Access Professional Edition

de Konfigurationshandbuch

Inhaltsverzeichnis

1 Übersicht

1.1 Modulares Design

Das Access Professional Edition System (im Folgenden als **Access PE** bezeichnet) bietet eigenständige Zutrittskontrolle für kleine und mittelgroße Unternehmen. Es besteht aus mehreren Modulen:

- LAC-Service: ein Prozess, der ständig mit den lokalen Zutrittscontrollern (Local Access Controller, LAC – im Folgenden als Controller bezeichnet) kommuniziert. Als Controller werden AMCs (Access Modular Controller) verwendet.
- Konfigurator
- Personalverwaltung
- Log-Viewer
- Alarmmanagement
- Videoverifikation

1.2 Server- und Client-Module

Die Module werden in Server- und Client-Module aufgeteilt.
Der LAC-Service muss sich in ständigem Kontakt mit den Controllern befinden, da er erstens von ihnen ständig Nachrichten über Bewegungen sowie An- und Abwesenheit von Ausweisinhabern erhält, zweitens Datenänderungen, z. B. die Zuweisung neuer Ausweise, an die Controller überträgt, aber vor allem deshalb, weil er Prüfungen auf Metaebene durchführt (Zutrittsfolgekontrollen, Zutrittswiederholkontrollen, Mitarbeiterauslosung).
Der Konfigurator sollte ebenfalls auf dem Server ausgeführt werden; allerdings lässt er sich auch auf Client-Bedienplätzen installieren und kann von dort aus betrieben werden.
Die Module Personalverwaltung und Log-Viewer gehören zur Client-Komponente und können zusätzlich auf dem Server oder auf einem anderen PC mit einer Netzwerkverbindung zum Server ausgeführt werden.
Die folgenden Controller können verwendet werden:

- AMC2 4W (mit vier Wiegand-Leserschnittstellen) – kann durch das AMC2 4W-EXT erweitert werden
- AMC2 4R4 (mit vier RS485-Leserschnittstellen)

2 Allgemein

2.1 Einführung

Access PE ist ein Zutrittskontrollsystem, das gezielt für die Überwachung kleiner und mittlerer Objekte mit höchsten Anforderungen an Sicherheit und Flexibilität entworfen wurde.
Seine hohe Ausfallsicherheit und Erweiterungsfähigkeit verdankt Access PE einem 3-Ebenen-Konzept: **Die oberste Ebene** ist die Verwaltungsebene mit den Kontrolldiensten. Hier werden alle administrativen Aufgaben ausgeführt, z. B. die Registrierung neuer Ausweise und die Vergabe von Zutrittsrechten.
Die zweite Ebene besteht aus den lokalen Zutrittscontrollern (LACs) zur Steuerung der einzelnen Gruppen von Türen oder Durchtritten. Selbst wenn das System offline ist, kann ein LAC selbstständig Zutrittskontrollentscheidungen treffen. LACs sind für die Kontrolle der Durchtritte verantwortlich, überwachen Türöffnungszeiten oder fragen PINs an kritischen Zutrittspunkten ab.
Die dritte Ebene besteht aus Kartenlesern.
Die Kommunikation zwischen Client, Server und Ausweisinhabern ist AES-verschlüsselt.
Die Multibenutzerversion von Access PE bietet die Möglichkeit, das System von verschiedenen Arbeitsplätzen aus zu steuern. Frei definierbare Stufen für Benutzerrechte regeln den Zutritt und gewährleisten die Sicherheit. So ist es z. B. möglich, an einem Arbeitsplatz die Ausweisdaten zu verwalten und an einem anderen Arbeitsplatz zu überprüfen, ob ein bestimmter Mitarbeiter gerade im Haus anwesend ist.
Access PE erlaubt eine außerordentlich flexible Konfiguration von Zutrittsrechten, Zeitmodellen und Durchtrittsparametern. Die folgende Aufstellung gibt einen Überblick über die wichtigsten Funktionen:

Schnelle und einfache Ausweiszuweisung

Die Zuweisung von (bis zu drei) Ausweisen zu einer Person erfolgt entweder manuell oder über einen Dialogleser, der über eine serielle Schnittstelle an einen PC angeschlossen ist. Alle zugewiesenen Ausweise sind aktiv. Bei einer Aktualisierung des Ausweises wird der alte Ausweis automatisch überschrieben und verliert seine Gültigkeit. Dadurch wird verhindert, dass alte Ausweise, die versehentlich nicht gesperrt wurden oder nicht gesperrt werden konnten, weiterhin zum Zutritt verwendet werden können.

Zutrittsrechte (einschließlich Gruppenberechtigungen)

Einer Person können sowohl Gruppenberechtigungen als auch Einzelberechtigungen zugewiesen werden. Die Gültigkeit der Berechtigungen kann nach Raumzonen und Zeit minutengenau eingeschränkt werden. Mit Gruppenberechtigungen können Zutrittsrechte für einzelne oder alle Ausweisinhaber gleichzeitig erteilt und eingeschränkt werden. Zusätzlich können Gruppenberechtigungen mit einem Zeitmodell verknüpft werden, welches den Zutritt auf bestimmte Tageszeiten einschränkt.

Zutrittsfolgekontrolle

Durch die Definition von Raumzonen ist es möglich, eine korrekte Zutrittsfolge zu überwachen und umzusetzen. Selbst ohne Überwachung kann über diese Konfiguration der Aufenthaltsort eines Ausweisinhabers angezeigt werden.

Zutrittswiederholsperre

Wenn ein Ausweis gelesen wurde, kann dieser gesperrt werden, sodass er für einen definierten Zeitraum nicht mehr zum Begehen des betreffenden Zutrittspunktes verwendet werden kann. Dadurch wird verhindert, dass ein Benutzer seinen Ausweis nach dem Passieren einer Schranke einer anderen Person überreicht und dieser einen unberechtigten Zutritt ermöglicht.

Automatische Sperrung von Ausweisen nach Ablauf der Gültigkeit

Besucher oder temporäre Mitarbeitern benötigen häufig nur für einen begrenzten Zeitraum Zutritt.
Es ist möglich, Ausweise nur für einen bestimmten Zeitraum auszustellen, sodass diese nach Ablauf dieser Frist automatisch ihre Gültigkeit verlieren.

Zeitmodelle und Tagesmodelle
Jedem Ausweisinhaber können bestimmte Zeitmodelle zugeordnet werden, die festlegen, zu welchen Zeiträumen der Zutritt für die betreffende Person zulässig ist. Zeitmodelle können flexibel mithilfe von Tagesmodellen definiert werden. Diese legen fest, inwieweit bestimmte Wochentage, Wochenenden, Feier- und Sondertage von normalen Arbeitstagen abweichen.

Identifikation über PIN-Code
Anstelle eines Ausweises kann einer Person der Zutritt auch nach Eingabe eines speziellen PIN-Codes gewährt werden.

Verifikation über PIN-Code
Für besonders sensible Bereiche kann die Eingabe zusätzlich erforderlicher PIN-Codes parametriert werden. Dieser Schutz kann mit Zeitmodellen kombiniert werden, wenn z. B. die zusätzliche Eingabe eines PIN-Codes nur außerhalb bestimmter Arbeitszeiten oder an freien Tagen gefordert ist.

Flexible Zutrittsverwaltung
Die flexible Parametrierung der einzelnen Türmodelle gestattet eine optimale Balance zwischen Sicherheit und Komfort. Für jeden Durchtritt kann separat festgelegt werden, wie lange er ohne Alarmmeldung in geöffnetem Zustand verbleiben darf. In Kombination mit einer Alarmanlage kann der Zutrittspunkt dann optional verriegelt werden.

Dauerfreigabe von Türen
Zur Erleichterung des Zutritts können Türalarme unterdrückt werden, um Türen für einen bestimmten Zeitraum freizugeben. Diese Freigabezeiträume können entweder manuell definiert oder mithilfe eines Zeitmodells automatisch gesteuert werden.

Zeit und Anwesenheit
Zutrittspunkte können so parametriert werden, dass Ein- und Ausgänge zur Buchung von Zeit und Anwesenheit erfasst werden.

Ausweiserstellung
Das grafische Zusatzmodul **Card Personalization** (CP) ist vollständig in das Zutrittskontrollsystem integriert. Damit ist bei der Ausweiserstellung kein Wechsel zwischen verschiedenen Anwendungsprogrammen erforderlich.

Zuweisung von Fotos
Ist das Zusatzmodul **Card Personalization** (CP) nicht aktiviert, kann die Fotoidentifikation einer Person trotzdem importiert und dem Ausweisinhaber zugeordnet werden.

Offline Locking System
Werden bestimmte Anlagenbereiche vom hoch verfügbaren Zutrittskontrollsystem – egal aus welchen Gründen – nicht online überwacht, können diese trotzdem offline gesichert werden.

Verwaltung von Videogeräten
Durchtritte können zusätzlich mit Kameras ausgerüstet werden, mit denen die Identität einer Person festgestellt und deren Bewegungen verfolgt werden können.

2.2 Benutzeranmeldung

Die folgenden Anwendungen sind verfügbar. Weitere Informationen finden Sie in den entsprechenden Benutzerhandbüchern:

Personalverwaltung

Konfigurator

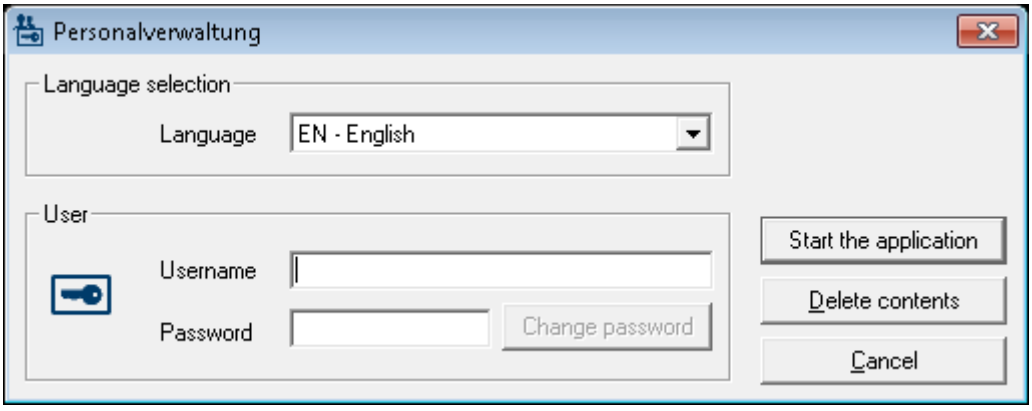
Log-Viewer

Lageplan-Anzeige und Alarmmanagement

Videoverifikation

Hinweis!
Eine Anmeldung vom Client ist nur möglich, wenn der LAC-Service auf dem Server ausgeführt wird.

Client-Anmeldung
Die Anwendungen des Systems sind vor unbefugter Verwendung geschützt. Die **Standardzugangsdaten** für die erste Verwendung sind:
– Benutzername: **bosch**
– Kennwort: **bosch**



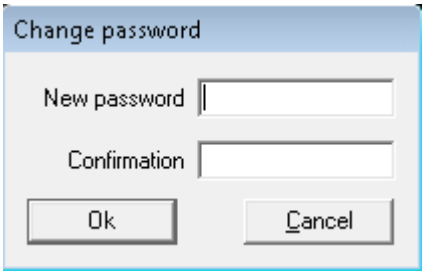
Nachdem Benutzername und Kennwort eingegeben wurden, wird die Schaltfläche **Kennwort ändern** aktiv.
Nach 3 fehlgeschlagenen Anmeldeversuchen muss eine bestimmte Wartezeit bis zum nächsten Anmeldeversuch verstreichen. Dies gilt für die Schaltflächen „Anwendung starten” und „Kennwort ändern”.
In der oberen Dropdown-Liste kann die gewünschte **Sprache** für die Interaktion ausgewählt werden. Standardmäßig ist die Sprache ausgewählt, die bei der Installation der Anwendung verwendet wurde. Bei einem Benutzerwechsel ohne Neustart der Anwendung bleibt die zuletzt ausgewählte Sprache erhalten. Aus diesem Grund kann ein Dialogfeld in einer unerwünschten Sprache erscheinen. Melden Sie sich erneut bei Access PE an, damit die gewünschte Sprache angezeigt wird.

Anwendungen von Access PE können in den folgenden Sprachen ausgeführt werden:

- Englisch
- Deutsch
- Französisch
- Japanisch
- Russisch
- Polnisch
- Chinesisch (VRC)
- Niederländisch
- Spanisch
- Portugiesisch (Brasilien)

Hinweis!
Alle Einrichtungen, wie Gerätenamen, Bezeichnungen, Modelle und Schemata für Benutzerrechte, werden in der Sprache angezeigt, in der sie eingegeben wurden. Entsprechend werden Schaltflächen und Bezeichnungen, die über das Betriebssystem gesteuert werden, möglicherweise in der Sprache angezeigt, in der das Betriebssystem installiert wurde.

Geben Sie nach einem Klick auf die Schaltfläche **Kennwort ändern** einen neuen Benutzernamen und ein neues Kennwort in diesem Dialog ein:



Hinweis!
Vergessen Sie nicht, das Kennwort zu ändern!

Über die Schaltfläche **Anwendung starten** werden die Benutzerberechtigungen geprüft, und die Anwendung wird ggf. gestartet. Ist das System nicht in der Lage, die Anmeldung zu authentifizieren, wird die folgende Fehlermeldung angezeigt: **Benutzername oder Kennwort nicht korrekt!**

2.3 Symbolleiste der Konfigurators

Die folgenden Funktionen können über die Menüs, die Symbole in der Symbolleiste oder über bestimmte Tastatur-Kurzbefehle aufgerufen werden.

Funktion	**Symbol/ Kurzbefehl**	**Beschreibung**
Menü **Datei**		
Neu	 Strg + N	Löscht alle Konfigurationsdialogfelder (außer für Standardeinstellungen), damit eine neue Konfiguration konfiguriert werden kann.
Öffnen ...	 Strg + O	Öffnet ein Dialogfeld, um eine andere Konfiguration auszuwählen, die geladen werden soll.
Speichern	 Strg + S	Speichert die Änderungen in der aktuellen Konfigurationsdatei.
Speichern unter ...		Speichert die aktuelle Konfiguration in einer neuen Datei.
Konfiguration aktivieren		Aktiviert eine geladene Konfiguration und speichert die bisher gültige Konfiguration.
Konfiguration an LAC senden		Übernimmt die gespeicherten Konfigurationsänderungen für den LAC-Service.
Zuletzt gültige Konfigurationen aufführen		Öffnet Konfigurationen direkt ohne den Umweg über den Auswahldialog der Funktion **Öffnen**.
Verlassen		Beendet den Access PE Konfigurator.
Menü **Ansicht**		
Symbolleiste		Schaltet die Anzeige der Symbolleiste ein/aus (Standardwert = ein).

Funktion	Symbol/ Kurzbefehl	Beschreibung
Statusleiste		Schaltet die Anzeige der Statusleiste am unteren Bildschirmrand ein/aus (Standardwert = ein).

Menü **Konfiguration**		
Allgemein		Öffnet das Dialogfenster **Allgemeine Einstellungen** zum Einrichten der Controller und allgemeinen Systemparameter.
Eingangssignale		Öffnet das Dialogfeld für die Parametrierung der **Eingangs**signale.
Ausgangssignale		Öffnet das Dialogfeld für die Parametrierung der **Ausgangs**signale.
Durchtritte		Öffnet das Dialogfenster **Durchtritte** für die Parametrierung von Türen und Kartenlesern.
Raumzonen		Öffnet das Dialogfenster **Raumzonenkonfiguration** zur Aufteilung der geschützten Anlage in virtuelle Bereiche.
Feiertage		Öffnet das Dialogfeld **Feiertage** zur Definition von Feier- und Sondertagen.
Tagesmodelle		Öffnet das Dialogfeld **Tagesmodelle** zur Definition von Zeiträumen am Tag, während derer die Zutrittsfunktionen aktiviert werden.
Zeitmodelle		Öffnet das Dialogfenster **Zeitmodelle** zur Definition von Zeitzonen auf der Grundlage von bestimmten Wochen- oder Kalendertagen.
Personalgruppen		Öffnet das Dialogfeld **Personalgruppen** zur Aufteilung des Personals in logische Gruppen.

Zutrittsberechtigungsgruppen		Öffnet das Dialogfeld **Zutrittsberechtigungsgruppen** zur Definition von Gruppen, für die der Zutritt zu Durchtritten zulässig ist.
Offline-Schließsystem		Öffnet das Dialogfenster **Offline-Schließsystem** zur Konfiguration bestimmter Elemente der Anlage (Durchtritte, Zeitmodelle, Berechtigungsgruppen).
Anzeigetexte		Öffnet das Dialogfeld **Anzeigetexte** zur Bearbeitung der Texte, die auf den Kartenlesern angezeigt werden.
Logbuchmeldungen		Öffnet das Dialogfeld **Logbuchmeldungen** zur Bearbeitung und Kategorisierung von Protokollmeldungen.
Zusätzliche Personaldatenfelder		Öffnet das Dialogfeld **Zusätzliche Personaldatenfelder** zur Definition von Datenfeldern für das Personal.
Wiegand-Ausweise		Öffnet das Dialogfeld **Wiegand-Ausweise** zur Definition der Struktur von Ausweisdaten.
Verwaltung von Videogeräten		Öffnet das Dialogfenster **Videogeräte** zur Konfiguration von Kameras, die für die Videoverifikation verwendet werden.
Lageplan-Anzeige und Alarmmanagement		Öffnet die **Lageplan-Anzeige**, die eine Luftaufnahme von Lageplänen und Kontrollgeräten sowie eine Alarmliste für die Alarmbearbeitung bietet.

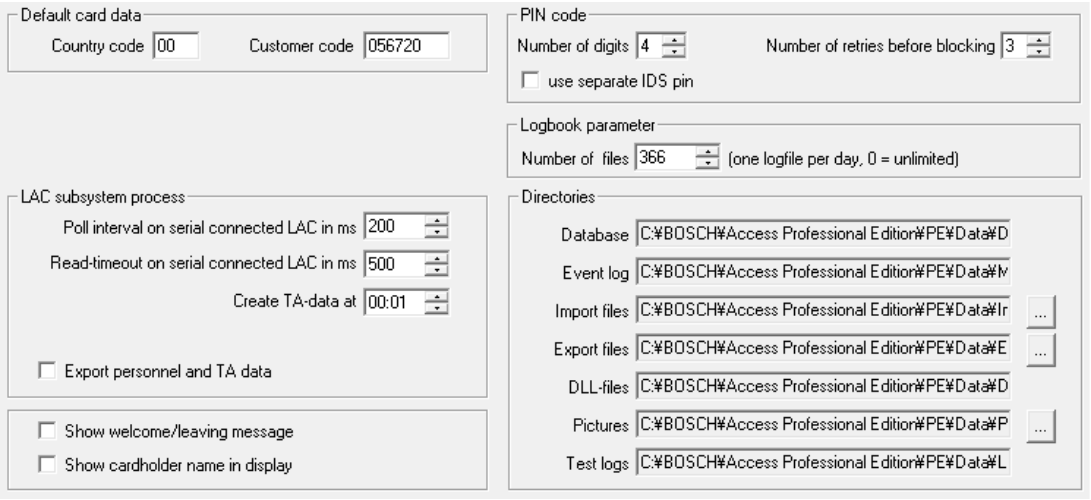
Menü **Einstellungen**		
Lizenzaktivierung		Öffnet ein Menü, mit dem Sie Lizenzen auswählen oder abwählen können.

Anzeige- und Meldungstexte zurücksetzen		Öffnet eine Anforderung dazu, ob Logbuch und Meldungstexte aktualisiert werden sollen.

Menü **?** (**Hilfe**)		
Hilfethemen		Öffnet diesen Hilfetext.
Info zu Access Professional Edition – Konfigurator		Zeigt allgemeine Informationen zu Access Professional Edition – Konfigurator an.

2.4 Allgemeine Systemeinstellungen

Die allgemeinen Systemeinstellungen werden unter der Liste der Controllereinstellungen angezeigt. Sie gelten für alle Installationen.



Parameter	Standard	Beschreibung
Ländercode	00	Bestimmte Ausweisdaten werden an die manuell eingegebene Ausweisnummer angehängt.
Kundencode	056720	
Poll-Intervall auf seriell angeschlossenem LAC in ms	200	Das Zeitintervall in Millisekunden zwischen Abfragen vom LAC-Service zur Überprüfung intakter Anschaltungen zu einem Controller.
Lese-Timeout auf seriell angeschlossenem LAC in ms	500	Wertebereich für Poll-Intervall: 1 bis 500 Mögliche Werte für Lese-Timeout: 1 bis 3000
ZA-Daten erstellen um	00:01	Legt die Uhrzeit fest, zu der die Datei mit den Zeit- und Anwesenheitsdaten erstellt werden soll.
Personal- und ZA-Daten exportieren	deaktiviert	Wenn diese Option aktiviert ist, werden die Zeit- und Anwesenheitsdaten durchgängig in die Exportdatei geschrieben. Ist die Option nicht aktiviert, wird die Datendatei zu der mit dem Parameter **ZA-Daten erstellen um** festgelegten Uhrzeit erstellt.
Die Datei mit den Anwesenheits-Zeitstempeln wird im folgenden Verzeichnis erstellt: C:\Programme\Bosch\Access Professional Edition\PE\Data\Export Unter dem Namen: **ZA_<Aktuelles Datum JJJJMMTT>.dat**		

Parameter	Standard	Beschreibung
Begrüßungs-/ Verabschiedungsnachricht anzeigen	aktiviert	Bei richtigem Lesertyp und richtigen Einstellungen (**Ankunft**, **Verlassen** oder **Prüfung OK** im Dialogfenster „Durchtritte“) werden auf dem Leser die Begrüßungs- und Verabschiedungstexte angezeigt, die für den Ausweisinhaber im Dialogfeld „Personaldaten“ der Personalverwaltungsanwendung hinterlegt sind. Dies gilt nicht für Wiegand-Leser.
Name des Ausweisinhabers im Display anzeigen	aktiviert	Leser mit Display zeigen den **Anzeigenamen** wie in den Personaldaten für den Ausweisinhaber hinterlegt an. Dies gilt nicht für Wiegand-Leser.
Anzahl Ziffern	4	Legt fest, wie viele Ziffern für eine Verifikations- oder Scharfschalte-PIN erforderlich sind. Diese Einstellung gilt auch für die Tür-PIN, die bei der Konfiguration der Durchtritte festgelegt werden kann. Mögliche Werte: 4 bis 8
Getrennte EMA-PIN verwenden		Wenn keine getrennte EMA-PIN festgelegt wurde, kann die EMA mit einer Prüf-PIN scharfgeschaltet werden. Nur wenn das Kontrollkästchen aktiviert ist, werden die Eingabefelder für die Scharfschalte-PIN im Personaldialogfenster aktiv. In diesem Fall kann die Verifikations-PIN nicht mehr zum Scharfschalten der EMA verwendet werden.
Anzahl Wiederholungen vor Sperrung	3	Anzahl von Fehlversuchen bei der Eingabe der PIN. Wenn der Ausweisinhaber die PIN so oft falsch eingibt, wird die betreffende Person für die gesamte Anlage gesperrt. Die Sperrung kann nur durch einen autorisierten Systembenutzer in der Personalverwaltung aufgehoben werden. Mögliche Werte: 1 bis 9
Logbuch-Parameter	366	Anzahl Protokolldateien pro Tag

Parameter	Standard	Beschreibung
		Mögliche Werte: 180 bis 9999 Hinweis: Bei Eingabe eines Werts < 180 wird er automatisch auf den Mindestwert von 180 gesetzt.
Verzeichnispfade zu: Datenbank Protokolldatei Importdateien Exportdateien DLL-Dateien Bilddaten Test-Protokollierung	C: \Programme \Bosch \Access Professional Edition\PE \Data... \Db \MsgLog \Import \Export \Dll \Pictures \Log	Dies sind die Standardpfade. Die Verzeichnisse für Import, Export und Bilddateien können geändert werden.

Hinweis!
Bei Wiegand-Controllern und -Lesern muss zur Verwendung von Identifikations-, Scharfschaltungs- und Tür-PINs die Wiegand-Ausweisdefinition **PIN oder Ausweis** aktiviert sein.

3 Konfigurationen

Die Zusammenstellung eines Systems (welche Eingänge es wo gibt, wie viele und welche Leser, wie die Zutrittsberechtigungen eingerichtet wurden usw.) wird in speziellen Dateien gespeichert. Von diesen Konfigurationsdateien (*.cfg) können beliebig viele existieren, aber nur die Datei mit dem Dateinamen ***active.cfg** kann das laufende System aktivieren. Auf diese Weise können neue Szenarien getestet, Probeläufe durchgeführt und schnelle Systemwechsel vollzogen werden.

3.1 Neue Konfigurationen erstellen

Alle Konfigurationen zu Access PE werden im Verzeichnis **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (sofern bei der Installation die Standardpfade und -verzeichnisse übernommen wurden) gespeichert. Mit der Installation werden zwei Konfigurationsdateien angelegt: **Active.acf** und **Default.acf**. Während Active.acf bereits einige Beispieldaten enthalten kann, die dem Anwender als Konfigurationshilfe dienen können, sind in Default.acf nur die vordefinierten Systemdaten enthalten.

Zu den Systemdaten gehören:

- Die Raumzone **--außerhalb--**
- Die in Deutschland gültigen Feier- und Sondertage
- Die Personalgruppen **Personal** und **Besucher**
- Anzeigetexte für Leser
- Logbuchmeldungstexte

Beim Start verwendet Access PE immer die Konfiguration **Active.acf.**

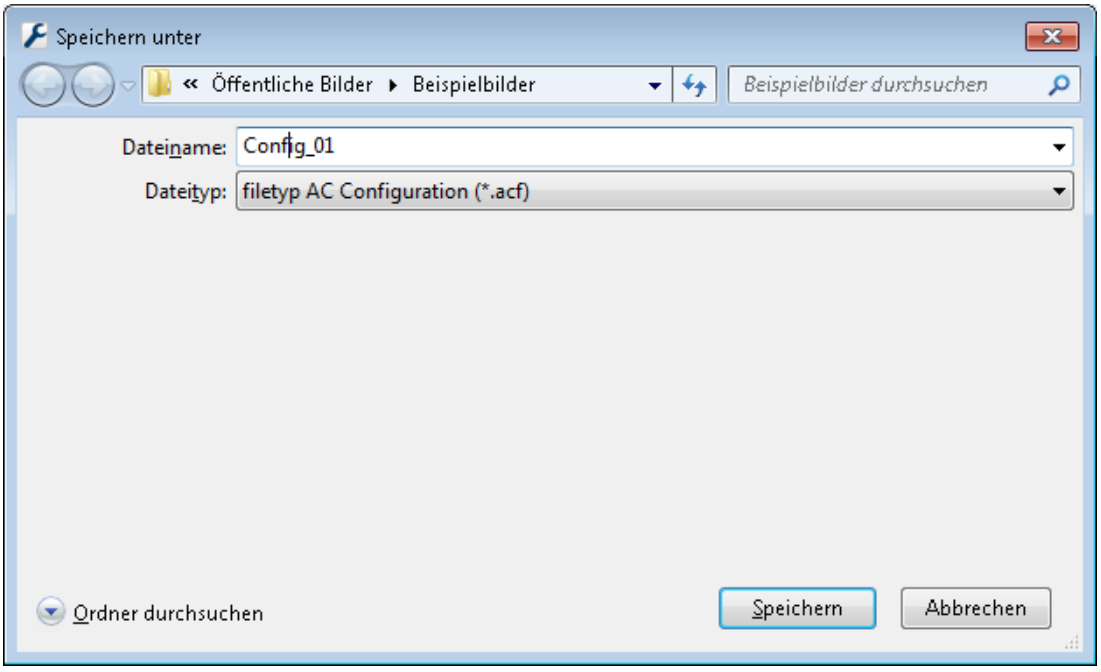
Bei den Konfigurationen wird zwischen folgenden Status unterschieden:

- **Aktive** Konfiguration = Diese Einstellungen und Parametrierungen werden vom laufenden System verwendet.
- **Offene** (geladene) Konfiguration = Diese wird zurzeit von Systemanwendern bearbeitet. Ihre Einstellungen sind in einer separaten ACF-Datei hinterlegt, die **bis zur Aktivierung jedoch keinen Einfluss auf das laufende System** haben.

Für Access PE können beliebig viele Konfigurationen erstellt werden. Da neue Konfigurationen unabhängig vom laufenden System erstellt und bearbeitet werden können, ist es z. B. möglich, neue Raumzonen zu parametrieren, die erst zu einem späteren Zeitpunkt in Betrieb gehen.

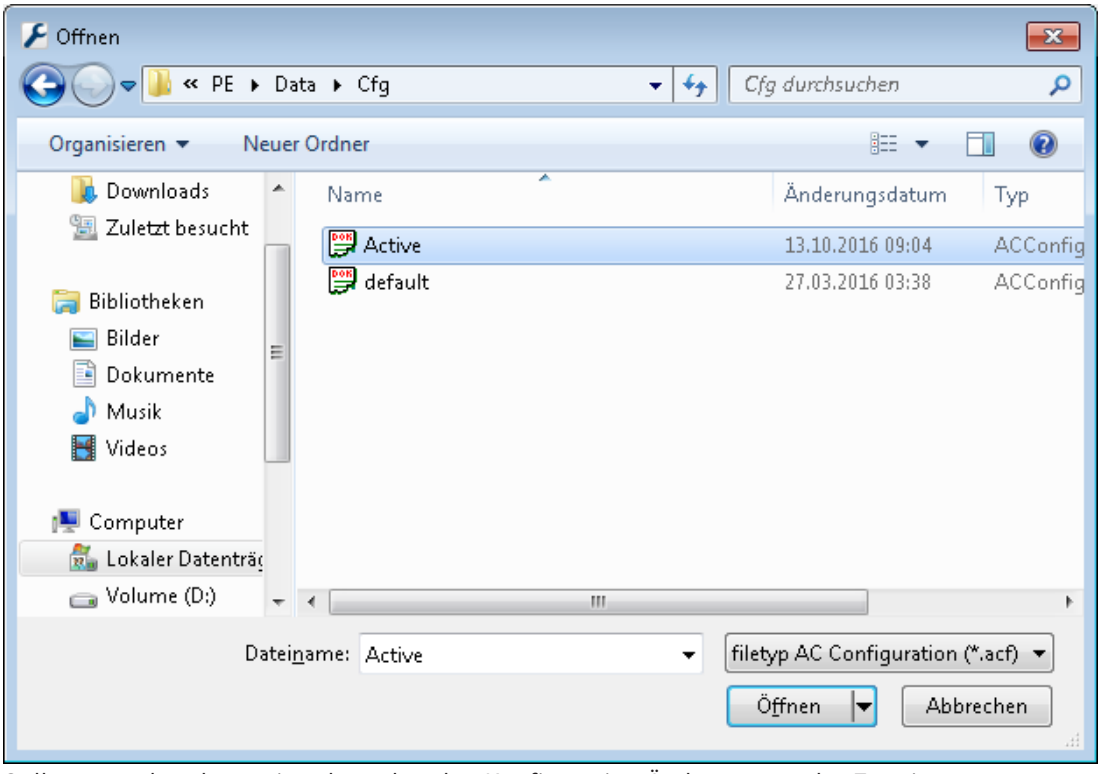
Durch Betätigung der Schaltfläche  in der Symbolleiste wird auf Grundlage von **Unbenannt.acf** der Konfigurator mit den Grundeinstellungen geladen. Jede neue Konfiguration sollte zunächst mit einer passenden Bezeichnung gespeichert werden.

Über die Schaltfläche  wird zum Cfg-Verzeichnis ein Dialog geöffnet, über den die neue Konfiguration gespeichert werden kann. Als Standardbezeichnung wird **Unbenannt.acf** vorgeschlagen. Dieser Name sollte durch eine erläuternde Bezeichnung ersetzt werden.


Speichern unter
« Öffentliche Bilder ▸ Beispielbilder
Beispielbilder durchsuchen
Dateiname: Config_01
Dateityp: filetyp AC Configuration (*.acf)
Ordner durchsuchen
Speichern
Abbrechen

3.2 Konfigurationen öffnen

Der Konfigurator wird immer mit der Konfiguration **Active.acf** geöffnet. Soll stattdessen mit einer anderen Konfiguration gearbeitet werden, kann über die Schaltfläche  eine der bestehenden Konfigurationen aus dem Verzeichnis **C:\BOSCH\Access Professional Edition \PE\Data\Cfg** (= Standardinstallationspfad) geöffnet werden.



Sollen ausgehend von einer bestehenden Konfiguration Änderungen oder Erweiterungen vorgenommen, jedoch noch nicht aktiviert werden, wird diese Basiskonfiguration geöffnet und unter einer neuen Bezeichnung gespeichert. Auf diese Weise können Sie bereits bestehende Konfigurationselemente wiederverwenden und müssen nicht jedes Mal neu mit den Grundeinstellungen von **Default.acf** beginnen.

Hinweis!
Auch von der aktiven Konfiguration kann durch Speichern unter einer anderen Bezeichnung eine Arbeitskopie erstellt werden, die dann geöffnet und geladen werden kann.

3.3 Eine neue Konfiguration aktivieren

Der Konfigurator bietet Ihnen die Möglichkeit, mehrere Konfigurationen in verschiedenen .acf-Dateien zu verwalten. Die aktive Konfiguration ist immer in der Datei **Active.acf** abgelegt.

Vorsicht!
Es wird empfohlen, unbedingt eine Sicherungskopie der aktiven Konfiguration unter einem anderen Dateinamen zu speichern, da die Datei **Active.acf** bei Aktivierung einer neuen Konfiguration überschrieben wird.

Es können nur Konfigurationen aktiviert werden, die geöffnet sind. Deshalb muss zunächst eine neue Konfiguration erstellt oder geöffnet werden.
Um diese Konfiguration zu aktivieren, gehen Sie folgendermaßen vor:

– Auswahl der Funktion **Konfiguration aktivieren** über das Menü **Datei** – oder –

– Betätigung der Schaltfläche  in der Werkzeugleiste

Die geöffnete Konfiguration wird dann in mehreren Schritten aktiviert:

– Bestätigung der Sicherheitsabfrage:
Wollen Sie wirklich die aktuelle Konfiguration mit der neuen Konfiguration ersetzen?
– Die bisher aktive Konfiguration wird mit einem Dateinamen im Format **$jjjjMMtthhmmssW[S]-Active.acf** (j = Jahr, M = Monat, t = Tag, h = Stunde, m = Minute, s = Sekunde, W/S = Winter-/Sommerzeit) gespeichert.
– Die geöffnete Konfiguration wird unter dem Dateinamen **Active.acf** gespeichert, d. h. die alte aktive Konfiguration wird überschrieben!

Ein entsprechendes Infofeld gibt den Namen der gesicherten Datei an: **Die aktuelle Konfiguration wurde aktiviert. Die alte Konfiguration wurde unter <Dateiname> gesichert.**

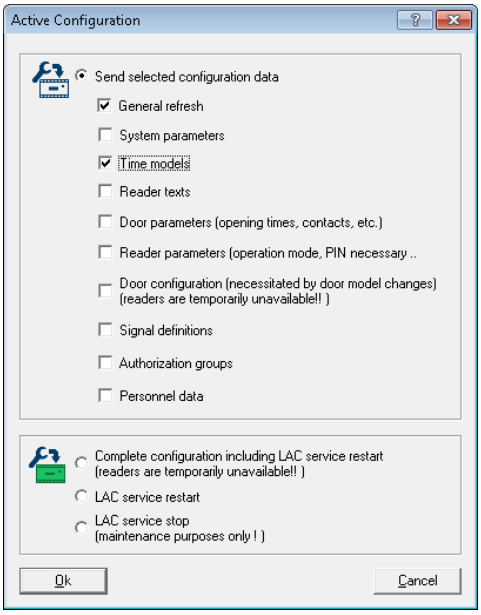
3.4 Konfigurationen an Controller senden

Nach Änderungen in der aktiven Konfiguration **Active.acf** müssen diese Änderungen an die Controller gesendet werden. Dazu haben Sie zwei Möglichkeiten:

– Auswahl der Funktion **Konfiguration an LAC senden** über das Menü **Datei** – oder –

– Betätigung der Schaltfläche  in der Werkzeugleiste

Der folgende Dialog wird angezeigt, in dem Sie auswählen können, welche Konfigurationsdaten an die Controller gesendet werden sollen.

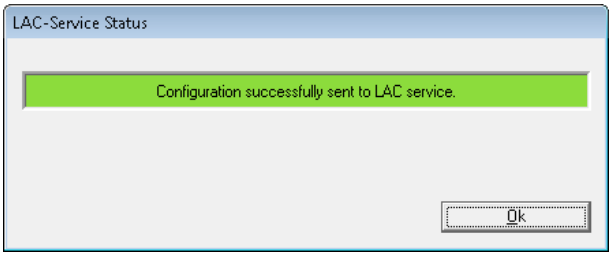


Geänderte und gespeicherte Daten werden hier bereits vorselektiert. Sie können weitere hinzufügen oder auch von der Auswahl ausschließen.
Sie wählen aus, welche Daten an die Controller gesendet werden sollen, und aktivieren die Auswahl über die Schaltfläche **OK**.

Konfigurationsdaten	**Konfigurationen müssen an die LACs gesendet werden, wenn ...**
Allgemeine Aktualisierung	... Logbuchtexte, Zusatzfelder oder Ausweisdefinitionen geändert wurden.
Systemparameter	... sich die LAC-Hardware geändert hat.
Zeitmodelle	... Feiertage, Tages- oder Zeitmodelle geändert wurden.
Lesertexte	... Anzeigetexte geändert wurden.
Türdaten	... bei Eingängen eines oder mehrere der Folgenden geändert wurden – die Öffnungszeit (in 1/10 s) – der Türkontakt – Daten zur Freigabe der Türen (Öffnungszeiten, Kontakte, Zeitprofile usw.) geändert wurden.
Leserdaten	... bei Eingängen eines oder mehrere der Folgenden geändert wurden – die Daten beim Eingangs-/ Ausgangsleser – die Alarmunterdrückung (in 1/10 s) – die Doppelzutrittssperre am Eingang – der Taster für die Türöffnung geändert wurden.

Konfigurationsdaten	Konfigurationen müssen an die LACs gesendet werden, wenn ...
Türkonfiguration	... bei Eingängen das Türmodell geändert wurde. **Hinweis:** Die Neueingabe und Änderung der Adressierung (Seriennummer, Lesertyp) kann nur in der Eingabemaske „Eingänge neu anlegen, ändern und parametrieren“ vorgenommen werden.
Signaldefinitionen	... Parametrierungen der Eingangs- oder Ausgangssignale geändert wurden.
Zutrittsberechtigungsgruppen	... Zutrittsberechtigungsgruppen ohne Zeitmodell geändert wurden oder ein Zeitmodell hinzugefügt oder entfernt wurde.
Personaldaten	... Personendaten neu angelegt oder geändert wurden oder Zutrittsberechtigungsgruppen oder Zeitmodelle geändert wurden.
Gesamte Konfiguration inklusive Neustart des LAC-Services	... die Erstkonfiguration von Access PE abgeschlossen ist. Auch über ein RESET am Controller kann die gesamte Konfiguration geladen werden.
Neustart des LAC-Services	... bei den allgemeinen Einstellungen das Poll-Intervall oder der Zeitpunkt für die Zeiterfassungsdaten geändert wurde.
Beenden des LAC-Services	Dieser Menüpunkt sollte nur in Ausnahmefällen benutzt werden, z. B. bei einer Deinstallation, um einen Neustart des Rechners zu vermeiden.

Der Konfigurator sendet an den **LAC-Service** die Aufforderung, die Konfigurationsdaten an die Controller zu senden. Der LAC-Service ist für die Kommunikation vom und zum Controller zuständig. Dieses Programm wird bei der Installation auf dem Server als Service eingerichtet, der automatisch beim Neustart des Rechners gestartet wird.
Die erfolgreiche Weiterleitung an den LAC-Service wird wie folgt gemeldet und angezeigt:

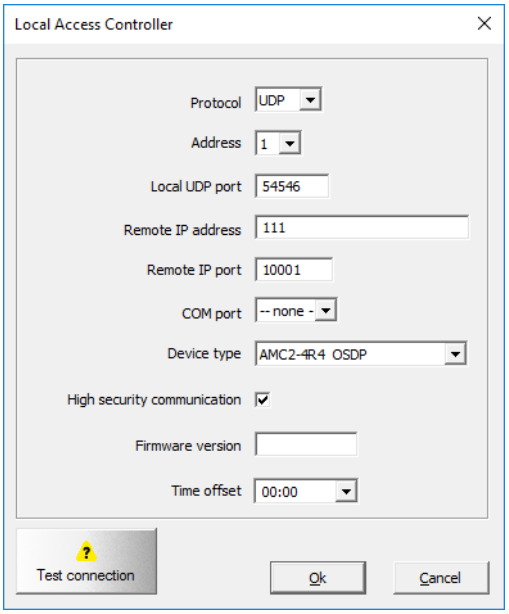


4 Controller

Die Local Access Controller (LAC) sind in Access PE die Stellen, an denen die meisten Zutrittskontrollentscheidungen getroffen werden. Bis auf systemweite Kontrollfunktionen, wie z. B. die Zutrittsfolgekontrolle, können die Controller selbstständig entscheiden, wer Zutritt erhält. Aus diesem Grund verfügen sie in einem eigenen Speicher über sämtliche zutrittsrelevante Daten, sodass auch ein begrenzter und eingeschränkter Offlinebetrieb möglich ist.
Bei Access PE AMC2 (Access Modular Controller) werden Controller verwendet.

4.1 Controller neu anlegen/ändern

Über die Schaltflächen  (Hinzufügen) und  (Ausgewähltes Listenelement bearbeiten) wird bei selektiertem Listeneintrag ein Dialog zur Konfiguration der Schnittstellen vom Access PE Server zu den Controllern geöffnet.



Hinweis!
Unter „Device type“ (Gerätetyp) wird das Kontrollkästchen „High Security Communication“ (Hochsicherheitskommunikation) angezeigt.
Achten Sie darauf, das Kontrollkästchen zu deaktivieren, bevor Sie zu einem anderen Gerätetyp wechseln.

Für jeden Controller muss ein Protokoll festgelegt werden. Folgende Einstellungen sind möglich:

COM Anschluss über serielle (COM) Schnittstelle mit Angabe der physischen COM-Schnittstelle (COMx)

CIP Anschluss über COM-Umleitung per TCP/IP mit Angabe der virtuellen COM-Schnittstelle (COMx) – nur bei LACi mit Schnittstellenwandlern

UDP Anschluss über UDP mit der Angabe des lokalen UDP-Ports und der IP-Adresse bzw. des Netzwerknamens bei Verwendung von DHCP.

Hinweis!
Achten Sie darauf, dass bei der Verwendung der CIP- und UDP-Schnittstellen der DIL-Adressschalter des Controllers an Position **5** auf **EIN** gesetzt ist.

Je nach Auswahl des Protokolls sind verschiedene weitere Einstellungen erforderlich (siehe folgende Tabelle):

Para-meter	**COM**	**CIP**	**UDP**	**Hinweis**
Adresse	1 bis 8	1 bis 8	Immer 1	Bei COM und CIP muss der DIL-Schalter des Controllers dieselbe Adresseinstellung haben.
Lokaler UDP-Port	Deakti-viert	Deakti-viert	Fort-laufend	Der Port, über den der Access PE-Server Informationen vom Controller empfangen soll. Die Controller erhalten entsprechend ihrer Position den nächsten freien Port. Diese Angabe kann jedoch geändert werden.
Remote-IP-Adresse	Deakti-viert	Deakti-viert	IP-Adresse oder Netzwerkna me	Bei Netzwerken, in denen DHCP verwendet wird, muss der Netzwerkname angegeben werden, ansonsten die IP-Adresse des Controllers.

Para-meter	COM	CIP	UDP	Hinweis
Remote-IP-Port	Deakti-viert	Deakti-viert	10001 (fest)	Dies ist der Port am Controller zum Empfang der Servermeldungen.
COM-Port	Auswahlliste der COM-Ports	Auswahllist e der COM-Ports	<keine>	Die Nummer des COM-Ports, mit dem der Controller auf dem Access PE-Server verbunden ist.
LAC-Typ	Auswahlliste der verfügbaren Controller	Auswahllist e der verfügbaren Controller	Auswahlliste der verfügbaren Controller	Die folgenden Controllertypen sind verfügbar:
	AMC-4W Wiegand			mit Wiegand Leserschnittstelle
	AMC2-2W Wiegand			mit RS485- und Wiegand Leserschnittstelle
	AMC-4R4-BG900			mit RS485-Leserschnittstelle
	AMC-4R4-L-BUS			mit RS485-Leserschnittstelle
	AMC-4R4-OSDP			mit RS485-Leserschnittstelle
Hochsichere Kommunikation	Kontrollkästchen zur Auswahl von controllerspezifischer, sitzungsbasierter Verschlüsselung mit AES 128 zwischen **Host und Controller**.			
Firmwareversion (Projekt)	keine	keine	keine	zur Angabe der Softwareversion
Zeitversatz	Dies ist eine Auswahlliste mit Zeitaufschlägen und -abzügen. Befindet sich der AMC in einer anderen Zeitzone als der Server, kann hier die abweichende Zeit eingestellt werden. Mögliche Werte sind -12:00 bis +12:00 in 30-Minuten-Schritten. Der Zeitversatz wird für alle Zeiten übernommen, die vom Server zum AMC gesendet werden. Entsprechend wird der Zeitversatz bei Zeitwerten, die vom AMC gesendet werden,			

Para-meter	COM	CIP	UDP	Hinweis
	abgezogen. Die lokalen AMC-Zeiten werden in die Logbuchmeldungen übernommen und können im Logbuch angezeigt werden.			

Controller-Test (LAC-Test)

Die Erreichbarkeit des Controllers mit den eingestellten Werten kann vorm Speichern getestet werden. Auf diese Weise können fehlerhafte Angaben schnell korrigiert oder ergänzt werden. Die Schaltfläche **Test LAC** unten im Dialogfeld versucht, anhand der getätigten Angaben die Verbindung zum Controller herzustellen. Dieser Test kann auch nach dem Festlegen eines Controllers durch Auswahl des betreffenden Controllers im Listenfeld und Betätigung der Schaltfläche  erfolgen.

Diese Schaltfläche kann vier unterschiedliche Zustände über entsprechende Symbole darstellen, die auch in der ersten Spalte des Listenfeldes angezeigt werden.

 Der Controller wurde noch nicht getestet oder ist nicht aktiviert.

 Der Test war erfolgreich. Die Verbindung konnte aufgebaut werden.

 Der Test war nicht erfolgreich.

 Der Status steht noch aus.

Hinweis!

Diese Symbole zeigen den aktuellen Status an und werden automatisch aktualisiert. Erneute Verbindungsversuche können die Anzeige der Statusaktualisierung verzögern.

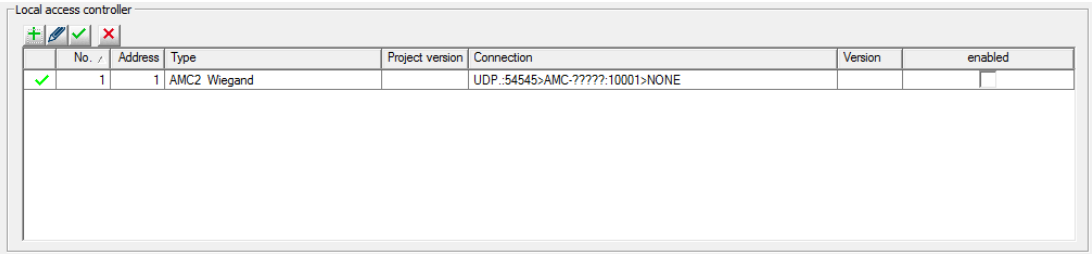
Ein Controller-Test kann verschiedene Phasen durchlaufen. Einzelne Phasen können dabei auch übersprungen werden:

- Start des LAC-Services
- Download des LAC-Programms
- Wartezustände:
  - Lesen der Konfigurationsdaten für den Controller
  - Statusmeldung vom Controller
- Meldung zum Verbindungsaufbau

Das Testergebnis wird im Dialog **LAC-Service Status** angezeigt. Nach Bestätigung der Meldung über die Schaltfläche **OK** wird das Testergebnis im Listenfeld angezeigt.

4.2 Controllereinstellungen (LAC-Einstellungen)

Im Dialog **Allgemeine Einstellungen**, der über die Schaltfläche  aufgerufen wird, werden unter anderem die Local Access Controller (LAC) angelegt und parametriert.



Oberhalb des Listenfeldes befinden sich die Schaltflächen für folgende Funktionen:

 Einen neuen Controller **hinzufügen**

 Den selektierten Controller **bearbeiten**

 Den selektierten Controller **testen**

 Den selektierten Controller **löschen**

Das Listenfeld enthält alle angelegten Controller und zeigt folgende Informationen an:

Spalte	Inhalt	Beschreibung
	 oder	Status LAC-Test: negativ, noch nicht durchgeführt oder erfolgreich
Nr.	1 bis 128	Laufende Nummerierung der Controller
Adresse	1 bis 8	Am DIL-Schalter eingestellte und konfigurierte Adresse des Controllers, bei UDP-Protokoll immer 1
Typ	AMC-Wiegand AMC-4R4-BG900 AMC-4R4-L-Bus AMC-4R4 OSDP AMC2-2W	Ausgewählter Controllertyp.
Projektversion	Beispiel: 37.50	Vom Controller geladene spezielle Projektprogrammversion
Anschluss	Beispiel: UDP: 54545>AMC DEMO: 10001>NONE	Schnittstellenparameter: Protokoll: lokaler UDP-Port>Netzwerkname oder IP-Adresse: Remote IP-Port>COM-Port

Spalte	Inhalt	Beschreibung
Version	Beispiel: 37.02	Vom Controller geladene Programmversion
Aktiviert	Aktiviert oder deaktiviert	Wenn das Kontrollkästchen deaktiviert ist, baut der LAC-Dienst keine Verbindung zum AMC2 auf. Der AMC2 wird eigenständig arbeiten.

Der untere Dialogteil enthält allgemeine Systemeinstellungen, die für alle Geräte und Anwendungen von Access PE gelten.

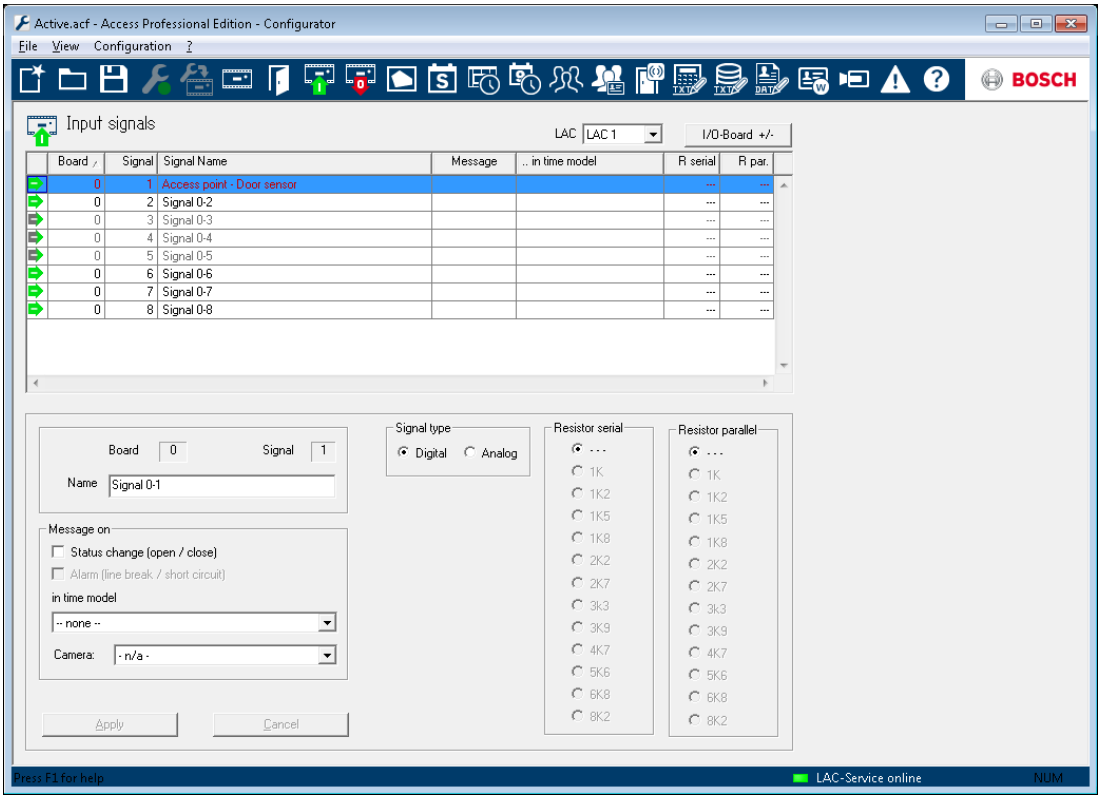
Hinweis!
Nach einer Installation oder Aktualisierung müssen Sie das Kontrollkästchen **Enabled** (Aktiviert) aktivieren, um den ausgewählten AMC2 zu aktivieren.

5 Signale

Über die Eingangs- und Ausgangssignale der Controller können z. B. Türzustände ermittelt werden und Türsteuerungen erfolgen. Darüber hinaus lassen sich über diese Signale auch zusätzliche Kontrollfunktionen mit Zutrittsanfragen verbinden. So können beispielsweise Kameras, optische oder akustische Signalgeber und Alarmanlagen angesteuert und aktiviert werden.

5.1 Eingangssignale

Während unter **Eingänge** die Türsteuerungen und andere Kontrolleinrichtungen sowie Zustandsmeldungen parametriert wurden, werden im Dialog **Eingangssignale** die Signaltypen definiert und überwacht.



Bei Aufruf dieses Dialoges wird immer der erste Controller angezeigt. Wählen Sie den gewünschten Controller in der Auswahlliste **LAC** anhand der fortlaufenden Nummerierung aus. Bei der Standardeinrichtung eines Controllers werden 8 Eingangs- und 8 Ausgangssignale angelegt. Verfügt der verwendete Controller über mehr als diese 8 Kontakte, können über die Schaltfläche **I/O Platine +/-** weitere Signale aktiviert werden.
Im Listenfeld werden alle angegebenen Signale aufgeführt. Die jeweiligen Einstellungen werden in den einzelnen Spalten sowie zu den selektierten Signalen auch in der Parameterübersicht unter dem Listenfeld angezeigt. Alle Einstellungen können sowohl in den entsprechenden Spalten der Liste als auch in der Parameterübersicht vorgenommen werden.

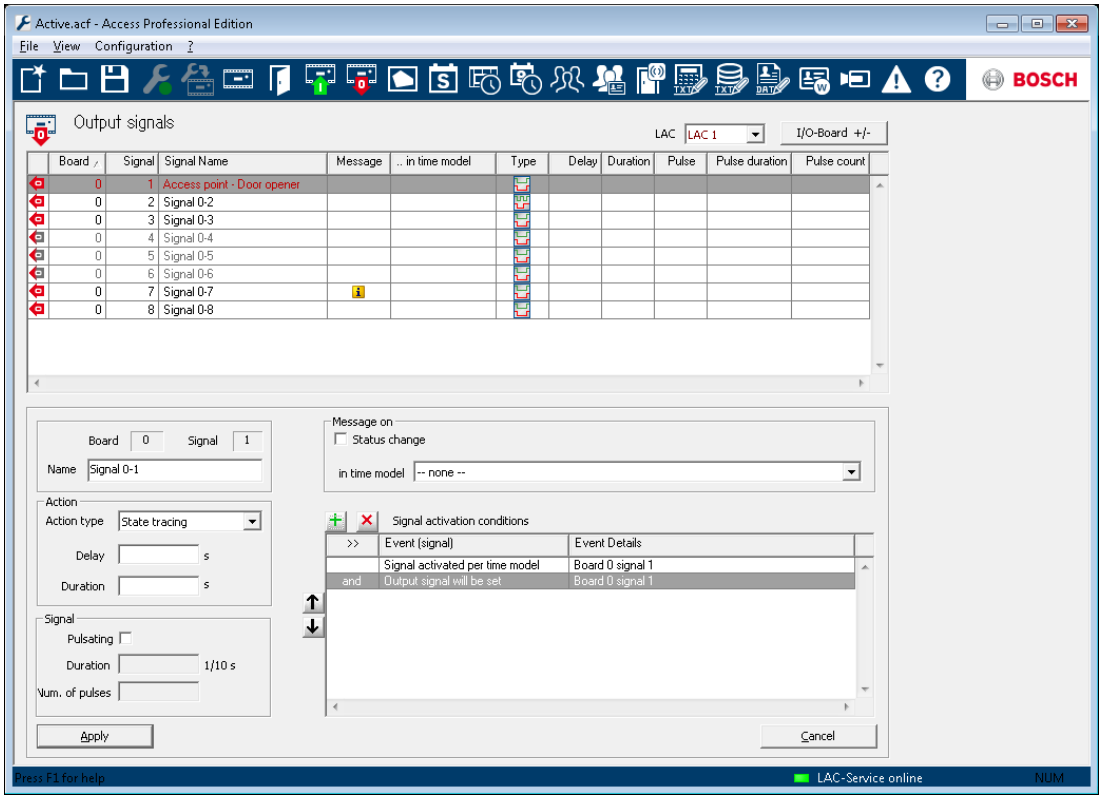
Spalte	Parameter	Beschreibung
1 (ohne Bezeichnung)	-	Damit wird der Signalzustand angegeben:  = Signal aktiviert  = Signal deaktiviert Der jeweils andere Zustand kann per Doppelklick gesetzt werden.
Platine	Platine	Dies ist die Nummerierung der Platine, an der sich das Signal befindet. 0 = Basisplatine 1 = Erweiterungsplatine Dieser Parameter kann nicht geändert werden.
Signal	Signal	Dies ist die Nummer des Platinensignals (1 bis 16). Dieser Parameter kann nicht geändert werden.
Signalbezeichnung	Name	Dies ist die Bezeichnung des Signals. In der Standardeinstellung erhalten die Signale die Bezeichnung: Signal <Platine-Nr.>-<Signal-Nr.> Durch einen Doppelklick in das Listenfeld wird der Änderungsmodus aktiviert.
Meldung	Meldungen bei ... Zustandsänderung (offen/ geschlossen): Alarm:	Visualisierung der Parametereinstellung in der Liste:   ist nur für den Signaltyp **Analog** möglich. Die Listendarstellung kann per Doppelklick geändert werden.
	Kamera	Eine Kamera in der Auswahlliste kann bestimmten Eingangssignalen zugeordnet werden. Bei Aktivierung des entsprechenden Signals wird eine Logbuchmeldung generiert, über die auch die Kamerabilder abgerufen werden können.
- nur im Zeitprofil	im Zeitmodell	Damit wird das ausgewählte Zeitmodell angezeigt.

Spalte	Parameter	Beschreibung
		Durch einen Doppelklick öffnet sich eine Auswahlliste für die Zeitmodelle.
<keine>	Signaltyp Digital Analog	Die Option **Analog** aktiviert die Optionsfelder zur Auswahl der Widerstandswerte.
R seriell	Widerstand seriell	Ein Doppelklick in das entsprechende Listenfeld öffnet eine Auswahlliste der Widerstandswerte. Die Auswahl eines seriellen oder parallelen Widerstandswerts setzt den Signaltyp von der Standardeinstellung „Digital“ auf „Analog“.
R par.	Widerstand parallel	

Hinweis!
Nicht alle aufgelisteten Werte sind miteinander kombinierbar. Eine Aufstellung über die Verwendung geeigneter Widerstandspaare finden Sie im Installationshandbuch des AMC2-Geräts.

5.2 Ausgangssignale

Mit diesem Dialog werden Ausgangssignale parametriert und gegebenenfalls weitere Signalplatinen angelegt.

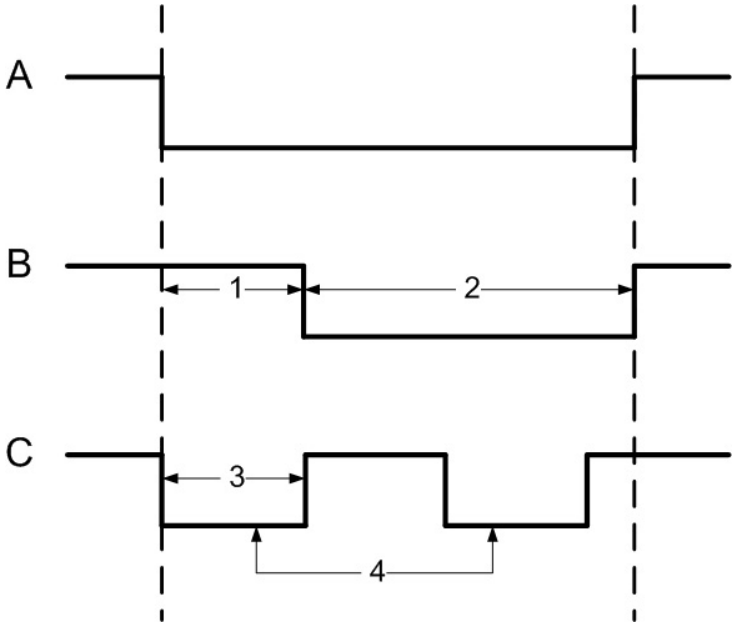


Bei Aufruf dieses Dialoges wird immer der erste Controller angezeigt. Wählen Sie den gewünschten Controller über die Auswahlliste **LAC** anhand der fortlaufenden Nummerierung aus. Bei der Standardeinrichtung eines Controllers werden 8 Eingangs- und 8 Ausgangssignale angelegt. Verfügt der verwendete Controller über mehr als diese 8 Kontakte, können über die Schaltfläche **I/O Platine +/-** weitere Signale aktiviert werden.
Im Listenfeld werden alle angegebenen Signale aufgeführt. Die jeweiligen Einstellungen werden in den einzelnen Spalten sowie zu den selektierten Signalen auch in der Parameterübersicht unter dem Listenfeld angezeigt. Alle Einstellungen können sowohl in den entsprechenden Spalten der Liste als auch in der Parameterübersicht vorgenommen werden.
Neben den hier aufgeführten Einstellungen für die Ausgangssignale können zusätzlich **Bedingungen** definiert werden, die erfüllt sein müssen, damit das Ausgangssignal aktiviert wird.

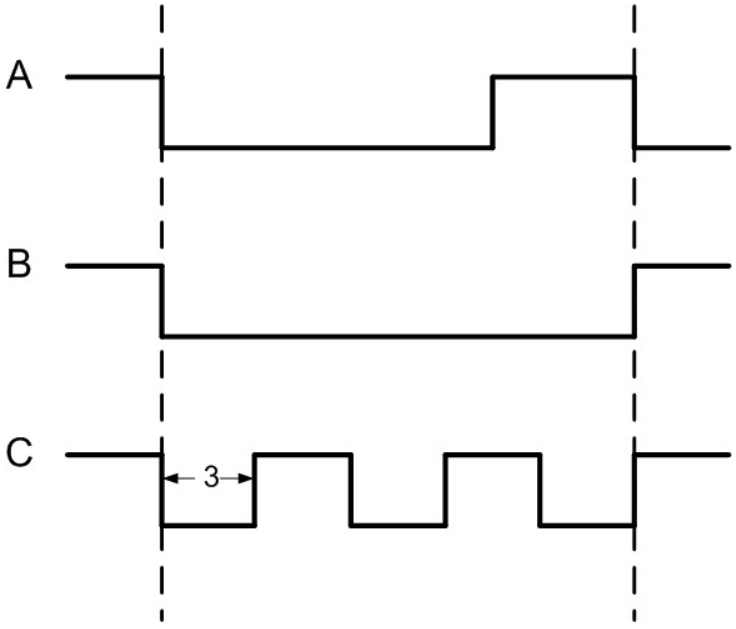
Spalte	Parameter	Beschreibung
1 (ohne Bezeichnung)	-	Damit wird der Signalzustand angegeben:  = Signal aktiviert  = Signal deaktiviert Der jeweils andere Zustand kann per Doppelklick gesetzt werden.
Platine	Anschluss	Dies ist die Nummerierung der Platine, an der sich das Signal befindet. 0 = Basisplatine 1 = Erweiterungsplatine Dieser Parameter kann nicht geändert werden.
Signal		Dies ist die Nummer des Platinensignals (1 bis 16). Dieser Parameter kann nicht geändert werden.
Signalbezeichnung	Name	Dies ist die Bezeichnung des Signals. In der Standardeinstellung erhalten die Signale die Bezeichnung: Signal <Platine-Nr.>-<Signal-Nr.> Signale, die im Dialog **Eingänge neu anlegen, ändern und parametrieren** definiert und aktiviert wurden, werden mit Angabe der Eingangsbezeichnung und der Signalfunktion angezeigt. Durch einen Doppelklick in das Listenfeld wird der Änderungsmodus aktiviert.

Spalte	Parameter	Beschreibung
Meldung	Meldungen bei ... Zustandsänderung	Visualisierung der Parametereinstellung in der Liste:  Die Einstellung wird per Doppelklick umgeschaltet.
- nur im Zeitprofil	im Zeitmodell	Hier wird das Zeitmodell angezeigt und ausgewählt.
Typ	Aktionstyp: Impulsansteuerung Zustandsnachführung Zustandswechsel	Es können drei Aktionstypen ausgewählt werden:    Durch einen Doppelklick wird der nächste Zustand in der gezeigten Reihenfolge ausgewählt.
Verzögerung	Verzögerung	Dies ist die Verzögerung, bis das Signal gegeben werden soll [0 bis 9999].
Dauer	Dauer	Dies ist die Zeitspanne in 1/10 s, bis das Signal gegeben werden soll [1 bis 9999, 0 = immer oder bis zu einer Abbruchmeldung].
Puls	Pulsierend	Die Impulsgebung wird aktiviert. Ansonsten wird das Signal konstant gegeben. Ein Doppelklick aktiviert diese Option, kennzeichnet sie jedoch als undefiniert mit einem  , bis Dauer und Anzahl angegeben werden. Danach erfolgt die Kennzeichnung mit .
Pulsdauer	Dauer	Dies ist die Dauer der Impulsgebung.
Pulsanzahl	Anzahl der Impulse	Damit wird Anzahl der Impulse pro Sekunde angegeben.

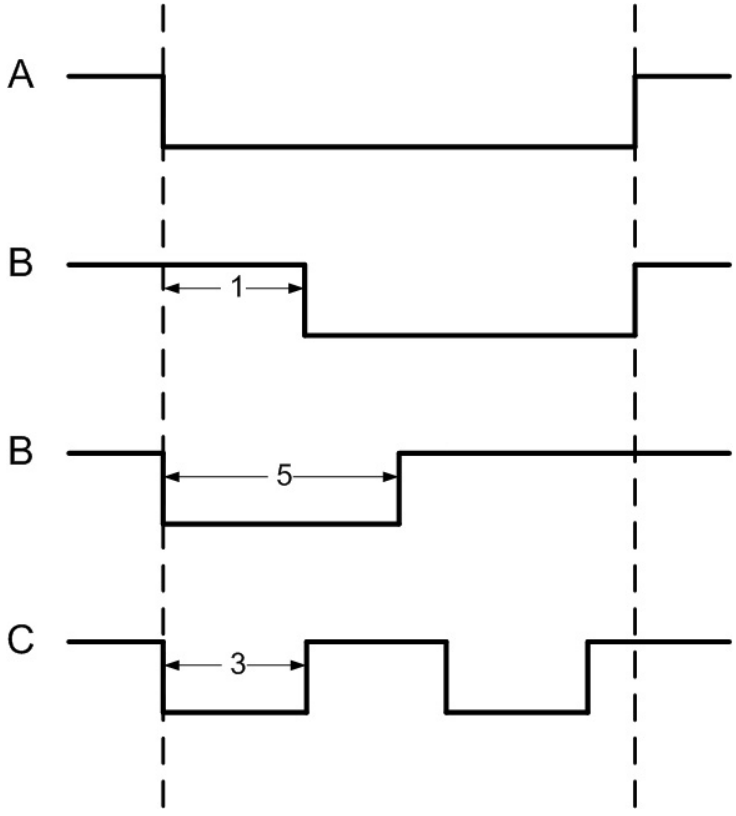
Aktionstyp: Impulsansteuerung



Aktionstyp: Zustandswechsel



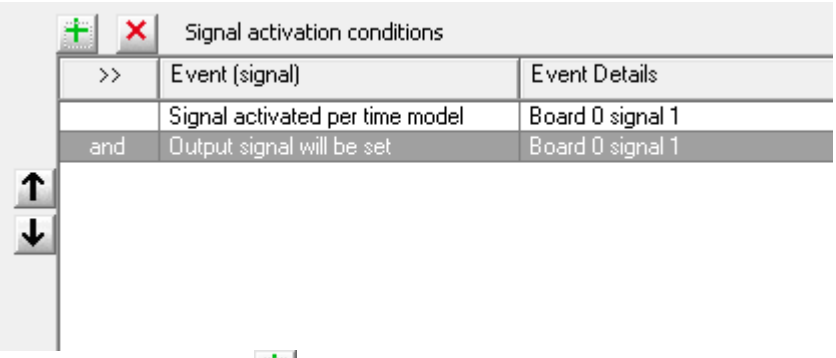
Aktionstyp: Zustandsnachführung



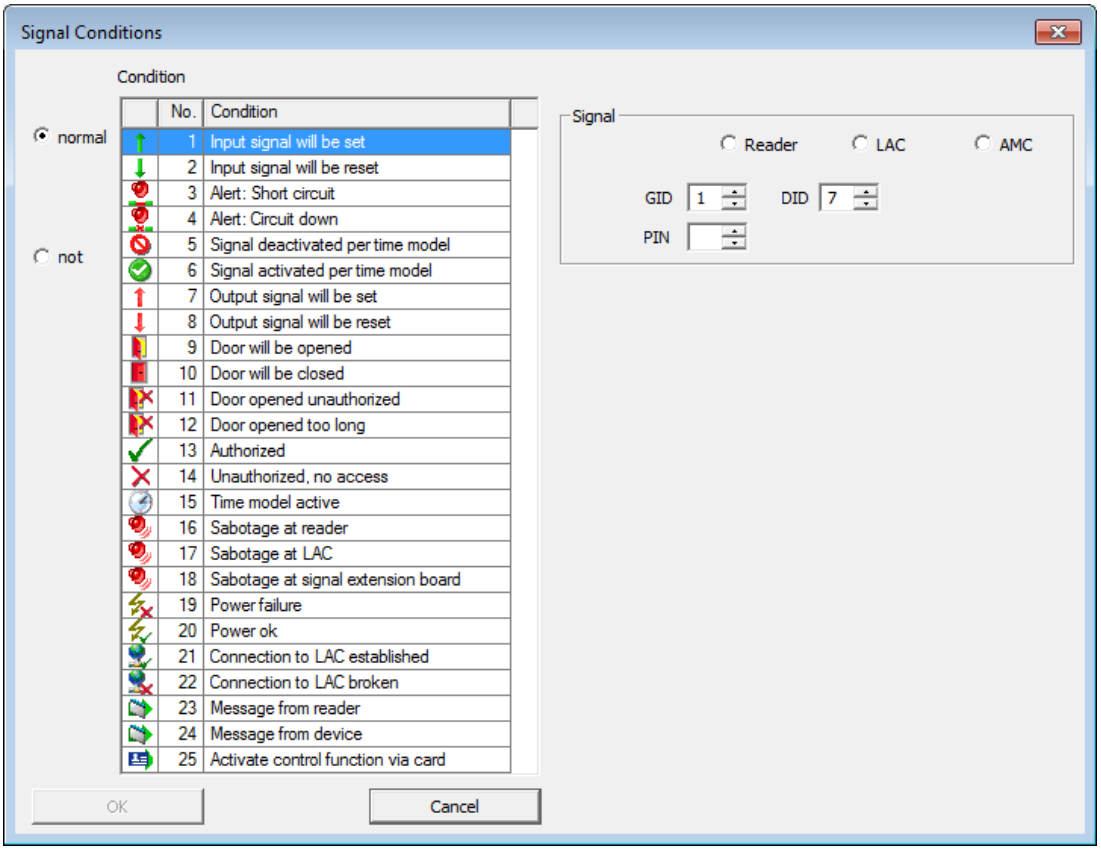
A =	Polling
B =	nicht pulsierend
C =	pulsierend
1 =	Verzögerung
2 =	Periode
3 =	Impulsdauer
4 =	Impulsanzahl (hier = 2)
5 =	maximale Dauer

5.3 Bedingungen für Ausgangssignale festlegen

Auf der Dialogseite **Ausgangssignale** können neben den Einstellungen zusätzliche Bedingungen definiert werden, die dafür sorgen, dass Ausgangssignale nur unter bestimmten Voraussetzungen aktiviert werden.
Die besonderen Bedingungen zum ausgewählten Signal des Listenfeldes können im unteren rechten Dialogbereich festgelegt werden.



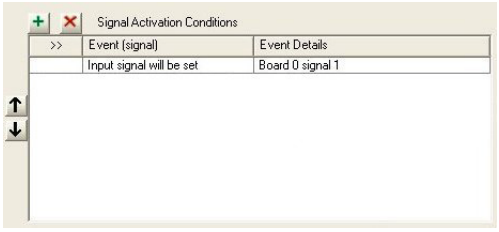
Über die Schaltfläche wird der nachstehende Dialog geöffnet. In diesem Dialog können Sie die jeweiligen Bedingungen konfigurieren.



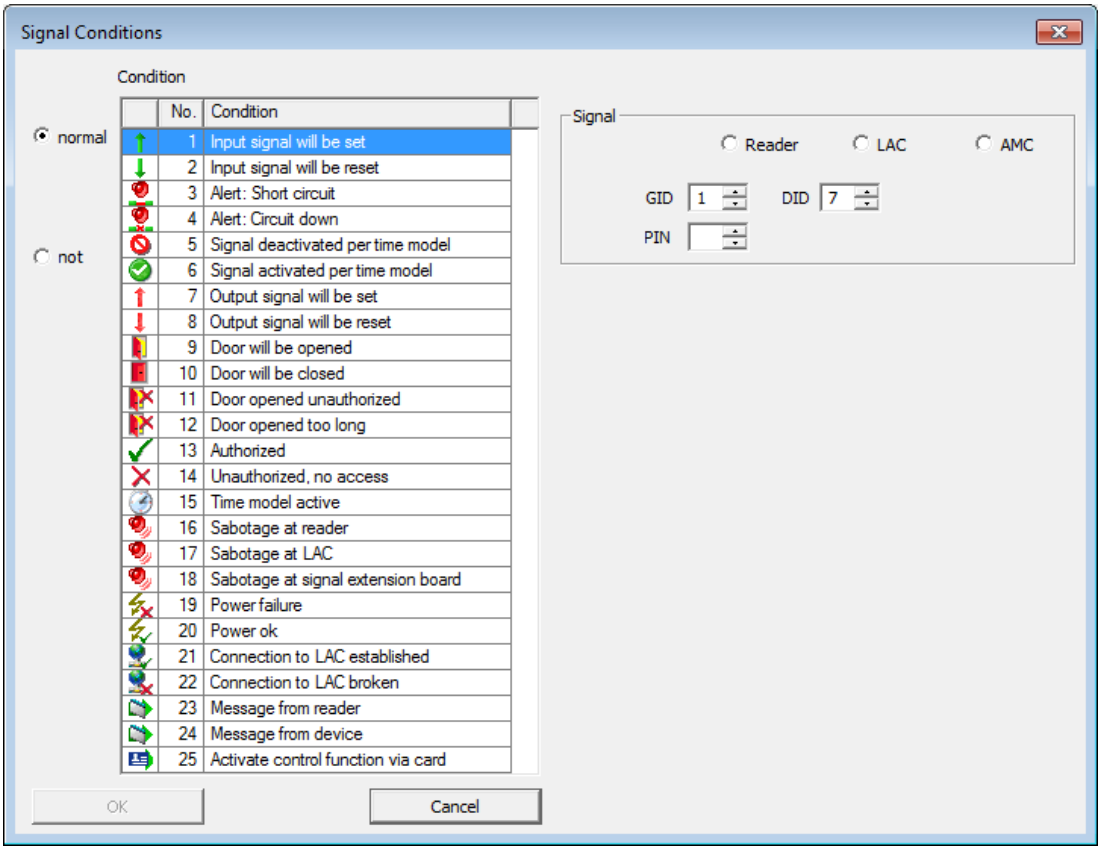
Je nach Bedingung sind ergänzende Angaben, z. B. der Name des Lesers, anzugeben, bevor die Bedingung über Betätigung der Schaltfläche **OK** übernommen werden kann.
Zu jedem Signal können beliebig viele Bedingungen ergänzt werden. Der Dialog muss für jede neue Bedingung über die Schaltfläche neu geöffnet werden.

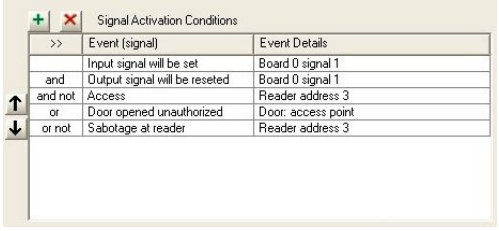
Hinweis!
Es können nur Signale und Einrichtungen (Eingänge, Leser, Türen) ausgewählt werden, die an den Controller angeschlossen sind, zu dem Sie das Ausgangssignal parametrieren.

Für die erste Bedingung können Sie zwischen den Optionen **normal** (wenn die Bedingung zutreffen soll) und **not** (wenn die Bedingung nicht zutreffen soll) wählen.



Jede weitere Bedingung wird über die Auswahl der Operatoren **and**, **and not**, **or** oder **or not** mit der ersten verknüpft.

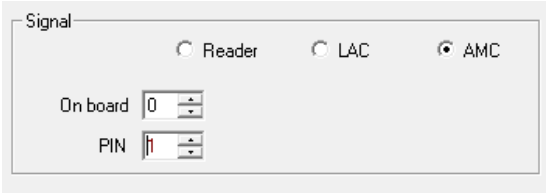
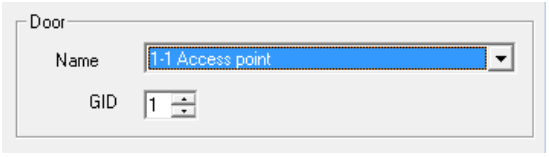
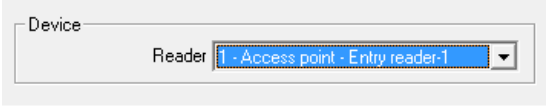
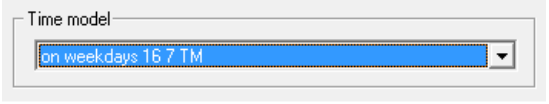
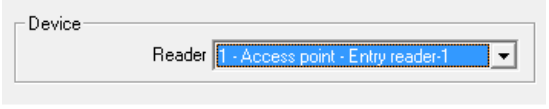
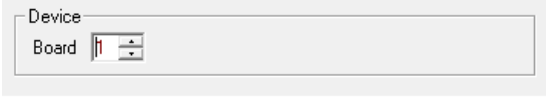


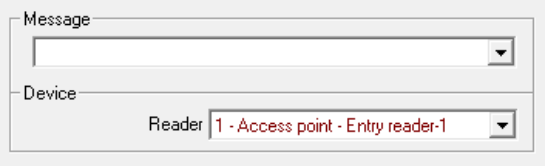
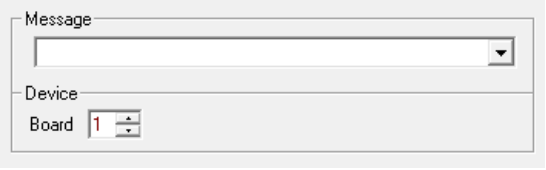
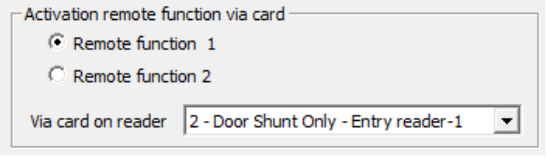


Die Bedingungen werden in der aufgelisteten Reihenfolge abgearbeitet. Entspricht die Auflistung nicht dem notwendigen Ablauf, können Bedingungen verschoben werden. Die betreffende Bedingung wird in der Liste ausgewählt und anschließend über die Schaltflächen ↑ bzw. ↓ an die gewünschte Position gesetzt.

Notwendige ergänzende Angaben zu den Bedingungen sind in der folgenden Tabelle zu finden:

Bedingung	Ergänzende Angaben
Eingangssignal wird gesetzt	– Angabe zum Gerätetyp, an dem sich das Signal befindet

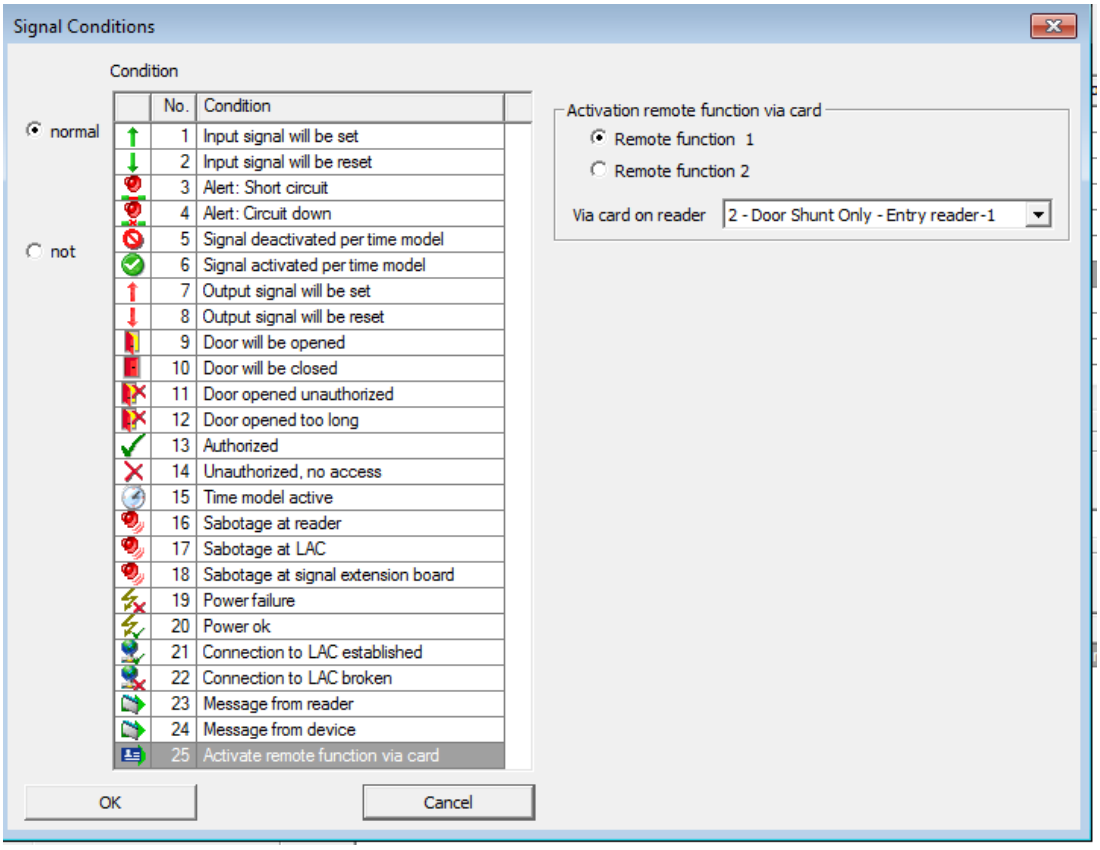
Bedingung	Ergänzende Angaben
Eingangssignal steht an	– Auswahl der Platine – Auswahl des Anschlusses 
Alarm: Kurzschluss	
Alarm: Leitungsbruch	
Signal deaktiviert durch Zeitmodell	
Signal aktiviert durch Zeitmodell	
Ausgangssignal wird gesetzt	
Ausgangssignal wird zurückgesetzt	
Tür wird geöffnet	– Auswahl des Eingangs – GID (Gruppen-ID) wird automatisch gesetzt 
Tür wird geschlossen	
Tür unerlaubt geöffnet	
Tür zu lange geöffnet	
Zutritt	– Auswahl des Lesers 
Unberechtigt, kein Zutritt	
Zeitmodell aktiv	– Auswahl des Zeitmodells 
Sabotage am Leser	– Auswahl des Lesers 
Sabotage am LAC	– Keine zusätzlichen Angaben notwendig
Sabotage an Signalerweiterung	– Auswahl der Platine 
Netzausfall	– Keine zusätzlichen Angaben notwendig
Netzwiederkehr	
Verbindung LAC -> APE hergestellt	

Bedingung	Ergänzende Angaben
Verbindung LAC -> APE gestört	
Meldung von Leser	– Auswahl der Meldung aus vordefinierter Meldungsliste – Auswahl des Lesers 
Meldung von Gerät	– Auswahl der Meldung aus vordefinierter Meldungsliste – Auswahl der Platine 
Aktivieren der Steuerungsfunktion per Ausweis	Legen Sie eine Ausgabe basierend auf einer Berechtigung fest, die einem Ausweisinhaber erteilt wurde. Siehe Kapitel **Aktivieren der Steuerungsfunktion per Ausweis**. 

5.3.1 Aktivieren der Steuerungsfunktion per Ausweis

Mit dieser Steuerungsfunktion kann eine Person zwei verschiedene Ausgangssignale auslösen.
Zum Verwenden dieser Option müssen folgende Voraussetzungen erfüllt sein:

- Es muss eine Person konfiguriert sein, die zur Aktivierung von Steuerungsfunktionen berechtigt ist.
- Ihr Ausweis muss gültig sein und den Zutritt beim Durchtritt erlauben.
- Unter **Signal conditions** (Signalbedingungen) muss das Ausgangssignal **25 – Activate remote function via card** (25 – Remote-Funktion per Ausweis aktivieren) ausgewählt sein.
- Die Remote-Funktion muss ausgewählt und ein Leser zugewiesen sein.



So geht es weiter:

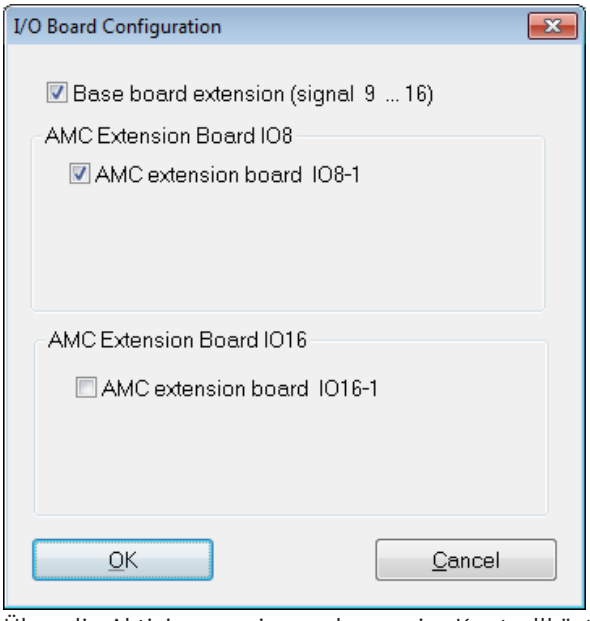
- Halten Sie den Ausweis an den Leser. Die Autorisierung der Person wird überprüft.
- Bei Autorisierung wird das Ausgangssignal als konfiguriert festgelegt.

5.4 Erweiterungsplatinen anlegen

Erweiterungsplatinen können sowohl im Dialog für die **Eingangssignale** als auch bei den **Ausgangssignalen** angelegt werden. Die Einstellungen, die in einem Dialog vorgenommen werden, werden im anderen übernommen.
Im Zutrittskontrollsystem Access PE können drei Arten von Erweiterungsplatinen verwendet und parametriert werden. Alle drei Arten werden über einen der Signaldialoge bearbeitet.

- **AMC2-4W-EXT**: zur Erweiterung (Verdopplung) der Schnittstellen eines Wiegand AMCs (AMC2-4W)
- **AMC2-8I-8O-EXT**: jeweils 8 weitere Signale
- **AMC2-16I-16O-EXT**: jeweils 16 weitere Signale

Wählen Sie über dem Listenfenster zunächst aus der Auswahlliste **LAC** den gewünschten Controller aus. Die Controller werden mit 8 Signalen an der Basisplatine (= 0) angelegt.
Zum Anlegen einer Erweiterungsplatine betätigen Sie die Schaltfläche **I/O-Platine +/-**, über die der folgende Dialog angezeigt wird:



Über die Aktivierung eines oder zweier Kontrollkästchen können folgende Einstellungen vorgenommen werden:

- **AMC-Hauptplatine** (Signale 9 bis 16)
  Damit wird eine Wiegand-Erweiterungsplatine **AMC2 4W-EXT** angelegt.
  Diese Platine umfasst dieselben Schnittstellen wie ein AMC2 4W-Controller (4 Wiegand-Leserschnittstellen und jeweils 8 Eingangs- und 8 Ausgangssignale). Sie kann jedoch nicht eigenständig arbeiten, sondern muss mit einem AMC2 4W verbunden sein.
  Diese Erweiterung kann nur mit einem AMC2 4W verwendet werden.
  Zu einem AMC2 4W-EXT können zusätzlich **3** IO-Platinen konfiguriert werden.
  Im Listenfeld der Eingangs- bzw. Ausgangssignale wird die Erweiterungsplatine wie der Controller selbst mit der Platinennummer 0 und den Signalnummern 9 bis 16 angelegt.
- **AMC-Erweiterungsplatine IO8**
  Dies ist eine Platine mit 8 Eingangs- und 8 Ausgangssignalen zur Erweiterung der Schnittstellen eines Controllers.
  Diese Platine kann an jeden AMC2-Controller angeschlossen werden und bei der Verwendung mit einem AMC2 4W-Controller auch mit der Wiegand-Erweiterungsplatine AMC2 4W-EXT kombiniert werden.

Im Listenfeld der Eingangs- bzw. Ausgangssignale wird die Erweiterungsplatine mit der Platinennummer 1 und den Signalnummern 1 bis 8 angelegt.

– **AMC-Erweiterungsplatine IO16**
  Dies ist eine Platine mit 16 Eingangs- und 16 Ausgangssignalen als Erweiterung der Schnittstellen eines Controllers.
  Diese Platine kann an jeden AMC2-Controller angeschlossen werden und bei der Verwendung mit einem AMC2 4W-Controller auch mit der Wiegand-Erweiterungsplatine AMC2 4W-EXT kombiniert werden.
  Im Listenfeld der Eingangs- bzw. Ausgangssignale wird die Erweiterungsplatine mit der Platinennummer 1 und den Signalnummern 1 bis 16 angelegt.

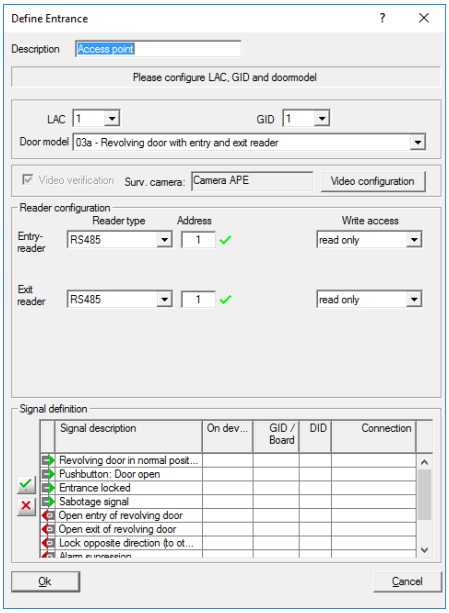
Hinweis!
Die hier vorgenommenen Einstellungen für die **I/O-Platinen** gelten sowohl für die Eingangs- als auch für die Ausgangssignale des jeweiligen Controllers und können in einem der beiden Dialoge vorgenommen werden.

6 Eingänge/Durchtritte

Wenn von Eingängen die Rede ist, ist stets ein Gesamtes aus mehreren Bestandteilen, die zu einer Zutrittskontrolle gehören, gemeint. Neben der Tür, die auch ein Drehkreuz, eine Schleuse, eine Schranke oder ein Aufzug sein kann, gehören einer oder mehrere Leser, eventuell Taster sowie Steuereinheiten (Riegel, Motorschloss usw.) dazu. Außerdem können als zusätzliche Kontrollfunktionen noch optische oder akustische Signalgeber oder Kameras enthalten sein.

6.1 Eingänge neu anlegen und ändern

Ein neuer Eingang kann entweder über die Schaltfläche  oder über das Kontextmenü des Listenfeldes (rechte Maustaste und die Option **Neuer Eingang** wählen) angelegt werden. Name, Türmodell und Geräteadressen für einen selektieren Eingang können über die Schaltfläche  , per Doppelklick oder über das Kontextmenü (rechte Maustaste und die Option **Eingang ändern** wählen) geändert werden.

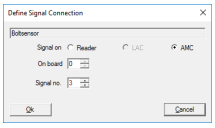


Beim Anlegen eines neuen Eingangs wird der Name des Eingangs festgelegt. Dieser sollte eindeutig und aussagekräftig sein, da über diesen Namen die Zutrittsberechtigungen bei der Konfiguration von Gruppen vergeben und die Einzelberechtigungen in der Personalverwaltung zugeordnet werden.
Weiterhin sind die Gruppen-ID (GID) und die laufende Nummer des Controllers zu wählen, an den der Eingang angeschlossen werden soll. In der Regel muss nur auf die Nummer des Controllers geachtet werden, da Access PE automatisch die nächste freie GID zuweist. Das passende Türmodell muss aus der Liste der **Türmodelle** ausgewählt werden. Die Funktionalität der einzelnen Türmodelle können Sie dem Anhang entnehmen.
Entsprechend der Variante des Türmodells werden Auswahllistenfelder für Eingangs- und/oder Ausgangsleser angezeigt, zu denen der Lesertyp aus der Liste selektiert werden muss. Jeder Leser erhält eine für den ausgewählten Controller eindeutige Adresse. Für Leser mit **Wiegand**-Schnittstelle wird lediglich die **Nummer der Schnittstelle des Controllers** angegeben, an die der Leser angeschlossen ist. Für Leser mit **RS485**-Schnittstelle ist die eingestellte **DIP-Adresse** maßgeblich.

Hinweis!
Achten Sie darauf, dass die Leseradressierung mit den installierten Gegebenheiten übereinstimmt.
Bei Controllern des Typs **AMC-Wiegand** können Sie maximal 4 Leser, bei den Typen **AMC-RS485** und **LACi** maximal 8 Leser anschließen.

Verwendung der Leseradresse 9:
Die Leseradresse 9 wurde als Parametrierhilfe angelegt und dient als Platzhalter bei eventuell notwendigen Umparametrierungen. Wenn Sie alle Leseradressen eines Controllers belegt haben und anschließend Umparametrierungen vornehmen müssen, können Sie einen der Leser auf Adresse 9 platzieren, um die ursprüngliche Adresse freizusetzen.
Beispiel: Sie möchten die Leser 4 und 7 tauschen. Da Sie dieselbe Adresse nicht doppelt vergeben können, setzen Sie zunächst Leser 4 auf Adresse 9. Nun können Sie Leser 7 auf Adresse 4 umparametrieren und anschließend Leser 9 (= ursprünglich Leser 4) auf Adresse 7 setzen.

Signaldefinition
Mit der Auswahl des Türmodells werden alle für dieses Türmodell infrage kommenden und verwendbaren Eingangs- und Ausgangssignale im Listenfeld angezeigt. Durch die Auswahl des gewünschten Listeneintrags und Betätigung der Schaltfläche ✓, die sich links vom Listenfeld befindet, oder per Doppelklick auf einen Listeneintrag öffnen Sie einen Dialog zur Definition der Signale.



Das im Listenfeld selektierte Signal wird zur Kontrolle mit seiner Bezeichnung angezeigt. Die Verwendung des Signals ist in der Standardeinstellung der parametrierten Controller eingerichtet, kann aber bei Bedarf geändert werden.
Des Weiteren werden die Platine, an der sich der Signalanschluss befindet, und die Nummer der Signalschnittstelle angegeben. Informationen zur Nummerierung der Signale am Controller bzw. an der Erweiterungsplatine finden Sie in den jeweiligen Installationshandbüchern.

Hinweis!
Sie sollten vom Techniker eine Auflistung der Signalverdrahtung verlangen, die Ihnen die identische Parametrierung ermöglicht.
Werden hier falsche Zuordnungen getroffen, kann dies erhebliche Fehlfunktionen der Türsteuerung und der Meldungsgenerierung zur Folge haben.

In diesem Dialog wird der Anschluss (DCU, Leser, LAC oder AMC) ausgewählt. Bei der Angabe von „DCU“ oder „Leser“ müssen zusätzlich GID und DID des Geräts angegeben werden. Dabei gelten folgende Regeln:

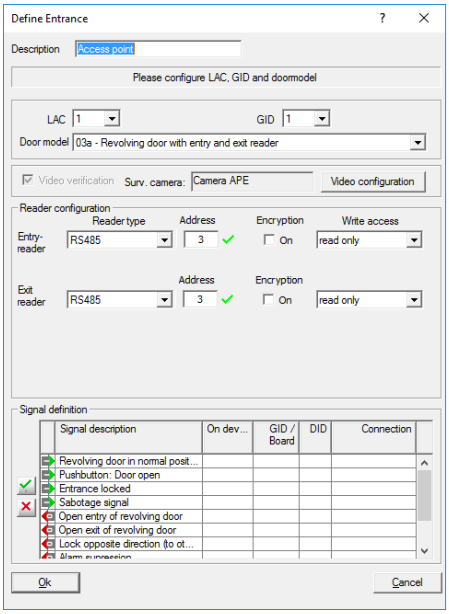
- **Leser**
  - GID = GID des Lesers dem Eingang
  - DID = 1 bei ersten **Eingang**sleser, = 2 bei zweiten **Eingang**sleser, = 3 bei ersten **Ausgang**sleser, = 4 bei zweiten **Ausgang**sleser
  - Signalnummer = Signal an Leser 1 ... 4
- **LAC**
  - Signalnummer = Signal an LAC 1 ... 16

- **AMC**
  - auf Platine = Platinennummer 0 oder 1
  - Signalnummer = Signal an AMC 1 ... 8 oder bei Erweiterungsplatinen 1 ... 16

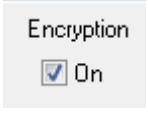
Die parametrierten Anschlüsse werden im Listenfeld in den entsprechenden Spalten angezeigt. Die erste Spalte enthält verschiedene Symbole zur Anzeige des Signalzustands:

	Eingangssignal nicht gesetzt
	Eingangssignal gesetzt
	Ausgangssignal nicht gesetzt
	Ausgangssignal gesetzt

Ein bereits definiertes Signal kann mit der Schaltfläche ✕ gelöscht werden.
Das Beispiel oben zeigt das Bearbeiten eines Türmodells mit einem **Wiegand**-Leser.
Im Falle eines **OSDP**-Lesers sieht der Dialog folgendermaßen aus:



Die **Verschlüsselungsoption** ist standardmäßig nicht ausgewählt. Für die Nutzung mit **OSDPv2 secure**-fähigen Lesern sollten Sie die **Verschlüsselungsoption** auswählen:



Auswahl von OSDP-Lesern:

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

Die folgenden OSDP-Leser werden unterstützt:

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!
Bei Verwendung von MIFARE-Ausweisen mit OSDP-Leser und Bosch Codierung muss die Ausweisart **MIFARE (63 Bit)** ausgewählt werden, damit die Bosch Codierung aktiviert wird.

Verschiedene Produktfamilien (z. B. **LECTUS duo** und **LECTUS secure**) dürfen nicht gleichzeitig mit einem OSDP-Bus verbunden werden. Achten Sie darauf, Leser an einem OSDP-Bus entweder als „verschlüsselt" oder „unverschlüsselt" zu konfigurieren, jedoch keine Kombination von beidem.

Warnung!
ACHTUNG! WICHTIGER HINWEIS!
Ein Schlüssel wird zur verschlüsselten Datenübertragung zum OSDP-Leser erstellt. Speichern Sie diese Datei
D:...\BOSCH\Access Professional Edition\PE\cfg\Active.acf
unbedingt auf einem sicheren lokalen Laufwerk.
Diese Datei wird zur Wiederherstellung einer vorhandenen Installation benötigt.

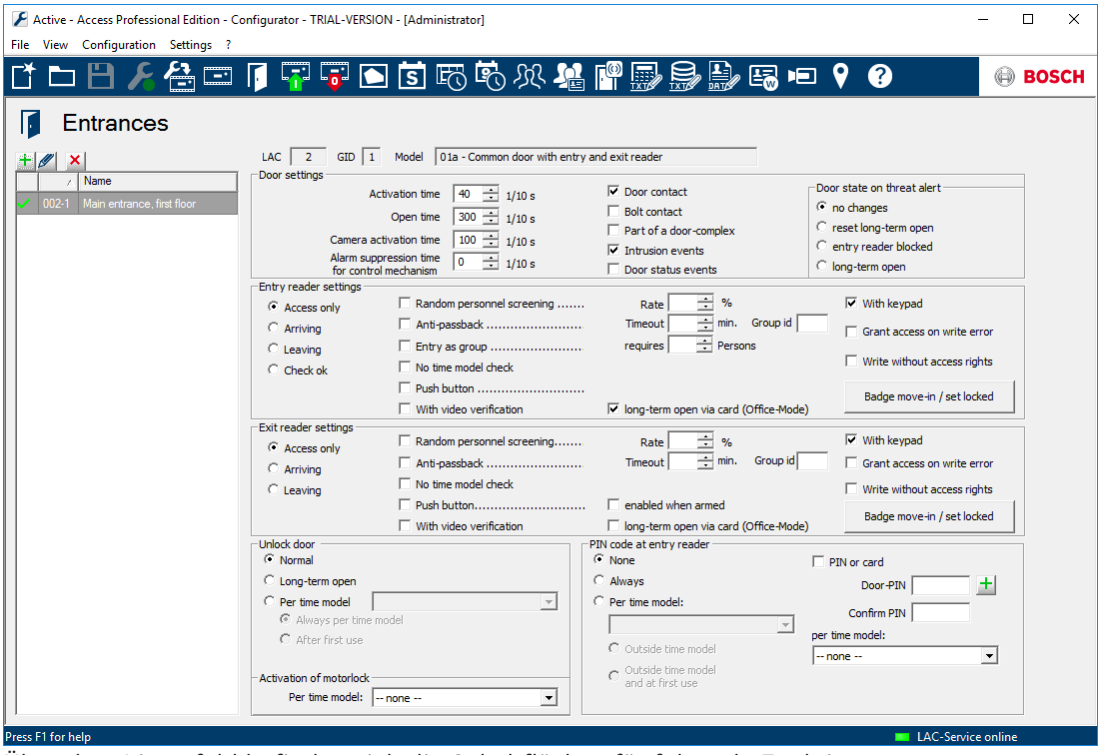
Warnung!
Falls **OSDPv2 secure**-fähige Leser im sicheren Modus verwendet werden, benötigen die Leser den ersten Masterschlüssel.
Geht der Masterschlüssel verloren, können die Leser nicht mit einem neuen Masterschlüssel erneut konfiguriert werden!

Wenn Sie den Masterschlüssel verlieren, müssen alle Leser vom Support in den Auslieferungszustand zurückgesetzt werden.

Hinweis!
Die Verwendung von OSDP-Lesern wurde nicht von UL untersucht.
Folgen

6.2 Anzeige und Parametrierung

Alle dem System bekannten Eingänge werden auf der linken Seite in einer Liste angezeigt. Wenn Sie mit der Maus einen Eingang in der Liste selektieren, werden die Daten des Eingangs in der rechten Hälfte der Maske angezeigt.



Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

 Einen neuen Eingang **hinzufügen**

 Den selektierten Eingang **bearbeiten**

 Den selektierten Eingang **löschen**

Über den Parametrierfeldern werden die Anschlussoptionen des jeweiligen Eingangs angezeigt:

LAC Laufende Nummer des Controllers, an dem der Eingang parametriert wurde

GID Nummer der Gruppe, die dieser Eingang mit seiner Tür und den Lesern bildet

Modell Bezeichnung des ausgewählten Türmodells

Diese Angaben können mit der Bearbeitungsfunktion  (oder per Doppelklick auf den Listeneintrag) geändert werden.
Zu einem Eingang können folgende **Türoptionen** parametriert werden:

Optionen Tür	Beschreibung
Freigabezeit in 1/10 s	Ist kein Türrahmenkontakt konfiguriert, wird der Türöffner für die festgelegte Dauer betätigt. Ansonsten endet die Betätigung des Türöffners, wenn über den Kontakt erkannt wird, dass die Tür offen ist. Standardwert = 40
Öffnungszeit in 1/10 s	Maximale Dauer, für die die Tür für den Durchtritt geöffnet sein darf. Wird diese Dauer überschritten, meldet das System „Tür zu lange geöffnet“. Standardwert = 300
Kameraaufblendung in 1/10 s	Ist der Durchtritt mit einer Überwachungskamera ausgerüstet, kann hier die Zeitdauer für die Ansteuerung der Kamera parametriert werden. Standardwert = 100
Alarmunterdrückung vor Türöffnung in 1/10 s	Dauer der Alarmunterdrückung, bevor der Türöffner betätigt wird. Die Alarmunterdrückung ist nur wirksam, wenn diese Zeit größer 0 ist. Standardwert = 0
Türöffnungskontakt	Ist die Tür mit einem Türrahmenkontakt versehen, kann das System mit dessen Parametrierung den Durchtritt von Personen überwachen. Zugleich wird das Signal für die Türöffnung abgeschaltet, wenn über diesen Kontakt die Türöffnung erkannt wird. Über dieses Signal wird auch die **Alarmunterdrückung** gesteuert.
Türriegelkontakt	Ist die Tür mit einem Türriegelkontakt versehen, kann über diese Parametrierung erkannt werden, ob die Tür tatsächlich geschlossen ist.
Teil einer Schleuse	Gibt an, ob die Tür als Teil einer Schleuse parametriert wird, z. B. als Drehtonne oder Luftschleuse. In diesem Fall wird über die Signale für die Schleusenverriegelung sichergestellt, dass immer nur eine Tür der Schleuse geöffnet ist. Wird nur eine Tür als Teil einer Schleuse parametriert, ist die Türsperre (Blockade) unwirksam.
Einbruchmeldung	Hier können Sie angeben, ob bei einer unberechtigten Türöffnung eine Meldung generiert werden soll. Voraussetzung dafür ist das Vorhandensein eines **Türöffnungskontakts**.
Türöffnungsmeldungen	Das System kann jede Türöffnung melden, wenn ein **Türöffnungskontakt** vorhanden ist. Hier können Sie parametrieren, ob das Öffnen und Schließen der Tür gemeldet werden soll.
Türzustand bei Bedrohungsalarm	Konfiguration von Türzuständen für Bedrohungsalarme (siehe Kapitel *Konfigurieren von Bedrohungsalarmen*).

Zu einem Eingang können folgende Leseroptionen parametriert werden:

Leseroptionen Eingangs- und Ausgangsleser	**Beschreibung**
nur Zutrittskontrolle	Bei Begehung über diesen Leser werden ausschließlich Zutrittsmeldungen generiert.
Kommt	Bei einer Begehung an diesem Ausweisleser wird zusätzlich eine Kommt-Buchung für die **Zeiterfassung** generiert und die Person als anwesend markiert.
Geht	Bei einer Begehung an diesem Ausweisleser wird zusätzlich eine Geht-Buchung für die **Zeiterfassung** generiert und die Person als abwesend markiert.
Buchungen, die an Lesern vorgenommen werden, die für die Zeiterfassung parametriert wurden, werden in einer täglich neu angelegten Datei im Verzeichnis C:\BOSCH\Access Professional Edition\PE\Data\Export (= Standardpfad) gespeichert. Die Datei **TA_<Tagesdatum jjjjmmtt>.dat** wird angelegt. Sie kann bearbeitet werden. Die einzelnen Angaben sind durch Semikolon voneinander getrennt und können somit beispielsweise in Tabellenkalkulationsprogrammen anderer Anbieter bearbeitet werden. Zu jeder Buchung werden folgende Daten ausgegeben: Name; Vorname; Firma; Personalnummer; Ausweisnummer; Zusatzfelder 1 bis 10 (sofern parametriert); Bezeichnung des Durchtritts; Datum (jjjjmmtt); Uhrzeit (hhmmss sowie ggf. ein „s“ zur Kennzeichnung der Sommerzeit); Richtung als nummerischer Wert (1 = Eingang, 2 = Ausgang); Richtung als Textstring (ENTER, LEAVE)	
Kontrolle OK	Nur für **Eingangsleser**. Mit dieser Option kann der Leser als **Freigabeleser** für die **zufällige Personenkontrolle** eingerichtet werden, d. h. die durch die Personenkontrolle eingerichtete Sperre wird mit diesem Leser zurückgesetzt. Achten Sie darauf, dass der Freigabeleser nicht gleichzeitig auch Auswahlleser für die zufällige Personenkontrolle ist.
Zufällige Personenkontrolle – Zufallsrate	Mit dieser Option kann der Leser als **Auswahlleser** für die **zufällige Personenkontrolle** eingerichtet werden. Neben der Aktivierung des Kontrollkästchens ist der Prozentsatz (1 bis 99) der Zufallsrate anzugeben. Werden keine Angaben gemacht, findet eine 100%ige Kontrolle statt. Achten Sie darauf, dass der Auswahlleser nicht gleichzeitig auch Freigabeleser für die zufällige Personenkontrolle ist.
Doppelzutrittssperre – Wartezeit – Gruppen-ID	Bei dieser Option wird eine Sperre mit der eingerichteten Wartezeit für die wiederholte Buchung mit demselben Ausweis eingerichtet. Damit soll der Missbrauch von Ausweisen durch Rückgabe durch ein Drehkreuz verhindert werden. Die **Wartezeit** wird in Minuten von 1 bis 480 angegeben. Mehrere Leser können zu einer Gruppe zusammengefasst werden. Die Doppelzutrittssperre gilt dann für alle Leser mit derselben **Gruppen-ID**. Mögliche Werte: 1 bis 2 Zeichen (0 bis 9 und/oder A bis Z)

Leseroptionen Eingangs- und Ausgangsleser	**Beschreibung**
Zutritt nur als Gruppe – mit mindestens ... Personen	Nur für **Eingangsleser**. Der Zutritt wird erst gewährt, wenn die eingestellte Anzahl Personen berechtigt an einem Leser gebucht haben. Mögliche Werte: 2 bis 6
mit Tastatur	Aktivieren Sie diese Option, wenn der Leser über ein Tastenfeld verfügt.
Zeitmodell NICHT prüfen	In der Standardeinstellung wird der Zugang anhand zugewiesener Zeitmodelle geprüft. Soll dies an bestimmten Leser nicht erfolgen, kann die Prüfung durch Aktivierung dieser Option ausgeschaltet werden.
Mit Motoreinzug	Aktivieren Sie diese Option, wenn der Leser über einen Karteneinzug verfügt.
Taster für Türöffnung – immer aktiv	Hier kann die Erkennung eines Eingangssignals für den Ein-/Ausgang parametriert werden, über das die Tür geöffnet wird. Das Signal kann an einen Taster oder auch an eine Telefonanlage angeschlossen sein, z. B. wenn kein Ausgangsleser vorhanden ist. **immer aktiv**: Bei normaler Einstellung funktioniert der Türtaster bei aktivierter GMA (Gefahrenmeldeanlage) nicht. Der überwachte Bereich kann dann nicht verlassen werden. Mit dieser Option bleibt der Türtaster auch nach einer Scharfschaltung funktionsbereit. Diese Funktion betrifft auch einen Ausgangsleser, sofern ein Türtaster aktiviert ist.
Mit Videoverifikation	Aktivieren Sie dieses Kontrollkästchen, wenn die Videoverifikation aktiviert werden soll.
Langfristig öffnen per Ausweis (Büromodus)	Diese Option 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 (siehe Kapitel „Büromodus“).

Hinweis!
Kontrollen, die über die Basisprüfungen von Berechtigungen und Zeitmodellen hinausgehen (Zutrittsfolgekontrolle, Doppelzutrittssperre, zufällige Personenkontrolle), werden vom LAC-Subsystem-Prozess durchgeführt. Zur Gewährleistung dieser Funktionen muss der Access PE-Server ständig laufen (24 Stunden/Tag und 7 Tage/Woche).

Die **Türfreigabe** kann wie folgt konfiguriert werden:

Freigabe der Tür	Beschreibung
Normalbetrieb	Die Tür ist geschlossen und wird nur geöffnet, wenn ein gültiger Ausweis am Leser präsentiert wird.
Dauerfreigabe	Die Tür ist für einen längeren Zeitraum offen, z. B. tagsüber oder solange die Rezeption durchgehend besetzt ist.
mit Zeitmodell	Die Dauerfreigabe der Tür erfolgt über das angegebene Zeitmodell in folgenden Varianten: – **strikt nach Zeitmodell**: Die Tür ist in den Zeitintervallen des Modells offen. – **nach erster Begehung**: Die Tür bleibt nach der ersten Begehung innerhalb eines Zeitintervalls des Modells bis zum Ende des Intervalls geöffnet. – **Aktivierung über Dialog**: Die längere Öffnung in einem bestimmten Zeitintervall wird durch einen speziellen dialogfähigen Leser gesteuert.
Zuschaltung des Motorschlosses	Hier kann ein zuvor definiertes Zeitmodell ausgewählt werden, über das das Motorschloss einer Tür angesteuert wird (in der Regel außerhalb der normalen Geschäftszeiten).

Die **PIN-Eingabe am Eingang** kann wie folgt konfiguriert werden:

PIN-Eingabe am Eingang	Beschreibung
Keine	Es ist keine PIN erforderlich.
Immer	Die PIN muss immer eingegeben werden.
mit Zeitmodell	Die Eingabe der PIN wird über das Zeitmodell in folgenden Varianten gesteuert: – **außerhalb des Zeitmodells**: Die PIN muss außerhalb der Intervalle des Zeitmodells eingegeben werden. – **außerhalb des Zeitmodells und bei erster Begehung**: Die PIN muss außerhalb der Intervalle des Zeitmodells und bei der ersten Begehung einer Person innerhalb eines Intervalls eingegeben werden.
PIN oder Ausweis	Bei aktivierter Funktion kann der Zutritt sowohl mit der alleinigen Eingabe einer Tür-PIN als auch mit einem Ausweis erfolgen.
Tür-PIN	Hier kann eine Tür-PIN mit 4 bis 8 Stellen eingegeben werden (Parametereinstellung – Allgemeine Systemeinstellungen).
Bestätigung	Hier wird die Tür-PIN wiederholt.
mit Zeitmodell	Die Möglichkeit der alternativen PIN-Eingabe kann über ein Zeitmodell auf bestimmte Tage bzw. Tageszeiten eingeschränkt werden.

Hinweis!
Die Varianten **Identifikations-** und **Tür-PIN** können bei Türmodellen mit EMA-/GMA-Scharfschaltung (Türmodelle 10 und 14) nicht verwendet werden.

Hinweis!
Gruppenbegehung an einem Leser mit Tastatur funktioniert nicht gemeinsam mit der PIN-oder-Ausweis-Funktion.

Siehe auch

– *Konfigurieren von Bedrohungsalarmen, Seite 99*

6.3 Büromodus

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

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

So geht es weiter:

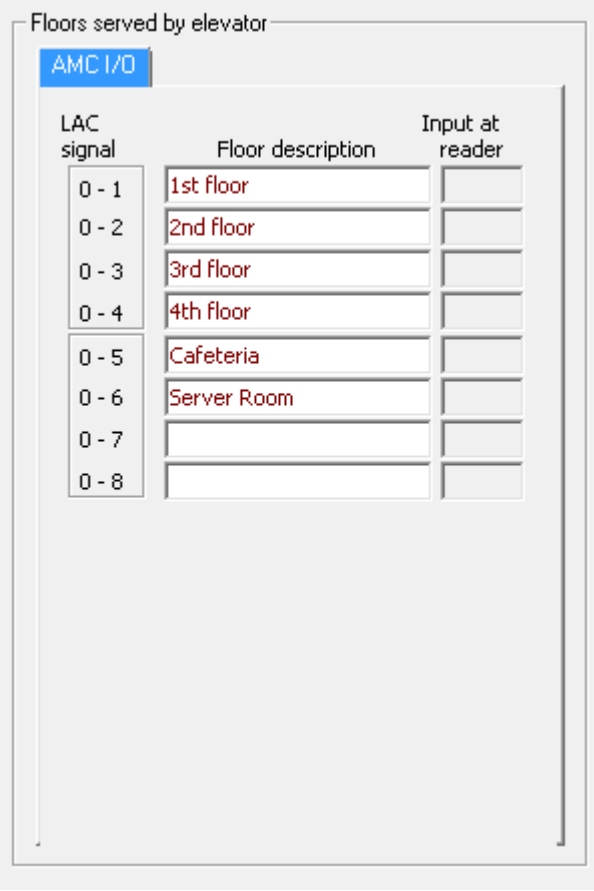
- Drücken Sie die Taste „3” auf dem Tastenfeld des Lesers.
- Halten Sie den Ausweis gegen den Leser. Die Autorisierung der Person wird überprüft.
- Liegt eine Berechtigung vor, wird der Türzustand auf „dauerhaft geöffnet” geändert.
- Der Türzustand wird bei jeder Ausführung der beschriebenen Schritte umgeschaltet.

Hinweis!
Die Büromodus-Option öffnet keine gesperrte Tür.
Wenn der Büromodus bei einer bestimmten Tür konfiguriert ist, darf für diese Tür kein Zeitmodell konfiguriert werden.

6.4 Türmodelle mit Besonderheiten

Türmodelle mit Besonderheiten
Einige Türmodelle erfordern besondere Angaben zu ihrer Einrichtung oder spezielle Verfahrensweisen zu ihrer Verwendung.

Türmodell 07 – Aufzug
Bei Auswahl dieses Türmodells wird der Dialog um Eingabefelder erweitert, die die Einrichtung von Etagen ermöglichen.



Standardmäßig kann ein AMC2 für acht Etagen verwendet werden. Unter den folgenden Voraussetzungen kann diese Anzahl erhöht werden:

– 64 Etagen bei Verwendung von Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)
– 56 Etagen bei Verwendung von RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

Die hier definierten Etagen können als Zutrittsberechtigungen vergeben werden.

Türmodell 14 – Tür mit EMA-Steuerung

Diese Türmodelle werden wie alle anderen auch angelegt, nur dass hier neben der Zutrittsberechtigung für den Eingang Berechtigungen für die Scharf- und Unscharfschaltung eingerichtet werden. Diese Berechtigungen werden in der Regel getrennt zugewiesen.

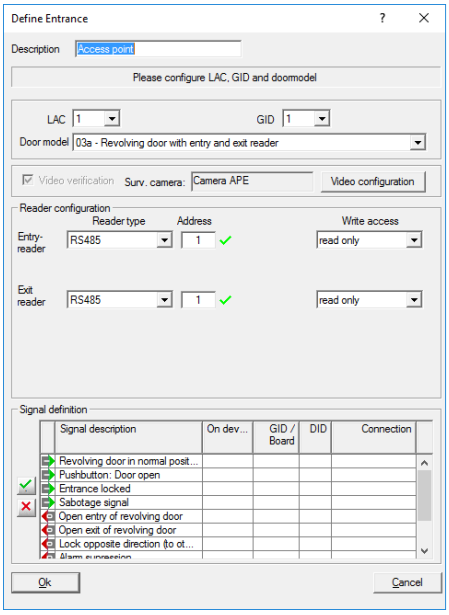
6.5 Zuweisen von Videogeräten zu einem Durchtritt

Der Dialog zur Erstellung von Durchtritten bietet ebenfalls eine Option zur Einrichtung der Kameras an diesem Durchtritt.

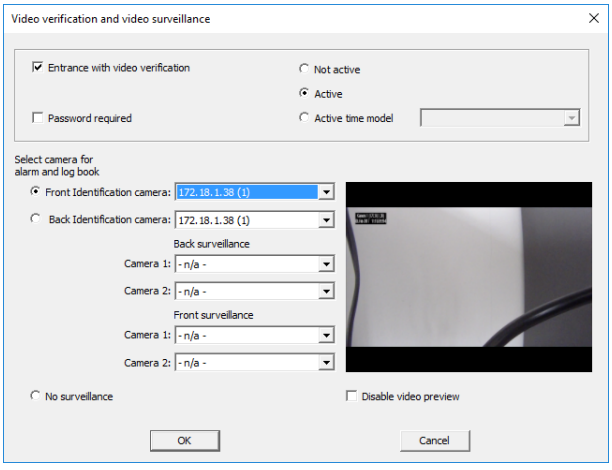
Um die Optionen für die **Videoverifikation** zu aktivieren und festzulegen, können Sie in einem speziellen Dialog, der durch Klicken auf die Schaltfläche **Videokonfiguration** geöffnet wird, Änderungen vornehmen und andere Einstellungen konfigurieren. Gehen Sie wie folgt vor:

– Aktivieren Sie das Kontrollkästchen **Videoverifikation** für die Leser, die dem Durchtritt zugeordnet sind.
– Klicken Sie auf  oder doppelklicken Sie unter **Durchtritte** auf den ausgewählten LAC.

Der folgende Bildschirm wird angezeigt:

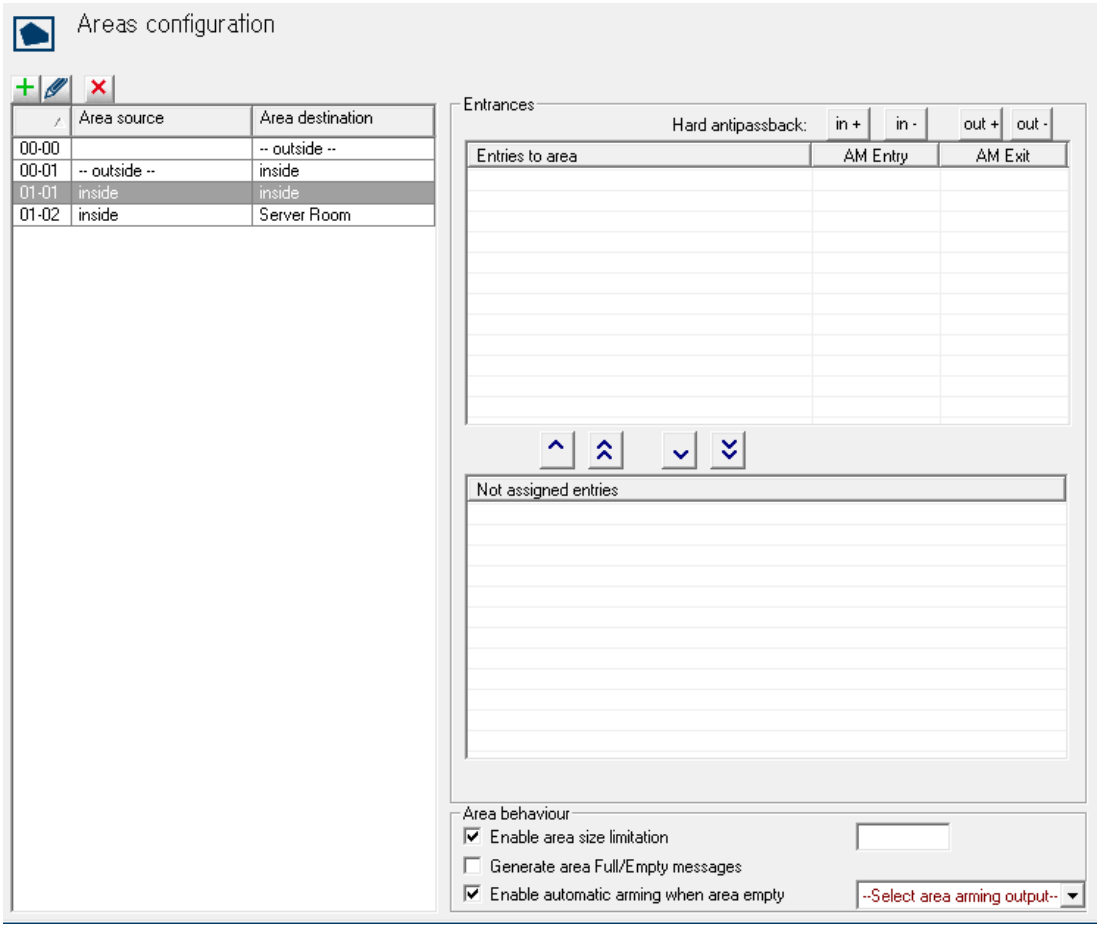


Klicken Sie auf die Schaltfläche **Videokonfiguration**, um den Konfigurationsbildschirm zu starten:



7 Raumzonen

Die Raumzonenkonfiguration ermöglicht sowohl die Ortsverfolgung von Personen als auch die Überwachung der korrekten Zutrittsfolge. Damit kann verhindert werden, dass eine Person eine Raumzone auf unzulässigen Wegen betritt. In der Regel kommt diese Funktion nur bei Bereichen mit erhöhten Sicherheitsanforderungen zum Einsatz.



Auf der linken Seite werden alle bereits eingerichteten Raumzonen in einer Liste angezeigt.
Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

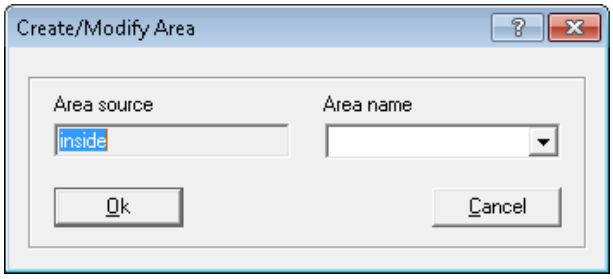
 Eine neue Raumzone **hinzufügen**

 Eine Raumzone **bearbeiten**

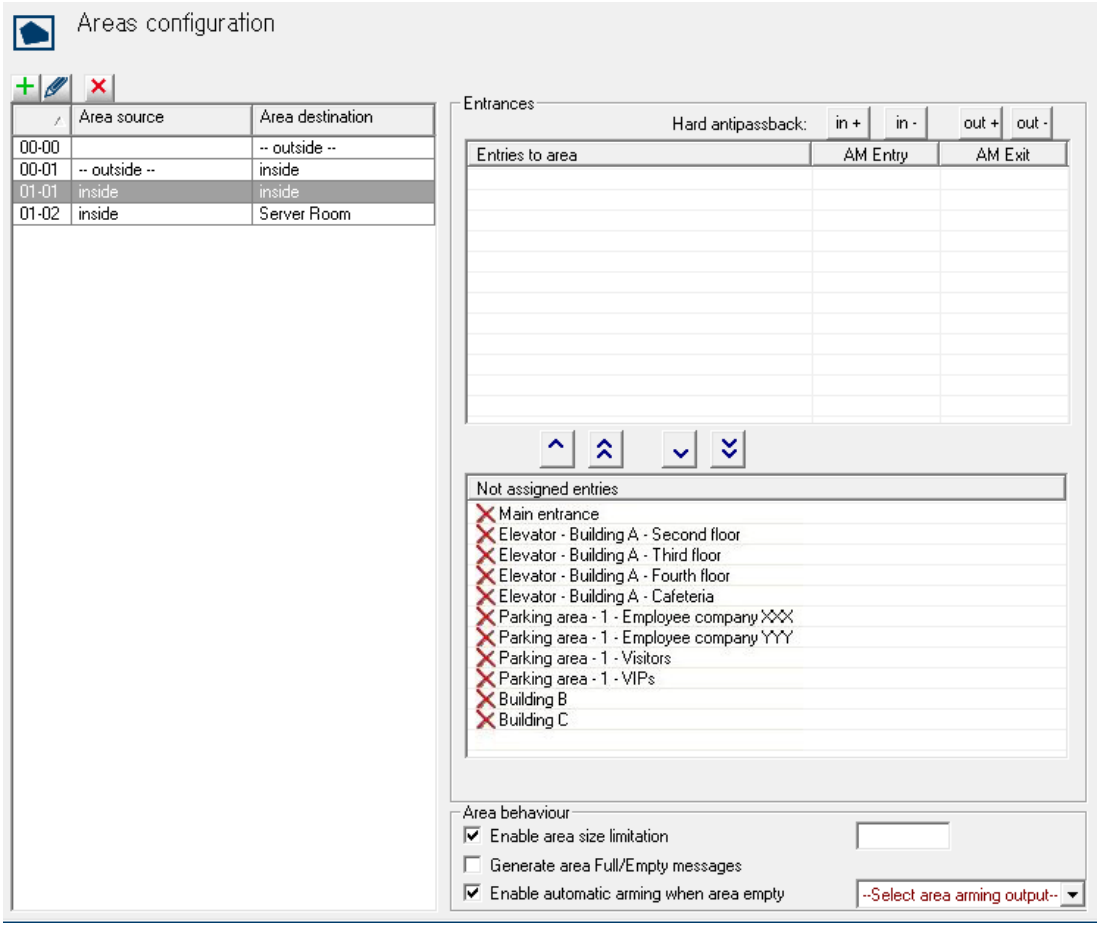
 Eine Raumzone **löschen**

Standardmäßig wird bei der Installation die Raumzone **--außerhalb--** angelegt. Dieser Raumzone können keine Eingänge zugewiesen werden, da sie mit dem nicht überwachten Bereich zusammenfällt.
Ausgehend von dieser vorinstallierten Raumzone können nun weitere Bereiche definiert werden. Diese Raumzonen müssen nicht mit tatsächlichen Gegebenheiten übereinstimmen, sondern sind rein virtueller Natur. Diese Bereiche können ein oder mehrere Gebäude (z. B. Raumzone Firma XXX) oder auch nur einzelne Etagen oder Räume umfassen.

Hinweis!
Neue Raumzonen werden immer anhand vorhandener Listeneinträge angelegt. Die Raumzone eines selektierten Listeneintrags wird zur **Quellzone** der neuen Raumzone. Diese Voreinstellung kann nicht geändert werden, sodass beim Neuanlegen von Raumzonen darauf zu achten ist, dass der Listeneintrag mit der Raumzone, die zur **Quellzone** werden soll, selektiert wurde.

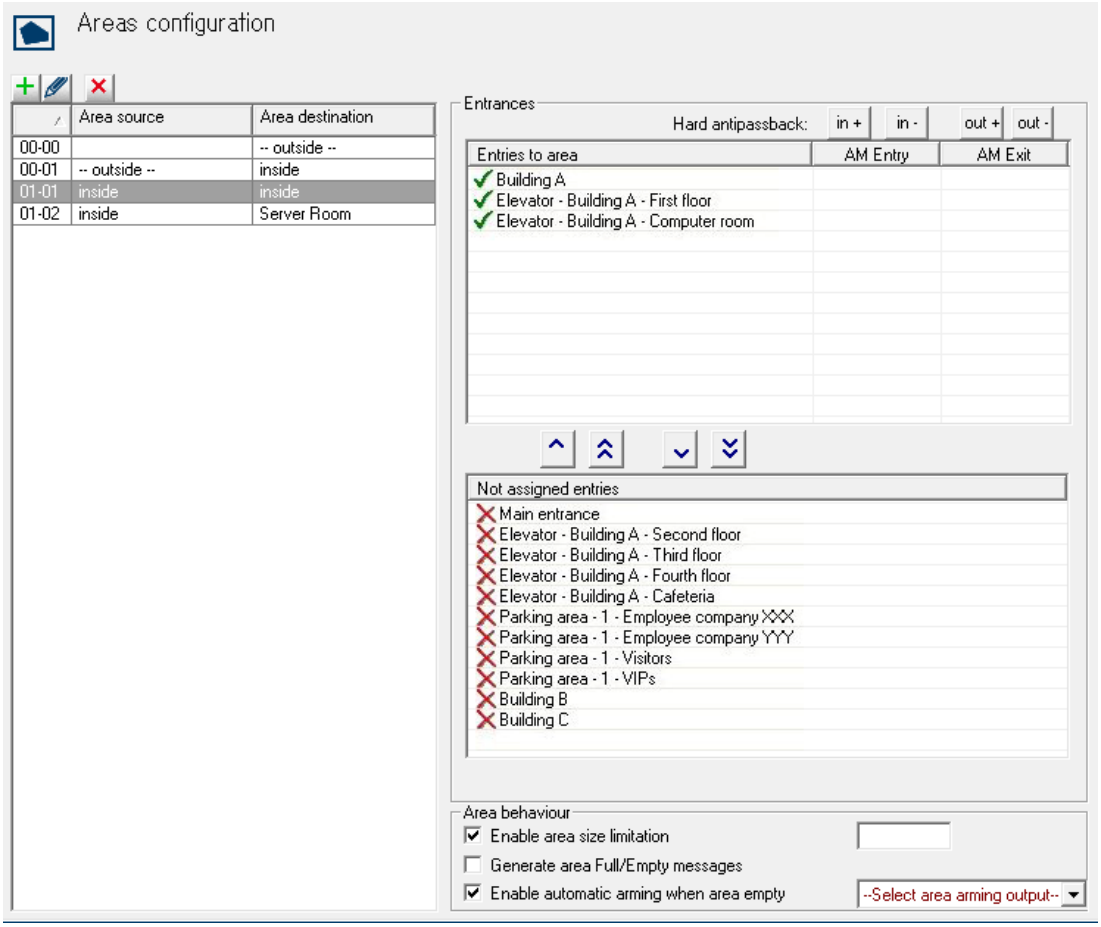


Die Bezeichnung der Raumzone kann aus einer Liste der bereits eingerichteten Raumzonen selektiert oder als Neueintrag angegeben werden.
Raumzonen müssen so konfiguriert werden, dass die lückenlose Begehung (ohne fehlende Eingänge) von einer Raumzone zur nächsten gewährleistet ist.
Beispiel:
Von der vordefinierten Raumzone **--außerhalb--** gelangt man über den Haupteingang zur Raumzone **Empfang** und von dort zu den Gebäuden A, B und C. Somit müssen Raumzonen in Access PE eingerichtet werden, die von der **Quellzone Empfang** zu den Gebäuden A, B und C führen.
Nach dem Anlegen einer Raumzone muss dieser mindestens ein Eingang zugewiesen werden. Zum Betreten einer Raumzone ist mindestens ein Eingangsleser erforderlich. Dazu stehen im rechten Bereich des Dialogs zwei Listenfelder zur Verfügung.



Im Listenfeld **NICHT zugeordnete Eingänge** sind alle verfügbaren, d. h. noch keiner Raumzone zugewiesenen, Eingänge aufgeführt. Der Eingang wird der in der linken Liste selektierten Raumzone per Doppelklick auf den gewünschten Eintrag oder über die Schaltfläche zugewiesen. Die Schaltfläche fügt alle Einträge der unteren Liste der oberen zu.

Über einen Doppelklick in die obere Liste oder die Schaltfläche kann eine solche Zuweisung für die ausgewählte Raumzone wieder rückgängig gemacht werden. Ein Klick auf die Schaltfläche macht alle Zuweisungen rückgängig.



Hinweis!
Ein Eingang kann nur einer Raumzone zugewiesen werden.
Haben Sie bestimmte Eingänge einer Raumzone zugewiesen, enthält die Liste der **NICHT zugeordneten Eingänge** diese Einträge bei Einrichtung weiterer Raumzonen nicht mehr.

Die Spalten **AM Entry** (Zutrittsüberwachung Eingang) und **AM Exit** (Zutrittsüberwachung Ausgang) beziehen sich auf die Zutrittsüberwachung. Wenn Sie in Ihrem System die Zutrittsüberwachung nutzen möchten, müssen Sie die Eingangs- und/oder Ausgangsleser entsprechend aktivieren.

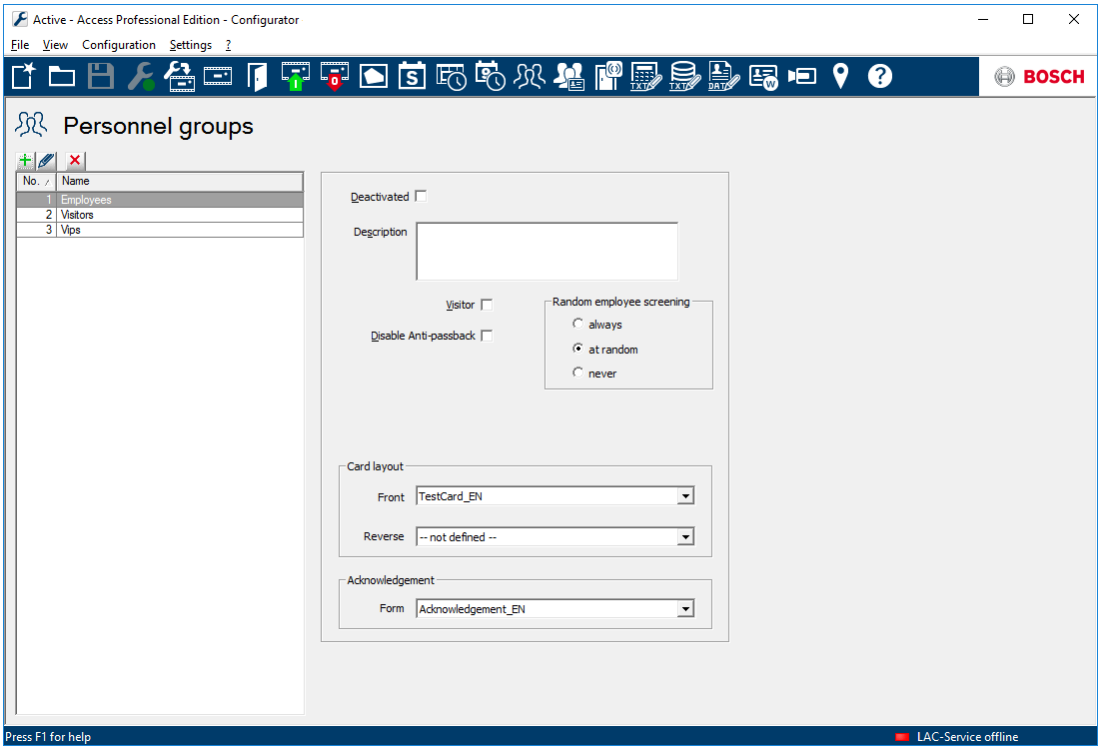
– Wählen Sie in der Liste **Eingänge zu Raumzone** den betreffenden Eintrag, und aktivieren Sie diesen über die Schaltfläche in + als Eingangsleser bzw. über out + als Ausgangsleser, um die Zutrittsüberwachung zu aktivieren. Aktivierte Leser können über die Schaltflächen in - und out - wieder deaktiviert werden.

Diese Funktionen können auch über die Kontextmenüs (rechte Maustaste) der Listeneinträge aufgerufen werden.

Hinweis!
Kontrollen, die über die Basisprüfungen von Berechtigungen und Zeitmodellen hinausgehen (z. B. Zutrittsfolgekontrolle, Doppelzutrittssperre, zufällig Personenkontrolle), werden vom LAC-Subsystem-Prozess durchgeführt. Zur Gewährleistung dieser Funktionen muss der Access PE-Server ständig laufen (24 Stunden/Tag und 7 Tage/Woche).

8 Personalgruppen

Personalgruppen dienen der sinnvollen Strukturierung Ihres Unternehmens. Diese Definition kann unter anderem für die Vergabe von Standard-Zutrittsberechtigungen bei der Neueingabe von Personen genutzt werden.



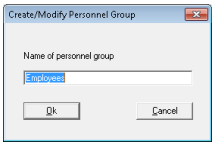
Auf der linken Seite werden alle bereits eingerichteten Personalgruppen in einer Liste angezeigt.
Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

Eine neue Personalgruppe **hinzufügen**

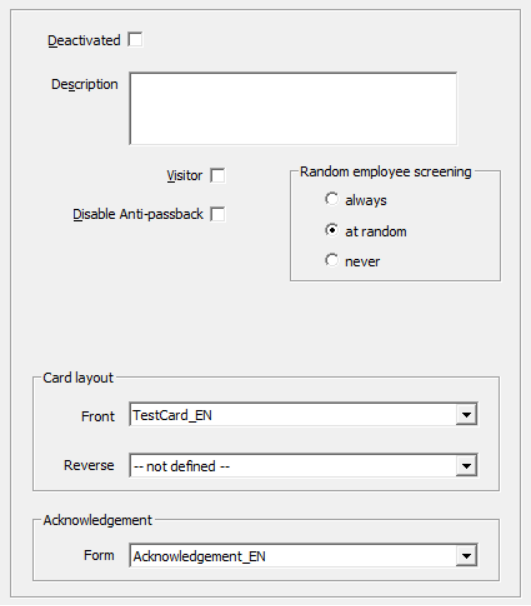
Die selektierte Personalgruppe **bearbeiten**

Die selektierte Personalgruppe **löschen**

Das System wird mit den vordefinierten Personalgruppen **Personal** und **Besucher** installiert. Diese entsprechen auch den Filtermöglichkeiten in der **Personalverwaltung** von Access PE.



Auf diese Weise können Sie das Personal differenzieren (z. B. Angestellte, Arbeiter, Reinigungspersonal) und diesen Gruppen im Dialog **Zutrittsberechtigungsgruppen** Standardberechtigungen zuweisen. Beim Neuanlegen von Personendaten werden mit der Auswahl einer dieser Personalgruppen automatisch die Standardberechtigungen zugewiesen.



Zur selektierten Personalgruppe können auf der rechten Dialogseite folgende Angaben festgelegt werden:

Einstellungen	Beschreibung
Deaktiviert	Mit der Deaktivierung einer Personalgruppe wird das Löschen der betreffenden Gruppe vorbereitet. Diese Personalgruppe kann dann keiner Person mehr zugeordnet werden, ist aber weiter vorhanden. **Eine Personalgruppe sollte erst dann gelöscht werden, wenn dieser Gruppe keine Person mehr zugeordnet ist.**
Beschreibung	Zu jeder Personalgruppe können Sie eine ausführliche Beschreibung hinterlegen.
Besucher	Zusätzlich kann die Personalgruppe als Besucher klassifiziert werden. Die Listenansicht der **Personalverwaltung** kann über die Filter **alle Personen**, **Personal** und **Besucher** angepasst werden. Personalgruppen, die hier als **Besucher** gekennzeichnet werden, lassen sich dann getrennt vom Filter **Personal** anzeigen.
Zutrittswiederholsperre deaktivieren	Eine bestimmte Personengruppe (z. B. VIPs) kann von der Zutrittswiederholsperre ausgeschlossen werden.

Einstellungen	Beschreibung
Personenkontrolle: – immer – zufällig – nie	Diese Option gilt nur für Leser, die als Auswahlleser für die zufällige Personenkontrolle eingerichtet wurden. Die Optionen haben folgende Bedeutung: = Es findet eine 100%ige Kontrolle statt. = Es erfolgt eine Kontrolle entsprechend der angegebenen Zufallsrate. = Diese Personalgruppe wird nie kontrolliert.
Ausweislayout Vorderseite Rückseite	Beim Erstellen von Ausweisen muss ein Layout ausgewählt werden. Für jede Personalgruppe können spezielle Layouts erstellt und zugewiesen werden. Die Auswahl eines Layouts für die Rückseite ist optional.
Empfangsbestätigung **Formular**	Die Ausgabe eines Ausweises kann ggf. nur gegen die Unterzeichnung einer Empfangsbestätigung erfolgen. Für jede Personalgruppe kann diese unterschiedlich gestaltet sein und hier zugewiesen werden.

8.1 Gruppenbegehung bei Lesern mit Tastatur

Wie in der Onlinehilfe des Configuration Browser beschrieben, kann jeder Ausweisleser so konfiguriert werden, dass er erst den Zutritt gewährt, wenn eine bestimmte Anzahl an Ausweisen mit geeigneter Berechtigung eingelesen wurde. Diese Funktion wird als „Gruppenbegehung” bezeichnet.
Der Vorgang der Gruppenbegehung variiert abhängig von der Ausweisleserart leicht. Leser mit Tastatur erlauben grundsätzlich auch den Durchtritt von mehr Gruppenmitgliedern als vorher konfiguriert, erfordern aber einen zusätzlichen Tastendruck zur Bestätigung, dass die Gruppe vollständig ist.

Leser ohne Tastatur:
- Einlesen der genauen konfigurierten Anzahl an autorisierten Ausweisen am Leser
- Zutritt wird gewährt

Leser mit Tastatur (außer IBPR):
- Einlesen der konfigurierten Mindestanzahl an autorisierten Ausweisen am Leser
- Optional: Einlesen weiterer Ausweise
- Druck auf die Eingabetaste oder Taste „#” am Leser
- Zutritt wird gewährt

IBPR-Leser mit Tastatur:
- Einlesen der konfigurierten Mindestanzahl an autorisierten Ausweisen am Leser
- Optional: Einlesen weiterer Ausweise
- Druck auf die Eingabetaste oder Taste „0” am Leser
- Druck auf die Eingabetaste oder Taste „#” am Leser

– Zutritt wird gewährt

8.2 Einschränkungen der Gruppenbegehung

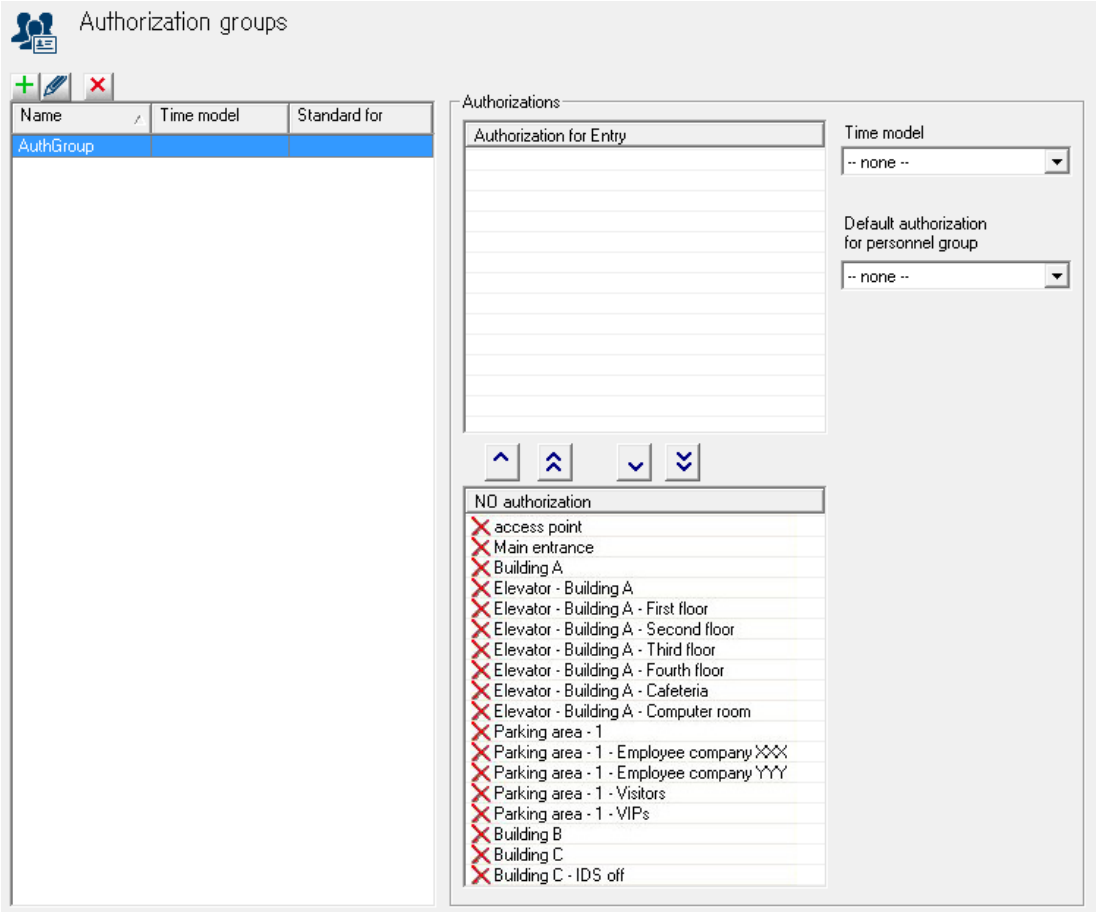
– Die Gruppenbegehung kann nur für die Türmodelle 1 und 3 konfiguriert werden.
– Gruppenbegehung und die Begrenzung der Anzahl an Personen in einem Bereich kann dazu führen, dass sich mehr Personen als erlaubt in einem Bereich aufhalten. Nachdem die gesamte Gruppe den Bereich betreten hat, wird die Anzahl überprüft.
– Gruppenbegehung und mehrere Ausweise funktionieren mit dem Zählen von Ausweisen, aber möglicherweise nicht von eintretenden Personen.
– Gruppenbegehung an einem Leser mit Tastatur funktioniert nicht gemeinsam mit der PIN-oder-Ausweis-Funktion (jede Konfiguration erfordert dieselbe Bestätigung).

9 Zutrittsberechtigungsgruppen

Zutrittsberechtigungsgruppen erleichtern die administrativen Aufgaben des Systembetreuers und -bedieners, indem einzelne Eingänge, die in ihren Zutrittsanforderungen (Personenkreis, zeitliche Begrenzung usw.) ähnlich sind oder die räumlich eng zusammen- oder nebeneinanderliegen, in beliebiger Anzahl zu Gruppen zusammengefasst werden können. Sie können dann in einem einzigen Arbeitsschritt Personen zugewiesen werden.

9.1 Anlegen und zuweisen

Mit der Definition von **Zutrittsberechtigungsgruppen** können einzelne Eingänge zu Gruppen zusammengefasst werden. Die Vergabe von Zutrittsberechtigungen in der **Personalverwaltung** erfolgt dann durch die Zuordnung einer oder mehrerer solcher Gruppen.



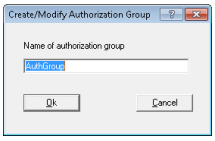
Auf der linken Seite werden alle bereits eingerichteten Zutrittsberechtigungsgruppen in einer Liste angezeigt.
Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

Eine neue Zutrittsberechtigungsgruppe **hinzufügen**

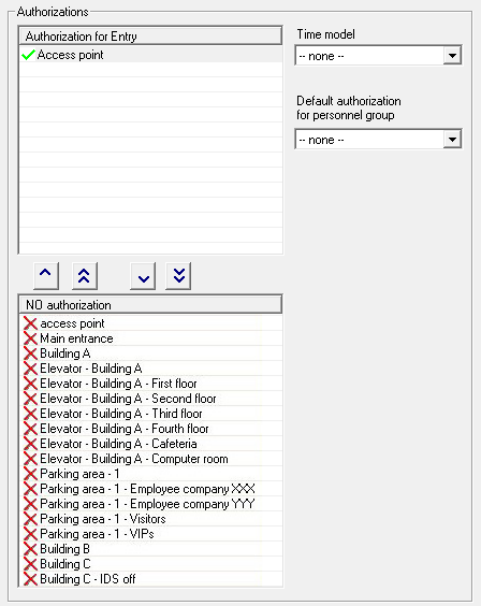
Die selektierte Zutrittsberechtigungsgruppe **bearbeiten**

Die selektierte Zutrittsberechtigungsgruppe **löschen**

Über die Schaltfläche wird ein Dialog zur Angabe der Bezeichnung für eine neue Zutrittsberechtigungsgruppe geöffnet.

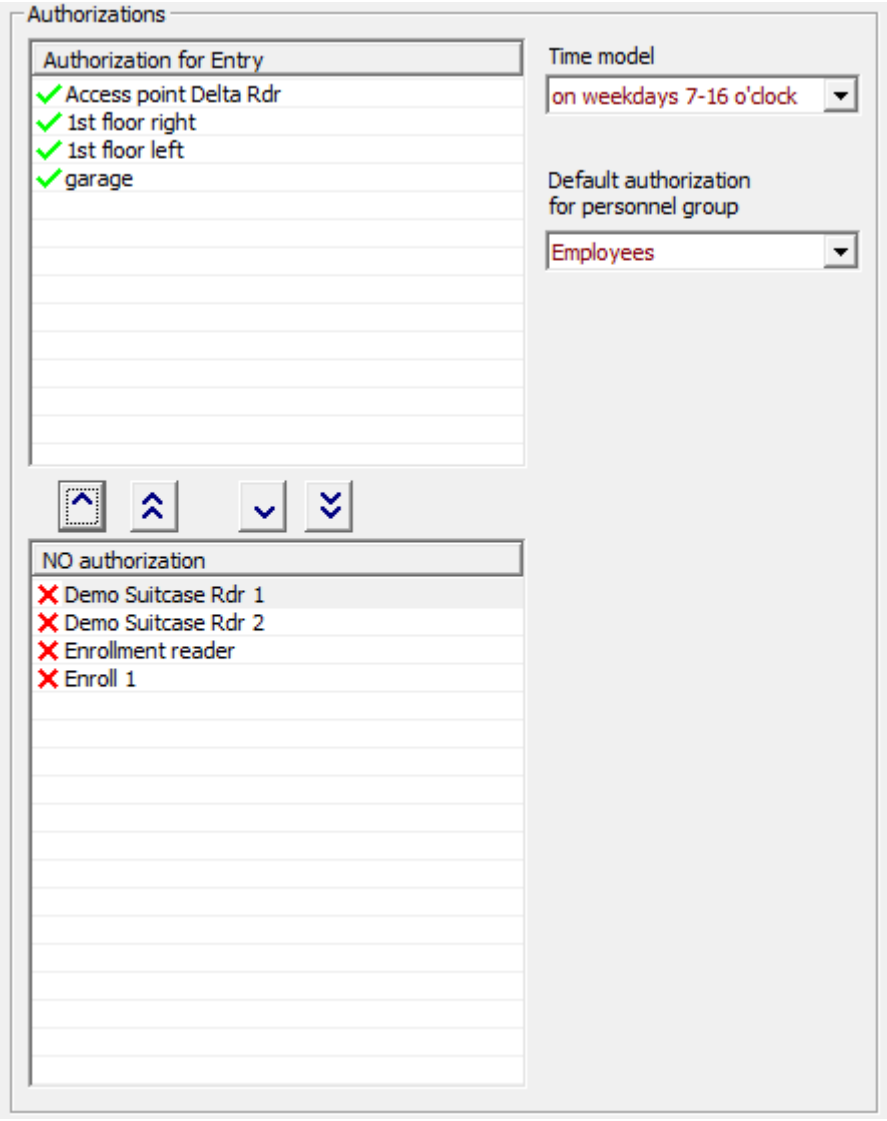


Dem selektierten Listeneintrag können anschließend auf der rechten Dialogseite Eingänge zugewiesen werden.



Die verfügbaren Eingänge werden in der Liste **KEINE Berechtigung** aufgeführt, d. h. Eingänge, die noch keiner Zutrittsberechtigungsgruppe zugewiesen wurden. Der Eingang wird der in der linken Liste selektieren Zutrittsberechtigungsgruppe per Doppelklick auf den gewünschten Eintrag oder über die Schaltfläche zugewiesen. Die Schaltfläche fügt alle Einträge der unteren Liste der oberen zu. Über die Schaltflächen und kann eine solche Zuweisung zu Raumzonen wieder rückgängig gemacht werden.

Vorsicht!
Nachträgliche Änderungen bei der Zuweisung von Eingängen und Zeitmodellen wirken sich auch auf bereits zugewiesene Berechtigungen aus.



Jeder Gruppe kann ein **Zeitmodell** zugeordnet werden, das die Gültigkeit der Berechtigungen eingeschränkt. Beachten Sie die **Anwendung von Zeitmodellen** (*Zeitmodelle, Seite 75*) in Access PE.

Hinweis!
Markieren Sie Zutrittsberechtigungsgruppen, denen Sie Zeitmodelle zugewiesen haben, in den Bezeichnungen, indem Sie z. B. den Zusatz **ZM** verwenden. Bei der Zuweisung in der **Personalverwaltung** sind diese dann besser von unbeschränkten Berechtigungen zu unterscheiden.

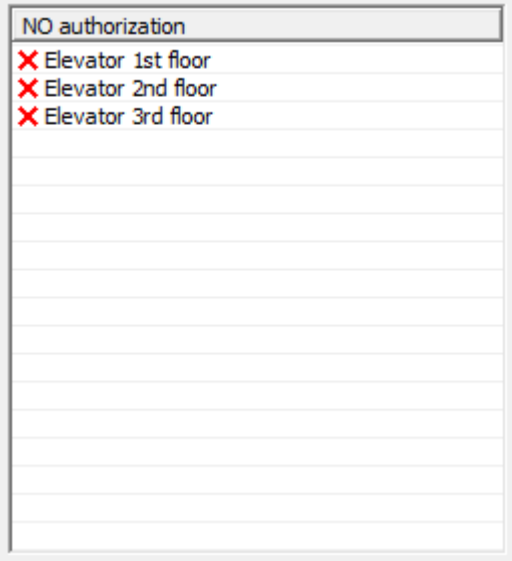
Zusätzlich kann eine Gruppe als **Standardberechtigung** für eine **Personalgruppe** (z. B. Mitarbeiter oder Besucher) definiert werden. Die Zutrittsberechtigungsgruppe wird dann bei der Neueingabe einer Person in der **Personalverwaltung** entsprechend der gewählten Personengruppe zugewiesen.

9.2 Spezielle Berechtigungen

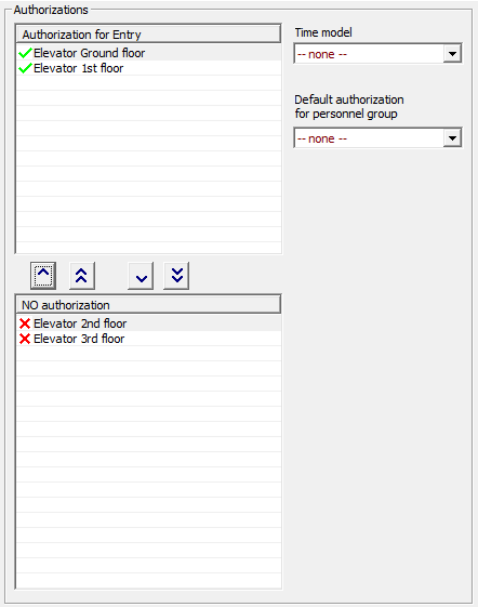
Für die Türmodelle 07 und 14 müssen bereits beim **Konfigurieren** zusätzliche Angaben (*Türmodelle mit Besonderheiten, Seite 53*) gemacht werden. Aber auch in Bezug auf ihre Zuweisung und Nutzung als Berechtigung unterscheiden sie sich von den übrigen Türmodellen.

Türmodell 07 – Aufzug

Die Liste der verfügbaren Berechtigungen enthält für den Aufzug und für jede definierte Etage einen eigenen Eintrag.

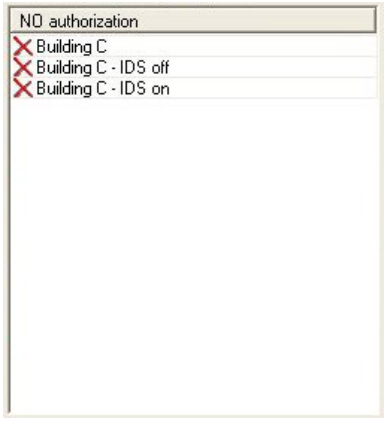


Bei der Zusammenstellung von Zutrittsberechtigungsgruppen müssen ein Leser für den **Aufzug** und **mindestens eine Etage** zugewiesen werden.

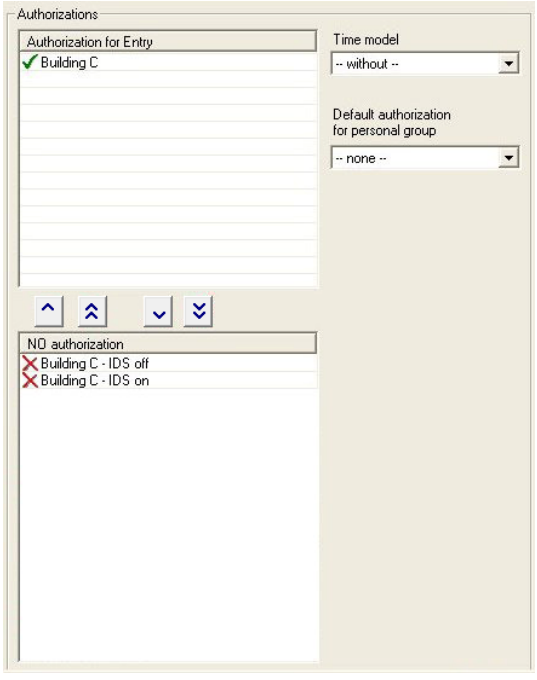


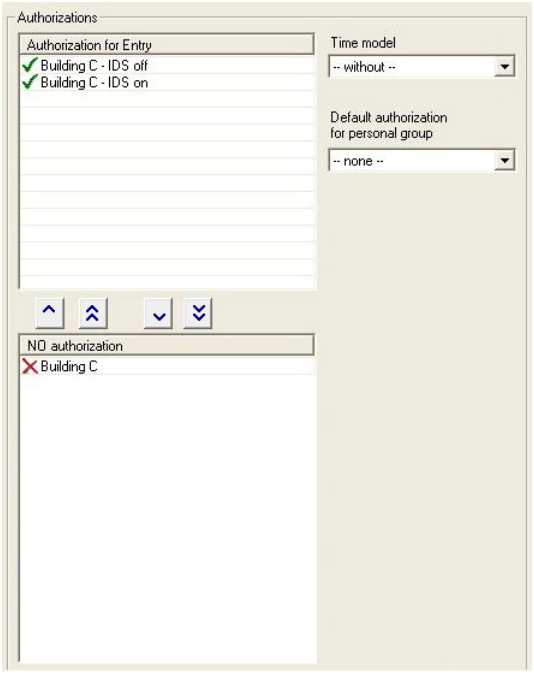
Türmodell 14: EMA-Scharfschaltung

In der Liste der verfügbaren Berechtigungen ist für den Eingang und für die Scharf- sowie die Unscharfschaltung je ein Eintrag vorhanden.



Diese Berechtigungen werden unabhängig voneinander zugewiesen. Wird nur die Berechtigung für den Eingang zugewiesen, kann die betreffende Person keine Scharf- oder Unscharfschaltungen der EMA (Einbruchmeldeanlage) vornehmen, sondern lediglich den Durchtritt benutzen.
Werden dagegen nur die Scharf- und/oder Unscharfschalteberechtigungen zugewiesen, kann die betreffende Person zwar scharf- und unscharfschalten, jedoch nicht den Durchtritt benutzen.



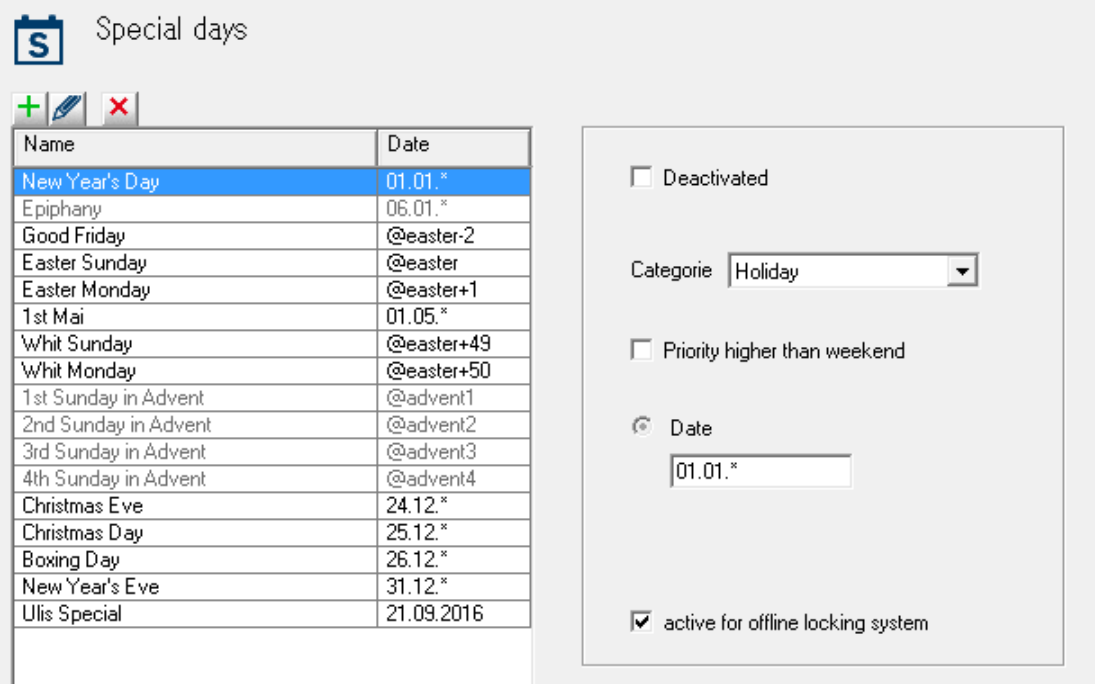

Authorizations
Authorization for Entry
Building C - IDS off
Building C - IDS on
Time model
-- without --
Default authorization for personal group
-- none --
NO authorization
Building C

10 Feier- und Sondertage

Die in diesem Dialog definierten Tage erhalten eine abweichende Regelung von dem Wochentag, auf den sie fallen. Statt des für den Wochentag geplanten Tagesmodells wird das dem Feier-/Sondertag zugewiesene Tagesmodell verwendet.
Die vorkonfigurierte Liste kann nach Belieben geändert und ergänzt werden. Nicht benötigte Feier-/Sondertage können deaktiviert oder gelöscht werden, sodass an diesen Tagen das normale Tagesmodell des jeweiligen Wochentags gilt. Nicht vorhandene und kundenspezifische Feier-/Sondertage können hinzugefügt und individuell definiert werden. Dadurch wird erreicht, dass die Perioden der Zeitmodelle klein gehalten werden und nur Tage umfassen, die in ihrer Abfolge voneinander abweichen, sodass der Kalender von Periode zu Periode und von Jahr zu Jahr fortgeschrieben werden kann.

10.1 Anlegen und ändern

Die in Deutschland geltenden Feiertage sind in Access PE bereits vorkonfiguriert. Diese können, falls sie für bestimmte Bundesländer nicht gelten, deaktiviert werden.



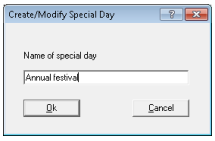
Hinweis!
Die Anzahl der Elemente für Offline-Schließanlagen ist auf ## begrenzt.

Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

- Einen neuen Feiertag/Sondertag **anlegen**
- Den selektierten Feiertag/Sondertag **bearbeiten**
- Den selektierten Feiertag/Sondertag **löschen**

Hinweis!
Es wird empfohlen, die vorkonfigurierten Feier- und Sondertage mit **variablem Datum** nicht zu löschen, sondern zu deaktivieren, wenn sie nicht verwendet werden sollen. Feier- und Sondertage mit variablen Daten können später nicht mehr per Dialog angelegt werden.

Über die Schaltfläche  , wenn Sie einen weiteren Feier- oder Sondertag hinzufügen wollen, oder  , wenn Sie die Bezeichnung eines bestehenden Listeneintrags ändern möchten, wird zunächst ein Dialogfenster zur Angabe der Feiertagsbezeichnung eingeblendet:



Mit der Bestätigung der Angaben über die Schaltfläche OK wird die geänderte oder neue Bezeichnung im Listenfeld angezeigt. Die Parameter des ausgewählten Listenelements können rechts neben dem Listenfeld festgelegt werden.

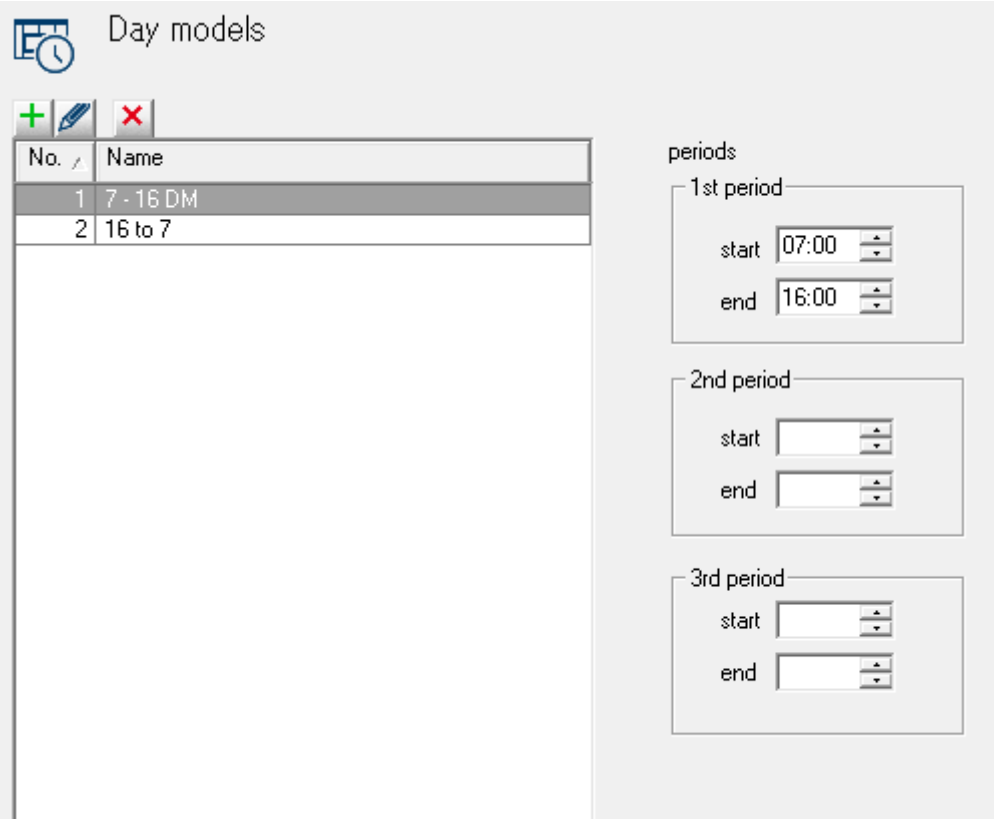
Deaktiviert	Damit legen Sie fest, ob der Feier-/Sondertag im Kalender berücksichtigt wird oder nicht.
Kategorie	Sie können die aktiven Feier-/Sondertage in 11 Kategorien (Feiertag, Sondertag Typ 1 bis 10) unterteilen und bei der Erstellung der Zeitmodelle jeder Kategorie spezielle Tagesmodelle zuweisen.
Höhere Priorität als Samstag/ Sonntag	Damit legen Sie fest, was passieren soll, wenn ein jährlich wiederkehrender Feiertag auf einen Samstag oder Sonntag fällt. Ist die Option aktiviert, gilt auch an Samstagen/ Sonntagen das Tagesmodell, das dem Feiertag zugeordnet ist, im anderen Fall hat das Tagesmodell für Samstag/Sonntag Vorrang.
Datum	Handelt es sich um einen jährlich an einem bestimmten Datum wiederkehrenden Feiertag, müssen Sie statt einer Jahreszahl einen * eingeben. Bestimmte Feier-/Sondertage (z. B. Weihnachten) haben immer feste Daten.

11 Tagesmodelle

Tagesmodelle regeln einen fiktiven Tagesablauf. Ein Tagesmodell gibt an, zu welchen Tageszeiten Zutritt gewährt werden soll bzw. nicht, ohne dass ein konkreter Wochentag definiert wird.
Es muss also für jeden abweichenden Tagesablauf ein eigenes Tagesmodell erstellt werden.
Zur Definition können 3 Intervalle mit Anfangs- und Endzeiten verwendet werden.
Mit der Verwendung von Tagesmodellen in den Zeitmodellen werden die Tagesmodelle konkreten Tagen der Periode zugeordnet.

11.1 Anlegen und ändern

Dieser Dialog dient zum Anlegen und Bearbeiten von Tagesmodellen, die selbst in Zeitmodellen verwendet werden.



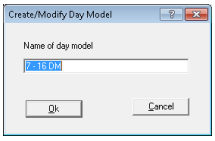
Auf der linken Seite werden alle eingerichteten Tagesmodelle in einer Liste angezeigt.
Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

 Ein neues Tagesmodell **anlegen**

 Das selektierte Tagesmodell **bearbeiten**

 Das selektierte Tagesmodell **löschen**

Zum Ändern der Bezeichnung eines selektierten Tagesmodells betätigen Sie die Schaltfläche  und zum Neuanlegen  :



Mit der Bestätigung der Angaben über die Schaltfläche **OK** wird die geänderte oder neue Bezeichnung im Listenfeld angezeigt. Dafür können auf der rechten Seite nun die Zeitintervalle angegeben werden, die für dieses Tagesmodell gelten sollen. Der mit einem Tagesmodell festgelegte Tagesablauf kann in bis zu 3 Intervalle unterteilt werden.
Die Startzeit eines Intervalls (von) muss kleiner als die Endzeit (bis) sein. Wenn Sie also Modelle erstellen möchten, die über Mitternacht hinausgehen, müssen Sie 2 Intervalle definieren:

1. Intervall: von: ... bis: 24:00
2. Intervall: von: 00:00 bis: ...

12 Zeitmodelle

Über Zeitmodelle wird der generelle Zutritt an den zugewiesenen Durchtritten auf bestimmte Tageszeiten eingeschränkt. Dies bietet die Möglichkeit, z. B. während der Nachtstunden oder an Wochenenden erteilte Berechtigungen zu entziehen oder nur mit zusätzlichen Kontrollverfahren zu erlauben.
Zeitmodelle können in Access PE an mehreren Stellen eingesetzt werden, z. B. in Verbindung mit:

– **Zutrittsberechtigungsgruppen**:

Zeitmodelle können bestimmten Zutrittsberechtigungen zugewiesen werden, sodass die Benutzung der in diesen Berechtigungen enthaltenen Durchtritte nur zu den Zeiten erlaubt ist, die im Zeitmodell freigegeben sind. Gleichzeitig können auch Zutrittsberechtigungen ohne zeitliche Begrenzungen verwendet werden.

– **Personen**:

Zeitmodelle, die Personen zugewiesen werden, beschränken die generelle Benutzung des Ausweises auf die freigegebenen Zeiten.

– **Controller und Erweiterungsplatinen**:

Die Meldungsgenerierung der Eingangs- und Ausgangssignale durch Controller und Erweiterungsplatinen kann ebenfalls über Zeitmodelle geregelt werden.

– **Türen**:

Die Türfreigabe kann über Zeitmodelle gesteuert werden.

– **PIN-Code**:

Die Eingabe eines PIN-Codes als zusätzlicher Kontrollmechanismus kann neben der generellen Anforderung auch nur zu den Zeiten verlangt werden, die außerhalb der Zeiten des Zeitmodells liegen.

– **Zuschaltung des Motorschlosses**:

Ein Motorschloss wird über die Zuweisung eines Zeitmodells zu den dort angegebenen Zeiten aktiviert.

Je nach ihrer Verwendung müssen Zeitmodelle unterschiedlich erstellt werden, da die definierten Zeiten die jeweiligen Funktionen aktivieren.

Beispiel:

Werden Zeitmodelle für Zutrittsberechtigungen oder Personen verwendet, mit denen der Zutritt an Wochentagen von 07:00 bis 19:00 Uhr und an Wochenenden von 09:00 bis 15:00 Uhr erlaubt werden soll, werden 2 Tagesmodelle benötigt:

1. Mit dem Intervall von 07:00 bis 19:00 Uhr
2. Mit dem Intervall von 09:00 bis 15:00 Uhr

Soll dagegen die Zuschaltung des Motorschlosses mittels Zeitmodell in der Form geregelt werden, dass außerhalb der oben angegebenen Zeiten das Motorschloss aktiviert wird, müssen die Tagesmodelle dieses Zeitmodells folgendermaßen eingerichtet werden:

1. Mit den Intervallen 00:00 bis 07:00 Uhr und 19:00 bis 24:00 Uhr
2. Mit den Intervallen 00:00 bis 09:00 Uhr und 15:00 bis 24:00 Uhr

Anwendung von Zeitmodellen

Zeitmodelle, die in irgendeiner Form mit Personendaten verknüpft sind, werden nur dann geprüft, wenn die entsprechende Standardeinstellung der Leser nicht geändert wurde und die Option **Zeitmodell NICHT prüfen** (*Anzeige und Parametrierung, Seite 47*) daher deaktiviert ist.
Da es aufgrund der vielfachen Verwendungsmöglichkeiten für Zeitmodelle zu Mehrfachzuweisungen kommen kann, sind diesbezüglich folgende Regeln zur Lösung von Konflikten zu beachten:

– Werden einer Person Eingänge über eine Zutrittsberechtigungsgruppe zugewiesen, die ein Zeitmodell hat, und erhält diese Person weitere Einzelberechtigungen oder Zutrittsberechtigungsgruppen ohne Zeitmodell für dieselben Eingänge, gilt die **generelle Berechtigung**, d. h., das Zeitmodell wird für die betreffenden Eingänge nicht berücksichtigt.

  Beispiel:

  Eine Person erhält folgende Berechtigungen:

  – Zutrittsberechtigung für die Eingänge A, B, C und D mit einem Zeitmodell mit dem Intervall 09:00 bis 17:00 Uhr für jeden Tag
  – Einzelzutrittsberechtigungen für die Eingänge B und D ohne Zeitmodell

Diese Person hat an den Eingängen A und C zwischen 09:00 und 17:00 Uhr und an den Eingängen B und D unbegrenzten Zutritt.

– Werden einer Person mehrere Zutrittsberechtigungsgruppen für dieselben Eingänge mit unterschiedlichen Zeitmodellen zugewiesen, wird die **Gesamtmenge** der Zeitintervalle gebildet.

  Beispiel:

  Eine Person erhält folgende Berechtigungen:

  – Zutrittsberechtigung für die Eingänge A, B, C und D mit einem Zeitmodell mit dem Intervall 07:00 bis 13:00 Uhr für jeden Tag
  – Zutrittsberechtigung für die Eingänge B, D, E und F mit einem Zeitmodell mit dem Intervall 09:00 bis 17:00 Uhr für jeden Tag

Diese Person hat an den Eingängen A und C zwischen 07:00 und 13:00 Uhr, an den Eingängen B und D zwischen 07:00 und 17:00 Uhr und an den Eingängen E und F zwischen 09:00 und 17:00 Uhr Zutritt.

– Werden einer Person Zutrittsberechtigungsgruppen mit Zeitmodellen zugewiesen, und erhält diese Person zusätzlich ein Zeitmodell für die Benutzung des Ausweises, wird die **Schnittmenge** der definierten Intervalle gebildet.

  Beispiel:

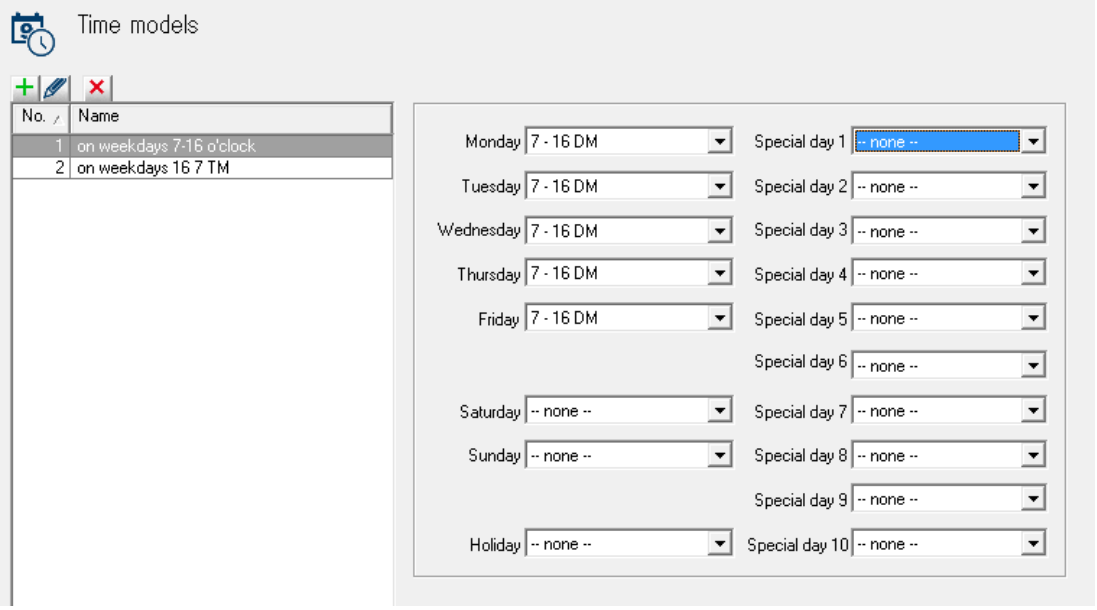
  Eine Person erhält folgende Berechtigungen:

  – Zutrittsberechtigungsgruppe mit den Eingängen A, B, C und D und einem Zeitmodell mit dem Intervall 07:00 bis 13:00 Uhr für jeden Tag
  – Zutrittsberechtigungsgruppe mit den Eingängen B, D, E und F und einem Zeitmodell mit dem Intervall 09:00 bis 17:00 Uhr für jeden Tag
  – Zusätzlich ein Zeitmodell mit dem täglichen Intervall von 11:00 bis 19:00 Uhr

Diese Person hat an den Eingängen A und C zwischen 11:00 und 13:00 Uhr und an den Eingängen B, D, E und F zwischen 11:00 und 17:00 Uhr Zutritt.

12.1 Anlegen und ändern

Mit diesem Dialog werden Zeitmodelle erstellt, die je nach Verwendung bestimmte Systemeinrichtungen aktivieren.



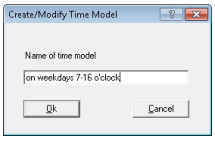
Auf der linken Seite werden alle eingerichteten Zeitmodelle in einer Liste angezeigt.
Über dem Listenfeld befinden sich die Schaltflächen für folgende Funktionen:

 Ein neues Zeitmodell **anlegen**

 Das selektierte Zeitmodell **bearbeiten**

 Das selektierte Zeitmodell **löschen**

Bei Betätigung der Schaltfläche  zum Neuanlegen oder der Schaltfläche  zum Ändern der Bezeichnung eines bestehenden Zeitmodells wird ein Dialogfenster zur Angabe einer Bezeichnung geöffnet:



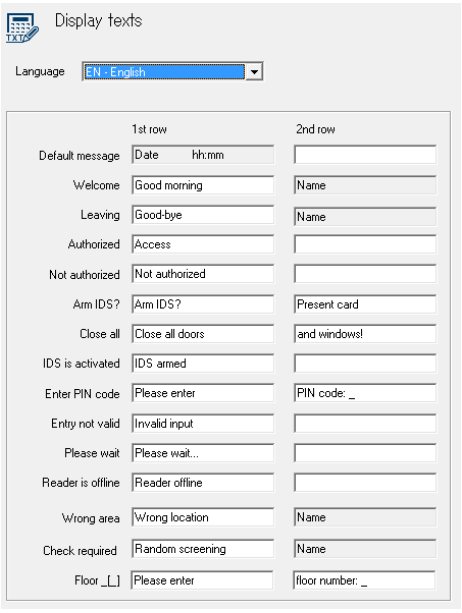
Mit der Bestätigung der Angaben über die Schaltfläche **OK** wird die geänderte oder neue Bezeichnung im Listenfeld angezeigt. Dafür können auf der rechten Dialogseite für jeden Wochentag sowie für die Kategorien Feiertag und Sondertag 1 bis 10 Tagesmodelle zugewiesen werden.
Mit den Zeitmodellen werden Perioden von einer Woche abgebildet, die sich fortlaufend wiederholen. Dabei werden die normalen Abläufe für die Wochentage durch die Zuweisung von Tagesmodellen beschrieben. Außerdem werden die definierten Feier- und Sondertage zu den angegebenen Daten berücksichtigt und dann die hier zugewiesenen Tagesmodelle für die betreffenden Wochentage verwendet.

Hinweis!
Wird bestimmten Wochentagen oder Kategorien kein eigenes Tagesmodell zugewiesen und stattdessen der Standardeintrag **--ohne--** belassen, werden diese Angaben wie Tagesmodelle ohne Intervalle behandelt, d. h., an dem betreffenden Tag wird **kein Durchtritt** gewährt.

13 Anzeige- und Meldungstexte

Für jede Applikationssprache, die bei der Installation ausgewählt wurde, existiert eine Liste mit Anzeigetexten für Displayleser sowie für die Logbuchmeldungen. Die in der jeweiligen Sprachliste enthaltenen Texte werden im Log-Viewer verwendet, z. B. für die mit Auswahl der Applikationssprache erstellten Logbuchmeldungen.

13.1 Anzeigetexte



Hinweis!
Geben Sie bei „Etage” eine einstellige Zahl ein, wenn die Anzahl der Etagen zwischen 1 und 9 liegt. Geben Sie ab 10 Etagen eine zweistellige Zahl ein.

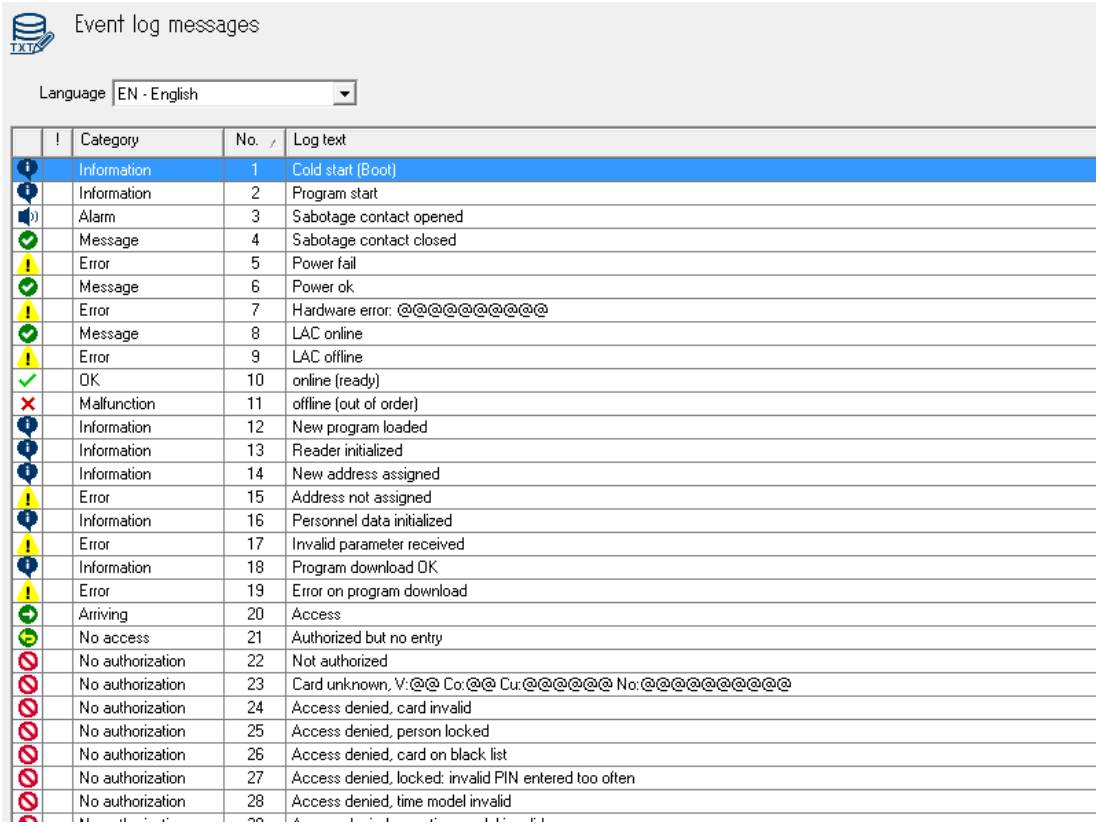
Einige der Texte, die am Ausweisleser angezeigt werden, können in diesem Dialog geändert werden. Die Leseranzeige umfasst 2 Zeilen à 20 Zeichen.

Vorsicht!
Bei der „Abfrage nach PIN” darf der Unterstrich „_“ nicht gelöscht werden, da er das Einlesen der PIN auslöst.

Die Texte sind anwenderdefiniert und werden daher bei Auswahl einer anderen Sprache nicht automatisch umgesetzt. Durch die Auswahl einer anderen Sprache aus der Auswahlliste **Sprache** über dem Listenfeld und erneute Eingabe der Texte können jedoch für jede installierte Sprachvariante in Access PE Äquivalente festgelegt werden. Damit werden auch diese Daten bei der Umschaltung des Arbeitsplatzes auf eine andere Sprache umgesetzt.

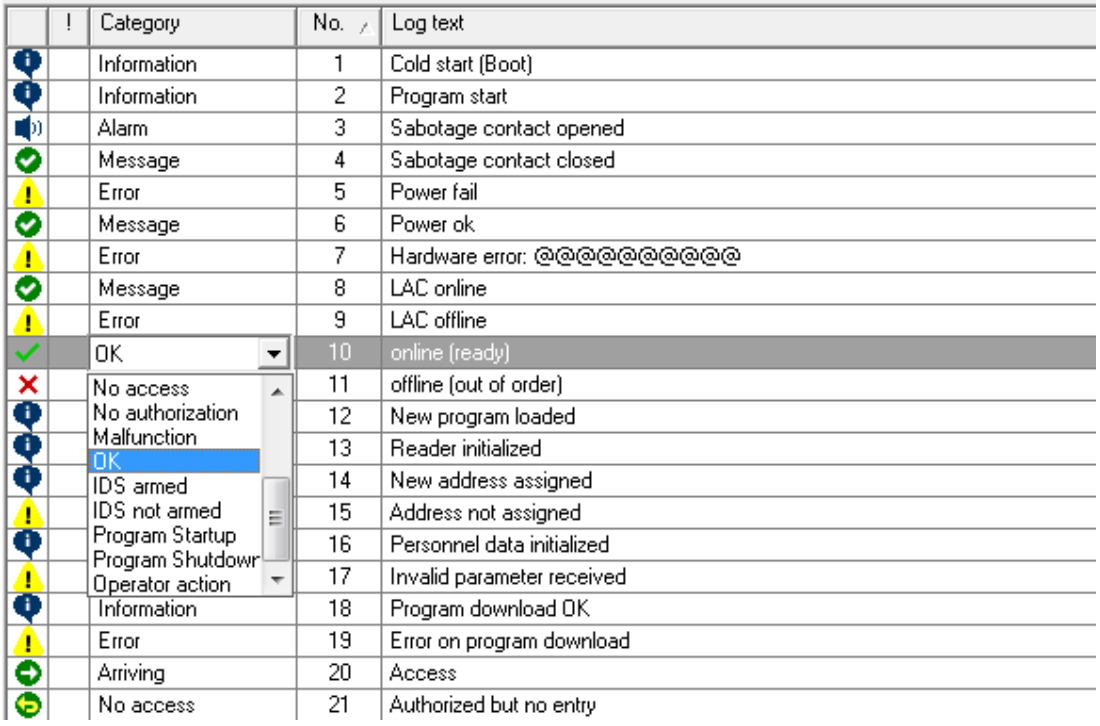
13.2 Logbuchtexte

Hier können Sie sowohl den Text als auch die Kategorie aller Meldungen ändern, die von den Controllern generiert werden.



!	Category	No.	Log text
	Information	1	Cold start (Boot)
	Information	2	Program start
	Alarm	3	Sabotage contact opened
	Message	4	Sabotage contact closed
	Error	5	Power fail
	Message	6	Power ok
	Error	7	Hardware error: @@@@@@@@@@
	Message	8	LAC online
	Error	9	LAC offline
	OK	10	online (ready)
	Malfunction	11	offline (out of order)
	Information	12	New program loaded
	Information	13	Reader initialized
	Information	14	New address assigned
	Error	15	Address not assigned
	Information	16	Personnel data initialized
	Error	17	Invalid parameter received
	Information	18	Program download OK
	Error	19	Error on program download
	Arriving	20	Access
	No access	21	Authorized but no entry
	No authorization	22	Not authorized
	No authorization	23	Card unknown, V:@@ Co:@@ Cu:@@@@@@@ No:@@@@@@@@@@
	No authorization	24	Access denied, card invalid
	No authorization	25	Access denied, person locked
	No authorization	26	Access denied, card on black list
	No authorization	27	Access denied, locked: invalid PIN entered too often
	No authorization	28	Access denied, time model invalid

Nach einem Doppelklick in das Feld **Kategorie** in der gewünschten Zeile erhalten Sie eine Auswahl der möglichen Kategorien und können die Meldungen nach Ihren Anforderungen klassifizieren.



!	Category	No.	Log text
	Information	1	Cold start (Boot)
	Information	2	Program start
	Alarm	3	Sabotage contact opened
	Message	4	Sabotage contact closed
	Error	5	Power fail
	Message	6	Power ok
	Error	7	Hardware error: @@@@@@@@@@@
	Message	8	LAC online
	Error	9	LAC offline
	OK	10	online (ready)
	No access	11	offline (out of order)
	No authorization	12	New program loaded
	Malfunction	13	Reader initialized
	OK	14	New address assigned
	IDS armed	15	Address not assigned
	IDS not armed	16	Personnel data initialized
	Program Startup	17	Invalid parameter received
	Program Shutdowr	18	Program download OK
	Operator action	19	Error on program download
	Information	20	Access
	Error	21	Authorized but no entry
	Arriving		
	No access		

Jede Kategorie wird durch ein eindeutiges Symbol in der ersten Spalte repräsentiert. Diese Symbole werden auch im Logbuch verwendet und kennzeichnen dort die eingegangenen Meldungen. Folgende Symbole und Kategorien stehen zur Unterscheidung und Klassifizierung der Meldungen zur Verfügung.

- kein Logbuch
- Information
- Meldung
- Fehler
- Alarm
- Kommt
- Geht
- Kein Zutritt
- Keine Berechtigung
- Störung
- OK
- EMA scharf
- EMA unscharf
- Programmstart
- Programmende
- Bedieneraktion

In der zweiten Spalte (mit **!**) werden die Meldungen selektiert, die als spezielle Alarmmeldungen im Dialog **Alarmmanagement** angezeigt werden sollen. Per Doppelklick in die entsprechende Zelle blenden Sie das Alarmsymbol ein bzw. aus. Mit der Installation werden die Meldungen der Kategorien **Alarm** und **Fehler** als standardmäßige Alarmmeldungen voreingestellt.

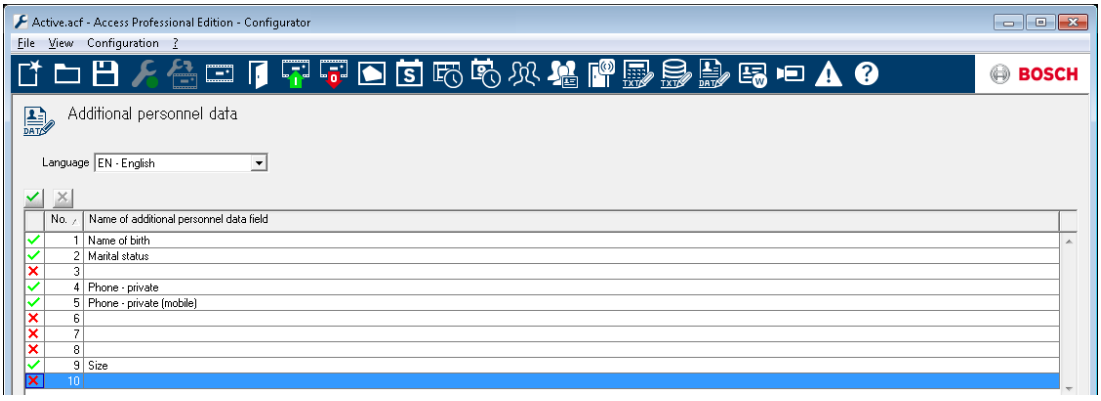
Per Doppelklick in das Feld **Logbuchtext** in der gewünschten Zeile können Sie den angezeigten Text nach Ihren Vorstellungen modifizieren.

!	Category	No.	Log text
	Information	1	Cold start (Boot)
	Information	2	Program start
	Alarm	3	Sabotage contact opened
	Message	4	Sabotage contact closed
	Error	5	Power fail
	Message	6	Power ok
	Error	7	Hardware error: @@@@@@@@@@
	Message	8	LAC online
	Error	9	LAC offline
	OK	10	online (ready)
	Malfunction	11	offline (out of order)
	Information	12	New program loaded

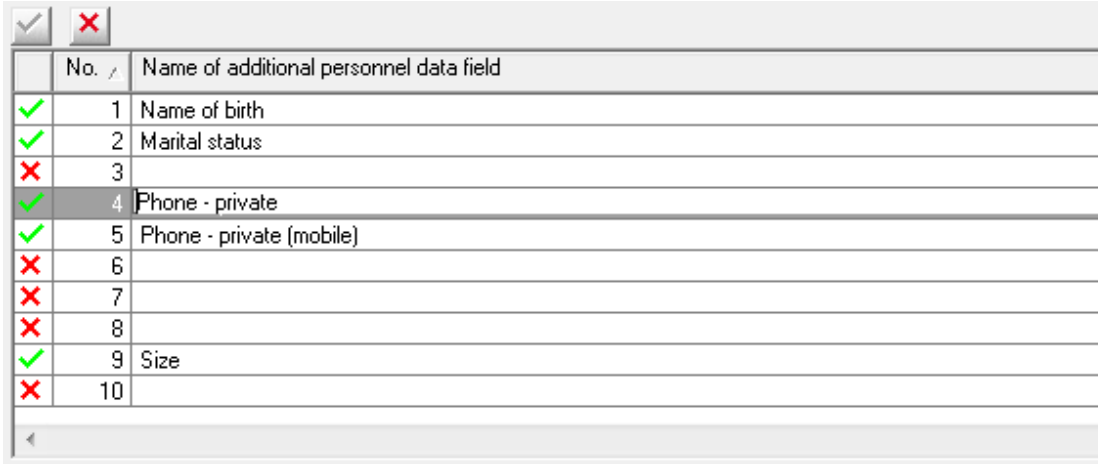
Die Texte sind anwenderdefiniert und werden daher bei Auswahl einer anderen Sprache nicht automatisch umgesetzt. Durch die Auswahl einer anderen Sprache aus der Auswahlliste **Sprache** über dem Listenfeld und erneute Eingabe der Texte können jedoch für jede installierte Sprachvariante in Access PE Äquivalente festgelegt werden. Damit werden auch diese Daten bei der Umschaltung des Arbeitsplatzes auf eine andere Sprache umgesetzt.

14 Zusätzliche Personaldatenfelder

Neben den fest vordefinierten Eingabefeldern für die Personaldaten können bis zu 10 Felder frei definiert werden.

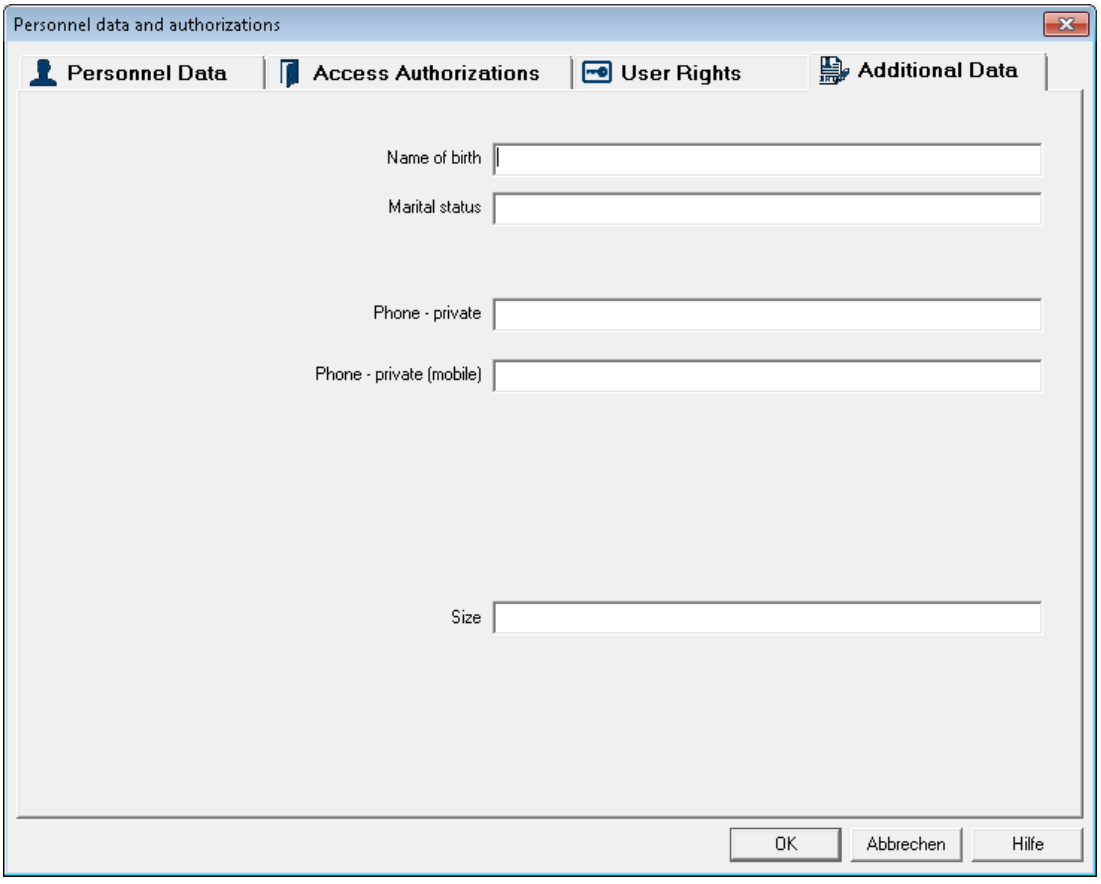


Das Listenfeld enthält bereits 10 Zeilen zur Definition der Zusatzfelder. Per Doppelklick in das entsprechende Feld der Spalte **Name des Personaldatenfeldes** wird dieses editierbar, und der gewünschte Feldname kann eingetragen werden.



Hinweis!
Die Angabe eines Feldnamens aktiviert das entsprechende Zusatzfeld noch nicht. Die Aktivierung erfolgt per Doppelklick auf in der ersten Spalte oder per Klick auf . Die Kennzeichnung wird dann durch ersetzt.

Sobald mindestens ein Zusatzdatenfeld aktiviert wurde, erscheint in der Personalverwaltung im Dialog für die Personaldaten und Zutrittsberechtigungen eine weitere Registerkarte **Zusatzdaten**. Die Reihenfolge der Felder muss dabei nicht eingehalten werden – für nicht aktivierte Felder werden entsprechende Lücken freigehalten.



In jedes Feld können bis zu 40 beliebige Zeichen eingetragen werden.

Hinweis!
Jedes Eingabefeld ist einem bestimmten Datenbankfeld zugeordnet, sodass die Daten gespeichert werden und auch nach den entsprechenden Inhalten selektiert werden können bzw. die zugehörigen Berichte diese Angaben danach sortieren. Wurden bereits Datensätze angelegt, die Angaben zu bestimmten Zusatzfeldern enthalten, kann dieses Feld nicht mehr geändert werden, ohne einen Datenverlust in Kauf zu nehmen.

Die Bezeichnungen der Zusatzfelder sind anwenderdefiniert und werden daher bei Auswahl einer anderen Sprache nicht automatisch umgesetzt. Durch die Auswahl einer anderen Sprache aus der Auswahlliste **Sprache** über dem Listenfeld können jedoch für jede installierte Sprachvariante in Access PE Äquivalente festgelegt werden. Damit werden auch diese Daten bei der Umschaltung des Arbeitsplatzes auf eine andere Sprache umgesetzt.
Zusatzfelder aktivieren/deaktivieren
Neben der Angabe einer Feldbezeichnung müssen die Zusatzfelder speziell aktiviert werden. Die Aktivierung erfolgt per Doppelklick auf das Symbol in der ersten Spalte oder per Klick auf . Das Symbol wird dann von in geändert.
Die Registerkarte **Zusatzdaten** in der **Personalverwaltung** wird erst angezeigt, wenn mindestens ein Zusatzfeld aktiviert wurde.

Hinweis!
Es können auch Felder aktiviert werden, die keine Feldbezeichnung haben.

Aktivierte Felder können per Doppelklick auf  oder über die Schaltfläche  deaktiviert werden. Daraufhin wird ein Sicherheitshinweis mit Informationen zu den zwei Deaktivierungsvarianten angezeigt:

Hinweis!
Beim Deaktivieren des Feldes werden die angegebenen Feldinhalte bei den Personen nur gelöscht, wenn auch die Feldbeschreibung gelöscht wird. Wollen Sie die Feldbeschreibung und damit die Feldinhalte bei den Personen ebenfalls löschen?

Nein = Das Feld wird unter Beibehaltung des Feldnamens und der Feldinhalte deaktiviert.

Ja = Das Feld wird unter **Löschung des Feldnamens und der Feldinhalte** deaktiviert.

15 Verwalten von Videogeräten

15.1 Öffnen des Konfigurators

Es gibt drei Möglichkeiten, den Konfigurator zu öffnen:

Option 1

1. Doppelklicken Sie auf Ihrem Desktop auf das Konfigurator-Symbol 

.
– Der Konfigurator wird geöffnet.

Option 2

1. Öffnen Sie die Anwendung **Access PE Personalverwaltung**.
2. Klicken Sie in der Menüleiste der Anwendung **Access PE Personalverwaltung** auf  .
– Der Konfigurator wird geöffnet.

Option 3

1. Öffnen Sie die Anwendung **Access PE Personalverwaltung**.
2. Wählen Sie in der Menüleiste **Tools** aus.
3. Wählen Sie in der Dropdown-Liste **Konfigurator ausführen** aus.
– Der Konfigurator wird geöffnet.

15.2 Finden von Videogeräten

Voraussetzung:
– Installieren und konfigurieren Sie alle Videogeräte.
– Öffnen Sie den Konfigurator.

1. Klicken Sie in der Menüleiste des Access PE Konfigurators auf  .
2. Klicken Sie auf die Schaltfläche **Neue Geräte suchen**, um nach Videogeräten zu suchen.
– Während der Suche ändert sich der Name der Schaltfläche zu **Suche beenden**, sodass Sie die Suche abbrechen können.
– Alle Videogeräte, die vom Bosch Video SDK unterstützt werden, werden erkannt und erscheinen im Konfigurator-Dialog im Listenfeld unten rechts.

Siehe auch

– *Öffnen des Konfigurators, Seite 86*

15.3 Hinzufügen eines Videogeräts zum Zutrittskontrollsystem

1. Öffnen Sie den Konfigurator.
2. Klicken Sie in der Menüleiste des Access PE Konfigurators auf  .
3. Klicken Sie auf die Schaltfläche **Neue Geräte suchen**, um nach Videogeräten zu suchen.
– Während der Suche ändert sich der Name der Schaltfläche zu **Suche beenden**, sodass Sie die Suche abbrechen können.
– Alle Videogeräte, die vom Bosch Video SDK unterstützt werden, werden erkannt und erscheinen im Konfigurator-Dialog im Listenfeld unten rechts.
– Sobald ein Videogerät aktiviert wurde, wird die Aktivierungsschaltfläche deaktiviert.
4. Wählen Sie ein Videogerät im Konfigurator-Dialog im Listenfeld unten rechts.
5. Klicken Sie auf die Schaltfläche **Gerät aktivieren**.

– Das ausgewählte Videogerät wird in das linke Listenfeld im Konfigurator-Dialog verschoben.

Hinweis!
Sie können nur Geräte bewegen, die mit einem grünen Häkchen gekennzeichnet sind. Stellen Sie sicher, dass Sie zunächst passwortgeschützte Listeneinträge (mit einem roten Kreuz markiert) zugänglich machen, indem Sie auf die Schaltfläche **Zugriffsdaten ändern** klicken.

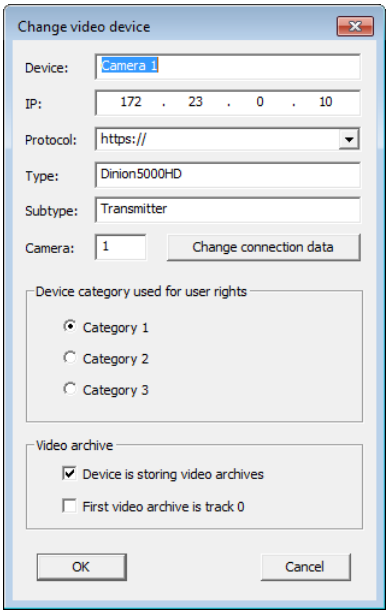
Hinweis!
Die Anzahl von Geräten, die Sie übertragen können, ist möglicherweise durch die Lizenz begrenzt.

Siehe auch
– *Öffnen des Konfigurators, Seite 86*

15.4 Ändern von Zugriffsdaten

Option 1
1. Öffnen Sie den Konfigurator.
2. Klicken Sie in der Menüleiste des Access PE Konfigurators auf  .
3. Klicken Sie auf die Schaltfläche **Neue Geräte suchen**, um nach Videogeräten zu suchen.
– Während der Suche ändert sich der Name der Schaltfläche zu **Suche beenden**, sodass Sie die Suche abbrechen können.
– Alle Videogeräte, die vom Bosch Video SDK unterstützt werden, werden erkannt und erscheinen im Konfigurator-Dialog im Listenfeld unten rechts.
4. Wählen Sie ein Videogerät im Konfigurator-Dialog im Listenfeld unten rechts.
5. Klicken Sie auf die Schaltfläche **Zugriffsdaten ändern**.
– Das Dialogfeld **Verbindungsparameter ändern** wird geöffnet.
6. Geben Sie den Benutzernamen und das Passwort ein.
– Stellen Sie sicher, dass Sie ein autorisiertes Benutzerkonto verwenden.
7. Klicken Sie auf **OK**.

Option 2
1. Öffnen Sie den Konfigurator.
2. Doppelklicken Sie auf ein Videogerät im linken Listenfeld des Konfigurator-Dialogs.
– Anhand der Angaben der Encoder-Geräte (Nummer, Name, Adresse, Kamera, Typ) können Sie die einzelnen Videogeräte leicht identifizieren.
– Das Dialogfeld **Videogerät ändern** wird geöffnet.
3. Klicken Sie auf die Schaltfläche **Zugriffsdaten ändern**.
4. Geben Sie den Benutzernamen und das Passwort ein.
– Stellen Sie sicher, dass Sie ein autorisiertes Benutzerkonto verwenden.
– Beachten Sie, dass Sie die Zugriffsdaten für das Videogerät nur mit der geräteeigenen Software ändern können.
5. Klicken Sie auf **OK**.



Siehe auch

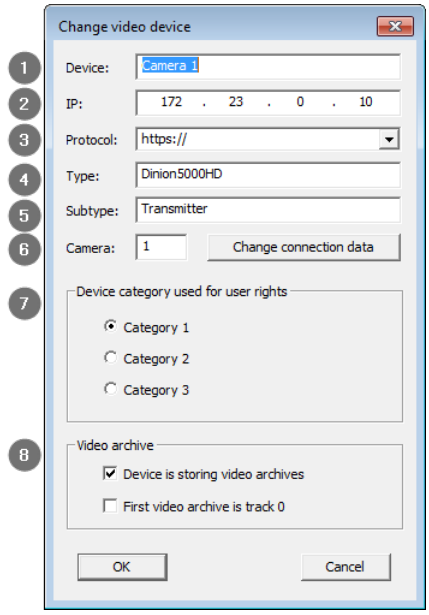
– *Öffnen des Konfigurators, Seite 86*

15.5 Ändern von Videogerätedaten

1. Öffnen Sie den Konfigurator.
2. Klicken Sie in der Menüleiste des Access PE Konfigurators auf .
3. So öffnen Sie das Dialogfeld **Videogerät ändern**:

– Doppelklicken Sie auf ein Videogerät im linken Listenfeld des Konfigurator-Dialogs.
– Klicken Sie auf das grüne Plus-Symbol über dem Listenfeld auf der linken Seite des Konfigurator-Dialogs.

4. Geben Sie die Videogerätedaten ein bzw. ändern Sie sie entsprechend den unten genannten Möglichkeiten.
5. Klicken Sie auf **OK**.



1	Geben Sie den Namen des Videogeräts ein bzw. ändern Sie ihn.
2	Geben Sie die IP-Adresse des Videogeräts ein bzw. ändern Sie sie.
3	Videogeräte werden standardmäßig über das https-Protokoll verbunden. Wenn das ausgewählte Videogerät nicht das https-Protokoll unterstützt, wählen Sie in der Dropdown-Liste „keine“ aus.
4	Geben Sie den Typ des Videogeräts ein bzw. ändern Sie ihn.
5	Geben Sie den Subtyp des Videogeräts ein bzw. ändern Sie ihn.
6	Ändern Sie die Zugriffsdaten.
7	Weisen Sie eine von drei Benutzerrecht-Kategorien zu, damit nur ausgewählte Benutzer bestimmte Kameras bedienen können.
8	Aktivieren oder deaktivieren Sie die Kästchen abhängig davon, wie Sie die Videos archivieren möchten.

Siehe auch

– *Öffnen des Konfigurators, Seite 86*

15.6 Anzeigen von Live-Videobildern

1. Öffnen Sie den Konfigurator.
2. Klicken Sie in der Menüleiste des Access PE Konfigurators auf  .

– Wählen Sie ein Videogerät aus dem Listenfeld auf der linken Seite des Konfigurator-Dialogs aus.
– Klicken Sie auf die Schaltfläche **Video anzeigen**.

Siehe auch

– *Öffnen des Konfigurators, Seite 86*

15.7 Anzeigen von Archivaufzeichnungen

1. Öffnen Sie den Konfigurator.
2. Klicken Sie in der Menüleiste des Access PE Konfigurators auf  .
3. Wählen Sie ein Videogerät aus dem Listenfeld auf der linken Seite des Konfigurator-Dialogs aus.
4. Klicken Sie auf die Schaltfläche Aufzeichnung anzeigen.

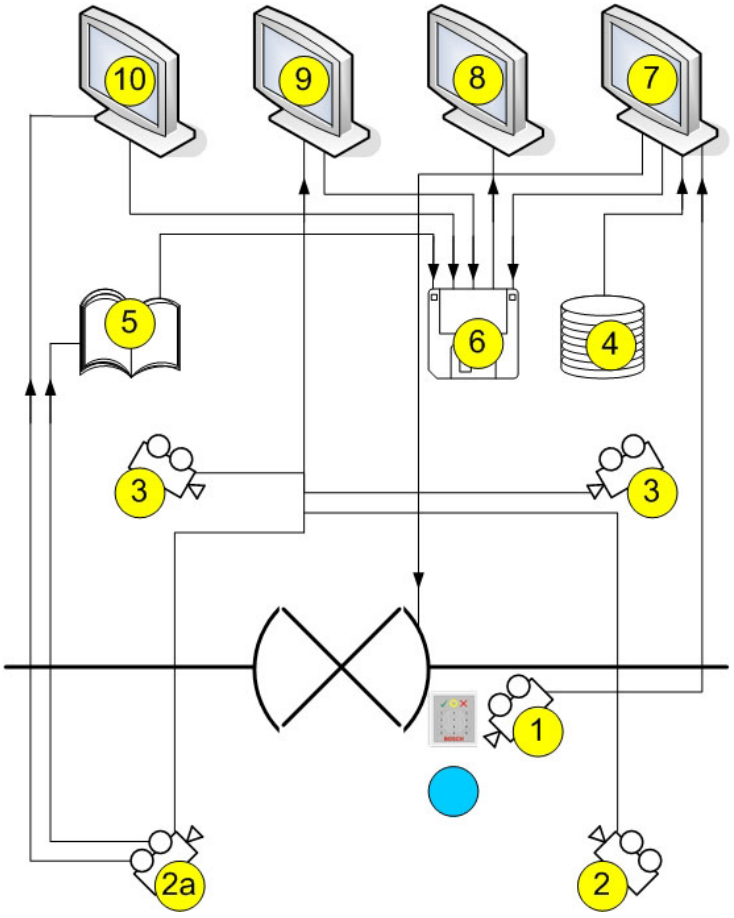
– Das Dialogfeld Wiedergabe starten wird geöffnet.

5. Wählen Sie den Zeitpunkt aus, ab dem Sie die Aufzeichnung sehen möchten.
6. Klicken Sie auf **OK**.

Siehe auch

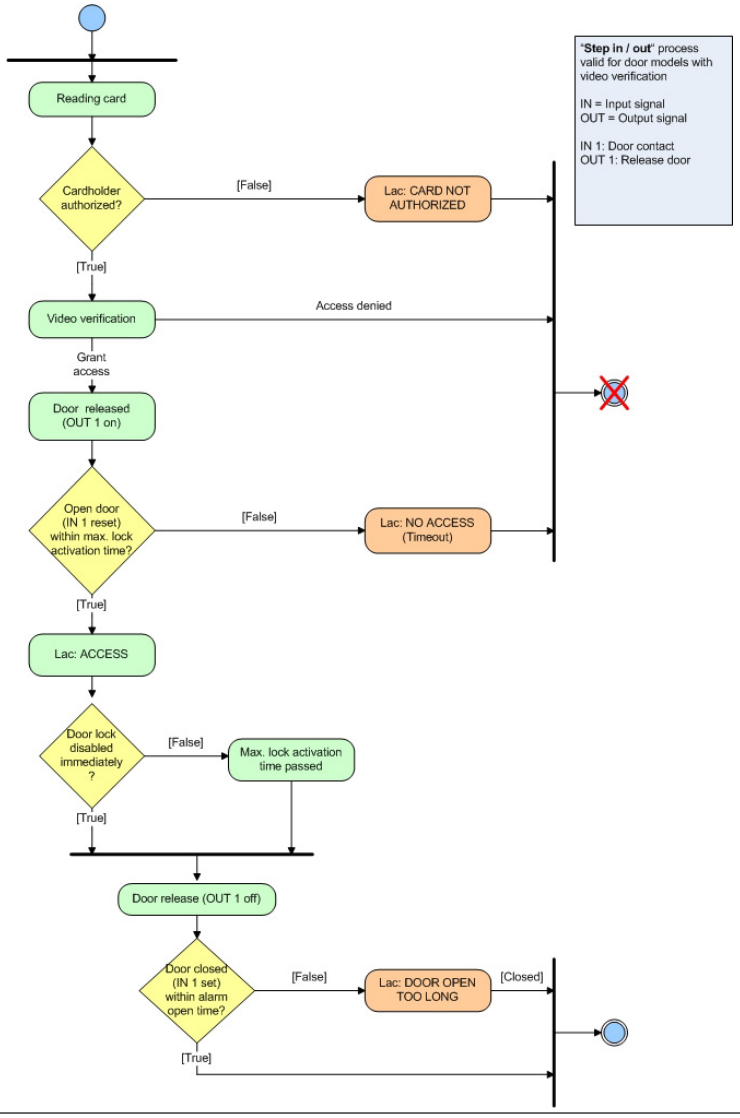
– *Öffnen des Konfigurators, Seite 86*

15.8 Darstellungen und Abläufe



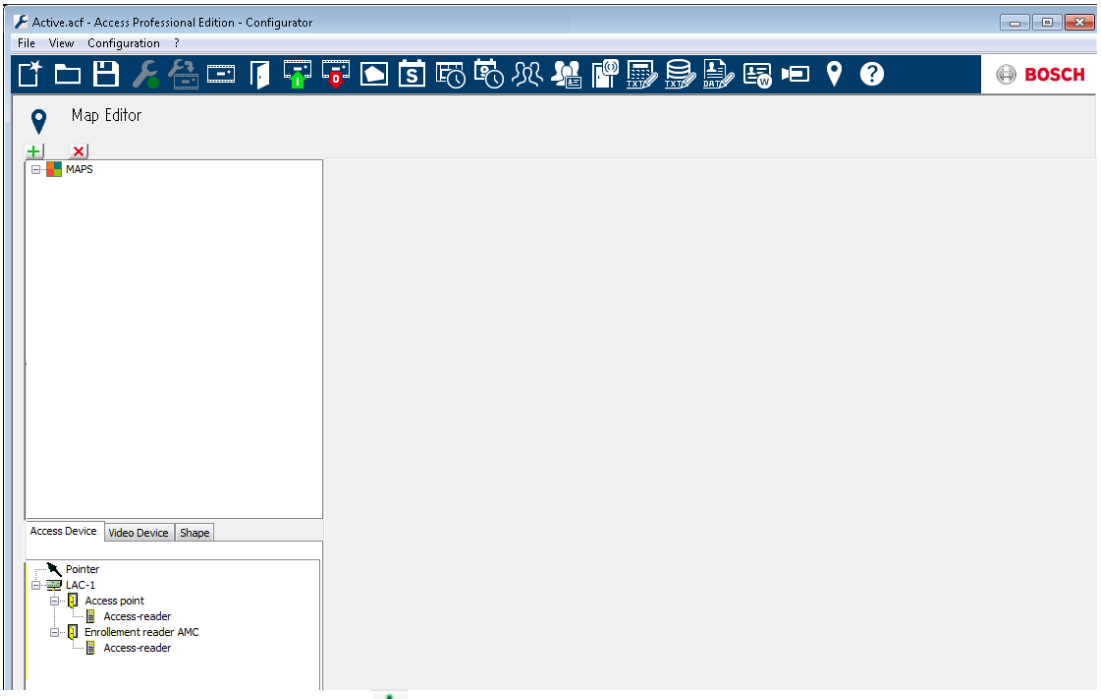
1 =	Identifikationskamera Bei Zutrittsanfragen wird das Bild von dieser Kamera im Dialog „Videoverifikation“ (7) angezeigt.
2 =	Überwachungskameras – hinterer Bereich
2a =	Alarm- und Logbuchkamera Dazu kann eine der Kameras (1, 2 oder 3) ausgewählt werden.
3 =	Überwachungskameras – vorderer Bereich
4 =	Datenbank Bei der Videoverifikation (7) wird ein Bild aus der Datenbank einem Livebild von der Identifikationskamera (1) zum Vergleich gegenübergestellt.
5 =	Logbuch Wenn Sie eine Alarm- und Logbuchkamera (2a) konfiguriert haben, werden Bilder zu den Alarmen gespeichert.
6 =	Lokale Festplatte/Speichermedium Lokale Dateien können über die Dialoge „Videoverifikation“ (7), „Videoanzeige“ (9) and „Alarm Management“ (10) sowie von den Bildern der Logbuchmeldungen gespeichert werden (5). Handelt es sich dabei um Videoaufzeichnungen (.vxx-Format) können diese mit dem Bosch Video Player (8) angezeigt werden.

7 =	Videoverifikation – Bildvergleich zwischen Livebild der Identifikationskamera (1) und einem Datenbankbild (4). – Türfreigabe/-sperrung per Dialogschaltfläche. – Lokale Speicherung der angezeigten Bilder (6).
8 =	Bosch Video Player Lokale gespeicherte .vxx-Aufzeichnungen (6) können mit diesem Dialog angezeigt werden.
9 =	Videoanzeige – Bilder von bis zu vier Kameras können gleichzeitig in dieser Ansicht gezeigt werden. – Zu jeder Kamera sind lokale Aufzeichnungen (6) möglich.
10 =	Alarm Management Falls eine Alarm- und Logbuchkamera (2a) konfiguriert wurde, können zu Alarmmeldungen des entsprechenden Durchtritts auch die Videobilder angezeigt werden. Davon können lokale Kopien erstellt (6) und über den Video Player (8) angezeigt werden.

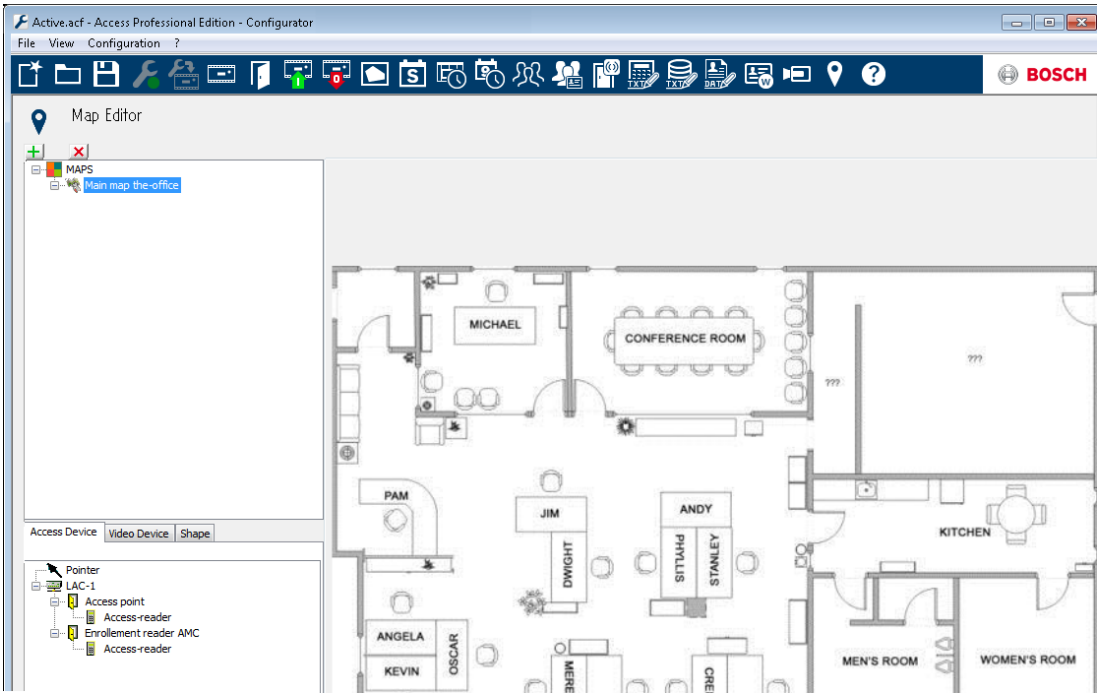


16 Konfigurieren einer Karte

Lageplan-Editor starten



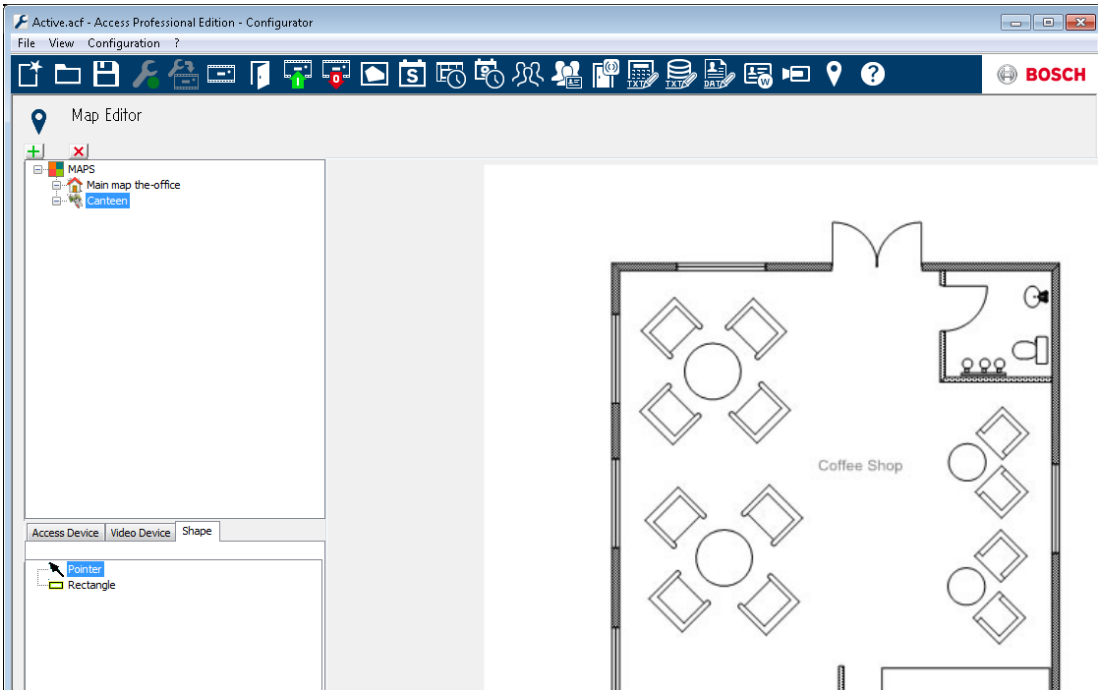
Klicken Sie auf die Schaltfläche , um einen Plan hinzuzufügen.



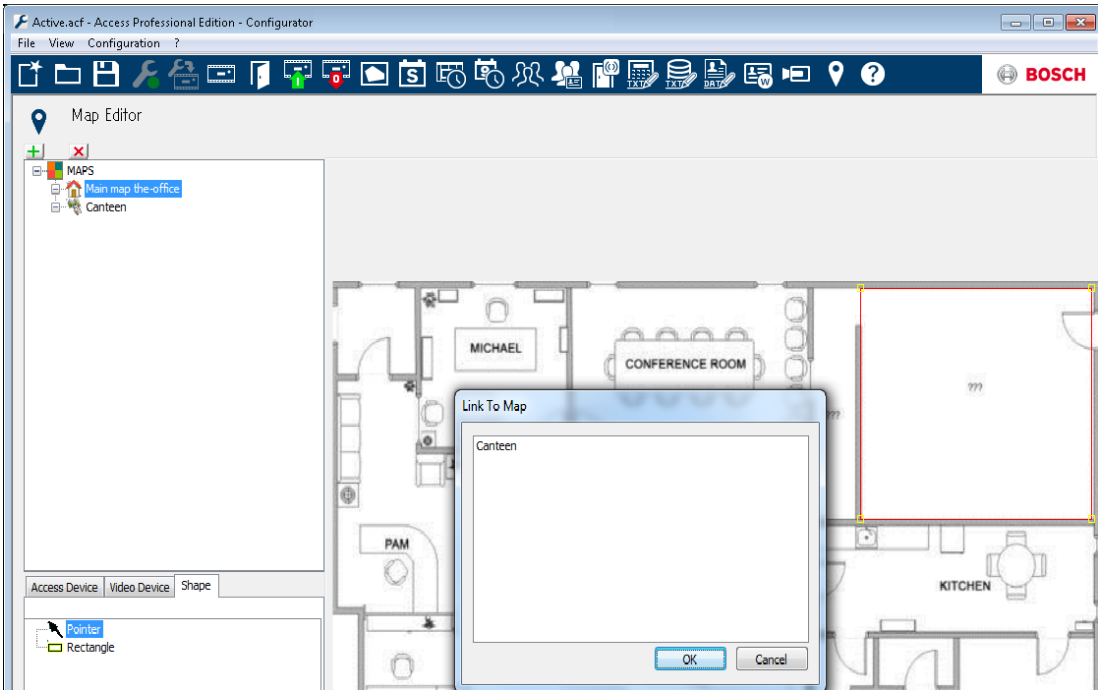
Der Plan wird im Dialog angezeigt.

– Konfigurieren Sie optional diesen Plan als **Startlageplan**

Fügen Sie dem Lageplanbaum eine Detailansicht hinzu, z. B. die Kantine.



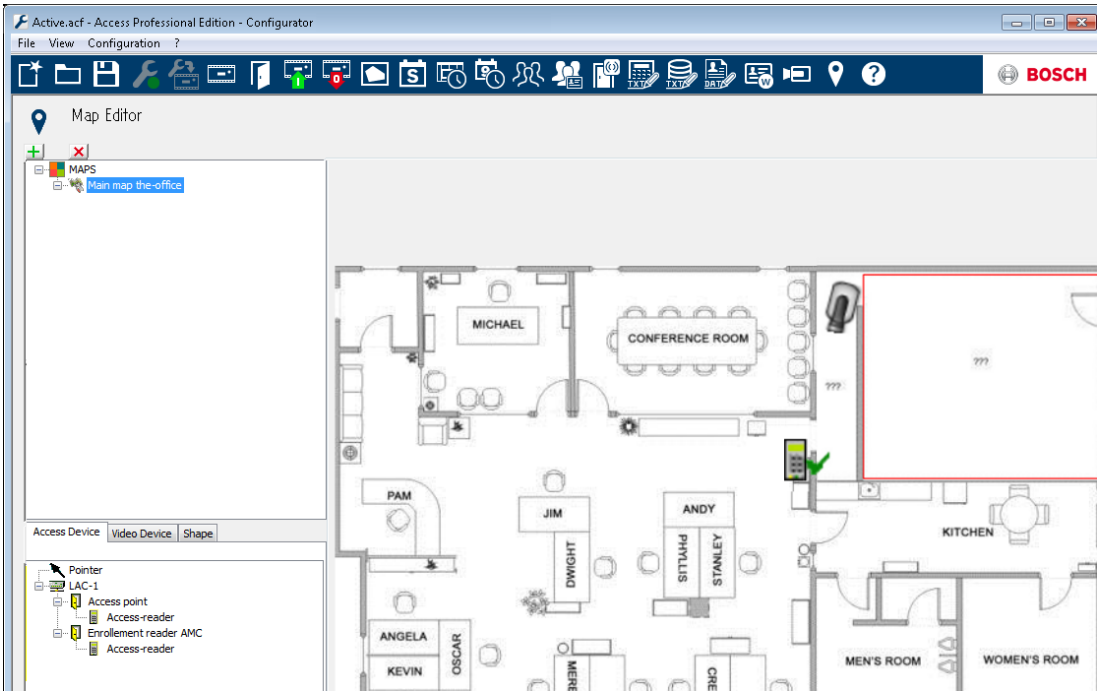
– Um den neuen **Kantinenplan** mit dem Hauptplan zu verbinden, gehen Sie zur Registerkarte **Form** und wählen ein **Rechteck**.
– Platzieren Sie das Rechteck über den Bereich des Plans, der als Detailansicht angezeigt werden soll (im Beispiel unten als rotes Rechteck dargestellt).
– Wählen Sie in der Anzeige **Verknüpfung mit Lageplan** die entsprechende Detailansicht, in diesem Beispiel „Kantine“.



17 Hinzufügen eines Geräts zum Lageplan

Wählen Sie die Registerkarte **Geräte**, und fügen Sie dem Lageplan Geräte hinzu, indem Sie diese mit der Maus in den Plan ziehen. Im Beispiel unten wurden folgende Geräte hinzugefügt:

- Ein Zutrittspunkt
- Ein Leser
- Zwei Kameras



- Klicken Sie auf ein Gerät im Plan und verändern Sie die Größe mit der gedrückten Maustaste.
- Klicken Sie auf ein Gerät und drehen Sie es nach Wunsch durch Verwenden des Mausrads.

Gerätetypen	Steuerelemente
	Tür
	Leser
	Kamera

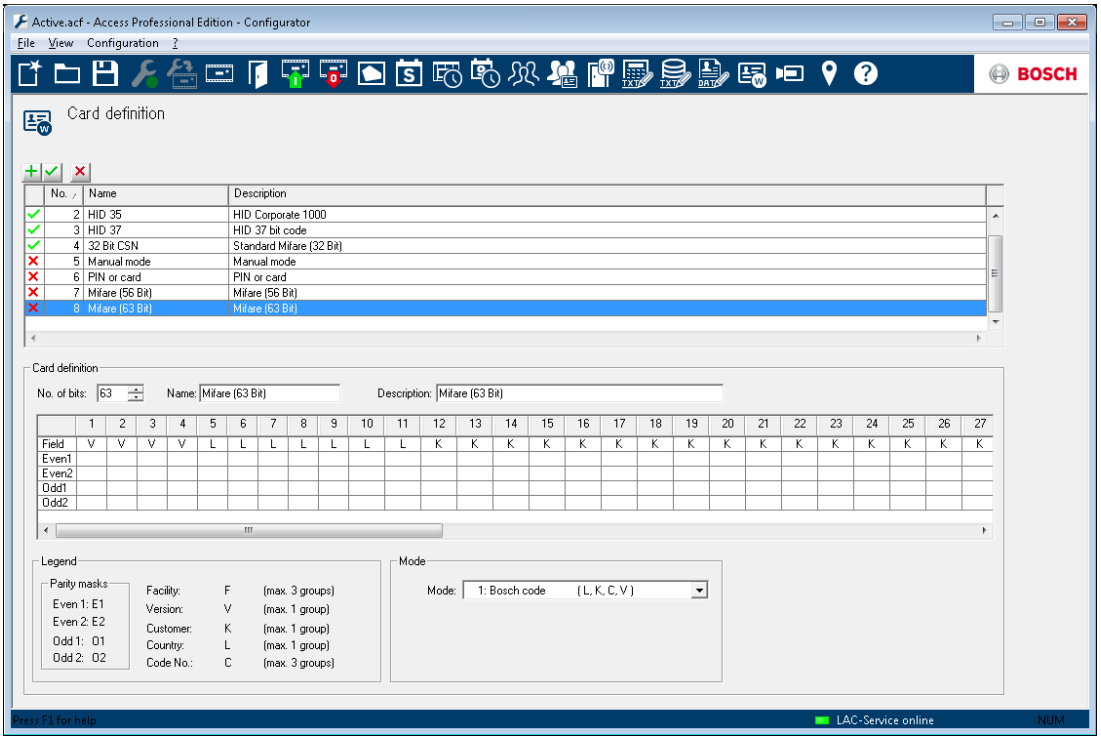
Gerätetypen	Alarme
Zutrittspunkt (Durchtritt)	
	Tür ohne Berechtigung geöffnet
	Tür zu lange geöffnet
	(Alle Leseralarmmeldungen sind ebenfalls Durchtrittsalarme*)
Leser	Leserfehler
	

Gerätetypen	Alarme
Kamera	n. z.

* Diese Alarmereignisse können vom Benutzer angepasst werden. Ein Benutzer kann also mithilfe von **AcConfig -> Logbuch** alle Ereignisse als Alarmereignisse konfigurieren (mit einem Doppelklick auf die zweite Spalte wird ein Alarm ausgelöst).

18 Ausweisdefinition

Mit diesem Dialog werden die vom Leser übermittelten Daten definiert, sodass auch zu einem späteren Zeitpunkt neue Ausweisdefinitionen ins System aufgenommen werden können.



Das Listenfeld enthält die vorhandenen Ausweisdefinitionen. Die Standardsystemeinstellungen enthalten sechs Standardeinträge, von denen die ersten vier aktiviert sind (= grüner Haken in der ersten Spalte). Bis auf die Definition **Eingabemodus** sind alle anderen schreibgeschützt und können weder geändert noch gelöscht werden.

Hinweis!
Bei Wiegand-Controllern und -Lesern muss zur Verwendung von Identifikations-, Scharfschaltungs- und Tür-PINs die Wiegand-Ausweisdefinition **PIN oder Karte** (Nr. 6) aktiviert sein.

Hinweis!
Achten Sie darauf, dass nur 4 Ausweistypen aktiviert sind, da die maximale Anzahl gültiger Ausweistypen 4 ist.

Zum Anlegen eines neuen Eintrags wird zunächst über die Schaltfläche ein neuer Listeneintrag generiert. Anhand der Herstellerangaben wird die **Anzahl Bits** und deren Codeaufteilung ausgewählt und angegeben.

Hinweis!
Die maximale Anzahl Bits ist auf 64 pro Definition begrenzt. Außerdem stehen für jeden Codeteil (Facility, Version, Kunde, Land und Codenummer) maximal 32 Bits zur Verfügung.

Zur besseren Unterscheidung sollten ein eindeutiger Name und eine Beschreibung für die Ausweisdefinition angegeben werden.
Mit der Angabe oder Auswahl der **Anzahl Bits** werden im darunterliegenden Listenfeld entsprechend viele Spalten angezeigt. Es werden fünf vordefinierte Zeilen angezeigt, die zu jedem Spalten- und Zeileneintrag die Aktivierung einzelner Bits ermöglichen.
Durch Eingabe der folgenden möglichen Werte in die Zellen der Zeile **Feld** kann nun bestimmt werden, wie der jeweilige Codeteil zu interpretieren ist:

F	Facility: kennzeichnet den Codeteil für die Anlagenzugehörigkeit	
V	Version: Codeteil, der die Versionsvariante beinhaltet	
K	Kunde: Codeteil, der den speziellen Kundencode enthält	
L	Land: Codeteil, der die Länderkennung enthält	
C	Codenummer: Codeteil, der die individuelle Ausweisnummer enthält	
E1	Even 1: Ausgleichsbit für die erste Even-Parity-Maske	Mit der Angabe eines dieser Werte wird das Kontrollkästchen der entsprechenden Zeile aktiviert.
E2	Even 2: Ausgleichsbit für die zweite Even-Parity-Maske	
O1	Odd 1: Ausgleichsbit für die erste Odd-Parity-Maske	
O2	Odd 2: Ausgleichsbit für die zweite Odd-Parity-Maske	
1 0	Feste Bitwerte, aus denen der Code an sich besteht	

Bei der Definition **Eingabe Modus** sowie bei allen neu angelegten Definitionen kann ein sogenannter **Modus** festgelegt werden, der bestimmt, wie der Code gelesen wird. Bei Auswahl des Modus **PIN oder Karte** wird dann beispielsweise nur die Codenummer gelesen, also alles, was als **C** gekennzeichnet ist. Folgende Modusvarianten stehen zur Auswahl:

Ordnungsnummer	**Modus**	**Akzeptierte Codeteile**
0	Facility + Codenummer	F, C
1	Bosch Code	L, K, C, V
100	Manuell	C
200	PIN oder Karte	C

Erläuterung:
Das Signal oder „Telegramm“, das ein Leser überträgt, wenn ein Ausweis eingelesen wird, setzt sich aus einer Reihe von Nullen und Einsen zusammen. Die Länge dieses Signals (d. h. die Anzahl der Bits) ist für jeden Typ von Ausweis(leser) genau festgelegt. Das Signal enthält neben den Nutzdaten auch Kontrolldaten, um zum einen das Telegramm zu identifizieren und zum anderen die korrekte Übertragung verifizieren zu können. Zur Verifizierung der korrekten Übertragung dienen die Paritätsbits, die als Quersumme (Prüfsumme) über ausgewählte Bits des Telegramms entweder eine Null (Even Parity, gerade Parität) oder eine Eins (Odd Parity, ungerade Parität) ergeben müssen. Die Controller können so konfiguriert werden, dass 1 oder 2 Prüfsummen für gerade Paritäten und 1 oder 2 Prüfsummen für ungerade Paritäten berechnet werden. In dem Listenfeld können in den jeweiligen Zeilen für die Paritätsprüfsummen (Even 1, Even 2, Odd 1 und Odd 2) die Bits markiert werden, die in die Prüfsumme einbezogen werden sollen.
In der obersten Zeile (Feld) wird zu jeder genutzten Quersumme ein Bit festgelegt, das die Quersumme entsprechend dem Paritätstyp ausgleicht. Wird eine Paritätsoption (Even 1, Even 2, Odd 1, Odd 2) nicht genutzt, bleibt die entsprechende Zeile einfach leer.

Ausweisdefinitionen aktivieren/deaktivieren
Das Symbol der ersten Spalten des Listenfeldes kennzeichnet den Aktivierungsstatus der jeweiligen Definition.

 aktiviert

 deaktiviert

Der Status kann per Doppelklick auf das entsprechende Feld dieser Spalte geändert werden. Sicherheitsabfragen weisen auf die Konsequenzen der Änderung hin.

Hinweis!
Eine falsche Ausweiskodierung sowie eine schlechte Kombination aktiver Kodierungen können dazu führen, dass alle Ausweise nicht mehr korrekt gelesen werden können. Möchten Sie diese Ausweiskodierung wirklich aktivieren?

Hinweis!
Alle Ausweise, die mit dieser Ausweiskodierung aufgenommen wurden, sind anschließend nicht mehr lesbar. Möchten Sie diese Ausweiskodierung wirklich deaktivieren?

19 Konfigurieren von Bedrohungsalarmen

Einführung

Eine **Bedrohung** ist eine kritische Situation, die eine sofortige und gleichzeitige Reaktion von einigen oder allen Durchtritten in einem Zutrittskontrollsystem erfordert.

Ein **Bedrohungsalarm** ist ein Alarm als Reaktion auf eine Bedrohung. Abhängig von den Einstellungen im Access PE Konfigurator können Durchtritte unterschiedlich auf Bedrohungsalarme reagieren.

Entsprechend autorisierte Personen können einen Bedrohungsalarm mit einer einzelnen Aktion auslösen, zum Beispiel über die Access PE Benutzeroberfläche, indem Sie auf eine Taste drücken oder einen bestimmten Ausweis an einem beliebigen Leser vorzeigen.

Hinweis!

Berücksichtigen Sie stets die örtlichen Notfall-Sicherheitsvorschriften zu Durchtritten! Für Durchtritte ist in der Regel ein ausfallsicherer Modus erforderlich.

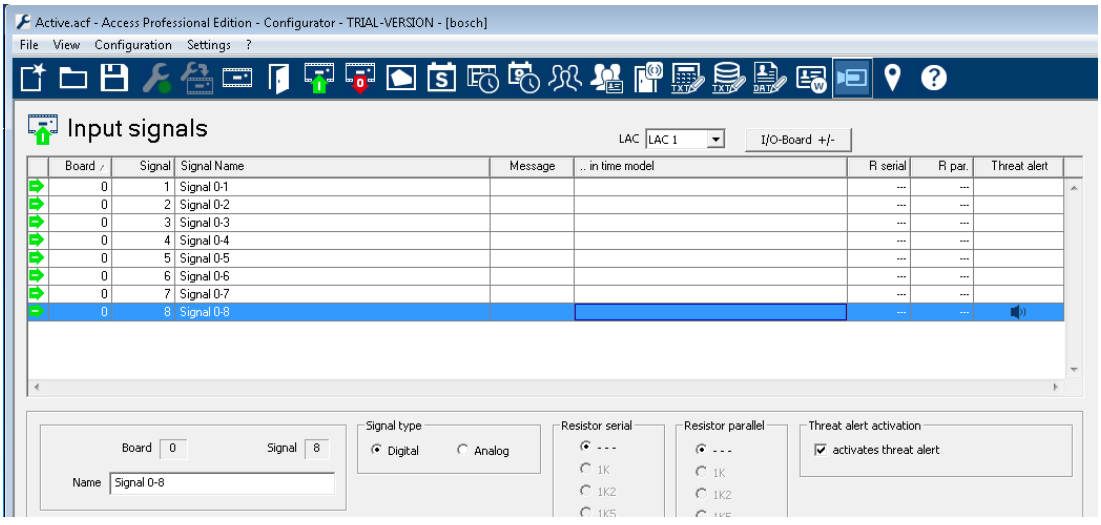
19.1 Konfigurieren der Hardware für Bedrohungsalarme

Übersicht

- Zuweisen eines AMC-Eingangssignals für die Weiterleitung von Bedrohungsalarmen
- Definieren der Reaktion von einzelnen Durchtritten auf den Bedrohungsalarm

Zuweisen eines Eingangssignals für Bedrohungsalarme

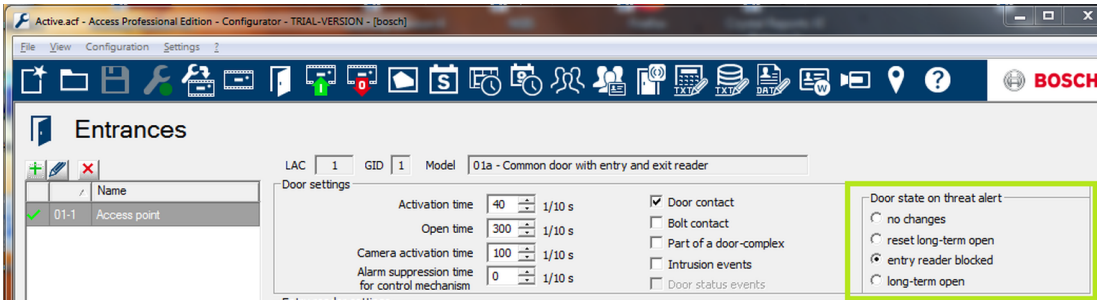
1. Wählen Sie im Access PE Konfigurator die Option **Eingangssignale** aus. 
2. Doppelklicken Sie in der Zeile, die dem gewünschten Eingangssignal entspricht, in die Spalte **Bedrohungsalarm** oder aktivieren Sie das Kontrollkästchen **aktiviert Bedrohungsalarm**.
   In der Zelle erscheint ein Lautsprechersymbol.



Definieren der Reaktion von Durchtritten auf einen Bedrohungsalarm

1. Wählen Sie im Access PE Konfigurator die Option **Durchtritte** aus. 

2. Wählen Sie aus der Liste der Durchtritte einen Durchtritt aus, der auf Bedrohungsalarme reagieren soll.
3. Legen Sie den Parameter **Türzustand bei Bedrohungsalarm** auf einen der folgenden Werte fest:
   - **keine Änderungen**: Der Durchtritt darf seinen Zustand als Reaktion auf den Bedrohungsalarm nicht ändern.
   - **langfristig offen zurücksetzen**: Jeder im Büromodus entsperrte Zeitraum wird beendet und die Tür wechselt in den Normalmodus. Die Tür kann anschließend nur noch durch gültige Ausweise geöffnet werden.
   - **Tür blockiert:** Die Tür ist gesperrt und gesichert. Der Normalmodus wird unterbrochen.
   - **langfristig offen**: Die Tür ist geöffnet und ermöglicht uneingeschränkten Zutritt.
4. Wiederholen Sie diese Vorgehensweise für alle Durchtritte, die auf Bedrohungsalarme reagieren sollen.



Beachten Sie, dass die Auswirkungen eines Bedrohungsalarms so lange anhalten, bis der Bedrohungsalarm explizit über die Benutzeroberfläche des Zutrittskontrollsystems gelöscht wird. Weitere Informationen finden Sie in der Online-Hilfe für die APE Personalverwaltung im Abschnitt **Verwenden der Schaltflächen „Bedrohungsalarm auslösen/deaktivieren“**.

Hinweis!
„Blockierte“ (gesicherte) Türen
Ein Durchtritt, der explizit in den Zustand **Tür blockiert (gesichert)** versetzt wurde, bleibt gesichert, wenn ein Bedrohungsalarm durch die Schaltfläche **Bedrohungsalarm deaktivieren** deaktiviert wird. Ein gesicherter Zustand muss explizit an der Tür deaktiviert werden, um zusätzliche Sicherheitsverletzungen nach Bedrohungsalarmen zu vermeiden.
Dialogpfad:
Hauptbildschirm **Personalverwaltung** > Baum **Gerätezustände** > Rechtsklick auf den gesicherten Durchtritt (mit einem Vorhängeschloss markiert) für das Kontextmenü

20 Anhang

20.1 Signale

Es stehen folgende Signale für Eingänge und Ausgänge zur Verfügung:

Eingangssignale	**Beschreibung**
Tür Rahmenkontakt	
Tür Öffnungstaster	Dies ist ein Druckknopf zum Öffnen der Tür.
Tür Riegelkontakt	Dieses Signal wird nur für Meldungen genutzt, ohne dass ein Steuerablauf angestoßen wird.
Durchtritt sperren	Diese Option wird verwendet, um die Gegenrichtung in Schleusen vorübergehend zu verriegeln. Die Option kann jedoch auch zum dauerhaften Verriegeln verwendet werden.
Sabotage	Dies ist das Sabotagesignal eines externen Controllers.
Drehkreuz in Ruhelage	Das Drehkreuz ist geschlossen.
Durchtritt beendet	Ein Durchtritt wurde erfolgreich abgeschlossen. Hierbei handelt es sich um einen Impuls eines externen Controllers.
EMA: scharfschalteberei t	Wird von der EMA gesetzt, wenn sich alle Melder in Ruhestellung befinden und die EMA scharfgeschaltet werden kann.
EMA: scharfgeschaltet	Die EMA ist scharfgeschaltet.
EMA: Taste zum Anfordern der Scharfschaltung	Taste zum Scharfschalten der EMA.
lokale Türöffnung	Wird verwendet, wenn die Tür aufgrund einer bestimmten Regelung ohne Beteiligung des AMC geöffnet wird. Der AMC sendet keine Einbruchsmeldung, sondern die Meldung, dass die Tür lokal geöffnet wurde.

Ausgangssignale	**Beschreibung**
Tür Öffnungskontakt	

Ausgangssignale	Beschreibung
Schleuse Sperre für Gegenrichtung	Sperrt die andere Seite der Schleuse. Wird gesetzt, wenn sich die Tür öffnet.
Alarmunterdrückung	... zur EMA. Wird gesetzt, solange die Tür geöffnet ist, um zu vermeiden, dass die EMA eine Einbruchsmeldung generiert.
Anzeige grün	Anzeigelampe – wird verwendet, solange die Tür geöffnet ist.
Tür zu lange geöffnet	Impuls von 3 Sekunden, wenn die Tür zu lange geöffnet ist.
Kameraaufschaltung	Die Kamera wird zu Beginn eines Durchtritts aktiviert.
Drehkreuz – Freigabe Eingang	
Drehkreuz – Freigabe Ausgang	
Tür permanent offen	Zeigt an, dass die Tür dauerhaft geöffnet ist.
EMA: scharfschalten	Impuls oder Dauerkontakt zum Scharfschalten der EMA.
EMA: unscharfschalten	Impuls zum Unscharfschalten der EMA.

20.2 Standard-Türmodelle

Standard-Türmodelle
Standardmäßig stehen die folgenden Türmodelle zur Verfügung:

01a Einfache Tür mit Eingangs- und Ausgangsleser

01b Einfache Tür mit Eingangsleser und Türöffnungsknopf

01c Einfache Tür mit Eingangsleser

01r Ein Leser, der nur zur Registrierung von Personen an einem Sammelplatz dient, z. B. im Falle einer Evakuierung. Es existiert keine physische Barriere und es werden keine Signale erzeugt.

03b Umschaltbares Drehkreuz mit Eingangsleser und Türöffnungsknopf

03c Drehkreuz mit Eingangsleser

06c Anmeldung über AMC – keine Eingangskontrolle!

07a Aufzug mit maximal 16 Stockwerken

07b Aufzug mit maximal 16 Stockwerken

10a Einfache Tür mit Eingangs- und Ausgangsleser und EMA-Unscharfschaltung

10b Einfache Tür mit Eingangsleser, Türöffnungsknopf und EMA-Unscharfschaltung

10c Einfache Tür mit Eingangsleser und EMA-Unscharfschaltung

10d Einfache Tür mit Eingangs- und Ausgangsleser und dezentraler EMA-Unscharfschaltung

10e Einfache Tür mit Eingangsleser, Türöffnungsknopf und dezentraler EMA-Unscharfschaltung

10f Einfache Tür mit Eingangsleser und dezentraler EMA-Unscharfschaltung

14a Einfache Tür mit Eingangs- und Ausgangsleser und EMA-Unscharfschaltung (Scharfschalteberechtigung)

14b Einfache Tür mit Eingangsleser, Türöffnungsknopf und EMA-Unscharfschaltung (Scharfschalteberechtigung)

14c Einfache Tür mit Eingangsleser und EMA-Unscharfschaltung

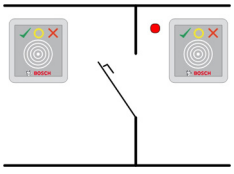
14d Einfache Tür mit Eingangs- und Ausgangsleser und dezentraler EMA-Unscharfschaltung

14e Einfache Tür mit Eingangsleser, Türöffnungsknopf und dezentraler EMA-Unscharfschaltung

14f Einfache Tür mit Eingangsleser und dezentraler EMA-Unscharfschaltung

20.3 Türmodell 01

Einfache Tür



Signale:

Eingangssignale	**Ausgangssignale**
Door sensor (Türsensor)	Door opener (Türöffner)
Pushbutton: door open (Drucktaste: Tür geöffnet)	Sluice: lock opposite direction (Schleuse: Gegenrichtung verriegeln)
Bolt sensor (Riegelkontakt)	Alarm suppression (Alarmunterdrückung)

Eingangssignale	Ausgangssignale
Entrance locked (Durchtritt verriegelt)	Camera activation (Kameraaktivierung)
Sabotage signal (Sabotagesignal)	Tür zu lange geöffnet
Local open enable (Lokale Öffnung aktivieren)	

Modellvarianten:

01a Einfache Tür mit Eingangs- und Ausgangsleser

01b Einfache Tür mit Eingangsleser und Türöffnungsknopf

01c Einfache Tür mit Eingangsleser

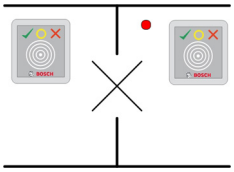
01r Ein Leser, der nur zur Registrierung von Personen an einem Sammelplatz dient, z. B. im Falle einer Evakuierung. Bei diesem Türmodell existiert keine physische Barriere und es werden keine Signale erzeugt.

Hinweis:
Die Schleusenverriegelung ist nur aktiv, wenn die Tür als Teil einer Schleuse konfiguriert wird. **Ist die Tür nicht Teil einer Schleuse, wird das Eingangssignal 03 als Lesersperre interpretiert. In diesem Fall wird bei anstehendem Eingangssignal 03 der Leser gesperrt. Die Alarmunterdrückung wird nur aktiviert, wenn die Alarmunterdrückungszeit vor der Türöffnung größer als 0 ist.**
Optional können Sekundärleser angeschlossen werden. In Kombination mit einer zweiten Tür und einer Schleusenverriegelung können so beide Türen zusammen als Schleuse gesteuert werden. Dieses Modell kann auch für Fahrzeugschranken oder Tore verwendet werden. Für diese Fälle wird die Anbringung eines Sekundärlesers für Lkw/Pkw empfohlen.

Hinweis!
Vereinzelungen können nur mit Türmodell 03 parametriert werden.

20.4 Türmodell 03

Umschaltbares Drehkreuz



Signale:

Eingangssignal	Ausgangssignale
Turnstile in normal Position (Drehkreuz in normaler Position)	Open turnstile inbound (Drehkreuz nach innen öffnen)
Pushbutton: door open (Drucktaste: Tür geöffnet)	Open turnstile outbound (Drehkreuz nach außen öffnen)
Entrance locked (Durchtritt verriegelt)	Sluice: lock opposite direction (Schleuse: Gegenrichtung verriegeln)
Sabotage signal (Sabotagesignal)	Alarm suppression (Alarmunterdrückung)
	Camera activation (Kameraaktivierung)
	Door open too long (Tür zu lange geöffnet)

Modellvarianten:

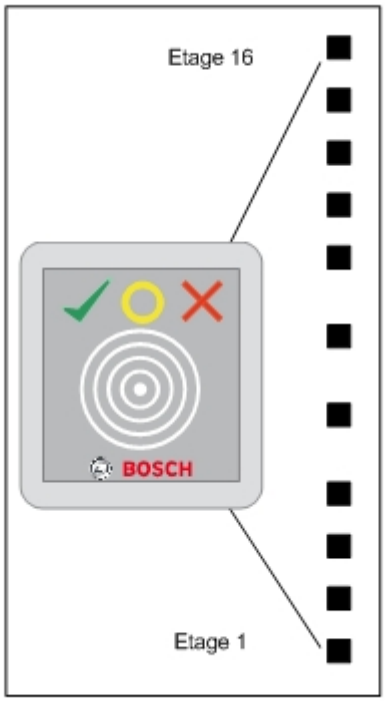
03a	Umschaltbares Drehkreuz mit Eingangs- und Ausgangsleser
03b	Umschaltbares Drehkreuz mit Eingangsleser und Öffnungsknopf
03c	Drehkreuz mit Eingangsleser

Hinweis:
Die Schleusenverriegelung ist nur aktiv, wenn die Tür als Teil einer Schleuse konfiguriert wird. Ist die Tür nicht Teil einer Schleuse, wird das Eingangssignal 03 als Lesersperre interpretiert. In diesem Fall wird bei anstehendem Eingangssignal 03 der Leser gesperrt.
In Kombination mit einer zweiten Tür und einer Schleusenverriegelung können so beide Türen zusammen als Schleuse gesteuert werden. Je nach Konstruktion erlaubt dieser Durchtritt eine Vereinzelung.

20.5 Türmodell 06c

Mit dem Türmodell 06c wird ein Leser mit Anmeldung über AMC konfiguriert. Es dient nicht dazu, einen Eingang zu steuern.

20.6 Türmodell 07



Modellvarianten:

07a	Aufzug
07b	Aufzug mit Lesereingang

Hinweis!
Standardmäßig kann ein AMC2 für acht Etagen verwendet werden. Unter den folgenden Voraussetzungen können mehrere Durchtritte angeschlossen werden:
64 Etagen bei Verwendung von Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)
56 Etagen bei Verwendung von RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

Signale für Türmodell 07a:

Eingangssignal	Ausgangssignale
Frei	Etage 01
Frei	Etage 02
Frei	Etage 03
Frei	Etage 04
...	...
Frei	Etage 16

Ablauf:
Zunächst wird der Aufzug angefordert. Dies kann mit den üblichen Funktionstasten der Aufzugssteuerung oder über einen Leser (z. B. mit Türmodell 01c) geschehen.
Anschließend wird im Aufzug ein weiterer Leser bedient (Türmodell 07a). Dieser schaltet die Etagen frei, für die der Ausweisinhaber Berechtigungen hält. Die Freischaltung wird z. B. über Aufleuchten der Tasten der Etagenanwahl des Aufzugs angezeigt. Daraufhin kann eine der freigegebenen Etagen angewählt werden.

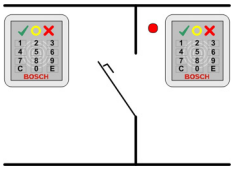
Signale für Türmodell 07b:

Eingangssignal	**Ausgangssignale**
Eingabetaste – Etage 01	Etage 01
Eingabetaste – Etage 02	Etage 02
Eingabetaste – Etage 03	Etage 03
Eingabetaste – Etage 04	Etage 04
...	...
Eingabetaste – Etage 16	Etage 16

Ablauf:
Zunächst wird der Aufzug angefordert. Dies kann mit den üblichen Funktionstasten der Aufzugssteuerung oder über einen Leser (z. B. mit Türmodell 01c) geschehen.
Anschließend wird im Aufzug ein Leser bedient (Türmodell 07b) und über die Lesertastatur die gewünschte Etage angewählt. Der AMC prüft, ob der Ausweisinhaber eine Berechtigung für die angewählte Etage besitzt, und fährt diese bei vorhandener Berechtigung an.

20.7 Türmodell 10

Einfache Tür mit EMA-Scharf-/Unscharfschaltung



Signale:

Eingangssignale	Ausgangssignale
Door sensor (Türsensor)	Door opener (Türöffner)
Pushbutton: door open (Drucktaste: Tür geöffnet)	IDS: Disarm (EMA: unscharfschalten) [nur bei den Modellen **d** und **f** mit einem Impuls von 1 s]
IDS: Ready to arm (EMA: scharfschaltebereit)	Kamera/Motorschloss
IDS: Arrmed (EMA: scharfgeschaltet)	IDS: Arm (EMA: scharfschalten) [nur bei den Modellen **d** und **f** mit einem Impuls von 1 s]
Sabotage signal (Sabotagesignal)	Tür zu lange geöffnet (Einbruch)
IDS: Arming (EMA: Scharfschalten)	

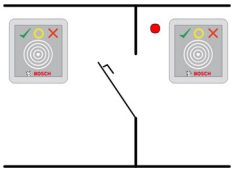
Modellvarianten:

10a	Einfache Tür mit Eingangs- und Ausgangsleser und EMA-Unscharfschaltung
10b	Einfache Tür mit Eingangsleser, Türöffnungsknopf und EMA-Unscharfschaltung
10c	Einfache Tür mit Eingangsleser und EMA-Unscharfschaltung
10d	Einfache Tür mit Eingangs- und Ausgangsleser und dezentraler EMA-Unscharfschaltung
10e	Einfache Tür mit Eingangsleser, Türöffnungsknopf und dezentraler EMA-Unscharfschaltung
10f	Einfache Tür mit Eingangsleser und dezentraler EMA-Unscharfschaltung

Hinweise:
Mit der Taste **E** am Eingangsleser kann die EMA (Einbruchmeldeanlage) scharfgeschaltet werden. Dafür sind zusätzlich ein berechtigter Ausweis und die Eingabe der PIN erforderlich. Das Unscharfschalten der EMA erfolgt bei der ersten berechtigten Begehung, wobei hierbei ebenfalls eine zusätzliche Identifikation per PIN erforderlich ist. Bei den Modellen a bis c wird dies über das Ausgangssignal zum Scharf-/Unscharfschalten der EMA gesteuert.
Bei den Modellen **d** bis **f** wird die Scharf-/Unscharfschaltung über separate Impulse von 1 s Dauer gesteuert. Über ein angeschlossenes bistabiles Relais kann die EMA von mehreren Türen gesteuert werden, wobei die Signale aller Türen über eine ODER-Verknüpfung auf das Relais zu schalten sind. Die Signale **EMA: scharfgeschaltet** und **EMA: unscharf** sind auf die Eingänge der relevanten Türen zu doppeln.

20.8 Türmodell 14

Tür mit EMA-Steuerung



Signale:

Eingangssignale	Ausgangssignale
Door sensor (Türsensor)	Door opener (Türöffner)
Pushbutton: door open (Drucktaste: Tür geöffnet)	IDS: Disarm (EMA: unscharfschalten) [nur bei den Modellen **d** und **f** mit einem Impuls von 1 s]
IDS: Ready to arm (EMA: scharfschaltebereit)	Kamera/Motorschloss
IDS: Arrmed (EMA: scharfgeschaltet)	IDS: Arm (EMA: scharfschalten) [nur bei den Modellen **d** und **f** mit einem Impuls von 1 s]
Sabotage signal (Sabotagesignal)	Tür zu lange geöffnet (Einbruch)
IDS: Arming (EMA: Scharfschalten)	

Modellvarianten:

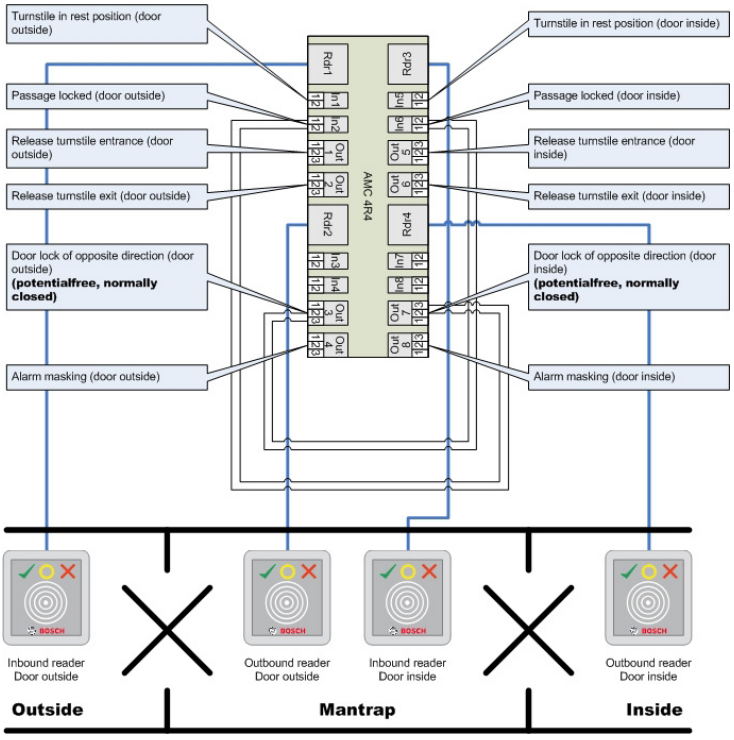
14a	Einfache Tür mit Eingangs- und Ausgangsleser und EMA-Scharfschaltung/Unscharfschaltung
14b	Einfache Tür mit Eingangsleser, Türöffnungsknopf und EMA-Scharf-/Unscharfschaltung
14c	Einfache Tür mit Eingangsleser und EMA-Scharf-/Unscharfschaltung
14d	Einfache Tür mit Eingangs- und Ausgangsleser und dezentraler EMA-Scharf-/Unscharfschaltung
14e	Einfache Tür mit Eingangsleser, Türöffnungsknopf und dezentraler EMA-Scharf-/Unscharfschaltung
14f	Einfache Tür mit Eingangsleser und dezentraler EMA-Scharf-/Unscharfschaltung

Hinweise:
Im Gegensatz zu Modell 10 können für das Türmodell 14 Leser mit oder ohne Tastenfeld verwendet werden. Ein weiterer Unterschied besteht in der Vergabe von Scharf- und Unscharfschalteberechtigungen: Nur Ausweisinhaber mit den entsprechenden Rechten können scharf- bzw. unscharfschalten.
Der Vorgang der Scharf- und Unscharfschaltung wird hierbei nicht über die Eingabe von PIN geregelt, sondern geschieht über einen Taster in Lesernähe, der die gleiche Funktion wie die Taste 7 bei Tastaturlesern besitzt. Nach Betätigung dieses Tasters wird der Zustand der Alarmanlage über die farbigen LEDs des Lesers angezeigt:
– Unscharf = abwechselnd grünes und rotes Blinken
– Scharf = rotes Dauerlicht
Die Scharfschaltung erfolgt mit der Präsentation einer berechtigten Karte.
Die Unscharfschaltung erfolgt durch Betätigung des Tasters und Präsentation einer berechtigten Karte.
Die Tür wird nicht automatisch freigegeben. Vielmehr muss die Karte dazu nach der Unscharfschaltung nochmals präsentiert werden.

20.9 Beispiele für Schleusenkonfigurationen

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).

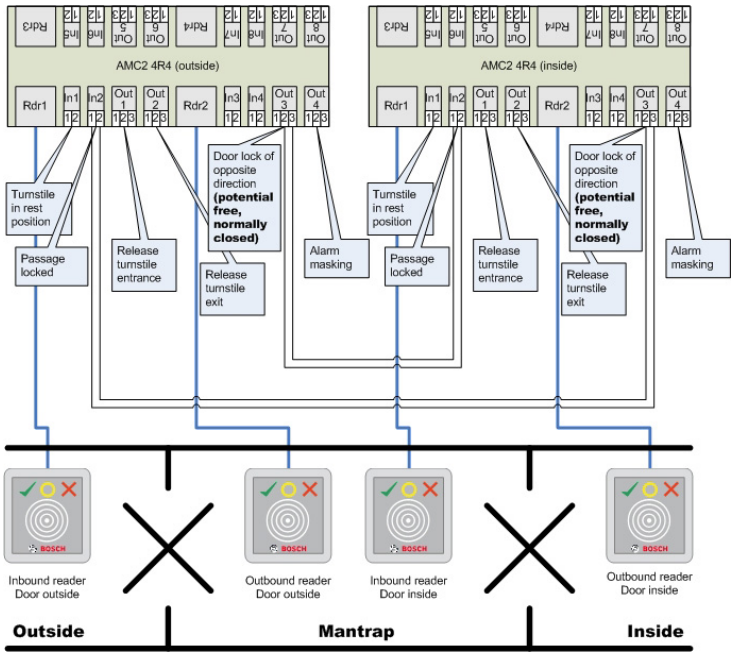
Schleusenkonfiguration mit 2 Drehkreuzen (Türmodell 03a)



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“ muss bei Deaktivierung geschlossen sein (Widerstand = 0). Für die Ausgänge 3 und 7 ist der Öffner zu verwenden.

Schleusenkonfiguration mit 2 Drehkreuzen (Türmodell 03a), die auf zwei Controller verteilt sind

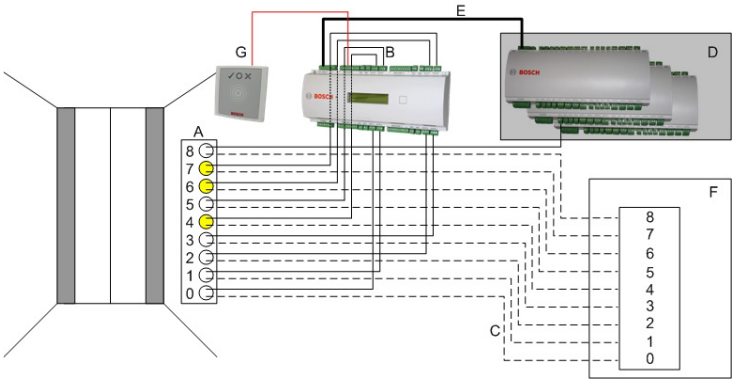


Verbindungen zu den Türverriegelungen für die Gegenrichtung gewährleisten, dass jeweils nur eines der Drehkreuze geöffnet werden kann.

Hinweis!
Das Ausgangssignal (Out) 3 muss potenzialfrei geschaltet werden (spannungsloser Modus). Das Signal „Türsperre für Gegenrichtung“ muss bei Deaktivierung geschlossen sein (Widerstand = 0). Für die Ausgänge 3 und 7 ist der Öffner zu verwenden.

20.10 Konfiguration von Türmodell 07

Die folgende Abbildung veranschaulicht die Anschlussverdrahtung eines Aufzugs unter Verwendung des Türmodells 07a:



Legende:

A = Tastenfeld des Aufzugs

B = (durchgezogene Linie) AMC-Ausgangssignale

C = (gestrichelte Linie) Anschluss an die Aufzugsteuerung

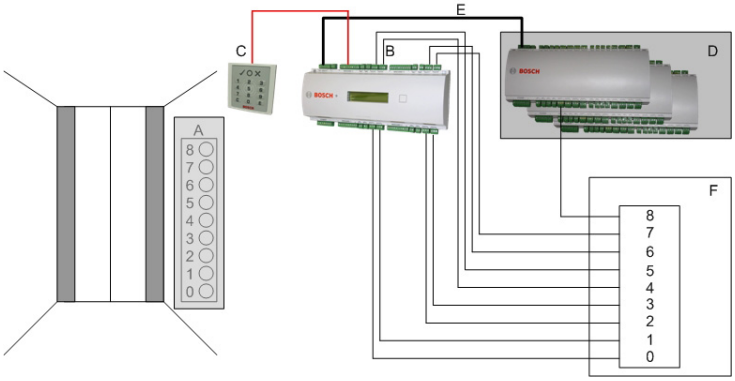
D = Möglichkeit zum Anschluss einer I/O-Erweiterungsplatine (AMC2-8I-8O-EXT, AMC2-16I-EXT oder AMC2-16I-16O-EXT)

E = Daten und Stromversorgung vom AMC zu den I/O-Platinen

F = Aufzugsteuerung

G = Leser (Türmodell 07a)

Die folgende Abbildung veranschaulicht die Anschlussverdrahtung eines Aufzugs unter Verwendung des Türmodells 07b:



Legende:

A = Tastenfeld des Aufzugs

B = (durchgezogene Linie) AMC-Eingangssignale

C = (gestrichelte Linie) AMC-Ausgangssignale

D = Möglichkeit zum Anschluss einer I/O-Erweiterungsplatine (AMC2-8I-8O-EXT, AMC2-16I-EXT oder AMC2-16I-16O-EXT)

E = Daten und Stromversorgung vom AMC zu den I/O-Platinen

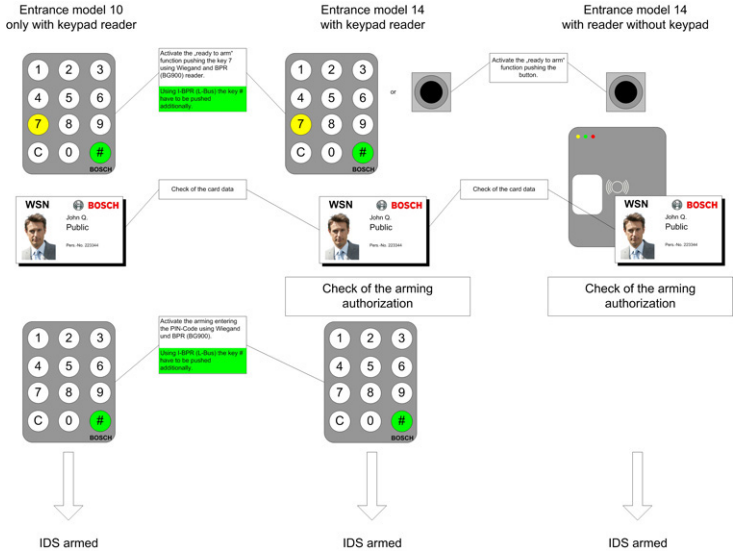
F = Aufzugsteuerung

G = Leser (Türmodell 07b)

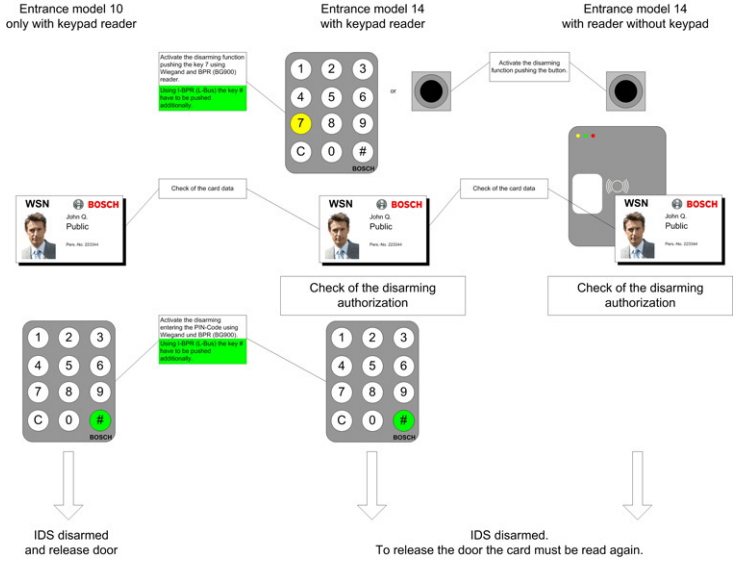
Hinweis!
Bei der Verdrahtung der einzelnen Etagen (bis zu 16) auf die Ausgänge des AMC werden zunächst die Signale des Controllers selbst und dann ggf. die ersten 8 einer I/O-Erweiterungsplatine angeschlossen. [Bei Verwendung von Wiegand-Erweiterungen (AMC2-4W-EXT) werden deren Ausgänge in aufsteigender Reihenfolge nach denen des AMC2-Controllers und vor den Ausgängen von I/O-Erweiterungsplatinen verwendet.] Deshalb können an einem AMC, der zur Aufzugssteuerung benutzt wird, keine anderen Türen oder weiteren Aufzüge parametriert werden.

20.11 Darstellung Scharf-/Unscharfschaltung

Vergleich der **Aktivierung** der Alarmanlage bei den Türmodellen 10 und 14:



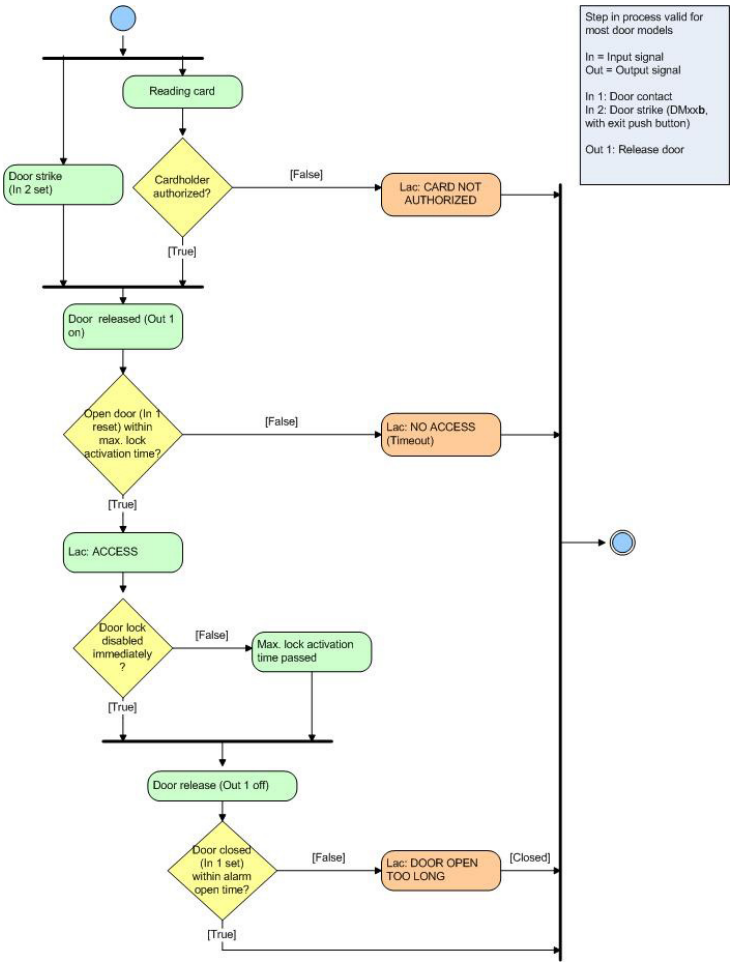
Vergleich der **Deaktivierung** der Alarmanlage bei den Türmodellen 10 und 14:



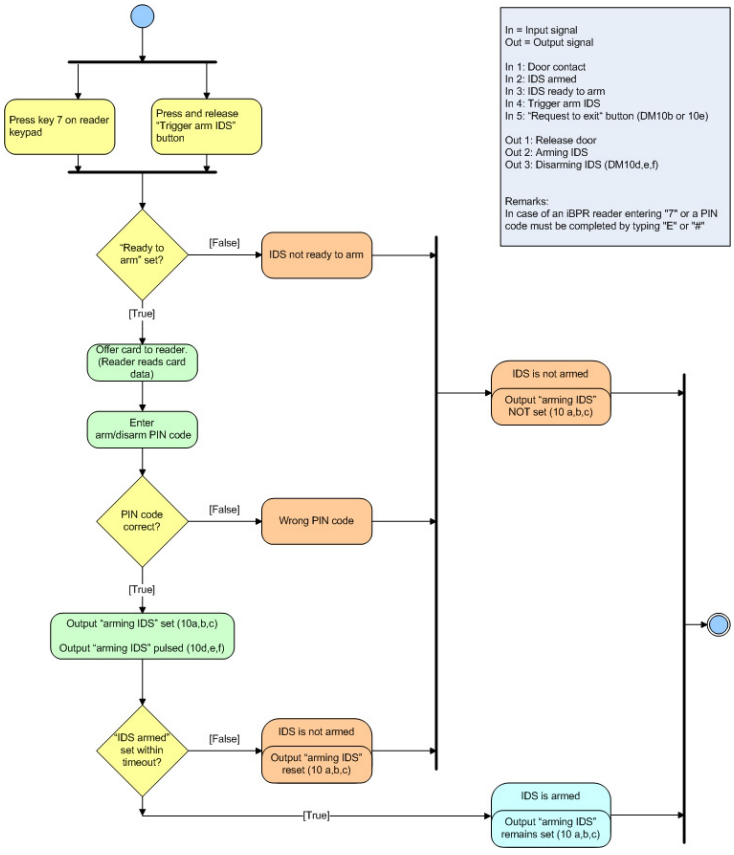
20.12 Abläufe bei der Zugriffskontrolle

Flussdiagramme von Zutrittskontrollverfahren

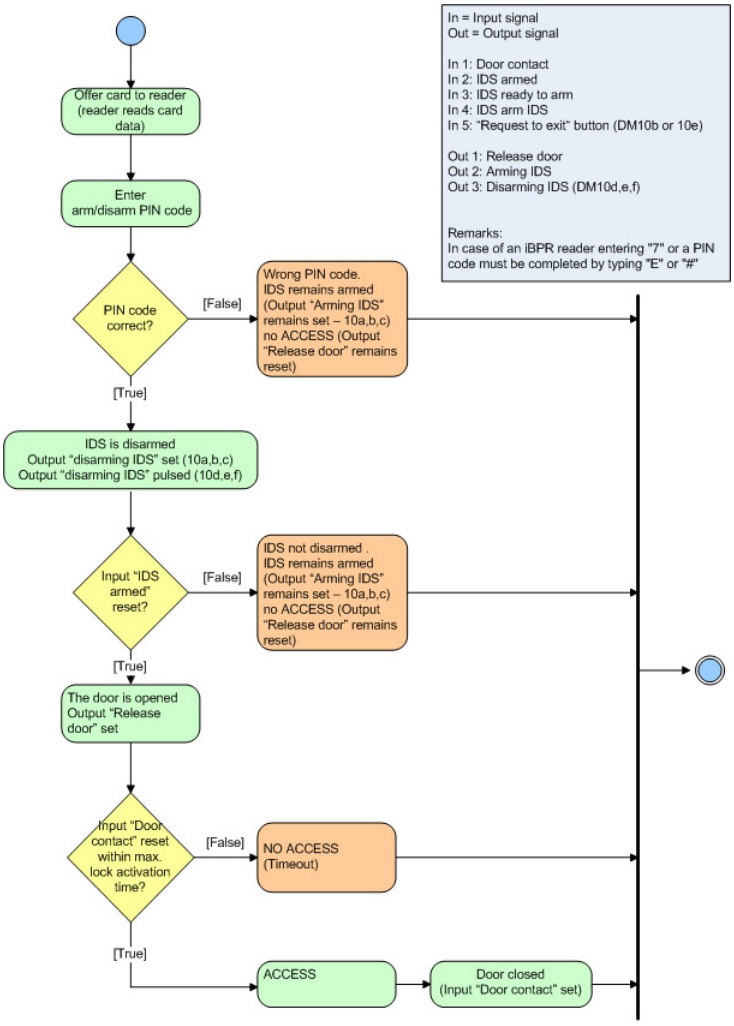
Türmodell DM01



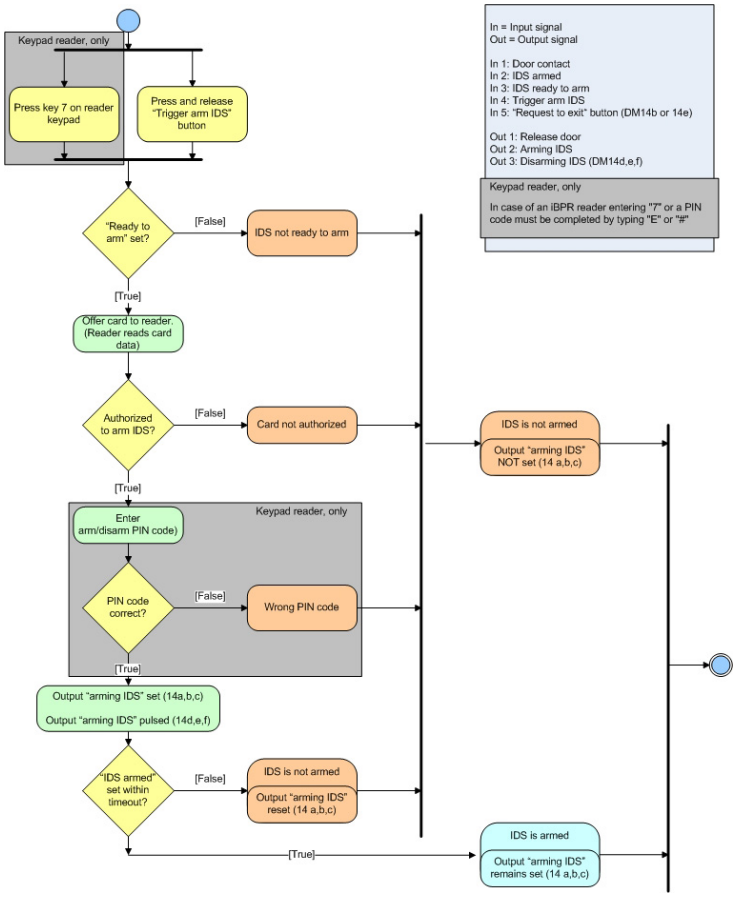
Türmodell DM10 – Scharfschalten



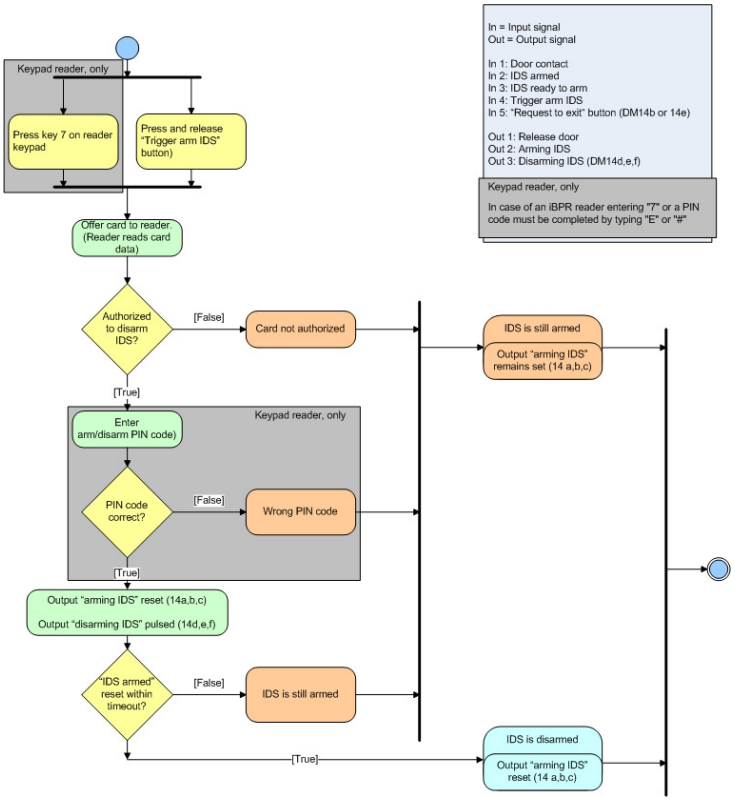
Türmodell DM10 – Unscharfschalten



Türmodell DM14 – Scharfschalten



Türmodell DM14 – Unscharfschalten



20.13 Access PE-Ports

Von den einzelnen Prozessen und Anwendungen in Access PE werden folgende Ports verwendet.

Verbindung zwischen ...	**Client/AMC**	**Server**
Client – LacSp	Nicht definiert	43434/tcp
AcPers – CP	Nicht definiert	20005/tcp
LacSp – AMC	10001/udp	54545/udp und höher

21 PIN-Varianten

In Access Personal Edition können jeder Person bis zu 3 persönliche Identifikationsnummern (**PIN**s) zugewiesen werden, die für unterschiedliche Zwecke verwendet werden können.

– **Verifikations-PIN**
  Diese PIN kann als zusätzliches Sicherheitsmerkmal an besonderen Eingängen (mit Tastaturlesern) verlangt werden. Durch den Vergleich der Verifikations-PIN mit den gespeicherten Daten wird überprüft, ob es sich tatsächlich um die betreffende Person handelt.
  Jede Person kann diese 4- bis 8-stellige PIN nach den allgemeinen Regeln (keine Zahlenreihen und keine Palindrome) selbst festlegen. [Der Parameter für die Länge der PIN gilt für Verifikations-, Scharfschaltungs- und Tür-PINs gleichermaßen.] Eine Verifikations-PIN kann auch mehrfach im System vorkommen.
  Wird keine separate Scharfschaltungs-PIN vergeben [d. h. so lange das Kontrollkästchen **getrennte EMA-PIN** (Konfigurator > Allgemeine Einstellungen) nicht aktiviert ist], kann die Verifikations-PIN auch zur Aktivierung/Deaktivierung der Alarmanlage verwendet werden.

– **Scharfschaltungs-PIN/EMA-PIN**
  Diese spezielle PIN wird ausschließlich zur Aktivierung und Deaktivierung einer Alarmanlage verwendet. Bei den Türmodellen 10 und 14 wird zuerst die Taste 7 oder der Türtaster betätigt.
  Jede Person kann diese 4- bis 8-stellige PIN nach den allgemeinen Regeln (keine Zahlenreihen und keine Palindrome) selbst festlegen. [Der Parameter für die Länge der PIN gilt für Verifikations-, Scharfschaltungs- und Tür-PINs gleichermaßen.] Eine Scharfschaltungs-PIN kann auch mehrfach im System vorkommen.
  Möchte die Person dagegen den Eingang lediglich passieren und muss neben dem Ausweis auch eine PIN eingegeben werden, muss die Verifikations-PIN verwendet werden.
  Sobald das Kontrollkästchen **getrennte EMA-PIN** (Konfigurator > Allgemeine Einstellungen) aktiviert ist, kann die Verifikations-PIN nicht mehr zur Aktivierung/Deaktivierung der Alarmanlage verwendet werden. Erst dann werden auch die entsprechenden Eingabefelder in der Personalverwaltung sichtbar.

Hinweis!
Aus Gründen der Kompatibilität mit früheren Versionen von Access PE Versionen ist die Verwendung von Scharfschaltungs-PINs in der Standardeinstellung ausgeschaltet.

– **Identifikations-PIN/ID-PIN**
  Diese PIN identifiziert wie ein Ausweis eine Person und muss deshalb im gesamten System eindeutig sein. Mit der Eingabe dieser PIN am Leser wird die Person identifiziert und erhält im Rahmen ihrer Berechtigungen Zutritt. Um ihre Eindeutigkeit zu gewährleisten, wird die Identifikations-PIN vom System generiert und der Person zugewiesen. Auch hier werden die allgemeinen Regeln (keine Zahlenreihen und keine Palindrome) beachtet.
  Die Identifikations-PIN unterliegt wie ein Ausweis den Einschränkungen der zugehörigen Person (Sperren, Zeitmodelle, Berechtigungen usw.).
  Je nach Leserprotokoll muss die Identifikations-PIN mit begleitenden zusätzlichen Zeichen am Leser eingegeben werden. Bei Lesern mit L-Bus bzw. I-BPR-Protokoll erfolgt die Eingabe der PIN mit **4 # (Enter) PIN # (Enter)**. Bei allen anderen Protokollen wird die PIN direkt eingegeben und mit **# (Enter)** abgeschlossen.
  Die Länge der PIN ist mit 4 bis 8 Stellen parametrierbar.

[**Hinweis:** Die PIN-Länge sollte im Verhältnis zur Anlagengröße gewählt werden, um zu verhindern, dass die PIN abzählbar ist. So sollte bei Anlagen mit 1000 Personen die PIN mindestens 6-stellig sein, damit entsprechende Fehlversuche zuverlässiger erkannt werden.]

Die oben beschriebenen PIN-Varianten sind alle personenbezogene PINs und werden deshalb auch in den Personaldaten angelegt und verwaltet. Eine vierte Variante ist die sogenannte Tür-PIN.

– **Tür-PIN**
  Hierbei erhält der Eingang (Konfigurator > Eingänge) eine PIN. Diese muss allen berechtigten Personen bekannt sein. Wahlweise kann an diesen Eingängen die Tür-PIN oder der Ausweis benutzt werden (= Funktion **PIN oder Karte**).
  Auch diese PIN kann 4- bis 8-stellig sein. Ist die Verwendung der PIN deaktiviert (z. B. durch ein Zeitmodell), kann der Zutritt ausschließlich per Ausweis erfolgen. Auch die Identifikations-PIN funktioniert in diesem Fall nicht.

Hinweis!
Die Varianten der Identifikations- und der Tür-PIN können bei den Türmodellen 10 und 14 mit EMA-Scharfschaltung nicht verwendet werden.

22 UL 294-Anforderungen

Die folgenden Bosch Ausweisleser wurden von UL auf Kompatibilität mit dem Bosch APE-SW Softwaresystem untersucht:

- LECTUS secure 1000 WI
- LECTUS secure 4000 WI
- LECTUS secure 5000 WI

Von UL untersuchte Funktionen:

- Leser mit 26-Bit-Wiegand-Format
- AMC2-Controller:
  - APC-AMC2-4WCF
  - API-AMC2-4WE
  - API-AMC2-8IOE
  - API-AMC2-16IOE
- APE-SW als zusätzliche Überwachungsausstattung

Nicht von UL untersuchte Funktionen:

- Videoverifikationssystem
- Lageplan-Anzeige und Alarmmanagement mit Lageplan- und Videoverifikation
- Video Player
- Ausweisdesigner
- Delta 1200 Serie
- Rosslare ARD-1200EM Serie
- LAC-Controller
- LACi-Controller
- APC-AMC2-4R4CF-Controller
  - BG 900-Leserschnittstellenprotokoll
  - L-BUS-Leserschnittstellenprotokoll
- Sicherheitssystem IDS – Scharfschalten/Unscharfschalten
- Aufzugbenutzung
- Anzeige- und Meldungstexte
- Verwendung des Einbruchmeldesystems

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