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.

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.

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
With RMAC (Mit RMAC) (Kontrollkästchen)	**Selected** (Ausgewählt) Neben der Registerkarte **MAC** erscheint die neue Registerkarte **RMAC**.
RMAC-Port	*6199* (der statische Standardwert) Alle MACs und RMACs verwenden diesen Port, um zu überprüfen, ob ihre Partner aktiv und erreichbar sind.
Active (Aktiv) (Kontrollkästchen)	**Selected** (Ausgewählt) Dies ermöglicht die Synchronisierung zwischen diesem MAC und seinen untergeordneten Geräten.
Load devices (Geräte laden) (Kontrollkästchen)	**Selected** (Ausgewählt) 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
Name	Der Name, der im Gerätebaum angezeigt werden soll. Wenn der entsprechende MAC beispielsweise MAC-01 heißt, kann dieser RMAC RMAC-01 genannt werden.
Beschreibung	Optionale Dokumentation für Bediener der Zutrittskontrolle.
IP address (IP-Adresse)	Die IP-Adresse des RMAC.

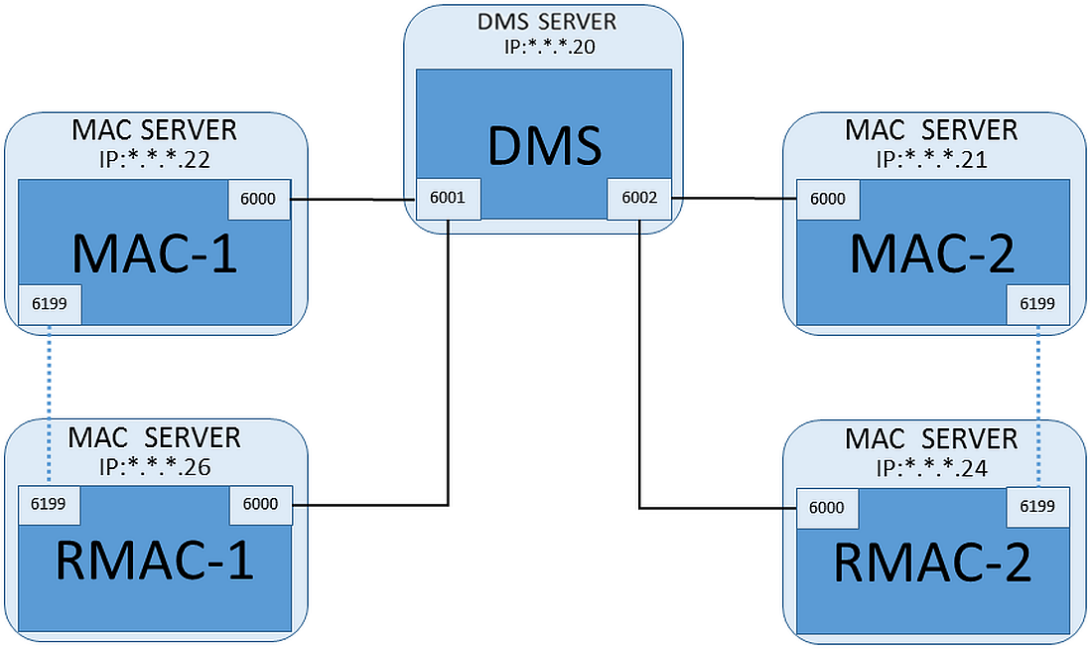
Parameter	Beschreibung
MAC Port (MAC-Port)	*6199* (der statische Standardwert) Alle MACs und RMACs verwenden diesen Port, um zu überprüfen, ob ihre Partner aktiv und erreichbar sind.

Siehe

– *Verwenden des MACInstaller-Tools, Seite 55*

13.1.5 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.

13.1.6 Verwenden des MACInstaller-Tools

MACInstaller.exe ist das Standardtool zum Installieren 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 Installationsmedium unter folgendem Pfad gefunden werden:

– *\AddOns\MultiMAC\MACInstaller.exe*

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

Bildschirmnr.	Parameter	Beschreibung
3	**Destination Folder** (Zielordner)	Das lokale Verzeichnis, in dem der MAC installiert werden muss.
4	**Server**	Der Name oder die IP-Adresse des Servers, auf dem der DMS ausgeführt wird.
4	**Port (Port to DMS)** (Port zu DMS)	Die Portnummer auf dem DMS-Server, der für die Kommunikation zwischen dem MAC und dem DMS verwendet wird. **Einzelheiten finden Sie unten.**
4	**Number (MAC System Number)** (Nummer [MAC-Systemnummer])	Stellen Sie 1 für alle ursprünglichen MACs ein. Stellen Sie 2 für alle redundanten Failover-MACs (RMACs) ein.
4	**Twin (Name or IP address of partner MAC)** (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.

Parameter: Port (Port to DMS) (Port (Port zu DMS))

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.
– Der DMS empfängt Signale vom ersten MAC oder MAC/RMAC-Paar am Port 6001, vom zweiten MAC oder MAC/RMAC-Paar am Port 6002 usw.

Parameter: Nummer (MAC-Systemnummer)
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.

Parameter: Nur konfigurieren (Optionsfeld)
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.

Parameter: Software aktualisieren (Optionsfeld)
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.

13.2 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 anzeigten 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.

AMC2 4W	**A**ccess **M**odular **C**ontroller mit vier Wiegand-Lesern.	Maximal vier Wiegand-Leser können für den Anschluss an bis zu vier Durchtritte konfiguriert werden. Der Controller unterstützt acht Eingangs- und acht Ausgangssignale. Bei Bedarf können mit Erweiterungen bis zu 48 zusätzliche Eingangs- und Ausgangssignale bereitgestellt werden.

AMC2 4R4	**A**ccess **M**odular **C**ontroller mit vier RS485-Leserschnittstellen	Maximal acht RS485-Leser können für den Anschluss an bis zu acht Durchtritte konfiguriert werden. Der Controller unterstützt acht Eingangs- und acht Ausgangssignale. Bei Bedarf können mit Erweiterungen bis zu 48 zusätzliche Eingangs- und Ausgangssignale bereitgestellt werden.
AMC2 8I-8O-EXT	Erweiterung für den AMC mit acht Eingangs- und Ausgangssignalen	Zusätzliche Signale werden bereitgestellt. Bis zu drei Erweiterungen können an einen AMC angeschlossen werden.
AMC2 16I-16O-EXT	Erweiterung für den AMC mit sechzehn Eingangs- und Ausgangssignalen	
AMC2 8I-8O-4W	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

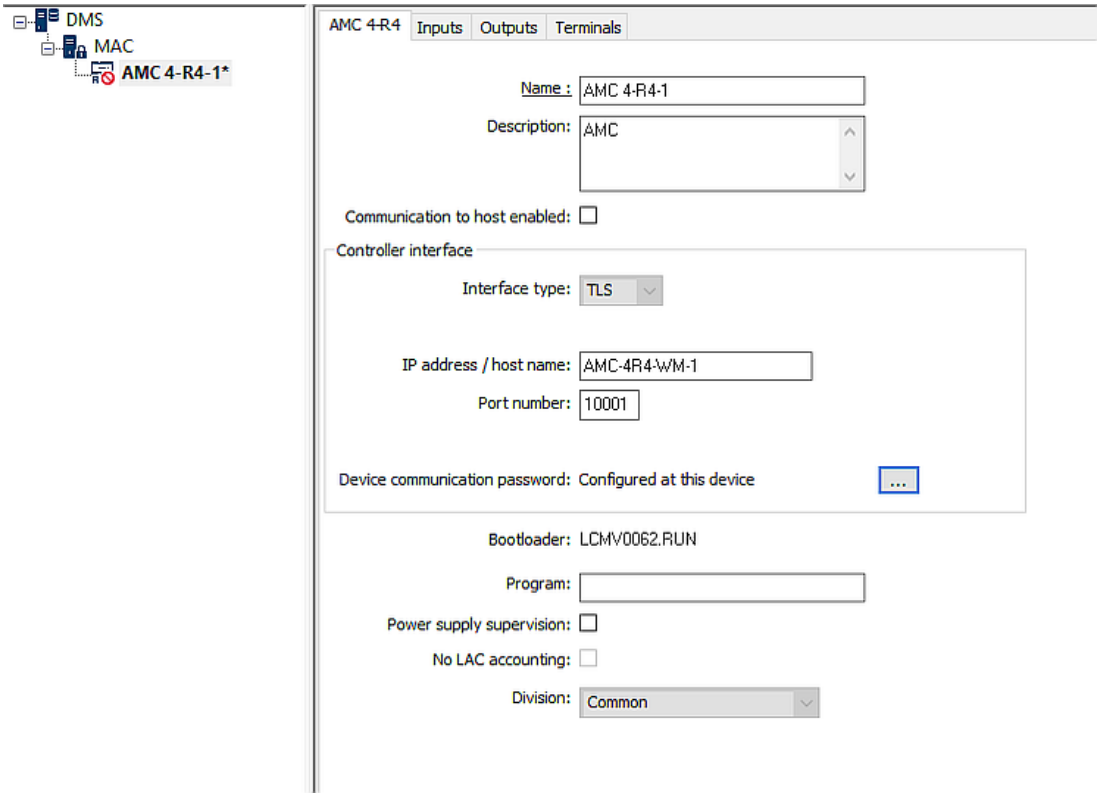
Zutrittskontrollsysteme werden in der Regel mit nur einem Typ von Controller und Leser ausgerüstet.

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.

13.2.1 AMC-Parameter und -Einstellungen

Allgemeine Parameter des AMC



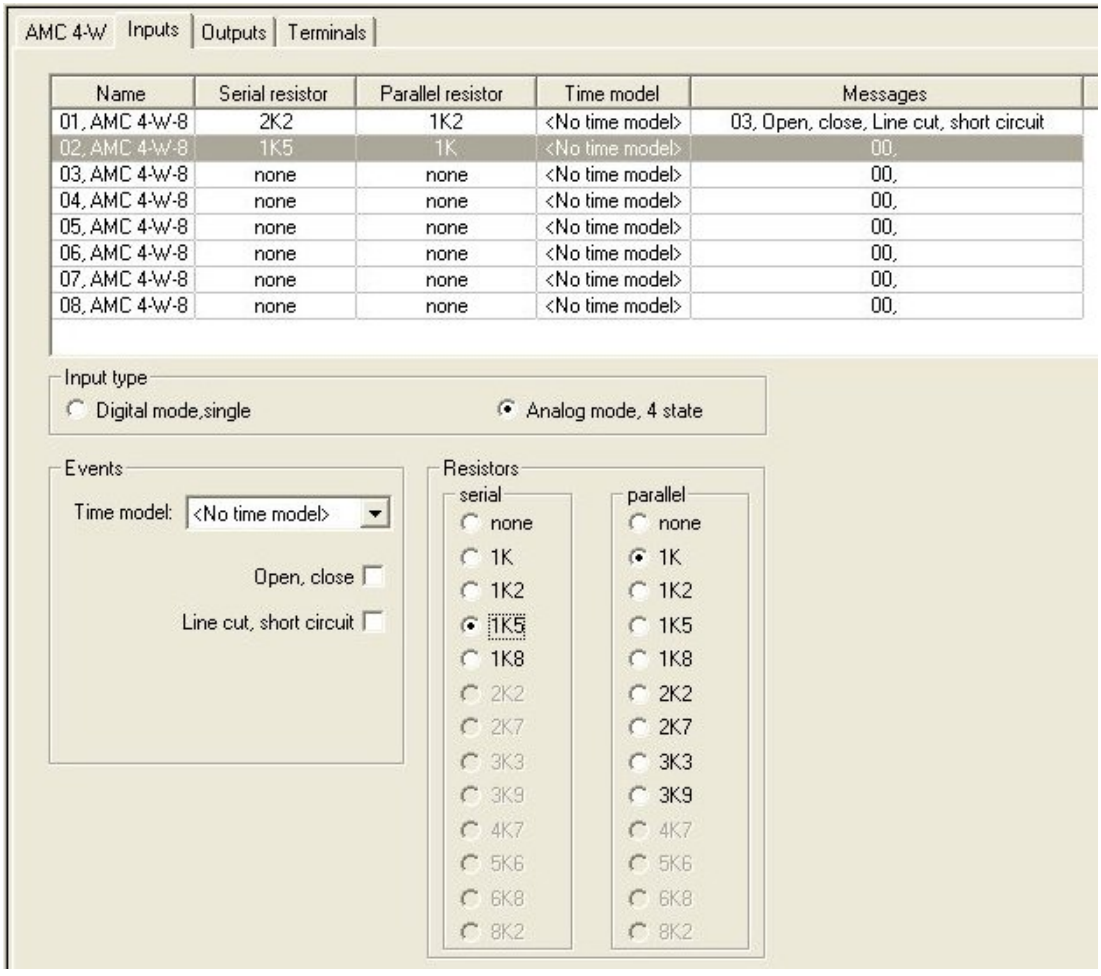
Konfiguration der AMC-Parameter

Parameter	Mögliche Werte	Beschreibung
Controllername	Alphanumerisch mit Einschränkungen: 1 – 16 Zeichen	ID-Generierung (Standard) gewährleistet eindeutige Namen, die jedoch von Benutzern überschrieben werden können. Wenn Sie einen Namen überschreiben, müssen Sie sicherstellen, dass die IDs eindeutig sind.
Controller description (Controllerbeschreibung)	Alphanumerisch: 0 – 255 Zeichen	Freitext.
Communication to host enabled (Schnittstelle zum Host aktiv)	0 = deaktiviert (Kontrollkästchen ist deaktiviert) 1 = aktiviert (Kontrollkästchen ist aktiviert)	Default (Standard) = aktiviert Overlay-Symbole auf den Controllern im Gerätebaum weisen auf den Status der Hostverbindung (aktiviert/deaktiviert) hin. Durch Deaktivieren des Kontrollkästchens wird das AMS vorübergehend offline geschaltet, was bei Neukonfiguration und Tests nützlich ist.

		Durch Aktualisieren des Zutrittskontrollsystems auf eine neue Version werden die Kontrollkästchen aller Controller automatisch deaktiviert. Aktivieren und deaktivieren Sie die Kontrollkästchen von AMCs, um sie einzeln in der aktualisierten Software zu testen.
		Aktivieren Sie das Kontrollkästchen, wenn Sie den Geräteeditor verwenden, um während der Top-down-Bereitstellung von DTLS ein DCP (Gerätekommunikationspasswort) auf dem AMC festlegen. Dies öffnet ein 15-Minuten-Zeitfenster für die Weitergabe des DCP an die AMCs. Deaktivieren und aktivieren Sie das Kontrollkästchen, um das Zeitfenster neu zu starten.
Controller-Schnittstelle		
Interface Type (Schnittstellentyp)	UDP TLS	UDP (User Datagram Protocol): Die Verbindung wird über das Netzwerk hergestellt und es wurde noch kein DCP (Gerätekommunikationspasswort) auf dem AMC festgelegt. TLS (Transport Layer Security): Wenn Sie ein DCP (Gerätekommunikationspasswort) für den AMC festgelegt haben, ist die Kommunikation mit dem MAC mit DTLS geschützt. Achten Sie bei UDP und TLS darauf, dass die DIP-Schalter 1 und 5 des AMC auf „ON“ (EIN) gesetzt sind.
IP Address/ Hostname (IP-Adresse/Hostname)	Netzwerkname oder IP-Adresse des AMC	Dieses Textfeld ist nur aktiv, wenn **UDP** als Porttyp festgelegt wurde. 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. Geben Sie bei Netzwerken ohne DHCP die IP-Adresse ein.
Port number (Port Nr.)	numerisch: 10001 (Standard)	Dies ist der AMC-Port, der die MAC-Meldungen empfängt.
Weitere Parameter		

Program (Programm)	Alphanumerisch	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. 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.
Power supply supervision (Überwachung der Stromversorgung)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	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. 0 = keine Überwachung 1 = Überwachung aktiviert
No LAC accounting (Keine LAC-Berücksichtigung)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (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. **Hinweis**: Wenn diese Option ausgewählt und der AMC offline ist, kann der AMC den Zutritt zu überfüllten Bereichen nicht verhindern, da er keinen Zugriff auf die Gesamtzahlen hat.
Division (Mandant)	Standardwert „Common“ (Allgemein)	Nur relevant, wenn die **Mandantenfunktion** lizenziert ist.

Konfigurieren von AMC-Eingängen



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 „Keine“ oder „---“ = Digitalmodus
Parallel resistor (Parallelwiderstand)	Anzeige des gesetzten Widerstandswerts für den Parallelwiderstand „Keine“ oder „---“ = Digitalmodus

Time model (Zeitmodell)	Name des gewählten Zeitmodells
Messages (Meldungen)	Ordnungsnummer und Bezeichnung der Meldungen, die generiert werden 00 = keine Meldungen 01 = wenn die Ereignisse **Open** (Offen), **close** (Geschlossen) aktiviert wurden 02 = wenn die Ereignisse **Line cut** (Leitungsbruch), **short circuit** (Kurzschluss) aktiviert wurden 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), C**losed** (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 (Tür geöffnet)	Summe der Serienwiderstandswerte (R_S) und Parallelwiderstandswerte (R_P): $R_S + R_P$
Door closed (Tür geschlossen)	Entspricht den Serienwiderstandswerten: R_S
Circuit break (Leitungsbruch)	Summe der Serienwiderstandswerte (R_S) und Parallelwiderstandswerte (R_P) geht gegen unendlich.
Short-Circuit (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)

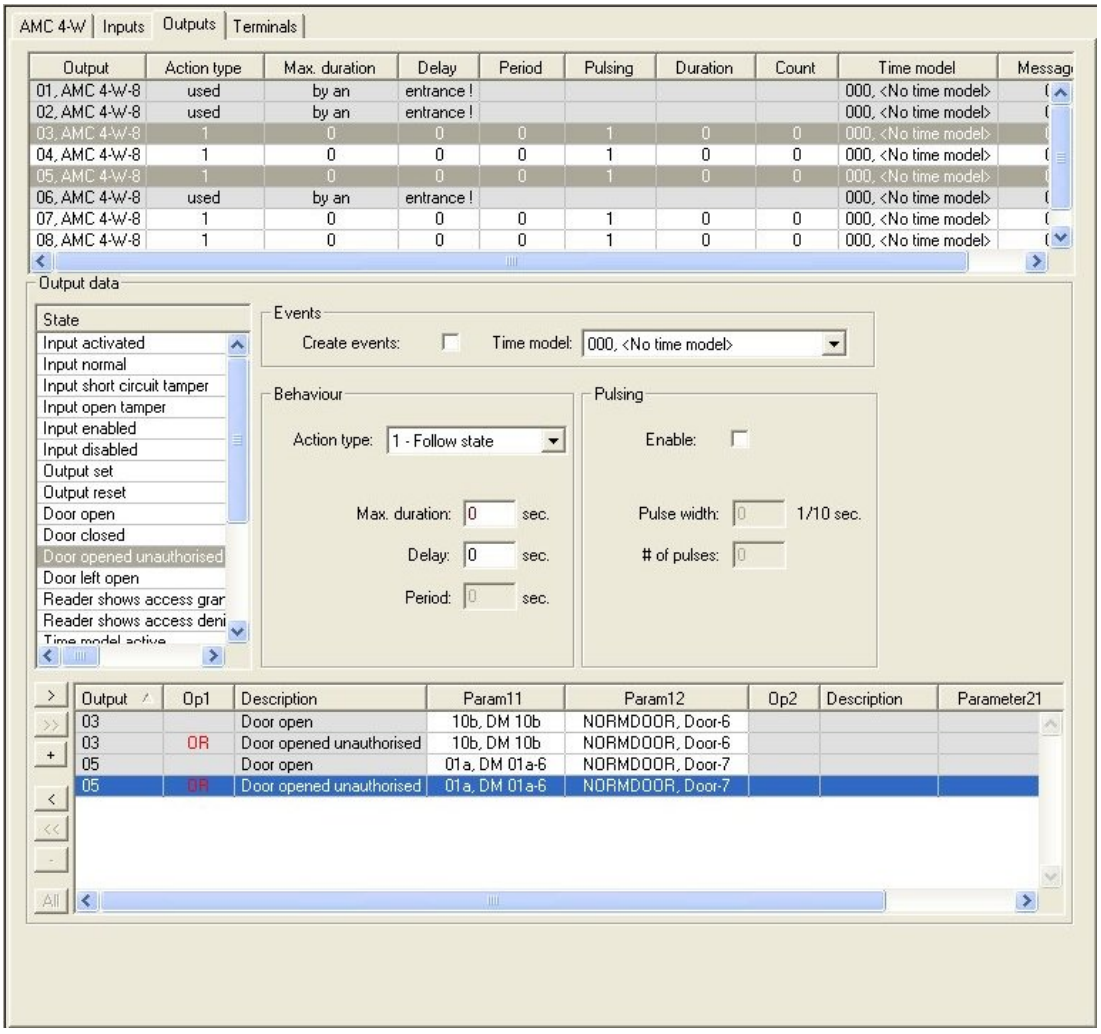
Abhängig vom gewählten Widerstandswert sind für den entsprechenden Widerstand nur eingeschränkte Bereiche verfügbar.
In den folgenden Tabellen werden in der linken Spalte die gewählten Werte und in der rechten Spalte die verfügbaren Bereiche des anderen Widerstands angezeigt.

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

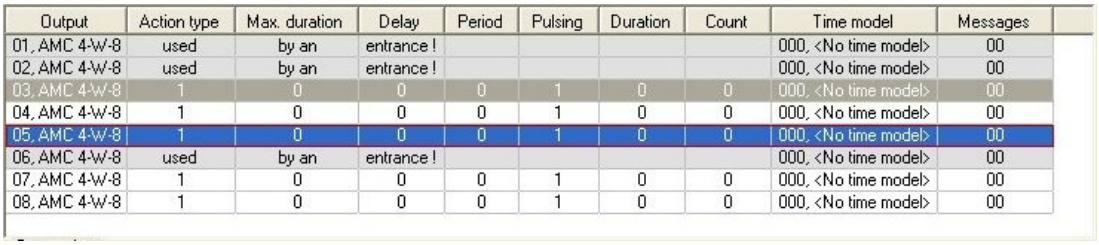
Auf dieser Dialogseite können Sie jeden Ausgang eines AMC oder AMC-EXT konfigurieren.
Diese Seite setzt sich aus drei Hauptbereichen zusammen:

- 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.



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.

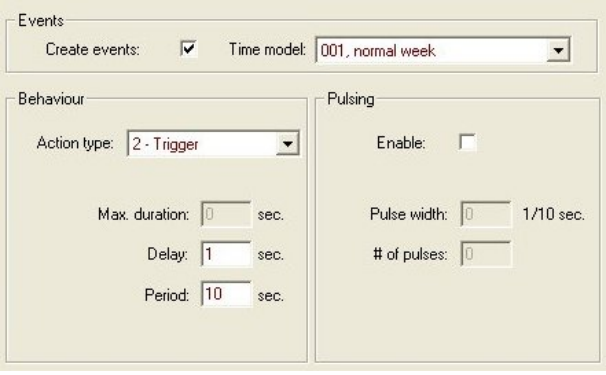
Parameter von AMC-Ausgängen

Spaltenname	Beschreibung
Ausgang	Aktuelle Nummerierung der Ausgänge am jeweiligen AMC oder AMC-EXT

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

Ausgänge: Ereignisse, Aktion, Impuls

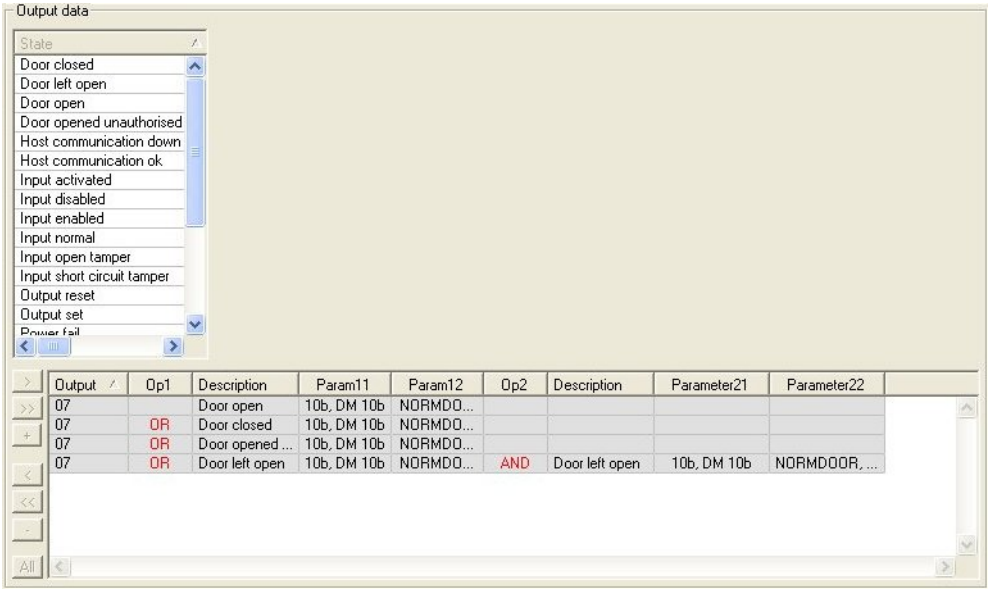
Alle Einträge aus der obigen Liste werden mithilfe von Kontrollkästchen und Eingabefeldern in den Bereichen **Events** (Ereignisse), **Action** (Aktion) und **Pulsing** (Impuls) des Dialogs generiert. Wenn Sie einen Listeneintrag wählen, werden die jeweiligen Einstellungen in diesen Bereichen angegeben. 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 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.

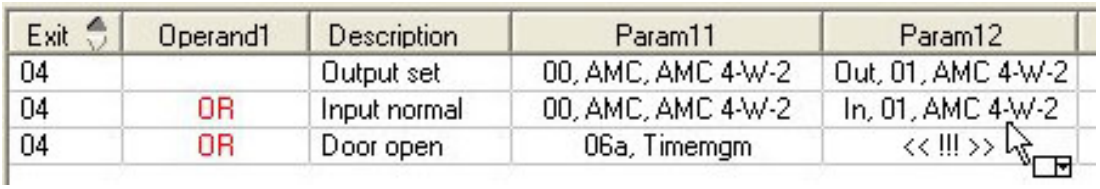
Nachdem einem Gerät oder einem System ein Status zugewiesen wurde, kann er auch allen anderen vorhandenen Geräten und Systemen zugewiesen werden.

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

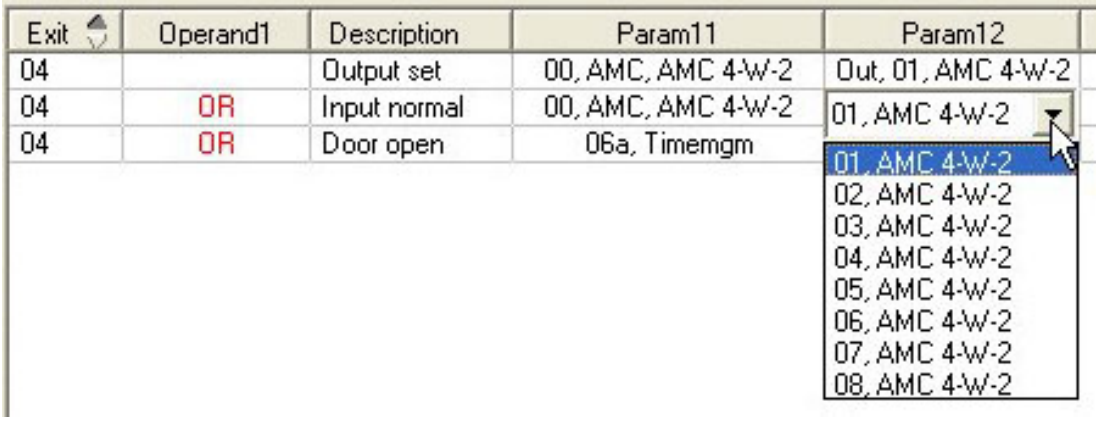
Modifizieren der Parameter von Ausgängen

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

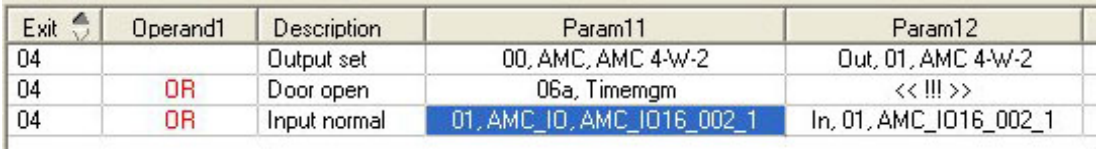
In den Spalten **Param11** (Parameter11) und **Param21** (Parameter21) (mit AND-Verknüpfungen) werden die Geräte (beispielsweise AMC, Durchtritt) angezeigt. Die Spalten **Param12** (Parameter12) und **Param22** (Parameter22) enthalten Sondersysteme (zum Beispiel Eingangssignal, Tür, Leser).
Wenn mehrere Geräte (beispielsweise E/A-Platinen) oder Systeme (beispielsweise Zusatzsignale, Zusatzleser) vorhanden sind, ändert sich der Mauszeiger, während Sie auf diese Spalte zeigen.



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



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



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.

State (Zustand)	**Type** (Typ)	**Beschreibung**
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

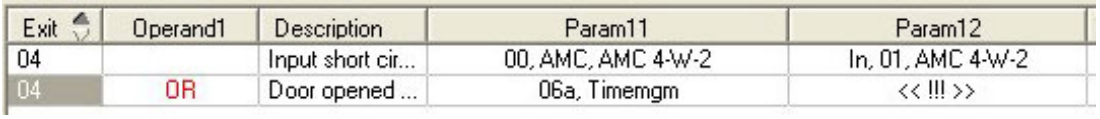
Reader shows access granted (Leser zeigt „Zutritt gewährt“)	13	Adresse des Lesers
Reader shows access denied (Leser zeigt „Zutritt verwehrt“)	14	Adresse des Lesers
Time model active (Zeitmodell aktiv)	15	Konfiguriertes Zeitmodell
Tamper reader (Leser Sabotage)	16	Adresse des Lesers
Tamper AMC (AMC, Sabotage 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 (Host-Kommunikation ok)	21	---
Host communication down (Host-Kommunikation gestört)	22	---
Message from reader (Meldung von Leser)	23	Adresse des Lesers
Message from LAC (Meldung von LAC)	24	Platinennummer
Card control (Ausweissteuerung)	25	Adresse des Lesers, Funktion zur Ausweissteuerung

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 ein externes Gerät durch die Signale **Input short circuit tamper** (Eingang kurzgeschlossen) und **Door opened unauthorized** (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 das externe Gerät 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

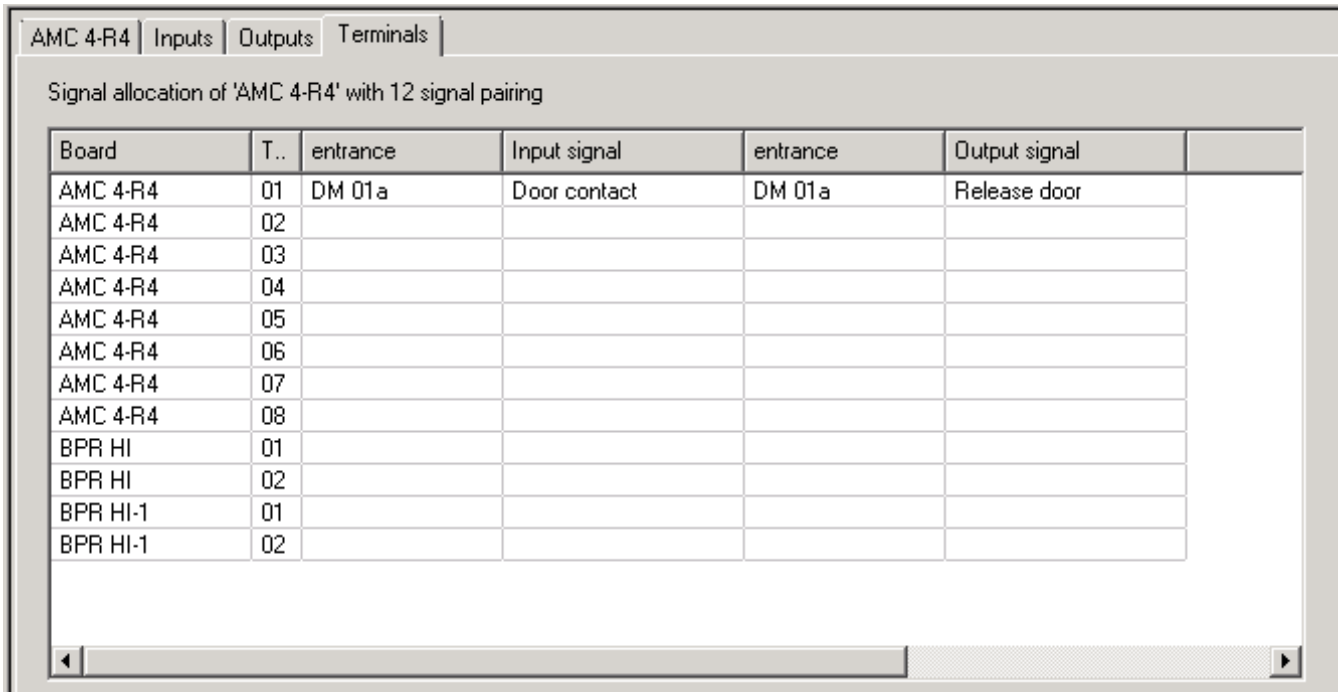
Liste aller vorhandenen Zustände mit den Standardwerten für die Parameter 11/21 und 12/22:

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.



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				

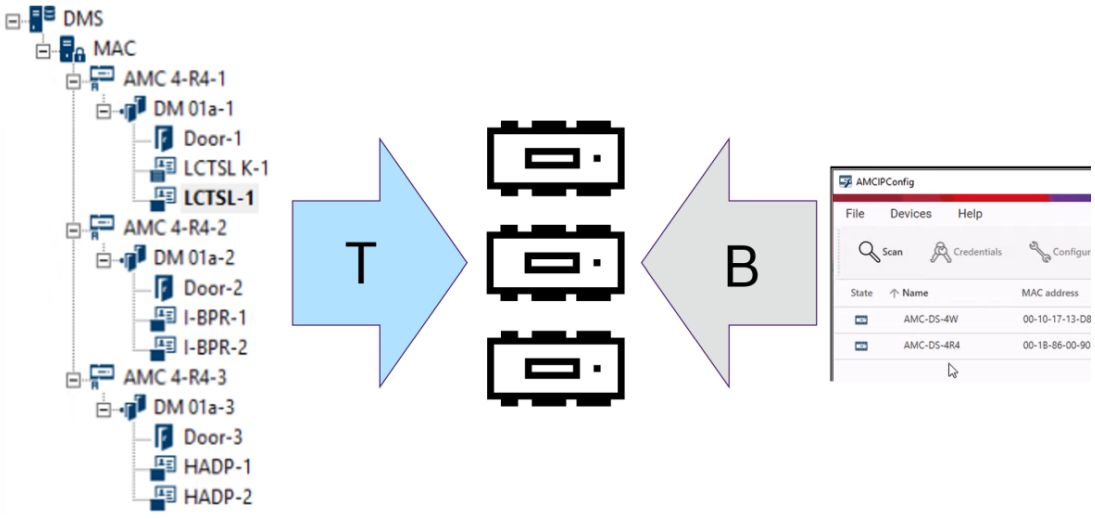
14 Konfigurieren von DTLS für sichere Kommunikation

Einführung

Das Zutrittskontrollsystem (ACS) ermöglicht eine äußerst sichere, DTLS-geschützte Kommunikation zwischen Geräten. Es gibt prinzipiell zwei Möglichkeiten, um die DTLS-Kommunikation zwischen Geräten im ACS bereitzustellen:

Top-down-Bereitstellung (T) erfolgt im Geräteeditor im ACS.

Bottom-up-Bereitstellung (B) erfolgt hauptsächlich im AMCIPConfig-Tool, erfordert aber zur Fertigstellung den Geräteeditor.



- (T) Top-down-Bereitstellung kann im Geräteeditor auf zwei Arten erfolgen:
  - Verwenden eines einzigen Gerätekommunikationspassworts (DCP) auf der DMS-Ebene für alle AMCs
  - Verwenden mehrerer DCPs für verschiedene Zweige des Gerätebaums, beginnend mit ihren jeweiligen MACs oder AMCs
- (B) Bottom-up-Bereitstellung kann ebenso auf zwei Arten im AMCIPConfig-Tool initiiert werden:
  - Verwenden eines AMC-Hardwareschlüssels
  - Verwenden eines zufälligen LCD-Schlüssels

Hinweis!

Die Bottom-up-Bereitstellung erfordert trotzdem das Festlegen von DCPs im Geräteeditor. Bei der Bottom-up-Bereitstellung können Sie ein DCP auf dem AMC-Gerät festlegen. Sie müssen trotzdem dasselbe DCP auf demselben AMC im Geräteeditor festlegen, um eine vollständige DTLS-Kommunikation zwischen dem MAC und AMC zu ermöglichen.

Zusammenfassung der DTLS-Bereitstellungsoptionen

	Kurzbeschreibung	Vorteile	Nachteile
Top-down	Der Systemadministrator gibt ein starkes Passwort im **Geräteeditor** ein. Basierend auf diesem Passwort erzeugt das System einen **Masterschlüssel**, den es top-down (von oben nach	Schnelle, einfache Bereitstellung.	Während der Weitergabe des Masterschlüssels an die AMC-Türcontroller ist die

	Kurzbeschreibung	Vorteile	Nachteile
	unten) durch den Gerätebaum mit Zutrittskontrollgeräten weitergibt, vom DMS über die MACs bis hin zu den AMC-Türcontrollern. Sie können ein Passwort für den gesamten Gerätebaum oder verschiedene Passwörter für verschiedene Zweige des Gerätebaums festlegen.		Gerätekommunikation nicht durch DTLS geschützt.
Bottom-up mit AMC-Hardware schlüssel	Der Systemadministrator verwendet das **AMCIPConfig**-Tool, um DTLS auf der Ebene der AMC-Türcontroller bereitzustellen.	Größere Differenzierung und Flexibilität bei der Bereitstellung. Bei dieser Methode wird der größte Nachteil der Top-down-Bereitstellung vermieden, nämlich die zeitweise ungeschützte Kommunikation des Masterschlüssels. Es ist trotzdem erforderlich, dass die Verbindung des AMCIPConfig-Tools zum AMC sicher ist, wenn das DCP festgelegt wird.	In der Zeit, in der das IPConfig-Tool das DCP auf dem AMC festlegt, müssen Sie die sichere Kommunikation auf andere Weise sicherstellen. Sie können beispielsweise den AMC direkt mit dem Computer verbinden, auf dem das IPConfig-Tool ausgeführt wird. Im IPConfig-Tool festgelegte DCPs müssen ebenfalls über den Geräteeditor auf denselben AMCs festgelegt werden.
Bottom-up mit zufälligem LCD-Schlüssel		Größere Differenzierung und Flexibilität bei der Bereitstellung. Höchste Sicherheit, da der LCD-Schlüssel nicht über das Netzwerk übermittelt wird, weshalb die Weiterleitung von Zugangsdaten jederzeit geschützt ist.	Kompliziertere und zeitaufwändigere Bereitstellung. Sie müssen den zufälligen 27-stelligen LCD-Schlüssel ohne Verwendung eines Netzwerks an das IPConfig-Tool übertragen.
Details und Anweisungen finden Sie in den folgenden Abschnitten dieses Kapitels.			

DTLS-Terminologie

DCP (Gerätekommunikationspasswort)	Ein einziges sicheres Passwort, aus dem ACS einen internen Masterschlüssel erzeugt. Das Passwort muss notiert und an einem sicheren Ort aufbewahrt werden, da es nicht im ACS gespeichert wird.
Masterschlüssel	Ein Code, den das System aus dem DCP erzeugt und der zum Schutz der Zutrittskontrollgeräte verwendet wird. Der Masterschlüssel wird keinem Benutzer jemals angezeigt.
Zufälliger LCD-Schlüssel	Ein temporärer alphanumerischer Code, den der AMC bei jedem Bootvorgang neu erzeugt. Der Schlüssel kann im LC-Display des AMC angezeigt und von Softwaretools zur Authentifizierung der Netzwerkkommunikation angefordert werden.
AMC-Hardwareschlüssel	Ein interner Authentifizierungscode, den der AMC aus bestimmten Hardwareparametern erzeugt. Er wird Benutzern nicht angezeigt.

14.1 Top-down-DTLS-Bereitstellung

Voraussetzungen

- AMS 4.0 oder BIS-ACE 4.9.1 oder höher.
- Der Baum mit Zutrittskontrollgeräten von DMS zu AMCs ist physisch eingerichtet und mit dem Netzwerk verbunden, aber die AMCs sind nicht aktiviert. „Aktiviert“ bedeutet, dass die Kontrollkästchen **Communication to host enabled** (Kommunikation mit Host aktiviert) der AMCs aktiviert sind.
- DTLS wurde auf den AMCs noch nicht durch eine der Bottom-up-Methoden über das IPConfig-Tool konfiguriert.

Vorgehensweise: ein DCP für alle

1. Starten Sie im ACS den Geräteeditor.
   - AMS-Hauptmenü > **Configuration** > **Device data** > **Device tree** (Konfiguration > Gerätedaten > Gerätebaum) 
   - Es wird ein Dialogfenster angezeigt, in dem Sie ein starkes Gerätekommunikationspasswort (DCP) eingeben können.
2. Um einen einziges DCP für alle AMCs im Gerätebaum festzulegen, geben Sie ein sicheres Passwort gemäß Ihren lokalen Passwortrichtlinien ein und bestätigen Sie es.
   - Das Dialogfenster zeigt die Passwortstärke basierend auf der Passwort-Entropie an.
3. Notieren Sie sich das Passwort sorgfältig und bewahren Sie es an einem sicheren Ort auf, da es nicht im ACS gespeichert wird.
4. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Alternative Vorgehensweise: Mehrere DCPs für verschiedene Zweige des Gerätebaums

1. Starten Sie im ACS den Geräteeditor.

– AMS-Hauptmenü > **Configuration** > **Device data** > **Device tree** (Konfiguration > Gerätedaten > Gerätebaum) 
– Es wird ein Dialogfenster angezeigt, in dem Sie ein starkes Gerätekommunikationspasswort (DCP) eingeben können.
2. Klicken Sie auf **Cancel** (Abbrechen), um verschiedene DCPs für verschiedene Zweige des Gerätebaums (MACs und AMCs) festzulegen.
– Ein Popup-Dialogfenster zeigt an, wie viele AMCs im System noch nicht über ein DCP verfügen.
– Der Gerätebaum wird im Geräteeditor geöffnet.
3. Klappen Sie den Gerätebaum aus, um den MAC oder AMC auszuwählen, für den Sie ein DCP festlegen möchten.
– Wenn Sie das DCP auf einer MAC-Ebene festlegen, wird es für alle untergeordneten AMCs des MAC festgelegt.
– Wenn Sie das DCP auf einer AMC-Ebene festlegen, wird es nur für diesen AMC festgelegt.
4. Klicken Sie auf die Schaltfläche mit den Auslassungspunkten … neben dem Textfeld **Device communication password** (Gerätekommunikationspasswort):
5. Geben Sie ein sicheres Passwort gemäß Ihren lokalen Passwortrichtlinien ein und bestätigen Sie es.
6. Notieren Sie sich das Passwort und seinen zugehörigen Zweig sorgfältig, da dies nicht im ACS gespeichert wird.
7. Wiederholen Sie diesen Vorgang für jeden MAC oder AMC, für den Sie ein separates DCP festlegen möchten.
8. Klicken Sie auf **OK**, um das Dialogfenster zu schließen.

Ergebnis der Top-down-Bereitstellung

Das ACS verwendet das DCP oder die DCPs, um interne Schlüssel für alle AMCs unterhalb des ausgewählten DMS oder MAC zu erzeugen.

Sie müssen diesen Vorgang nur wiederholen, wenn Sie das DCP nachträglich auf einem oder mehreren AMCs mithilfe des AMCIPConfig-Tools ändern (siehe „Bottom-up-Bereitstellung“). In diesem Fall müssen Sie sofort dasselbe DCP top-down (von oben nach unten) auf denselben AMCs im Geräteeditor festlegen.

Wenn Sie später im Gerätebaum Geräte unterhalb von DMSs und MACs hinzufügen, die bereits über DCPs verfügen, erben die neuen Geräte automatisch dasselbe DCP von den ihnen übergeordneten Geräten.

15 Konfigurieren von Durchtritten

15.1 Durchtritte – 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:

a	Leser für eingehenden **und** ausgehenden Verkehr
b	Leser für eingehenden Verkehr und Ausgangsdrucktaste
c	Eingangs- **ODER** Ausgangsleser (nicht beides – dies wäre Variante **a**)
r	(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.

15.2 Erstellen von Durchtritten

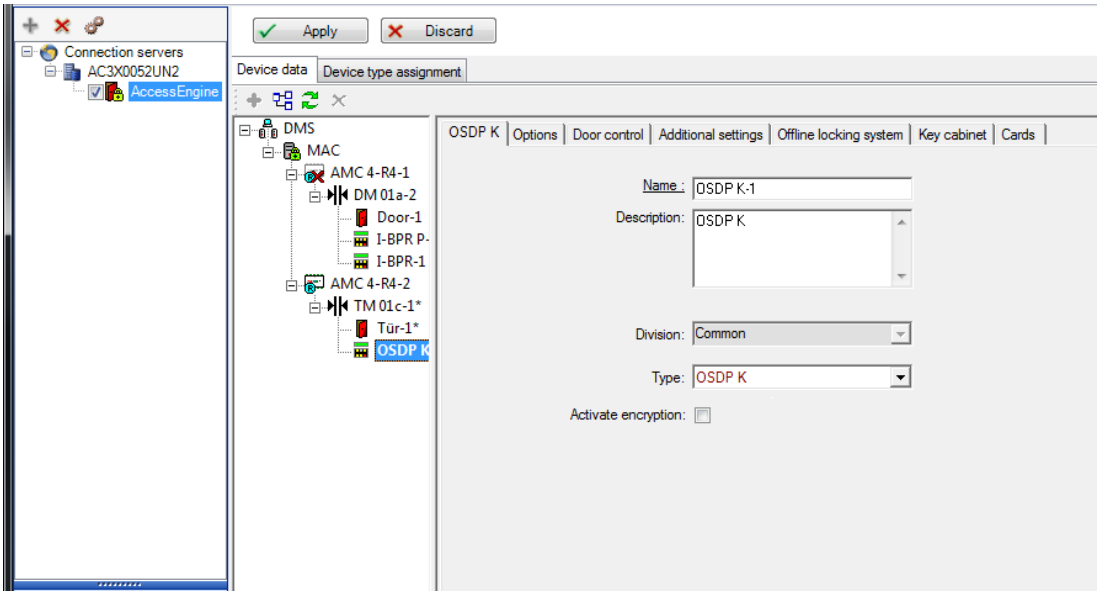
Die Liste der Leser, die zur Auswahl angezeigt werden, wird auf den ausgewählten Controllertyp zugeschnitten.

– 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	HADP-Protokoll	OSDP-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			
TB15 HI1		X			
TB30 LE		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	

R15				X	
R30				X	
R40				X	
RK40				X	
RKL55				X	

* Das BPR-Protokoll wurde eingestellt und wird nur aus Kompatibilitätsgründen genannt.
Im Falle eines **OSDP-Lesers** sieht der Dialog folgendermaßen aus:



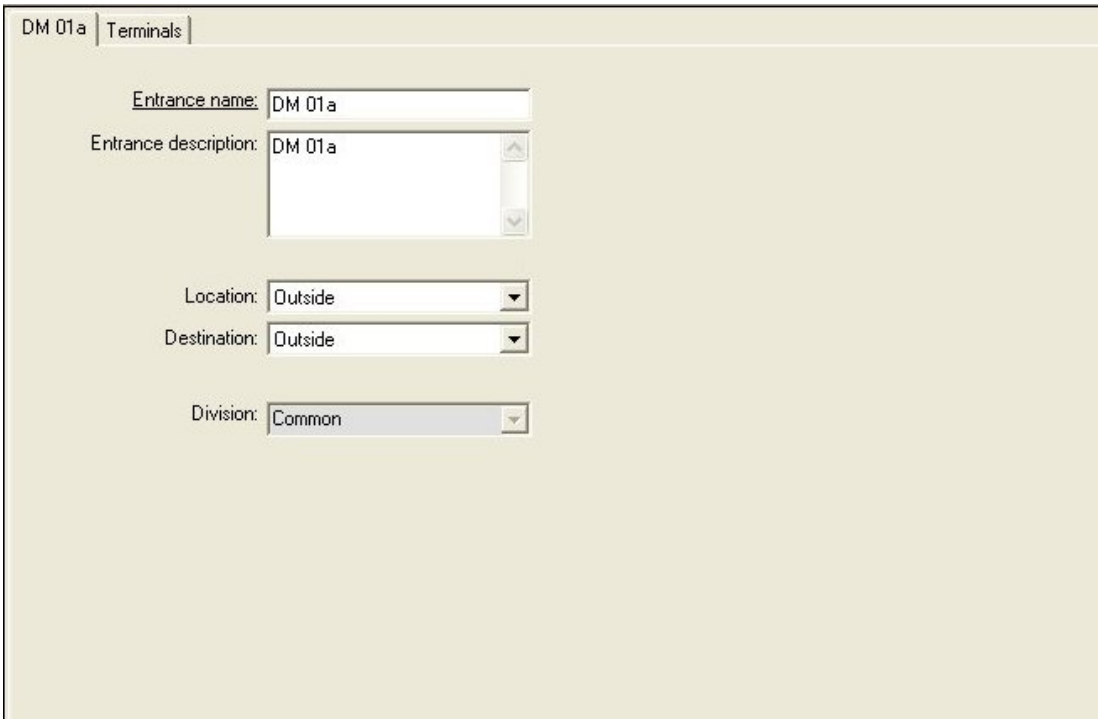
Sichere Kommunikation mit OSDP
Standardmäßig ist das Kontrollkästchen **Activate encryption** (Verschlüsselung aktivieren) nicht aktiviert. Aktivieren Sie das Kontrollkästchen, wenn Sie Leser mit **OSDPv2 secure**-Unterstützung verwenden.
Wenn Sie die Verschlüsselung später deaktivieren, indem Sie das Kontrollkästchen deaktivieren, müssen Sie die Leser-Hardware entsprechend den Anweisungen des Herstellers zurücksetzen.
Als zusätzliche Sicherheitsmaßnahme wird bei jedem Versuch, einen konfigurierten OSDP-Leser durch einen anderen OSDP-Leser zu ersetzen, ein Alarm in Zutrittskontrollsystem ausgelöst. Der Bediener kann den Alarm im Client bestätigen und gleichzeitig die Berechtigung für den Austausch erteilen.
Alarmmeldung: **Exchange of OSDP reader refused** (Austausch von OSDP-Leser abgelehnt)
Befehl: **Allow exchanging the OSDP reader** (Austausch von OSDP-Leser zulassen)
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 LECTUS duo 3000 CK – MIFARE classic LECTUS duo 3000 E – MIFARE Desfire EV1 LECTUS duo 3000 EK – MIFARE Desfire EV1
OSDPv2 – unsicherer und sicherer Modus	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

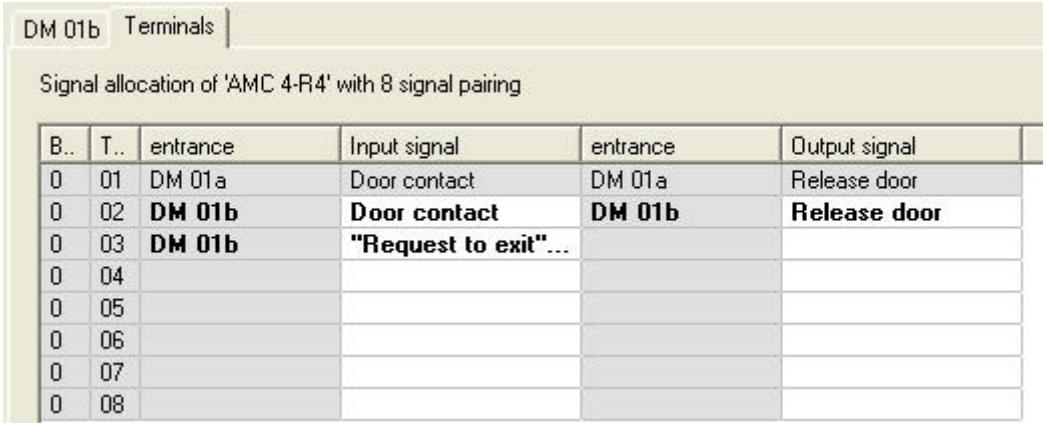
Hinweis!
Hinweise für OSDP
Vermischen Sie keine Produktfamilien, z. B. **LECTUS duo** und **LECTUS secure**, auf demselben OSDP-Bus.
Zur verschlüsselten Datenübertragung zum OSDP-Leser wird ein kundenspezifischer Schlüssel erstellt und verwendet. Achten Sie darauf, dass das System ordnungsgemäß gesichert 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 verschlüsselte und unverschlüsselte Modi nicht zusammen auf demselben OSDP-Bus verwendet werden.
Wenn Sie die Verschlüsselung deaktivieren, indem Sie das Kontrollkästchen auf der Registerkarte „OSDP“ des Lesers im Geräteeditor deaktivieren, müssen Sie die Leser-Hardware entsprechend den Anweisungen des Herstellers zurücksetzen.



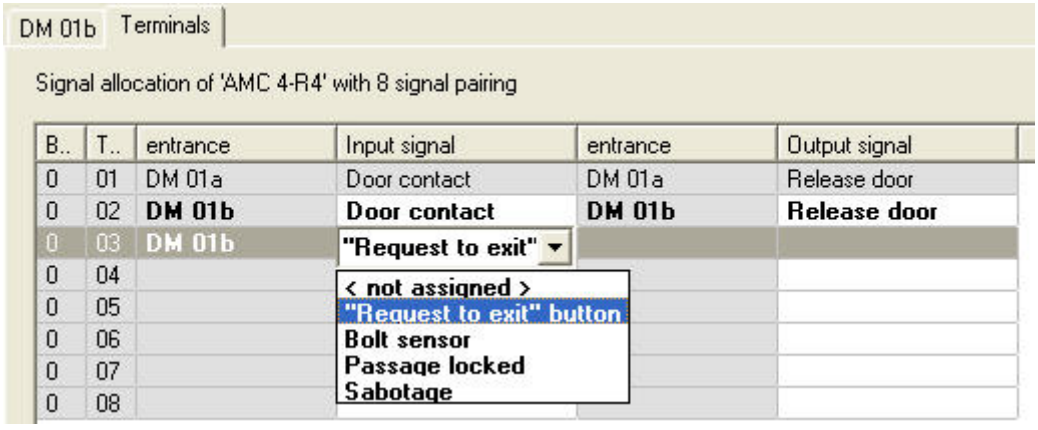
Parameter	Mögliche Werte	**Description** (Beschreibung)
Durchtrittsname (Durchtrittsname)	Alphanumerisch, zwischen 1 und 16 Zeichen	Der Dialog erzeugt einen eindeutigen Namen für den Durchtritt, dieser Name kann jedoch auf Wunsch vom Bediener überschrieben werden, der den Durchtritt konfiguriert.
Entrance description (Durchtrittsbeschreibung)	Alphanumerisch: 0 bis 255 Zeichen	Ein beliebiger Beschreibungstext zur Anzeige im System.
Location (Standort)	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.
Destination (Ziel)	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 **Destination** (Ziel) aktualisiert.
Waiting time external access decision (Wartezeit für externe Zutrittsentscheidung)	Anzahl in Zehntelsekunden	Die Zeit, die eine Zutrittskontrollzentrale auf eine Entscheidung von einem externen System oder Gerät wartet, das mit einem seiner Eingänge verbunden ist.
Division (Mandant)	Der Mandant, zu dem der Leser gehört. Standardwert **Common** (Allgemein)	Nur relevant, wenn die **Mandantenfunktion** lizenziert ist.
Arming Area (Scharfschaltebereich) (nur für Türmodell 14)	Ein Buchstabe: A bis Z	Durchtritte einer EMA-Gruppe werden durch die Aktivierung der Leser des Bereichs aktiviert.

15.3 Konfigurieren von AMC-Signalen

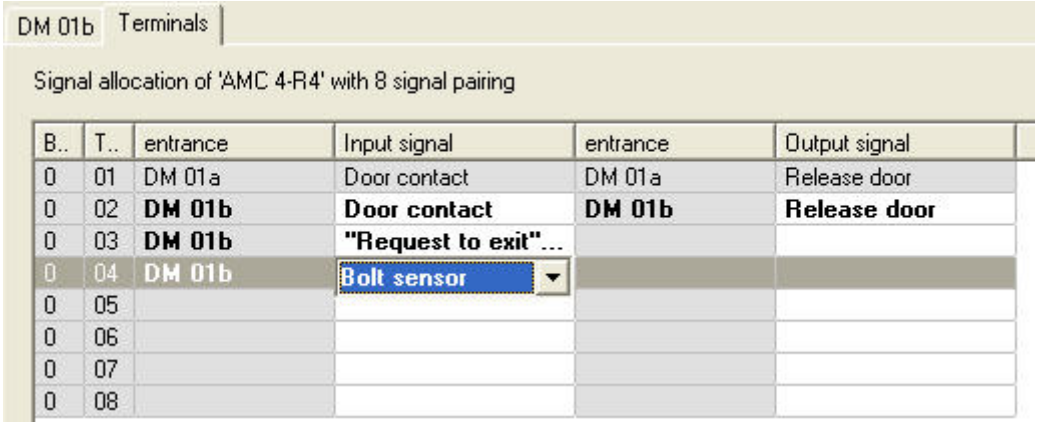
Was den Inhalt und die Struktur anbelangt, ist diese Registerkarte mit der AMC-Registerkarte **Terminals** (Signale) identisch.



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



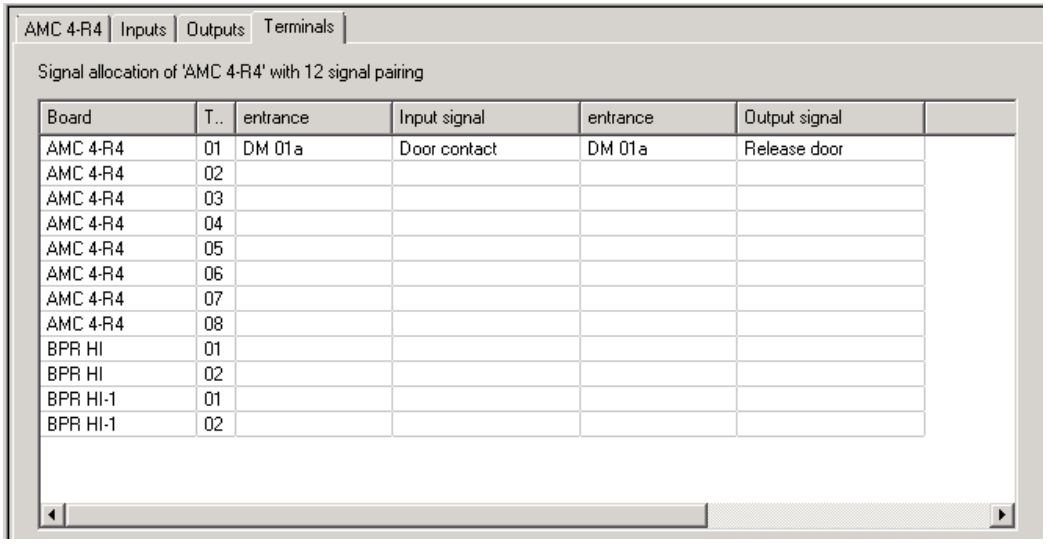
Ebenso können Sie zusätzliche Signale für den jeweiligen Durchtritt erstellen. Wenn Sie auf eine leere Zeile doppelklicken, wird das entsprechende Kombinationsfeld geöffnet:



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** parametriert 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

Eingangssignale	Beschreibung
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.

External access decision accepted (Externe Zutrittsentscheidung akzeptiert)	Signal wird gesetzt, wenn eine externe Zutrittsentscheidung akzeptiert wird.
External access decision denied (Externe Zutrittsentscheidung abgelehnt)	Signal wird gesetzt, wenn eine externe Zutrittsentscheidung abgelehnt 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.	- Door sensor (Türsensor) - "Request to exit" button (Türtaster) - Riegelkontakt - Entrance locked (Durchtritt verriegelt) - Sabotage - Local open enable (Lokale Öffnung aktivieren) - External access decision accepted (Externe Zutrittsentscheidung akzeptiert) - External access decision denied (Externe Zutrittsentscheidung abgelehnt)	- Door opener (Türöffner) - Sluice. lock opposite direction (Schleuse: Gegenrichtung verriegeln) - Alarm suppression (Alarmunterdrückung) - Indicator green (Anzeige grün) - Camera activation (Kameraaktivierung) - Door open too long (Tür zu lange geöffnet) - External access decision activated (Externe Zutrittsentscheidung aktiviert)
03	Drehtür mit Eingangs- und Ausgangsleser Leser für Zeit und Anwesenheit Externe Zutrittsentscheidung verfügbar.	- Turnstile in rest position (Drehkreuz in Ruhelage) - "Request to exit" button (Türtaster) - Entrance locked (Durchtritt verriegelt) - Sabotage - External access decision accepted (Externe Zutrittsentscheidung akzeptiert) - External access decision denied (Externe Zutrittsentscheidung abgelehnt)	- Sluice. lock opposite direction (Schleuse: Gegenrichtung verriegeln) - Open turnstile inbound (Drehkreuz nach innen öffnen) - Open turnstile outbound (Drehkreuz nach außen öffnen) - Alarm suppression (Alarmunterdrückung) - Camera activation (Kameraaktivierung) - Door open too long (Tür zu lange geöffnet) - External access decision activated (Externe Zutrittsentscheidung aktiviert)
05	Parkplatzeingang oder -ausgang – maximal 24 Parkzonen Leser für Zeit und Anwesenheit Externe Zutrittsentscheidung verfügbar.	- Door sensor (Türsensor) - "Request to exit" button (Türtaster) - Entrance locked (Durchtritt verriegelt) - Passage completed (Durchtritt beendet)	- Door opener (Türöffner) - Alarm suppression (Alarmunterdrückung) - Indicator green (Anzeige grün) - Door open too long (Tür zu lange geöffnet) - Door is permanent open (Tür ist dauerhaft geöffnet)

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

14	Einfache Tür mit Eingangs- und Ausgangsleser und Scharfschaltung/ Unscharfschaltung der EMA Leser für Zeit und Anwesenheit	- Door sensor (Türsensor) - "Request to exit" button (Türtaster) - IDS: ready to arm (EMA: bereit zum Scharfschalten) - IDS: is armed (EMA: ist scharfgeschaltet) - Sabotage - IDS: request to arm (EMA: Scharfschaltung anfordern)	- Door opener (Türöffner) - Camera activation (Kameraaktivierung) - IDS: arm (EMA: scharfschalten) - 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 parametriert 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 parametrierte Funktionen zur Verfügung stehen.

Bearbeiten von Signalen

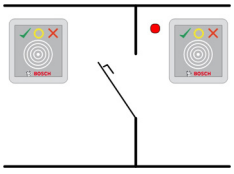
Wenn Sie einen Durchtritt erstellen, werden auf der Registerkarte **Terminals (Signale)** des entsprechenden Durchtritts zwei Eingangs- und zwei Ausgangssignale für jeden Leser unter den Controllersignalen angezeigt. In der Spalte „Board“ wird der Name des Lesers angezeigt. Die Standardsignale für den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

15.4 Vordefinierte Signale für Türmodelle

Türmodell 01



Modellvarianten:

01a	Normale Tür mit Eingangs- **und** Ausgangsleser
01b	Einfache Tür mit Eingangsleser und Türöffnungsknopf
01c	Normale Tür mit Eingangs- **oder** Ausgangsleser

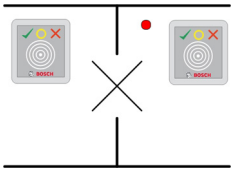
Mögliche Signale:

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 parametriert werden.

Die Alarmunterdrückung wird nur aktiviert, wenn die Alarmunterdrückungszeit vor der Türöffnung größer als 0 ist.
Dieses Türmodell kann auch für Fahrzeugdurchtritte vorteilhaft sein. In diesem Fall wird ein Sekundärleser für Lkw und Pkw empfohlen.

Türmodell 03



Modellvarianten:

03a	Umschaltbares Drehkreuz mit Eingangs- **und** Ausgangsleser
03b	Umschaltbares Drehkreuz mit Eingangsleser und Türöffnungsknopf
03c	Drehkreuz mit Eingangs- **oder** Ausgangsleser

Mögliche Signale:

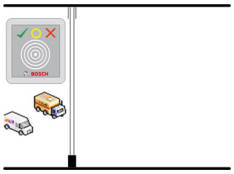
Eingangssignal	**Ausgangssignale**
Turnstile in normal Position (Drehkreuz in normaler Position)	Open turnstile inbound (Drehkreuz nach innen öffnen)
„Request to exit” button (Türtaster)	Open turnstile outbound (Drehkreuz nach außen öffnen)
Sabotage	Entrance locked (Durchtritt verriegelt)
	Camera activation (Kameraaktivierung)
	Door open too long (Tür zu lange geöffnet)
Zusätzliche Signale, die die Option **mantrap** (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:

05c	Eingangs- **oder** Ausgangsleser für Parkplatzzugang

Mögliche Signale für dieses Türmodell:

Eingangssignale	**Ausgangssignale**
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

06a	Eingangs- **und** Ausgangsleser für Zeit und Anwesenheit
06c	Eingangs- **oder** Ausgangsleser für Zeit und Anwesenheit

Leser, die mit diesem Türmodell erstellt werden, steuern keine Türen oder Schranken, sondern leiten nur Ausweisdaten an ein Zeitanwesenheitssystem weiter. Diese Leser befinden sich normalerweise an Orten, zu denen der Zutritt bereits kontrolliert wurde.
Daher sind keine Signale definiert.

Hinweis!
Damit gültige Buchungspaare (Eingangs- und Ausgangszeit) im Zeit- und Anwesenheitssystem erstellt werden können, müssen zwei getrennte Leser mit Türmodell 06 parametriert 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. Auf der Registerkarte **Time Management** (Zeitwirtschaft) der Dialoge **Access Authorizations** (Zutrittsberechtigungen) und **Area/time authorizations** (Raum-Zeit-Berechtigung) werden 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:
<SW_installation_folder>\AccessEngine\AC\TAExchange\
unter dem Namen *TAccExc_EXP.tx*t 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.
d = Tag, M = Monat, y = Jahr, h = Stunde, m = Minute, s = Sommerzeit, 0 = ausgehend, 1 = eingehend
Die Exportdatei enthält alle Buchungen in chronologischer Reihenfolge. Das Feldtrennzeichen innerhalb der Datei ist das Semikolon.

Türmodell 07 – Varianten

Modellvarianten:

07a	Aufzug mit maximal 56 Stockwerken
07c	Aufzug mit max. 56 Stockwerken und Zeitmodell

Türmodell 07a
Signale:

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

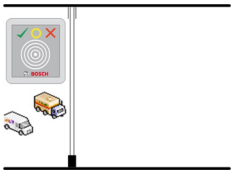
Bei Rufen des Aufzugs kann der Ausweisinhaber nur die Stockwerke wählen, für die sein Ausweis berechtigt ist.
Die Aufzugtürmodelle können nicht mit anderen Türmodellen auf demselben Controller gemischt werden. Mithilfe von AMC Erweiterungen können für jeden Aufzug auf einem AMC bis zu 56 Stockwerke definiert 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



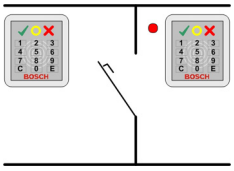
Mögliche Signale:

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:

10a	Normale Tür mit Eingangs- **und** Ausgangsleser **und** Scharfschaltung/ Unscharfschaltung der EMA (Einbruchmeldeanlage)
10b	Normale Tür mit Eingang, Türtaster und Scharfschaltung/Unscharfschaltung der EMA
10e	Normale Tür mit Eingang, Türtaster und dezentraler 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)	IDS: disarm [only DM 10e] (EMA: 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 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.

Serielle Leser (einschließlich I-BPR, HADP und OSDP)

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 (#).

Wiegand Leser (einschließlich serielles BPR-Protokoll)
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.]

15.5 Sonderdurchtritte

15.5.1 Aufzüge (DM07)

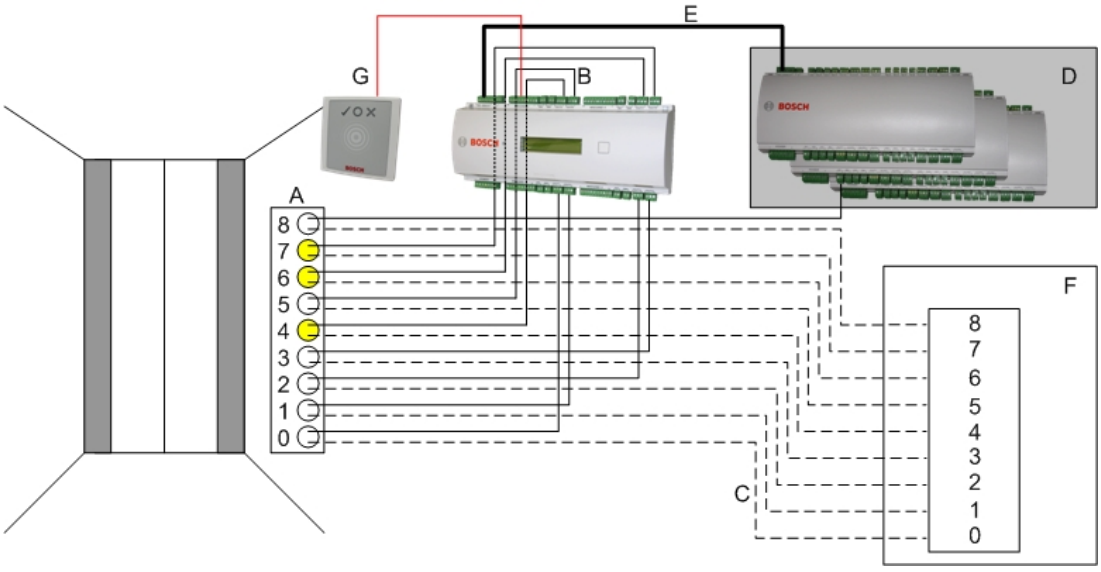
Allgemeine Hinweise zu Aufzügen (Türmodell 07)
Aufzüge können nicht mit anderen Türmodellen auf dem gleichen AMC-Controller kombiniert werden.
Aufzüge können nicht mit den Leseroptionen **Group access** (Gruppenbegehung) oder **Attendant required** (Begleiter erforderlich) verwendet werden.
Bis zu acht 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 können Sie der Berechtigung einer Person bestimmte Stockwerke zuweisen.

Wenn der Aufzug mithilfe des Türmodells **07a** erstellt wurde, liest die Person ihren Ausweis ein und die Stockwerke, zu denen sie Zugang hat, sind dann verfügbar.
Beim Türmodell **07c** überprüft das System die Berechtigung für das gewählte Stockwerk, 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.

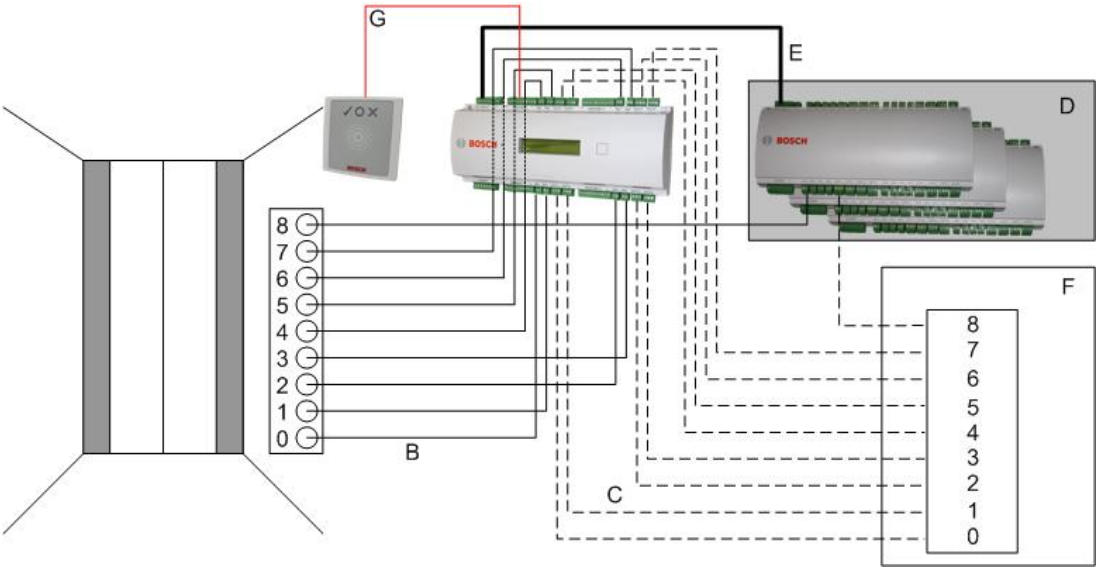
Verkabelungsschema für Aufzüge:

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.l

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



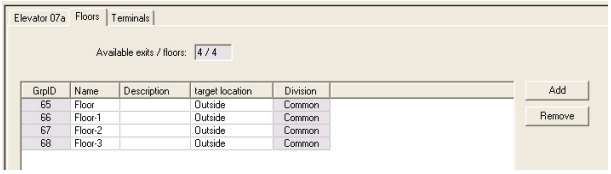
Legende:

- 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.

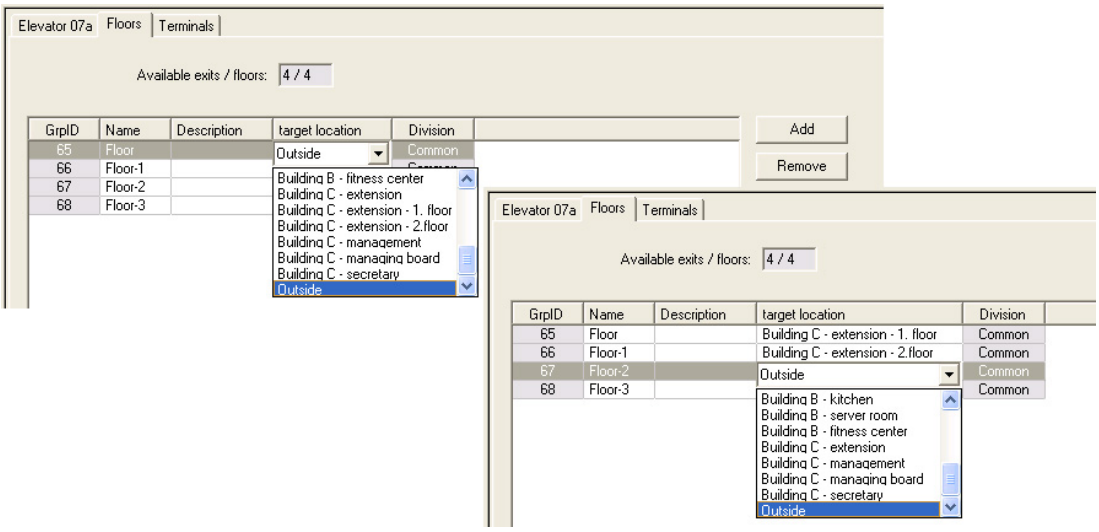
Wie Parkplätze haben Aufzüge den Parameter **Öffentlich.** Dieser Parameter kann für jedes Stockwerk individuell gesetzt werden. Wenn der Parameter **Öffentlich** aktiviert ist, werden Zutrittsberechtigungen nicht überprüft – so kann jeder Ausweisinhaber im Aufzug das Stockwerk auswählen.
Legen Sie auf Wunsch ein Zeitmodell für das Eintrittsmodell fest: Außerhalb der definierten Zeitzonen werden Berechtigungen geprüft.

Stockwerke für Türmodell 07

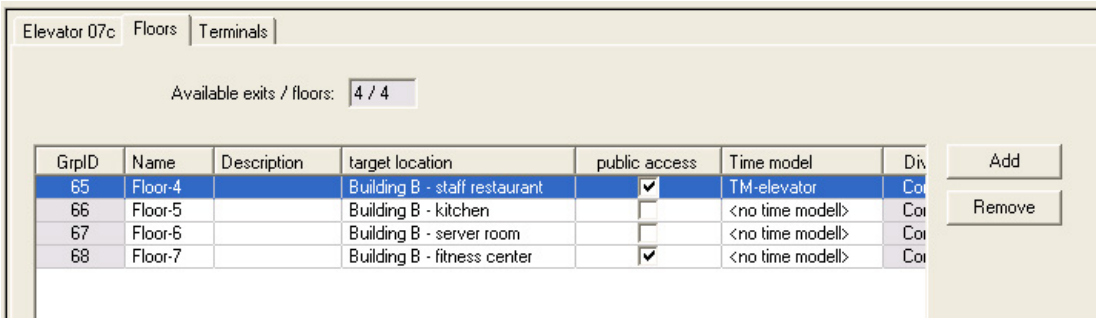
Verwenden Sie die Registerkarte **Floors** (Stockwerke) zum Hinzufügen und Entfernen von Stockwerken für den Aufzug mit den Schaltflächen **Add** (Hinzufügen) und **Remove** (Entfernen).



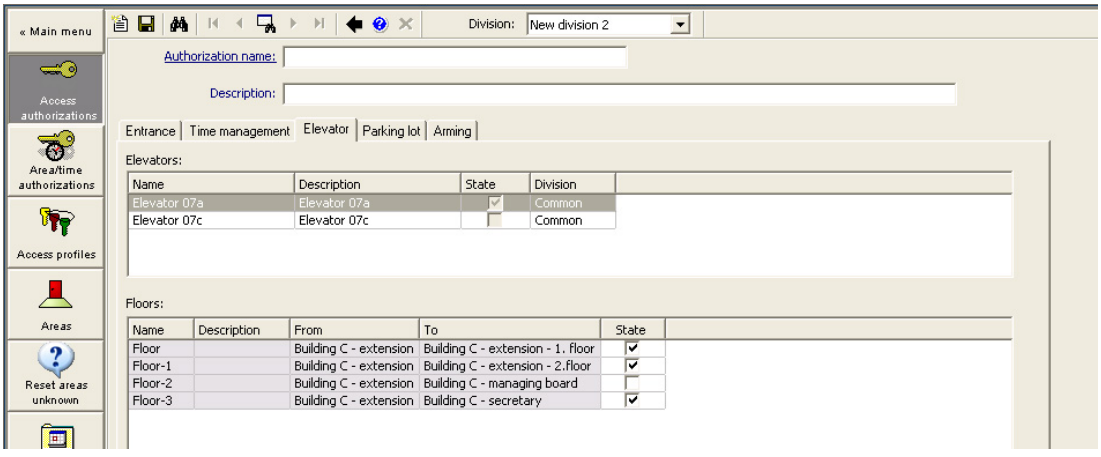
Zielorte für ein Stockwerk können alle **Bereiche** mit Ausnahme von Parkplätzen und Parkzonen sein.
Einem Stockwerk kann nur ein Bereich zugewiesen werden. Aus diesem Grund wird nach jeder Zuweisung die Auswahl in den Kombinationsfeldern verringert, um unbeabsichtigte Doppelzuweisungen zu verhindern.



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 Dialogen **Access authorizations** (Zutrittsberechtigungen) und **Area/time authorization** (Raum-Zeit-Berechtigung) zunächst den gewünschten Aufzug und anschließend darunter die Stockwerke, zu denen dem Ausweisinhaber Zugang gewährt werden soll.



15.5.2 Türmodelle mit Einbruchsalarmen (DM14)

Einführung

Im Gegensatz zum Durchtrittsmodell 10 (DM10) kann **DM14** eine Einbruchmeldeanlage (kurz EMA) für einen bestimmten Scharfschaltebereich scharfschalten und unscharfschalten Ein DM14 Durchtritt kann auch so konfiguriert werden, dass dem Ausweisinhaber, der ihn unscharfschaltet, Zutritt gewährt wird, sofern der Ausweisinhaber alle anderen erforderlichen Zutrittsberechtigungen hat.

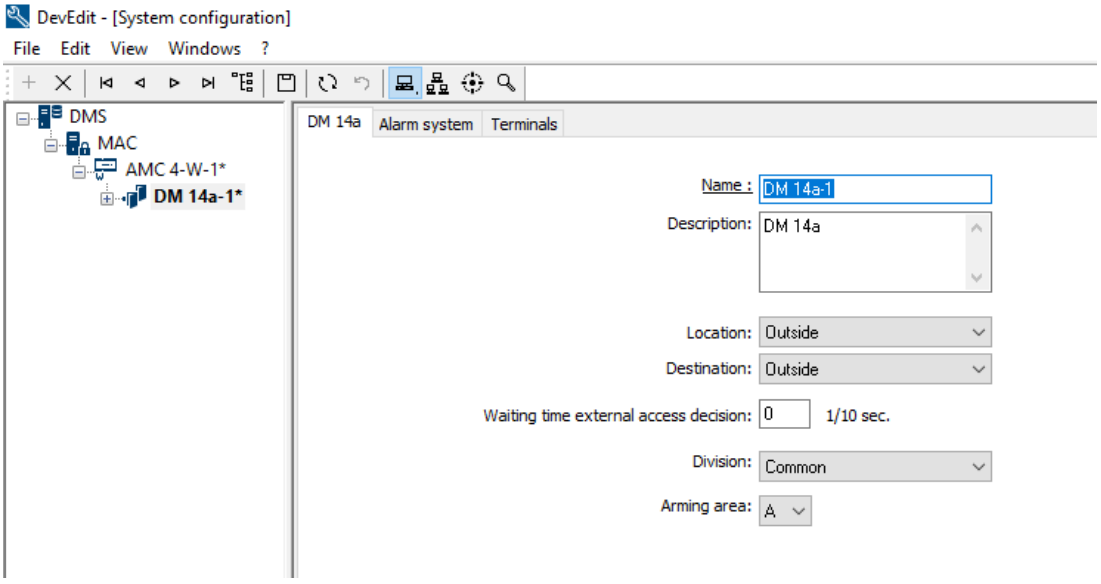
Die Konfiguration für DM14 im Geräteeditor und im Dialogmanager umfasst folgende Aufgaben:

1. Legen Sie allgemeine Parameter fest, um den Durchtritt und seinen Scharfschaltebereich zu identifizieren.
2. Legen Sie bestimmte Parameter fest, um die genaue Vorgehensweise zum Scharfschalten des Bereichs einzustellen.
3. Definieren Sie die EMA-spezifischen Eingangs- und Ausgangssignale an den Klemmen vom Türcontroller des Durchtritts.
4. Schließen Sie Berechtigungen zum Scharfschalten/Unscharfschalten in die Zutrittsberechtigungen der Ausweisinhaber ein, die DM14 Durchtritte bedienen sollen.

Die Aufgaben werden in den folgenden Abschnitten beschrieben.

Allgemeine Parameter

Legen Sie auf der ersten Registerkarte, **DM14a** oder **DM14b**, die folgenden Parameter fest.

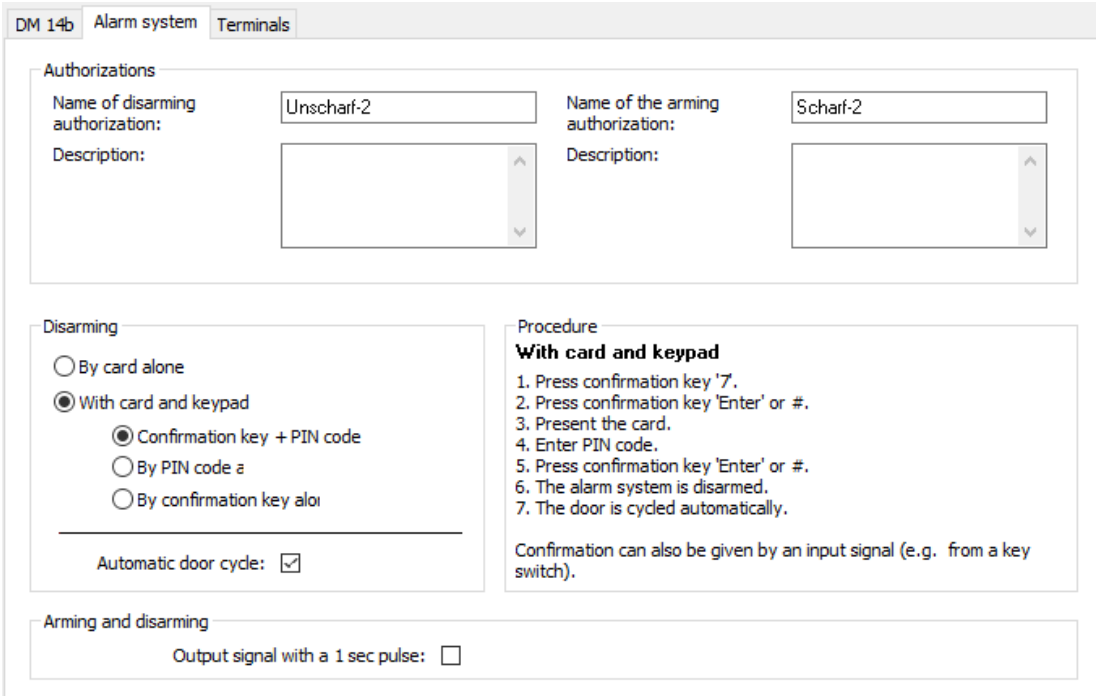


Parameter	Werttyp	Beschreibung
Name	Freitext	Der Name des Durchtritts.
Description (Beschreibung)	Freitext, optional	Eine Beschreibung des Durchtritts.
Location (Standort)	Liste der definiert	Der Zutrittsbereich, in dem sich der Durchtritt befindet.

Parameter	Werttyp	Beschreibung
	en Bereiche, falls verwendet	
Destination (Ziel)	Liste der definierten Bereiche, falls verwendet	Der Zutrittsbereich, zu dem der Durchtritt führt.
Division (Mandant)	Liste der definierten Mandanten, falls verwendet	Der Mandant oder Mieter innerhalb des Zutrittskontrollsystems, zu dem der Durchtritt gehört.
Waiting time external access decision (Wartezeit für externe Zutrittsentscheidung)	Zehntelsekunden.	Wenn Sie ein externes System mit der Klemme des AMC verbunden haben, um Zutrittsentscheidungen in seinem Namen zu treffen, beschränkt dieser Parameter die Wartezeit auf eine Antwort vom externen System. Hinweis: Die Zutrittsentscheidung erfordert die Erfüllung **aller** im Zutrittskontrollsystem definierten Bedingungen, z. B. Zutrittsberechtigungen, Zeitmodelle und Mandanten (falls verwendet). Der Standardwert ist 0, d. h. der Parameter wird ignoriert.
Arming Area (Scharfschaltebereich)	Liste mit Großbuchstaben A...Z	Ein Buchstabe, unter dem DM14 Durchtritte in Scharfschaltebereiche gruppiert werden.

Parameter für Einbruchmeldeanlage

Legen Sie auf der zweiten Registerkarte **Alarm system** (Einbruchmeldeanlage) die folgenden Parameter fest. Diese Parameter regeln die Anmeldeinformationen und das Verfahren zum Unscharfschalten der EMA. Die Unscharfschaltung wirkt sich auf alle Durchtritte innerhalb desselben Scharfschaltebereichs aus, wie auf der ersten Registerkarte definiert.



Parameter	Werttyp	Beschreibung
Bereich **Authorizations** (Berechtigungen)		
Name of disarming authorization (Name der Unscharfschalteberechtigung)	Freitext	Ein Name, der in Protokollen und Berichten angezeigt wird, wenn ein Ausweisinhaber die EMA an diesem Durchtritt unscharfschaltet.
Name of arming authorization (Name der Scharfschalteberechtigung)	Freitext	Ein Name, der in Protokollen und Berichten angezeigt wird, wenn ein Ausweisinhaber die EMA an diesem Durchtritt scharfschaltet.
Description (Beschreibung) (eine pro Berechtigung)	Freitext, optional	Beschreibungen der Scharfschalteberechtigungen
Bereich **Disarming** (Unscharfschalten)		
By card alone (Nur mit Ausweis)	Optionsfeld	Wählen Sie diese Option aus, um die Unscharfschaltung der EMA zu ermöglichen, indem am Leser ein Ausweis ohne weitere Authentifizierung präsentiert wird.

Parameter	Werttyp	Beschreibung
By card and keypad (Mit Ausweis und Bedienfeld)	Optionsfeld	Wählen Sie diese Option aus, um die Unscharfschaltung der EMA zu ermöglichen, indem am Leser ein Ausweis präsentiert und weitere Authentifizierung am Bedienfeld des Lesers eingegeben wird. Der genaue Authentifizierungs- und Unscharfschaltevorgang wird durch die folgenden Subparameter bestimmt:
Confirmation key + PIN code (Bestätigungsschlüssel + PIN-Code)	Optionsfeld	Ausweisinhaber müssen sich anhand eines Ausweises, eines Bestätigungsschlüssels und eines PIN-Codes authentifizieren.
By PIN code alone (Nur mit PIN-Code)	Optionsfeld	Ausweisinhaber müssen sich anhand eines Ausweises und eines PIN-Codes authentifizieren.
By confirmation key alone (Nur mit Bestätigungsschlüssel)	Optionsfeld	Ausweisinhaber müssen sich anhand eines Ausweises und eines Bestätigungsschlüssels authentifizieren.
Automatic door cycle (Automatischer Türzyklus)	Kontrollkästchen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie nach dem Unscharfschalten einen Türzyklus für das Schloss durchlaufen lassen möchten, damit der Ausweisinhaber gleichzeitig unscharfschalten und eintreten kann. **Hinweis:** Der Zyklus für das Schloss findet nur dann statt, wenn der Ausweisinhaber auch eine Zutrittsberechtigung für diese Tür hat.
Bereich **Procedure** (Verfahren)		
Abhängig von den im Bereich **Disarming** (Unscharfschalten) festgelegten Parametern wird in diesem Fenster ein Standardverfahren zum Unscharfschalten der EMA angezeigt. Informieren Sie die Ausweisinhaber über dieses Verfahren, die die DM14 Durchtritte in diesem Scharfschaltebereich verwenden werden.		
Bereich **Arming and disarming** (Scharfschalten und Unscharfschalten)		
Output signal with a 1 sec pulse (Ausgangssignal mit einem 1-Sek.-Impuls)	Kontrollkästchen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine Zentrale der **Bosch B oder G Series** verwenden. Der Effekt besteht darin, ein einzelnes Impulssignal zu senden, um den Scharfschaltezustand vom Einbruchmeldebereich des Durchtritts zu aktivieren, anstatt das Signal auf konstant 1 (Scharfschalten) oder 0 (Unscharfschalten) zu setzen.

Door controller terminals (Türcontrollerklemmen)

Um die Scharfschaltung und Unscharfschaltung mit einem DM14 Durchtritt zu ermöglichen, müssen Sie die Eingangs- und Ausgangssignale der EMA definieren, die Sie an den Klemmen vom Türcontroller des Durchtritts verwenden möchten.

Dieser Schritt ist für jeden Controller mit DM14 Durchtritten erforderlich. Alle nachfolgenden DM14 Durchtritte, die Sie auf demselben Controller und seinen Erweiterungen definieren, erben die Signale des gemeinsam genutzten Controllers.

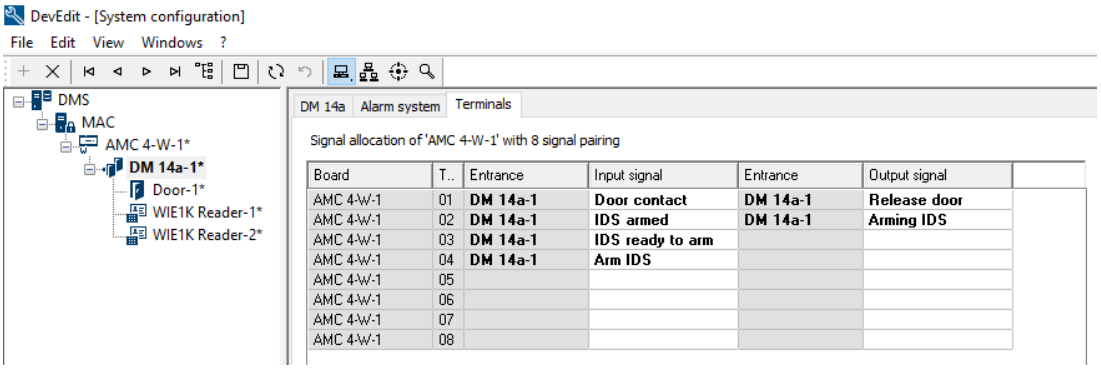
Die Standardsignale werden in der folgenden Tabelle beschrieben.

Signal	Eingang/ Ausgang	Beschreibung
IDS armed (EMA scharfgeschaltet)	Eingang	Die EMA ist für diesen Einbruchmeldebereich scharfgeschaltet.
IDS ready to arm (EMA bereit zum Scharfschalten)	Eingang	Kein Melder der EMA ist in einem ausgelösten Status (offen oder nicht bereit).
Arm IDS (EMA scharfschalten)	Eingang	Eine Anforderung zur Scharfschaltung der EMA.
Release door (Tür freigeben)	Ausgang	Entsperren Sie den Türmechanismus und versperren Sie ihn anschließend wieder, um den Zutritt zu ermöglichen.
Arming IDS (EMA scharfschalten)	Ausgang	Schalten Sie die EMA abhängig vom aktuellen Zustand scharf oder unscharf (umschalten).

Verfahren zum Zuweisen von Signalen zu Klemmen

1. Öffnen Sie die dritte Registerkarte **Terminals** (Klemmen).

– Die Klemmen des Türcontrollers dieses Durchtritts sowie alle potenziellen Erweiterungen werden in einer Tabelle angezeigt.



2. Wählen Sie die Zeile, die der Klemme entspricht, die Sie für das Eingangssignal verwenden möchten.
3. Wählen Sie in der entsprechenden Zelle in der Spalte **Input signal** (Eingangssignal) das gewünschte Signal aus der Dropdown-Liste aus. Beachten Sie, dass nur bisher nicht zugewiesene Signale in der Liste angezeigt werden.
4. Wiederholen Sie die vorherigen Schritte, um alle anderen Eingangssignale hinzuzufügen, die Sie für diesen Durchtritt benötigen.
5. Wiederholen Sie den Vorgang so oft wie nötig, um alle gewünschten Ausgangssignale in der Spalte **Output signal** (Ausgangssignal) hinzuzufügen.

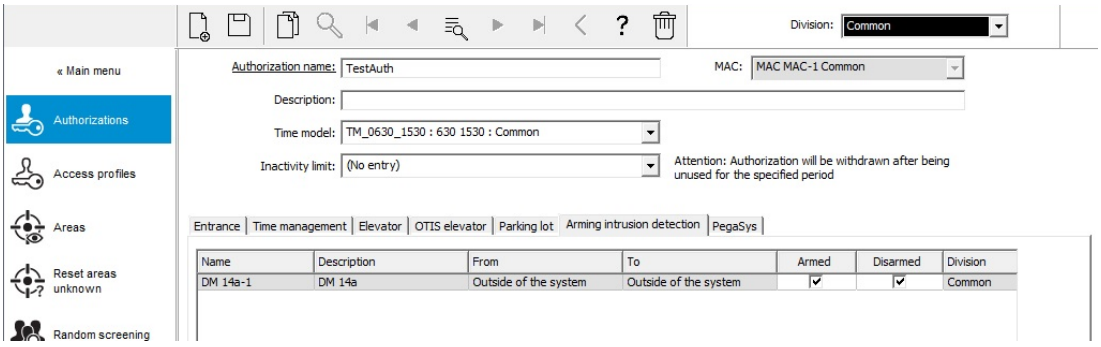
Berechtigungen zum Scharfschalten und Unscharfschalten von DM14 Durchtritten definieren

Nachdem Sie einen DM14 Durchtritt im Geräteeditor erstellt haben, ist der Durchtritt für Zutrittsberechtigungen verfügbar.

1. Navigieren Sie im Dialogmanager zu:

– Main menu > **System data** > **Authorizations** > Registerkarte: **Arming Intrusion detection** (Hauptmenü > Systemdaten > Berechtigungen > Registerkarte: Einbruchmeldeanlage scharfschalten)

2. Laden Sie eine vorhandene Zutrittsberechtigung in den Dialog oder klicken Sie auf  (Neu), um eine neue zu erstellen.
3. Suchen Sie den gewünschten DM14 Durchtritt in der Liste und aktivieren Sie die Kontrollkästchen **Armed** (Scharfgeschaltet) und/oder **Disarmed** (Unscharfgeschaltet).

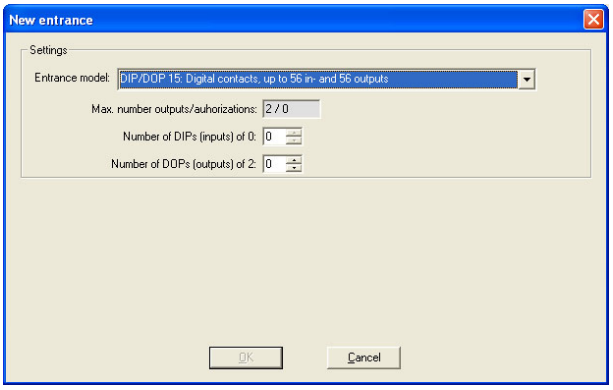


4. Klicken Sie auf  (Speichern), um die Zutrittsberechtigung mit den ausgewählten Berechtigungen zu speichern.
5. Weisen Sie diese Zutrittsberechtigung den Ausweisinhabern zu, die DM14 Durchtritte bedienen sollen.

15.5.3 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.

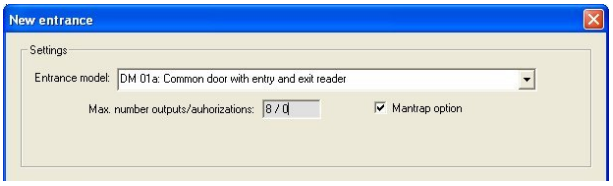
Eingangssignal	Ausgangssignal
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

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 im Geräteeditor 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.

15.5.4 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.



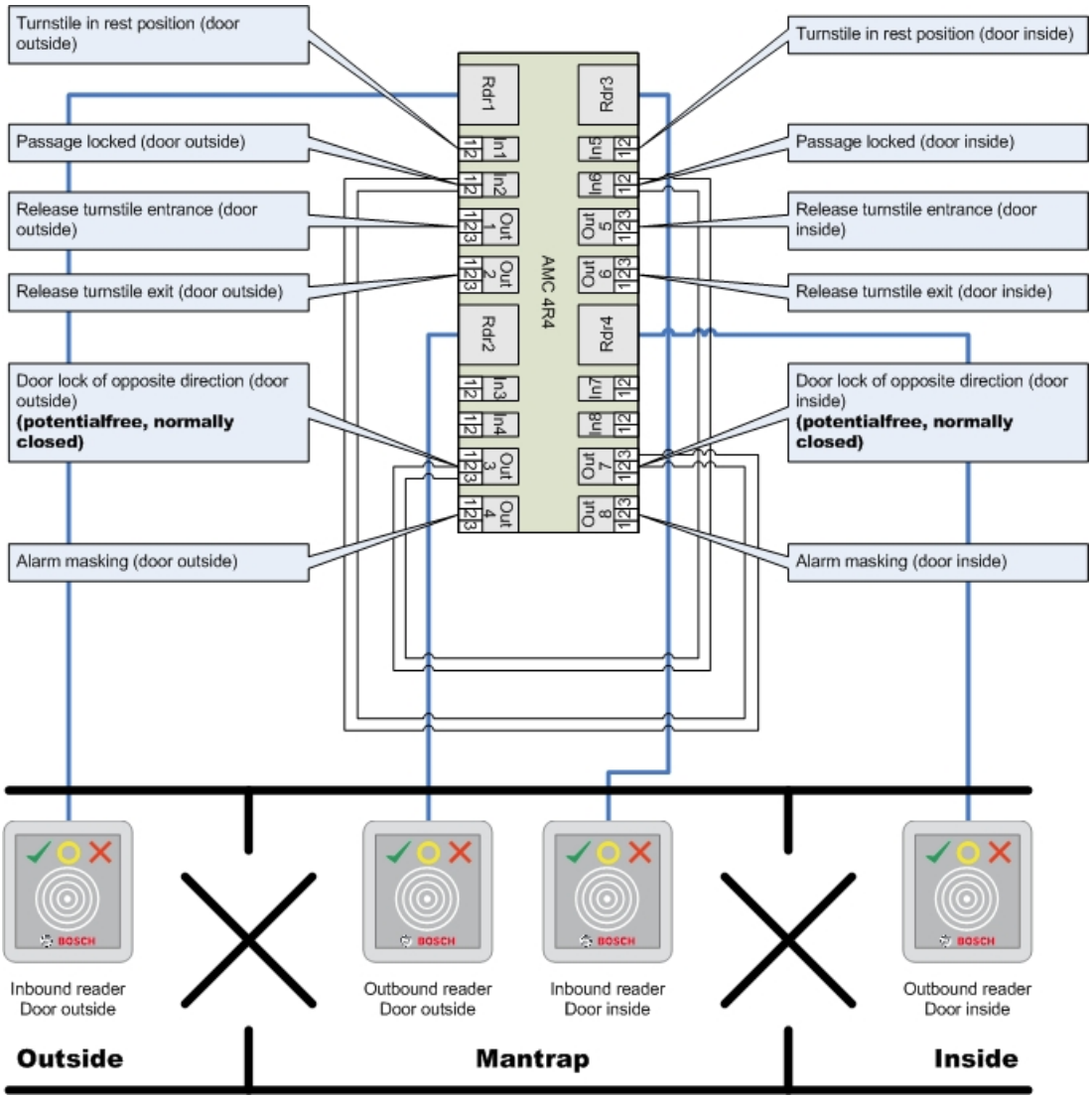
Sie können alle Modelle des Typs 01 und 03 kombinieren, müssen aber diese Option an beiden Durchtritten festlegen, die zur Schleuse gehören.

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.

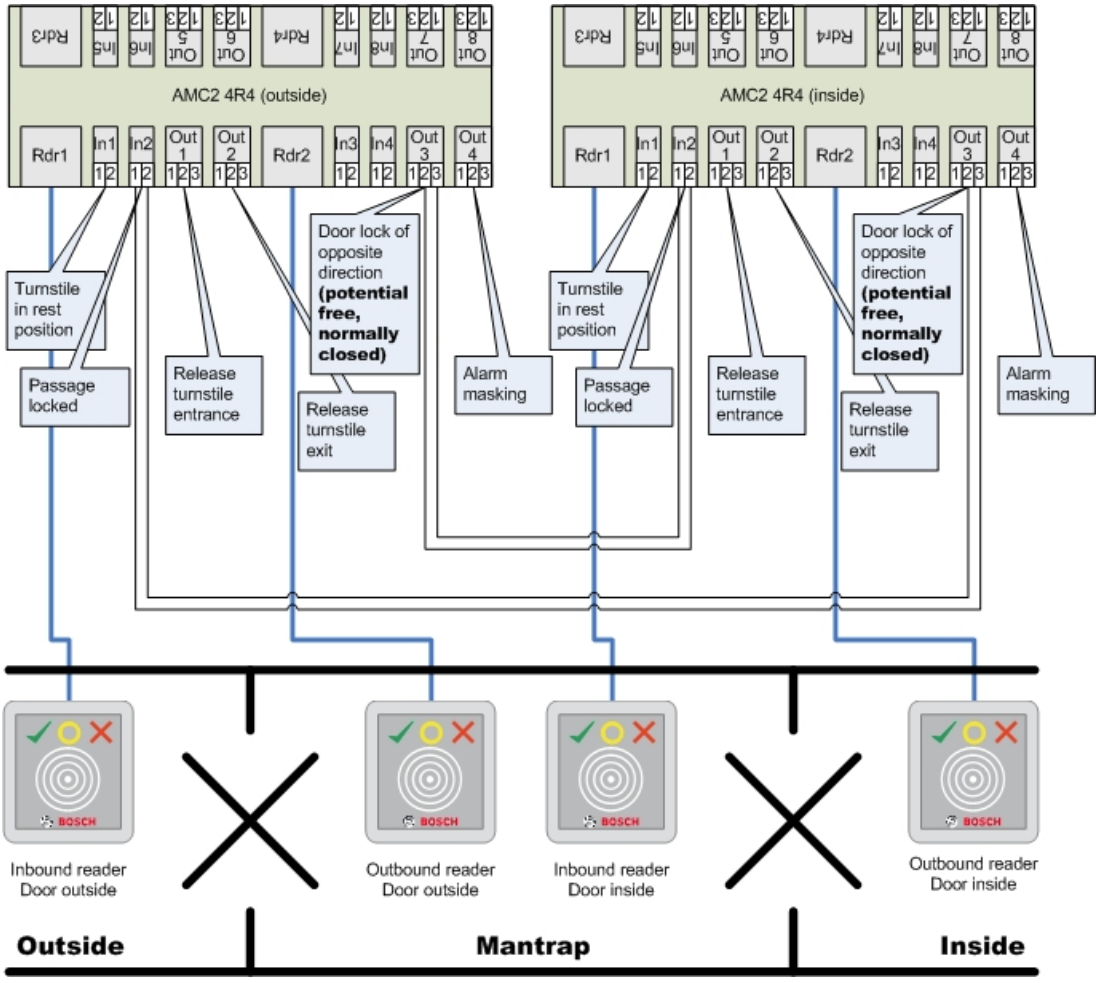
Hinweis!

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.

15.6 Türen

Konfigurieren einer Tür: Allgemeine Parameter

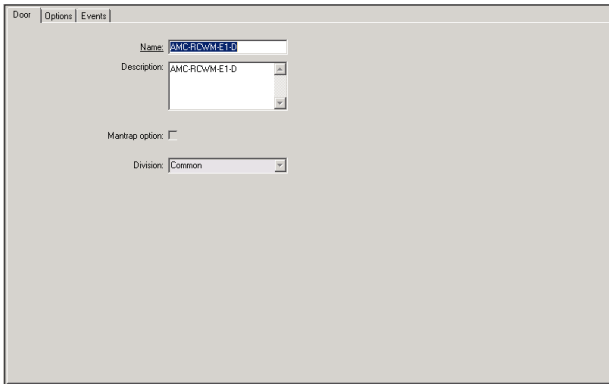
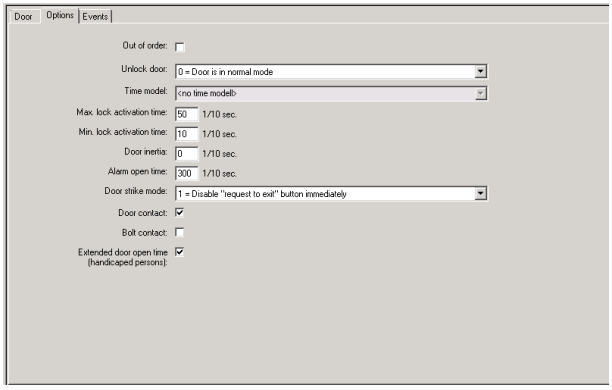


Abbildung 15.1:

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	
Division (Mandant)	Standardmandant „Common“ (Allgemein)	Nur relevant, wenn die **Mandantenfunktion** lizenziert ist.
Nur für Türmodelle 01 und 03 bei Konfiguration einer Schleuse:		
Mantrap option (Schleusenoption)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 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 **beide** Türen. Für die Türen ist ebenfalls eine spezielle physische Verdrahtung erforderlich.

Konfigurieren einer Tür: Optionen

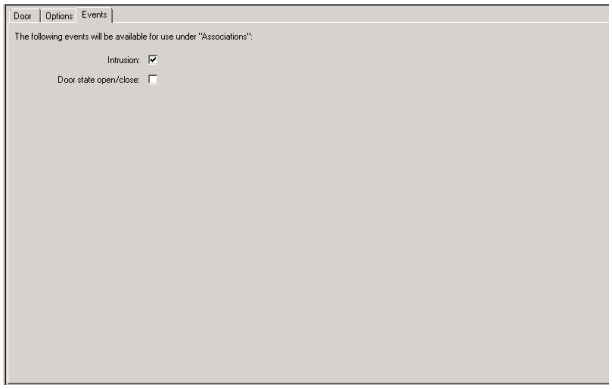


Parameter	Mögliche Werte	Bemerkung
Manual operation (Manuelle Bedienung)	0 = Kontrollkästchen ist deaktiviert 1 = Kontrollkästchen ist aktiviert	0 = Die Tür befindet sich im Normalmodus (Standard), d. h. sie unterliegt der Zutrittskontrolle durch das Gesamtsystem. 1 = Tür ist vom Zutrittskontrollsystem 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 1 = Tür ist entsperrt	0 = Normalmodus (Standard) – die Tür wird abhängig von den Zutrittsrechten der Anmeldedaten gesperrt oder entsperrt.

	2 = Tür ist zeitmodellabhängig entsperrt 3 = Tür ist zeitmodellabhängig geöffnet nach erster Begehung 5 = Tür ist dauerhaft gesperrt 6 = Tür ist zeitmodellabhängig gesperrt	1 = Für längere Zeit entsperren – Zutrittskontrolle ist für den Zeitraum aufgehoben. 2 = Für einen Zeitraum entsperren, der vom Zeitmodell definiert ist. Während dieser Zeit ist die Zutrittskontrolle aufgehoben. 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. 5 = blockiert, bis sie manuell entsperrt wird. 6 = gesperrt, solange das Zeitmodell aktiv ist. Die Tür wird nicht kontrolliert und die Tür kann nicht verwendet werden, wenn das Zeitmodell gültig ist.
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. 0 = kein Zeitlimit, keine Meldung
Türöffnermodus	Listenfeldeintrag	0 = Türtaster ist nach der Aktivierungszeit deaktiviert 1 = Türtaster ist sofort deaktiviert (= Standard)

Door contact (Türöffnungskontakt)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Tür hat keinen Rahmenkontakt 1 = Tür hat Rahmenkontakt. Ein geschlossener Kontakt bedeutet in der Regel, dass die Tür geschlossen ist (= Standard).
Bolt contact (Türriegelkontakt)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Tür hat keinen Riegelkontakt (= Standard) 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 (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Die Aktivierungszeit ist normal. 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).

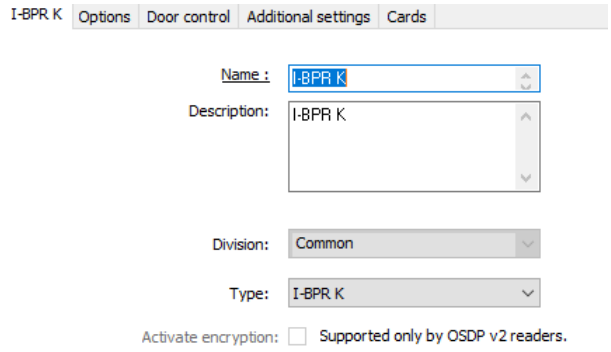
Konfigurieren einer Tür: Ereignisse



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

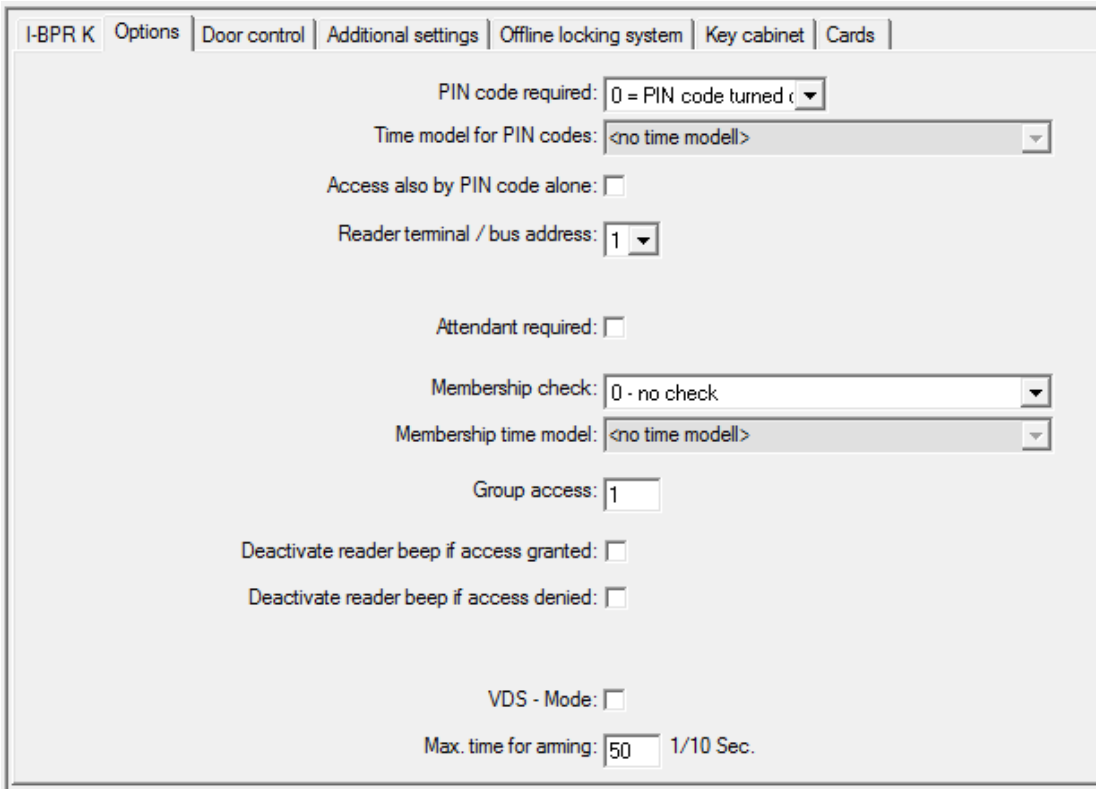
15.7 Leser

Konfigurieren eines Lesers: Allgemeine Parameter



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 Lesergruppe

Konfigurieren eines Lesers: Optionen



Parameter	Mögliche Werte	Beschreibung
PIN-Code erforderlich	0 = PIN-Code deaktiviert – keine Eingabe erforderlich (= Standard) 1 = PIN-Code aktiviert – Eingabe immer erforderlich 2 = PIN-Code durch Zeitmodell gesteuert – Eingabe nur außerhalb des Zeitmodells erforderlich	Dieses Feld wird nur aktiviert, wenn der Leser über ein Eingabegerät verfügt. 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 **PIN code required** (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 (Kontrollkästchen ist aktiviert)	
Leserterminal/ Busadresse	1 - 4	AMC 4W: nummeriert nach den Wiegand-Schnittstellen AMC 4R4: nummeriert nach der gebrückten Adresse des Lesers
Begleiter erforderlich	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Besuch braucht keinen Begleiter (= Standard) 1 = Begleiter muss den Leser ebenfalls verwenden
Zugehörigkeit zur Anlage prüfen	Listenfeldeintrag	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. **WICHTIG** Die Zugehörigkeitsprüfung funktioniert nur mit physischen Ausweisen, bei denen die Ausweisdefinitionen im System vordefiniert sind (grauer Hintergrund) und **nicht** mit benutzerdefinierten Definitionen oder biometrischen Nachweisen. **0 – keine Überprüfung** Die Zugehörigkeitsprüfung ist deaktiviert, aber der Ausweis wird wie üblich auf Autorisierungen geprüft (= Standard). **1 – Prüfung** Der Ausweis wird nur auf Firmen-ID geprüft, d. h. auf Zugehörigkeit im System. **2 – abhängig vom Zeitmodell** 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. Die Auswahl eines Zeitmodells ist für **Zugehörigkeitsprüfung**Option 2 obligatorisch.
Gruppenbegehung	1 - 10	**Für Leser mit Tastenfeld:** Mindestanzahl gültiger Ausweise, die am Dialogleser eingelesen werden müssen, bevor die Tür geöffnet wird. Diese Anzahl kann

		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. **Für Leser ohne Tastenfeld:** Genaue Anzahl gültiger Ausweise, die am Ausweisleser eingelesen werden müssen, bevor die Tür geöffnet wird. Der Standardwert ist 1.
Lesersignalton deaktivieren, wenn Zutritt gewährt wird	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 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) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Bei Aktivierung (1) bleibt der Leser still, wenn einem nicht autorisierten Benutzer der Zutritt verweigert wird.
 Die Funktionen für „(Lesersignalton deaktivieren“ hängen von der entsprechenden Firmware des Lesers ab. Die Firmware einiger Leser unterstützen diese Funktion möglicherweise nicht.		
VDS-Modus	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 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

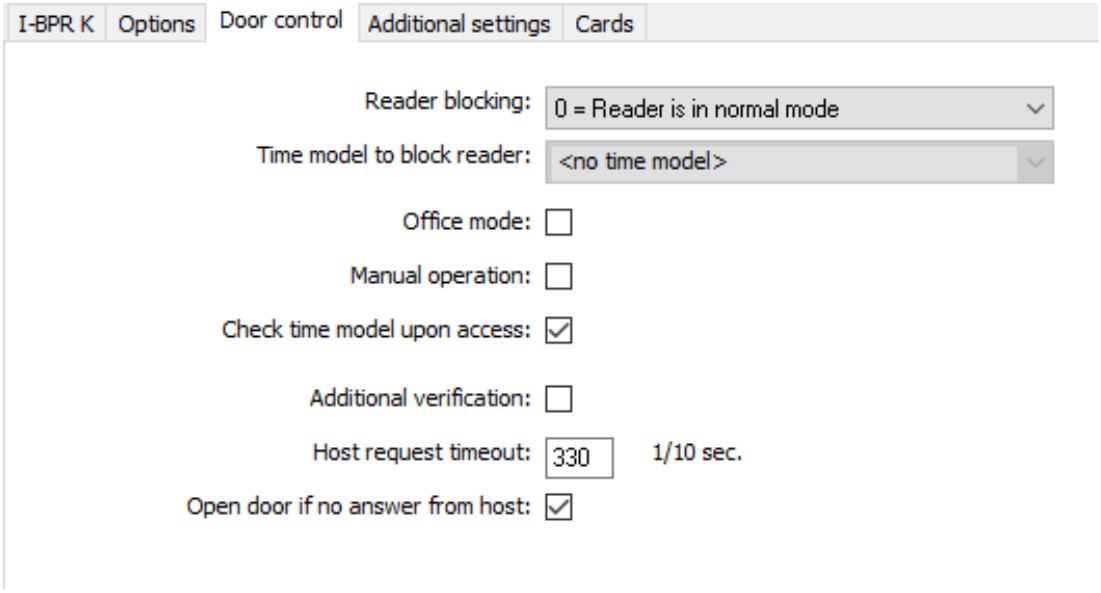
Diese Registerkarte wird nur für vernetzte biometrische Leser angezeigt.

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*.
Vorlagen auf Server	
Card only (Nur Ausweis)	Der Leser liest nur Ausweisdaten. Er authentifiziert sie gegen Daten aus dem Gesamtsystem.
Card and fingerprint (Ausweis und Fingerabdruck)	Der Leser liest sowohl Ausweisdaten als auch Fingerabdruckdaten. Er authentifiziert sie gegen Daten aus dem Gesamtsystem.
Vorlagen auf Gerät	
Person dependent verification (Personenabhängige Überprüfung)	Der Leser erlaubt Einstellungen des einzelnen Ausweisinhabers, um festzustellen, welchen **Identifikationsmodus** er verwendet. Die Personaldaten bieten folgende Möglichkeiten: – Fingerprint only (Nur Fingerabdruck) – Card only (Nur Ausweis) – Card and fingerprint (Ausweis und Fingerabdruck) Diese werden später in dieser Tabelle beschrieben.
Fingerprint only (Nur Fingerabdruck)	Der Leser liest nur Fingerabdruckdaten. Er authentifiziert sie gegen seine eigenen gespeicherten Daten.
Card only (Nur Ausweis)	Der Leser liest nur Ausweisdaten. Er authentifiziert sie gegen seine eigenen gespeicherten Daten.
Card and fingerprint (Ausweis und Fingerabdruck)	Der Leser liest sowohl Ausweisdaten als auch Fingerabdruckdaten. 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. Er authentifiziert sie gegen seine eigenen gespeicherten Daten.

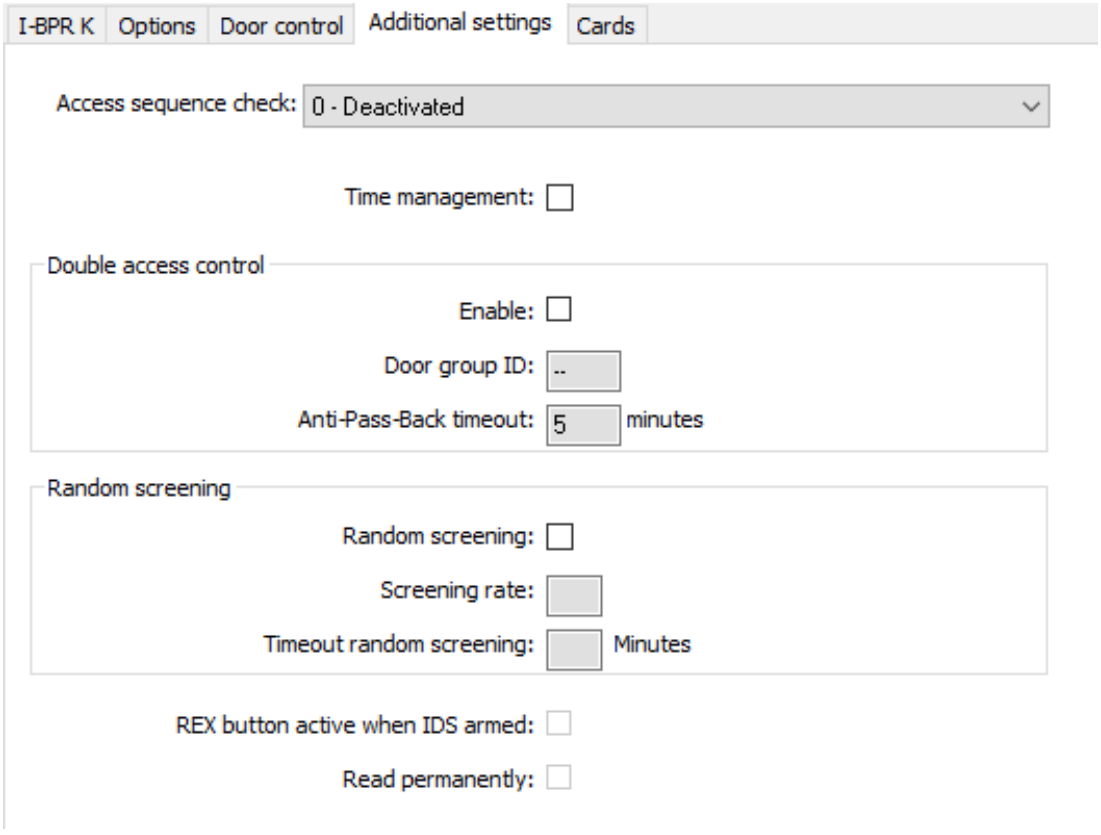
Konfigurieren eines Lesers: Türsteuerung



Parameter	Mögliche Werte	Bemerkung
Reader blocking (Leser sperren)	Listenfeldeintrag	0 = Leser ist im Normalbetrieb – keine Sperrung (= Standard) 1 = Leser ist dauerhaft gesperrt – dauerhafte Sperrung 2 = Leser ist zeitmodellabhängig gesperrt – Sperrung nach Zeitmodell, die mit Time model to block reader (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) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Ermöglicht die Verwendung dieses Lesers im Büromodus,
Manual operation (Manuelle Bedienung)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Leser ist im Normalbetrieb (= Standard) 1 = Leser wird effektiv aus dem Zutrittskontrollsystem entfernt, das heißt, er ist „außer Betrieb“. Es werden keine Befehle empfangen. Alle anderen Parameter für diesen Leser sind ausgeschaltet. Der Parameter muss für Leser und Tür unabhängig gesetzt werden.

Check time models upon access (Zeitmodelle bei Begehung prüfen)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Zeitmodelle werden nicht kontrolliert. Es besteht keine Zeitbeschränkung für den Zutritt. 1 = Wenn dem Ausweisinhaber ein Zeitmodell zugewiesen wurde, entweder direkt oder als Raum-Zeit-Berechtigung, wird das Zeitmodell überprüft. (= Standard)
Zusätzliche Überprüfung	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = Verifikation durch Host ist nicht erforderlich 1 = Verifikation durch Host ist erforderlich (Standard) (**WICHTIG**: Die Aktivierung dieser Option ist für eine zusätzliche Videoverifikation durch den Bediener eines BVMS Systems oder Bosch Zutrittskontrollsystems erforderlich.)
Host request timeout (Wartezeit auf Antwort)	0 = Deaktiviert	0 = AMC funktioniert ohne Verifikation durch Host (funktioniert nicht mit Bereichsänderung oder Personenzählung). Dieses Kontrollkästchen ist nur aktiv, wenn Verifikation durch Host deaktiviert ist (0) und Open door if no answer from host (Tür öffnen, wenn Host nicht antwortet) aktiviert ist (1). 1 bis 9999 x 1/10 Sekunden (Standard = 330 = 33 Sekunden). Der Leser fordert eine Bestätigung des Zutrittskontrollsystems an. Wenn die Bestätigung nicht innerhalb dieses Zeitraums empfangen wird, überprüft der AMC den Parameter **Open door if no answer from host** (Tür öffnen, wenn Host nicht antwortet) und gewährt oder verweigert den Zutritt entsprechend.
Open door if no answer from host (Tür öffnen, wenn Host nicht antwortet)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Standard) (Kontrollkästchen ist aktiviert)	Dieses Kontrollkästchen ist nur aktiv, wenn der Parameter **Host verification** (Verifikation durch Host) gesetzt ist. 0 = Tür wird nicht geöffnet, wenn das Hostsystem nicht vor dem Timeout bestätigt. 1 (Standard) = Tür wird nach dem Timeout geöffnet, wenn das Hostsystem nicht vor dem Timeout bestätigt.

Konfigurieren eines Lesers: Zusätzliche Einstellungen

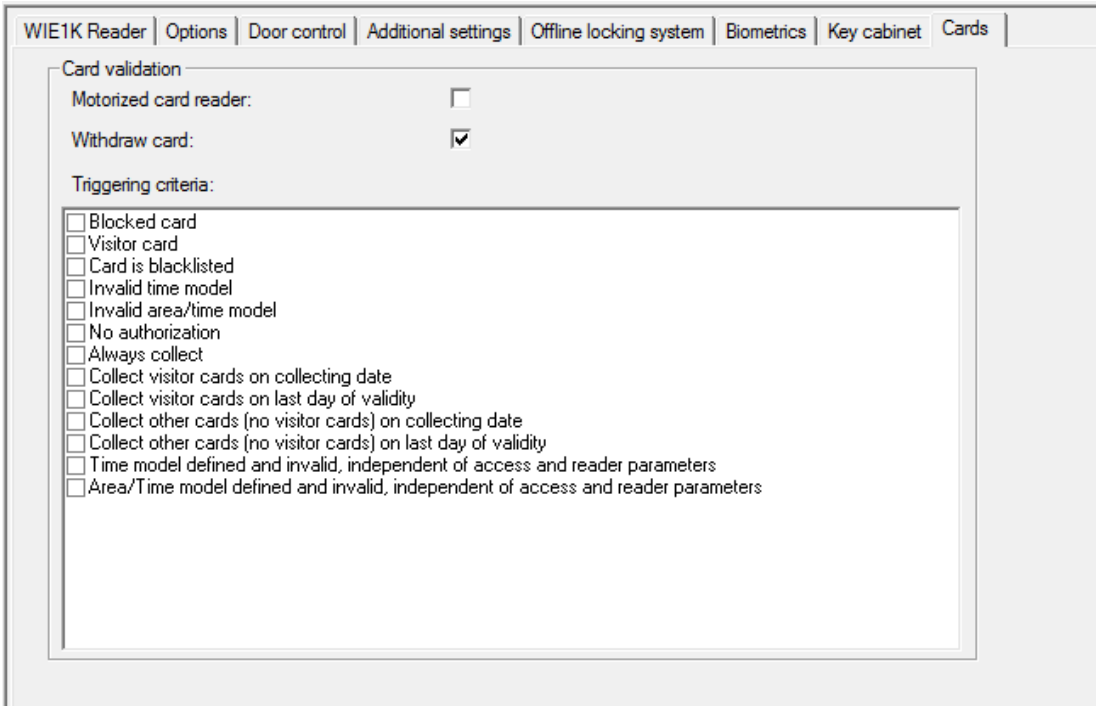


Parameter	Mögliche Werte	Bemerkung
Access sequence check (Zutrittsfolgekontrolle)	0 – Deactivated (0 – Ausgeschaltet) 1 – Activated; deactivate upon LAC malfunction (1 – Eingeschaltet, bei LAC Störung ausschalten) 2 – Activated; leave active upon LAC malfunction (2 – Eingeschaltet, bleibt bei LAC Störung aktiv) 3 – Activated; use strict sequence checking even when LAC malfunctions (3 – Eingeschaltet, bleibt aktiv, strikte Prüfung	0 = Leser nimmt an der Zutrittsfolgekontrolle nicht teil (= Standard). Mit aktivierter Folgekontrolle können UNBEKANNTE Personen wie folgt behandelt werden: 1 = Das erste Einlesen des Ausweises erfolgt ohne Kontrolle des Standorts. Alle Controller müssen online geschaltet sein. 2 = Das erste Einlesen des Ausweises erfolgt ohne Kontrolle des Standorts. 3 = Der Standort wird bei jedem Einlesen des Ausweises während der LAC Störung geprüft.

	erfordert manuelle Korrektur des Aufenthaltsortes)	
 Es gibt einen MAC-Befehl, um die Zutrittsfolgekontrolle generell zu aktivieren oder zu deaktivieren. 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. **Hinweis:** Mit diesem Befehl können Sie die Zutrittsfolgekontrolle nur für die Leser ändern, bei denen der Parameter **Enable access sequence** (Zutrittsfolge aktivieren) gesetzt ist. Die Zutrittsfolgekontrolle wird nicht für alle Leser deaktiviert/aktiviert.		
Time Management (Zeitwirtschaft)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Bei Auswahl sammelt das Zutrittskontrollsystem Daten für die Zeitwirtschaft gesammelt.
Double access control (anti-passback control) (Doppelzutrittskontrolle [Zutrittswiederholkontrolle])		
Enable (Aktivieren)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = ohne Doppelzutrittskontrolle (= Standard) 1 = mit Doppelzutrittskontrolle Innerhalb der Zeitspanne, die mithilfe des Parameters **Duration** (Dauer) 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 „-“ 2 Zeichen	Leser können mit einer Türgruppenkennung gruppiert werden. Wenn ein Ausweis an einem Leser eingelesen wird, werden nachfolgende Registrierungen an allen Lesern in der Türgruppe (Standard = **--**) gesperrt, bis das Zeitlimit verstrichen ist.
Anti-passback time out (Zeitlimit für Zutrittswiederholsperre)	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.

		Werte in Minuten. Standard = 5.
Random screening (Mitarbeiterauslosung)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	0 = keine Mitarbeiterauslosung 1 = Faktorabhängige Mitarbeiterauslosung erhält erst Zutritt, wenn Entsperrung durch den Dialog **Blocking** (Sperrung) erfolgt.
Screening rate (Auslosungsfaktor)	1 - 100	Prozentsatz der Mitarbeiterauslosung zur erweiterten Kontrolle. Verfügbar, wenn „random screening“ (Mitarbeiterauslosung) aktiviert ist.
Timeout random screening (Timeout-Mitarbeiterauslosung)	1 - 120	Innerhalb der Zeitspanne wird die Mitarbeiterauslosung auf den Benutzer angewendet. Werte in Minuten. Standard = 5.
REX button active when IDS armed (REX-Taste aktiv bei Scharfschaltung der EMA)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Nur bei **TM10** und **TM14**: 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.
Read permanently (Permanent lesen)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Der Leser liest permanent, wenn er mit der entsprechenden Firmware des Herstellers ausgestattet ist.

Konfigurieren eines Lesers: Ausweise



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

Hinweis!
Motorisierte Ausweisleser können nur mit IBPR-Lesern verwendet werden.

15.7.1 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.

15.8 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 Bediener der Zutrittskontrolle 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

15.9 AMC-Erweiterungen

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

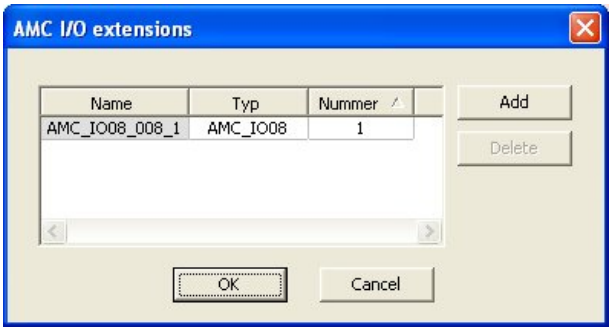
AMC Erweiterungen bieten zusätzliche Eingangs- und Ausgangssignale, wenn die acht Kontakte des AMC für den Anschluss der erforderlichen Kontakte (beispielsweise bei Aufzügen) nicht ausreichen.

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 Durchtritte erstellt. Erweiterungen können im Kontextmenü gewählt werden.

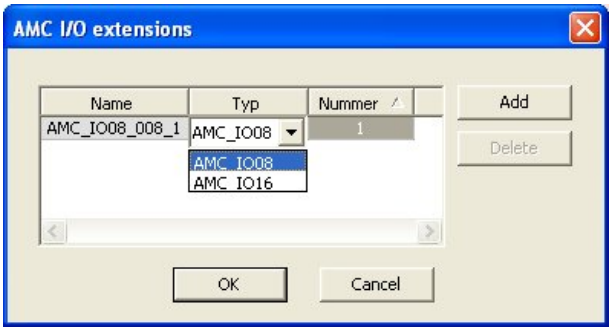
Ein Auswahldialog zum Erstellen der Erweiterungen wird angezeigt.



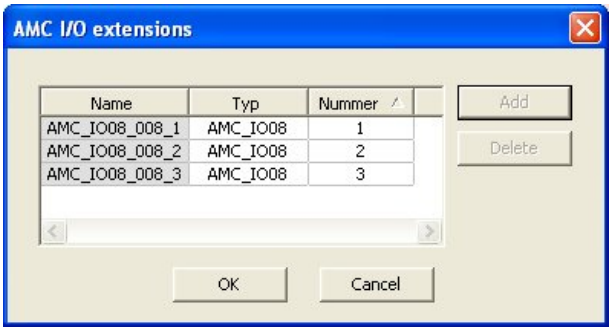
AMC-EXT ist in zwei Varianten verfügbar:

- 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

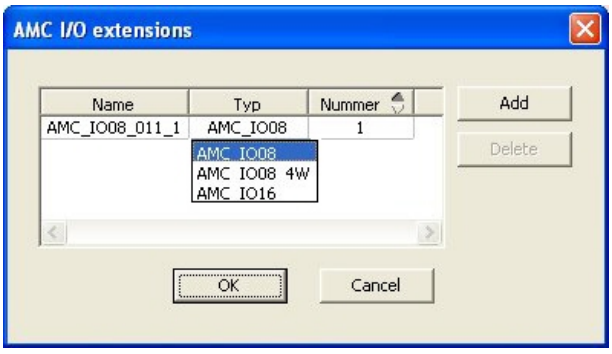
Es ist möglich, spezielle AMC Erweiterungen (AMC2 4W-EXT) für Controller mit Wiegand-Leserschnittstellen (AMC2 4W) zu konfigurieren. Diese Module bieten 4 zusätzliche Wiegand-Leseranschlüsse sowie jeweils 8 Eingangs- und 8 Ausgangskontakte. Somit kann die maximale Anzahl der Leser und Türen, die pro 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 Durchtritte 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 (Platinenname)	Alphanumerisch mit Einschränkungen: 1 – 16 Zeichen	Mit der Standard-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 (Platinenbeschreibung)	Alphanumerisch: 0 – 255 Zeichen	Dieser Text wird im OPC-Zweig angezeigt.
Board number (Platinennummer)	1 - 3	Nummer der an den AMC angeschlossenen Erweiterung. Schreibgeschütztes Feld.
Power supply (Stromversorgung)	0 = Deaktiviert (Kontrollkästchen ist deaktiviert) 1 = Aktiviert (Kontrollkästchen ist aktiviert)	Überwachung der Stromversorgung. Bei Spannungsausfällen wird eine Meldung nach Ablauf einer Verzögerung generiert. Bei der Überwachungsfunktion wird die Verwendung einer USV vorausgesetzt, sodass eine Meldung generiert werden kann.

		0 = keine Überwachung 1 = Überwachung aktiviert
Division (Mandant)	Standardwert **Common** (Allgemein)	Nur relevant, wo die **Mandantenfunktion** lizenziert ist.

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 Durchtritten gelöscht werden. Erst dann kann die AMC2 4W-EXT ebenfalls entfernt werden.

16 Angepasste Leserkonfigurationen

16.1 Einführung

Ab BIS 4.9 und AMS 4.0 ermöglichen Zutrittskontrollsysteme von Bosch die Verwendung angepasster MIFARE DESFire-Einstellungen. Sie können verschlüsselte Parameterdateien mit dem Hilfstool `Bosch.ReaderConfigTool.exe.` erstellen. Dieses Tool ist in den Setups für BIS ACE 4.9, AMS 4.0 und höhere Versionen mit eigener Dokumentation enthalten. In der Dokumentation finden Sie die aktuelle Liste der kompatiblen Leser.
In den folgenden Abschnitten wird beschrieben, wie Sie mit dem Geräteeditor eine verschlüsselte Parameterdatei importieren und auf einen oder alle kompatible Leser in der Hierarchie der Zutrittskontrollgeräte anwenden.

16.2 Die Lesereigenschaft: Extended reader parameters (Erweiterte Leserparameter)

Die verfügbaren erweiterten Parametersätze für kompatible Leser werden auf ihren Eigenschaftenseiten im Geräteeditor unter der Überschrift **Extended Reader Parameters** (Erweiterte Leserparameter) angezeigt.

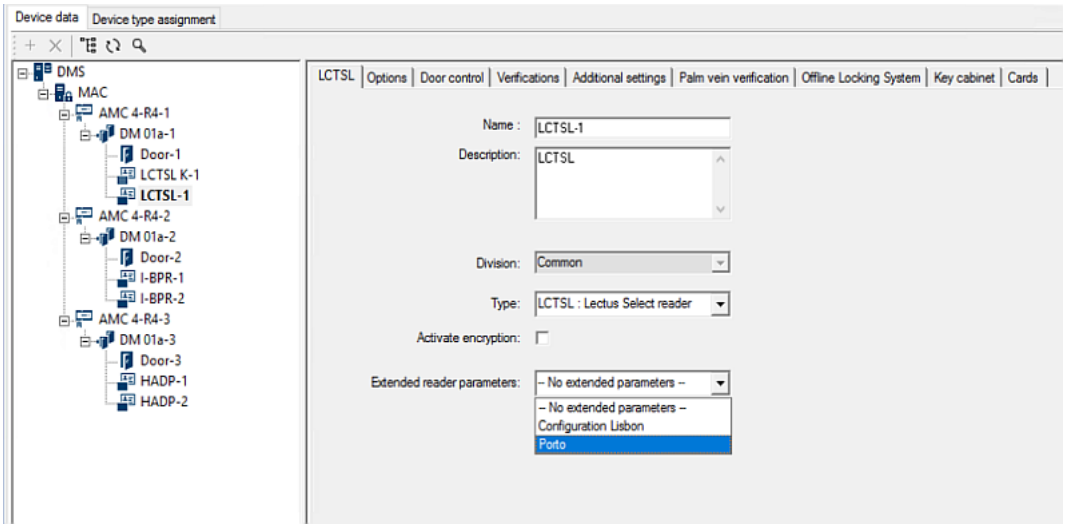


Abbildung 16.1: Extended reader parameters (Erweiterte Leserparameter)

Der Standardwert der Dropdownliste ist `No extended parameters`. Dies ist der einzige mögliche Wert, es sei denn, Sie importieren zusätzliche Parametersätze.

Vorgehensweise

So wenden Sie einen importierten Parametersatz auf einen kompatiblen einzelnen Leser an:

1. Wählen Sie im Geräteeditor im Gerätebaum den Leser aus.
2. Wählen Sie die erste Eigenschaftenregisterkarte aus.
3. Wählen Sie aus der Liste **Extended reader parameters** (Erweiterte Leserparameter) den gewünschten Parametersatz aus.
4. Klicken Sie auf **Apply** (Übernehmen) oder  .

16.3 Importieren eines Leserparametersatzes

Sie können Parameterdateien nur auf der DMS-Ebene der Gerätehierarchie importieren und löschen.

Voraussetzungen

Zugriff auf eine genehmigte Parameterdatei für Ihr Zutrittskontrollsystem. Standardmäßig hat die Datei den Typ *.ReaderConfigSave*.

Vorgehensweise

1. Klicken Sie im Geräteeditor mit der rechten Maustaste auf den DMS-Knoten und wählen Sie im Kontextmenü **Import reader parameter sets** (Leserparametersätze importieren) aus.
   Anschließend wird das Popup-Fenster **Import reader parameter sets** (Leserparametersätze importieren) angezeigt.
2. Klicken Sie auf **File** (Datei) und suchen Sie mithilfe des Datei-Explorers die Parameterdatei.
3. Geben Sie das Passwort der Parameterdatei ein, wenn Sie dazu aufgefordert werden. Wenn das Passwort korrekt ist, wird die untere Hälfte des Popup-Fensters mit den folgenden Informationen aufgefüllt:

– Die Liste der Lesertypen, auf die der Parametersatz angewendet wird.
– Der Name des Parametersatzes. Sie können den Namen in diesem Dialog bearbeiten.
– Eine Freitextbeschreibung, wenn der Ersteller des Parametersatzes ihn bereitgestellt hat. Sie können in diesem Dialog eine Beschreibung hinzufügen oder bearbeiten.

4. Klicken Sie auf **Import** (Importieren), um den Parametersatz für eine mögliche zukünftige Verwendung durch das Zutrittskontrollsystem zu importieren.

– Der Parametersatz wird importiert und im Zutrittskontrollsystem gespeichert.
– Er wird der Liste der verfügbaren Parametersätze oben im Popup-Fenster hinzugefügt.

5. Klicken Sie auf **Exit** (Beenden), um das Popup-Fenster **Import reader parameter sets** (Leserparametersätze importieren) zu verlassen.

16.4 Anwenden eines Parametersatzes auf Leser

Einführung

Durch das Importieren eines Parametersatzes in das Zutrittskontrollsystem wird dieser für eine zukünftige Verwendung gespeichert, jedoch nicht auf Leser im System angewendet. Die Anwendung des Parametersatzes stellt einen zusätzlichen Schritt dar, den Sie auf verschiedenen Ebenen der Gerätehierarchie ausführen können:

– DMS
– MAC
– AMC

Wenn Sie einen Parametersatz auf DMS-, MAC- oder AMC-Ebene anwenden, kann dieser nur auf untergeordnete Leser der Lesertypen angewendet werden, für die der Satz erstellt wurde. Alle anderen untergeordneten Leser bleiben unverändert.

Voraussetzungen

Sie haben erfolgreich einen Leserparametersatz importiert.

Vorgehensweise

1. Klicken Sie im Geräteeditor mit der rechten Maustaste auf einen Leser oder ein Gerät (DMS, MAC oder AMC), dessen Leser Sie parametrieren möchten.
2. Wählen Sie im Kontextmenü **Manage reader parameter sets** (Leserparametersätze verwalten) aus.
3. Wählen Sie im oberen Listenbereich **Parameter sets for reader types** (Parametersätze für Lesertypen) den Parametersatz aus, den Sie anwenden möchten.
   Die entsprechenden Leser werden im Bereich links unten aufgelistet: **Readers parametrizable with this parameter set** (Mit diesem Parametersatz parametrierbare Leser).

4. Wählen Sie in der Liste **Readers parametrizable with this parameter set** (Mit diesem Parametersatz parametrierbare Leser) die Leser aus, auf die Sie den ausgewählten Parametersatz anwenden möchten.
– Wenn die Anzahl der Leser groß ist, verwenden Sie die Dropdown-Listen, um die Anzeige auf untergeordnete Leser eines bestimmten MAC- oder AMC-Geräts einzuschränken.
5. Verwenden Sie die Pfeilschaltflächen, um ausgewählte Leser in den Bereich unten rechts zu verschieben: **All readers parametrized with the selected parameter set** (Alle mit dem ausgewählten Parametersatz parametrierten Leser).

Hinweis!
Anzeige kompatibler Leser
Es werden ausschließlich Leser aufgelistet, die mit dem Parametersatz kompatibel sind. Wenn Sie das Kontrollkästchen **Show all readers** (Alle Leser anzeigen) auswählen, werden auch Leser mit anderen Parametersätzen angezeigt. Diese werden mit einem grauen Hintergrund angezeigt, um sie für den ausgewählten Parametersatz als schreibgeschützt zu markieren.

6. Klicken Sie auf **OK**, um das Popup-Fenster zu schließen.
7. Klicken Sie im Geräteeditor auf **Apply** (Anwenden) oder auf .
Der Parametersatz wird auf alle Leser angewendet, die sich noch in der Liste **All readers parametrized with the selected parameter set** (Alle mit dem ausgewählten Parametersatz parametrierten Leser) befinden.

16.5 Verwalten von Leserparametersätzen

Einführung
Sie können die Anwendung von Parametersätzen auf verschiedenen Ebenen in der Gerätehierarchie ändern:
– DMS
– MAC
– AMC
Änderungen auf DMS-, MAC- oder AMC-Ebene können nur auf untergeordnete Leser der Lesertypen angewendet werden, für die der betreffende Satz erstellt wurde. Alle anderen untergeordneten Leser bleiben unverändert.

Voraussetzung
Sie haben erfolgreich einen Leserparametersatz importiert.

Vorgehensweise
1. Klicken Sie im Geräteeditor mit der rechten Maustaste auf einen Leser oder ein Gerät (DMS, MAC oder AMC).
2. Wählen Sie im Kontextmenü **Manage reader parameter sets** (Leserparametersätze verwalten) aus.
3. Wählen Sie im oberen Listenfeld **Parameter sets for reader types** (Parametersätze für Lesertypen) den Parametersatz aus, den Sie anwenden möchten.
– Die jeweiligen Leser werden im Bereich links unten aufgelistet: **Readers parametrizable with this parameter set** (Mit diesem Parametersatz parametrierbare Leser).
– Leser, auf die die Parameterdatei bereits angewendet wurde, werden im Bereich unten rechts aufgelistet: **All readers parametrized with the selected parameter set** (Alle mit dem ausgewählten Parametersatz parametrierten Leser).

4. Sie können Leser aus beiden Listen auswählen. Mit den Pfeilschaltflächen können Sie Leser in den Bereich und aus dem Bereich unten rechts verschieben: **All readers parametrized with the selected parameter set** (Alle mit dem ausgewählten Parametersatz parametrierten Leser).
– WICHTIG: Notieren Sie sich die Leser, die Sie aus der Liste entfernen, da sie die Namen dieser Leser für den letzten Schritt in diesem Verfahren benötigen.
5. Wenn Sie die Änderungen abgeschlossen haben, klicken Sie auf **OK**, um das Popup-Fenster zu schließen.
6. Klicken Sie im Geräteeditor auf **Apply** (Übernehmen) oder  .
– Der Parametersatz wird auf alle Leser angewendet, die sich noch in der Liste **All readers parametrized with the selected parameter set** (Alle mit dem ausgewählten Parametersatz parametrierten Leser) befinden.
– Er wird von den Lesern entfernt, die Sie aus dieser Liste entfernt haben.
7. Führen Sie für alle Leser, die Sie aus der Liste entfernt haben, einen der folgenden Schritte aus:
– Setzen Sie die Leser mit den DIP-Schaltern in der Leser-Hardware auf die Werkseinstellungen zurück.
– Wenden Sie einen anderen Parametersatz auf die Leser an.

Hinweis!
Durch das Löschen eines Parametersatzes werden die Leser, die diesen verwendet haben, nicht neu konfiguriert.
Die Leser, für die Parametersätze gelöscht wurden, behalten ihre Konfiguration bei, bis Sie die Leser-Hardware zurücksetzen oder einen anderen Parametersatz anwenden.

16.6 Löschen von Leserparametersätzen

Sie können Parameterdateien nur auf der DMS-Ebene der Gerätehierarchie importieren und löschen.

Voraussetzungen
Es wurde mindestens eine Parameterdatei bereits in Ihr Zutrittskontrollsystem importiert.

Vorgehensweise
1. Klicken Sie im Geräteeditor mit der rechten Maustaste auf den DMS-Knoten und wählen Sie im Kontextmenü **Delete reader parameter sets** (Leserparametersätze löschen) aus. Anschließend wird das Popup-Fenster **Delete reader parameter sets** (Leserparametersätze löschen) angezeigt.
2. Wählen Sie in der Liste **Parameter sets for reader types** (Parametersätze für Lesertypen) den Parametersatz aus, den Sie löschen möchten.
– Anschließend wird unten rechts im Popup-Fenster die Liste aller Leser angezeigt, die zurzeit mit dem ausgewählten Parametersatz parametriert (konfiguriert) sind.
– Notieren Sie sich diese Leser, da sie nach dem Löschen des Parametersatzes zurückgesetzt oder neu konfiguriert werden müssen. Weitere Informationen hierzu finden Sie im letzten Schritt dieses Verfahrens.
3. Klicken Sie auf **Delete** (Löschen).
4. Klicken Sie auf **Exit** (Beenden).
5. Klicken Sie im Geräteeditor auf **Apply** (Übernehmen) oder  .
6. Führen Sie für alle Leser, die den gelöschten Parametersatz verwendet haben, einen der folgenden Schritte aus:

– Setzen Sie die Leser mit den DIP-Schaltern in der Leser-Hardware auf die Werkseinstellungen zurück.
– Wenden Sie einen anderen Parametersatz auf die Leser an.

Hinweis!
Durch das Löschen eines Parametersatzes werden die Leser, die diesen verwendet haben, nicht neu konfiguriert.
Die Leser, für die Parametersätze gelöscht wurden, behalten ihre Konfiguration bei, bis Sie die Leser-Hardware zurücksetzen oder einen anderen Parametersatz anwenden.

17 Benutzerdefinierte Felder für Personaldaten

Einführung

Datenfelder für Personal sind auf verschiedene Arten anpassbar:

- ob sie **sichtbar** sind, d. h. ob sie im 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 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.

17.1 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:

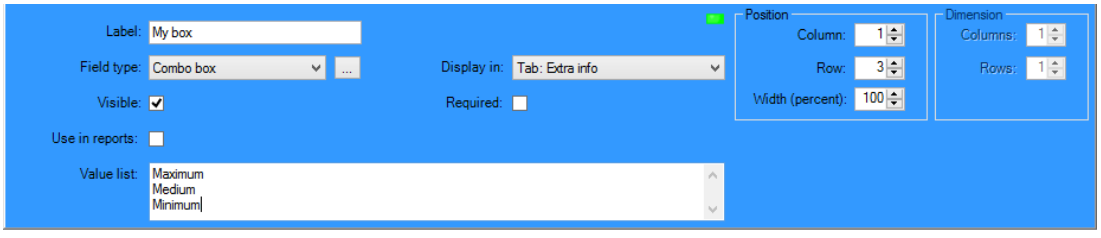
Overview (Übersicht) Diese Registerkarte und ihre Unterregisterkarten **Address, Contact, Additional person data, Additional Company data, Remarks, Card Control** und **Extra Info** (Adresse, Kontaktinformationen, Zusätzliche Personendaten, Zusätzliche Firmendaten, Anmerkungen, Ausweiskontrolle und Reserve)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

Beschriftungstext	Beschreibung
Label (Beschriftung)	**Label** (Beschriftung) ist die Beschriftung des Datenfelds, wie es im Client erscheint. Es kann nach Belieben verändert werden, um der Terminologie Ihres Standorts zu entsprechen.
Field type (Feldtyp)	**Field type** (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. – **Text field** (Textfeld) – Klicken Sie auf die daneben liegende Schaltfläche mit den Auslassungspunkten, um die Anzahl der zulässigen Zeichen festzulegen. – **Check box** (Kontrollkästchen) – **Date field** (Datumsfeld) – **Time** (Uhrzeit) – **Date-time field** (Datum-Zeit-Feld) – **Combo box** (Auswahllistenfeld) – Geben Sie die gültigen Werte für das Auswahllistenfeld in das entsprechende Textfeld ein. Trennen Sie sie durch Kommas oder Zeilenumbrüche. – **Numerical input** (Numerische Eingabe) – Geben Sie in den dafür vorgesehenen Drehfeldern Ihren minimalen und maximalen Wert für die numerische Eingabe ein. – **Building control 1** und **Building control 2** (Gebäudesteuerung) – Dies sind spezielle Steuerelemente, die hier umbenannt werden können (im Feld **Label**; 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.
Visible (Sichtbar)	Deaktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass das Datenfeld im Client angezeigt wird.
Unique (Einzigartig)	Aktivieren Sie dieses Kontrollkästchen, um sicherzustellen, dass die in diesem Feld eingegebenen Werte einzigartig sind. Das System lehnt dann die Eingabe eines beliebigen Werts ab, der bereits für dieses Feld in der Datenbank gespeichert wurde. So sollten z. B. Personalnummern für Personen und Kennzeichen für Fahrzeuge einzigartig sein.
	Das grüne Licht bedeutet, dass dieses Datenfeld in der Datenbank derzeit **nicht** verwendet wird. Das rote Licht bedeutet, dass dieses Datenfeld momentan in der Datenbank verwendet wird.
Display in (Angezeigt in)	Verwenden Sie diese Dropdown-Liste, um die Registerkarte im Client auszuwählen, in der das Datenfeld angezeigt werden soll.

Beschriftungstext	Beschreibung
Required (Pflichtfeld)	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. Beachten Sie, dass erforderliche Datenfelder nicht mit dem Kontrollkästchen **Visible** (Sichtbar) unsichtbar gemacht werden können. Für mehr Benutzerfreundlichkeit im Client wird empfohlen, alle erforderlichen Felder auf der ersten Registerkarte zu platzieren.
Position	Verwenden Sie die Drehfelder **Column** (Spalte) und **Row** (Zeile), um die Datenfelder auf der in der Dropdown-Liste **Display in** (Angezeigt in) festgelegten Registerkarte zu positionieren. Beachten Sie, dass der Editor Ihnen nicht erlaubt, eine bereits verwendete Position auszuwählen oder vorhandene Datenfelder zu überlagern. Verwenden Sie das Drehfeld **Width (percent)** (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.
Dimension (Abmessung)	Verwenden Sie die Drehfelder für **Column** (Spalte) und **Row** (Zeile), um die Anzahl der Spalten und Zeilen anzugeben, die auf der in der Dropdown-Liste angegebenen Registerkarte **Display in** (Angezeigt in) belegt werden sollen. Beachten Sie, dass Sie mit dem Editor keine vorhandenen Datenfelder überlagern können.

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:

Use in reports (In Berichten nutzen) (Kontrollkästchen)	Aktivieren Sie dieses Kontrollkästchen, damit das neue Datenfeld in den Standardberichten erscheint.
Sequence number (Sequenznummer) (Drehfeld)	Die Sequenznummer bestimmt die Spalte, die das Datenfeld in den Standardberichten belegen wird.

Hinweis!

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

17.2 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.

18 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.

18.1 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 Mitarbeiterauslosung von diesem Personentyp oder Lesegerät ausgelöst wird.

18.2 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.

18.3 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.

18.3.1 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.

18.3.2 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

18.3.3 Erstellen eines Lesersicherheitsprofils

In diesem Abschnitt wird beschrieben, wie Sicherheitsprofile für verschiedene Lesetypen 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.

18.3.4 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 Lesesicherheitsprofil 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 **Auslosungsfaktor** 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 **Auslosungsfaktor** der Leser angezeigt, wie sie wären, wenn die ausgewählte Bedrohungsstufe in Betrieb wäre.

18.3.5 Zuweisen einer Bedrohungsstufe zu einem Hardwaresignal

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.

18.4 Konfigurationsschritte in Systemdatendialogen

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

18.4.1 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 R	Auslosungsfaktor (%) im Personensicherheitsprofil P	Person für zusätzliche Sicherheitsüberprüfungen ausgewählt?
0	Beliebig	**Nein**
100	Beliebig	**Ja**
1..99	0	**Nein**
1..99	100	**Ja**
1..99	1..99	**Mögliche** Wahrscheinlichkeit = MAX(R,P)

18.4.2 Zuweisen eines Personensicherheitsprofils zu einem Personentyp

Dialogpfad

– **Main menu** (Hauptmenü) > **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.

18.5 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.

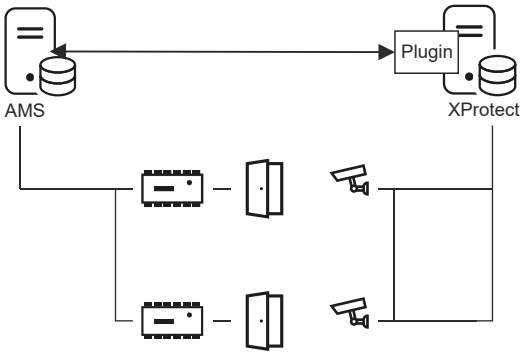
Siehe

– *Zuweisen eines Personensicherheitsprofils zu einem Personentyp, Seite 144*
– *Anlegen und Verwalten von Personaldaten, Seite 189*

19 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 Maustasten 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.

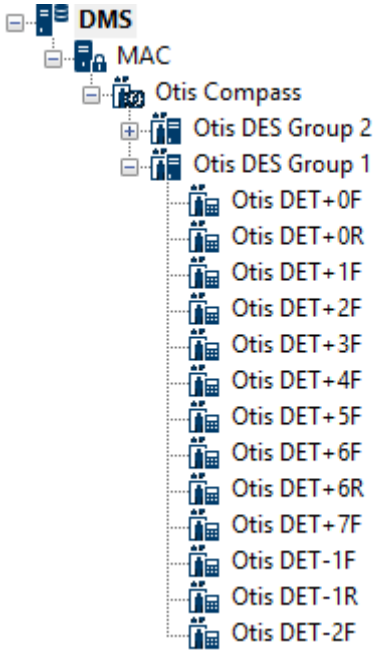
20 Integrieren von Otis Compass

Einführung

Compass ist ein Zielwahlsteuerungssystem des Unternehmens Otis Elevator. Es dient dazu, mehrere Aufzugsgruppen zu verwalten und Aufzüge Fahrgästen zuzuweisen, damit diese ihre Ziele so effizient wie möglich erreichen können. Zum Bereitstellen der notwendigen Daten drücken Fahrgäste nicht mehr einfach auf die **Aufwärts**- oder **Abwärts**-Tasten, sondern geben Ihre Ziele über Ausweisleser, Touchscreens oder Terminals mit Tastatur an.
Die Integration mit Bosch Zutrittskontrollsystemen erhöht die Sicherheit. Auf Grundlage ihrer Ausweise und der aktuellen Zeitmodelle gelangen Fahrgäste effizient zu ihren eigenen Etagen und anderen autorisierten Zielen. Anfragen für Etagen, die nicht in den Berechtigungsprofilen des Fahrgasts enthalten sind, oder zu einer Tageszeit, die sich außerhalb des aktuellen Zeitmodells befindet, werden vom System nicht akzeptiert.

Hardware-Topologie eines Compass-Systems

Die Hardware eines Compass-Systems wird von oben nach unten als 3-Ebenen-Hierarchie unter einem einzelnen MAC im Geräteeditor konfiguriert.

<table>
<tr>
<td> 

Die obige Hierarchie zeigt:
ein Otis Compass-System auf einem dedizierten MAC
eine einzelne Aufzugsgruppe, die von einem DES gesteuert wird
eine Reihe von Terminals (DET), jedes mit einer Etagennummer von -2 bis +7 und F (front) oder R (rear) für die vorderen oder hinteren Türen</td>
<td>Erste Ebene: (Otis Compass)
Das Zielwahlsteuerungssystem. Jedes Compass-System kann bis zu 8 Aufzugsgruppen steuern.
Parameter: Etagenbereich, Netzwerkadressen, Portnummern und Timeouts.

Zweite Ebene: (Otis DES/DER)
Bis zu 8 Aufzugsgruppen, die jeweils von einem logischen Destination Entry Server (DES), bestehend aus 1 oder 2 physischen Geräten, verwaltet werden.
Darüber hinaus kann diese Ebene bis zu zwei optionale Geräte zur Optimierung enthalten, die als Destination Entry Redirectors (DER) bezeichnet werden.
Parameter: 1 Gruppenkennung pro Aufzugsgruppe.
1 IP-Adresse pro Gerät.
Die Tabelle der Etagen mit Aufzugtüren, und ob sie öffentlich zugänglich sind.

Dritte Ebene: (Otis DET)
Die Destination Entry Terminals (DET).
Parameter: 1 IP-Adresse pro Terminal.
Erreichbare Etagen mit Aufzugtüren für jedes Terminal.</td>
</tr>
</table>

Überblick der Integration in das Zutrittskontrollsystem

Die Administratoren des Zutrittskontrollsystems können Compass in den folgenden Phasen integrieren, die später im Kapitel ausführlich beschrieben werden:

1. Konfigurieren von Compass-Hardware mit einem einzelnen MAC im Geräteeditor
2. Konfigurieren von benutzerdefinierten Feldern für Otis-spezifische Eigenschaften von Ausweisinhabern, z. B. eigene Etage
3. Erstellen von Berechtigungsprofilen, die den Zutritt zu bestimmten Aufzugszielen regeln
4. Zuweisen von Berechtigungsprofilen zu den entsprechenden Ausweisinhabern

20.1 Konfigurieren eines Compass-Systems im Geräteeditor

In diesem Abschnitt werden die Schritte zur Konfiguration eines Otis Compass-Systems im Geräteeditor beschrieben.

Dialogpfad

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

20.1.1 Ebene 1: Einrichten des Compass-Systems

Vorgehensweise für Ebene 1: Einrichten des Compass-Systems

1. Wählen Sie den gewünschten MAC in der Baumstruktur des Geräteeditors aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **New Otis Compass** (Neuer Otis Compass) aus. Die Eigenschaftsseite enthält zwei Registerkarten:
   – **Otis Compass**
   – **Floors** (Etagen)
3. Die folgenden wichtigen Parameter müssen Sie auf der Registerkarte **Otis Compass** festlegen:
   – **Name** (der Name, der im Gerätebaum angezeigt werden soll)
   – **MAC IP-Address** (MAC IP-Adresse) (Die Callback-IP-Adresse für das Compass-System auf einer dedizierten Netzwerkkarte, über die das Compass-System mit dem MAC kommuniziert.
   HINWEIS: Dies ist **nicht** die IP-Adresse des MAC selbst.)
   – **Division** (Mandant) (ausschließlich dann, wenn Mandanten lizenziert sind und in Ihrer Installation verwendet werden)

Behalten Sie die Standardwerte für die restlichen Parameter, es sei denn, Sie wurden vom technischen Support dazu angewiesen. Sie werden in der folgenden Tabelle kurz erklärt:

Parameter	Standardwert	Beschreibung
MC group address (MAC-Gruppenadresse)	234.46.30.7	IP address for the multicast group (IP-Adresse für die Multicast-Gruppe)
MC port for DES/DER remote (MC-Port für DES/DER remote) MC port for DES/DER local (MC-Port für DES/DER lokal)	48307 47307	Multicast ports (Multicast-Ports)
UDP port for DES/DER remote (UDP-Port für DES/DER remote)	46303 45303	UDP ports for the DES and DER devices (UDP-Ports für DES- und DER-Geräte)

Parameter	Standardwert	Beschreibung
UDP port for DES/DER local (UDP-Port für DES/DER lokal)		
UDP port for DET remote (UDP-Port für DET remote) UDP port for DET local (UDP-Port für DET lokal)	45308 46308	UDP ports for the DET devices (UDP-Ports für DET-Geräte)
Multicast Time-to-Live (TTL)	5 Sekunden	
Heartbeat-Intervall	1 Sekunde	Der Zeitraum zwischen Heartbeat-Signalen. Diese Signale zeigen anderen Geräten, dass ein Gerät „lebendig“ (funktionsfähig) ist.
Max. Anzahl verpasster Heartbeats	3	Anzahl der Heartbeats, die verpasst werden können, bevor ein Gerät als „tot“ (nicht mehr funktionsfähig) angesehen wird.
Meldungs-Timeout	1 Sekunde	
Meldungswiederholungen	3	

1. Klicken Sie auf der Registerkarte **Floors** (Etagen) auf **Change floor range** (Etagenbereich ändern).
2. Geben Sie die Nummern der untersten und obersten Etagen ein, die von allen Aufzugsgruppen des Otis Compass-Systems bedient werden sollen.
   – Der maximale Bereich ist -127 bis +127.
3. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

20.1.2 Ebene 2: Aufzugsgruppen, DES- und DER-Geräte

Vorgehensweise für Ebene 2: Einrichten der Aufzugsgruppen (DES/DER-Geräte)
Einführung
Der DES (Destination Entry Server) ist der Computer, der eine Aufzugsgruppe verwaltet. Auf Wunsch können zwei physische DES-Geräte mit separaten IP-Adressen in einem logischen DES mit Failover-Funktion kombiniert werden.
Der DER (Destination Entry Redirector) verbindet Aufzugsgruppen und ermöglicht es DETs an einem gemeinsamen Eintrittspunkt im Gebäude, z. B. der Lobby, Zielanfragen für jede Etage im Gebäude zu akzeptieren. Der DER ist nicht für die Funktion in einem Failover-Modus konfiguriert.

Erstellen von DES-Geräten im Gerätebaum:
1. Wählen Sie den gewünschten Otis Compass in der Baumstruktur des Geräteeditors aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **New Otis DES** (Neuer Otis DES) aus. Die Eigenschaftsseite enthält zwei Registerkarten:
   – **Otis DES**
   – **Floors** (Etagen)
3. Legen Sie auf der Registerkarte **Otis DES** die folgenden Parameter fest:

- **Name**: der Name, der im Gerätebaum angezeigt werden soll.
  Verwenden Sie ein systematisches Benennungsschema, das eine klare Orientierung für die Konfiguratoren von DES- und DET-Geräten zu einem späteren Zeitpunkt im Konfigurationsprozess bietet.
- **Description** (Beschreibung) (optional): eine Freitextbeschreibung des Geräts.
- **Group** (Gruppe): eine Ganzzahl zwischen 1 und 10. Diese Ganzzahl muss bei allen Aufzugsgruppen (durch ihre DES/DER-Geräte bezeichnet) in diesem Otis Compass-System eindeutig sein. Sie können Ihre Geräteänderungen nicht speichern, wenn Sie dieselbe **Gruppen**nummer mehrmals verwenden.
- **1st IP address** (1. IP-Adresse): die IP-Adresse dieses DES-Geräts.
- **2nd IP address** (2. IP-Adresse): Wenn dieser DES einen redundanten Zwilling hat, geben Sie hier seine IP-Adresse ein.
- **Division** (Mandant) (ausschließlich dann, wenn Mandanten lizenziert sind und in Ihrer Installation verwendet werden)

Auf der Registerkarte **Floors** (Etagen) werden die für Ebene 1 (das Compass-System) definierten Etagen als Tabelle mit bearbeitbaren Zellen dargestellt.

Erstellen von DER-Geräten im Gerätebaum:
DER-Geräte werden mit beinahe derselben Vorgehensweise wie DES-Geräte erstellt. Der einzige Unterschied besteht darin, dass ein DER kein Failover-Gerät benötigt, also keinen Parameter für die **2. IP-Adresse** hat.

Aufzugsgruppen-Beispiel.
Das folgende Beispiel zeigt die Etagen für eine 10-stöckige Aufzugsgruppe mit vorderen und hinteren Türen sowie öffentlich zugänglichem Erdgeschoss und 6. Etage.

OTIS DES | Floors

Highest floor: 7

Lowest floor: -2

Change floor range

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

1. Aktivieren Sie in der Spalte **Front door** (Vordere Tür) die Kontrollkästchen aller Etagen, auf denen der Aufzug seine vordere Tür verwendet.
2. Aktivieren Sie ggf. die Kontrollkästchen bei **Rear door** (Hintere Tür) nach demselben Prinzip.
3. Aktivieren Sie für die Spalte **Front door publicly accessible** (Vordere Tür, öffentlich zugänglich) die Kontrollkästchen der Etagen, die für alle Fahrgäste ohne Einschränkung zugänglich sind.

4. Aktivieren Sie ggf. die Kontrollkästchen bei **Rear door publicly accessible** (Hintere Tür, öffentlich zugänglich) nach demselben Prinzip.
5. (Optional) Klicken Sie auf dieser Registerkarte auf **Change floor range** (Etagenbereich ändern), um den auf der Ebene **Otis Compass** festgelegten Etagenbereich weiter einzuschränken.
6. Überschreiben Sie die Standardnamen in den Spalten **Name** und **Description** (Beschreibung) mit aussagekräftigen Alternativen.
7. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

20.1.3 Ebene 3: DET-Geräte

Vorgehensweise für Ebene 3: Einrichten der Terminals (DET-Geräte)
Einführung:
Ein DET (auch als DEC/Destination Entry Computer bezeichnet) liest physische Anmeldedaten oder PIN-Codes. Ein DET kann sich auf einer bestimmten Etage außerhalb der vorderen oder hinteren Tür eines Aufzugs oder in der Aufzugskabine befinden.

Erstellen von DET-Geräten im Gerätebaum:
1. Wählen Sie das gewünschte Otis DES/DER-Gerät in der Baumstruktur des Geräteeditors aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **New Otis terminal** (Neues Otis Terminal) aus.
   – Ein Popup-Fenster **Create Otis terminals** (Otis Terminals erstellen) wird angezeigt.
3. Geben Sie die Anzahl der Terminals ein, die Sie auf diesem DES/DER konfigurieren möchten.
4. Akzeptieren Sie die Standardwerte oder geben Sie neue Startwerte für die vier Oktette seiner IP-Adresse ein.
   – Aktivieren Sie für jedes Oktett, aber typischerweise für das vierte, das Kontrollkästchen **Automatic increment** (Automatische Erhöhung), wenn Sie möchten, dass das System durch Erhöhen des Oktetts eine eindeutige IP-Adresse für jedes Terminal konfigurieren soll.
5. Klicken Sie auf **OK**.
   – Die gewünschte Anzahl von DET-Geräten wird im Gerätebaum erstellt.
   – Ihre IP-Adressen werden erhöht, wie im vorherigen Schritt festgelegt.

Konfigurieren von DET-Geräten
Die Eigenschaftsseite für jedes DET enthält zwei Registerkarten:
– **Otis terminal** (Otis Terminal)
– **Floors** (Etagen)
1. Legen Sie auf der Registerkarte **Otis terminal** (Otis Terminal) die folgenden Parameter fest:
   – **Name**: der Name, der im Gerätebaum angezeigt werden soll.
   – **Description** (Beschreibung) (optional): eine Freitextbeschreibung des Geräts.
   – **IP address** (IP-Adresse): die IP-Adresse dieses DET-Geräts.

– **Operational mode** (Betriebsmodus) *1..4*:
Hiermit wird festgelegt, wie das Terminal Ziele von Fahrgästen anfordert und die Anfragen für die Validierung an den DES/DER übergibt. Die folgende Tabelle enthält Details:

Modus	**Beschreibung**	**Verhalten**
1	Default floor (Standardetage)	(Standardbetriebsmodus) Der Fahrgast präsentiert seinen Ausweis oder gibt einen PIN-Code ein. Wenn der Ausweis oder die PIN gültig ist und der Fahrgast keine weiteren Eingaben macht, fordert der DET vom DES die Standard- oder „eigene“ Etage des Fahrgasts an. Wenn der Fahrgast eine andere Zieletage eingibt, fordert das DET dieses Ziel vom DES an.
2	Access to authorized floors (Zutritt zu autorisierten Etagen)	Der Fahrgast präsentiert seinen Ausweis oder gibt einen PIN-Code ein und gibt anschließend eine Zieletage ein. Das DET fordert dieses Ziel vom DES an. Das Zutrittskontrollsystem gewährt oder verweigert den Zutritt zum angeforderten Ziel.
3	User entry of destination floor (Benutzereingabe der Zieletage)	Der Fahrgast betritt eine Zieletage. Wenn das Ziel öffentlich zugänglich ist, fordert das DET das Ziel vom DES an. Andernfalls fordert das DET den Fahrgast auf, seinen Ausweis für die Validierung zu präsentieren.
4	Default floor or User entry of destination floor (Standardetage oder Benutzereingabe der Zieletage)	Der Fahrgast präsentiert seinen Ausweis oder gibt einen PIN-Code ein. Wenn der Ausweis oder die PIN gültig ist, fordert der DET vom DES die Standard- oder „eigene“ Etage des Fahrgasts an. Innerhalb eines festgelegten Timeout-Zeitraums kann der Fahrgast die Auswahl der Standardetage überschreiben und ein anderes Ziel auswählen.

– **Audit records** (Prüfprotokoll): Aktivieren Sie dieses Kontrollkästchen, um Fahrgasteingaben an diesem Terminal für das Logbuch zu erfassen.
– **PIN code** (PIN-Code): Aktivieren Sie dieses Kontrollkästchen, um die Verwendung eines Identifikations-PIN-Codes an diesem Terminal als Alternative zu physischen Ausweisen zuzulassen.
Hinweis: Verwenden Sie Bekanntmachungsleser vom Typ **Dialog PIN card (enter)** (Dialog PIN Ausweis (Eingabe)), um PIN-Codes für die Verwendung an Otis Terminals zu registrieren.
– **Time models** (Zeitmodelle): Aktivieren Sie dieses Kontrollkästchen, damit Zeitmodelle die Verwendungszeiten für dieses Terminal einschränken können.

– **Division** (Mandant) (ausschließlich dann, wenn Mandanten lizenziert sind und in Ihrer Installation verwendet werden)

Auf der Registerkarte **Floors** (Etagen) der Eigenschaftsseite **Otis terminal** (Otis Terminal) werden die für Ebene 2 (den DES/DER) definierten Etagen als Tabelle mit bearbeitbaren Zellen dargestellt.
Hinweis: Das für Ebene 2 definierte Benennungsschema sollte eine klare Orientierung bieten. Andernfalls sollten Sie Ihre Arbeit speichern und zu Ebene 2 zurückkehren, um das Benennungsschema abzuschließen.

1. Wählen Sie nacheinander jedes DET aus, das Sie soeben im Gerätebaum erstellt haben, und öffnen Sie die Registerkarte **Floors** (Etagen).
   – Die Tabelle **Floors** (Etagen) wird angezeigt.
2. Aktivieren Sie in der Spalte **Front door** (Vordere Tür) die Kontrollkästchen jeder Etage, die vom aktuellen DET aus erreichbar sein soll.
3. Aktivieren Sie in der Spalte **Front door publicly accessible** (Vordere Tür öffentlich zugänglich) die Kontrollkästchen jeder vorderen Tür, die öffentlich zugänglich sein soll, d. h. ohne ausdrückliche Berechtigung.
4. (Optional) Wählen Sie in der Spalte **Time model for front door** (Zeitmodell für vordere Tür) ein Zeitmodell aus, um den öffentlichen Zutritt zur vorderen Tür auf dieser Etage ggf. einzuschränken. Beispielsweise kann die Restaurant-Etage nur zu bestimmten Tageszeiten zugänglich sein.
5. Wiederholen Sie ggf. die vorherigen Schritte für die Spalten **Rear door** (Hintere Tür), **Rear door publicly accessible** (Hintere Tür öffentlich zugänglich) und **Time model for rear door** (Zeitmodell für hintere Tür).
6. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

Beispiel:
Das folgende Beispiel zeigt die Etagen für eine 10-stöckige Aufzugsgruppe mit den Etagen und Türen, die über die vordere Aufzugtür in der Lobby erreichbar sind. Der Zutritt zur Restaurant-Etage ist sowohl bei der vorderen als auch hinteren Aufzugtür durch ein Zeitmodell eingeschränkt.

OTIS terminal | Floors

Highest floor: 7
Lowest floor: -2
Change floor range

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

20.2 Konfigurieren von benutzerdefinierten Feldern für Otis-spezifische Eigenschaften von Ausweisinhabern

Einführung

In diesem Abschnitt wird das Erstellen der benutzerdefinierten Felder beschrieben, in denen Bediener die Otis-spezifischen Eigenschaften für einen Ausweisinhaber eingeben können, insbesondere die „eigene Etage“ oder das Standardziel des Ausweisinhabers. Diese „eigene Etage“ muss mit **drei Koordinaten** definiert werden:

1. Aufzugsgruppe
2. Etage
3. Tür

Beachten Sie, dass Bediener bei der Angabe der „eigenen Etage“ eines Ausweisinhabers im Zutrittskontrollsystem-Client die Daten in derselben Reihenfolge eingeben muss: Aufzugsgruppe, Etage, Tür. Aus diesem Grund sollten die drei benutzerdefinierten Felder in Lesereihenfolge positioniert werden, vorzugsweise von oben nach unten.

Klicken Sie auf **OK**, um alle Popup-Meldungen zu bestätigen, die darauf hinweisen, dass Sie alle drei Koordinaten erstellen müssen.

Definieren Sie die drei erforderlichen benutzerdefinierten Felder sowie alle weiteren gewünschten Otis-spezifischen Optionen, damit diese auf der Registerkarte **Elevators** (Aufzüge) in der Bedienoberfläche des Zutrittskontroll-Clients angezeigt werden.

Allgemeine Informationen zum Konfigurieren von benutzerdefinierten Feldern finden Sie in der ACE/AMS-Konfigurationshilfe unter **Benutzerdefinierte Felder für Personaldaten**.

Dialogpfad

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

Vorgehensweise

Wählen Sie auf der Eigenschaftenseite **Custom fields** (Benutzerdefinierte Felder) die Registerkarte **Elevators** (Aufzüge) aus.

Erste Koordinate: Aufzugsgruppe

1. Doppelklicken Sie auf der Registerkarte in eine Zelle und klicken Sie auf **Yes** (Ja), um ein neues Eingabefeld zu erstellen.
2. Wählen Sie in der Liste **Field type** (Feldtyp) die Option **Otis DES selection** (Otis DES-Auswahl) aus.
3. Geben Sie im Feld **Label** (Beschriftung) *Elevator Group* ein.
4. Wählen Sie in der Liste **Display in** (Angezeigt in) die Option *Tab:Elevators* aus.
5. Wählen Sie in der Gruppe **Position** einen eindeutigen Ort auf der Registerkarte **Elevators** (Aufzüge) aus, an dem dieses benutzerdefinierte Feld angezeigt werden soll.

Zweite Koordinate: Eigene Etage

1. Klicken Sie auf **New field** (Neues Feld), um ein neues benutzerdefiniertes Feld zu erstellen.
2. Wählen Sie in der Liste **Field type** (Feldtyp) die Option **Home floor** (Eigene Etage) aus.
3. Geben Sie im Feld **Label** (Beschriftung) *Home floor* ein.
4. Wählen Sie in der Liste **Display in** (Angezeigt in) die Option *Tab:Elevators* aus.
5. Wählen Sie in der Gruppe **Position** einen eindeutigen Ort auf der Registerkarte **Elevators** (Aufzüge) aus, an dem dieses benutzerdefinierte Feld angezeigt werden soll. Für eine höhere Benutzerfreundlichkeit sollte sich das Feld unter der vorherigen Koordinate befinden.

Dritte Koordinate: Ausgangstür

1. Klicken Sie auf **New field** (Neues Feld), um ein neues benutzerdefiniertes Feld zu erstellen.
2. Wählen Sie in der Liste **Field type** (Feldtyp) die Option **Exit door** (Ausgangstür) aus.
3. Geben Sie im Feld **Label** (Beschriftung) *Exit door* ein.
4. Wählen Sie in der Liste **Display in** (Angezeigt in) die Option *Tab:Elevators* aus.
5. Wählen Sie in der Gruppe **Position** einen eindeutigen Ort auf der Registerkarte **Elevators** (Aufzüge) aus, an dem dieses benutzerdefinierte Feld angezeigt werden soll. Für eine höhere Benutzerfreundlichkeit sollte sich das Feld unter der vorherigen Koordinate befinden.

Otis-spezifische Optionen für Ausweisinhaber

Einführung

Gemäß der Otis Standardfunktionalität werden acht Otis-spezifische binäre Optionen bereitgestellt. Wenn diese Optionen auf der Registerkarte **Elevators** (Aufzüge) als benutzerdefinierte Felder definiert sind, werden Sie als Kontrollkästchen auf der Registerkarte **Elevator data** (Aufzugsdaten) der Ausweisinhaber im Dialog **Persons** (Personen) angezeigt (Main menu > **Personnel data** > **Persons**; Hauptmenü > Personaldaten > Personen). Sie können dann von Bedienern des Zutrittskontrollsystems aktiviert und deaktiviert werden. Konfigurieren Sie diese Optionen nur entsprechend den Anweisungen Ihres Otis Vertreters.

Vorgehensweise

1. Klicken Sie auf **New field** (Neues Feld), um ein neues benutzerdefiniertes Feld zu erstellen.
2. Wählen Sie in der Liste **Field type** (Feldtyp) die Option **Otis options** (Otis-spezifische Optionen) aus.
3. Geben Sie im Feld **Label** (Beschriftung) eine eigene Beschriftung ein, z. B. *Otis flag 1* oder eine Beschriftung, die der Otis Dokumentation entspricht.
4. Wählen Sie in der Liste **Display in** (Angezeigt in) die Option *Tab:Elevators* aus.
5. Wählen Sie in der Liste **Function type** (Funktionstyp) eine der Optionen von *OTIS option 1* bis *OTIS option 8* aus.
6. Wählen Sie in der Gruppe **Position** einen eindeutigen Ort auf der Registerkarte **Elevators** (Aufzüge) aus, an dem dieses Kontrollkästchen angezeigt werden soll.
7. Klicken Sie auf  (Speichern), um die Änderungen zu speichern.

20.3 Erstellen und Konfigurieren von Berechtigungen für Otis Aufzüge

Einführung

In diesem Abschnitt wird beschrieben, wie Sie Zutrittsrechte für Otis Aufzugsgruppen, Etagen und Aufzugtüren in einer **Berechtigung** einbeziehen.

Berechtigungen werden den Ausweisinhabern direkt zugewiesen oder in den meisten Fällen mit anderen Berechtigungen in **Zutrittsprofilen** kombiniert, die dann den Ausweisinhabern zugewiesen werden.

Voraussetzungen

Ein Otis Compass-System wurde auf einem MAC im Geräteeditor definiert. Es umfasst eine Aufzugsgruppe (vertreten durch sein DES), Etagen und Türpaare (vertreten durch ihre DETs).

Dialogpfad

Main menu > **System data** > **Authorizations** (Hauptmenü > Systemdaten > Berechtigungen)

Vorgehensweise

1. Geben Sie im Feld **Authorization name** (Berechtigungsname) den Namen einer vorhandenen Berechtigung ein oder klicken Sie auf  (Neu), um eine neue Berechtigung zu erstellen.
2. Wählen Sie in der Liste **MAC** den Namen des MAC aus, auf dem das Otis Compass-System erstellt wurde.
3. Klicken Sie auf die Registerkarte **Otis elevator** (Otis Aufzug).
4. Wählen Sie in der Liste **Otis elevators** (Otis Aufzüge) den DES/DER für die Aufzugsgruppe aus, die Sie zur Berechtigung hinzufügen möchten (beachten Sie, dass eine Berechtigung nur einen DES/DER enthalten kann).
   – Die Etagen der ausgewählten Aufzugsgruppe werden im Bereich **Floors** (Etagen) angezeigt.
5. Wählen Sie in den Spalten **Front door** (Vordere Tür) und **Rear door** (Hintere Tür) im Bereich **Floors** (Etagen) die Türen auf den Etagen aus, die in diese Berechtigung aufgenommen werden sollen.
   – Beachten Sie, dass die Etagen und Türen, die bei der Definition im Geräteeditor **nicht** für diese Aufzugsgruppe ausgewählt wurden, ausgegraut sind und in diesem Dialog nicht ausgewählt werden können.
6. Sie können stattdessen auch auf die Schaltflächen **Assign all floors** (Alle Etagen zuweisen) und **Remove all floors** (Alle Etagen entfernen) klicken, um alle Etagen und Türen gleichzeitig zuzuweisen oder zu entfernen.
7. Klicken Sie auf  (**Speichern**), um die Berechtigung zu speichern.

21 Konfigurieren der IDEMIA Universal BioBridge

In diesem Abschnitt wird die Konfiguration der biometrischen IDEMIA-Geräte für die Zusammenarbeit mit Bosch Zutrittskontrollsystemen über **MorphoManager** und **BioBridge** beschrieben.
Die Unterabschnitte behandeln die erforderlichen Konfigurationsaufgaben für die folgenden Bereiche:

- das Bosch Zutrittskontrollsystem
- MorphoManager
- der BioBridge-Registrierungsclient in MorphoManager
- Adaptionen für verschiedene Ausweistechnologien und -formate

21.1 Einrichten von BioBridge im Bosch Zutrittskontrollsystem

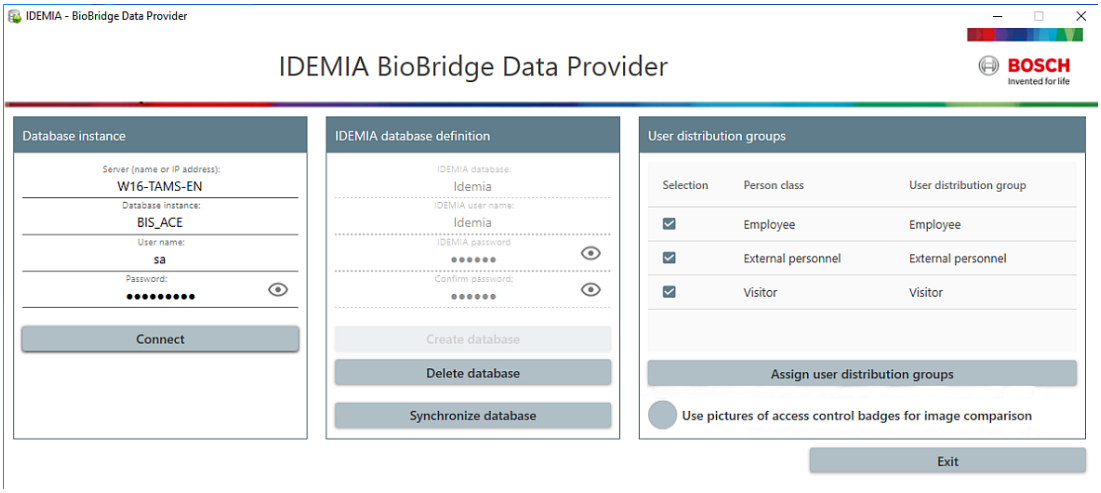
Die folgenden Schritte werden in AMS ausgeführt, um die Datenbank zu erstellen, die biometrische IDEMIA-Geräte mit dem Bosch Zutrittskontrollsystem verknüpft. Die Datenbank ordnet die folgenden Datenbankentitäten einander zu:

- **Personenklasse** (Bosch)
- **Benutzerverteilergruppe** (IDEMIA)

Dialogpfad

- AMS-Hauptmenü > **Configuration** > **Tools** > **Configuration IDEMIA database** (Konfiguration > Tools > Konfiguration IDEMIA-Datenbank)

1. Klicken Sie auf **Configuration IDEMIA database** (Konfiguration IDEMIA-Datenbank). Das Dialogfenster **IDEMIA BioBridge Data Provider** (IDEMIA BioBridge-Datenanbieter) wird angezeigt.



2. Geben Sie im Bereich **Database instance** (Datenbankinstanz) die folgenden Informationen ein:

- **Server**: Der Hostname oder die IP-Adresse des Computers, auf dem die ACS SQL Server-Datenbankinstanz ausgeführt wird. Dies kann der lokale Hostname sein, wenn der SQL Server lokal ausgeführt wird.
- **Database Instance** (Datenbankinstanz): die Instanz der AMS-Datenbank (Standard: *ACE*).
- **Username** (Benutzername): der Name des Administratorkontos der AMS-Datenbankinstanz (Standard: *sa*).
- **Password** (Passwort): das Passwort des Administratorkontos, das bei der Installation von AMS konfiguriert wurde.

Im Bereich „IDEMIA database definition“ (IDEMIA-Datenbankdefinition)
Die ersten beiden Felder sind schreibgeschützt:
– **Idemia database** (Idemia-Datenbank): der Name der Datenbank, die Daten von Bosch und IDEMIA verbindet.
– **Idemia username** (Idemia-Benutzername): der Name des Datenbankbenutzers, in dessen Namen die Software Befehle in der Datenbank ausführt.
1. Geben Sie ein sicheres Passwort für **Idemia username** (Idemia-Benutzername) ein und bestätigen Sie es.
2. Notieren Sie das Passwort sorgfältig. Er wird in folgenden Konfigurationsaufgaben benötigt und kann bei Verlust nicht wiederhergestellt werden.
3. Klicken Sie auf **Create database** (Datenbank erstellen).
   Ein Meldungsfeld gibt an, ob die Erstellung erfolgreich war. Klicken Sie auf **OK**.
4. Klicken Sie auf **Connect** (Verbinden), um die Datenbankverbindung zu testen.
5. Wenn die Tests erfolgreich abgeschlossen wurden, klicken Sie auf **Exit** (Beenden), um das Dialogfenster zu schließen.

Im Bereich „User distribution groups“ (Benutzerverteilergruppen)
Benutzerverteilergruppen sind MorphoManager-Objekte, die Benutzer (Ausweisinhaber) zu Gruppen von biometrischen Lesern oder MorphoManager-Clients zuordnen. Wir ordnen sie den **Personenklassen** von Bosch Zutrittskontrollsystemen zu.
1. Aktivieren Sie in der Spalte „Select“ (Auswählen) das Kontrollkästchen jeder AMS-**Personenklasse**, die von Ihrer Installation verwendet wird.
2. Kopieren Sie für jede ausgewählte Zeile den Namen dieser Personenklasse in die entsprechende Zelle in der Spalte **User distribution group** (Benutzerverteilergruppe).
3. Klicken Sie nach Abschluss der Zuordnung auf **Assign user distribution groups** (Benutzerverteilergruppen zuweisen).

Bereitstellen von Ausweisfotos für die VisionPass-Gesichtserkennung
So konfigurieren Sie, dass IDEMIA-Leser eine VisionPass-Gesichtserkennung mithilfe von Ausweisfotos der Ausweisinhaber aus der AMS-Datenbank durchführen können:
▸ Klicken Sie auf **Use pictures of access control badges for image comparison** (Bilder von Zutrittskontrollausweisen für Bildvergleich verwenden).
  Das Fenster **IDEMIA BioBridge Data Provider** (IDEMIA BioBridge-Datenanbieter) bestätigt, dass die Synchronisierung durchgeführt wird.
  Beachten Sie, dass die Datenübertragung je nach Anzahl der involvierten Bilddaten sehr lange dauern kann.

21.2 Einrichten von BioBridge in MorphoManager

Voraussetzungen
MorphoManager ist auf einem MorphoManager-Server in Ihrem Netzwerk installiert. Weitere Informationen finden Sie im Installationshandbuch und in der Online-Hilfe für MorphoManager.

Übersicht
Zur Verwendung der BioBridge-Schnittstelle zwischen Bosch Zutrittskontrollsystemen und MorphoManager müssen Sie Folgendes in MorphoManager konfigurieren:
– Wiegand-Profile
– Biometrische Geräteprofile

- Biometrisches Gerät
- Benutzerrichtlinie
- Benutzerverteilergruppe
- BioBridge-Systemkonfiguration

Darüber hinaus muss die Open Database Connectivity (ODBC) für die Kommunikation zwischen MorphoManager BioBridge und der Datenbank eingerichtet werden, die gemeinsam mit AMS verwendet wird.
Alle diese Konfigurationsaufgaben werden in den folgenden Abschnitten beschrieben.

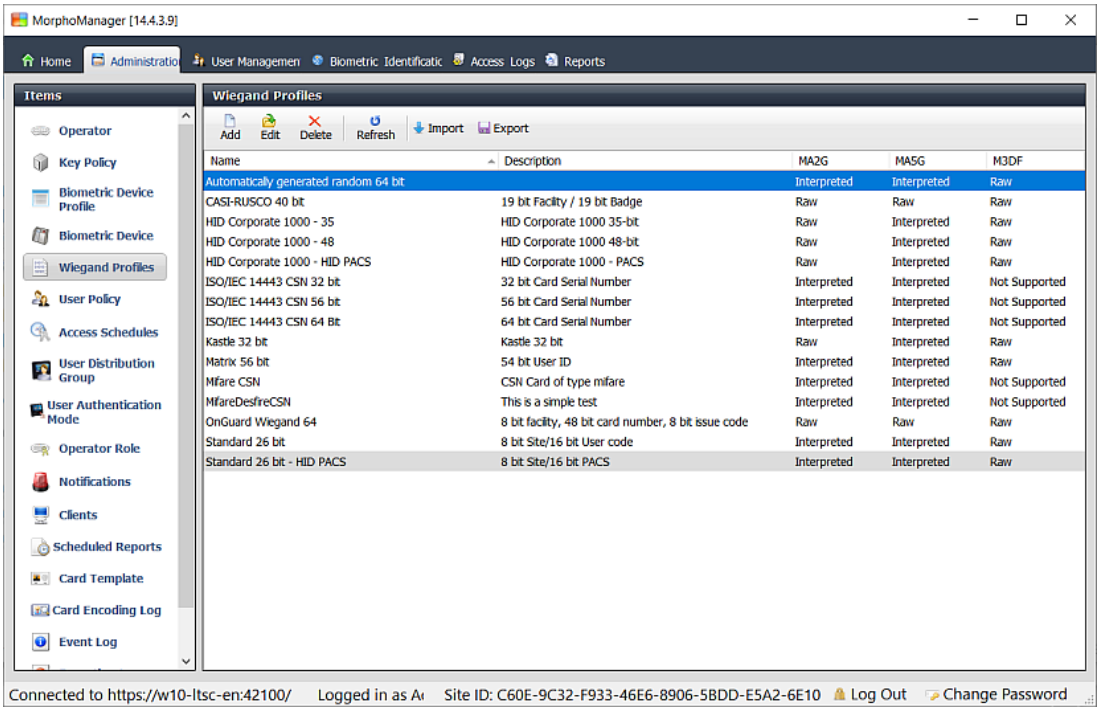
21.2.1 Wiegand-Profile

Hinweis!
Unabhängig vom Namen können Wiegand-Profile für alle Lesertypen (einschließlich OSDP-Lesern) eingesetzt werden.

Wiegand-Profile definieren, welche Informationen die biometrischen Geräte über Ihre Wiegand-Schnittstelle ausgeben, wenn ein Benutzer identifiziert wird. Diese Informationen werden an das Bosch Zutrittskontrollsystem übermittelt, das sie verwendet, um eine Zutrittsentscheidung zu treffen.

Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **Wiegand Profile** (Verwaltung > Wiegand-Profil).
2. Wählen Sie eines der vordefinierten Wiegand-Profile aus oder klicken Sie auf **Add** (Hinzufügen), um ein benutzerdefiniertes Profil zu erstellen.
   Im Allgemeinen sind alle CSN-Profile für die Verwendung mit Bosch Zutrittskontrollsystemen geeignet, darunter auch die standardmäßigen 26-Bit-Profile.
   Wenn Ihr Installationsprogramm ein Profil für Ihr System bereitgestellt hat, klicken Sie auf **Import** (Importieren), um die bereitgestellte Datei zu suchen und zu importieren, und wählen Sie sie anschließend in der Liste aus.



3. Geben Sie im Dialogfenster die Informationen ein, die Ihr Zutrittskontrollsystem von den biometrischen Geräten benötigt.
4. Notieren Sie sich den Namen des hier ausgewählten oder erstellten Wiegand-Profils sorgfältig. Sie müssen später in den MorphoManager-Konfigurationen von **User Policy** (Benutzerrichtlinie) und **Biometric Device Profile** (Biometrisches Geräteprofil) darauf verweisen.

21.2.2 Biometrisches Geräteprofil

Das biometrische Geräteprofil definiert allgemeine Einstellungen und Parameter für ein oder mehrere biometrische Geräte. Wenn Sie später im Abschnitt **Biometric Device** (Biometrisches Gerät) von **Administration** (Verwaltung) biometrische Geräte zum System hinzufügen, wenden Sie ein biometrisches Geräteprofil auf sie an.
Bei der folgenden Vorgehensweise wird vorausgesetzt, dass Sie biometrische Leser von IDEMIA mit zusätzlicher Ausweislesetechnologie bereitstellen.

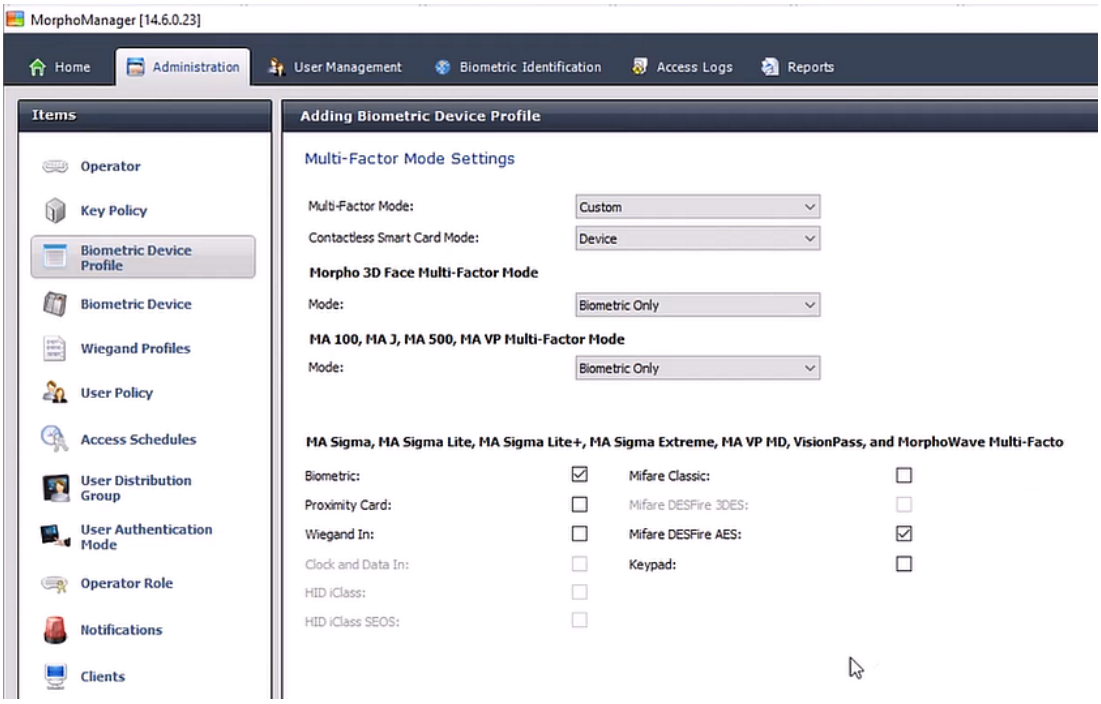
Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil).
2. Klicken Sie auf **Add** (Hinzufügen), um ein neues biometrisches Geräteprofil zu erstellen.
3. Geben Sie auf dem nächsten Bildschirm einen Namen für das Profil und (optional) eine Beschreibung ein. Wenn Sie das Beschreibungsfeld nicht verwenden, empfehlen wir einen Namen, der auf Typ und Identifikationsmodi (biometrisch und/oder Ausweis) der Lesergruppe hinweist.
4. Klicken Sie auf **Next** (Weiter), bis Sie bei **Biometric Device Settings** (Biometrische Geräteeinstellungen) angelangt sind.

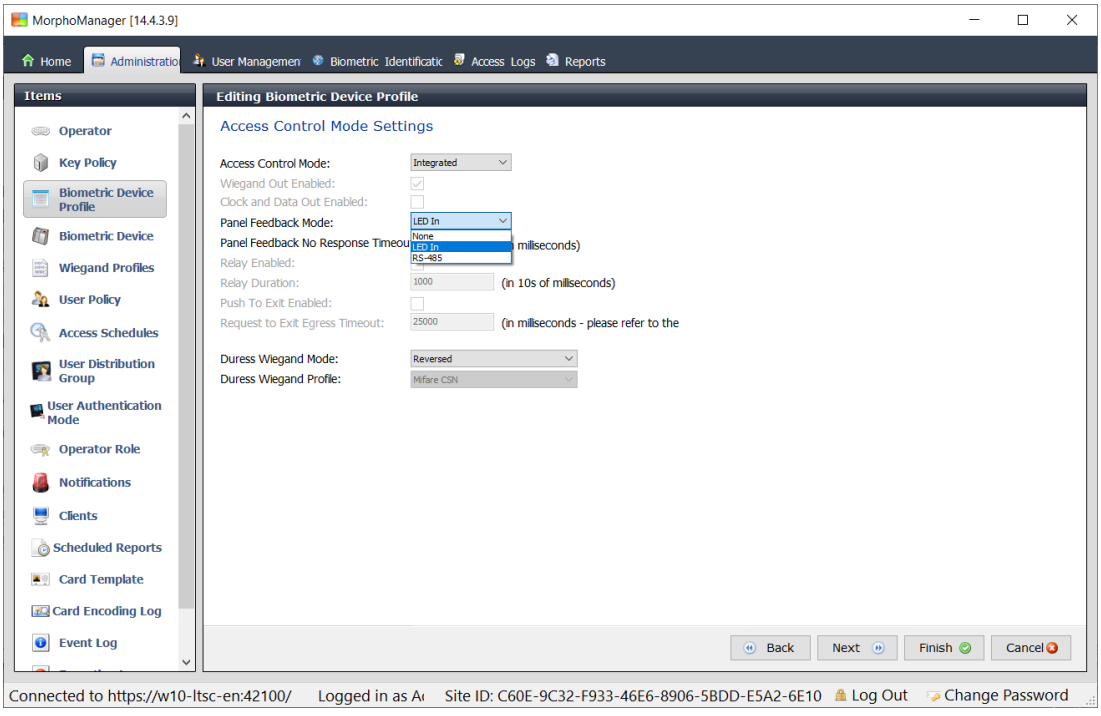
– Wählen Sie das Wiegand-Profil aus, das Sie zuvor für die Installation erstellt haben.

5. Klicken Sie auf **Next** (Weiter), bis Sie bei **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) angelangt sind.

– Für **Multi-Factor Mode** (Mehrfach-Modus), d. h. eine Kombination von biometrischen und Zutrittsausweislesefunktionen: Wählen Sie *Custom* aus der Liste aus.
– Für **Contactless Smart Card Mode** (Berührungsloser Smartcard-Modus): Wählen Sie *Device* aus der Liste aus.



6. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Access Control Mode Settings** (Einstellungen für Zutrittskontrollmodus) angelangt sind.



Ab diesem Punkt unterscheiden sich die Vorgehensweisen für Wiegand und OSDP AMCs. Folgen Sie dem Verfahren, das Ihrem AMC-Controllertyp entspricht:

Für Wiegand AMCs

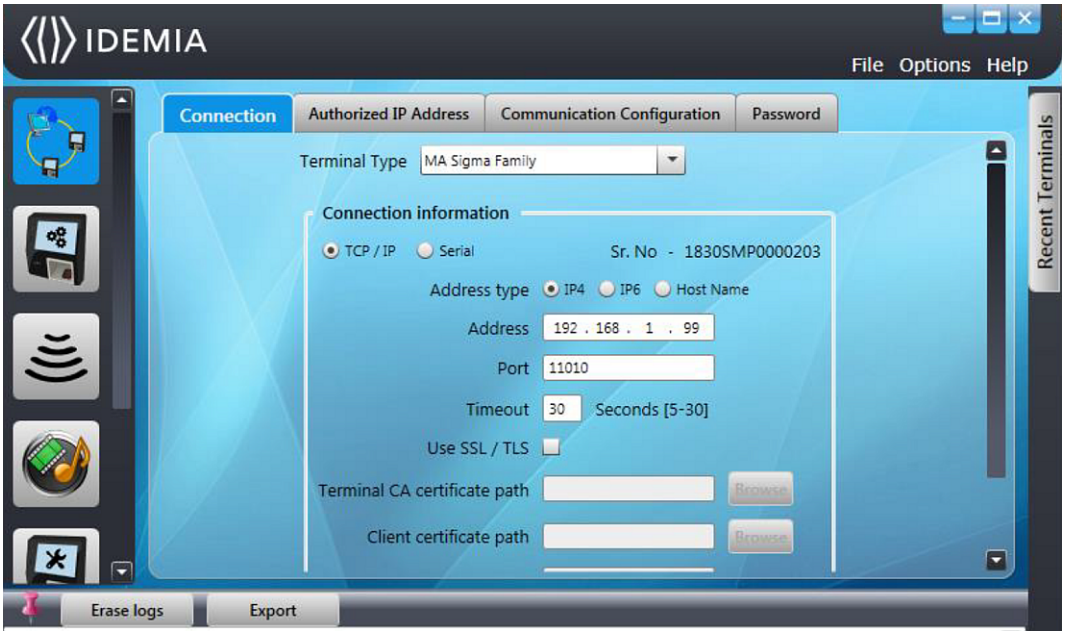
1. Legen Sie **Access Control Mode** (Zutrittskontrollmodus) auf *Integrated* fest.
2. Legen Sie **Panel feedback Mode** (Rückmeldungsmodus der Zentrale) auf *LED In* fest.
3. Klicken Sie auf **Finish** (Fertigstellen).

Für OSDP AMCs

1. Legen Sie **Access Control Mode** (Zutrittskontrollmodus) auf *Integrated* fest.
2. Legen Sie **Panel feedback Mode** (Rückmeldungsmodus der Zentrale) auf *LED In* fest.
3. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
4. Klicken Sie auf **Add** (Hinzufügen), fügen Sie vier benutzerdefinierte Parameter hinzu und legen Sie ihre Werte wie folgt fest:

– *Comm_channels_state.serial =1* (Kommunikationskanäle aktivieren)
– *OSDP.channel=1* (OSDP aktivieren)
– *OSDP.device_serial_address = <value>* (*<value>* auf die Bus-Adresse des Lesers festlegen)
– *OSDP.secure_connection=1* (Sicheren Kanal aktivieren)

5. Klicken Sie auf **Finish** (Fertigstellen).
6. Starten Sie das separate Programm **MorphoBioToolBox (MBTB)**.
7. Legen Sie auf der Registerkarte **Connection** (Verbindung) die IP-Adresse des biometrischen Lesers fest.



1. Navigieren Sie im MorphoBioToolBox-Programm zu **Network & Secure Communication** > Registerkarte: **Communication Configuration** (Netzwerk und sichere Kommunikation > Registerkarte: Kommunikationskonfiguration).

1. Nehmen Sie die folgenden Einstellungen im Bereich **Serial Settings** (Serielle Einstellungen) vor:

– **Type** (Typ): *Half Duplex*
– **Baud rate** (Baudrate): *9600*

– **Data Bits** (Datenbits): *8*
– **Stop Bits** (Stoppbits): *1*
– **Parity Bit** (Paritätsbit): *No parity*
– **Terminal identifier** (Terminal-Bezeichner): *0*
2. Wenn Sie einen der Werte ändern, klicken Sie auf **Write** (Schreiben), um die Änderungen an das Gerät zu senden.

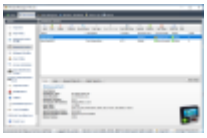
21.2.3 Biometrische Geräte

Die biometrischen Geräte testen, ob die von ihnen eingelesenen biometrischen Nachweise mit den Datensätzen in der Datenbank übereinstimmen. Sie führen zudem Protokoll über alle Nutzungsereignisse.

Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **Biometric Device** (Verwaltung > Biometrisches Gerät).
2. Klicken Sie auf **Add** (Hinzufügen), um ein neues biometrisches Gerät zu erstellen.
3. Geben Sie mindestens die folgenden wesentlichen Details für das Gerät ein:
– (aus der Liste) **Hardware Family** (Hardwareserie)
– **Hostname\IP address** (Hostname\IP-Adresse)
– (aus der Liste) das zuvor definierte **Biometric Device Profile** (Biometrisches Geräteprofil)
4. Klicken Sie auf **Finish** (Fertigstellen).

Im Dialogfenster „Biometric Device“ (Biometrisches Gerät) werden jetzt Geräte aufgeführt, die bereits konfiguriert sind:



21.2.4 Benutzerrichtlinie

Benutzerrichtlinien sind Pakete mit Zutrittsrechten, die Sie Benutzern mit denselben Zutrittsanforderungen zuweisen. Die Zutrittsrechte legen fest, welche biometrischen Geräte die Benutzer in welchen Modi und zu welchen Zeiten verwenden dürfen.

Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **User Policy** (Verwaltung > Benutzerrichtlinie).
2. Klicken Sie auf **Add** (Hinzufügen), um eine neue Benutzerrichtlinie zu erstellen.

3. Geben Sie im Dialogfenster **Adding User Policy** (Benutzerrichtlinie hinzufügen) Folgendes ein:
– ein **Name** für die Benutzerrichtlinie und (optional) eine Beschreibung

- der **Access Mode** (Zutrittsmodus) *Per User*
- ein **Access Schedule** (Zutrittszeitplan) mit Tagen und Uhrzeiten, zu denen der Zutritt gewährt wird
- dasselbe **Wiegand Profile** (Wiegand-Profil), das Sie bei **Biometric Device Profile** (Biometrisches Geräteprofil) definiert und verwendet haben
- ein **User Authentication Mode** (Benutzerauthentifizierungsmodus), abhängig davon, wie die Gerätebenutzer die Geräte verwenden (Fingerabdruck, Finger, Gesicht, Ausweise usw.); weitere Informationen siehe Benutzerhandbuch für MorphoManager

4. Klicken Sie auf **Finish** (Fertigstellen).

Die standardmäßige Benutzerrichtlinie hat den Benutzerauthentifizierungsmodus *(1: Many)*. Zur Verwendung anderer Authentifizierungsmodi müssen Sie zusätzliche Benutzerrichtlinien erstellen. Weitere Informationen zu den verschiedenen Eigenschaften, die einer Benutzerrichtlinie zugewiesen werden können, finden Sie im Benutzerhandbuch für MorphoManager.

21.2.5 Benutzerverteilergruppen

Benutzerverteilergruppen ordnen Benutzer zu Gruppen von biometrischen Lesern oder MorphoManager-Clients zu.

Voraussetzungen:

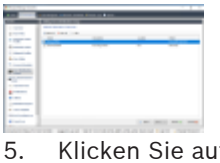
Benutzer in Benutzerverteilergruppen müssen eine Benutzerrichtlinie haben, bei der **Access Mode** (Zutrittsmodus) auf *Per User* festgelegt ist.

Jede Benutzerverteilergruppe muss mindestens einer Personenklasse in AMS zugeordnet sein. Erstellen Sie daher mindestens eine Benutzerverteilergruppe für jede verwendete Personenklasse.

Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **User Distribution Group** (Verwaltung > Benutzerverteilergruppe).
2. Klicken Sie auf **Add** (Hinzufügen), um eine neue Benutzerverteilergruppe zu erstellen.

3. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Select Biometric Devices** (Biometrische Geräte auswählen) angelangt sind.
4. Aktivieren Sie die Kontrollkästchen der biometrischen Geräte, die von den Personen in dieser Benutzerverteilergruppe verwendet werden sollen.



5. Klicken Sie auf **Finish** (Fertigstellen).

21.2.6 Einrichten von ODBC für BioBridge

Einführung

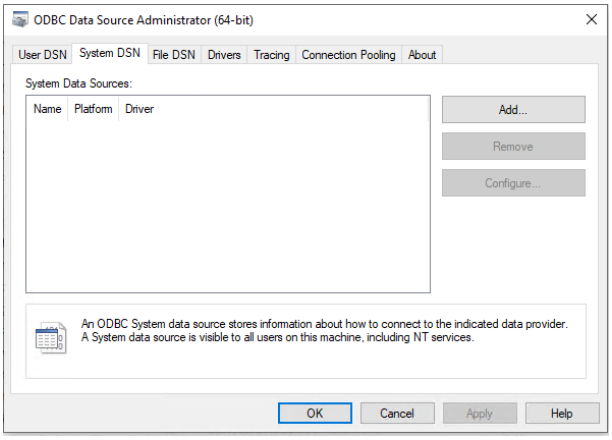
Open Database Connectivity (ODBC) ist eine Voraussetzung für die Verwendung von MorphoManager BioBridge. ODBC ist eine standardisierte Programmierschnittstelle für den Zugriff auf verschiedene Datenbanken. Der empfohlene Treiber ist *OdbCDriver17SQLServer*. Sie finden ihn auf dem BIS-Installationsmedium unter

BIS\3rd_Party\OdbCDriver17SQLServer

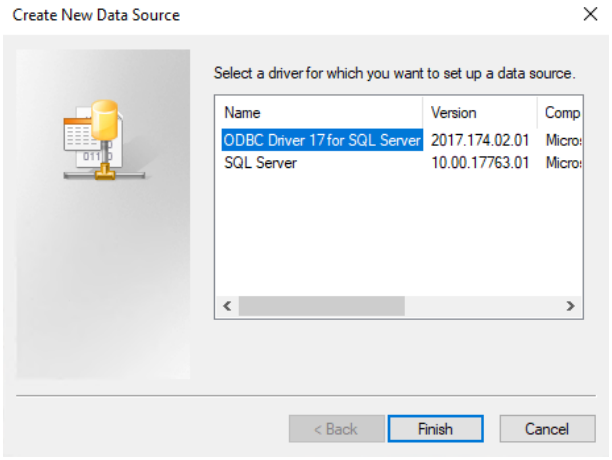
Erstellen einer Datenquelle

Erstellen Sie einen Datenquellennamen (DSN) für ODBC.

1. Wählen Sie **Administrative Tools** (Verwaltungstools) in der Windows-Systemsteuerung aus.
2. Wählen Sie *ODBC Data Sources (64-bit)* in der Liste aus.
3. Wählen Sie die Registerkarte **System DSN** (System-DSN) aus.

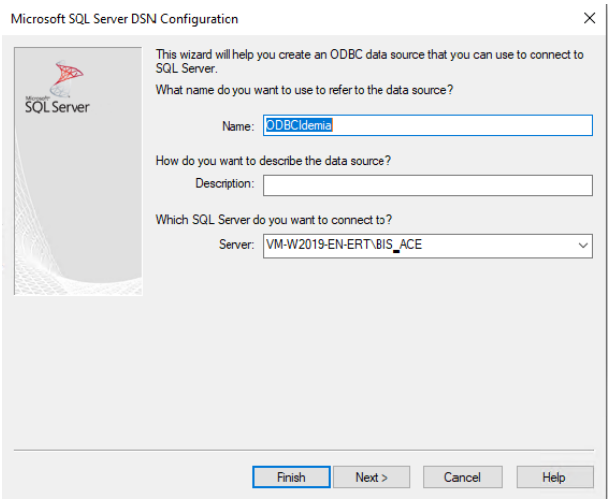


4. Klicken Sie auf **Add** (Hinzufügen), um einen Treiber auszuwählen.
5. Wählen Sie *ODBC Driver 17 for SQL Server* als Treiber aus und klicken Sie auf **Finish** (Fertig stellen).

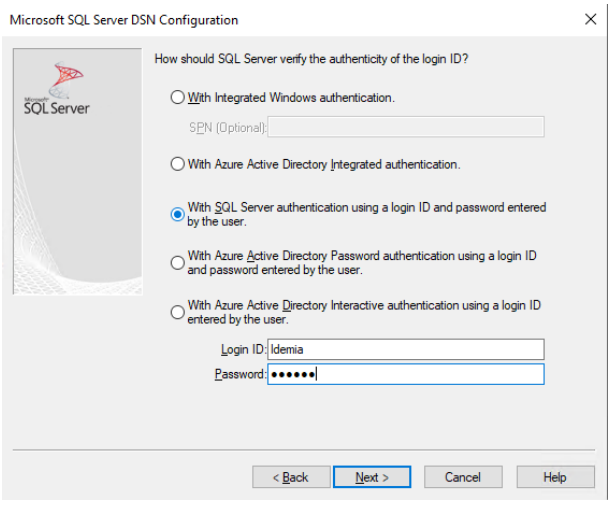


6. Geben Sie die folgenden Details für die Datenquelle ein.

– **Name**: ein Name für die Datenquelle
– **Description**: Beschreibung (optional)
– **Server**: der Name des Computers, auf dem die AMS-Datenbank installiert ist, und der Name der Datenbank (Standard: <Mein ACS -Server>*ACE*)



7. Klicken Sie auf **Next >** (Weiter >).
   Ein Dialogfenster zum Erfassen von Anmeldeinformationen wird angezeigt.



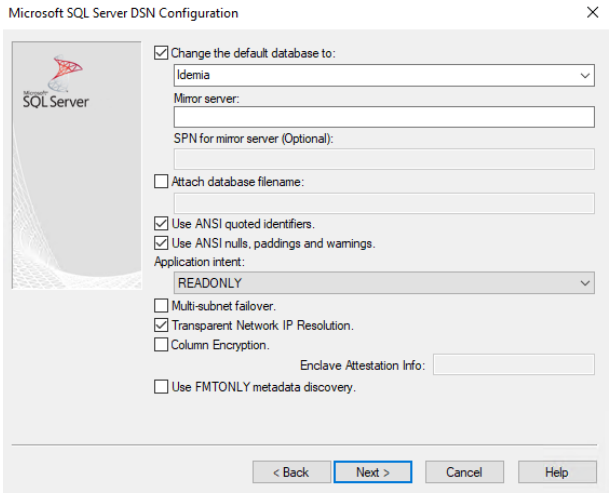
8. Wählen Sie **With SQL Server authentication using a login ID ...** (Mit SQL Server-Authentifizierung anhand des vom Benutzer ...) aus.
9. Geben Sie die folgenden Informationen ein:

– **Login ID** (Benutzername): der Benutzername des Idemia-Datenbankbenutzers, wie in AMS konfiguriert. Dies ist immer `Idemia`.
– **Password** (Kennwort): das für den Idemia-Datenbankbenutzer festgelegte Passwort, wenn es in AMS konfiguriert wurde.

10. Klicken Sie auf **Next >** (Weiter >).
11. Aktivieren Sie im nächsten Dialogfenster die folgenden Kontrollkästchen:

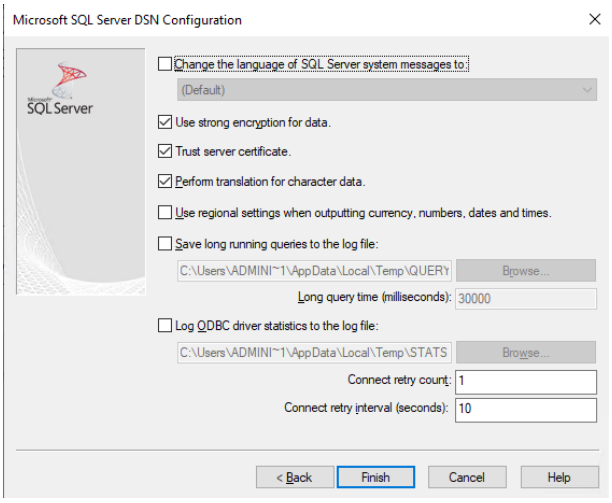
– **Change the default database to** (Die Standarddatenbank ändern auf) und `Idemia` auswählen
– **Use ANSI quoted identifiers** (ANSI-Anführungszeichen verwenden)
– **Use ANSI nulls, paddings and warnings** (ANSI-Nullen, -Leerstellen und Warnungen verwenden)
– **Transparent Network IP Resolution** (Transparente Netzwerk-IP-Auflösung)

12. **Application intent** (Anwendungsabsicht) auf `READONLY` festlegen

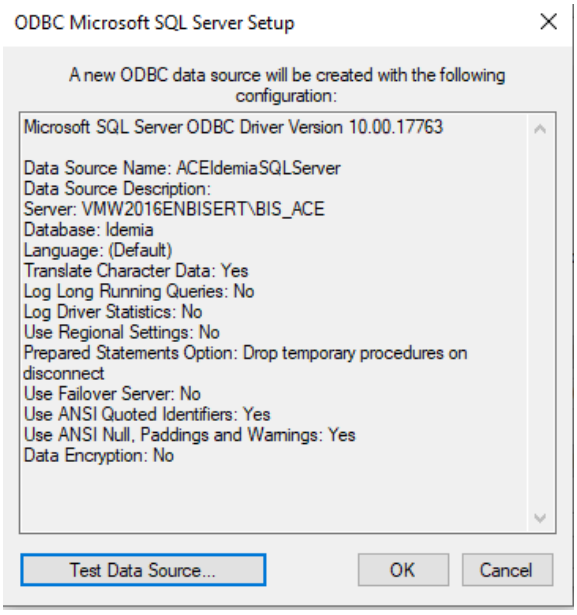


13. Klicken Sie auf **Next >** (Weiter >).
14. Aktivieren Sie im nächsten Dialogfenster die folgenden Kontrollkästchen:

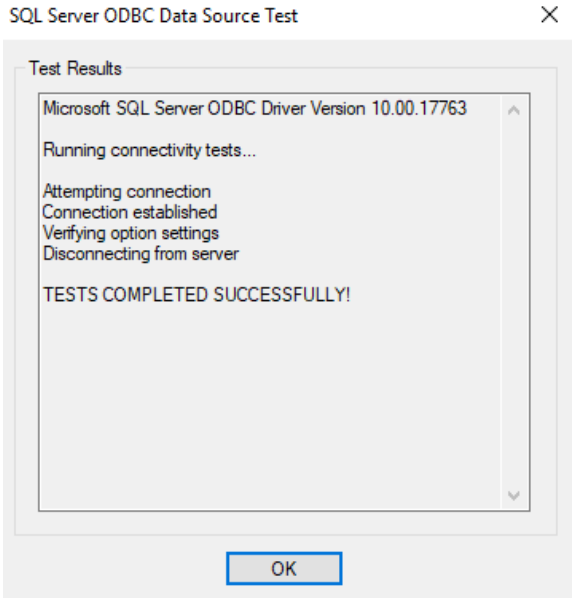
– **Use strong encryption for data** (Starke Verschlüsselung für Daten verwenden)
– **Perform translation for character data** (Konvertierung für Zeichendaten ausführen)
– **Trust server certificate** (Serverzertifikat vertrauen)



15. Klicken Sie auf **Finish** (Fertigstellen).
16. Überprüfen Sie im nächsten Dialogfenster die Zusammenfassungsdaten.



17. Klicken Sie auf **Test Data Source...** (Datenquelle testen...) und stellen Sie sicher, dass die Tests erfolgreich abgeschlossen wurden.



18. Speichern Sie alle Änderungen und schließen Sie den ODBC-Setup-Assistenten.

21.2.7 BioBridge-Systemkonfiguration

In diesem Abschnitt werden die restlichen Einstellungen beschrieben, die erforderlich sind, damit Zutrittskontrollsysteme die BioBridge-Schnittstelle nutzen können.

Voraussetzung

ODBC ist für BioBridge eingerichtet. Siehe *Einrichten von ODBC für BioBridge, Seite 166*

Vorgehensweise:

1. Navigieren Sie im MorphoManager zu **Administration** > **System Configuration** (Verwaltung > Systemkonfiguration).
2. Wählen Sie die Registerkarte **BioBridge**.

3. Wählen Sie in der Dropdown-Liste **System** die Option *MorphoManager Universal BioBridge* aus.
4. Klicken Sie auf **Configure** (Konfigurieren).
   Es wird ein Popup-Dialogfenster angezeigt.

Im Popup-Fenster:

1. Wählen Sie in der Dropdown-Liste **Provider** (Anbieter) die Option *ODBC* aus.
2. Geben Sie den DSN (Datenquellenname) aus dem ODBC-Setup ein.
3. Geben Sie unter **Logon details** (Anmeldedetails) den Benutzernamen (*Idemia*) und das Passwort ein, die im ODBC-Setup definiert wurden.
4. Klicken Sie auf **OK**, um zum Dialogfenster **System Configuration** (Systemkonfiguration) zurückzukehren.

Im Dialogfenster **System Configuration** (Systemkonfiguration):

1. Für **Wiegand Profile** (Wiegand-Profil): Wählen Sie das Wiegand-Profil aus der Liste aus, das Sie zuvor definiert haben.

Gruppierungsmodus

Diese Einstellung legt fest, wie MorphoManager die MM Universal BioBridge-Benutzer den MorphoManager-Benutzerverteilergruppen zuordnen soll. Wählen Sie eine der folgenden Optionen:

- **Automatic** (Automatisch): in diesem Modus werden **Zutrittsberechtigungsgruppen** von MM Universal BioBridge automatisch MorphoManager **Benutzerverteilergruppen** zugeordnet, sofern Sie derselben Benennungsregel folgen.
- **Manual** (Manuell): Wenn die **Zutrittsberechtigungsgruppen** von MM Universal BioBridge und die **Benutzerverteilergruppen** von MorphoManager nicht identisch sind, können Sie die Zuordnung manuell in **Benutzerrichtlinienzuordnungen** ausführen.

Weitere Einstellungen

In den meisten Fällen ist es nicht nötig, die Standardwerte der folgenden Einstellungen zu ändern:

Enable Forced User Policy (Erzwungene Benutzerrichtlinie aktivieren)	Bei Auswahl dieser Option erhalten alle Benutzer, die im BioBridge-Registrierungsclient registriert sind, die Benutzerrichtlinie, die aus der benachbarten Liste ausgewählt wird. Wenn Sie dieses Kontrollkästchen aktivieren, sollten Sie immer die Benutzerrichtlinie *Per User* verwenden.
User Synchronization Start Time and End Time (Start- und Endzeit der Benutzersynchronisierung)	Die Benutzersynchronisierungs-Engine darf nur im festgelegten Zeitraum ausgeführt werden.
Delay between Each User Synchronization (Verzögerung zwischen einzelnen Benutzersynchronisierungen)	Das Zeitintervall zwischen Benutzersynchronisierungsvorgängen. Durch Erhöhen der Verzögerung werden Systemressourcen geschont, aber die Aktualisierung aller Benutzer dauert länger.
Allow User Sync While User Cache Is Refreshing (Benutzersynchronisierung zulassen, während Benutzercache aktualisiert wird)	Wenn diese Option aktiviert ist, wird die Benutzersynchronisierungs-Engine parallel zur Benutzercache-Aktualisierung ausgeführt. Dadurch werden die Systemressourcen stark belastet. Es wird empfohlen, diese Einstellung bei Einsatz großer Datenbanken zu deaktivieren.
User Cache Refresh Schedule (Aktualisierungszeitplan für Benutzercache)	Die Tage und Uhrzeiten, zu denen der Benutzercache aktualisiert werden kann. Für maximale Genauigkeit sollte dies jederzeit sein, aber bei Systemen mit großen Datenbanken ist ein Kompromiss erforderlich, damit es nicht zu Leistungseinbußen kommt.

Zuordnungen von Benutzerverteilergruppen

– Stellen Sie in der Zuordnungstabelle sicher, dass alle **Gruppen** (**Personalklassen**, definiert in ACS) den **Benutzerverteilergruppen** (definiert in MorphoManager) zugeordnet sind.

21.3 Konfigurieren des BioBridge-Registrierungsclients

Einführung

Ein BioBridge-Registrierungsclient ist ein Computer, auf dem Sie biometrische Datensätze für Benutzer des Zutrittskontrollsystems erstellen können. Die Einrichtung eines BioBridge-Registrierungsclients besteht aus drei Teilen:

– Hinzufügen eines Registrierungsbedieners zu MorphoManager
– Konfigurieren des MorphoManager-Clientcomputers für Registrierungsaufgaben
– Testen des Registrierungsclients

Voraussetzungen

MorphoManager BioBridge ist an jedem AMS-Bedienplatz installiert, von dem aus Sie biometrische Registrierungen für IDEMIA-Systeme durchführen.

21.3.1 Hinzufügen eines Registrierungsbedieners zu MorphoManager

Vorgehensweise

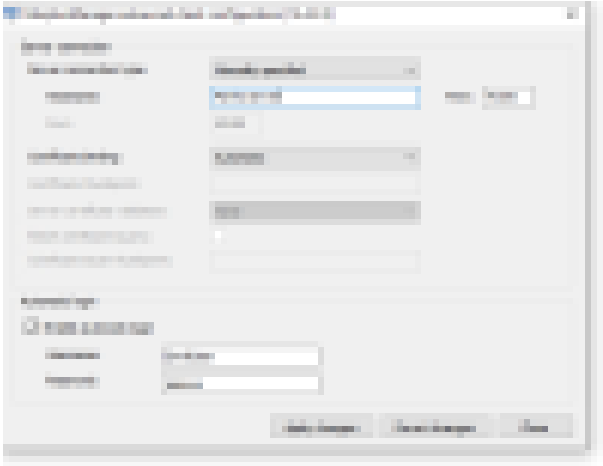
Befolgen Sie die Anweisungen im Installationshandbuch für den MorphoManager-Client.
Hinweis: Aus Sicherheitsgründen werden Active Directory-Benutzerkonten empfohlen.

21.3.2 Konfigurieren des MorphoManager-Clientcomputers für Registrierungsaufgaben

Führen Sie diesen Vorgang auf jedem Computer aus, den Sie für die biometrische Registrierung verwenden möchten.

Vorgehensweise

1. Im MorphoManager-Installationsverzeichnis (Standard: *C:\Program,Files(x86)\Morpho\MorphoManager\Client*)
   Führen Sie die Datei *ID1.ECP4.MorphoManager.AdvancedClientConfig.exe* als Administrator aus.

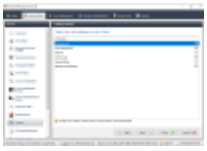


2. Geben Sie den Hostnamen des Morpho-Servers unter **Hostname** ein.
3. Unter **Automatic login** (Automatische Anmeldung):

– Aktivieren Sie das Kontrollkästchen **Enable Automatic login** (Automatische Anmeldung aktivieren).
– Geben Sie Benutzernamen und Passwort ein, die Sie im vorherigen Abschnitt für den Registrierungsbediener eingegeben haben.

1. Im MorphoManager-Installationsverzeichnis (Standard: *C:\Program Files(x86)\Morpho\MorphoManager\Client*)
   Führen Sie die Datei *Start ID1.ECP4.MorphoManager.Client.exe* als Administrator aus.
2. Navigieren Sie zu **Administration** > **Clients** (Verwaltung > Clients).
3. Wählen Sie einen Clientrechner aus.
4. Klicken Sie auf **Edit** (Bearbeiten).

5. Geben Sie den Namen des gewünschten Registrierungsclients und optional den Standort und eine Beschreibung ein.
6. Klicken Sie auf **Next** (Weiter).



7. Aktivieren Sie die Kontrollkästchen der Registerkarten, die auf dem Registrierungsclient angezeigt werden sollen:
   - **Administration** (Verwaltung)
   - **User Management** (Benutzerverwaltung)
   - **Reports** (Berichte)
   - **Access Logs** (Zutrittsprotokolle)
   - **Biometric Identification** (Biometrische Identifikation)
8. Klicken Sie auf **Next** (Weiter).

9. Für **Camera** (Kamera): Wählen Sie *No camera* aus der Liste aus.
10. Klicken Sie auf **Next** (Weiter).

11. Für **Key Policy** (Schlüsselrichtlinie): Wählen Sie *Default* aus der Liste aus.
12. Klicken Sie auf **Next** (Weiter).

13. Wählen Sie den biometrischen Bekanntmachungsleser aus, den Sie am Registrierungsbedienplatz verwenden möchten.
14. Klicken Sie auf **Finish** (Fertigstellen).
15. Schließen Sie die MorphoManager-Anwendung.

Siehe

- *Konfigurieren des BioBridge-Registrierungsclients, Seite 172*

21.3.3 Testen des Registrierungsclients

1. Im MorphoManager-Installationsverzeichnis (Standard: *C:\Program,Files(x86)\Morpho\MorphoManager\Client*)
   Führen Sie die Datei *ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe* aus.

1. Stellen Sie sicher, dass Sie den Registrierungsbildschirm aufrufen können, ohne Benutzernamen und Passwort des Registrierungsbedieners eingeben zu müssen.

21.4 Unterstützung verschiedener Ausweistechnologien und -formate

Damit der MAC Ihre Zutrittsausweise richtig interpretieren kann, müssen Sie sicherstellen, dass das in MorphoManager definierte Wiegand-Profil (oder die Wiegand-Profile) das Format (oder die Formate) dieser Zutrittsausweise enthält:

Allgemeine Vorgehensweise

1. Navigieren Sie im MorphoManager zu **Administration** > **Wiegand Profile** (Verwaltung > Wiegand-Profil).
2. Klicken Sie auf **Add** (Hinzufügen), um ein benutzerdefiniertes Wiegand-Profil zu erstellen.
3. Geben Sie in den entsprechenden Dialogfenstern die Formatierungsinformationen und die Ausweistechnologie ein, die Ihr System verwendet.
4. Um Ihr neu definiertes Wiegand-Profil im System zu verwenden, geben Sie seinen Namen im Feld **Wiegand Profile** (Wiegand-Profil) der folgenden MorphoManager-Dialogfenster ein:

– **Administration > Biometric Device profile** (Verwaltung > Biometrisches Geräteprofil)
– **Administration > User policy** (Verwaltung > Benutzerrichtlinie)

MIFARE classic CSN

1. Fügen Sie das Wiegand-Element *User CSN Element* hinzu und geben Sie die folgenden Details ein.

– **Name** (beispielsweise): *CSN*
– **Length** (Länge): *32*
– **Transformation mode** (Transformationsmodus): *Reversed*

2. Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen **MIFARE classic**.

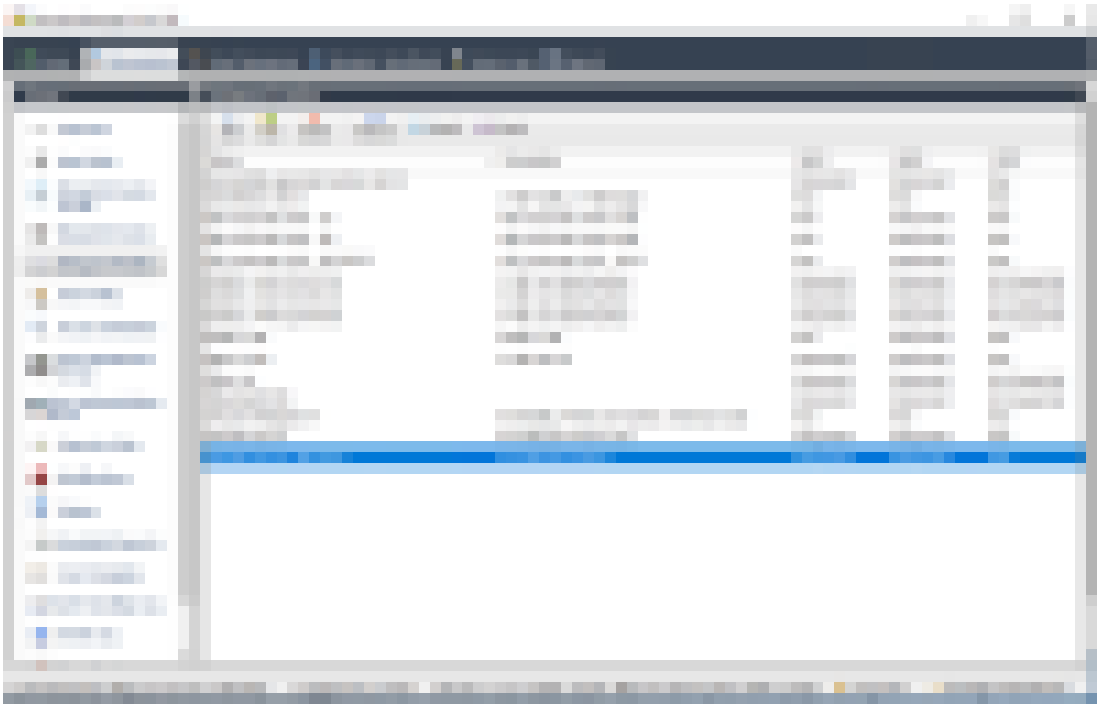
MIFARE DESFire CSN

Die Konfiguration ist bis auf die folgenden Details identisch mit MIFARE classic:

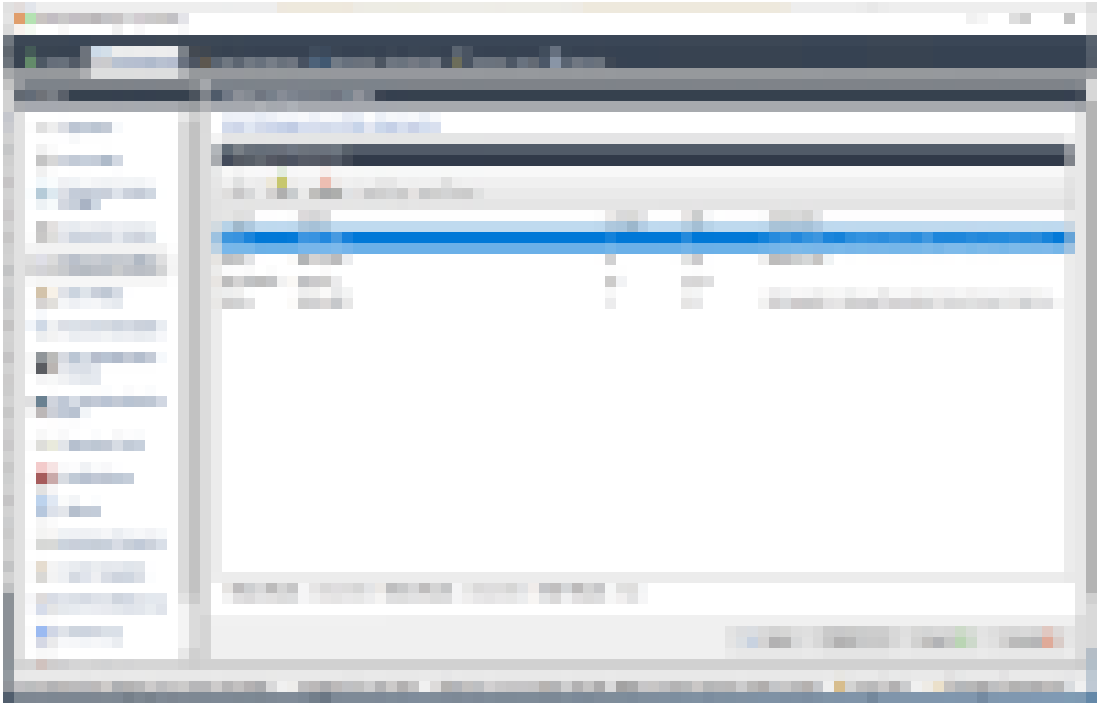
– **Length** (Länge): *56*
– Fügen Sie das Wiegand-Element **User CSN Element** hinzu.
  – Für **Name**: Geben Sie einen Namen ein.
  – Für **Length** (Länge): Geben Sie „56“ ein.
  – Für **Transformation mode** (Transformationsmodus): Geben Sie *Reversed* ein.
– Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen **MIFARE DESFire 3DES**.

iClass 26 BIT

1. Wählen Sie das vordefinierte Profil *Standard 26 bit-HID PACS* aus.



2. Klicken Sie auf **Edit** (Bearbeiten).
3. Klicken Sie auf **Next** (Weiter).



4. Klicken Sie auf **Edit** (Bearbeiten).
5. Löschen Sie die Zeile *Fixed Facility Code*.
6. Wählen Sie die Zeile *HID iClass SEP User ID* aus.
7. Klicken Sie auf **Edit** (Bearbeiten).
8. Ändern Sie die Länge der Benutzerkennung von *1..16* in *1..24*.

9. Wählen Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite „Biometric Device Settings“ (Biometrische Geräteeinstellungen) *Standard 26 BIT-HID-PACS* für das Wiegand-Profil.
10. Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen *HID iClass*.
11. Klicken Sie auf „Next“ (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
12. Klicken Sie auf **Add** (Hinzufügen).
13. Fügen Sie den benutzerdefinierten Parameter „Wiegand.site_code_propagation“ hinzu (Groß-/Kleinschreibung beachten).
14. Legen Sie seinen Wert auf *1* fest.
15. Klicken Sie auf **Finish** (Fertigstellen).
16. Geben Sie dieses ausgefüllte Wiegand-Profil unter **Administration > User policy** (Verwaltung > Benutzerrichtlinie) ein.

iClass 35 BIT

1. Wählen Sie das vordefinierte Profil *HID Corporate 1000 35 BIT* aus.
2. Klicken Sie auf **Edit** (Bearbeiten).
3. Klicken Sie auf **Next** (Weiter).
4. Wählen Sie die Elementzeile *Fixed Company ID* aus und löschen Sie sie.
5. Wählen Sie die Elementzeile *User Card ID Number* aus und löschen Sie sie.
6. Fügen Sie die Elementzeile *HID iClass/iClass SE PACS Data* hinzu und geben Sie in den Elementdetails Folgendes ein:

– Name: *Card ID Number*
– Length (Länge): *32*
– Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen *HID iClass*.
– Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
– Klicken Sie auf **Add** (Hinzufügen).
– Fügen Sie den benutzerdefinierten Parameter „Wiegand.site_code_propagation“ hinzu (Groß-/Kleinschreibung beachten).
– Legen Sie seinen Wert auf *1* fest.
– Klicken Sie auf **Finish** (Fertigstellen).
– Geben Sie dieses ausgefüllte Wiegand-Profil unter **Administration > User policy** (Verwaltung > Benutzerrichtlinie) ein.

iClass 37 BIT

– **Length** (Länge): *37*

1. Fügen Sie die Elementparität hinzu:

– **Name** (beispielsweise): *EvenParityBit 1*
– **Priority** (Priorität): *1*
– **Length** (Länge): *18*
– **Mode** (Modus): *Even*
– **Basis bits** (Basisbits): *1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18*

2. Fügen Sie das Element *User HID iClass/iClass* hinzu.

– **Name** (beispielsweise): *Parity Bits 2*

- **Priority** (Priorität): *2*
- **Length** (Länge): *19*
- **Mode** (Modus): *Odd*
- **Basis bits** (Basisbits): *19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37*
- Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen *HID iClass*.
- Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
- Klicken Sie auf **Add** (Hinzufügen).
- Fügen Sie den benutzerdefinierten Parameter „Wiegand.site_code_propagation“ hinzu (Groß-/Kleinschreibung beachten).
- Legen Sie seinen Wert auf *1* fest.
- Klicken Sie auf **Finish** (Fertigstellen).
- Geben Sie dieses ausgefüllte Wiegand-Profil unter **Administration > User policy** (Verwaltung > Benutzerrichtlinie) ein.

iClass 48 BIT

1. Wählen Sie das vordefinierte Profil *HID Corporate 1000 48 BIT* aus.
2. Klicken Sie auf **Edit** (Bearbeiten).
3. Klicken Sie auf **Next** (Weiter).
4. Wählen Sie die Elementzeile *Fixed Company ID* aus und löschen Sie sie.
5. Wählen Sie die Elementzeile *User Card ID Number* aus und löschen Sie sie.
6. Fügen Sie die Elementzeile *HID iClass/iClass SE PACS Data* hinzu und geben Sie in den Elementdetails Folgendes ein:

- Name: *User*
- Length (Länge): *45*

7. Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) das Kontrollkästchen *HID iClass*.
8. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
9. Klicken Sie auf **Add** (Hinzufügen).
10. Fügen Sie den benutzerdefinierten Parameter *Wiegand.site_code_propagation* hinzu (Groß-/Kleinschreibung beachten).

- Legen Sie seinen Wert auf *1* fest.

11. Klicken Sie auf **Finish** (Fertigstellen).
12. Geben Sie dieses ausgefüllte Wiegand-Profil unter **Administration** > **User policy** (Verwaltung > Benutzerrichtlinie) ein.

HID Prox

1. Wählen Sie das vordefinierte Profil *Standard 26 BIT* aus.
2. Klicken Sie auf **Edit** (Bearbeiten).
3. Klicken Sie auf **Next** (Weiter).
4. Löschen Sie die Zeile *Fixed Facility Code*.
5. Klicken Sie auf **Edit** (Bearbeiten).

6. Ändern Sie die Länge der Benutzerkennung von *1..16* in *1..24*.
7. Wählen Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite „Biometric Device Settings“ (Biometrische Geräteeinstellungen) *Standard 26 BIT* für das Wiegand-Profil.
8. Aktivieren Sie unter **Administration > Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil) auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) die folgenden Kontrollkästchen:

– **Biometry** (Biometrie)
– **Proximity card** (Berührungsloser Ausweis)

9. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.
10. Klicken Sie auf **Add** (Hinzufügen).
11. Fügen Sie den benutzerdefinierten Parameter *Wiegand.site_code_propagation* hinzu (Groß-/Kleinschreibung beachten).

– Legen Sie seinen Wert auf *1* fest.

12. Klicken Sie auf **Finish** (Fertigstellen).
13. Geben Sie dieses ausgefüllte Wiegand-Profil unter **Administration** > **User policy** (Verwaltung > Benutzerrichtlinie) ein.

21.5 Identifikationsmodi bei biometrischen Geräten

Einführung

Biometrische Leser können Ausweisinhaber auf verschiedene Arten identifizieren, die als Identifikationsmodi bezeichnet werden.

– Mit **Ausweis ODER Biometrie**, abhängig davon, was der Ausweisinhaber am Leser präsentiert
– Mit **Ausweis UND Biometrie**, d. h. der Benutzer muss anhand biometrischer Nachweise bestätigen, dass er wirklich Ausweisinhaber ist
– **Nur** mit **Biometrie**

In diesem Abschnitt wird die Konfiguration dieser Modi in MorphoManager beschrieben.

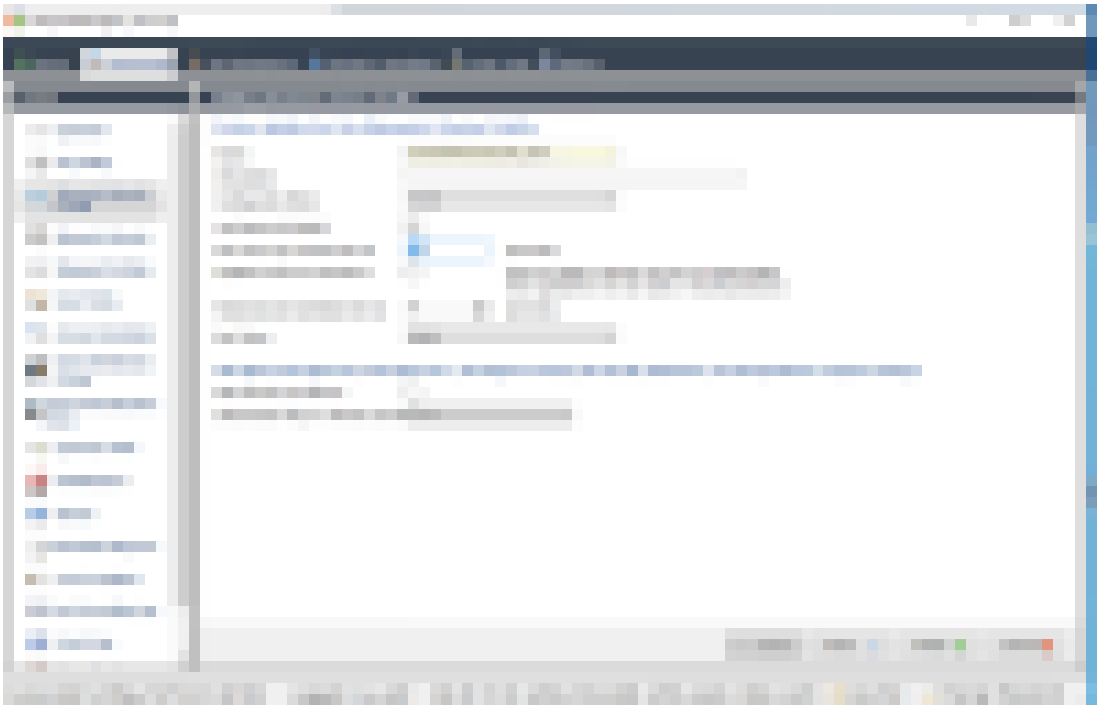
Dialogpfad

In MorphoManager auf der Registerkarte **Administration** (Verwaltung)

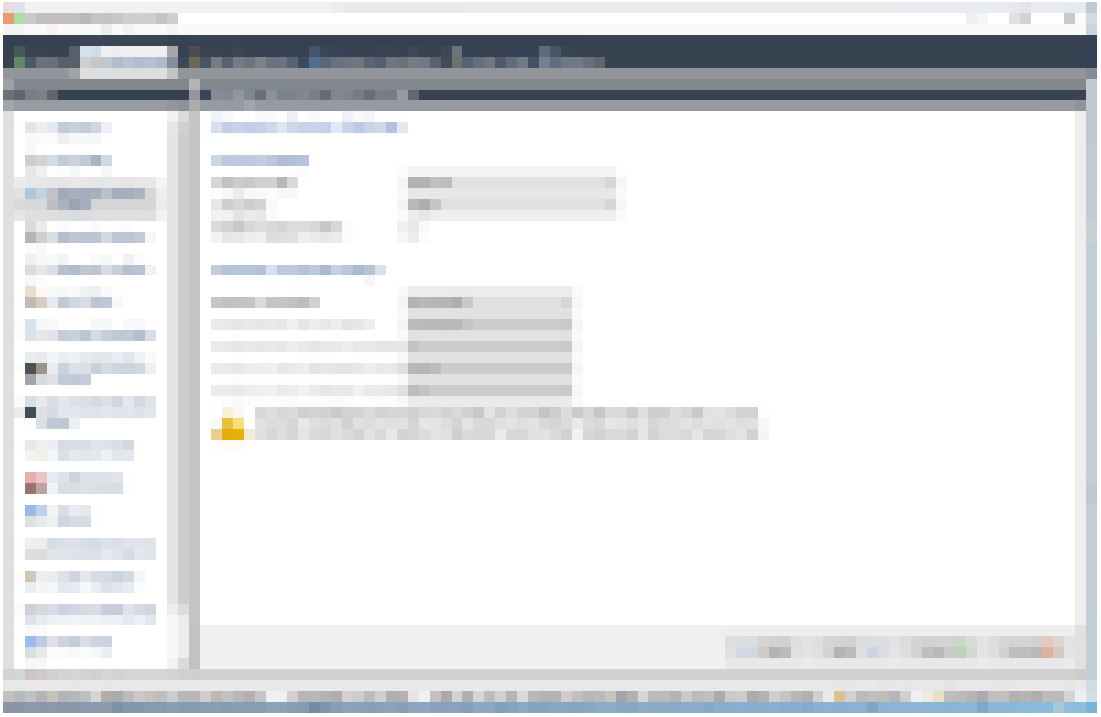
21.5.1 Ausweis ODER Biometrie

Nehmen Sie die folgenden Einstellungen vor, wenn Benutzer sich ENTWEDER mit Ausweis ODER biometrischen Nachweisen identifizieren sollen.

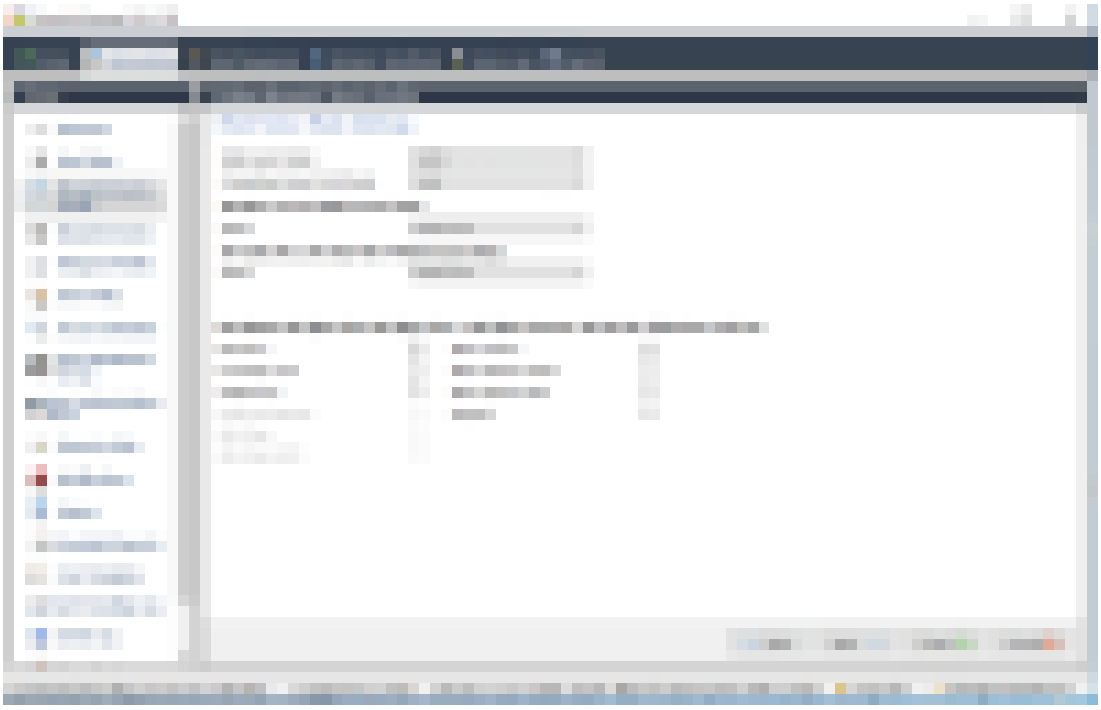
1. Navigieren Sie im MorphoManager zu **Administration** > **Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil).



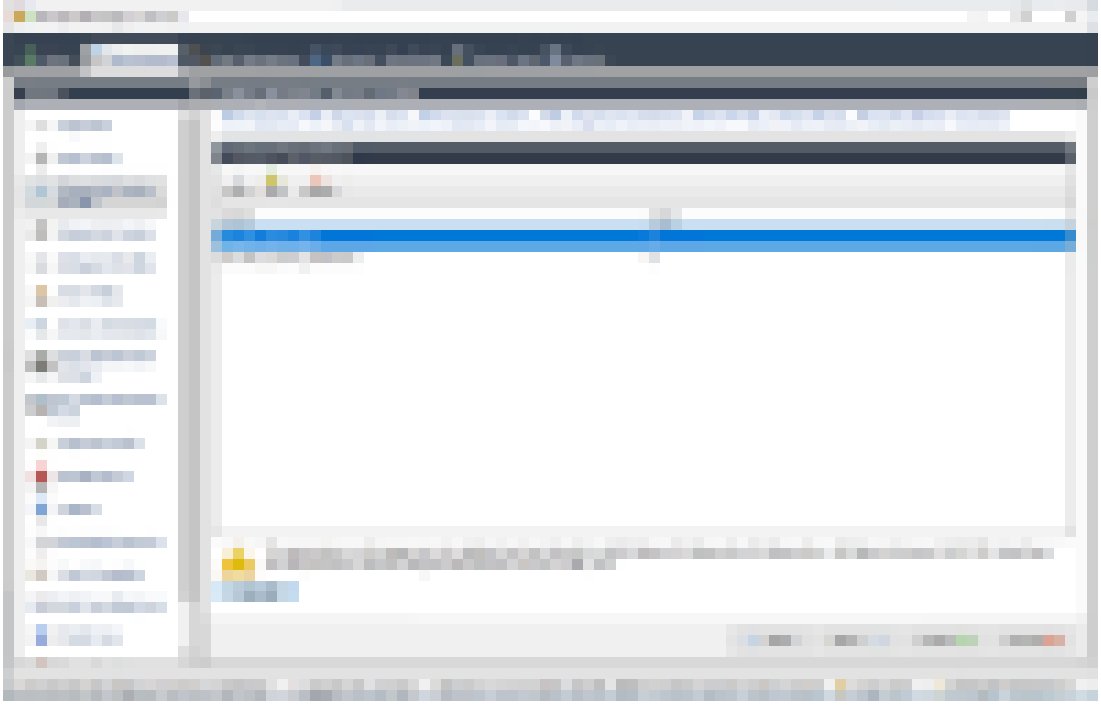
2. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Biometric Device Settings** (Biometrische Geräteeinstellungen) angelangt sind.



3. Wählen Sie für **Wiegand Profile** (Wiegand-Profil) dasselbe Profil aus, das Sie bei der Einrichtung von BioBridge für Ihre biometrischen Geräte definiert haben.



4. Aktivieren Sie das Kontrollkästchen **Biometric** (Biometrisch) und das Kontrollkästchen der Ausweistechnologie, die Ihre Installation verwendet.
5. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Custom Parameters** (Benutzerdefinierte Parameter) angelangt sind.



6. Klicken Sie auf **Add** (Hinzufügen), um zwei benutzerdefinierte Parameter hinzuzufügen. Hinweis: Wenn diese zwei Parameter festgelegt werden, sendet der Leser die Ausweisdaten direkt an den AMC. Der Benutzer muss nicht beim IDEMIA-Leser registriert sein.

- *ucc.per_user_rules*
- *ucc.user_record_reference*

7. Klicken Sie auf **Finish** (Fertigstellen).

Benutzern diese Benutzerrichtlinie zuweisen

1. Navigieren Sie im MorphoManager zu **Administration** > **User Policy** (Verwaltung > Benutzerrichtlinie).
2. Legen Sie die folgenden Attribute für **User Authentication Mode** (Benutzerauthentifizierungsmodus) fest:
– **Allow Start By Biometric** (Start durch biometrische Daten zulassen) aktivieren
– **Allow Start By Contactless Card** (Start durch berührungslosen Ausweis zulassen) aktivieren
– **Require Template Match** (Vorlagenübereinstimmung erforderlich) deaktivieren
3. Klicken Sie auf **Finish** (Fertigstellen).

21.5.2 Ausweis UND Biometrie

Nehmen Sie die folgenden Einstellungen vor, wenn Benutzer sich mit Ausweis UND biometrischen Nachweisen identifizieren müssen, um zu bestätigen, dass sie wirklich Ausweisinhaber sind.

1. Navigieren Sie im MorphoManager zu **Administration** > **Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil).
2. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Biometric Device Settings** (Biometrische Geräteeinstellungen) angelangt sind.
3. Wählen Sie für **Wiegand Profile** (Wiegand-Profil) dasselbe Profil aus, das Sie bei der Einrichtung von BioBridge für Ihre biometrischen Geräte definiert haben.
4. Klicken Sie auf **Next** (Weiter), bis auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) angelangt sind.
5. Aktivieren Sie das Kontrollkästchen der Ausweistechnologie, die von der Installation verwendet wird.
6. Klicken Sie auf **Finish** (Fertigstellen).

Benutzern diese Benutzerrichtlinie zuweisen

1. Navigieren Sie im MorphoManager zu **Administration** > **User Policy** (Verwaltung > Benutzerrichtlinie).
2. Für **User Authentication Mode** (Benutzerauthentifizierungsmodus): Wählen Sie *`Contactless Card ID + Biometric`* aus der Liste aus.
3. Klicken Sie auf **Finish** (Fertigstellen).

21.5.3 Nur Biometrie

Nehmen Sie die folgenden Einstellungen vor, wenn Benutzer sich nur mit biometrischen Nachweisen identifizieren können sollen.

1. Navigieren Sie im MorphoManager zu **Administration** > **Biometric Device Profile** (Verwaltung > Biometrisches Geräteprofil).
2. Klicken Sie auf **Next** (Weiter), bis Sie auf der Seite **Biometric Device Settings** (Biometrische Geräteeinstellungen) angelangt sind.
3. Wählen Sie für **Wiegand Profile** (Wiegand-Profil) dasselbe Profil aus, das Sie bei der Einrichtung von BioBridge für Ihre biometrischen Geräte definiert haben.
4. Klicken Sie auf **Next** (Weiter), bis auf der Seite **Multi-Factor Mode Settings** (Einstellungen für Mehrfach-Modus) angelangt sind.
5. Für **Multi-Factor Mode** (Mehrfach-Modus): Wählen Sie *`Biometry only`* aus der Liste aus.
6. Klicken Sie auf **Finish** (Fertigstellen).

Benutzern diese Benutzerrichtlinie zuweisen

1. Navigieren Sie im MorphoManager zu **Administration** > **User Policy** (Verwaltung > Benutzerrichtlinie).
2. Für **User Authentication Mode** (Benutzerauthentifizierungsmodus): Wählen Sie *Biometric(1:many)* aus der Liste aus.
3. Klicken Sie auf **Finish** (Fertigstellen).

21.6 Technische Hinweise und Grenzen

Offiziell unterstützte Windows-Betriebssysteme
IDEMIA unterstützt dieselben Versionen von Windows 10 wie AMS.

Offiziell unterstützte Version von Microsoft SQL Server
Die unterstützte Version ist SQL Server 2017.

Ein IDEMIA-System pro Zutrittssystem
Ein Bosch Zutrittskontrollsystem kann nur ein IDEMIA-System unterstützen.

Ein IDEMIA-Ausweis pro Ausweisinhaber
Bosch Zutrittskontrollsysteme unterstützen mehrere Ausweise pro Ausweisinhaber, aber IDEMIA unterstützt nur einen Ausweis. Daher wird bei der Registrierung und bei der Synchronisierung mit BIS der erste gültige Ausweis (d. h. mit Status = 1) vom Typ „Access“ (Zutritt), „Temporary“ (Temporär) oder „Parking“ (Parken) IDEMIA zugewiesen. Wenn der Ausweis später gesperrt wird, wird seine Nummer weiterhin übertragen und im Ereignisprotokoll erfasst.

Maximale Anzahl der IDEMIA-Ausweisinhaber
Der BioBridge MorphoManager kann bis zu 100.000 Ausweisinhaber verarbeiten.

Maximale Anzahl der Zutrittsgruppen
IDEMIA unterstützt bis zu 5000 Zutrittsgruppen (Benutzerverteilergruppen). Diese werden **Personenklassen** im Bosch Zutrittskontrollsystem zugeordnet.

Leistung von Vorlagen-Downloads
- 1000 Vorlagen auf 1 Gerät: der Download dauert weniger als 1 Minute.
- 1000 Vorlagen auf 100 Geräte: Der Download dauert einige Minuten.

Keine Mandantenunterstützung durch IDEMIA
Wenn ein IDEMIA-System in einem AMS-System integriert ist, können die Ausweisinhaber eines Mandanten nicht zuverlässig von den Zutrittskontrollbedienern eines anderen Mandanten überprüft werden. Wenn absoluter Datenschutz zwischen den Mandanten verpflichtend ist, sollten Sie kein IDEMIA-System integrieren.

Virtuelle Ausweise/Zutritt nur per PIN-Code
IDEMIA unterstützt keinen Zutritt nur mit PIN-Code. Es ist ein physischer Ausweis erforderlich.

IDEMIA-Bedrohungsfinger-Funktion

Die IDEMIA-Bedrohungsfinger-Funktion wird derzeit nicht von AMC-Controllern unterstützt.

Erforderliche Mindestkriterien zur Identifikation

Die Registrierung im IDEMIA-System erfordert mindestens die folgenden Identifikationskriterien:

- Vorname
- Nachname
- Personenklasse
- ein physischer Ausweis, der dem Ausweisinhaber zugewiesen wurde

Statusanzeige auf den Lesern

Auf Wiegand- und OSDP-Lesern wird kein Leserstatus (z. B. „Gerät blockiert“) angezeigt.

Backup und Wiederherstellung

Bevor Sie eine Sicherung eines AMS-Systems mit IDEMIA wiederherstellen können, müssen Sie die IDEMIA-Datenbank mit dem IDEMIA DataBridge-Anbietertool löschen und neu erstellen.

22

23 Definieren von Zutrittsberechtigungen und Profilen

23.1 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)

23.2 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.

24 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?

24.1 Personen

Die folgende Tabelle listet die Daten auf, die standardmäßig in den Dialogen **Persons** (Personen) angezeigt werden. Die Dialoge können in hohem Maße angepasst werden. Siehe Abschnitt **Benutzerdefinierte Felder für Personaldaten**.

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 (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 (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. Bestimmte Fingerabdrücke als Zeichen bei Bedrohung festlegen.

Siehe

– *Benutzerdefinierte Felder für Personaldaten, Seite 134*

24.1.1 Optionen zur Ausweis- oder Gebäudesteuerung

Übersicht

In der Registerkarte **Card control** (Ausweissteuerung) können Sie Ausweisinhabern die Möglichkeit geben, einen oder zwei generische Zutrittskontrollausgänge mit ihrem Ausweis zu aktivieren. Sie weisen einem Ausweisinhaber die Fähigkeit zu, indem Sie im Dialog **Persons** (Personen) das Kontrollkästchen **Building control** (Gebäudesteuerung) aktivieren. Die Kontrollkästchen **Building control** (Gebäudesteuerung) oder **Card control** (Ausweissteuerung) sind vordefinierte benutzerdefinierte Felder, die standardmäßig auf der Registerkarte **Card control** (Ausweissteuerung) der Person angezeigt werden, aber an anderer Stelle positioniert werden können.

Für die Option zur Gebäudesteuerung gibt es zwei Hauptaufgaben. Sie werden im Folgenden beschrieben:

– Konfigurieren Sie das Kontrollkästchen: Geben Sie ihm eine geeignete Bezeichnung und positionieren Sie es (falls gewünscht) auf einer anderen Registerkarte im Dialog **Persons** (Personen).
– Weisen Sie die Funktion einem Ausgang auf einer AMC-Zutrittskontrollzentrale und einem Kontrollkästchen zu.

Voraussetzungen

– Der Ausgang der Zutrittskontrollzentrale ist elektrisch mit dem Gerät verbunden, das durch den Ausweis aktiviert werden soll.

Dialogpfad

– AMS-Hauptmenü > **Configuration** > **Options** > **Custom fields** > Registerkarte **Card control** (Konfiguration > Optionen > Benutzerdefinierte Felder > Registerkarte „Ausweissteuerung“)

Konfigurieren der Kontrollkästchen

1. Wählen Sie auf der Seite **Custom fields** (Benutzerdefinierte Felder) im oberen Bereich die Registerkarte **Details** aus.
2. Suchen Sie die Funktion **Building control** (Gebäudesteuerung) 1 oder 2, die Sie verwenden möchten.
3. Ersetzen Sie die Bezeichnung mit einem geeigneten Namen (empfohlen). Positionieren Sie das Kontrollkästchen ggf. auf einer anderen Registerkarte als **Card control** (Ausweissteuerung). Weitere Informationen finden Sie im Abschnitt **Vorschauanzeige und Bearbeiten von benutzerdefinierten Feldern** unter dem unten stehenden Link.

Zuweisen der Funktion zu einem Ausgang der Zutrittskontrollzentrale und einem Kontrollkästchen

Siehe Abschnitt **AMC-Parameter und -Einstellungen** unter dem unten stehenden Link.

1. Wählen Sie im **Geräteeditor** im Gerätebaum die AMC-Zutrittskontrollzentrale aus, deren Ausgangssignal Sie verwenden möchten.
2. Wählen Sie auf der Registerkarte **Outputs** (Ausgänge) im oberen Bereich den gewünschten Ausgang aus.
3. Wählen Sie im mittleren Bereich **Output data** (Ausgabedaten) Typ **25, Card control** (Ausweissteuerung) aus.
4. Klicken Sie auf die Schaltfläche **>**, um den Ausgang zum unteren Bereich hinzuzufügen.
5. Wählen Sie im unteren Bereich in Spalte **Param11** die Bezeichnung der Gebäudesteuerungsfunktion aus, die Sie im vorherigen Verfahren **Konfigurieren der Kontrollkästchen** ausgewählt haben.
6. Speichern Sie den Gerätebaum.

Siehe

- *AMC-Parameter und -Einstellungen, Seite 58*
- *Vorschauanzeige und Bearbeiten von benutzerdefinierten Feldern, Seite 134*

24.1.2 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.

24.1.3 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.

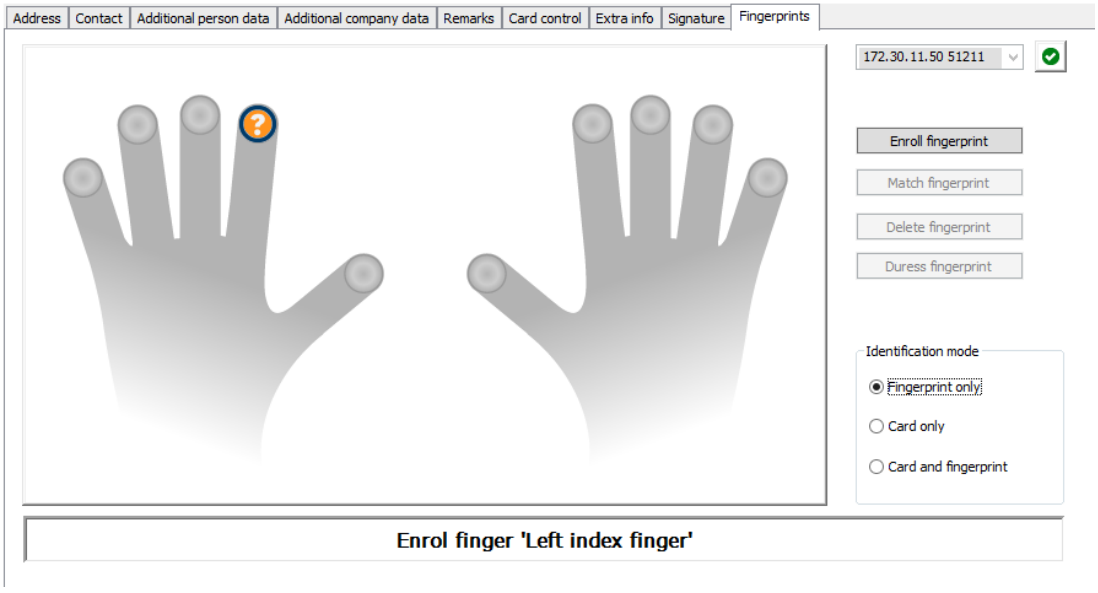
1. Klicken Sie auf die Registerkarte **Signature** (Unterschrift).
2. Klicken Sie zum Erfassen einer neuen Unterschrift auf die Schaltfläche **Capture Signature** (Unterschrift erfassen).
3. Unterzeichnen Sie mit dem besonderen Stift direkt auf der Unterlage.
4. Klicken Sie zur Bestätigung auf die Häkchen-Schaltfläche.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

24.1.4 Registrieren von Fingerabdruckdaten



Voraussetzungen

– Ein oder mehrere Fingerabdruckleser müssen an den Durchtritten 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.
– Die zu registrierende Person befindet sich vor einem Fingerabdruckleser, der mit Ihrer Bedienstation verbunden und für diese konfiguriert ist. Dieser Fingerabdruckleser für die Registrierung darf **kein** Zutrittsleser sein.
– Als Bediener kommunizieren Sie direkt mit der zu registrierenden 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

1. 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

- Fingerabdruckleser können nur Zeichen für Bedrohung senden, wenn Sie im **Geräteeditor** mit der folgenden Einstellung konfiguriert sind:
  Registerkarte **Network & Operation modes** > **Templates on server** > **Card and fingerprint** (Registerkarte „Netzwerk- und Betriebsmodi“ > Vorlagen auf Server > Ausweis und Fingerabdruck)
- Mindestens ein Fingerabdruck der zu registrierenden Person 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.

24.2 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.

24.3 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 entwerten 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).

24.3.1 Zuweisen von Ausweisen zu Personen

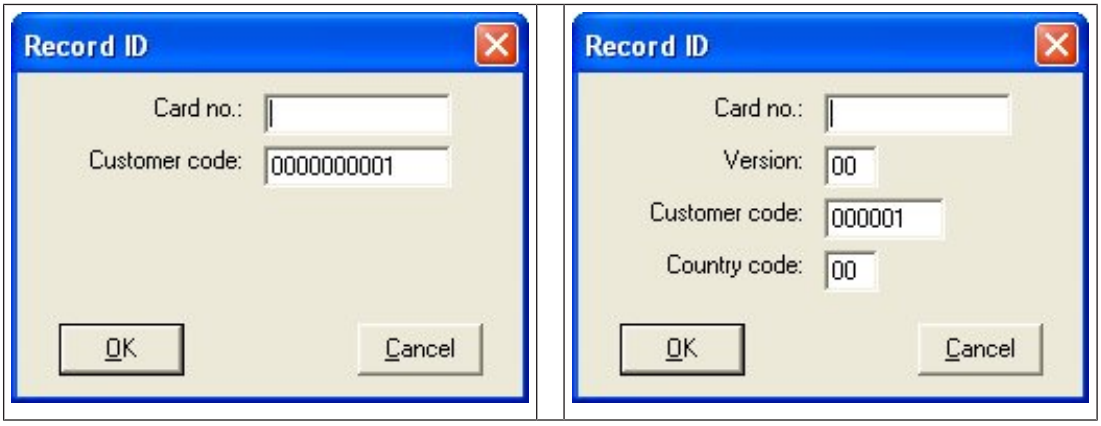
Einführung
Alle Personen, die der Zutrittskontrolle unterliegen, benötigen einen Ausweis oder einen anderen elektronischen Nachweis, der den Inhabern in dem Dialog **Cards** (Ausweis) zugewiesen wird.
Ausweisnummern können manuell oder über einen Bekanntmachungsleser zugewiesen werden.

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

Voraussetzungen

- 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

– Auf der Bedienstation ist ein Bekanntmachungsleser konfiguriert.

Vorgehensweise für die Registrierung

1. Klicken Sie auf die Schaltfläche rechts von der Schaltfläche **Record card** (Ausweis erfassen), um einen konfigurierten Bekanntmachungsleser auszuwählen.

– Beachten Sie, dass Sie beim AMS Dialog-Manager als Administrator angemeldet sein müssen, um die Auswahl des Bekanntmachungslesers zu ändern.

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. Wählen Sie einen Ausweis aus der Liste aus.
2. Klicken Sie auf die Schaltfläche **Change card** (Ausweis wechseln).
3. Im Popup-Fenster:

– Wählen Sie **Replace card** (Ausweis ersetzen), wenn das Original dauerhaft verloren oder beschädigt wurde.
– Wählen Sie **Temporary card** (Temporärer Ausweis), wenn das Original verlegt oder zu Hause vergessen wurde und nur ein vorübergehender Ersatz erforderlich ist.
  – Geben Sie eine Gültigkeitsdauer für den temporären Ausweis ein.
  – Wählen Sie diese Option, wenn Sie alle anderen Ausweise jetzt deaktivieren möchten.
  – Wählen Sie aus, ob die Originalausweise automatisch reaktiviert werden sollen, wenn der temporäre Ausweis abläuft.

4. 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.

24.3.2 Drucken von Ausweisen

Voraussetzungen

– Der Personendatensatz für den neuen Ausweisinhaber sollte bereits im System vorhanden sein.
– Eine Bedienstation mit folgender angeschlossener Hardware, normalerweise über USB:
  – Ausweisdrucker
  – Kamera zum Aufnehmen von ID-Fotos

Vorgehensweise

Dialogpfad

AMS-Client: **Personnel data** (Personendaten) > **Print badges** (Ausweise drucken)

1. Laden Sie den Personendatensatz, für den der Ausweis gedruckt werden soll.
2. Wählen Sie im Pulldown-Menü **Layout** das gewünschte Ausweislayout aus den gespeicherten Layouts aus.
3. Mit einer der folgenden Methoden können Sie ein Ausweisfoto einfügen:
  – Klicken Sie auf die Schaltfläche **Capture** (Bild aufnehmen) und wählen Sie aus der Liste der angeschlossenen Kameras die gewünschte Kamera aus.
  – Klicken Sie auf die Schaltfläche **Import picture** (Bild importieren), und wählen Sie mithilfe des Zuschneiderahmens den Ausschnitt des Fotos aus, der auf den Ausweis gedruckt werden soll.
4. Klicken Sie auf **Preview** (Vorschau), um sicherzustellen, dass die richtigen Daten im richtigen Layout auf dem Ausweis erscheinen.
5. Klicken Sie auf **Print** (Drucken), um den Ausweis zu drucken.

Unterstützte Kameras

Alle USB-Geräte, die das Betriebssystem als Kamera anerkennt.

24.3.3 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 187*
– 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.

24.3.4 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.

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 mehr Zeit (Standard ist 3x) für den Durchtritt zu geben, bevor der Zustand **Door open too long** (Tür zu lange geöffnet) generiert wird.
Hinweis: Der Standardfaktor für die Verlängerung kann in den Eigenschaften des MAC im Geräteeditor zurückgesetzt werden.
Navigieren Sie zu **Global Access Settings** > **Time factor for handicapped persons** (Globale Zutrittseinstellungen > Zeitfaktor für Personen mit Behinderung)

Wegekontrolle
Ein **Weg** oder ein **Rundgang** beschreibt eine strenge Abfolge von Lesern, die im Client-Menü festgelegt wird: **Tour monitoring** > **Define routes** (Wegekontrolle > 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**).

Siehe
– *Autorisieren von Personen zum Festlegen des Büromodus, Seite 200*

24.3.5 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 entsperrte 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.

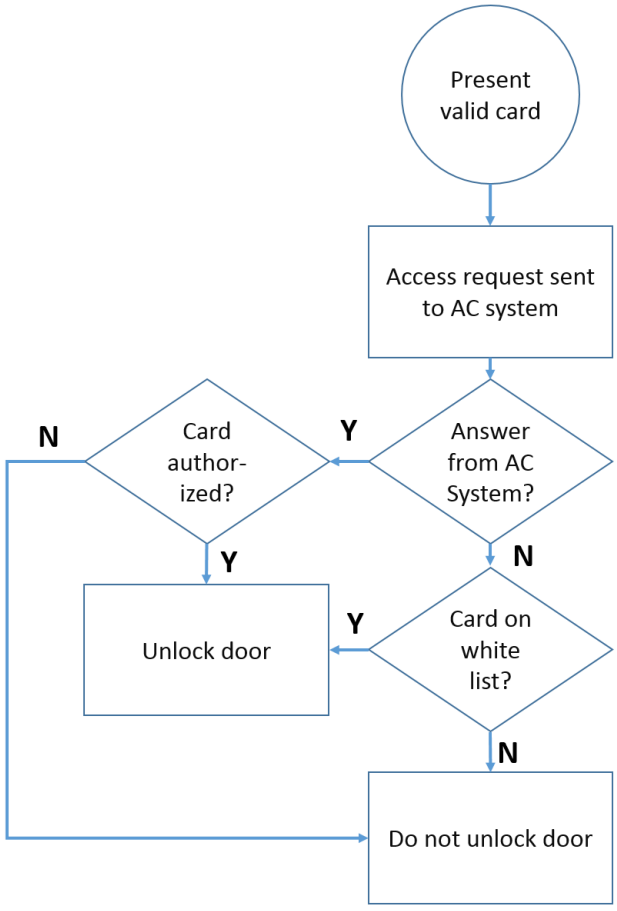
Hinweis!
Büromodus und Geräteparameter für Tür
Der Büromodus überschreibt den Parameter **Unlock door** (Tür entsperren) auf der Registerkarte **Options** (Optionen) einer Tür im Geräteeditor, sodass nur **0 Normal Modus** (Normalmodus) und **1 Unlocked** (Entsperrt) zulässig sind.

24.3.6 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.

24.3.7 Erstellen eines Alarmausweis

In diesem Abschnitt wird beschrieben, wie Sie einen Alarmausweis erstellen, der zum Auslösen einer Bedrohungsstufe verwendet werden kann.

Einführung

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

Voraussetzungen

- Im System ist ein Bekanntmachungsleser konfiguriert.
- Mindestens eine Bedrohungsstufe wurde im System definiert.

Dialogpfad

Hauptmenü > **Personnel data** > **Cards** > **Alert card** (Personaldaten > Ausweise > 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.

24.4 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 Bedienstation konfiguriert ist.
- Ein geeigneter physischer Ausweis ist für die Registrierung im System als temporärer Ausweis verfügbar.

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

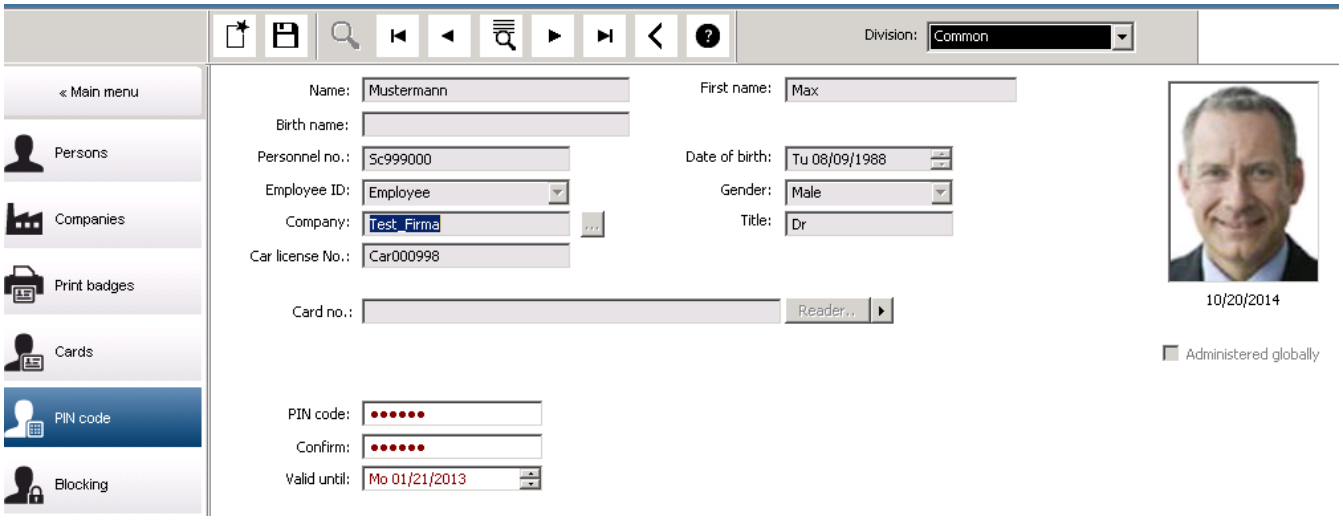
Vorgehensweise: Entfernen von temporären Sperren auf Ausweisen
Wenn die Sperrung des ursprünglichen Ausweises nicht mehr erforderlich ist, löschen Sie die Sperre wie folgt:
1. Navigieren Sie zum Dialog **Blocking** (Sperrung): **Personnel data** > **Blocking** (Personaldaten > Sperrung)
2. Wählen Sie in der Liste der Ausweise den persönlichen Ausweis aus, der in der Spalte **Lock(s)** (Sperre(n)) als gesperrt angezeigt wird.
3. Klicken Sie auf **Release temporary lock** (Temporäre Sperre aufheben)
   Beachten Sie, dass durch das Entfernen von **Blocking** (Sperrung) keine temporären Ausweise entfernt werden. Temporäre Ausweise laufen nach Ende ihrer Gültigkeitsdauer automatisch ab. Bei Bedarf können Sie sie manuell löschen.

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.

24.5 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.



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 parametriert werden. 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.

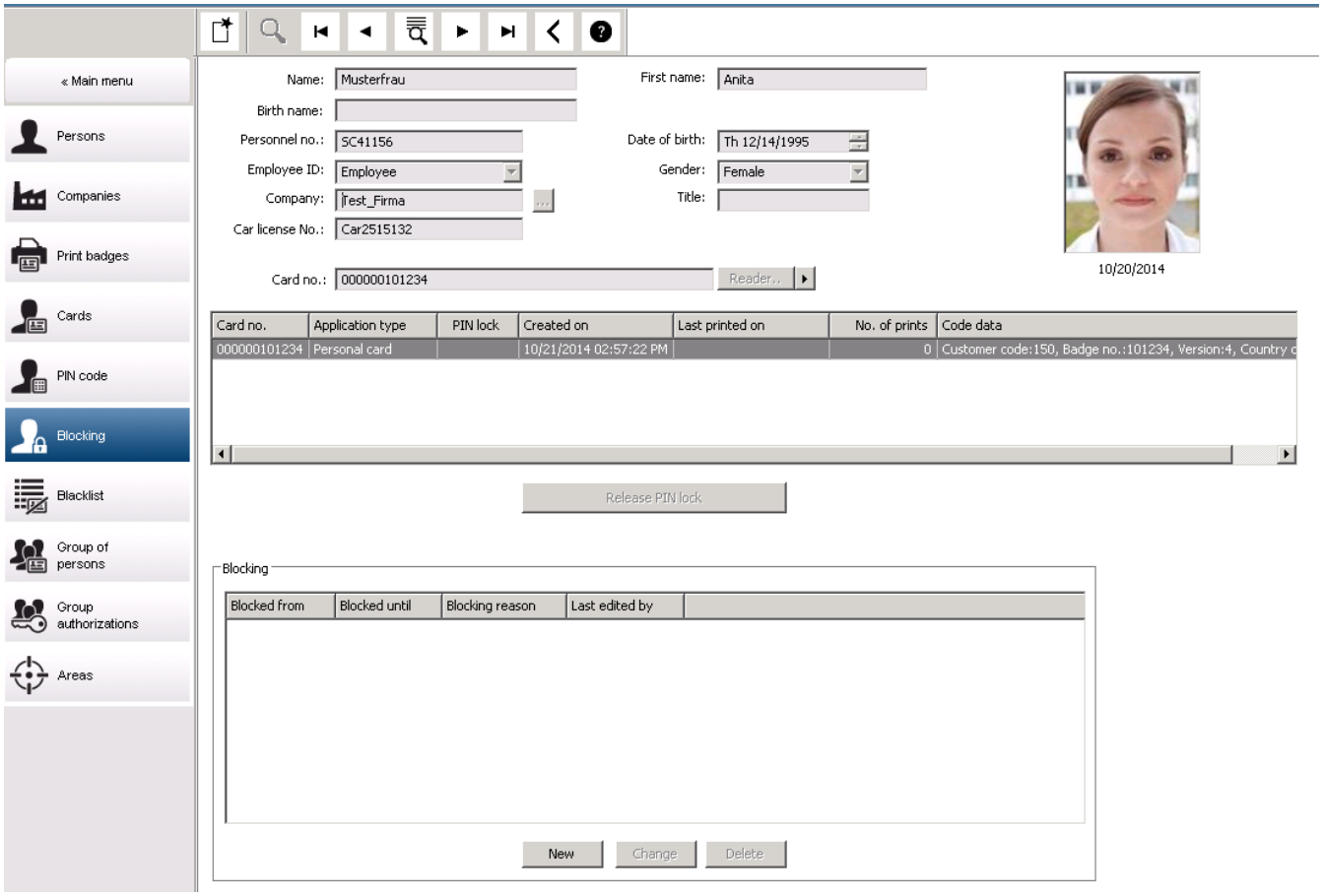
Es stehen zwei Varianten zur Verfügung, die gleichzeitig aktiviert sind und zwischen denen die bedrohte Person wählen kann:

– 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.

24.6 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 Mitarbeiterauslosung verhängt wurde, aufgehoben werden muss.
Sperren bedeutet, dass der Zutritt für diese Person unabhängig von den verwendeten Zugangsdaten verweigert wird.



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.

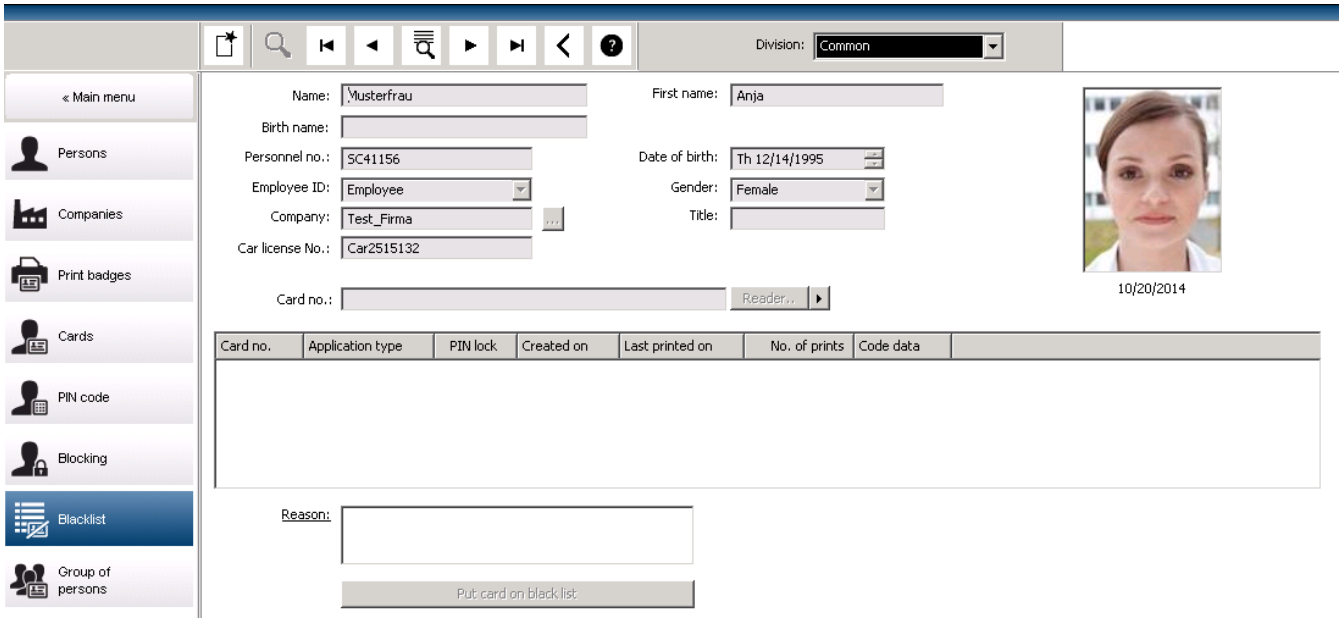
Hinweis!
Die Sperrung gilt für die Person, nicht für bestimmte Zugangsdaten. Es ist daher nicht möglich, die Sperre durch die Zuweisung eines neuen Ausweises aufzuheben oder zu umgehen.

24.7 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.



Main menu (Hauptmenü) > **Personnel data** (Personaldaten) > **Blacklist** (Schwarze Liste)

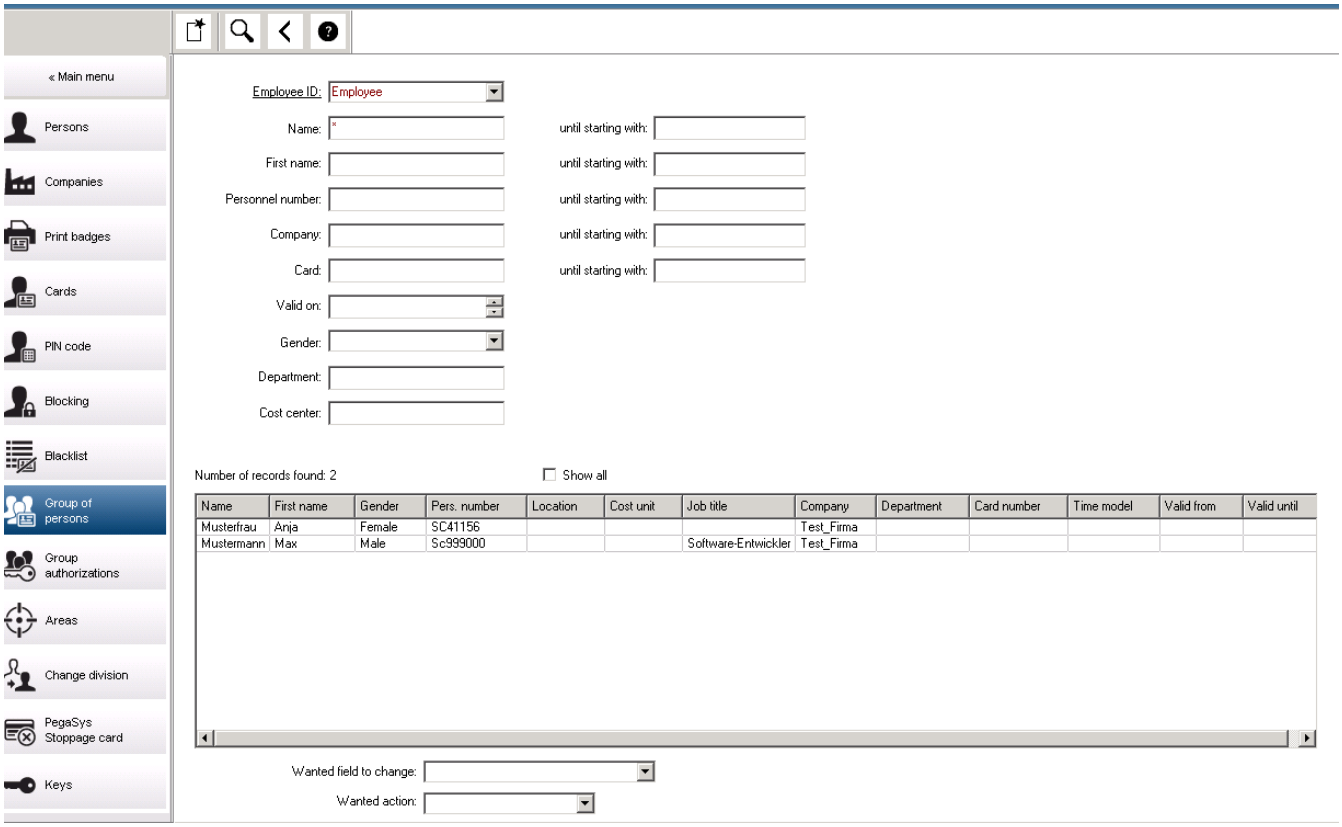
1. Wählen Sie die Person aus, deren Ausweis in die schwarze Liste aufgenommen werden soll.
2. Wenn diesem Ausweisinhaber mehrere Ausweise zugewiesen sind, wählen Sie den Ausweis aus der Liste **Ausweisnummer** aus.
3. Geben Sie im Eingabefeld **Reason** (Grund) den Grund für die Sperre an.
4. Klicken 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.

24.8 Bearbeiten von mehreren Personen gleichzeitig

Personengruppe



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.

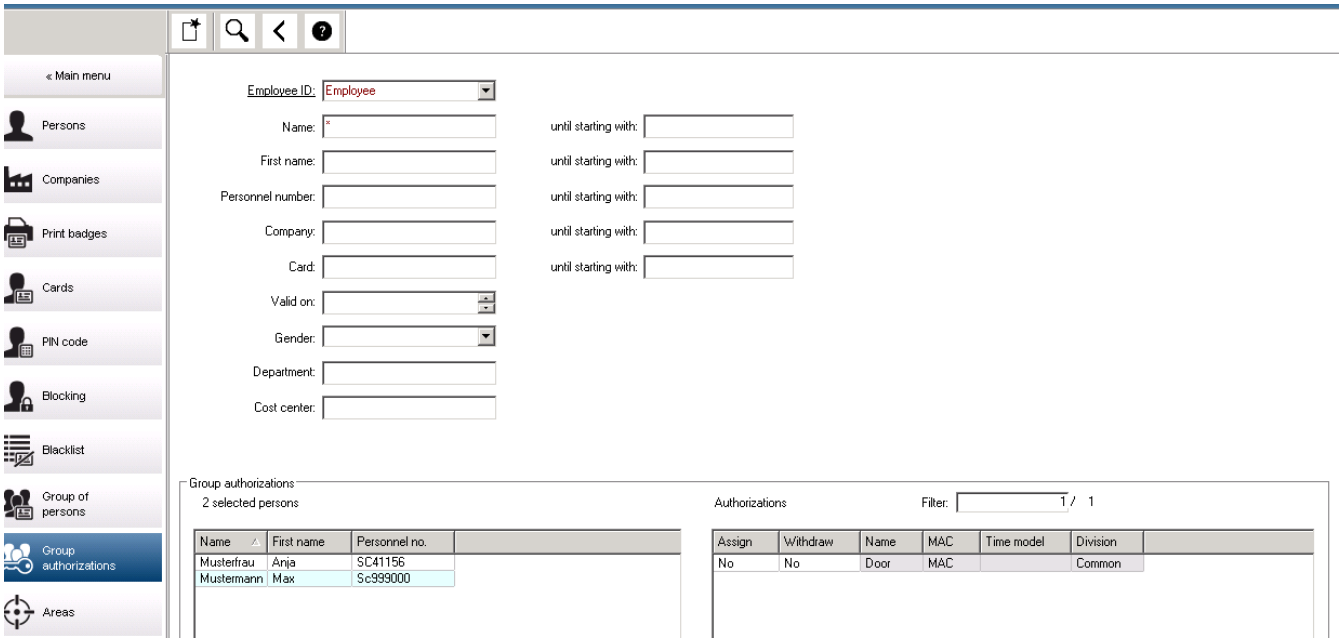
Nachdem die Personengruppe ausgewählt wurde, können Sie die folgenden Einträge auswählen:
- Employee ID (Personalkennung)
- Name
- First name (Vorname)
- Personnel number (Personalnummer)
- Company (Unternehmen)
- Card (Ausweis)
- Valid on (Gültig am)
- Gender (Geschlecht)
- Department (Abteilung)
- 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.

24.8.1 Gruppenberechtigungen

Gruppenberechtigungen



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
- Reservefelder, 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.

24.9 Ändern des Mandanten für Personen

Einführung
Change division (Mandant ändern) ist ein wichtiger Dialog zum Ändern des Mandanten für einen Satz von Personaldatensätzen im System.

Hinweis!
Gehen Sie beim Verwenden dieser Funktion besonders vorsichtig vor!
Eine Änderung des Mandanten hat weitreichende Auswirkungen auf die geänderten Personaldatensätze.

Voraussetzungen
Der Bediener, der den Mandanten von Personaldatensätzen ändert, muss Berechtigungen zum Bearbeiten dieser Personen und der entsprechenden Mandanten haben.

Dialogpfad
Main menu > **Personnel data** > **Change division** (Hauptmenü > Personaldaten > Mandant ändern)

Vorgehensweise
1. Geben Sie im Bereich **Filter persons** (Personen filtern) Filterkriterien in eines oder mehrere der folgenden Felder ein:

Filter	**Remarks/Description** (Anmerkungen/Beschreibung)
Last name (Nachname)	Verwenden Sie ein Asterisk (*), um alle Personen oder Buchstaben **ohne** Asterisk zu finden.
Personnel no. from/ to (Personalnummer von/bis)	Verwenden Sie beide Felder, um einen Wertebereich zu definieren.
Employee ID (Employee type) (Personalkennung (Personaltyp))	Treffen Sie eine Auswahl in der Liste.
Division (Mandant)	Mit der Schaltfläche „Apply filter“ (Filter anwenden) werden nur Personen aus diesem Mandanten angezeigt.
Company (Unternehmen)	Wählen Sie eines der verfügbaren Unternehmen aus.
Department (Abteilung)	
Card no. (from/to) (Kartennr. (von/bis))	Verwenden Sie beide Felder, um einen Wertebereich zu definieren.

2. Klicken Sie auf **Apply filter** (Filter anwenden).
   Alle Personen, auf die der Filter zutrifft, werden in der Liste **Selected persons** (Ausgewählte Personen) angezeigt.
3. Um die Gruppe der ausgewählten Personen weiter zu verfeinern, klicken Sie auf eine oder mehrere Zeilen in der Liste **Selected persons** (Ausgewählte Personen) und dann auf die Schaltfläche **Remove** (Entfernen). Verwenden Sie die Strg- und die Umschalttaste zur gleichzeitigen Auswahl mehrerer Datensätze.

– **WICHTIG:** Stellen Sie vor dem Fortfahren sicher, dass die Liste **Selected persons** (Ausgewählte Personen) nur Personen enthält, für die Sie den Mandanten ändern möchten.

4. Wählen Sie in der Liste **New division** (Neuer Mandant) den Zielmandanten für die ausgewählten Personen aus.
5. Klicken Sie auf **Change division of persons** (Mandant von Personen ändern).
   ALLE Personen in der Liste **Selected persons** (Ausgewählte Personen) werden zu **New division** (Neuer Mandant) verschoben.

Auswirkungen des Wechsels von einem Mandanten zu einem anderen
Personen
– Zutrittsberechtigungen und Wegekontrolle
– Verknüpfungen zum bisherigen Mandanten werden gelöscht.
– Verknüpfungen zu Daten der Kategorie „Common“ (Allgemein) bleiben erhalten.
Unternehmen
– Verknüpfungen zu Unternehmen des bisherigen Mandanten werden gelöscht.

Auswirkungen des Wechsels von „Common“ (Allgemein) zu einem anderen Mandanten
– Zutrittsberechtigungen und Wegekontrolle
– Verknüpfungen zu „Common“ (Allgemein) und dem neuen Mandanten bleiben erhalten.
– Verknüpfungen zu anderen Mandanten werden gelöscht.

Auswirkungen des Wechsels von einem Mandanten zu „Common“ (Allgemein)
Alle Verknüpfungen bleiben erhalten.

24.10 Festlegen des Bereichs für Personen oder Fahrzeuge

Einführung
In diesem Abschnitt wird beschrieben, wie Sie den aufgezeichneten Aufenthaltsort eines Ausweisinhabers oder seines Fahrzeugs von einem definierten Bereich zu einem anderen ändern. Dies kann erforderlich werden, wenn der Ausweisinhaber von einem Bereich zu einem anderen gewechselt ist, ohne den Ausweis zu scannen. Unter solchen Umständen verweigern System mit strenger Zutrittswiederholsperre dem Ausweisinhaber einen weiteren Zutritt, bis sein tatsächlicher mit dem aufgezeichneten Aufenthaltsort übereinstimmt.

Voraussetzungen
– Zutrittsbereiche wurden in Ihrem System definiert und werden verwendet. Die Dokumentation finden Sie unter dem folgenden Link.
– Als Bediener haben Sie die Berechtigung zum Ändern der Daten des Ausweisinhabers.

Vorgehensweise zum Zurücksetzen des Aufenthaltsorts von einzelnen Ausweisinhabern und Fahrzeugen
Dialogpfad
Main menu > **Personnel data** > **Areas** (Hauptmenü > Personaldaten > Bereiche)

1. Wählen Sie den Ausweisinhaber wie gewohnt aus der Datenbank aus.
2. Wählen Sie in der Liste **Location** (Aufenthaltsort) einen neuen Aufenthaltsort aus oder
3. Wählen Sie in der Liste **Location of the vehicle** (Aufenthaltsort des Fahrzeugs) einen neuen Aufenthaltsort für das Fahrzeug des Ausweisinhabers aus.
4. Klicken Sie zum Speichern auf  .

Siehe

– *Konfigurieren von Bereichen der Zutrittskontrolle, Seite 26*

24.10.1 Vorgehensweise zum Zurücksetzen des Aufenthaltsorts von allen Ausweisinhabern und Fahrzeugen

Diese Vorgehensweise kann beispielsweise nach einer Evakuierungsübung erforderlich sein. Alle Aufenthaltsorte werden auf **UNKNOWN** (UNBEKANNT) festgelegt, sodass Zutrittssequenzüberwachung und Zutrittswiederholsperre wieder aufgenommen werden können.

Vorgehensweise

Dialogpfad

Main menu > **System data** > **Reset areas unknown** (Hauptmenü > Systemdaten > Unbekannte Bereiche zurücksetzen)

– Klicken Sie auf **Set the areas of all persons present to UNKNOWN** (Bereiche aller bekannten Personen auf UNBEKANNT stellen)

oder

– Klicken Sie auf **Set the areas of all parking vehicles to UNKNOWN** (Bereiche aller parkenden Fahrzeuge auf UNBEKANNT stellen)

24.11 Anpassen und Drucken von Formularen für Personaldaten

Übersicht

Verwenden Sie **Forms** (Formulare), um Formularen zum Drucken von Ausweisinhaberdaten aus der Datenbank anzupassen. Diese Funktionalität kann von Ihren lokalen Datenschutzgesetzen vorgeschrieben sein.
Vorlagenformulare sind verfügbar. Diese Vorlagen können als HTML-Dateien exportiert, an Ihre Anforderungen angepasst und für die Verwendung im Dialog-Manager reimportiert werden. Instanziieren und drucken Sie die Formulare im Dialog **Personnel data** > **Print badges** (Personaldaten > Ausweise drucken).

Dialogpfad

– AMS-Hauptmenü > **Configuration** > **Options** > **Forms** (Konfiguration > Optionen > Formular)

Anpassen eines Formulars

1. Wählen Sie im Dialog **Forms** (Formular) in der Liste **Available forms** (Verfügbare Formulare) die Vorlage aus, die Sie anpassen möchten, in der Regel `AllPersonalData_EN,` die alle personenbezogenen Datenfelder in der Datenbank enthält.
2. Klicken Sie auf **Export** (Exportieren), um das Formular in einer neuen HTML-Datei auf Ihrem System zu speichern.
3. Verwenden Sie einen HTML-Editor, um die HTML-Datei an Ihre Anforderungen anzupassen.
4. Klicken Sie im Dialogfeld **Forms** (Formulare) auf **Insert** (Einfügen), um die angepasste HTML-Datei in den Dialog-Manager zu importieren.

- (Optional) Wenn das Formular nur für einen bestimmten Mandanten gültig ist, wählen Sie aus der Spalte **Division** (Mandant) einen Mandanten für das neue Formular aus.
- (Optional) Klicken Sie auf **Preview** (Vorschau), um das nicht instanziierte Formular in einem HTML-Viewer anzuzeigen.
- (Optional) Klicken Sie auf **Delete** (Löschen), um ein Formular aus der Liste zu löschen.

Instanziieren und Drucken eines Formulars

1. Navigieren Sie im Dialog-Manager zu:
– AMS-Hauptmenü > **Personnel data** > **Print badges** (Personaldaten > Ausweise drucken)
2. Laden Sie den gewünschten Personaldatensatz in das Formular.
3. Wählen Sie ein Formular aus der Liste **Form** (Formular) aus.
4. Klicken Sie auf **Print form** (Formular drucken).
   - Das Formular wird mit den Daten des ausgewählten Personaldatensatzes instanziiert und an den Drucker Ihrer Wahl gesendet.

25 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.

25.1 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 Ausweisrückgabe vom System gelöscht.

Für die Administration externer Besucher gibt es zwei Dialoge.

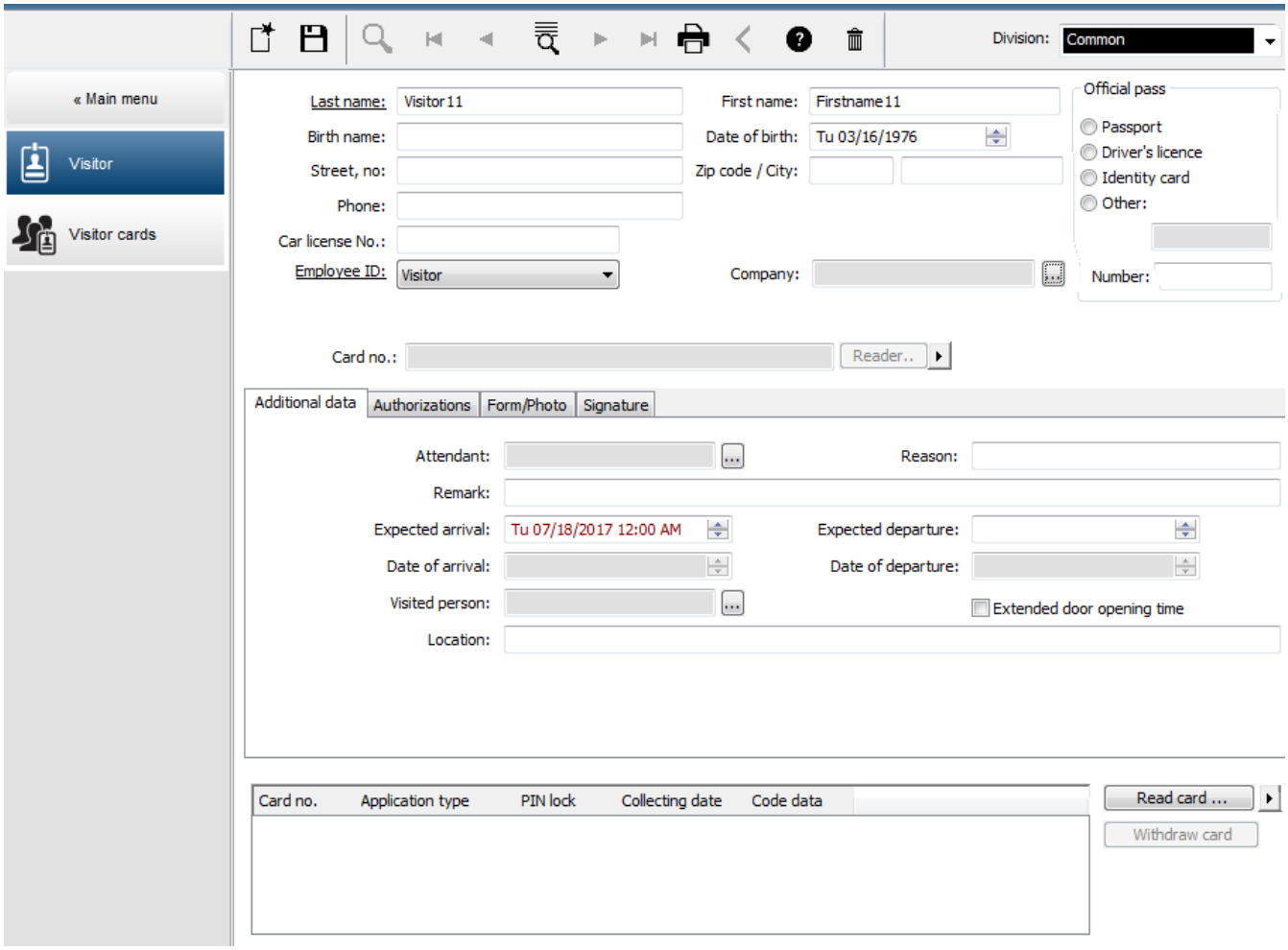
- Der Dialog **Visitors** (Besucher) dient zur Eingabe der Daten und Zutrittsberechtigungen der Besucher.
- Im Dialog **Visitor cards** (Besucherausweise) werden die Registrierung und die Löschung von Besucherausweisen geregelt.

Dialog: Visitors (Besucher)

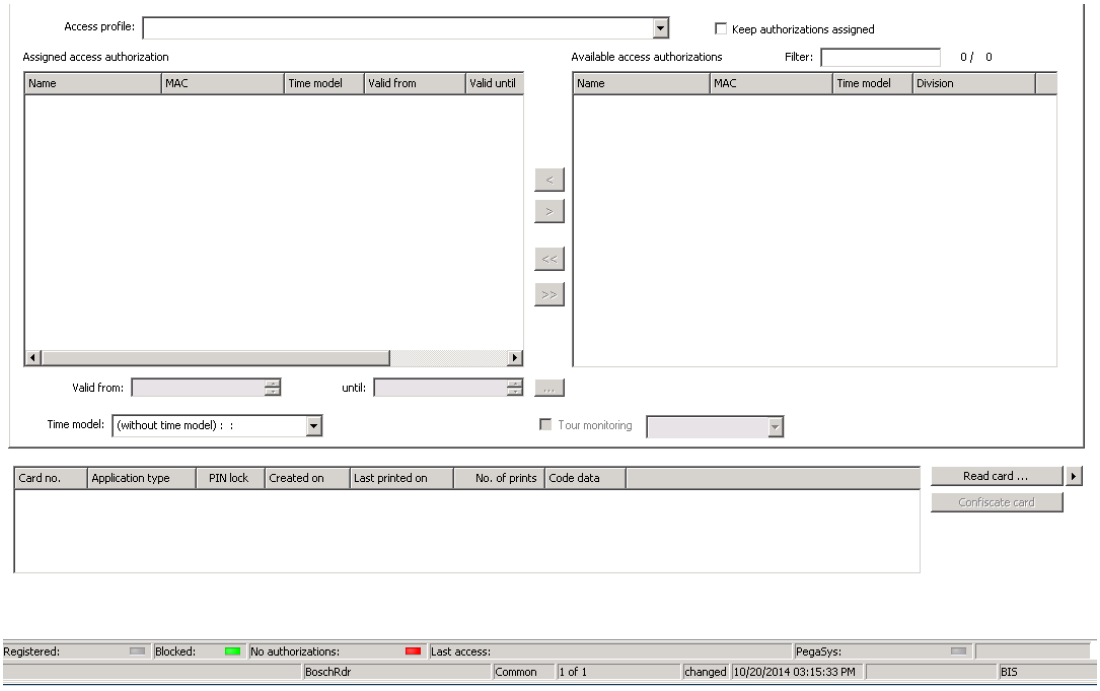
Besucher haben einen von den übrigen Personen streng getrennten Status und werden deshalb auch in einem separaten Dialog bearbeitet. Es ist im Dialog **Personen** nicht möglich, Personen mit der Kennung **Besucher** zu erstellen oder für diese Besucher Ausweise zu erfassen.

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.



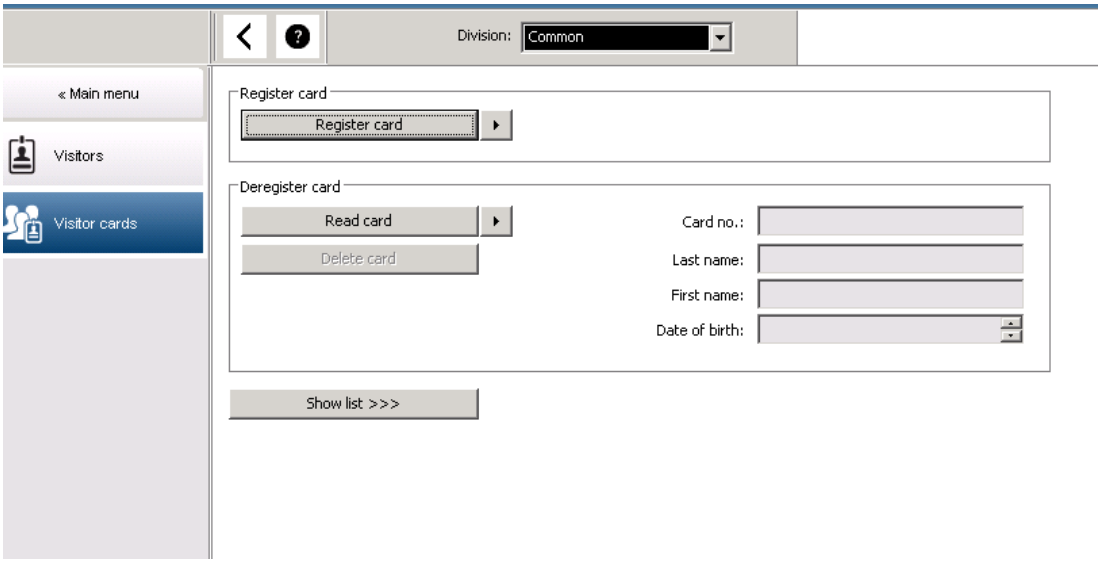
Der **Reason** (Grund) des Besuches, der besuchte **Location** (Ort) und eine **Remark** (Bemerkung) können in die unten stehenden Eingabefelder eingegeben werden.
Wenn Sie Daten in die Felder **Erwartete Ankunft** und **Erwartete Abreise** eingeben, werden die Daten in die Felder **Gültig von** und **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.



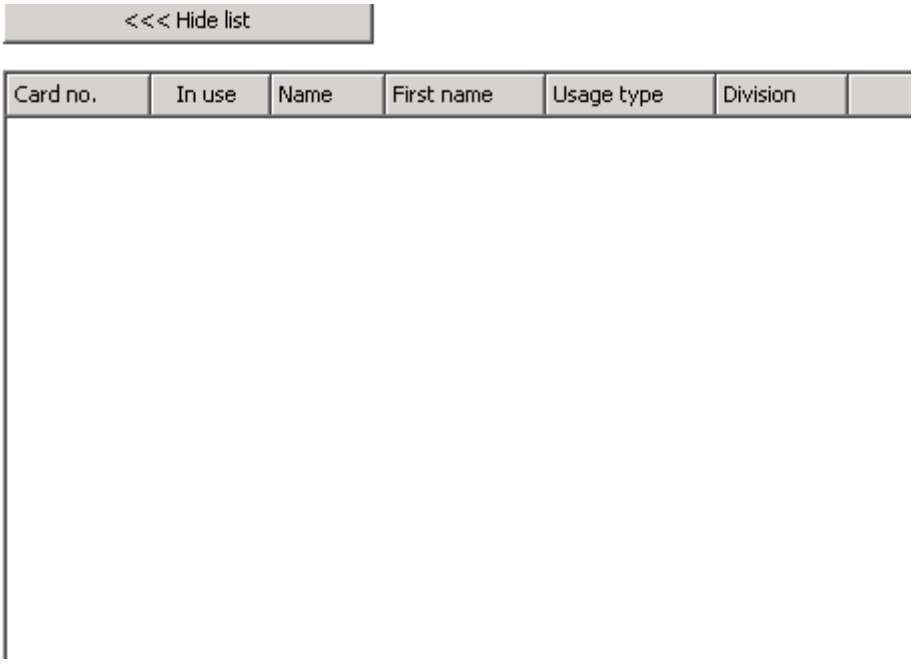
Im Dialog **Assign authorization** (Berechtigung zuweisen) kann ein vorhandenes Benutzerprofil in der Profilliste ausgewählt werden. Es können auch einzelne Zutrittsberechtigungen in der Liste **Available access authorization** (Verfügbare Zutrittsberechtigungen) markiert und in die links stehende Liste **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.



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
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?

☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at _____
Departure at _____

To sign on visited person

26 Verwalten von Parkplätzen

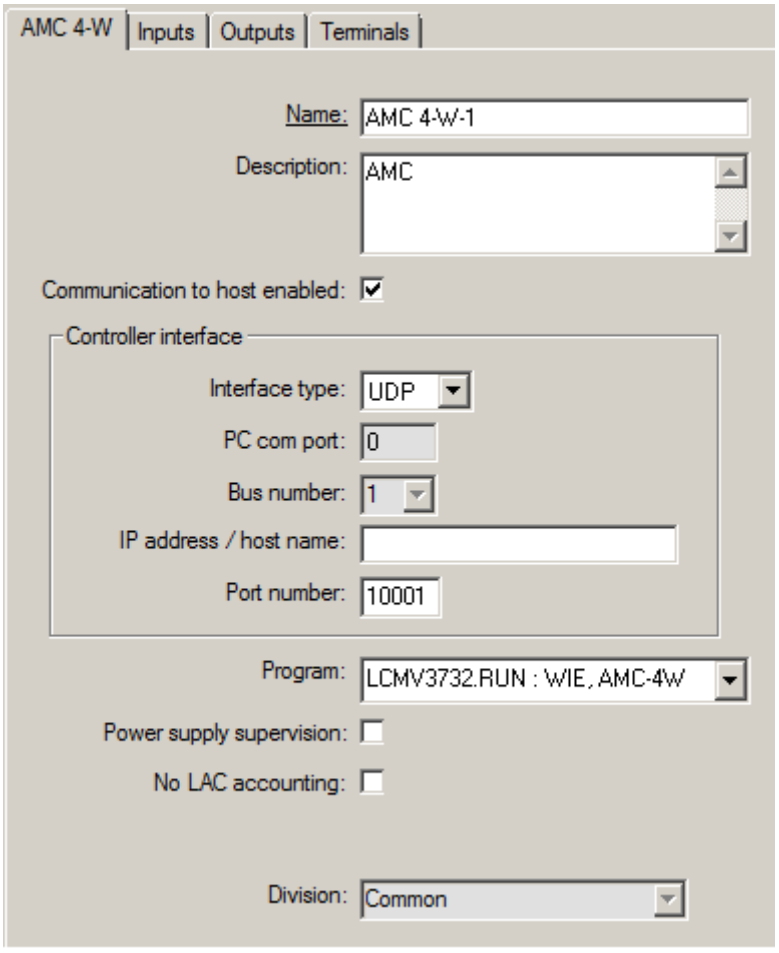
26.1 Berechtigungen für mehrere Parkzonen

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 LAC accounting** (Keine LAC-Berücksichtigung) in der AMC-Konfiguration.



26.2 Parkplatzbericht

Parking lot list Date 08.11.2013 , 14:51:23 Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

26.3 Erweitertes Parkplatzmanagement

Einführung

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

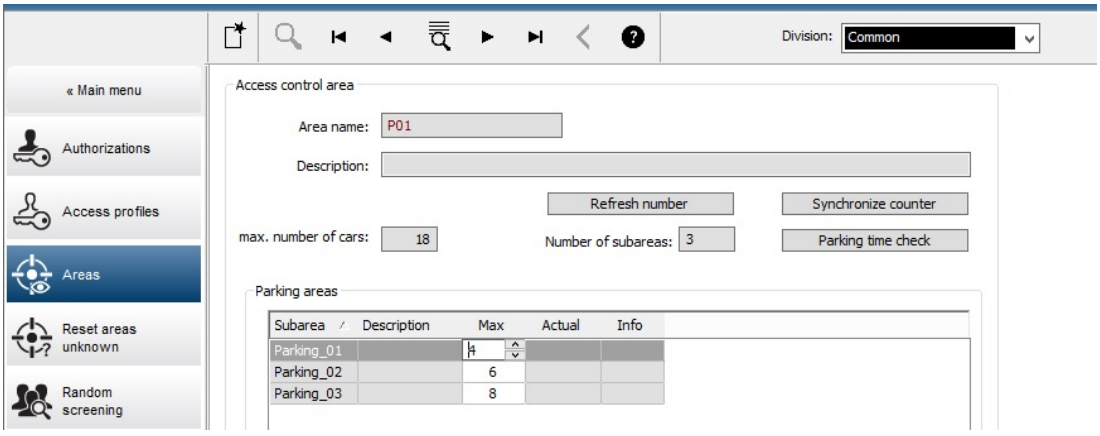
– Behindertengerechter Zugang
– Motorräder

Dialogpfad

Hauptmenü > **Systemdaten** > **Bereiche**

Vorgehensweise

1. Wählen Sie einen Parkplatz aus.
2. Passen Sie im Bereich **Parking areas** (Parkbereiche) den Wert in Spalte **Max** auf die neue Anzahl von Parkplätzen für diesen Bereich an.



Hinweise:

– In der Spalte **Max** vorgenommene Einstellungen überschreiben die Einstellungen, die in der Konfiguration **Areas** (Bereiche) vorgenommen wurden. Weitere Informationen finden Sie unter **Konfigurieren von Bereichen für Fahrzeuge** unter dem untenstehenden Link.
– Eine Null *0* in der Spalte **Max** bedeutet „unbegrenzt“. Die gesamte Fahrzeugzählung ist ausgeschaltet.

Siehe

– *Konfigurieren von Bereichen für Fahrzeuge, Seite 27*

27 Verwalten von Wächterrunden und Wächterkontrollgängen

Einführung in Wächterrunden

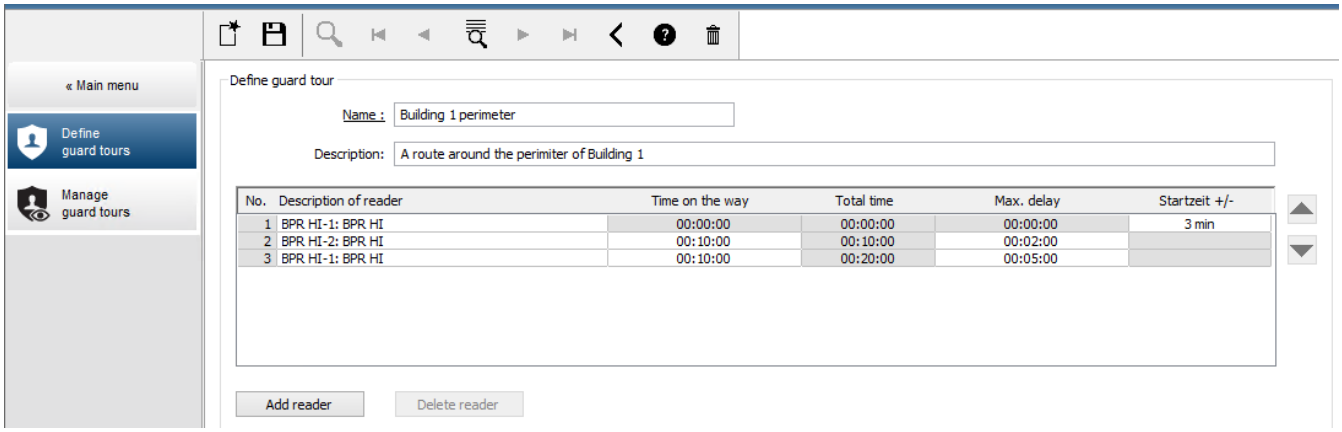
Eine **Wächterrunde** ist eine von Ausweislesern vorgegebene Route auf dem Gelände. Personen vom Mitarbeitertyp **Guard** (Wächter) müssen einen speziellen Wächterausweis vorlegen, um nachzuweisen, dass sie persönlich am Leser waren.
Mit Wächterausweisen werden keine Eingänge geöffnet, sie dienen lediglich 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.

27.1 Definieren von Wächterrunden

Wählen Sie **Guard tours** (Wächterrunden) > **Define guard tours** (Wächterrunden definieren)



– 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 Schaltflächen  und  per Klick nach oben oder unten.

27.2 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 Kontrollkäschen **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" ✔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.

27.3 Überwachung von Runden (ehemals Wegekontrolle)

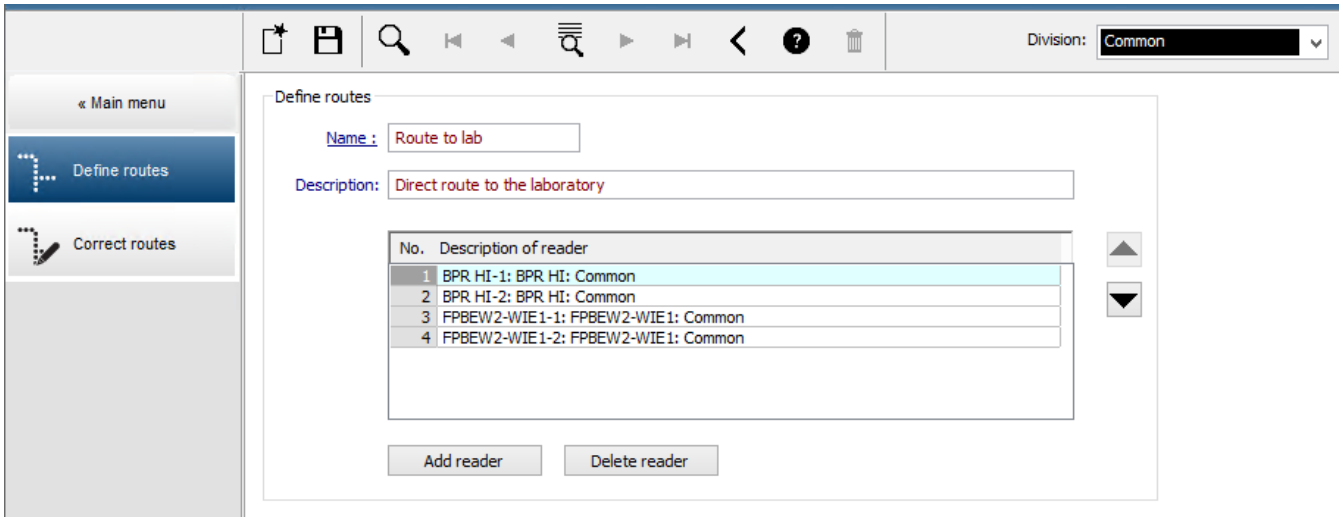
Einführung

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).

4. 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:

1. Klicken Sie im Hauptmenü auf **Personnel data** (Personaldaten) > **Cards** (Ausweise)
2. Laden Sie den Personendatensatz der zuzuweisenden Person
3. Aktivieren Sie auf der Registerkarte **Other data** (Weitere Daten) das Kontrollkästchen **Tour monitoring** (Wegekontrolle).
4. Wählen Sie in der Dropdown-Liste daneben einen definierten Weg aus (siehe vorherigen Abschnitt zum Definieren von Wächterrunden).
5. 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

1. Wählen Sie im Hauptmenü **Tour monitoring** (Wegekontrolle) > **Correct routes** (Wege korrigieren).
2. Laden Sie den Personaldatensatz der Person, die der Route zugeordnet ist.
3. Um diese Person auf der Route zu finden, klicken Sie auf die Schaltfläche **Determine location** (Position ermitteln).
4. Leser, die bereits angelaufen wurden, erhalten in der Liste ein grünes Häkchen ✔.
5. Um den Standort einer Person auf der Route zurückzusetzen oder zu korrigieren, klicken Sie auf die Schaltfläche **Set location** (Position setzen).

28 Zufällige Personenkontrolle

Prozess der Mitarbeiterauslosung

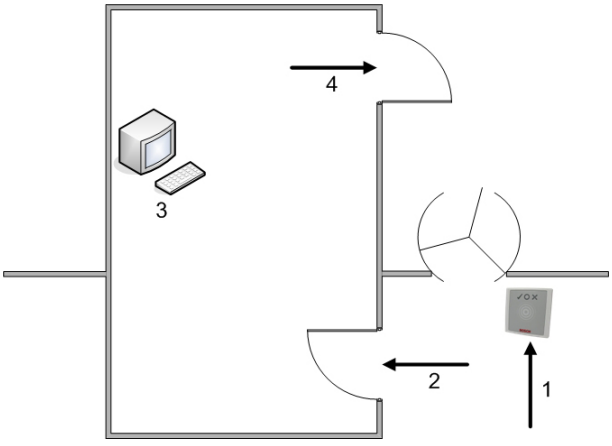
1. Ein Ausweisinhaber liest seinen Ausweis an einem Leser ein, der für die Mitarbeiterauslosung konfiguriert ist.
   Hinweis
   Nur Personen, die berechtigt sind, den Durchtritt in der definierten Richtung zu passieren, können zufällig ausgewählt werden. Da Berechtigungen vor der Mitarbeiterauslosung kontrolliert werden, werden nicht zutrittsberechtigte Personen sofort abgewiesen und nicht in den Auswahlprozess einbezogen.
2. Wenn der Zufallsgenerator diese Person zur Mitarbeiterauslosung wählt, wird ihr Ausweis für das gesamte System gesperrt.
   - Das Ereignis wird im Systemlogbuch aufgezeichnet.
   - An den Dialog **Blocking** (Sperrung) wird ein Eintrag mit unbegrenzter Dauer gesendet, der durch **Random screening** (Mitarbeiterauslosung) gekennzeichnet ist [Abbildung unten – Nummer 1].
   - In der Statusleiste des Dialogs „Personnel data“ (Personaldaten) werden die LEDs „Blocked“ (Gesperrt) (rot) mit dem Hinweis „Random screening“ (Mitarbeiterauslosung) (violett blinkend) angezeigt.

Hinweis!
Personen, für die der Parameter **Excluded from random screening** (Von MA-Auslosung ausgeschlossen) im Dialog **Cards** (Ausweise), Registerkarte **Other data** (Weitere Daten) gesetzt wurde, werden in den Auslosungsprozess 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 Mitarbeiterauslosung



1 = Ausweis einlesen – Auslosung – 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 x 1/10), dass zwei aufeinanderfolgende Personen ausgewählt werden.

29 Verwenden der Ereignisanzeige

Einführung

Mit der Ereignisanzeige können entsprechend autorisierte Bediener Ereignisse überprüfen, die vom System aufgezeichnet wurden, und Berichte erstellen: auf dem Bildschirm, gedruckt oder als *.CSV*-Dateien.

Um die gewünschten Datensätze aus der Logbuch-Datenbank abzurufen und anzuzeigen, legen Sie Filterkriterien fest und klicken Sie auf **Refresh** (Aktualisieren)  . Je nach Anzahl der angeforderten Daten kann dieser Vorgang einige Minuten dauern.

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)

29.1 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 **nicht**empfohlen, 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.

29.2 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 **nicht**empfohlen, 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.

29.3 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 **nicht**empfohlen, 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.

30 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.

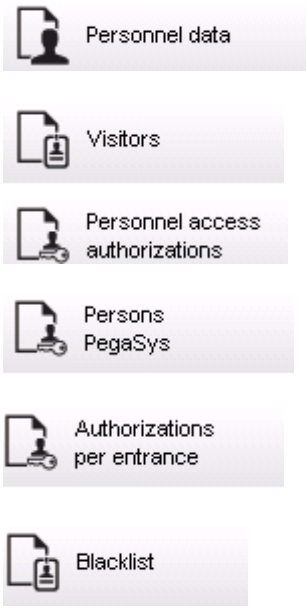
Die Vorschau hat eine eigene Symbolleiste:

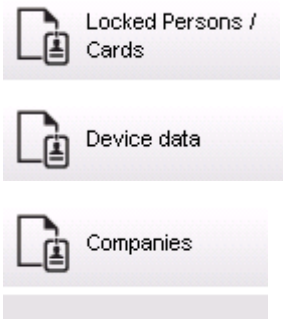
- Klicken Sie auf ✕, um die Vorschau ohne Drucken zu verlassen.
- Benutze die Pfeiltasten ◀| ◀ 2 of 17 ▶ |▶ in der Vorschau-Symbolleiste, um zwischen den Seiten hin- und herzublättern oder einzelne Seiten nach Seitenzahl auszuwählen.
- Klicken Sie auf  , um mit Ihrem Standarddrucker sofort zu drucken
- Klicken Sie auf  , um über einen Druckeinstellungen-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.

30.1 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.

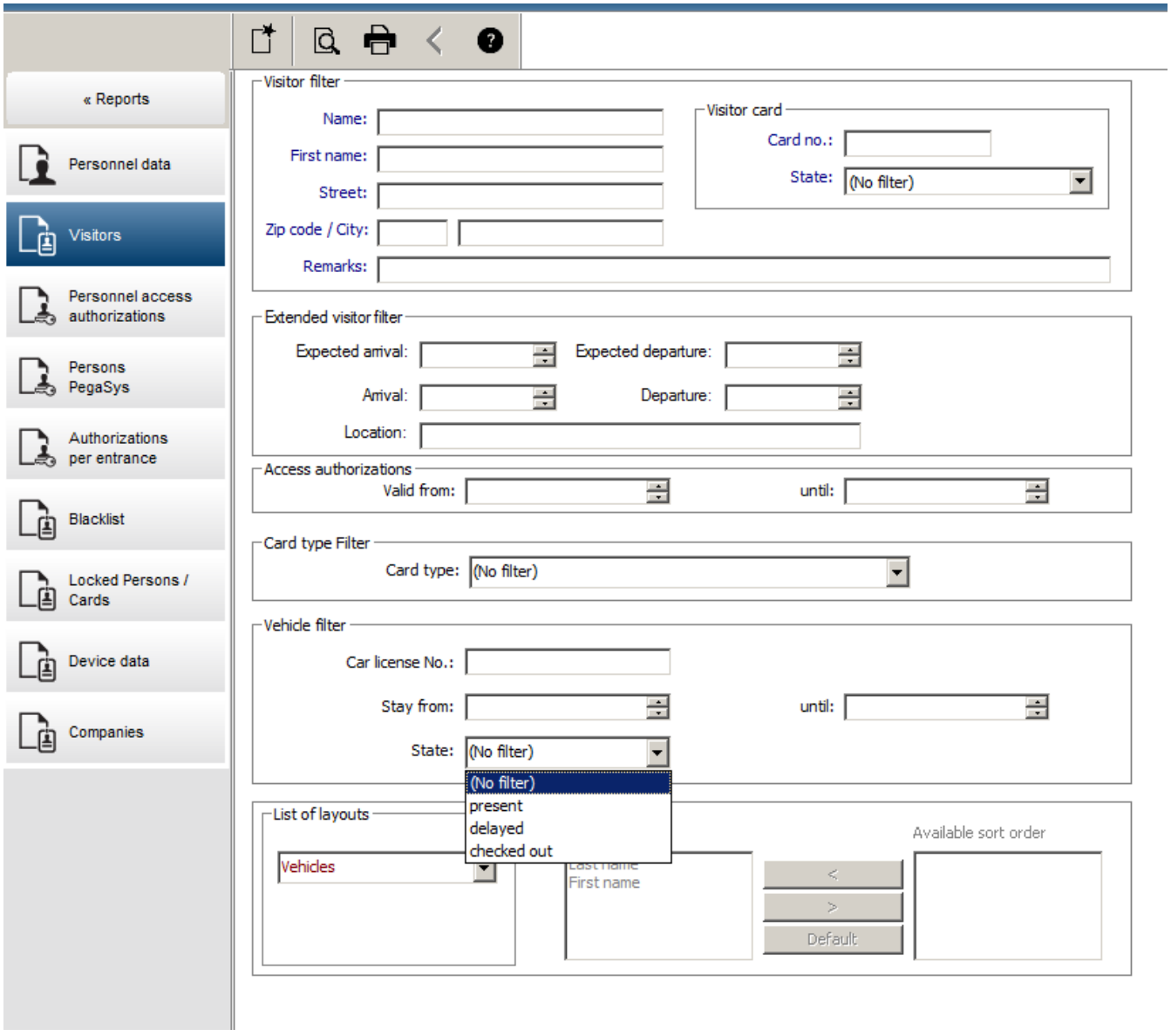
Bericht: Device Data (Gerätedaten)
Der Dialog kann verwendet werden, um Berichte basierend auf Gerätedaten zu erstellen, z. B. Gerätename oder Gerätetyp.

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.

30.1.1 Berichterstattung über Fahrzeuge

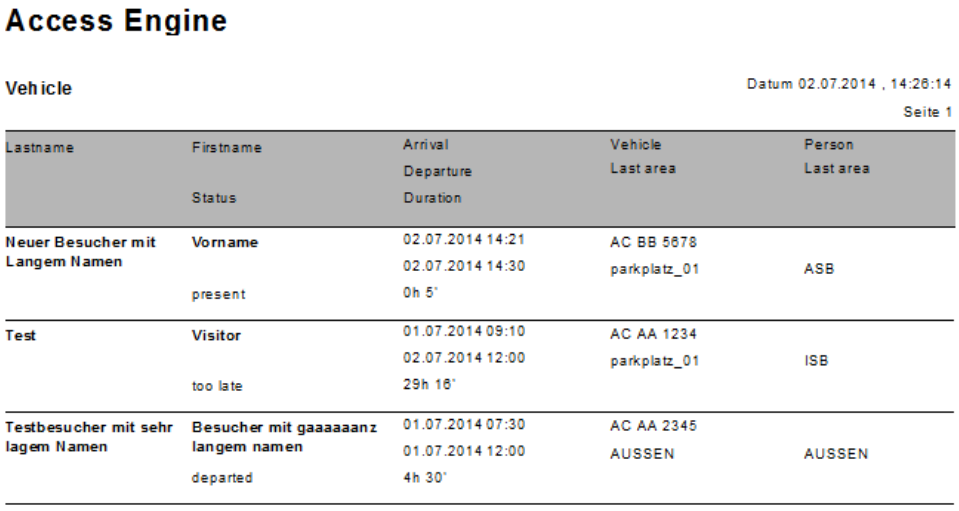
Im Dialog **Reports (Berichte)> Visitors (Besucher)** kann **Vehicles (Fahrzeuge)** von der Liste gewählt werden. Sobald **Vehicles (Fahrzeuge)**ausgewählt wurde, ist der **Vehicle filter (Fahrzeugfilter)** aktiviert und kann zum Filtern von Fahrzeugen und deren Status verwendet werden.
Die Statusinformationen 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

Vehicle

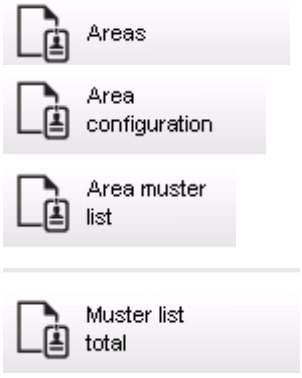
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

30.2 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.



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.

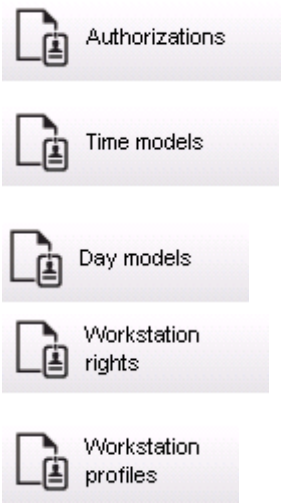
Bericht: Areas Configuration (Bereiche Konfiguration)
Definierte Bereiche und deren Unterbereiche mit einer Kennung für Parkplätze sowie Angabe der maximal erlaubten Anzahl von Personen oder Fahrzeugen in diesem Bereich.

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.

30.3 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.

31 Betriebs-Bedrohungsstufenverwaltung

In diesem Abschnitt werden die verschiedenen Möglichkeiten beschrieben, um eine Bedrohungsstufe auszulösen und abzubrechen. Hintergrundinformationen finden Sie im Abschnitt *Konfigurieren der Bedrohungsstufenverwaltung, Seite 138*

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 Hardwaresignal, jedoch nicht durch einen Alarmausweis abgebrochen werden können.

Siehe

- *Konfigurieren der Bedrohungsstufenverwaltung, Seite 138*

31.1 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.

31.2 Auslösen eines Bedrohungsalarms über Hardwaresignal

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.
– Hardwaresignale 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 Hardwareschalter, 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 Hardwaresignal, Seite 143*

31.3 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 Hardwareschalter ab. Grundsätzlich ist es nicht möglich, eine Bedrohungsstufe über einen Alarmausweis abzubrechen.

Siehe

– *Erstellen eines Alarmausweis, Seite 203*

32 Betrieb des Swipe-Tickers

Einführung
Swipe-Ticker ist ein Tool, das Bedienern der Kartenansicht hilft, in Echtzeit zu überwachen, wer die Räumlichkeiten betritt oder verlässt.

Übersicht
Swipe-Ticker ist eine Anwendung in der AMS Kartenansicht, die die letzten 10 Minuten der Zutrittsereignisse in einer dynamischen Bildlaufliste anzeigt. Es werden bis zu 50 Zutrittsereignisse angezeigt. Ereignisse, die älter als 10 Minuten sind, werden automatisch aus der Liste gelöscht. Der Bediener kann alle Lesegeräte im System überwachen oder eine Teilmenge auswählen.
Jeder Datensatz in der Liste enthält Details zum Ereignis und zu den verwendeten Ausweisen, z. B.:
- Der Name des Ausweisinhabers und sein gespeichertes Foto zur visuellen Bestätigung der Identität.
- Ein Zeitstempel.
- Firmen- und/oder Abteilungsname, falls gespeichert.
- Der Eingang und der Leser, an dem der Ausweis verwendet wurde.
- Eine Ereigniskategorie mit einem farbigen Etikett:
  - Grün: Ein abgeschlossener Zutritt mit einem gültigen Ausweis
  - Gelb: Ein unvollständiger Zutritt mit einem gültigen Ausweis, z. B. hat der Ausweisinhaber das Schloss geöffnet und geschlossen, aber die Tür nicht geöffnet.
  - Rot: Ein fehlgeschlagener Zutrittsversuch mit einem ungültigen Ausweis. Die Art der Ungültigkeit wird angezeigt. Beispiel: Der Ausweis ist auf der schwarzen Liste, unbekannt oder abgelaufen.

Swipe-Ticker hat keine eigenen Archive, sondern extrahiert und zeigt Zutrittsereignisse aus der Systemdatenbank an. Das dynamische Scrollen kann für eine genauere Untersuchung angehalten oder in einem separaten Fenster für die parallele Verwendung mit anderen Kartenansichtsanwendungen geöffnet werden.

Hinweis!
Latenz nach Bearbeitungen
Es dauert in der Regel einige Minuten, bis Änderungen an ID-Fotos in AMS an den Swipe-Ticker weitergeleitet werden.

Voraussetzungen
Das Benutzerprofil des Bedieners erfordert eine spezielle Autorisierung zum Ausführen des Swipe-Tickers.
1. Navigieren Sie in der AMS-Hauptanwendung zum Menü: **Configuration** (Konfiguration) > **User profiles** (Benutzerprofile)
2. Laden sie den Profilnamen des gewünschten Bedieners
3. Wählen Sie in der Tabelle **Access Manager Maps** (Access Manager-Karten) > **Special functions** (Besondere Funktionen) > Swipe ticker **(Swipe-Ticker)**.

Starten des Swipe-Tickers

- Klicken Sie in der Kartenansicht auf  , um das Tool zu starten.

Auswählen von zu überwachenden Lesern

Wenn noch keine Leser ausgewählt wurden oder wenn Sie die Auswahl ändern möchten, gehen Sie wie folgt vor:

1. Klicken Sie im Swipe-Ticker-Fenster auf  (Einstellungen).
   Das Fenster **Filter devices** (Geräte filtern) wird geöffnet.
2. Aktivieren Sie im Gerätebaum die Kontrollkästchen der Eingänge oder Leser, die Sie überwachen möchten. Die Kontrollkästchen verhalten sich wie folgt:
   Wenn Sie einen Eingang auswählen, werden standardmäßig alle untergeordneten Geräte ausgewählt.
   Die Kontrollkästchen einzelner untergeordneter Geräte können dann bei Bedarf abgewählt werden.
   Wenn **alle** untergeordneten Elemente eines übergeordneten Geräts ausgewählt sind, ist das Kontrollkästchen des übergeordneten Elements weiß. Wenn nur **einige** ausgewählt sind, ist das Kontrollkästchen des übergeordneten Elements grau.
3. Klicken Sie auf **OK**, um die Auswahl der Leser abzuschließen und das Fenster **Filter devices** (Geräte filtern) zu schließen.

Anzeigen ausgewählter Leser auf der Karte

- Doppelklicken Sie im Swipe-Ticker auf einen Datensatz.

✓ Der Swipe-Ticker wird automatisch angehalten.

✓ In der Kartenansicht wird im Hauptfenster die erste relevante Kartenszene in der Kartenhierarchie angezeigt und der Leser hervorgehoben, auf den Sie doppelgeklickt haben.

Anhalten des Swipe-Tickers

- Klicken Sie im Swipe-Ticker-Fenster auf  , oder doppelklicken Sie auf einen Datensatz in der Liste, um die dynamische Anzeige anzuhalten.

✓ Die dynamische Anzeige wird „eingefroren“. Eingehende Ereignisdatensätze werden gepuffert, aber nicht angezeigt.

✓ Oben in der Liste wird darauf hingewiesen, dass der Ereignisstream angehalten wurde.

Fortsetzen eines angehaltenen Swipe-Tickers

- Klicken Sie im Swipe-Ticker-Fenster auf  , um die dynamische Anzeige fortzusetzen.

✓ Die dynamische Liste zeigt in chronologischer Reihenfolge (neueste erste) alle Zutrittsereignisse an, die in den letzten 10 Minuten bei den ausgewählten Lesern aufgetreten sind (maximal 50).

✓ Zutrittsereignisse, die älter als die 50 neuesten oder älter als 10 Minuten sind, werden aus der Liste entfernt.

✓ Neue Zutrittsereignisse werden wieder in Echtzeit angezeigt, sobald sie auftreten.

Duplizieren des Swipe-Tickers in einem separaten Fenster

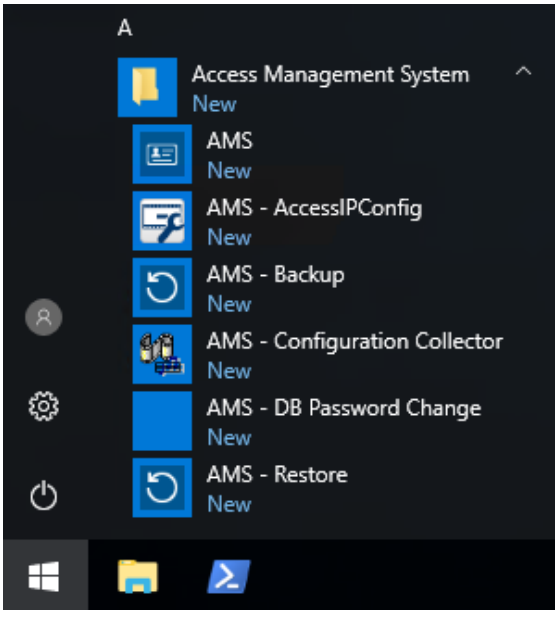
Beachten Sie, dass jeweils nur ein doppeltes Ticker-Fenster geöffnet werden kann.

1. Klicken Sie im Swipe-Ticker-Fenster auf  (zusätzliches Fenster).
   Das separate Fenster ist ein Duplikat und **nicht** unabhängig vom Ticker im Hauptfenster. Es hat die gleichen Einstellungen.
   Andere Kartenansichtsanwendungen, wie z. B. die Alarmliste, können nun parallel im Hauptfenster ausgeführt werden.
2. Wenn Sie mit der Bearbeitung im separaten Fenster fertig sind, schließen Sie es über die Titelleiste.

33 Backup und Wiederherstellung

Mit der Funktion **Backup and Restore** (Sichern und Wiederherstellen) können Sie Ihr System mit seinen Daten in eine neue Version von AMS oder auf einen neuen Computer verschieben. **Backup and Restore** (Sichern und Wiederherstellen) kann nur auf dem Rechner ausgeführt werden, auf dem der AMS-Server installiert ist. Im Startmenü von Windows sind zwei Verknüpfungen verfügbar:

- **AMS - Backup** (AMS - Sichern) zum Erstellen einer Sicherung
- **AMS - Restore** (AMS - Wiederherstellen) zum Wiederherstellen einer Sicherung:

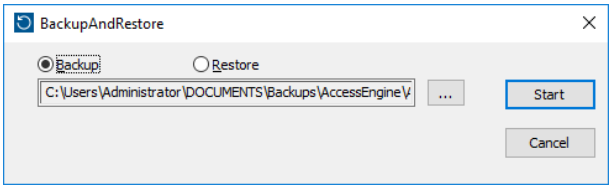


33.1 Sichern des Systems

In diesem Abschnitt wird beschrieben, wie Sie eine Sicherung der AMS-Anwendung erstellen und die Sicherungsdateien von SQL Server finden.

Erstellen einer Sicherung der AMS-Anwendung

1. Klicken Sie im Startmenü von Windows mit der rechten Maustaste auf **AMS - Backup** (AMS - Sichern) und wählen Sie **Als Administrator ausführen** aus.
   - Das Tool **Backup and Restore** (Sichern und Wiederherstellen) beginnt mit der vorausgewählten Option **Backup** (Sichern).



2. Geben Sie einen Pfad ein, unter dem die *.GZ*-Datei gespeichert werden soll.
3. Klicken Sie auf **Start** (Starten), um die Sicherung zu starten.
   - Das Tool **Backup and Restore** (Sichern und Wiederherstellen) erstellt eine einzelne *.GZ*-Datei und zeigt den Fortschritt in einem Popup-Fenster an.
4. Kopieren Sie diese Datei an einen sicheren Speicherort auf einem anderen Computer. Für hohe Datensicherheit dürfen Sie die einzige Kopie **nicht** auf dem DMS-Server speichern.

Finden und kopieren Sie die SQL Server-Sicherungsdateien.

1. Navigieren Sie mit einem Datei-Explorer auf dem AMS-Servercomputer zu dem Speicherort, an dem SQL Server die *.BAK*-Dateien speichert.
   - Der Dateipfad ist wie folgt, wobei *<version>* und *<instance name>* Variablen sind, die von Ihrem System abhängen:
     C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup
   - Die Dateinamen liegen in dieser Form vor:
     acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
     Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
     Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
     Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
     Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
     Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
2. Kopieren Sie **alle** *.BAK*-Dateien an einen sicheren Speicherort auf einem anderen Computer. Für hohe Datensicherheit dürfen Sie die Kopien **nicht** auf dem DMS-Server speichern.

Hinweis!
Der Standardpfad zum AMS-Logbuch ist:
C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog

33.2 Wiederherstellen einer Sicherung

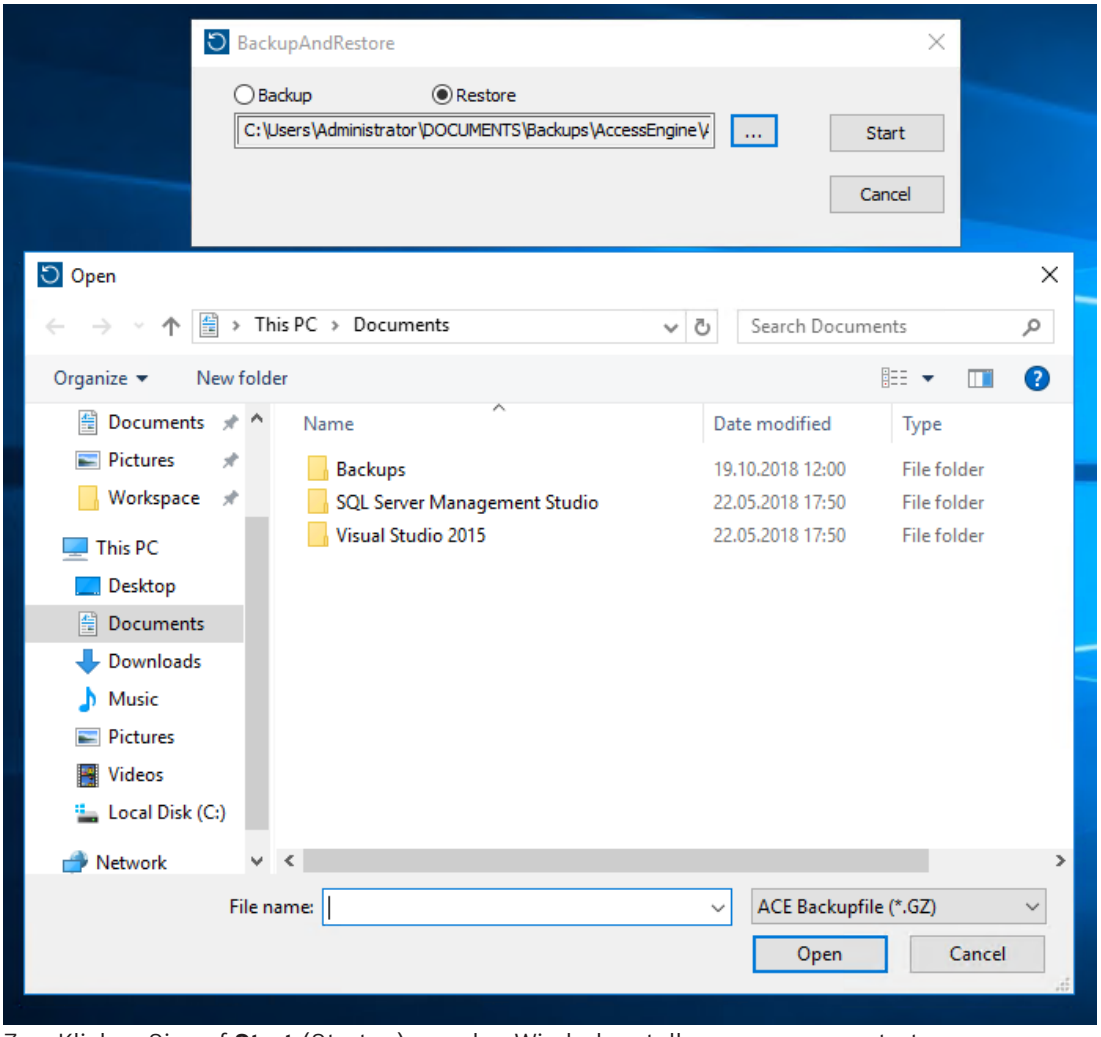
Voraussetzungen

- die *GZ*-Datei, die vom Tool **Backup and Restore** (Sichern und Wiederherstellen) erstellt wurde
- die von SQL Server erstellten *.BAK*-Dateien, die Sie bei der Sicherung gespeichert haben
- ein SQL-Konto mit **sysadmin**-Rechten, wie *sa*
- Ein entsprechend vorbereiteter Zielcomputer im Hinblick auf **Lizenzen** und **Zertifikate**:
  - **Lizenzen**: Der Zielcomputer (auf dem Sie die Sicherung wiederherstellen) erfordert Lizenzen, die mindestens gleichwertig mit denen des Computers sind, auf dem Sie die Sicherung vorgenommen haben.
  - **Zertifikate**: Alle Clients des Zielcomputers benötigen die neuen Zertifikate, die von der Installation auf dem Zielcomputer generiert werden, nicht die von der Installation auf dem ursprünglichen Computer generierten Zertifikate.
    Informationen zur Generierung und Installation von Clientzertifikaten finden Sie im **AMS-Installationshandbuch**.

Vorgehensweise

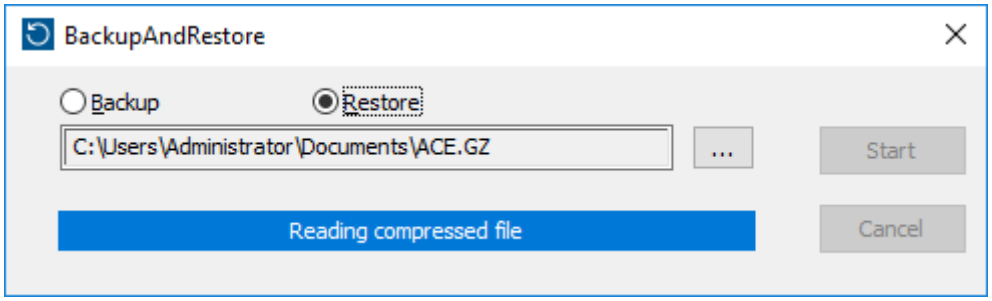
1. Klicken Sie im AMS-Programm auf **File** > **Exit** (Datei > Beenden), um die AMS-Anwendung zu schließen.
2. Wenn das Programm beendet wurde, führen Sie die Windows **Dienste**-Anwendung aus und stellen Sie sicher, dass alle *Access Engine*- und *Access Management System*-Dienste gestoppt wurden. Andernfalls beenden Sie die Dienste hier.
3. Wenn Sie einen RMAC (Redundant Failover MAC) mit Ihrem Haupt- oder 1. MAC ausführen, **dann und nur dann** wechseln Sie zum nächsten Unterkapitel und führen Sie das dort beschriebene Verfahren aus, bevor Sie zu diesem Schritt zurückkehren.

4. Kopieren Sie die MSSQL *.BAK*-Dateien, die Sie vom ursprünglichen Computer gespeichert haben, an den identischen Speicherort auf dem neuen Computer.
   – Der Dateipfad ist wie folgt, wobei *<version>* und *<instance name>* Variablen sind, die von Ihrem System abhängen:
   C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup
5. Klicken Sie im Startmenü von Windows mit der rechten Maustaste auf **AMS - Restore** (AMS - Wiederherstellen) und wählen Sie **Als Administrator ausführen** aus.
   – Das Tool **Backup and Restore** (Sichern und Wiederherstellen) beginnt mit der vorausgewählten Option **Restore** (Wiederherstellen).
6. Klicken Sie auf die Schaltfläche **[...]**, um die *GZ*-Sicherungsdatei im Dateisystem zu finden und klicken Sie auf **Open** (Öffnen), um sie auszuwählen.



7. Klicken Sie auf **Start** (Starten), um den Wiederherstellungsprozess zu starten.
8. Geben Sie bei Aufforderung zur Eingabe von Serveranmeldeinformationen nicht die Anmeldeinformationen des Servercomputers, sondern „MSSQL sysadmin“-Anmeldeinformationen wie z. B. *sa* ein.

– Der Wiederherstellungsvorgang beginnt.



9. Wenn der Wiederherstellungsvorgang abgeschlossen ist, führen Sie die Windows **Dienste**-Anwendung aus und starten Sie alle *Access Engine*- und *Access Management System*-Dienste manuell neu.
10. Führen Sie das Server-Setup-Programm *AMS Server Setup.exe* als Administrator aus, um die gesicherten Daten mit den aktuellen Systemdaten neu zu synchronisieren.

Siehe

– *Sichern des Systems, Seite 246*

33.2.1 Wiederherstellen von RMACs in einer neuen Installation

Hinweis: Diese Vorgehensweise ist nur relevant, falls Sie die Sicherung eines Systems mit MACs und RMACs auf unterschiedlicher Hardware wiederherstellen.

Einführung

Wenn Sie eine Sicherung auf neuen Computern wiederherstellen, müssen Sie die IP-Adressen des MAC und RMAC, die in der Sicherungsdatei gespeichert wurden, zunächst zu den IP-Adressen der neuen Hardware konfigurieren. Führen Sie diese Konfiguration durch Ausführen des MACInstaller-Tools auf der neuen Hardware aus.

Das MACInstaller-Tool befindet sich auf dem Installationsmedium unter: *\AddOns\MultiMAC\MACInstaller.exe*

Weitere Informationen zur Verwendung des MACInstaller-Tools finden Sie im Kapitel *Verwenden des MACInstaller-Tools, Seite 55*.

Vorgehensweise

1. Führen Sie das MACInstaller-Tool auf dem Computer aus, auf dem der 1. MAC läuft. Dieser Computer kann der DMS-Server oder ein dedizierter Server für den 1. MAC sein.
   – Legen Sie im Tool die neuen IP-Adressen des primären MAC (dieser Computer) und des RMAC fest.
2. Führen Sie das MACInstaller-Tool auf dem Computer aus, auf dem der RMAC läuft.
   – Legen Sie im Tool die neuen IP-Adressen des primären MAC und des RMAC (dieser Computer) fest.
3. Kehren Sie zu dem Schritt zurück, an dem Sie den **Wiederherstellungsvorgang** unterbrochen haben.

Siehe

– *Verwenden des MACInstaller-Tools, Seite 55*

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.

ACS

Allgemeiner Begriff für ein Bosch Zutrittskontrollsystem, z. B. AMS (Access Management System) oder ACE (BIS Access Engine).

AMC-Hardwareschlüssel

Ein interner Authentifizierungscode, den der AMC aus bestimmten Hardwareparametern erzeugt. Er wird Benutzern nicht angezeigt.

Area (Arming) (Bereich (Scharfschalten))

Eine Gruppe von Durchtritten des Durchtrittsmodell 14 in einem Zutrittskontrollsystem. Die Scharfschaltung oder Unscharfschaltung der Einbruchmeldeanlage an einem dieser Durchtritte hat gleichzeitig an allen Durchtritten denselben Effekt, wenn der Parameter „Arming area“ (Scharfschaltebereich) dieselbe einstellige Bezeichnung hat.

Aufzugsgruppe

Eine Gruppe von Aufzügen, die dieselben Etagen gemeinsam bedienen. Jede Aufzugsgruppe wird von einem Destination Entry Server (DES) gesteuert.

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 Hardwaresignal (z. B. Drucktaste) oder durch Vorzeigen eines speziellen Bedrohungsalarmausweises an einem beliebigen Ausweisleser.

Betriebsmodus

Der Zustand eines Zutrittskontrollgeräts im Geräteeditor, während es auf Befehle reagiert, die von außerhalb des Geräteeditors erteilt werden. Änderungen der Konfiguration werden erst wirksam, nachdem der Betriebsmodus beendet und der Konfigurationsmodus wiederhergestellt wurde.

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 im System. Der DMS liefert Daten an MACs (Main Access Controller), die wiederum Daten an lokale Zutrittskontrollzentralen (i. d. R. AMC) liefern.

DCP

Ein Passwort, mit dem das Zutrittskontrollsystem einen Masterschlüssel generiert, der zur Verschlüsselung der Netzwerkkommunikation mit allen untergeordneten lokalen Zutrittscontrollern (normalerweise AMC-Geräte) verwendet wird.

Destination Dispatching System (DDS)

Auch als Zielwahlsteuerungssystem bezeichnet, aber es wird nur die Abkürzung DDS verwendet. Otis CompassPlus ist eine Art DDS.

Destination Entry Redirector (DER)

Ein Computer auf derselben Ebene wie ein Destination Entry Server (DES) in einem Otis CompassPlus-System. Er ist mit allen Aufzugsgruppen verbunden und verbessert die Effizienz der DES-Geräte.

Destination Entry Server (DES)

Ein Computer, der eine Aufzugsgruppe steuert, um die Fahrtzeiten zu optimieren.

Destination Entry Terminal (DET)

Ein Gerät, mit dem Aufzugfahrgäste Zielanfragen für eine Aufzugsgruppe eingeben können.

DSN

Datenquellenname. Der Name einer Datenquelle in Open Database Connectivity (ODBC).

DTLS

Datagram Transport Layer Security ist ein sicheres Kommunikationsprotokoll, das vor Lauschangriffen und Sabotage schützt.

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.

IPConfig-Tool

Ein separates Hilfsprogramm zur Konfiguration der Netzwerk- und Netzwerksicherheitseinstellungen von Hardwarekomponenten im Zutrittskontrollsystem.

Konfigurationsmodus

Der Standardzustand von Zutrittskontrollgeräten im Geräteeditor. Änderungen werden sofort wirksam und an untergeordnete Geräte weitergegeben.

Lokale Zutrittssteuerung (Local Acess Controller, LAC)

Ein Hardwaregerät, das Zutrittsbefehle an die periphere Zutrittskontrollhardware, wie z. B. Leser und Schlösser, sendet und Anforderungen von dieser Hardware für das gesamte Zutrittskontrollsystem verarbeitet. Der häufigste LAC ist ein Access Modular Controller oder AMC.

MAC (Master 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.

Masterschlüssel

Ein Code, den das System aus dem DCP (Gerätekommunikationspasswort) erzeugt und der zum Schutz der Zutrittskontrollgeräte verwendet wird. Der Masterschlüssel wird keinem Benutzer jemals angezeigt.

Normalmodus

Im Gegensatz zum Büromodus gewährt der Normalmodus nur den Zutritt für Personen, die einen gültigen Ausweis am Leser vorzeigen.

Passwort-Entropie

Eine Messung der Passwortstärke, die aus Faktoren wie Zufälligkeit, Anzahl der verfügbaren Symbole und tatsächlicher Anzahl der verwendeten Symbole berechnet wird.

Point (Melder)

Ein Melder zur Erkennung von Einbrüchen in einem Einbruchmeldebereich. In einigen Kontexten können Melder auch als Meldegruppen bezeichnet werden.

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.

RPS

Remote Programming Software. Ein Programm, das Brand- oder Einbruchmeldezentralen in einem Netzwerk verwaltet.

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 Durchtritten 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.

Zufälliger LCD-Schlüssel

Ein temporärer alphanumerischer Code, den der AMC bei jedem Bootvorgang neu erzeugt. Der Schlüssel kann im LC-Display des AMC angezeigt und von Softwaretools zur Authentifizierung der Netzwerkkommunikation angefordert werden.

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.

Zutrittswiederholsperre

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 Zutrittswiederholsperre 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
Niederlande
www.bosch-sicherheitssysteme.de

Building solutions for a better life.

202112171439