Access Professional Edition 3.0

BOSCH

en Configuration Manual

Table of contents

1   System Overview

Access Professional Edition System (hereunder referred to as
Access PE) consists of four modules

–   LAC Service: a process which is in constant communication
with the LACs (Local Access Controllers – hereafter
referred to as Controllers). AMCs (Access Modular
Controllers) are used as Controllers.

–   Configurator

–   Personnel Management

–   Logviewer

These four can be divided into server and client modules.

The LAC service needs to remain in constant contact with the
controllers because firstly it constantly receives messages from
them regarding movements, presence and absence of
cardholders, secondly because it transmits data modifications,
e.g. assignment of new cards, to the controllers, but mainly
because it carries out meta-level checks (access sequence
checks, anti-passback checks, random screening).

The Configurator should also run on the server; however it can
be installed on client workstations and operated from there.

The modules Personnel Management and Logviewer belong to
the Client component and can be run on the Server in addition,
or on a different PC with a network connection to the server.

The following Controllers can be used.

–   AMC2 4W (with four Wiegand reader interfaces) - can be
extended with an AMC2 4W-EXT

–   AMC2 4R4 (with four RS485 reader interfaces)

1.1 Restrictions and options

You can use Access PE for systems that do not exceed the following thresholds for connectable components and manageable data volume.

– Max. 10,000 cards
– Up to three cards per person
– PIN length: 4 to 8 characters (configurable)
– PIN types:
  – Verification PIN
  – Identification PIN
  – Arming PIN
  – Door PIN
– Access variants:
  – Only with card
  – Only with PIN
  – PIN or card
– Max. 255 time models
– Max. 255 access authorizations
– Max. 255 area-time authorizations
– Max. 255 authorization groups
– Max. 16 workstations
– Max. 128 readers
– Max. one I/O extension board (AMC2 8I-8O-EXT, AMC2 16I-16O-EXT or AMC2 16I-EXT) per Controller
– The following restrictions apply to each controller type:

Controller Readers/entrances	AMC2 4W	AMC2 4W with AMC2 4W-EXT	AMC2 4R4
Max. readers per AMC	4	8	8
Max. readers per interface/bus	1	1	8

Table 1.1: System limits — readers and entrances

Video system — restrictions and options
– Max. 128 cameras
– Up to 5 cameras per entrance
    – 1 identification camera
    – 2 back surveillance cameras
    – 2 front surveillance cameras
    – You can configure one of these cameras as an alarm and log book camera.

Offline Locking System (OLS) — restrictions and options
– Max. 1024 doors
– The number of entrances and authorization groups in the authorizations depends on the dataset length that can be written to the cards.
– Max. 15 time models
– Up to 4 periods per time model
– Max. 10 special days/holidays (from the online system)

1.2 Installation on one computer

The following figure shows a complete Access PE system installed on a single computer. Controllers can be connected via a serial interface. If a dialog reader is used then this is also connected via a serial interface.
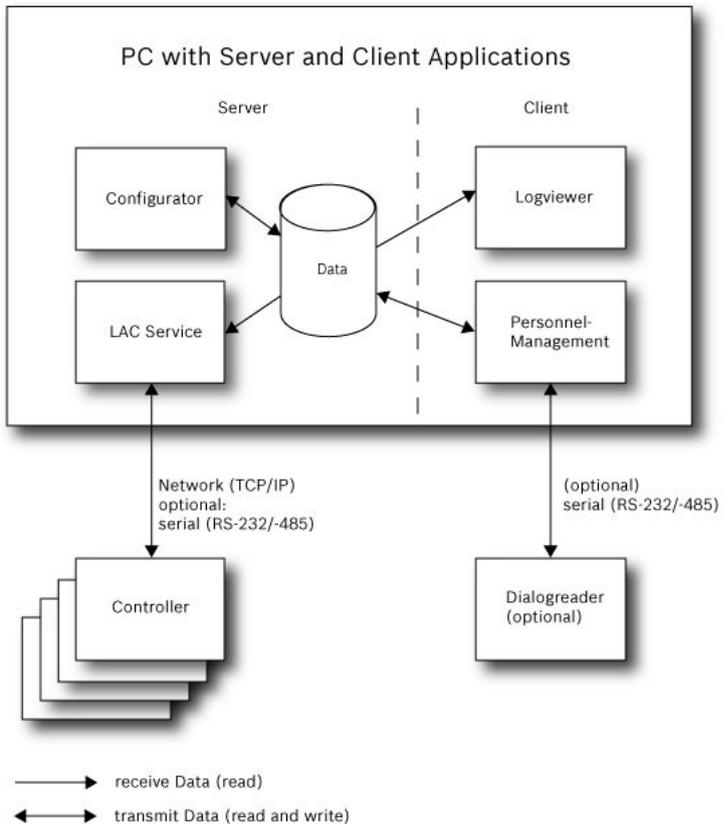
Figure 1.1: System Overview – Single Computer Configuration

1.3   Installation on multiple computers

The following figure shows an Access PE system distributed across 2 computers. This is particularly beneficial in cases where the Server to which the Controllers are connected is in a locked computer room, but the personnel data is maintained, for example, by the personnel department elsewhere.
The Access PE Client can be installed on up to 16 computers, which access common data on the Server via the network. Client workstations can be configured to use two monitors. Window positions maintained by the operating system, ensure a familiar operators' environment across login sessions.
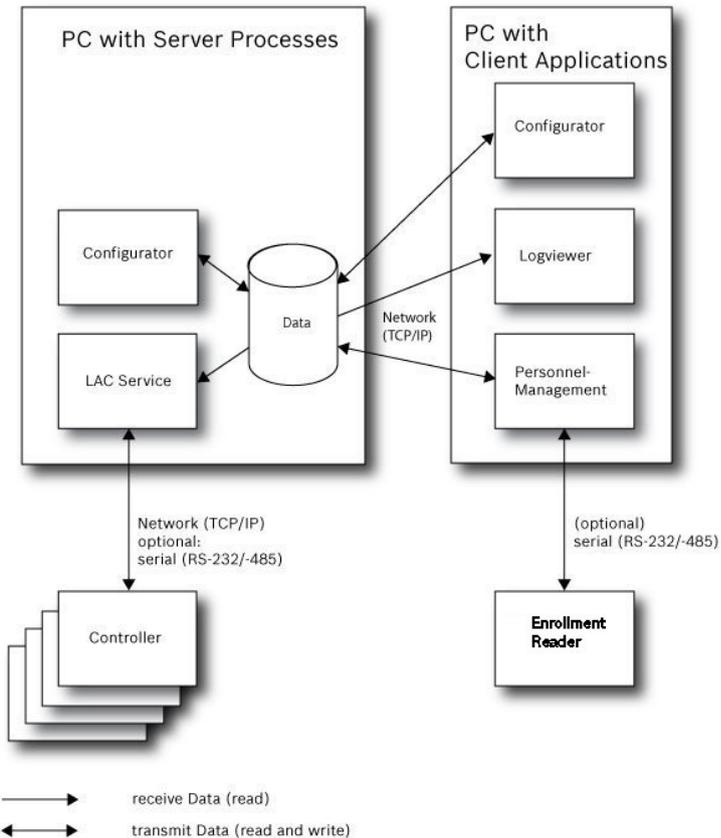
Figure 1.2: System overview – Distributed System

1.4   System Prerequisites

The installation of Access PE requires:

Operating Systems (one of):
–   Windows XP SP2 Professional
–   Windows XP SP3 Professional
–   Windows 2008 Server
–   Windows 7

Other software:

– To run the AmcIpConfig application supplied (and the Bosch Video SDK), you need the **.NET Framework 4.0** platform.
– To create and display lists and reports, you must install **Crystal Reports** applications.

Separate setups are available on the installation CD.

Hardware Requirements

Both Server an Client require a Standard Windows PC with:
– 4 GHz CPU
– 4 GB RAM at least
– 20 GB free disk space (Server)
– 1 GB free disk space (Client)
– 100 Mbit Ethernet Network Card (PCI)
– Graphical adapter with 1024x768 resolution and 32k colors
– Resolution support:
  – 1024 by 768
  – 1280 by 1024
  – 2048 by 768
  – 2560 by 1024
– CD/DVD-ROM Drive
– I/O Expansion Option
– USB Keyboard and Mouse

Notice!

Microsoft Windows XP Professional is required for any video integration.

Please consult the documentation of the chosen devices and ensure that you can use an operating system supported by both software and devices.

2 General

2.1 Introduction

Access PE is an Access Control System which has been designed to offer the highest standards of security and flexibility to small and medium sized installations.

Access PE owes its stability and upgradeability to a 3-tier design: The top tier is the administration level with its controlling services. All administrative tasks are carried out here, e.g. the registration of new cards and the assignment of access rights.

The second tier is formed by the Local Access Controllers (LACs) which govern each group of doors or entrances. Even when the system is offline a LAC is able independently to make access control decisions. LACs are responsible for controlling the entrances, governing door opening times or requesting PIN-codes at critical access points.

The third tier consists of card readers which, like the Controllers, are identical across all BOSCH access controls. They provide not only a consistently high degree of security, but also a simple upgrade and expansion path for the system, protecting previous investments.

Access PE multi-user version allows multiple workstations to control the system. Customizable user rights levels regulate access and guarantee security. In this way it is possible, for example, to maintain card data from one workstation whilst using another to verify whether an employee is present in the building.

Access PE offers exceptionally flexible configuration of access rights, time models and entrance parameters. The following list gives an overview of the most important features:

Quick & Easy card Assignment

Cards (up to three) can be assigned to persons either manually or using a dialog reader connected to a PC via a serial connection. Only one card can be active per person at any one time. When upgrading cards the old card is automatically overwritten and becomes invalid, thus preventing old cards from gaining access even if those responsible forgot or were unable to cancel them.

Access Rights (including Group Privileges)

Each person can inherit group privileges as well as having individual rights assigned to him. Privileges can be restricted by area and time to an accuracy of one minute. Group privileges can be used to grant and limit access rights for any or all cardholders simultaneously. Group privileges can be made dependent on time models which restrict their access to certain times of day.

Access tracking

By defining Areas it is possible to track and enforce a correct sequence of accesses. Even without monitoring, this configuration makes it possible to display a cardholder's location.

Anti-Passback

When a card has been read it can be blocked for a defined period from entering at the same access point. Hence it is possible to prevent "passback", where a user hands his card back across a barrier to provide access for an unauthorized person.

Automatic Cancelation of cards upon Expiration

Visitors and temporary staff frequently require access for a limited period only.

cards can be registered for a specific time period, so that they automatically lose their validity when that period expires.

Time Models and Day Models

A cardholder can be assigned to specific time models which regulate the hours in which that person has access. Time models can be defined flexibly using day models which determine how specific weekdays, weekends, holidays and special days deviate from normal working days.

Identification via PIN-Code

Instead of a card a person can use a special PIN-Code to enter.

Verification via PIN-Code

Particularly sensitive areas can be programmed to require additional PIN-Codes. This protection can in turn be made dependent on time models, so that, for instance, a PIN-Code is only required for access during holiday times or outside of defined working hours.

Flexible Door Management

Flexible parameterization of individual door models allows an optimum balance between security and comfort. The "shunt" or alarm suppression period can be individually specified to regulate for how long a door may remain open. In cooperation with an alarm system the access point can then optionally be locked.

Periodic Door Release

In order to facilitate access, door alarms can be shunted to release doors for specific periods. Door release periods can be defined manually or automatically via a time model.

Time and Attendance

Access points can be parameterized to record ingress and egress for time & attendance purposes.

Card Design

The graphical add-in module **Card Personalization** (CP) is fully integrated into the Access Control system to allow the operator to create cards without switching applications.

Assignment of Photos

If the add-in module **Card Personalization** (CP) is not activated photographic identification can nevertheless be imported and associated with cardholders.

Offline locking system

Areas which are not covered, for whatever reason, by the high-availability online access control system can nevertheless be locked offline.

Administration of video devices

Entrances can be equipped additionally with cameras to identify and track the movements of persons using them.

2.2   User Login

– Start the user applications using the desctop icons:

 Personnel Management

 Configurator

 Logviewer

 Map and Alarm Management

 Video Verification

or choose the tools via **: Start > Programs > Access Professional Edition**

– Start the **: Map & Alarm Management** application using the desctop icon or via **: Start > Programs > Access Professional Edition > Map & Alarm Management**.

– Start the **: Video Verification** application using the desctop icon or via **: Start > Programs > Access Professional Edition > Video Verification**.

– Start the **: Configurator** application using the desctop icon or via **: Start > Programs > Access Professional Edition > Configurator**.

– Start the **: Logviewer** application using the desctop icon 🖳
or via **: Start > Programs > Access Professional Edition >
Logviewer**.

– Start the **: Personnel Management** application using the
desctop icon 🐾 or via **: Start > Programs > Access
Professional Edition > Personnel Management**.

The system's applications are protected from unauthorized use.
A login with a valid **username** and **password** is required in order
to invoke the dialog-based subsystems.
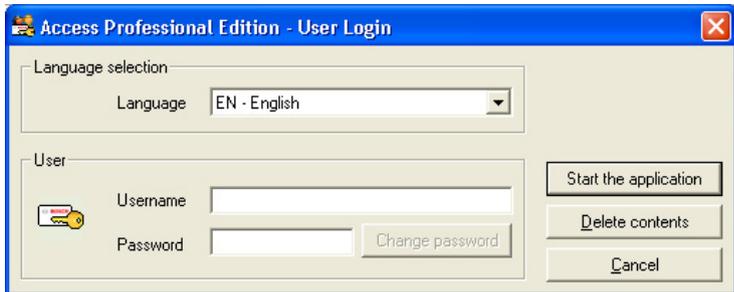
The upper drop-down list can be used to select the desired
interaction **language**. The default is that language which was
used to install the application. If there is a change of user
without restarting the application then the previous language is
retained. For this reason it is possible for a dialog box to appear
in an undesired language. In order to avoid this, please log in to
Access PE again.
Access PE applications can be run in the following languages:
– English
– German
– Russian
– Polish
– Chinese (PRC)
– Dutch
– Spanish

–   Portuguese (Brazil)

Notice!

All facilities such as device names, labels, models and user-rights schemes are displayed in the language in which they were entered.Similarly buttons and labels controlled by the operating system may appear in the language of the operating system.

If a valid username/password pair are entered then the button **:Change Password** appears. This can be used to start a new dialog to change the password.

The button **Start the application** checks the user's privileges and, based on these, starts the application. If the system is unable to authenticate the login then the following error message appears: **: Wrong username or password!**

Login via Personnel Management
If the user is already logged into the Access PE Personnel Management application, and if the user's rights include the other tools, he can start the **: LogViewer**, **: Configurator**, **: Alarm Management** and **: Video Verification** using the toolbar buttons.

If the user is already logged into the Access PE **Personnel Management** application, and if the user's rights include **: LogViewer**, then **: LogViewer** may be invoked directly using the

 button in the tools list, without requiring a separate login to the LogViewer application.

If the user is already logged into the Access PE **Personnel Management** application, and if the user's rights include **: Configurator**, then **: Configurator** may be invoked directly using the 🔧 button in the tools list, without requiring a separate login to the Configurator application.

If the user is already logged into the Access PE **Personnel Management** application, and if the user's rights include **: Video Verification**, then **: Video Verification** may be invoked directly using the 📹 button in the tools list, without requiring a separate login to the Configurator application.

If the user is already logged into the Access PE **Personnel Management** application, and if the user's rights include **: Alarm Management**, then **: Alarm Management** may be invoked directly using the 🔍 button in the tools list, without requiring a separate login to the Configurator application.

2.3   Menu and Tool bar

The following functions can be invoked via the menus, the icons in the toolbar or specific keyed shortcuts.

Function	Icon/ Shortcut	Description
Menu **File**		
New	🗐 Crtl + N	Clears all configuration dialog boxes (except for default settings) in order to define a new configuration.

Function	Icon/ Shortcut	Description
Open...	📂 Crtl + O	Opens a dialog box to select a different configuration for loading.
Save	💾 Crtl + S	Saves changes into the current configuration file.
Save as...		Saves the current configuration into a new file.
Activate Configuration		Activates a loaded configuration and saves the hitherto active configuration.
Send Configuration to LAC		Propagates saved configuration changes to the LAC-Service.
List recently active configurations		Opens configurations directly, circumventing the **Open** function's selection dialog.
Exit		Shuts down Access PE Configurator.

Function	Icon/ Shortcut	Description
Menu **View**		
Tool bar		Toggles display of the tool bar (default = on).
Status bar		Toggles display of the status bar at the bottom edge of the window (default = on).

Function	Icon/ Shortcut	Description
Menu **Configuration**		
General		Opens the **General Settings** dialog for setting up Controllers and general system parameters.
Input signals		Opens the dialog box for parametrizing **input** signals.
Output signals		Opens the dialog box for parametrizing **output** signals.
Entrances		Opens the **Entrances** dialog for parametrizing doors and card readers.
Areas		Opens the **Area Configuration** dialog for dividing the protected installation into virtual areas.
Holidays		Opens the **Holidays** dialog box for defining holidays and special days.
Day Models		Opens the **Day Models** dialog box for defining time periods within a day for the activation of access functions.
Time Models		Opens the dialog **Time Models** for defining timezones dependent on days of the week or calendar.

Function	Icon/ Shortcut	Description
Personnel Groups		Opens the dialog box **Personnel Groups** for dividing personnel into logical groups.
Access Authorization Groups		Opens the dialog box **Access Authorization Groups** for defining groupings of authorizations to entrances.
Offline locking system		Opens the **Offline locking system** dialog for configuring special elements of the installation (Entrances, Time models, Authorization groups).
Display Texts		Opens the dialog box **Display texts** for editing the texts to be displayed at the card readers.
Log Messages		Opens the dialog box **Log Messages** for editing and categorizing log messages.
Additional personnel fields		Opens the dialog box **Additional personnel fields** for defining data fields for personnel.
Wiegand - cards		Opens the dialog box **Wiegand-cards** for defining the structures of card data.
Administering video devices		Opens the **Video devices** dialog for configuring cameras to be used in video verification.

Function	Icon/ Shortcut	Description
Map Viewer and Alarm management		Opens the **Map Viewer** for an areal view of maps and control devices and the alarm list for alarm handling.
Menu **?** (**Help**)		
Help topics		Opens this help text.
About Access Professional Edition - Configurator		Displays general information about Access Professional Edition - Configurator

2.4 General system settings

General system settings are displayed below the list of controller settings. These are valid for all installations.

Parameter	Default value	Description
Country Code	00	Some card data are appended to the manually entered card number.
Customer Code	056720	

Parameter	Default value	Description
Poll interval on serial connected LAC in ms	200	The time interval in milliseconds between pollings by the LAC-Service to verify intact connections to a controller. Range of values for poll interval: 1 to 500 Possible values for read-timeout: 1 to 3000
Read-Timeout on serial connected LAC in ms	500	
Create TA data at	00:01	Specification of the time at which the Time & Attendance data file should be created.
Export personnel and TA data	deactivated	When activated this option causes time & attendance data to written continuously to the export file. When not activated the data file is created at the time specified by the parameter **Create TA data at**.
The file containing attendance time-stamps is created in the following directory: C:\Program Files\Bosch\Access Professional Edition\PE\Data \Export Under the name **TA_<Current date YYYYMMDD>.dat**		

Parameter	Default value	Description
Show welcome/ leaving message	activated	Given appropriate reader type and settings (**Arriving**, **Leaving** or **Check ok** in the Entrances dialog) the reader will display those welcome and leaving texts which are stored for the cardholder in the Personnel Data dialog of the Personnel Management application. Does not apply to Wiegand readers.
Show cardholder name in display	aktiviert	Readers with display will show the **Display Name** as stored in the cardholder's Personnel Data. Does not apply to Wiegand readers.
Number of digits	4	Determines the number of digits a verification or arming PIN requires. This setting applies also to the door PIN which can be set during the configuration of entrances. Possible values: 4 to 8

| Parameter	Default value	Description
use separate IDS PIN		If no separate IDS PIN is set, then a verification PIN can be used to arm the IDS. Only if the check box is selected do the input fields for the arming-PIN become active in the Personnel dialog screen. In this case the verification PIN can no longer be used to arm the IDS.

Parameter	Default value	Description
Count of retries before blocking	3	Number of failed attempts to enter the PIN. If the cardholder mistypes the PIN this many times then s/he will incur a system-wide block which can only be removed by an authorized system user (Personnel Management). Possible values: 1 to 9
Directory paths to: Database Log file Import files Export files DLL files Image data Test-Logging	C:\Program Files \BOSCH \Access Professiona l Edition\PE \Data... \Db \MsgLog \Import \Export \Dll \Pictures \Log	These are the default paths. The directories for import, export and image files can be changed.

Notice!

When using Wiegand controllers and readers, in order to use Identification-, arming- or door-PINs the Wiegand card definition **PIN or Card** (Nr. 6) needs to be activated.

2.5   Layout of the main dialog

The dialog consists of the following parts:
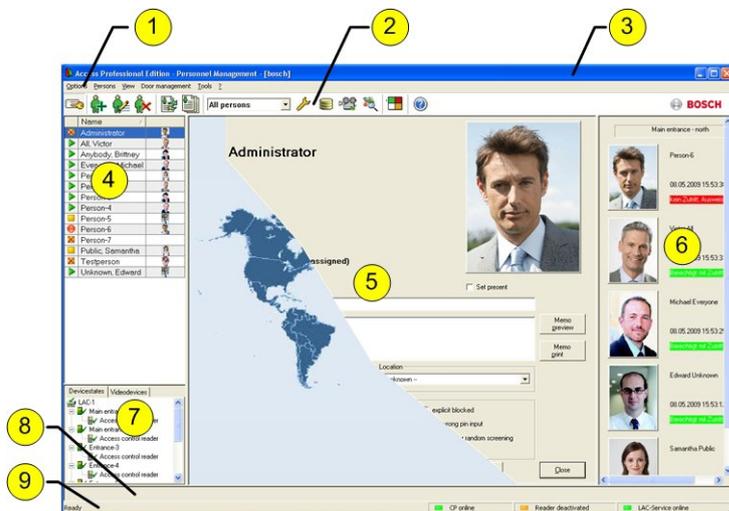
1 =   **Menu bar** — contains dialog functions displayed
       according to the menu order.

2 =   **Toolbar** — contains shortcut keys for the most
       important dialog functions.

3 =   **Title bar** — conforms to Windows standard and
       contains buttons for minimizing or closing the dialog
       window. The name of the registered user appears in
       square brackets.

4 =   **Personnel table** — lists all people known in the system
       along with their attendance status (authorization and
       location).

5 = **Dialog field** — the first time this field is opened or when no user is logged in, it shows a neutral image (map of the world). When an entry is selected from the Personnel list, this person's data is displayed.

6 = **Online swipe** — lists the last five people (with database image) that have swiped their cards at the entrance selected.

7 = **Device status** — lists the configured devices and entrances along with their connection status. Enables door control functions.

8 = **Event display** — faults are indicated by a flashing red bar (flashes three times) with details on the cause.

9 = **Status bar** — displays information on buttons and menu entries that are controlled with the cursor. Status display on card personalization program (CP), dialog readers and LAC service.

When you enable the **Video Verification** component, additional facilities will be added to this dialog; see Personnel Management.
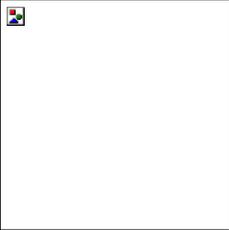
When you enable the **Video Verification** component, additional facilities will be added to this dialog.

2.6 Menu and tool bar

The following functions are available via the menus or the icon buttons.

Function	Icon	Description
Menu **Options**		
Refresh		Refreshes the Personnel list

Function	Icon	Description
Exit		Exits the **Access PE Personnel Management** application
Menu **Persons**		
New person		Opens a blank personnel and card data dialog
Modify person		Opens the personnel and card data dialog with the data of the selected person.
Delete person		Deletes the selected person (after confirming a safety check dialog).
Transmit selected person to the LAC service		Transmits the selected person's data to the LAC service and reports success.
Transmit all persons to the LAC service		Transmits all persons' data to the LAC service and reports success.
Set all persons absent		Sets all persons absent (after confirming a safety check dialog).
Set location of all persons present to **unknown**		Sets the location of all persons to unknown and deactivates access tracing for the next booking of each person.
View/print reports		Calls the dialog for creating report lists.

Function	Icon	Description
	List control	Restricts the persons shown to those of the selected group.
Menu **View**		
Symbol bar		Toggles display of the tool bar. Default = on.
Status bar		Toggles display of the status bar. Default = on.
Personnel data: State Card No. Personnel-No. Company Personnel Group Phone Location		Choice of columns displayed in the personnel overview in addition to symbol and name columns. Default = State - Company - Location
Menu **Door management**		
open door	These functions are also available via	The entrance selected in the device list is displayed and can be opened (one-off).

Function	Icon	Description
Long-term open	the context menu (right click on the desired door/entrance)	The entrance selected in the device list is displayed and can be opened (long-term).
lock door		The entrance selected in the device list is displayed and can be locked.
Menu **Tools**		
User logon		Log in/off Personnel management.
Execute the Configurator		Executes Configurator and transfers data from personnel management.
Execute log viewer		Executes Log viewer and transfers data from personnel management.
Execute Video verification		Starts the application for executing video verification.
Execute Alarm and Map management		Starts the Map viewer and Alarm management processing application.
Video panel		Shows four displays in the dialog field for individual video camera feeds.
Properties		Opens a dialog box for general system settings.
Menu **?** (Help)		

Function	Icon	Description
Help topics	⓪	Opens this help file.
About Access Professional Edition - Personnel Management		Displays information about Personnel Management.

2.7 Layout of the main dialog
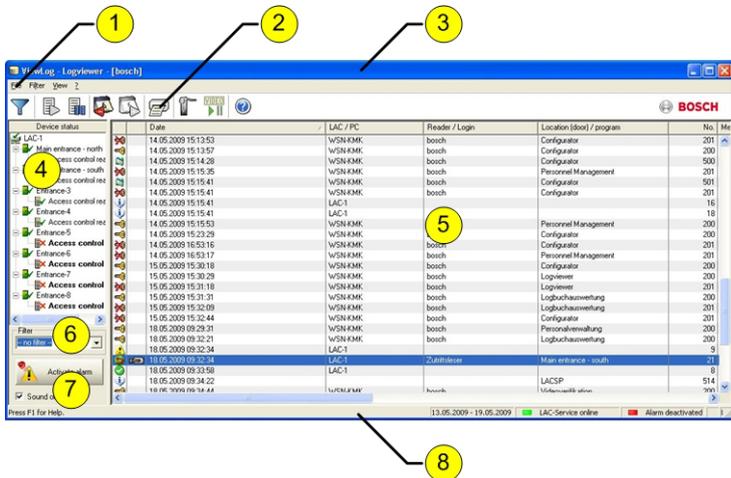
1 = **Menu bar** - Contains all dialog functions arranged in menus.

2 = **Tool bar** - Contains the most important dialog functions as icon buttons

3 = **Title bar** - Conforms to Windows standard and contains buttons to minimize and close the main dialog window. The name of the current user is displayed in square brackets.

4 =   **Device status** - List of the configured devices and
entrances along with their connection status.

5 =   **Message list** - List of messages arrived hitherto. The
display can be modified by specific filter settings.

6 =   **Filter selection** - Predefined and customized filters
can be selected from the combo-box.

7 =   **Alarm activation** - Triggers the activation/
deactivation of alarms for messages. An incoming
message can be accompanied by an acoustic signal.

8 =   **Status bar** - Dates of the log files opened. Status of
the LAC Service. Alarm settings.

2.8   Menu and Tool bars

The following functions are available for log evaluation via
menus and icon buttons.

Menu	Function	Icon button	Description
File	Print...	🖩	Print the log messages displayed
	Exit		Closes the LogViewer application.
Filter	Filter definition	▼	Opens the message filtering dialog.

Menu	Function	Icon button	Description
	Continuous mode on		Starts continuous message display. This icon is only active when the function is not already running and the message filter is set to the current day. Continuous message display is the default setting.
	Continuous mode off		Pauses the continuous message display. This icon is only active when continuous message display is running.
	Events previous day		Switch to previous day's messages.
	Events next day		Switch to next day's messages.
View	Symbol bar		Hides/Displays the tool bar. Default = on.
	Status bar		Hides/Displays the status bar. Default = on.
without a menuitem			

| Menu	Function	Icon button	Description
		📌	
		▶❚❚	
? (Help)	Help topics	🌐	Opens this help file.
	About LogViewer		Opens Help About Access PE LogViewer.

2.9 Enrollment Configuration

Enrollment Readers (RS 232) > Tools > Settings calls a dialog in which it is possible to perform basic configuration tasks (activate, modify) from any workstation.

– Administrative workplaces, where persons are assigned cards, can be fitted with an enrollment reader. This must be parameterized and configured according to the manufacturer's specifications, or those delivered with the device. If an enrollment reader is set up then manual card checking is deactivated.

The required settings for supported readers are:

Reader name	BAUD	D	P	S
DELTA 1200 Prox RS232	9600	8	N	1
DELTA 1200 iClass RS232	57600	8	E	1
DELTA 1200 USB Hitag, Legic, Mifare	9600	8	N	1
DELTA 1200 RS232 Hitag, Legic, Mifare	19200	8	N	1
Rosslare ARD-1200EM USB	9600	8	N	1
LECTUS secure 5000 MD	9600	8	N	1

| D =	Data bits	N =	none
P =	Parity	E =	even
S =	Stop bits	O =	odd
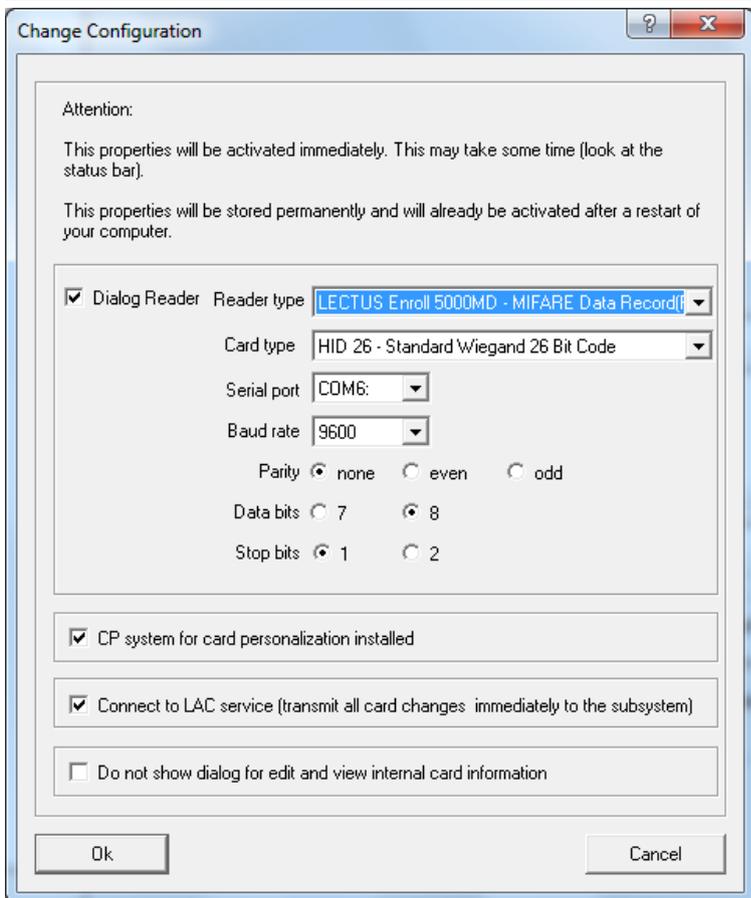
– If the system has been installed with the optional **Card Personalization** (CP) module then the corresponding check box is selected in settings. Unchecking this box blocks all functions for card design/creation.

–   In addition the automatic transfer of personnel data via
Connection to the LAC Server is also checked. This box
should always remain checked.
–   The display of card information during card assignment can
be disabled here. This display is only necessary when,
contrary to default settings (see General Settings in Access
PE Configurator) card data are required which do not
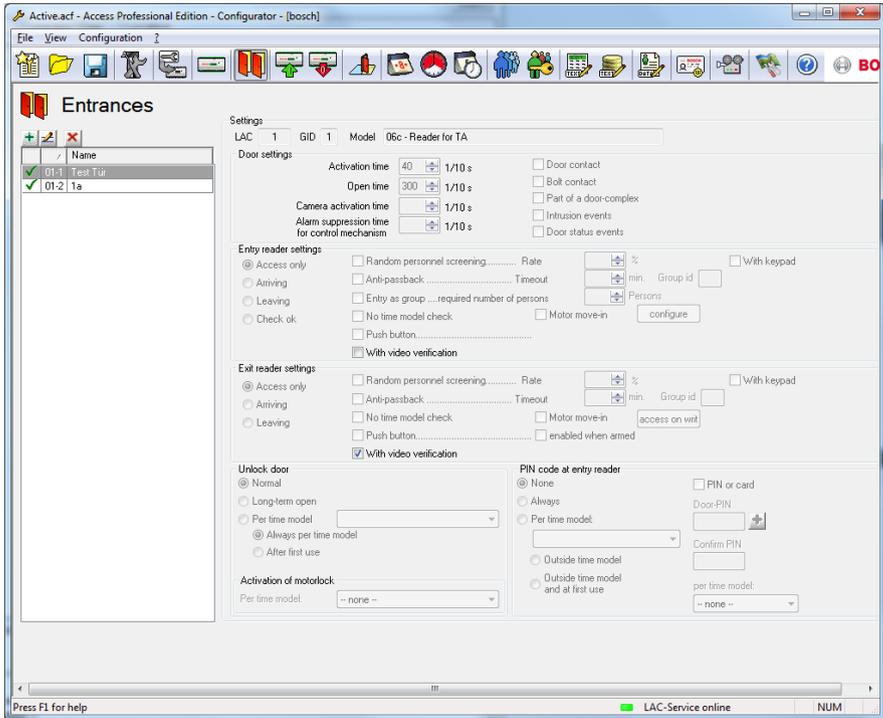conform to the company standard settings.

2.9.1   Enrollment via AMC connected readers

Make sure that at least one reader is configured with a **Door
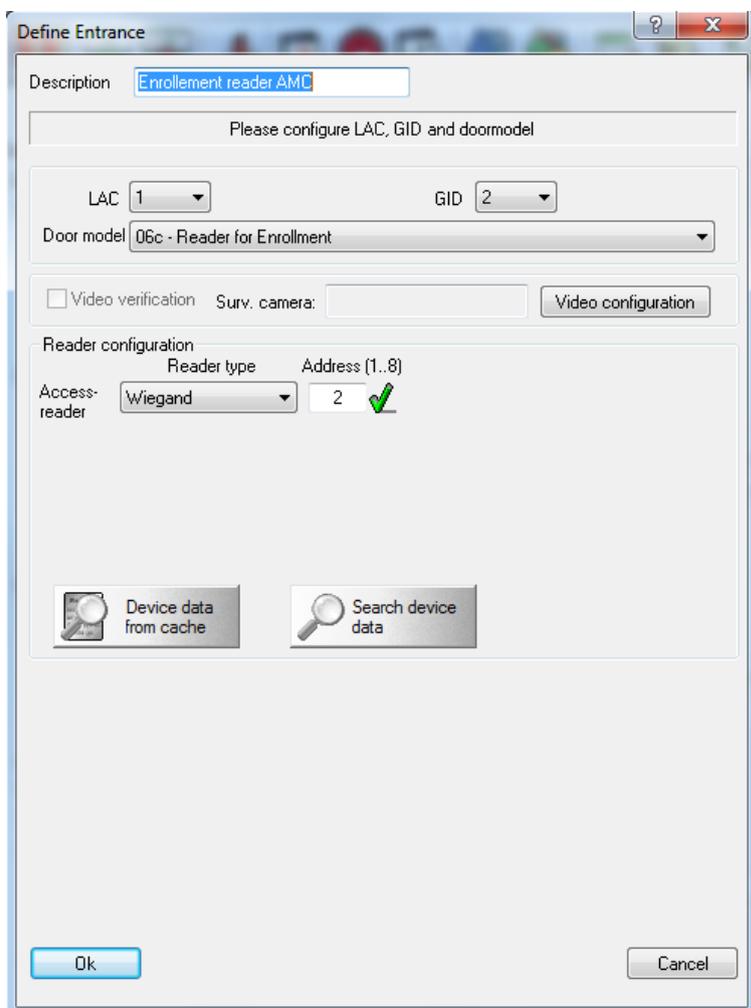Model 06c**, which is the door model for enrollment.
Start the **Configuration Browser** and select a **Local Access
Controller (LAC)** (e.g. AMC2...)
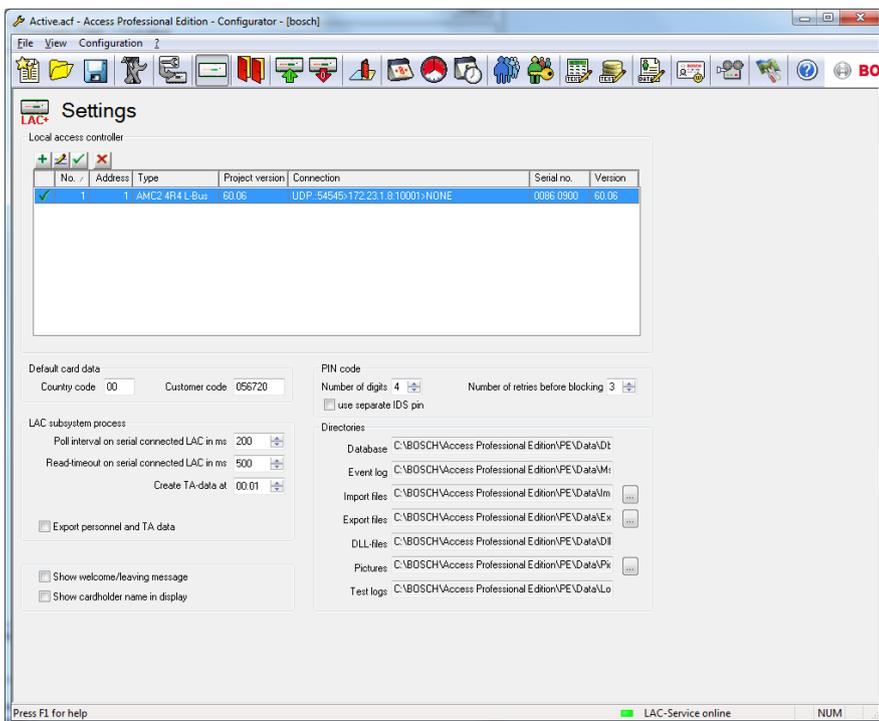
Click the **Entrances** symbol an add a new Entrance reader:


The dialog window **Define Entrance** opens:

In this dialog:

–   Enter a Description (e.g. Enrollment Reader AMC)
–   Select a LAC and a group ID (GID)
–   Select a reader type (e.g. Wiegand)
–   Select a number between 1 and 8 as Access Reader
     Address

Click OK to conform the enrollment configuration.

To assign the configured enrollment reader to a specific workstation, you have to change tot he APE client.
– Select Tool > Properties.
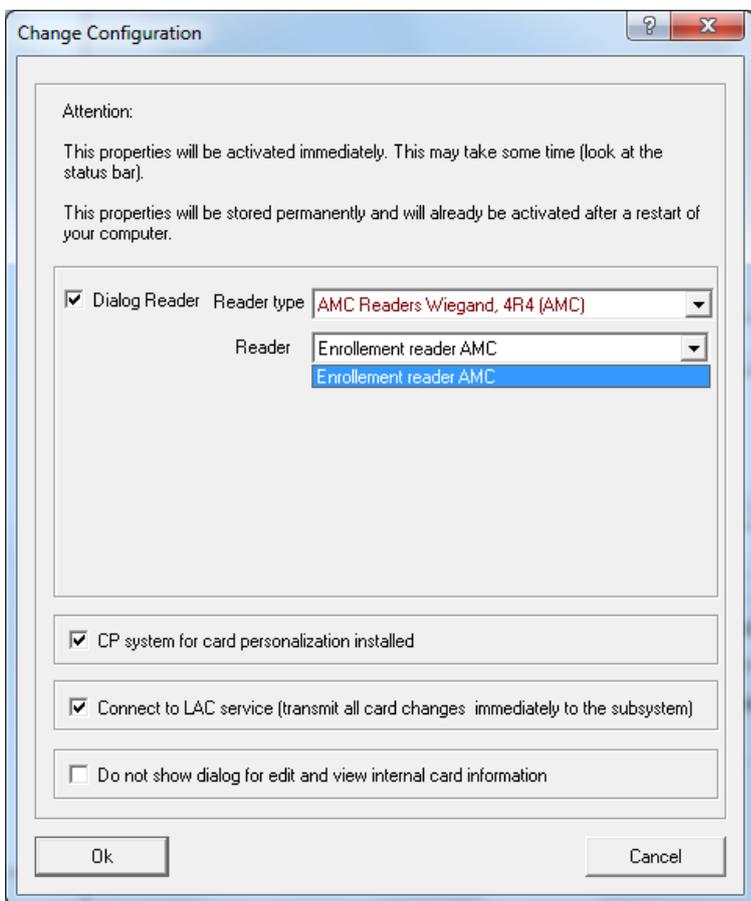
Select an available enrollment reader to activate the enrollment process.
Confirm that your enrollment reader is online.
If you don't get an immediate response, restart the Personnel Management dialog.

3 Configurations

The composition of a system (what entrances there are where, how many readers and of what type, how access authorizations are set up etc.) is saved in special files. Any number of these configuration files can exist — however, only one can apply to the current system. This makes it possible to test new scenarios, carry out test runs and carry out quick system changes.

3.1 Creating new configurations

All Access PE configurations are stored in the folder **C:\BOSCH \Access Professional Edition\PE\Data\Cfg** (unless non-default paths and folder names are chosen during installation). Two configuration files are created by the installation, namely **Active.acf** and **Default.acf**. Whereas Active.acf contains example data, which may be helpful to the user, Default.acf contains only predefined system data.

System data include:

– The area **--outside--**.
– Example holidays and special days
– The personnel groups **Employees** and **Visitors**
– Display texts for readers.
– Logbook texts

Upon startup Access PE always uses the configuration **Active.acf.**

A configuration may find itself in different states, and it is important to distinguish between them

– An **Active** configuration is one whose definitions, settings etc. are currently being used by the running system.
– An **Open** (aka loaded) configuration is one which is currently being edited by system users. It may later be stored in a separate .acf file and/or later activated, but **until it is activated it has no influence on the running system**.

Any number of configurations can be defined and stored in
Access PE. Because new configurations can be created and
modified independently of the running system, it is possible, for
example, to define new areas which will be included in the
monitored installation at a later date.
Using the 🏛 button in the toolbar the default configuration
Default.acf, with its basic settings, can be opened (loaded). If
modified to create a new configuration it should be saved under
a different and appropriate name.

The 💾 button starts a file-saving dialog in the Cfg directory.
The default filename **untitled.acf** should be replaced by a more
explanatory filename.
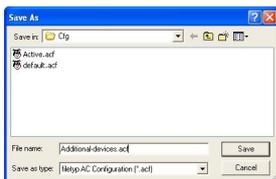
⚠️ **Warning!**

The default configurations active.acf and default.acf should
never be renamed or overwritten. Always store modifications of
default.acf under a new name.

3.2 Opening configurations

Configurator is always started with the configuration **Active.acf**.
If a different configuration is to be used, then the 🗁 button can
load an existing configuration from the folder **C:\BOSCH\Access
Professional Edition\PE\Data\Cfg** (by default).
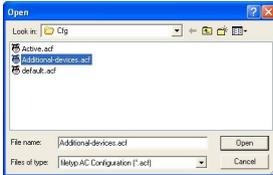
If the user wishes to make changes to or expand an existing
configuration to be activated at a later date, then s/he can open
a basic configuration, modify it and then save it under a
different name. In this way it is possible to re-use and expand
upon previous configurations, and one does not have to start
every time from the very basic settings in **default.acf.**

> **Notice!**
> The active configuration too can be saved as a working copy
> under a new name, and this loaded and worked on at a later
> date.

3.3   Activating a new configuration

Configurator offers the possibility of maintaining multiple
configurations in multiple .acf files. The active configuration is
always stored in the file **Active.acf** .

Caution!
As **active.acf** is overwritten when a new configuration is
activated, it is urgently recommended that the user make a
backup copy of the active configuration under a new filename.

Configuration files must be opened before they can be
activated. Therefore a previously modified and saved
configuration should be opened.
In order then to activate the opened configuration please
proceed as follows, either:
–   Menu: **File** > **Activate configuration** or

–   Use the   button in the toolbar.
The activation then proceeds in stages:
–   First confirm the safety check.
    **: Do you really want to replace the current configuration
    with the new configuration?**
–   The hitherto active configuration is backed up as a file with
    the name format: **$yyyyMMddhhmmss -Active.acf** (y =
    year; M = month; d = day; h = hour; m = minute; s =
    seconds).
–   The currently open configuration is then stored under the
   filename **Active.acf** i.e. the old active configuration will be
    overwritten!
A information box shows the name of the saved file: **: New
configuration was saved as <filename>!**

3.4 Propagating configurations to the controllers

After making changes in the active configuration **Active.acf** it is necessary to propagate these changes down to the controllers. This can be started in two ways:

– Menu **File** > **Send configuration to LAC service**
– Using the 🖳 button in the toolbar

The following dialog appears, in which you can choose which configuration data will be propagated to the controllers.
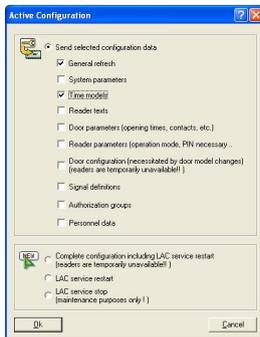
Modified and saved data are preselected. You may select further items or deselect already selected items.

When you have selected which data should be propagated to the controllers then click **OK**.

Configuration data	Propagation to the LACs becomes necessary if...
General refresh	... log messages, additional fields or card definitions have been modified.
System parameters	... LAC-Hardware has been modified.
Time models	... Holidays, Day or time models have been modified
Reader texts	... Display texts have been modified.

Configuration data	Propagation to the LACs becomes necessary if...
Door parameters	... at Entrances, one or more of the following have been modified – the opening time (in 1/10 sec.) – the door contact – data relating to door control (opening times, contacts, time profiles etc.)
Reader parameters	... at Entrances, one or more of the following have been modified – data for the entry or departure readers – alarm suppression time (in 1/10 sec.). – anti-passback behavior of the entrance – buttons to open the door
Door configuration	... at Entrances, the door model has been modified. **Notice:** Reinput and modification of the address (serial number, reader-type) can only be carried out in the input mask Define Entrance.
Signal definitions	... parametrization of input or output signals has been modified
Authorization groups	... authorization groups without time models have been modified, or a new time model added or deleted.

Configuration data	Propagation to the LACs becomes necessary if...
Personnel data	... personnel data has been added or modified, or access authorization groups or time models have been modified.
Complete configuration including LAC service restart	.. the initial configuration of Access PE has been concluded. A reset of the controller can also cause the complete configuration to be downloaded to the controllers.
LAC service restart	... in general settings the polling interval or the time for saving the TA data file has been modified.
LAC service stop	This option should only be used in exceptional circumstances, e.g during deinstallation in order to avoid a restart of the computer.

Configurator sends a command to the **: LAC Service** to propagate the configuration data to the controllers. The LAC Service is responsible for the communication to and from the controllers. This program is set up at installation time, as a Windows Service which is automatically started upon booting. Successful propagation to the LAC Service is reported as follows:
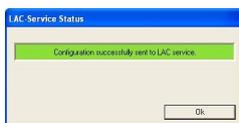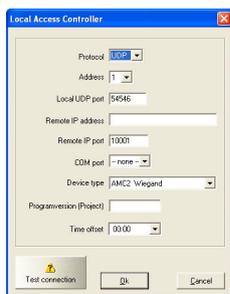
4 Controllers

The Local Access Controllers (LACs) are the points in Access PE at which most access control decisions are made. Except for system-wide control functions, such as the access sequence check, the controllers can take independent decisions regarding who is granted access. For this reason, they have all access-related data in their own memory so that limited and restricted offline operation is also possible.

In Access PE it is predominantly AMC2 (Access Modular Controller) controllers that are used. For replacements within legacy systems, LACi (Local Access Controller integral) controllers can also be configured.

4.1 Defining and modifying new controllers

The buttons ▣ (add) and ▨ (modify a selected list element) invoke a dialog box for configuring the interfaces between Access PE Server and the controllers.

Every controller must have a protocol assigned to it. The following are settings are available:

COM Connection via a serial (COM) interface requiring the COM interface number (COMx)

CIP Connection via TCP/IP over COM requiring the virtual COM interface number (COMx); only available for LACi with IP/Serial transducer.

UDP Connection via UDP requiring the local UDP port and the IP-Address (or the network name under DHCP).

> **i** **Notice!**
> Please ensure that when using CIP or UDP interfaces the DIL address switch on the controller at position **5** is set to **ON**.

Depending on which protocol is chosen different additional settings will be required, as shown in the following table:

Paramet er	COM	CIP	UDP	Note
Address	1 to 8	1 to 8	always 1	When using COM or CIP the DIL-switch on the Controllers must have the same address setting.
Local UDP-Port	Deacti-vated	Deacti-vated	consecutive	The port via which the Access PE server is to receive data from the controller. A new controller will receive the next free port, depending on its position, but this entry can be overwritten.
Remote-IP-Address	Deacti-vated	Deacti-vated	IP address or network name	In networks using DHCP the newtwork name should be used, otherwise the IP address of the controller.

Parameter	COM	CIP	UDP	Note
Remote-IP-Port	Deactivated	Deactivated	unmodifiable value 10001	The port on the controller to receive data from the server.
COM-Port	Pull-down list of COM-Ports	Pull-down list of COM-Ports	<none>	The number of the COM port on the Access PE server to which the controller is connected.
LAC-Type	Pull-down list of Controllers	Pull-down list of Controllers	Pull-down list of Controllers	The following controller types are available:
	AMC-Wiegand			with Wiegand reader interface
	AMC-RS485-BG900			with RS485 reader interface
	AMC-RS485-L-BUS			with RS485 reader interface for I-BPR reader
	LACi-BG900			with RS485 reader interface

Paramet er	COM	CIP	UDP	Note
	LACi-L-Bus			with RS485 reader interface for I-BPR reader
Program version (Project)	none	none	none	may be used to specify the software version
Time offset	Combo box for specifying the time offset from the server in cases where the AMC is in a different time zone. Possible values are -12:00 to +12:00 in 30 minute intervals. All times transmitted from the server to the AMC (or vice versa) are adjusted by this offset. Local AMC times are used in event messages and can be viewed in the Event Log.			

Controller (LAC) Test

Having made the settings the reachability of each controller can be tested before saving. Thus any incorrect settings can quickly be found and corrected or completed.

The **Test LAC** button at the lower edge of the dialog box attempts to connect to the controller using the current settings. This test can also be performed, after defining the controller, by selecting it in the list box and clicking the ▨ button.

The test displays one of three results using the icons below, which are also shown in the first column of the list.

 The controller has not yet been tested.

 Test was successful. A connection was made.

 Test was unsuccessful.

Notice!

These icons indicate only the result of the last test performed. They are **not** a continuously updated indicator of the reachability of each controller.

A controller test consists of various phases, some of which may be skipped:

– Startup the LAC-Services.
– Download the LAC-Program
– Wait states:
    – Read configuration data from the controller.
    – Receive a status message from the controller
– Display the result of the connection attempt.

Depending on the result, the **LAC-Service Status** dialog is displayed. After clicking **OK** the test result is displayed in the list.

4.2 Controller Settings

The dialog box **General Settings**, invoked by the button is where Local Access Controllers (LACs) are defined and configured.

Buttons for the following functions are displayed across the top
of the list:

⊞   **Add** a new controller.

⊿   **Modify** the selected controller.

☑   **Test** the selected controller.

☒   **Delete** the selected controller.

The list field includes all created controller and shows the
following informations:

Column	Contents	Description
	✕, ⚠, or ✔	Result of the LAC Test: negative, not yet tested or successful
No.	1 to 128	Number of the controller.
Address	1 to 8	The configured address of the controller as set by its DIL switch. In the case of UDP protocol this is always 1.
Type	AMC-Wiegand, AMC-4R4 BG900 AMC-4R4 L-Bus LACi BG900 LACi L-Bus	Selected controller type.

Column	Contents	Description
Projectversion	Example: 37.02	Special project program version loaded by the Controller.
Connection	Example: UDP.: 54545>AMC-DEMO: 10001>NONE	Interface parameters: Protocol: local UDP-Port>Nework name or IP-Address: Remote IP-Port>COM-Port
Serial-No.	Example: 9999 9999	Serial-No. of the controller.
Version	Example: 37.02	Program version loaded by the Controller.

The lower part of the dialog box contains general settings for all devices and applications in the Access PE installation.

5   Signals

The controllers' input and output signals can be used, for
example, to determine door states and control doors.
Furthermore, these signals can also be used to associate
additional control functions with access requests. This allows
you to control and activate cameras, optical or acoustic
signaling devices, and alarm systems.

5.1   Input signals

Whereas door control and other control signals, along with
status messages, are configured under **Entrances,** the **Input
Signals** dialog is concerned with the detailed definition of signal
types and their monitoring.

When this dialog is invoked the first controller is always
displayed. Please use the como-box **LAC** and the consecutive
numbering scheme to select the desired controller. The
standard controller definition process creates 8 input and 8
output signals. If the controller is able to handle more than
these, then the button **: I/O boards +/-** can be used to create
further signals.

All defined signals appear in the list. The settings for each signal
are shown in the various columns of the list as well as in the
parameter controls for the selected signal which appear below
the list. All settings can be carried out both in the list and in the
parameter controls below the list, as described in the following
table.

Column	Parameter	Description
1 (no label)	-	Describes the state of the signal: = Signal activated = Signal deactivated By double-clicking on the icon the status can be toggled back and forth
Board	Board	Number of the board where the signal is located. 0 = Base board 1 = Extension board This parameter is not modifiable
Signal	Signal	Number of the signal on the board (1 to 16). This parameter is not modifiable

Column	Parameter	Description
Signal name	Name	Name of the signal. In the standard settings each signal receives the name: Signal <Board-No.>-<Signal-No.> A double click in this column allows the user to edit the name.
Message	Message on... State change (open / close): Alarm:	Graphic display of the parameter setting in the List: (only possible for Signal type **Analog**) A double click in this column cycles through the message icons.
	Camera	A camera from the selection list can be assigned to certain input signals. When the relevant signal is activated, a log book message is created; you can also use this message to retrieve camera images.
- only on time model...	during time model	Shows the selected time model. A double click in this column allows the user to select from a list of time models
<none>	Signal type Digital Analog	The option **Analog** activates the radio buttons to select the resistance values.

Column	Parameter	Description
R serial	Serial resistance	A double click in this column opens a list of resistance values. Selecting a serial or parallel resistance value automatically resets the signal type to Analog.
R par.	Parallel resistance	

Notice!

Not all of the listed values can be combined with each other - a statement regarding the use of suitable resistance pairs can be found in the installation manual for the AMC2 device.

5.2 Output signals

This dialog box is used to parameterize the output signals and, if necessary, to define further signal boards.

When this dialog is invoked the first controller is always
displayed. Please use the combo-box **LAC** and the consecutive
numbering scheme to select the desired controller. The
standard controller definition process creates 8 input and 8
output signals. If the controller is able to handle more than
these, then the button **: I/O boards +/-** can be used to create
further signals.
All defined signals appear in the list. The settings for each signal
are shown in the various columns of the list as well as in the
parameter controls for the selected signal which appear below
the list. All settings can be carried out both in the list and in the
parameter controls below the list, as described in the following
table.
Along with the settings described here it is possible to define
additional **conditions** which must be fulfilled in order to activate
the output signal.

Column	Parameter	Description
1 (no name)	-	Describes the state of the signal: = Signal activated = Signal deactivated By double-clicking on the icon the status can be toggled back and forth.
Board	Connection	Number of the board where the signal is located. 0 = Base board 1 = Extension board This parameter is not modifiable.

Column	Parameter	Description
Signal		Number of the signal on the board (1 to 16). This parameter is not modifiable.
Signal Name	Name	Name of the signal. In the standard settings each signal receives the name: Signal <Board-No.>-<Signal-No.> Signals which have been defined and activated in the **Define entrance** dialog are displayed here with their entrance names and their signal descriptions. A double click in this column allows the user to edit the name.
Message	Message on... State change	Graphic display of the parameter setting in the List: ℹ️ A double click in this column toggles the setting on and off.
- only in time model...	during time model	Display and selection of the time model.

Column	Parameter	Description
Type	Action type: Momentary Follow state Toggle	Three action types are available: A double click in this column cycles through the action types in the order shown here.
Delay	Delay	Delay in seconds before the signal is transmitted [0 - 9999].
Duration	Duration	Delay in seconds before the signal is transmitted [0 - 9999 ; 0 = always or until halted by a cancellation message.
Pulse	Pulsating	Activates pulse transmission, otherwise the signal is transmitted at a constant rate. A double click activates this option but marks it as undefined with a ? icon until duration and number of pulses have been defined. Thereafter it is marked with a ✔.
Pulse duration	Duration	Duration of the pulse.
Pulse count	Num. of pulses	Number of pulses per second.

Actiontype: Momentary
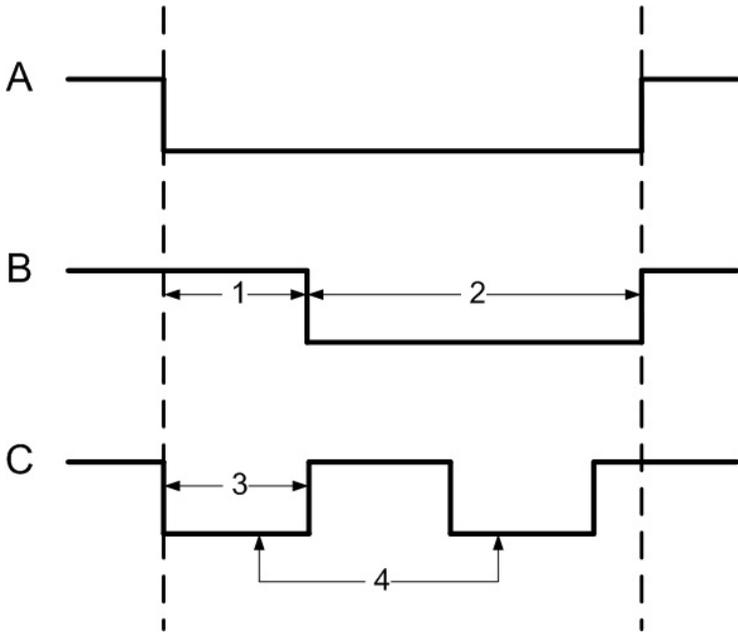
Actiontype: Toggle
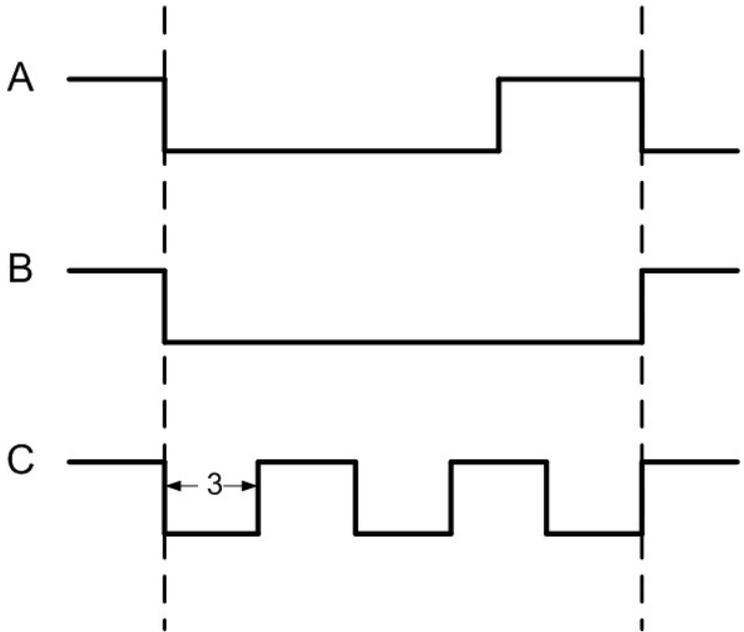
Actiontype: Follow state
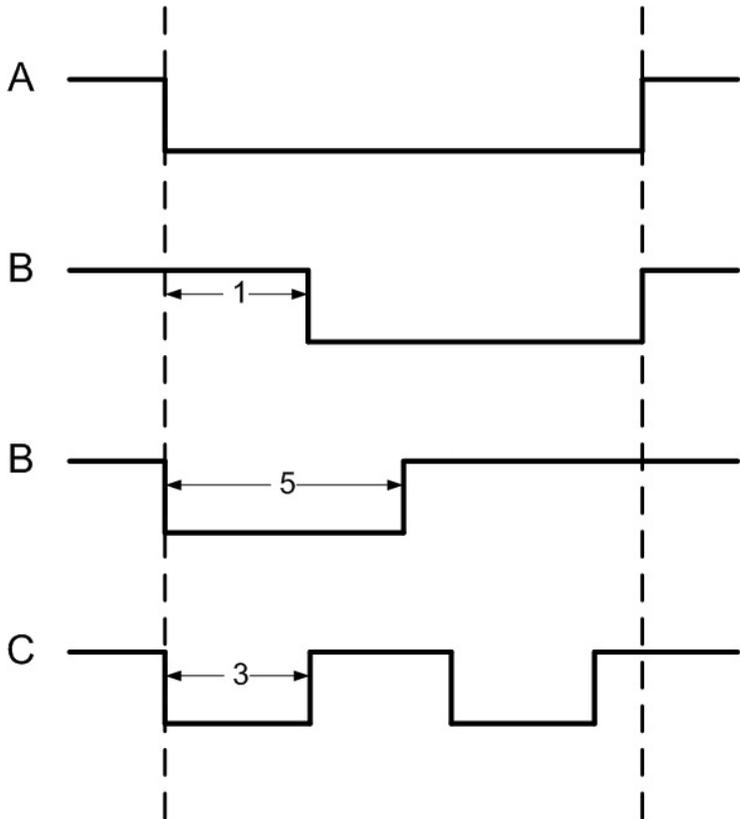
A =	polled state
B =	steady
C =	pulsed
1 =	delay time
2 =	action period
3 =	pulse width
4 =	pulse count (= 2)

5 =	max. activation time

5.3   Defining conditions for output signals

The dialog box **Output signals** offers, apart from settings, a way of defining additional conditions which allow the transmission of output signals only under specific circumstances.

These special conditions are defined in the lower-right dialog area for those signals selected in the main list.
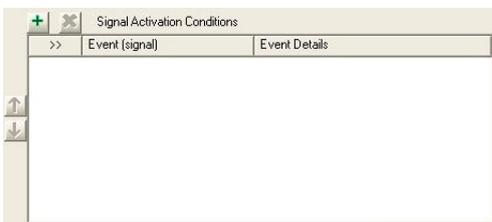
Press the ◾ button to open the dialog below. You can use this dialog to configure the relevant conditions.
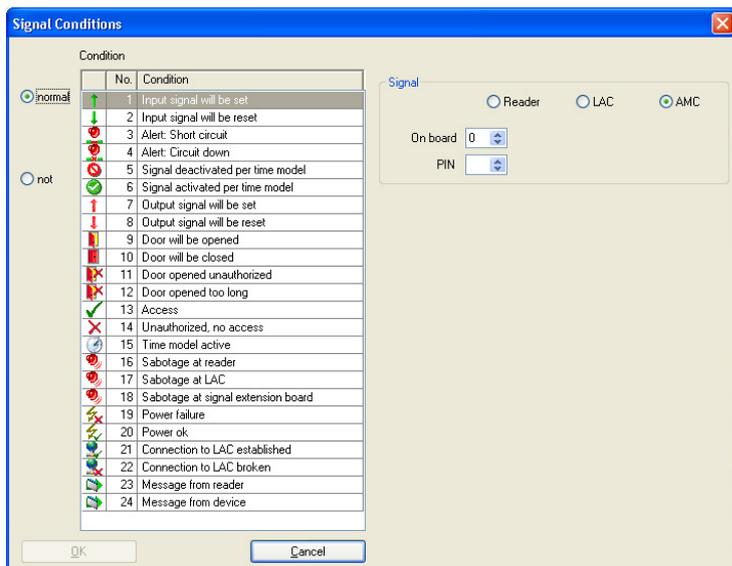
Depending on which activation condition is chosen it may be necessary to enter further information, e.g. the name of the door reader, before the dialog can be confirmed by clicking **OK**. You can apply any number of conditions to each signal. You must reopen the dialog for each new condition by pressing the 🔼 button.

Notice!

It is only possible to select those signals and installations (entrances, readers, doors) which are connected to the controller whose output signal you are parameterizing.

When defining the condition you can choose between the modes **normal** (if the condition needs to be fulfilled) and **not** (if the condition must not be fulfilled).
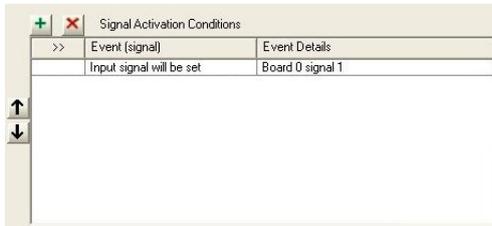
Further conditions are made dependent on the first by choosing one of the operators **and**, **and not**, **or** or **or not**.
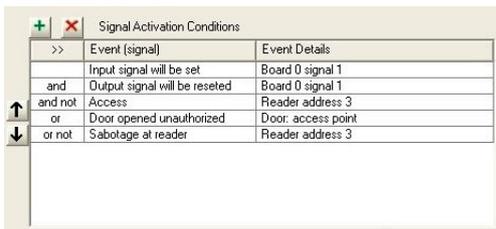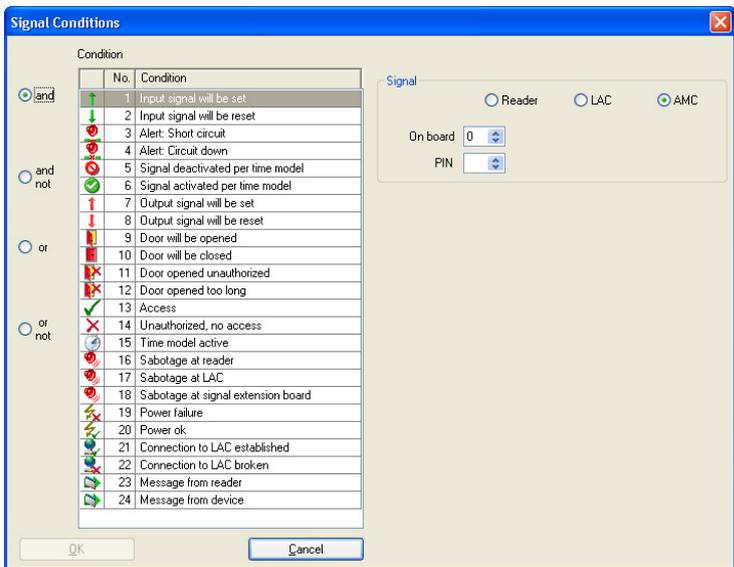
The conditions are processed in the order they are listed. If this order does not reflect the procedure required, conditions can be repositioned. Select the relevant condition from the list and then reposition it by pressing the ↑ or ↓ button.

What supplementary information is required for which condition can be found in the following table:

Condition	Further information required
Input signal will be set	Information about the device type where the signal is located. Selection of the board. Selection of the connection.
Input signal is set	
Alert: Short circuit	
Alert: Connection broken	
Signal deactivated by time model	
Signal activated by time model	
Output signal will be set	
Output signal will be reset	
Door will be opened	Selection of the entrance. GID (Group ID) is set automatically.
Door will be closed	
Door opening unauthorized	
Door open too long	
Access	Selection of the reader.
Unauthorized, no access	
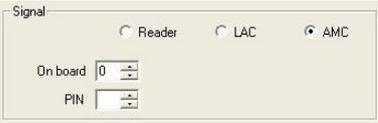
Condition	Further information required
time model active	Selection of the time model. Time model ▾
Sabotage at reader	Selection of the reader. Device — Reader ▾
Sabotage at LAC	No further information necessary.
Sabotage at signal extension board	Selection of the board. Device — Board ▢
Power failure	No further information necessary.
Power ok	
Connection LAC -> APE established	
Connection LAC -> APE broken	
Message from reader	Selection of the message from the predefined list. Selection of the reader. Message ▾ Device — Reader ▾
Message from device	Selection of the message from the predefined list. Selection of the board. Message ▾ Device — Board ▢

5.4   Creating Extension boards

You can configure extension boards in the dialogs for both **input signals** and **output signals**. The settings configured in one dialog will be activated in the other.

You can use and configure three types of extension board in the Access PE access control system — all three types are processed via one of the signal dialogs.

–   **AMC2 4W-EXT** - to extend the interfaces of a Wiegand AMC (AMC2 4W)
–   **AMC2 8I-8O-EXT** — 8 further signals each
–   **AMC2 16I-16O-EXT** — 16 further signals each

Above the list window please select the desired Controller from the **LAC** combo-box. These controllers are created with 8 signals on the main board (=0).

To create the extension board click the button marked **I/O Board +/-** , which will bring up the following dialog:
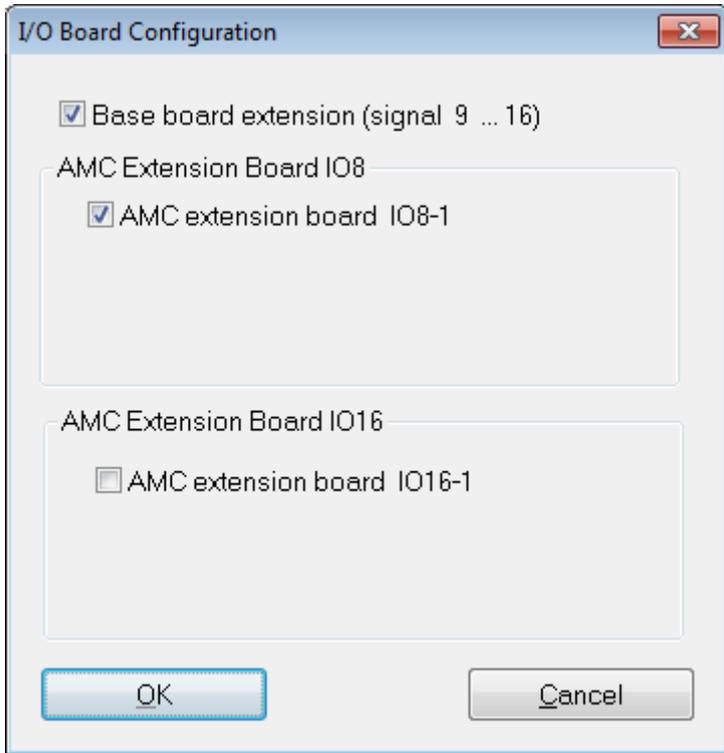
By checking one or two of the boxes the following settings can be made:

– **AMC Main Board** (Signals 9 - 16)

Creates a Wiegand Extension board **AMC2 4W-EXT**. This board has the same interfaces as an AMC2-4W controller (4 Wiegand reader interfaces, 8 input and 8 output signals). However it can not function independently and must be connected to an AMC2-4W.

This extension can only be used with an AMC2-4W.

An AMC2 4W-EXT can be configured with **one** additional IO-Board.

In the list field for the input and output signals the extension board, like the controller itself, is given the board number 0, and the signals numbered 9 through 16.

– **AMC Extension Board IO8**
Board with 8 input and 8 output signals as an extension to
the controller's interfaces.
This board can be connected to any AMC2 controller and,
when used with an AMC2-4W controller, can even be
combined with a Wiegand extension board AMC2 4W-EXT
In the list field of the input/output signals the extension
board is created with the board number 1 and signals
numbered 1 through 8.

– **AMC Extension Board IO16**
Board with 16 input and 16 output signals as an extension
to a controller's own interfaces.
This board can be connected to any AMC2 controller and,
when used with an AMC2-4W controller, can even be
combined with a Wiegand extension board AMC2 4W-EXT
In the list field of the input/output signals the extension
board is created with the board number 1 and signals
numbered 1 through 16.

Notice!
The settings made here for **I/O boards** apply equally to input
and output signals, and can be made in either of the two
dialogs.

6   Entrances

When we talk about entrances, we always mean a whole made up of several components that belong to an access control system. Along with the door (which can also be a turnstile, a mantrap, a barrier or an elevator), the system also includes one or more readers and potentially buttons and control units (bolts, motorlocks etc.). The system can also contain optical or acoustic signaling devices or cameras as additional control functions.

6.1   Creating and modifying door models

A new entrance can be defined using the ▣ button or via the context menu within the list (right-click and select **New Entrance**). The entrance name, the door model or device addresses of the selected door can be edited using the ▨ button, via double click or again via the context menu (right-click and select **Change Entrance**).

When defing an new entrance a name must be given, which should be unique and as descriptive as possible, because it will be used to define authorization groups and individual access rights in Personnel Management.

It is also necessary to select the number of the controller to which this entrance is connected, and the Group ID (GID). In general only the number of the controller requires attention, because Access PE automatically assigns the next free GID. A suitable door model must be chosen from the combo-box **Door model**. Please consult the Appendix for a table of predefined door models and their functionalities.

Depending on the door model combo-boxes are displayed for entry and exit readers, where reader types must be selected. Each reader must receive a unique address within its controller. For readers with **Wiegand** interface only the **number of its own controller's interface** is required. For readers with **RS485** interface the assigned **DIP-address** is essential.

The button **: Search device data** can be used to collect and display a list of the readers on the current controller. When collected these data are stored in cache, and can be retrieved by the **: Device data from cache** button. If the configuration is changed the cache will no longer be current and the list will need to be re-collected.
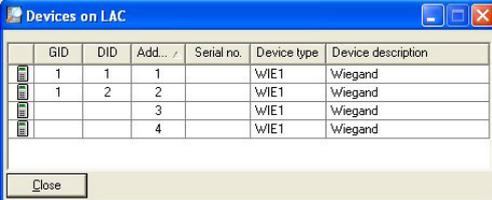
	GID	DID	Add... ↗	Serial no.	Device type	Device description
	1	1	1		WIE1	Wiegand
	1	2	2		WIE1	Wiegand
			3		WIE1	Wiegand
			4		WIE1	Wiegand

Close

Notice!

Please ensure that the reader addresses concur with the devices actually installed.

You can connect a maximum of four readers of type **AMC-Wiegand**, and eight of type **AMC-RS485** and **LACi.**

Use of reader address 9:

Reader address 9 has been set up as an aid to configuration, and serves as a buffer when rearranging parameters. If you have assigned all the reader addresses of a controller but still need to rearrange the parameters, then you can temporarily move a reader to address 9 in order to free another address.

Example: You wish to swap readers 4 and 7. As you can not use the same address twice proceed by assigning reader 4 to address 9, move reader 7 to address 4, and finally move reader 9 (originally reader 4) to address 7.

Signal definition

Having selected the door model, all possible input and output signals are displayed in the list box. By selecting one of the elements and clicking the **+** button to the left of the list, or by double clicking on the list element, you will invoke a dialog box for the definition of signals.
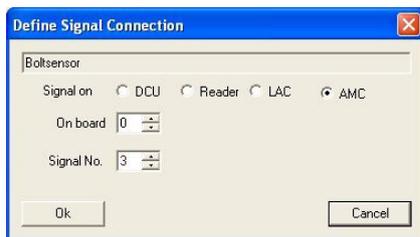
The signal selected from the list box is displayed for orientation. The effect of the signal is defined in the default settings of the parametrized controllers, but can be modified here if required. Additionally displayed are the board from which the signal emanates, and the number of the signal interface. For the enumeration of signals on the controller or an extension board please consult the relevant installation handbook for that device.

Notice!

You should ask the installing technician for a wiring plan/listing for the signals, which will enable you to parametrize the signals in Access PE accordingly.

False correspondences to physical wiring can cause considerable problems with the control of entrances and the correct processing of their signals.

The dialog box requires you to choose between DCU (Door Controler Unit), reader, LAC or AMC. If you choose DCU or reader it will be necessary to enter the GID and DID of the device. The following rules apply here:

– **Reader**
    – GID = GID of the reader at the entrance
    – DID = 1 for the first **entrance** reader, = 2 for the second **entrance** reader, = 3 for the first **exit** reader, = 4 for the second **exit** reader
    – Signal No. = Signal at the reader 1 ... 4
– **LAC**
    – Signal No. = Signal at the LAC 1 ... 16
– **AMC**
    – On board = Board No.. 0 or 1
    – Signal No. = Signal at the AMC 1 ... 8 or, in the case of extension boards, 1 ... 16

In the list box the parametrized connections are shown in their respective columns. The first colums contains icons representing the status of the signals:

→	Input signal not set
▶	Input signal set
←	Output signal not set
◀	Output signal set

A previously defined signal can be deleted using the **-** button.

6.2   Display and parameterization

All those entrances known to the system are shown in a list on
the left hand side. By clicking one of the listed entrances the
data for that entrance will be shown in the parameter fields on
the right.

The following buttons are situated along the top of the list box:

Add an entrance

Modify an entrance.

Delete an entrance

The following connections are shown at the top of the
parameter fields.

LAC   Sequential number of the controller assigned to this entrance.

GID   Group Number of this entrance with its door(s) and reader(s)

Model   The door model and description.

These entries can be modified by clicking the ◢ button or double clicking on an entrance in the list.

The following **door parameters** can be set:

Door Parameter	Description
Activation time in 1/10 s	If no door frame contact has been configured then the door opener will be activated for the duration set here. Otherwise the activation of the door opener will cease as soon as the frame contact sense that the door is open. Default value = 40
Open time in 1/10 s	Maximum time for which the door may remain open before sending the signal "Door open too long" . Default value = 300
Camera activation time in 1/10 s	If the entrance is equipped with a CCTV camera then it will be activated for the duration set here. Default value = 100
Alarm suppression time for control mechanism in 1/10 s	Duration of alarm supression (shunt) before the door opener is activated. The alarm suppression time is only effective if the time set is greater than 0. Default value = 0

Door Parameter	Description
Door contact	If the door has a frame contact then this can be parametrized to facilitate monitoring the entry of a person. At the same time, the signal to activate the door opener is turned off if the door contact shows that the door is open. This signal is also used to control the **alarm suppression time**.
Bolt contact	If the door has a bolt contact sensor then this can be parameterized to show whether the door is really closed.
Part of a door-complex	This parameter indicates whether the door is part of a door-complex, e.g. a "mantrap" or airlock. In this case the signals for the door-complex can ensure that both doors are never open simultaneously. If only one door is defined as part of a door-complex then the synchronisation is not active.
Intrusion events	Here you can parameterize whether a signal should be sent in the event of unauthorized door opening. A prerequisite for this is the existence of a **door contact**.
Door status events	Provided the entrace has a **door contact** the system can be parameterized to signal every open/close event.

The following reader settings can be parameterized for an entrance:

Reader Settings **Entry and exit readers**	Description
Access only	Only general access events are created by the reader.
Arriving	When accessing through this card reader a **time and attendance (TA)** booking is made and the person is booked as being present.
Leaving	When passing through this card reader a **time and attendance (TA)** booking is made and the person is booked as being absent.

Bookings created by readers which are configured for time and attendance are recorded daily in a file in the directory C:\Bosch\Access Professional Edition\PE\Data\Export (default path).

A file named **TA_<Current date YYYYMMDD>.dat** is created, which can be edited. Fields are separated by a semicolon and can thus be edited by 3rd party spreadsheet applications, for example.

Each booking record contains the following data:

Last name; First Name; Company; Personnelno.; Card no.; Additional fields 1-10 (if parametrized); Name of the entrance; Date (yyyymmdd); Time (hhmmss plus the letter "s" to indicate daylight-saving time); Direction of passage expressed numerically (1 = Arriving, 2 = Leaving); Direction as a text string (ENTER, LEAVE)

Reader Settings Entry and exit readers	Description
Check OK	Only for **entry readers.** This parameter enables a reader to be set up as **release reader** to unblock the cards of personnel who have been selected for **random screening.** It is important to ensure that a release reader is not simultaneously configured to be a screening reader which randomly selects personnel for screening.
Random personnel screening - Rate-%	This parameter enables a reader to be set up as a **screening reader** to select cards randomly for **personnel screening.** As well as checking the box it is necessary to enter a percentage rate (1 to 99) for random screening. If no entry is made then all cards will be selected (100% screening). It is important to ensure that a screening reader is not simultaneously configured to be a release reader which unblocks cards blocked by screening readers.

Reader Settings **Entry and exit readers**	**Description**
Anti-passback - Timeout - Group id	This option blocks a card for the specified timeout period from reentering where it has just entered, unless an exit has been recorded in the meantime. This is to prevent misuse of cards by passing them back across a turnstile. **Timeout** in minutes between 1 and 999. Several readers can be combined in a group. An anti-passback is valid for each reader with the same **group id**. Possible values: two characters 0 - 9 and/or A - Z
Entry as group - required number of persons	Only for **entry readers**. This option grants entry only after a group consisting of at least this number of persons has presented their cards. Possible values 2-6.
With keypad	Check this box if the door reader possesses a keypad
No time model check	By default accesses are checked against time models. This behaviour can be circumvented by setting this parameter.

Reader Settings **Entry and exit readers**	Description
Motor move-in	This option should be activated when the reader has a card feeder.
Push button - always enabled	This parameter enables the recognition of a signal to open the door. This signal can come from a push button or from a telephone e.g. if no reader is available. **always enabled**: If normal settings are configured, the push button does not work when the security system is activated. This means that it is not possible to exit the monitored area. With this option the push button remains operational, even with an armed alarm system. If the push button is activated, this function includes an exit reader, too.

Notice!

Checks which go beyond the basic verification of authorizations and time models (e.g. access sequence checks, anti-passback checks, random screening) are carried out by the LAC subsystem process. To deliver this functionality the Access PE server must be running round-the-clock (24 x 7).

The **unlocking of the entrance** can be configured with the following parameters:

Door unlock type	Description
Normal	The door is locked and will be opened only if its reader is presented with a valid card.
Long-term	The door is open for a prolonged period, e.g. during daylight hours, or as long as the reception is continuously manned.
Per time model	The long-term unlocking of the door is linked to a time model in various ways: – **Always per time model:** The door is unlocked during defined duty periods. – **After first use:** After the first use within a duty period the door remains unlocked until the end of that period. – **Activation via dialog**: Long-term opening during a duty period is regulated by a special dialog-capable reader.
Activation of motor lock	This parameter specifies a time model to govern the activation of a motor lock at the entrance. (usually outside normal business hours).

PIN-Code entry at the reader can be parameterized as follows:

PIN-Code	Description
None	No PIN-Code necessary.
Always	PIN-Code always necessary.

PIN-Code	Description
Per time model	PIN-Code entry is dependent on the time model, as per one of the following variants: – **Outside regular hours**: Outside of time model periods PIN entry is necessary. – **Outside regular hours and at first use:** Outside of time model periods and the first time a person crosses the entrance PIN entry is necessary.
PIN or card	If the function is active, access can be obtained either by entering the door PIN or with a card.
Door-PIN	option to enter a door PIN — 4 to 8 figures (parameter setting — general system settings)
Verification	re-enter the door PIN
per time model	The option of alternative PIN entry can be restricted to certain days or times of day via a time model.

Notice!

The **Identification-** and **Door-PIN** variants cannot be used for door models with security system arming (DM 10 and 14).

6.3   **Door models with special settings**

Door models with special settings
Some door models require special information for setup or
special modes of use.

Door model 07: Elevator
If this door model is selected then the dialog is expanded by
several fields to include the set up of floors.

A maximum of 16 floors can be defined. These floors can be
assigned as Access Authorizations.

Door model 14: Door with IDS rearming
The configuration of this door model corresponds to that of all
others, except that, along with access authorization for this
entrance, authorization to arm and disarm the security system
(IDS) itself is also assigned. These authorizations are typically
assigned separately.

7   Areas

The configuration of areas enables the system to locate persons and also to enforce a correct access sequence. In this way persons can be prevented from entering particular area by an unauthorized route. In general this function is used only for high security installations.
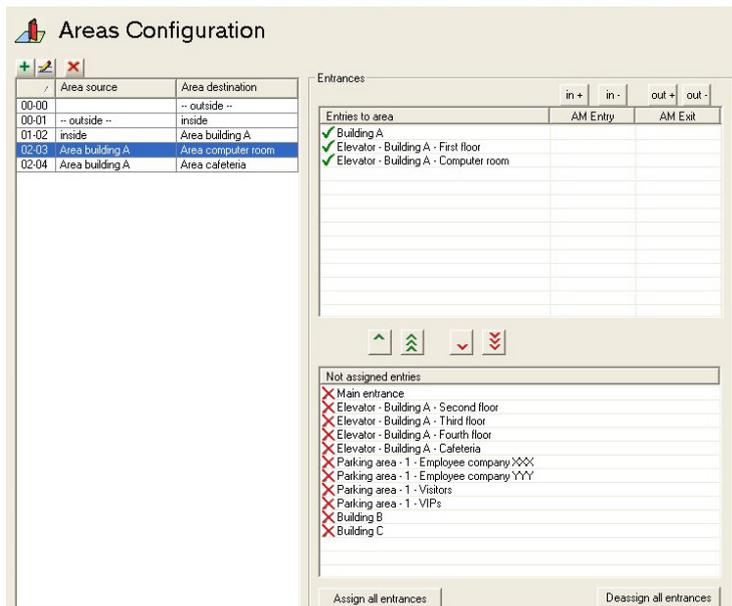
On the left hand side a list of already defined areas is displayed. **The following buttons are situated along the top of the list box:**

- ⊞   **Add** an area

- ⊿   **Modify** an area

- ⊠   **Delete** an area

By default the installation process creates the area **--outside--**.
No entrances can be defined for this area, because it denotes
unmonitored territory.

From this pre-installed area you can now define further areas.
These are purely virtual constructs and need not correspond to
real-world areas. The areas can consist of one or multiple
buildings (e.g. Area Company ACME Inc.), or individual floors or
even single rooms.

Notice!

The definition of a new area is always based on an existing
area. The existing area selected in the list box automatically
becomes the **area source** for the new area. This default can not
be overridden, therefore it is important to select the correct
area source in the list box when creating a new area.

The name of the new area can be selected from the combo-box
or a new name entered manually.

Areas must be configured so that it is in fact possible to move
from real source to real destination without gaps or missing
entrances between.

Example:

From the predefined area **--outside--** a person passes through
the main entrance to the area **Reception**; from there to
builidings A, B or C. Hence the areas in Access PE must be
configured so that **Reception** is the **area source** for buildings A,
B and C.

After creating a new area at least one entrance must be assigned to it, so that it is possible to enter the area. Two list boxes are provided on the right hand side of the dialog window for this purpose.
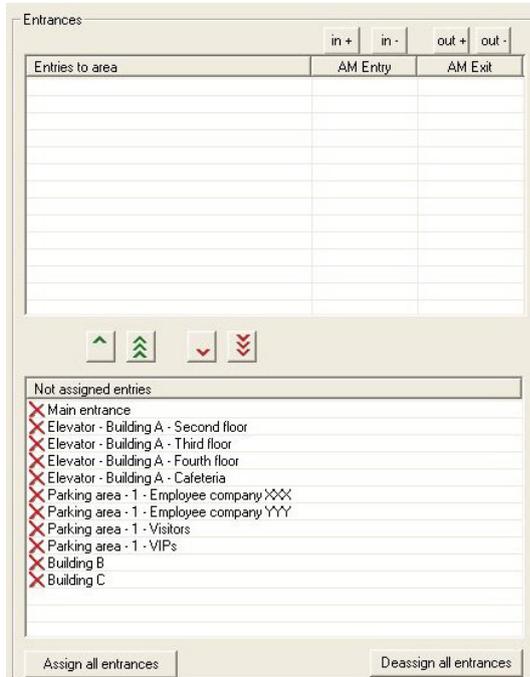
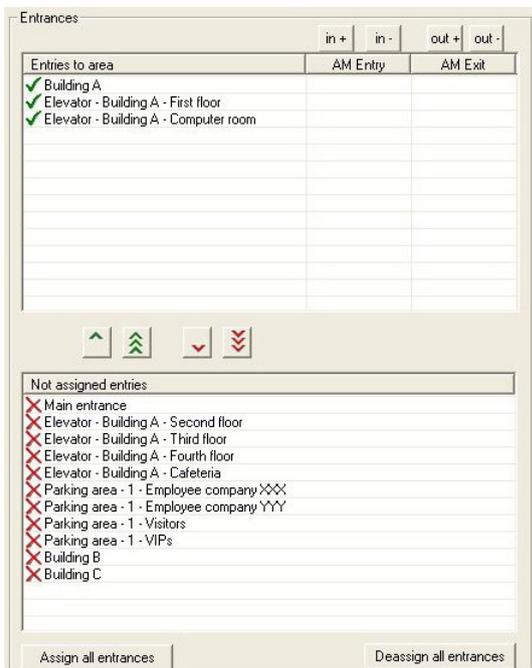The entrances in the **not assigned entrances** list are those available, i.e. those which have not yet been assigned to any

area. By double clicking on the desired entance, or on the button, that entrance is assigned to the area currently selected

in the left hand list. The button moves all the entrances in the lower list to the upper. Conversely, double clicking in the

upper list, or using the or buttons, undoes the assignment.

Notice!

An entrance can only be assigned to one area.
If you have already assigned certain entrances to an area then
they will no longer be available in the **not assigned entrances**
list.

If you wish to use your system for access tracing then the entry
and exit readers must be parameterize accordingly. Select the
entrance you wish to parametrize in the **entries to area** list, and
configure it as an entrance by clicking E+, or as an exit by
clicking A+. The buttons E- and A- can be used to undo
these configurations.

The same functions are available through context menus (right click on an entrance in the list).

Notice!

Checks which go beyond the basic verification of authorizations and time models (z.B. access sequence checks, anti-passback checks, random screening) are carried out by the LAC subsystem process. To deliver this functionality the Access PE server must be running round-the-clock (24 x 7).

8   Personnel Groups

Personnel groups allow a logical structuring of your company's
staff. For example newly created persons in the system can
inherit standard bundles of user rights from predefined
personnel groups.
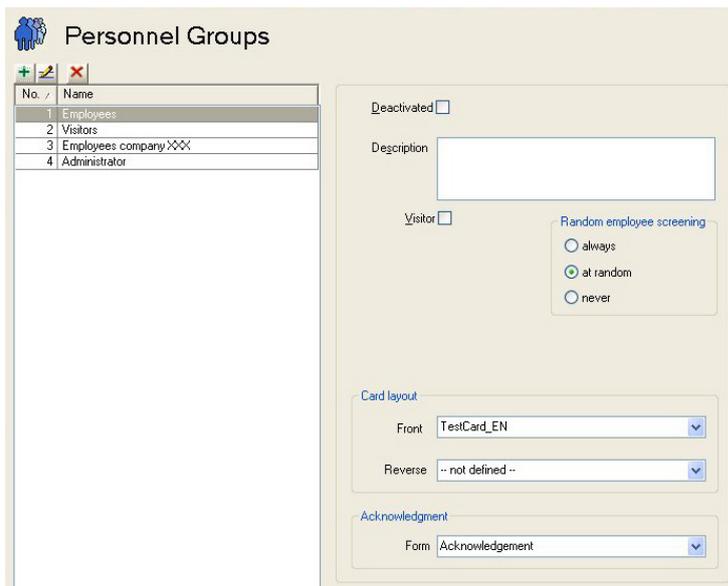
The list of all previously defined personnel groups appears on
the left hand side.
The following buttons are situated along the top of the list box:

Add a new personnel group

Modify the selected personnel group

Delete the selected personnel group

Two personnel groups are predefined by default: **Employees**
and **Visitors**. These groups correspond to the default filters in
the **Personnel Management** application of Access PE.

Thus it is possible to differentiate between different types of employee (e.g. white-collar, blue-collar, cleaning staff), and assign to such personnel groups standard bundles of user-rights in the **Authorization groups** dialog. Whenever a new employee is assigned to a particular personnel group s/he then automatically receives the corresponding group rights.
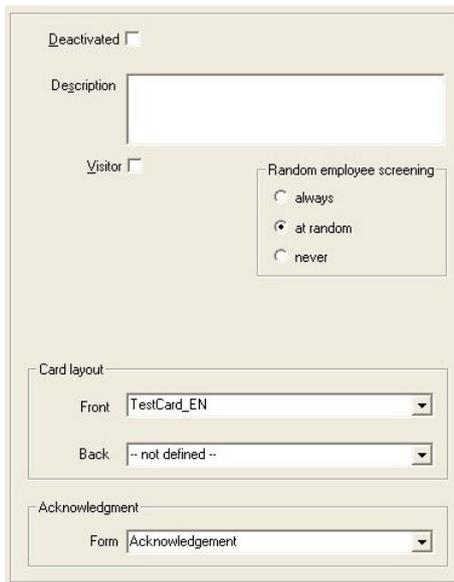
The following parameters, on the right hand side of the dialog box, can be defined for the selected personnel group:

Settings	Description
Deactivated	Deactivation is a preparatory phase for deletion. No new persons can be added to the group, but the group continues to exist. **A personnel group should not be deleted until all members have been removed from it.**
Description	A detailed description can be stored for each personnel group.
Visitor	A group can be classified as being of type Visitor. The **Personnel Management** application is able to filter lists of persons based on the categories **All persons**, **Employees** and **Visitors**. Personnel groups of type **Visitor** can thus be viewed in isolation from groups of type **Employee**.
Employee screening: always at random never	Applies only to readers which have been configured as screening readers for random personnel screening. The three options are defined as follows. = the percentage rate of screening is 100% = this group is screened randomly at the defined percentage rate. = this group is never screened

| Settings	Description
Badge Layout Front Back	In order to create cards it is necessary to define at least one layout. Layouts can be defined per personnel group. A layout for the reverse side of the card is optional.
Acknowledgement **Form**	cards can, if so desired, be handed out conditionally upon receipt of a signature on a form. These forms can be designed to be personnel-group specific.

9 Access Authorizations

Access authorization groups simplify the administrative tasks of
the system administrator and operator by grouping together any
number of individual entrances that have similar access
requirements (group of people, time restrictions etc.) or are
close/next to each other in geographical terms. These groups
can then be assigned to people in one step.

9.1 Create and assign

Authorization groups are logical groupings of entrances. The
access rights of a person in the **Personnel Management**
application can consist of one or more such authorization
groups.
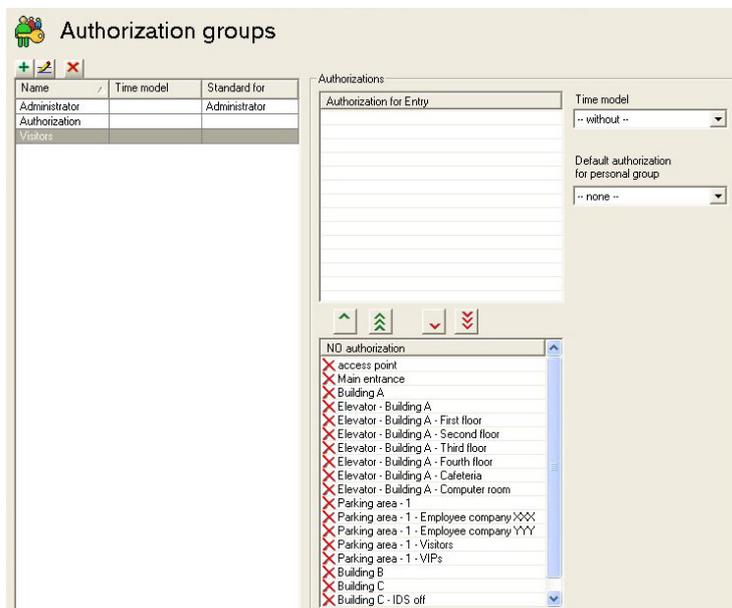
The list box on the left shows all hitherto defined authorization
groups.

The following buttons are situated along the top of the list box:

⊞　　　　　　**Add** an authorization group

⊿　　　　　　**Modify** the selected authorization group.

☒　　　　　　**Delete** the selected authorization group.

The ⊞ button opens a dialog for naming a new authorization group

The right hand list boxes can be used to assign entrances to the selected authorization group.
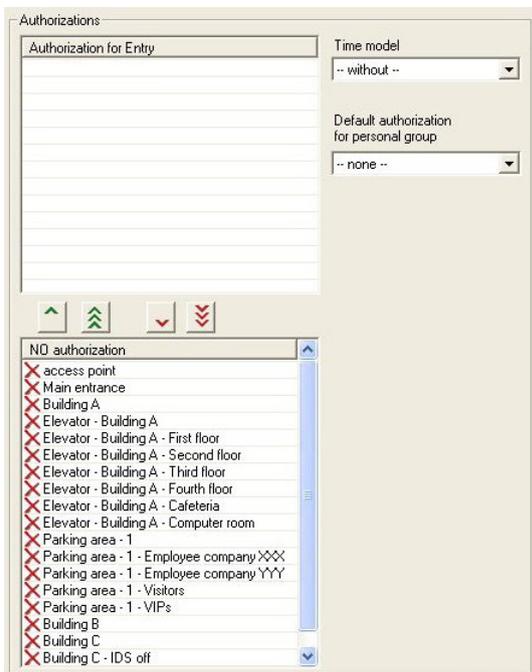
The entrances in the **NO authorization** list are those available, i.e. those which have not yet been assigned to any authorization group. By double clicking on the desired entry, or on the ![up] button, the entrance is assigned to the authorization group currently selected in the left hand list. The ![double up] button moves all the entrances in the lower list to the upper. Conversely, double clicking in the upper list, or using the ![down] or ![double down] buttons, undoes the assignment.

⚠ **Caution!**
Subsequent modifications in the assignments of entrances and time models affect the rights already assigned to persons.
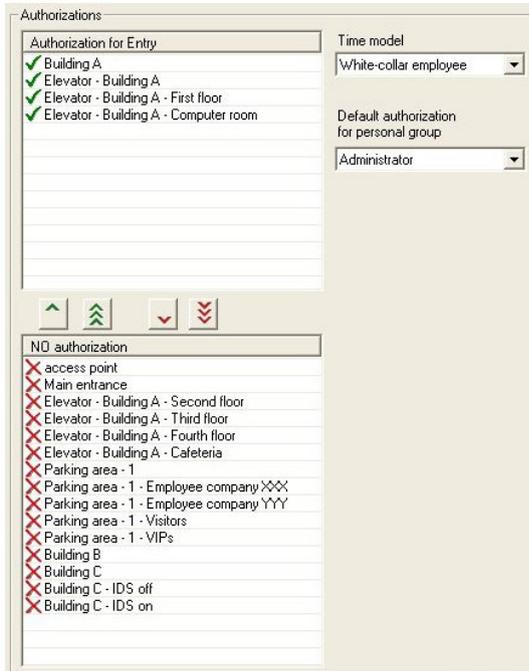
Any authorization group can have a **time model** assigned to it
which limits the user rights; see **Use of time models**
(*Timemodels, page 115*) in Access PE.

Notice!

Mark the names of authorization groups which are dependent
on time models e.g. with the prefix or suffix **DM**. This will help
when assigning these groups in **Personnel Management** to
distinguish them from unrestricted rights packages.

Additionally it is possible to assign the authorization group as
the **default authorization** for a **personnel group** (e.g. employees
or visitors). Thus when creating a new person in **Personnel
Management** the correct authorizations will be assigned
according to the person's personnel group.

9.2   Special rights

Door models 07 and 14 require additional information for their
configuration (*Door models with special settings, page 91*).
However they differ from other door models also in their
assignment and usage.

Door model 07: Elevator
The list of available rights contains a separate element for the
elevator, as well as for each floor.

When creating authorization groups, one reader for the **elevator**
plus **at least one floor** must be assigned.
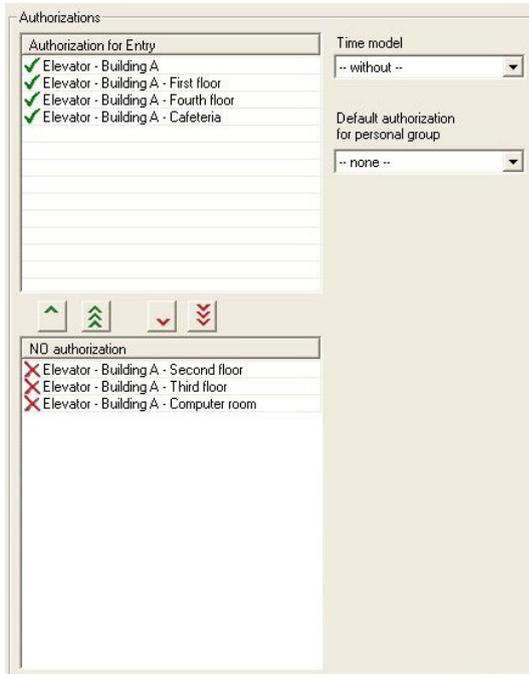
Door model 14: IDS-Rearming

The list of available rights contains a separate element for the entrance and also one each for the arming and disarming of the system.

NO authorization
X Building C
X Building C - IDS off
X Building C - IDS on
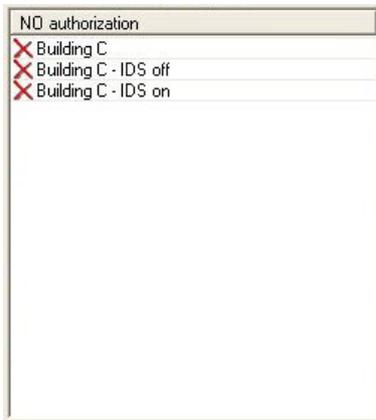
These two kinds of rights are assigned separately from one another. If a cardholder has only access rights to a particular entrance then s/he cannot arm or disarm the IDS (intrusion detection system) from there.
Conversely, if a cardholder has only arm/disarm rights at a particular entrance, then s/he cannot pass through the entrance.
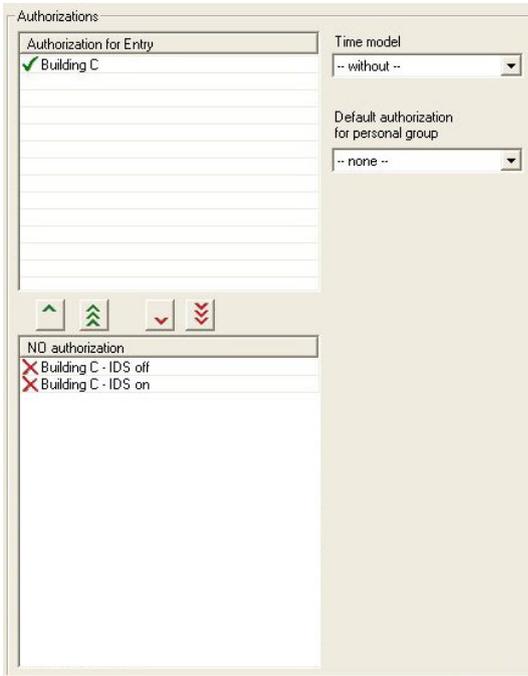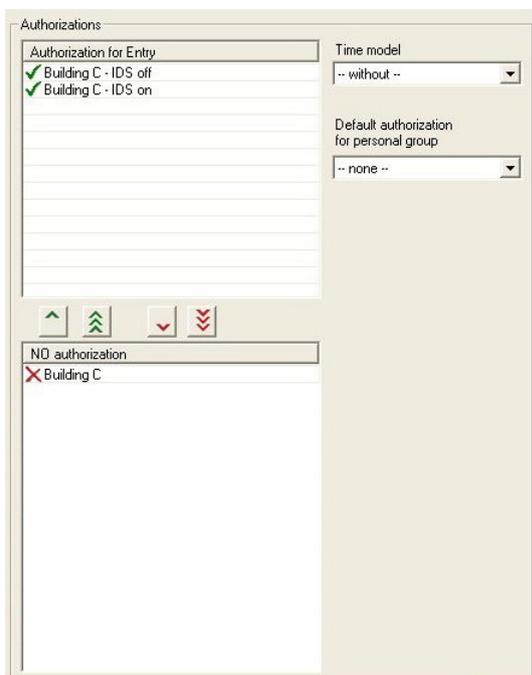
10 Special days

The special days defined in this dialog have different restrictions from the day of the week upon which they fall. The time models for the holidays and special days override those of the same day of the week in ordinary time.
The predefined list of special days can be changed, reduced or enlarged as desired. Holidays which are not required can be deactivated or deleted, in which case the time model for the normal day of the week takes precedence again. Non-existent or customer-specific days can be defined and added at will.
In this way it is possible to keep calendars small: Recurring special days are carried over from year to year, and only exceptions and irregular events need be defined specific to an individual year.

10.1 Create and modify

In Access PE a number of typical holidays are defined. These need to be altered, added to or deactivated depending on your location.

The following buttons are situated along the top of the list box:

±	**Create** a holiday/special day
◢	**Modify** a holiday/special day
✕	**Delete** a holiday/special day

Notice!

It is recommended that the predefined holidays and special days with **variable dates** (e.g. Easter) not be deleted but deactivated, if they are not to be used. Holidays and special days with variable dates can not be re-added later via the dialog.

If you use the ± or the ◢ button to add or modify holidays, you will be prompted by as follows for a new name:

By confirming with the OK button you will enter the new or modified name in the list. To the right of the list box the parameters for the selected list element can be defined.

Deactivated	Determines whether the holiday/special day is in use or not.
Category	You can divide active holidays/special days into 11 categories (holiday plus special day types 1..10), and can assign specific day models to each category when defining time models.

Priority higher than weekend	Specifies which option takes priority if an annually recurring holiday falls on a Saturday or Sunday. If the check-box is ticked then the duty model for the holiday takes precedence, otherwise the time model for the weekend.
Date	If the special day recurs annually on the same date then an asterisk (*) should be used instead of entering an explicit year. Some holidays (e,g, Christmas) always have the same date.

11   Daymodels

Day models describe an abstract daily schedule. Irrespective of the day of the week a day model defines at which times of the day access should be granted or denied.
A separate day model is required for every different daily schedule.
A day model can consist of up to three periods with start and end times.
By using day models in time models the day models become associated with specific calendar days.

11.1   Create and modify

This dialog box is used for the creating and modifying day models which in turn are used in time models.
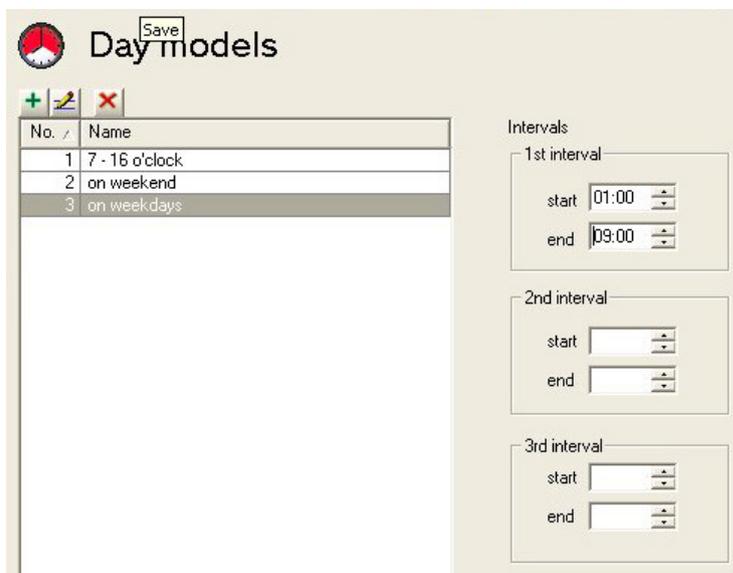
This list box on the left shows the day models defined hitherto. The following buttons are situated along the top of the list box:

⊞   **Create** a day model

⊿   **Modify** the selected day model

⊠   **Delete** the selected day model

Use the ⊞ button to add, or the ⊿ button to modify day models:
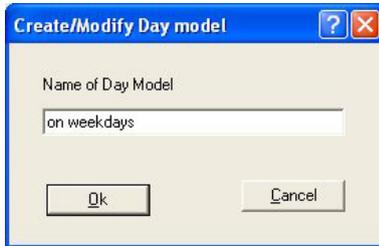
By confirming with the **OK** button you will enter the new or modified name in the list. To the right of the list box the periods which make up the selected day model can now be defined. A day model can consist of up to 3 periods.

The start of each subsequent period must be less than its end time. Hence if you wish to define a day model which spans midnight, then you need to define two periods:

1.   The period from: ... to 24:00
2.   The period from 00:00 to ...

12   Timemodels

Time models restrict access at the assigned entrances to specific times of day. This enables the system to deny access, for example, during the night, or to impose additional restrictions on access at weekends.

Access PE uses time models in several ways, for example in combination with:

– **Authorization groups**:

Time models can be associated with access rights so that these access rights apply only at particular times on particular days. It is equally and simultaneously possible to use access rights with no time limitations.

– **Persons**:

Time models assigned to persons restrict the general use of their cards to the defined dates and time periods.

– **Controllers and extension boards**:

The generation of entry and exit signals by controllers and extension boards can also be restricted by time models.

– **Doors**:

Door opening times can be governed by time models.

– **PIN codes**:

PIN code entry is an example of an additional security measure which can be imposed outside of the times defined by a time model.

– **Activation of a motor lock**:

A motor lock can be parameterized to be active only within a particular time model.

Depending on how they are to be used time models are created in different ways.

Example:

Supposing time models are to be used to restrict access of persons to weekdays 07:00 to 19:00 and weekends 09:00 to 15:00. Two day models are required:

1. with a period of 07:00 to 19:00
2. with a period of 09:00 to 15:00

If at the same time a motor lock is to be activated only outside of these times, then two day models for use by the lock's time model must be defined as follows:

1. with two periods of 00:00 to 07:00 and 19:00 to 24:00.
2. with two periods of 00:00 to 09:00 and 15:00 to 24:00.

The application of time models

Time models which are associated with personnel data will only be active if the reader's default settings have not been changed, and the option **No time model check** (*Display and parameterization, page 82*) thus remains unchecked.

Time models can be used in many ways, so in order to understand how the system handles multiple assignments please note the following conflict-resolution rules:

– If a person has access to certain entrances via a time model, and if that person is given access to the same entrances without a time model, then the **looser** restriction prevails. I.e. in this case the time model will not be applied.
   Example:
   A person is given the following access rights :
   – Access to entrances A, B, C and D within a time model of 09:00 to 17:00 every day.
   – Individual access rights to entrances B and D without time model.

This person now has access to entrances A and C between 09:00 and 17:00 every day, and unrestricted access to entrances B and D.

– If a person is given different access rights covering the same entrances, but governed by different time models, then the **union** of the time models is applied.
   Example:
   A person is given the following access rights:
   – Access to entrances A, B, C and D within a time model of 07:00 to 13:00 every day.

- Access to entrances B, D, E and F within a time model of 09:00 to 17:00 every day.

The person now has access to entrances A and C from 07:00 to 13:00, to entrances B and D from 07:00 to 17:00 and to entrances E and F from 09:00 to 17:00

- If a person is assigned to an authorization group with time models, and if the same person is given a time model for the use of his card, then the **intersection** of the defined periods is applied.

  Example:

  A person is given the following access rights:

  - An authorization group with access to entrances A, B, C and D, and a time model of 07:00 to 13:00 every day.
  - An authorization group with access to entrances B, D, E and F and a time model of 09:00 to 17:00 every day.
  - And additionally a duty model of 11:00 to 19:00 every day

The person now has access to entrances A and C from 11:00 to 13:00, and to entrances B, D, E, and F from 11:00 to 17:00.

12.1 Create and modify

This dialog box is used for the creating and modifying time models which, according to their usage activate certain system elements.
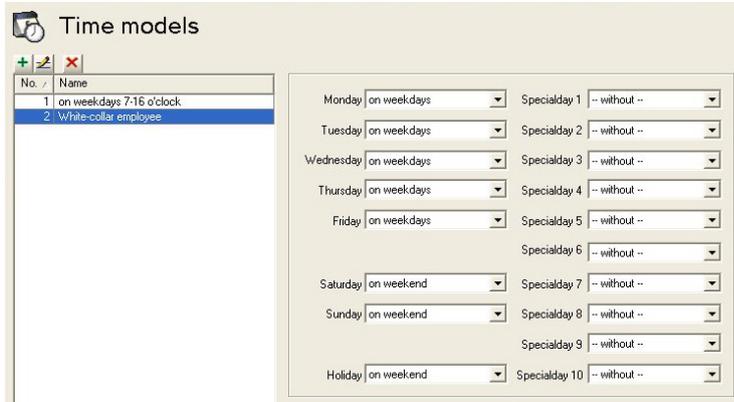
This list box on the left shows the time models defined hitherto. The following buttons are situated along the top of the list box:

| | **Create** a time model |

| | **Modify** the selected time model |

| | **Delete** the selected time model |

If you use the ⊞ or the ✎ button to add or modify a time model, you will be prompted as follows for a new name:
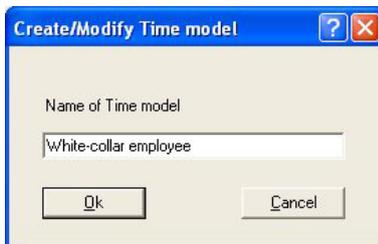
By confirming with the **OK** button you will enter the new or
modified name in the list. To the right of the list box day models
for the days of the week and for Holidays and Special Days
(1..10) can now be assigned to the selected time model.
Time models are defined as repeating periods of one week. The
course of each weekday is defined by assigning day models to
them. Additionally the day models of these normal weekdays
may be overridden by the day models of holidays or special days
which happen to fall on those weekdays.

Notice!

If, when defining a time model, a particular weekday or special
day is left without a day mode (i.e. left with the default setting
<none>) then these days will be treated as if they had a day
model without periods; i.e. on that day **no access** would be
granted by the time model.

13   Texts

Each application language you selected during installation has its own list with display texts for display readers and log book messages. The texts in the relevant language list are used in the Logviewer, for example in the log book messages created when the application language is selected.

13.1   **Displaytexts**

Some of those texts which are displayed at card readers can be modified in this dialog. The reader's display contains of two lines of 20 characters each.

> **Caution!**
> In the text for Enter PIN code the underscore "_"r; character should not be removed, as it triggers the reading of the PIN code.

The texts here are user-defined and not automatically translated by the application when switching languages. However by selecting a different language from the **Language** combo-box (above the list box) and re-entering the texts it is possible to define equivalents in every language variant installed in Access PE. Thus even these data can be viewed by a different user in his own language.

13.2 Event Log messages

In this dialog you can change not only texts of log messages, but also their categories.

The desired category can be chosen from a pull-down list which is invoked by double clicking in **Category** column in the line you wish to change.

	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 Shutdown		
⚠	Operator action		
ⓘ	Information	18	Program download OK

Each category is represented by a unique symbol in the first column. These symbols are also used to categorize incoming messages in the event log. The following symbols and categories can be used:

- ⓘ   Event log unavailable

- ⓘ   Information

- ●   Message

- ⚠   Error

- ●   Alarm

- ●   Arriving

- ●   Leaving

- ●   No access

- ●   No authorization

- ✕   Malfunction

✔ OK

◉ IDS armed

◉ IDS not armed

◀ Program startup

✖ Program shutdown

◩ Operator action

In the second column (headed by a **!**) select those messages which are to serve as special alarm messages in the **Alarm Management** dialog. Double-click in the corresponding cell to set or remove the alarm symbol ◉. The installation procedure defines messages of categories **Alarm** and **Error** as alarm messages by default.

The desired text can be modified by double clicking **Log text** column in the line you wish to change.

	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)

The texts here are user-defined and not automatically translated by the application when switching languages. However by selecting a different language from the **Language** combo-box (above the list box) and re-entering the texts it is possible to define equivalents in every language variant installed in Access PE. Thus even these data can be viewed by a different user in his own language.

14   Additional Personnel data

Ten freely definable extra fields are provided in addition to the default personnel data fields.
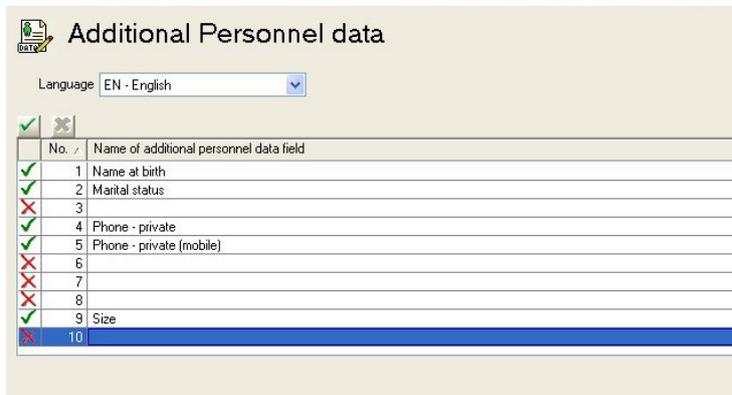
The list box already contains 10 lines for your use. By double clicking on a field in the column **Name of additional personnel data field** you render the field editable and can enter a name for it.

Notice!

Entering a name does not activate the field for use. Activation is done by double clicking on the ₓ in the leftmost column, or clicking on the ▣ button. When the field is active the ₓ is replaced by a ✓.

When at least one additional data field has been defined then a new tab called **Additional data** appears in the Personnel Management application (personal data and authorizations dialog). The order of fields need not be maintained as gaps will be left for inactive fields.

Each field can contain up to 40 arbitrary characters.

Notice!

Each text entry field is assigned a field in the database so that the data can be stored, selected and included in reports. This means however that changes to additional data fields which are in use will lead to the loss from the database of the data they contain .

The names of additional data fields are user-defined and not automatically translated by the application when switching languages. By selecting a different language from the **Language** combo-box (above the list box) it is possible to define equivalents in every language variant installed in Access PE. Thus even these data can be viewed by a different user in his own language.
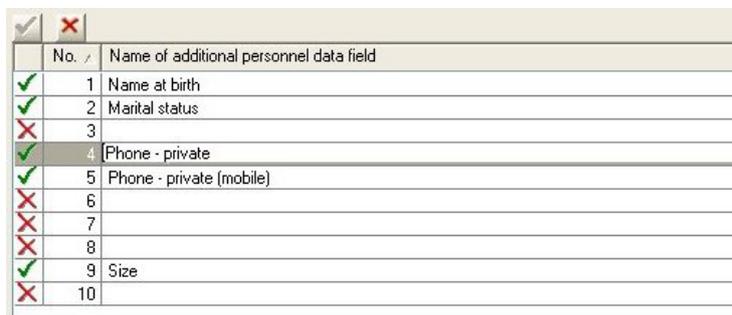
Activation/Deactivation of additional fields

As well as receiving a name additional data need to be activated. To do this double click the symbol in the leftmost column or click the ⊞ button. The symbol is changed from ✗ to ✓.

The **Additional data** tab in the **Personnel Management** application will not appear until at least one additional data field has been activated.

Notice!

Fields without names can also be activated.

Activated fields can be deactivated by double clicking ✓ or by clicking ✗ . A security pop-up message is then displayed offering two variants of deactivation:

Notice!

Deactivation of fields deletes corresponding personnel data only if the field description is also deleted. Do you wish to delete the field description and thus the personnel data also?

No   = Deactivate the field but keep its name and contents.

Yes   = Deactivate the field and **delete its name and contents.**

15   **Map Viewer and Alarm Management**

The Access PE Map Viewer enables to control devices as entrances, readers, cameras directly from a map.
The Access PE alarm list shows all incoming alarms to the operator. Alarms can be accepted by the operator. In case of an alarm, the location map will be displayed. The icon of the device that triggered the alarm is highlighted by animation. Related video live views are shown to verify the alarm.

1.   Map tree
2.   Active location map
3.   Device control from the map; controls are shown in the map
4.   Alarm list with event information (incl. video)
5.   Device tree with status overview and control elements

Mapviewer features:

–   Home map for easy navigation
–   Navigation between photo views and floor plans via hyperlink
–   Navigation via device tree structure up to three levels

- Interactive Graphical Maps for alarms with integrated alarm list
- Live view and door control from the map and device tree
- 128 maps per system
- 64 devices per map
- 64 hyperlinks per map
- Max 2 MB per map
- Map viewer use a standard image format .bmp, .jpg, .png

15.1 Configuring a map

Start the Map Editor
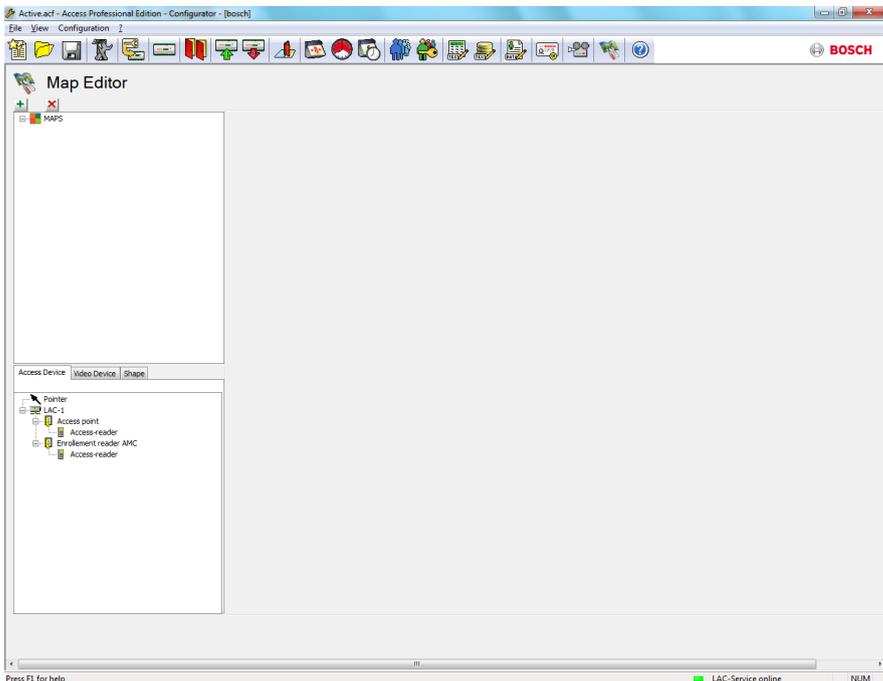
Klick the ➕ button to add a map.
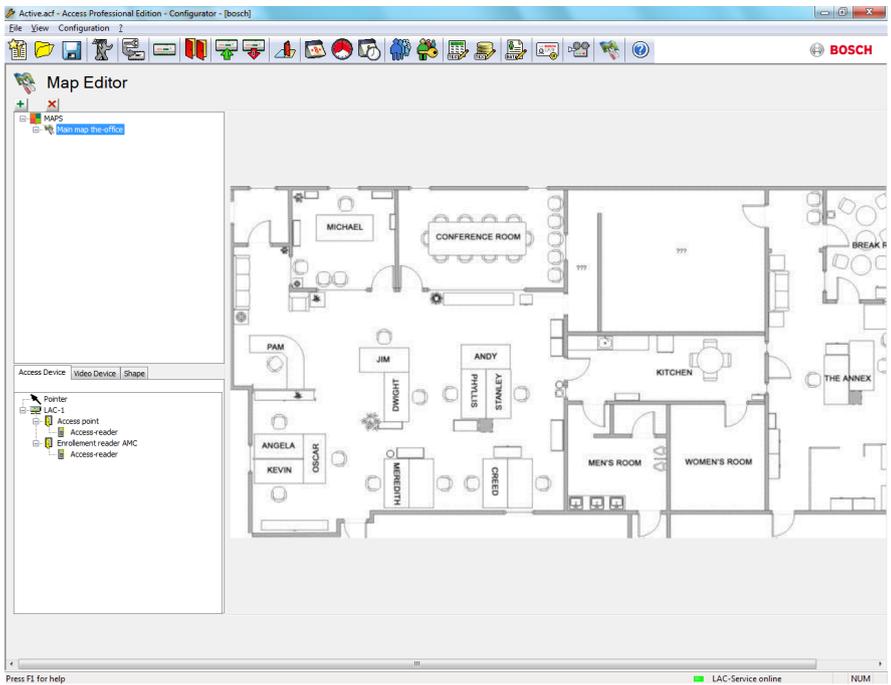
The map is shown on the dialog.
– Optionally configure this map as **Home Map**
Add a detail view, e.g. the canteen, to the map tree.
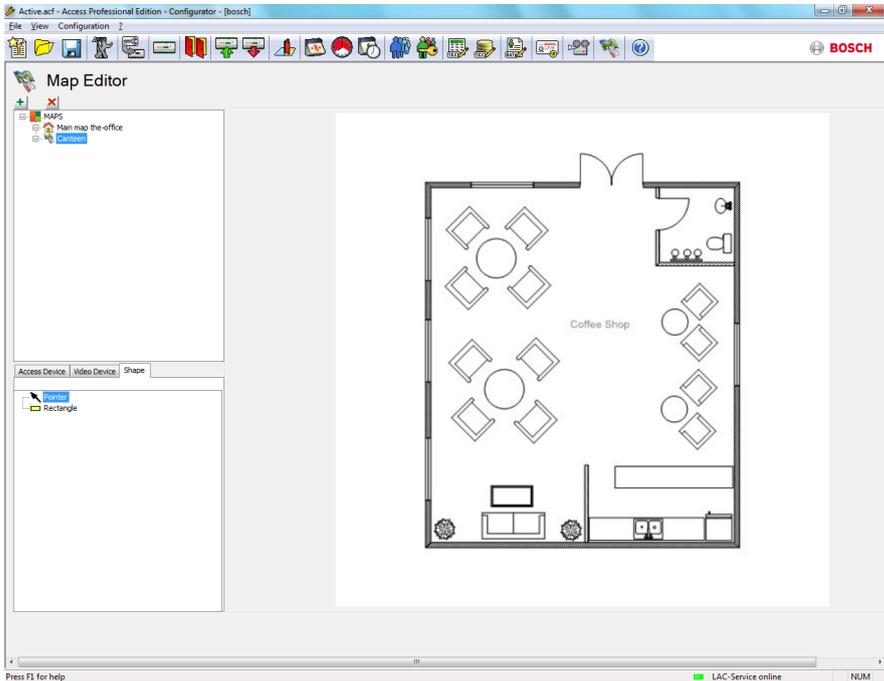
– To connect the new **Canteen map** with the main map, go to the **Shape Tab** and select a **Rectangle**.
– Place the rectangle over the area of the main map that should be shown as a detail view (shown as a red rectangle in the example below).
– In the **Link to Map** Display select the respective detail view, which is "Canteen" in this example.
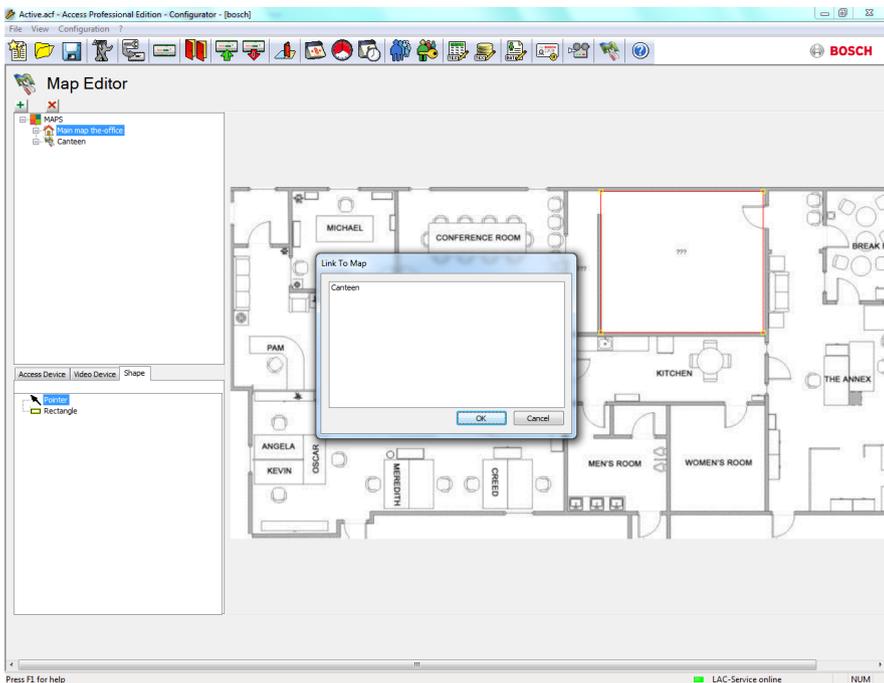
15.2   Adding a device to a map

Select the **Device Tab** and add Devices to the map by pulling
them with the mouse into the map. In the example below the
following devices have been added:
– One Access point
– One Reader
– Two Cameras
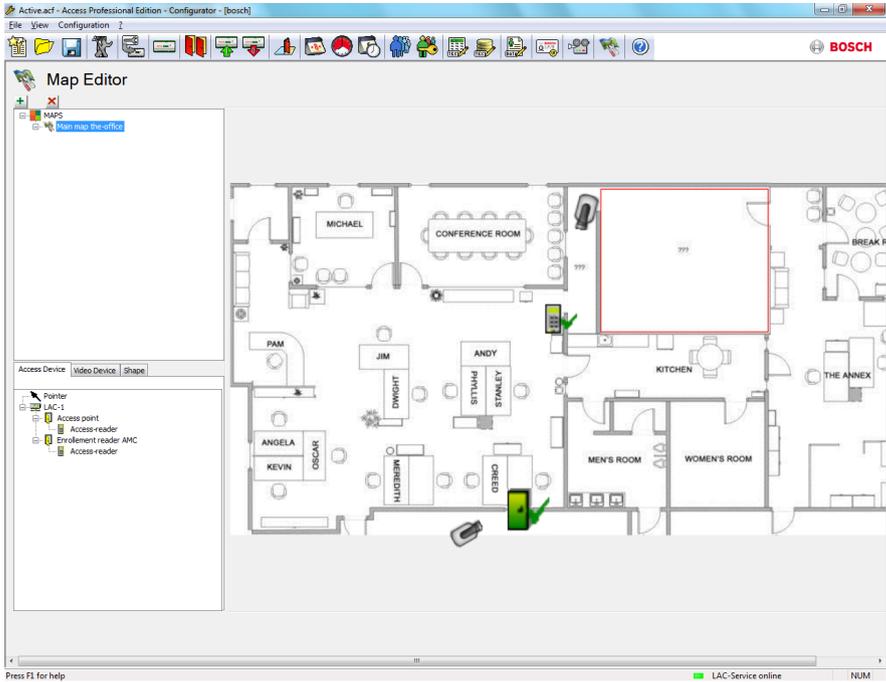
– Click a device in the map and resize by holding the mouse
  button pressed,
– Click a device and rotate as required using the scroll wheel
  of your mouse.

Device Types	Control elements
Access Point (Entrance)	Open door
	Open door long-term / Reset door long-term
	Lock door / Unlock door
	Front Identification Camera
	Back Identification Camera

Device Types	Control elements
	Back camera
	Front camera
Reader	All Entrance Controls
Camera	Live Video

Device Types	Alarms
Access Point (Entrance)	Door opened without authorization
	Door opened too long
	(* All Reader alarm also reflect as Entrance Alarm)
Reader	Reader error
Camera	N.A.

*) These alarm events can be customized by the user. That means, a user can configure any event as an alarm event using **AcConfig -> Event Log** message (Double click on second column will cause an alarm).

16 Card Definition

This dialog defines the data which the reader transmits, so that new card definitions can be entered into the system at a later date.

The list control contains existing card definitions. Default system settings include six standard entries, of which the first four are active (have a green tick in the first column). Apart from the setting **Input Mode** all others are write-protected and can neither be modified or deleted.

> **Notice!**
>
> When using Wiegand controllers and readers, in order to use Identification-, arming- or door-PINs the Wiegand card definition **PIN or Card** (Nr. 6) needs to be activated.

A new entry is initiated by clicking ⊞. Depending on the manufacturer's information the **number of bits** and their encoding are selected and displayed.

> **Notice!**
>
> The maximum number of bits is limited to 64 for all definitions. The maximum number for any coding part (facility, version, customer, country and code number) is 32 bits.

A unique name and a description should be entered to distinguish the new card definition from others.
Entering a value in the **No. of bits** field changes the number of columns in the list box underneath accordingly. Five rows are displayed and the resulting matrix enables you to activate/deactivate individual bits as desired.
The interpretation of the code can now be specified by entering the following possible values in the cells of the **Field** row.

F   Facility: earmarks those bits for encoding the facility.

V   Version: earmarks those bits for encoding the version variant.

K   Earmarks those bits for encoding the customer.

L   Land: earmarks those bits for encoding the country code.

C	Code No.: earmarks those bits for encoding the card number.	
E1	Even 1: Cancelling bit for the first Even Parity Mask	Entering a value in one of these fields activates the check box for the corresponding row.
E2	Even 2: Cancelling bit for the second Even Parity Mask	
O1	Odd 1: Cancelling bit for the first Odd Parity Mask	
O2	Odd 2: Cancelling bit for the second Odd Parity Mask	
1 0	Bit values which make up the code itself	

When defining **Manual Mode** or creating any new example, you can specify the **Mode** that will determine how the code is to be read; e.g. if you select **PIN or card** mode, only the code number will be read i.e. only those parts marked **C**. You can choose from the following mode variants:

Serial number	Mode	Code parts checked
0	Facility + Code no.	F,C
1	Bosch Code	L,K,C,V
100	Manual	C
200	PIN or card	C

Explanation:

The "telegram" sent by a reader when presented with a card is a series of zeros and ones. For each card/reader type the length of the telegram (the number of bits) is precisely defined. A telegram of this kind contains, in addition to user data, control data to identify the telegram type and to verify correct data

transfer. Correct data transfer is verified by parity bits which represent a checksum over selected bits in the mask, either a zero (even parity) or a one (odd parity). Controllers can be configured to calculate one or 2 checksums for even parities, and one or two checksums for odd parities. In the list box you can mark, in those lines reserved for parity check sums (Even1, Even2, Odd1 and Odd2), which bits should be included in the checksum.

In the topmost line (Field) one bit is designated for each checksum used to balance out the checksum depending on its parity type. If a parity type (Even1, Even2, Odd1, Odd2) is not used then its row is simply left blank.

Activation/Deactivation of card definitions

The symbol in the first column of the list box reflects the activation status of each card definition.

✓ activated

✗ deactivated

The activation status can be toggled by double clicking on the symbol.

Safety checks warn about the consequences of deleting a card definition that is in use.

> **Notice!**
> **Incorrect card encoding or a bad combination may lead to all cards become unreadable! Do you really wish to activate the selected card encoding?**.

> **Notice!**
> **All current cards using this encoding will become unreadable! Do you really wish to deactivate the selected card encoding?**.

17 Appendix

The section that follows collates interesting and often important (additional) information that does not belong to any particular topic in the preceding documentation, but may be applicable at several places.

17.1 Signals

A list of the available signals for inputs and outputs.

Input signals	Description
Door sensor	
Request to exit button	Button to open the door.
Bolt sensor	Is used for messages, only. There is no control function.
Entrance locked	Is used to lock the opposite door in sluices temporarily. But can also be used forpermanently locking.
Sabotage	Sabotage signal of an external controller.
Turnstile in normal position	Turnstile is closed.
Passage completed	A passage was completed successfully. This is a pulse of an external controller.
IDS: ready to arm	Will be set by the IDS, if all detectors are in rest and the IDS can be armed.
IDS: is armed	The IDS is armed.

Input signals	Description
IDS: request to arm button	Button to arm the IDS.
Local open enable	Will be used if a doorway arrangement opens the door without involving the AMC. The AMC sends no intrusion message but "door local open".

Output signals	Description
Door opener	
Sluice: lock opposite direction	Locks the other side of the sluice. Is set when the door opens.
Alarm suppression	... to the IDS. Is set as long as the door is open, to avoid that the IDS createsan intrusion message.
Indicator green	Indicator lamp - will be controlled as long as the door is open.
Door open too long	Pulse of three seconds. If the door is open too long.
Camera activation	Camera will be activated at the beginning of a passage.
Open turnstile inbound	
Open turnstile outbound	
Door is permanent open	Display that the door is permanent open.

Output signals	Description
IDS: arm	Pulse or permanent contact to arm the IDS.
IDS: disarm	Pulse to disarm the IDS.

17.2   Default Doormodels

Standard door models
The following door models are available by default:

01a   Normal door with entry and exit reader

01b   Normal door with entry reader and push button

01c   Normal door with entry reader

03a   Reversible turnstile with entry and exit reader

03b   Reversible turnstile with entry reader and push button

03c   Turnstile with entry reader

06c   Enrollment via AMC – no entrance control!

07a   Elevator with max. 16 floors

07b   Elevator with max. 16 floors

10a   Normal door with entry and exit reader and IDS rearming

10b   Normal door with entry reader, push button and IDS rearming

10c   Normal door with entry reader and IDS rearming

10d   Normal door with entry and exit reader and decentral IDS rearming

10e   Normal door with entry reader, push button and decentral IDS rearming

10f	Normal door with entry reader and decentral IDS rearming
14a	Normal door with entry and exit reader and IDS rearming (arming authorization)
14b	Normal door with entry reader, push button and IDS rearming (arming authorization)
14c	Normal door with entry reader and IDS rearming
14d	Normal door with entry and exit reader and decentral IDS rearming
14e	Normal door with entry reader, push button and decentral IDS rearming
14f	Normal door with entry reader and decentral IDS rearming

17.3   Doormodel 01

Normal door
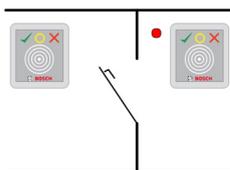
Signals:

Input signals	Output signals
Door sensor	Door opener
Request to exit button	Sluice: lock opposite direction
Bolt sensor	Alarm suppression
Entrance locked	Indicator green

Input signals	Output signals
Sabotage	Camera activation
	Door open too long

Model variants:

01a   Normal door with entry and exit reader

01b   Normal door with entry reader and push button

01c   Normal door with entry reader

Note:
Man-trap locking is only active if the door is parameterized as part of a man-trap.
If the door is not configured as part of a man-trap then input signal 03 is interpreted as a reader lock. In such a case if input signal 03 is set the reader will be locked.
Alarm suppression is only activated when the alarm suppression time before door opening is greater than 0.
Optional secondary readers can be connected. In combination with a second door and man-trap locking it is possible to control both doors together as a man trap. This usage can also be advantageous for vehicle entrances, in which case a secondary reader for trucks and cars is also recommended.

---

i **Notice!**
Singling function can be parametrized with DM 03, only.

17.4   Doormodel 03

Reversible turnstile
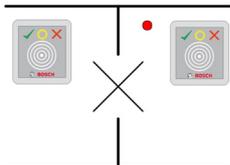
Signals:

Input signal	Output signals
Turnstile in normal position	Open turnstile inbound
Request to exit button	Open turnstile outbound
Entrance locked	Sluice: lock opposite direction
Sabotage	Alarm suppression
	Camera activation
	Door open too long

Model variants:

03a	Reversible turnstile with entry and exit reader
03b	Reversible turnstile with entry reader and push button
03c	Turnstile with entry reader

Note:
Man-trap locking is only active if the door is parameterized as part of a man-trap. If the door is not configured as part of a man-trap then input signal 03 is interpreted as a reader lock. In such a case if input signal 03 is set the reader will be locked.

In combination with a second door and man-trap locking it is possible to control both doors together as a man trap. Depending on the construction the entrance can perform a singling function.

17.5 Doormodel 06c

The doormodel 06c configures a reader connected to the AMC as enrollment device. It does not control an entrance.

17.6 Doormodel 07

Elevator with max. 16 floors
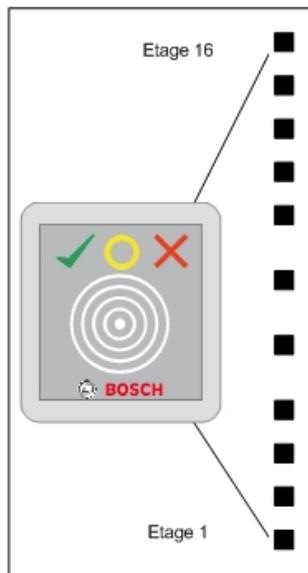
Model variants:

07a	Elevator with max. 16 floors
07b	Elevator with max. 16 floors

Signals of entrance model 07a:

Input signal	Output signals
Free	Floor 01
Free	Floor 02
Free	Floor 03
Free	Floor 04
...	...
Free	Floor 16

Procedure:

First, the cardholder summons the elevator. This can be done either via the elevator's own hardware button, or via a card reader (e.g. Door model 01c).

Next, inside the elevator is another card reader (Door model 07a). This reader grants access to those floors for which the user's card contains authorizations. The authorized floors can be indicated to the user, for example, by illuminating only the buttons for those floors. The user can then select only one of the authorized floors.

Signals of entrance model 07b:

Input signal	Output signals
Input key - floor 01	Floor 01
Input key - floor 02	Floor 02
Input key - floor 03	Floor 03
Input key - floor 04	Floor 04
...	...
Input key - floor 16	Floor 16

Procedure:

First, the cardholder summons the elevator. This can be done either via the elevator's own hardware button, or via a card reader (e.g. Door model 01c).

Next, inside the elevator the user presents his/her card to another card reader (Door model 07a), and then presses the button for the desired floor. The AMC checks whether the user is authorized for the selected floor and, if so, the lift takes the user there.

In addition this door model possesses the parameter Public Access, which can be set for each floor individually. If this parameter is set then authorizations for this floor are not checked, i.e. any user may proceed to this floor. Moreover Public Access can be made dependent on a particular time model, so that authorizations are only checked by the AMC outside of that time model's designated hours.

17.7   Doormodel 10

Normal door with IDS (intrusion detection system) arming/
rearming

Signals:

Input signals	Output signals
Door sensor	Door opener
Request to exit button	IDS: Disarm [only for models **d** and **f** with a pulse of 1 sec.]
IDS: ready to arm	Camera activation
IDS: is armed	IDS: Arm [only for models **d** and **f** with a pulse of 1 sec.]
Sabotage	Door open too long
IDS: request to arm button	

Model variants:

10a	Normal door with entry and exit reader and IDS rearming
10b	Normal door with entry reader, push button and IDS rearming
10c	Normal door with entry reader and IDS rearming

10d	Normal door with entry and exit reader and decentral IDS rearming
10e	Normal door with entry reader, push button and decentral IDS rearming
10f	Normal door with entry reader and decentral IDS rearming

Notes:

The **E** button at the entry reader can arm the IDS (intrusion detection system). An authorized card and the entry of a PIN code are required. The IDS will be disarmed upon the first authorized entry, whereby PIN-code identification will also be required. In the case of models a to c this is controlled by the output signal arm/disarm IDS.

In the case of models **d** to **f** the arming or disarming is triggered by a separate pulse of 1 second. A connected bistable relay can control the IDS for several doors (DCUs / Door control units), whereby the signals require a logical OR connection to the relay. The signals **IDS is armed** and **IDS is disarmed** must be double connected at all the relevant DCUs.

17.8   Doormodel 14

Door with IDS control

Signals:

Input signals	Output signals
Door sensor	Door opener
Request to exit button	IDS: Disarm [only for models **d** to **f** with a pulse of 1 sec.]
IDS: ready to arm	Camera activation
IDS: is armed	IDS: Arm [only for models **d** to **f** with a pulse of 1 sec.]
Sabotage	Door open too long
IDS: request to arm button	

Model variants:

14a   Normal door with entry and exit reader and IDS arming / disarming

14b   Normal door with entry reader, push button and IDS arming / disarming

14c   Normal door with entry reader and IDS arming / disarming

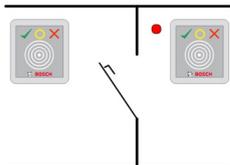| 14d | Normal door with entry and exit reader and decentral IDS arming / disarming |
| 14e | Normal door with entry reader, push button and decentral IDS arming / disarming |
| 14f | Normal door with entry reader and decentral IDS arming / disarming |

Notes:

In contrast to door model 10, door model 14 can use readers with or without a keypad. A further difference exists in the assignment of IDS arming rights: only cardholders with sufficient rights are able to arm or disarm the IDS.

The arming/disarming process is not governed here by use of a PIN code, but by a button close to the reader which has the same function as key 7 on the readers with keypads. After pressing this button the status of the IDS is displayed by the colored LEDs of the reader.

– Disarmed = alternating green/red blinking light
– Armed = continuous red light

The IDS is armed when presented with a valid card.

Disarming is carried out by pressing the button and presenting a valid card.

The door does not unlock immediately. To unlock, present the card once more after disarming.

17.9   Examples of mantrap configurations

Turnstiles are the most common means of singling cardholders' access. In the following examples we have therefore used door model 3a (turnstile with entry and exit reader).

Mantrap configuration with two turnstiles (DM 03a)
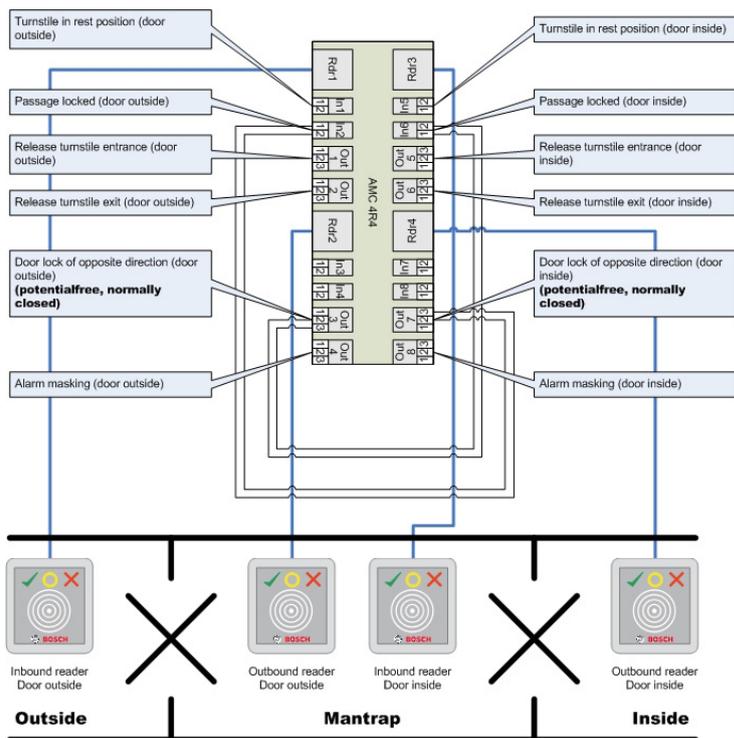
Connections to the door locks for the opposite direction ensure that only one of the turnstiles can be opened at any one time.

Notice!

The output signal (Out 3) is to be set potential free (dry mode).
The signal "door lock of opposite direction" must be closed
(resistance=0) when de-energized. Use the "normally closed"
(NC) contact of outputs 3 and 7.

**Mantrap configuration with two turnstiles (DM 03a) which are
distributed across two controllers.**
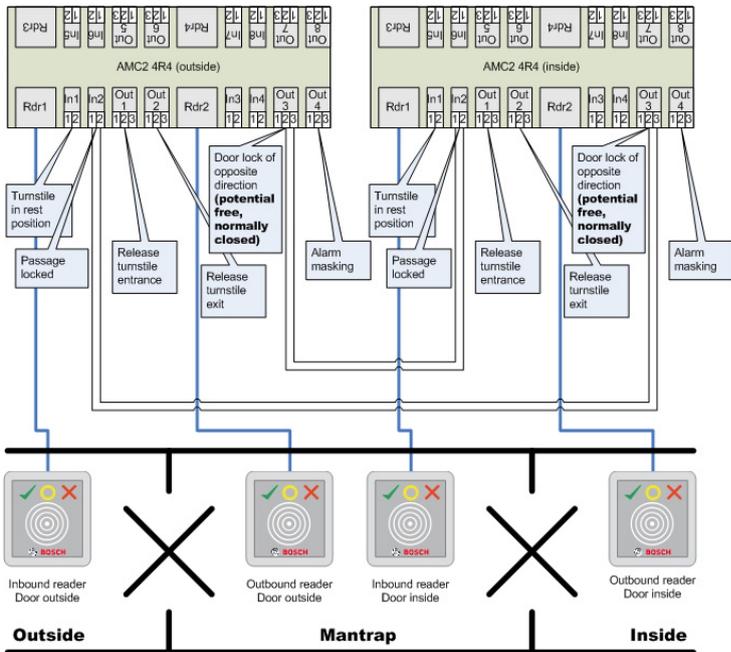
Connections to the door locks for the opposite direction ensure
that only one of the turnstiles can be opened at any one time.

Notice!

The output signal (Out 3) is to be set potential free (dry mode). The signal "door lock of opposite direction" must be closed (resistance=0) when de-energized. Use the "normally closed" (NC) contact of outputs 3 and 7.

17.10   Configuring Entrance Model 07

The following illustrates the wiring of an elevator using Door
Model 07a
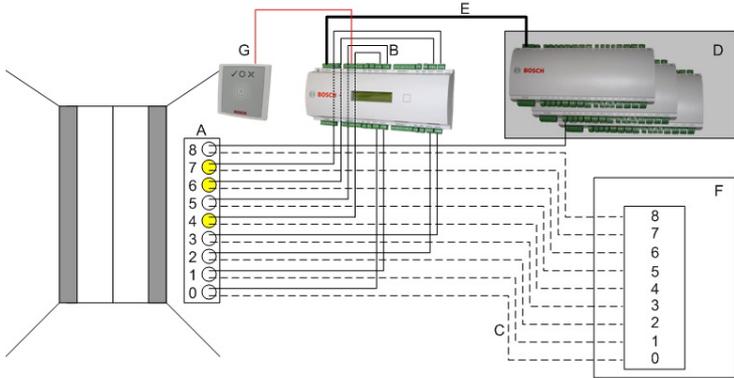
Legend:

A = Floor buttons inside elevator

B = (solid line) AMC-output signals

C = (dashed line) Connection to elevator control

D = An I/O extension board (AMC2 8I-8O-EXT, AMC2 16I-EXT or
AMC2 16I-16O-EXT) can be connected

E = Data- and power supply from the AMC to the I/O boards

F = Elevator control

G = Reader (Door model 07a)

The following illustrates the wiring of an elevator using Door
Model 07b
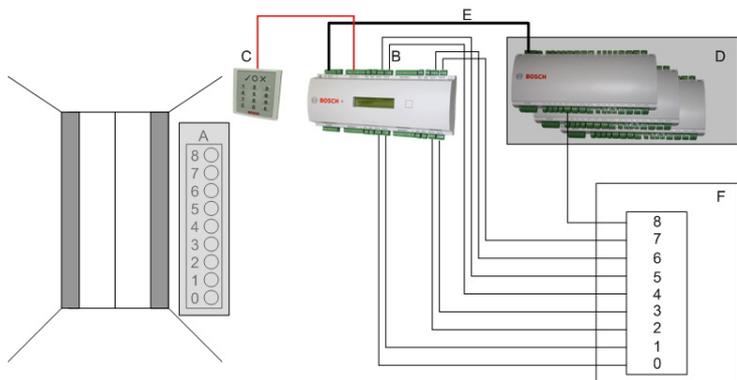
Legend:

A = Floor buttons inside elevator

B = (solid line) AMC input signals

C = (dashed line) AMC output signals

D = An I/O extension board (AMC2 8I-8O-EXT, AMC2 16I-EXT or AMC2 16I-16O-EXT) can be connected

E = Data and power supply from the AMC to the I/O boards

F = Elevator control

G = Reader (Door model 07b)

Notice!

When wiring individual floors (up to 16) to the AMC's outputs, connect first the controller's own signals and then, if present, the first eight outputs of any I/O extension boards in ascending order. [Where Wiegand extension boards(AMC2 4W-EXT) are in operation, use their outputs in ascending order after those of the AMC2 controller, and before the outputs of any I/O extension board.] For this reason it is not possible to configure any other kinds of door, or any further elevators, to an AMC that is used for elevator control.

17.11   Display Arming/Disarming

Comparison between **arming** an alarm system in Entrance
(Door) models 10 and 14.
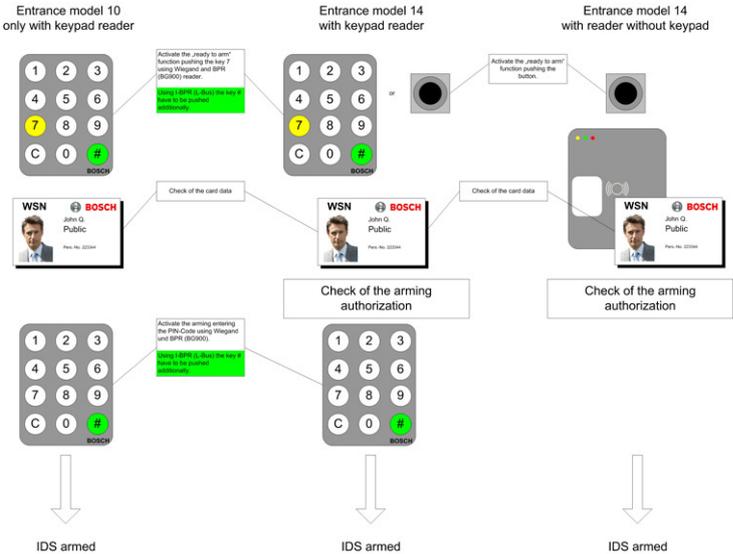
Comparison between **disarming** an alarm system in Entrance
(Door) models 10 and 14.

17.12 Procedures in Access Control

Flow charts of procedures in Access Control

Door model DM01

Door model DM10 - arming

Press key 7 on reader keypad

Press and release "Trigger arm IDS" button

In = Input signal
Out = Output signal

In 1: Door contact
In 2: IDS armed
In 3: IDS ready to arm
In 4: Trigger arm IDS
In 5: "Request to exit" button (DM10b or 10e)

Out 1: Release door
Out 2: Arming IDS
Out 3: Disarming IDS (DM10d,e,f)

Remarks:
In case of an iBPR reader entering "7" or a PIN code must be completed by typing "E" or "#"

"Ready to arm" set?

[False] — IDS not ready to arm

[True]

Offer card to reader. (Reader reads card data)

IDS is not armed
Output "arming IDS" NOT set (10 a,b,c)

Enter arm/disarm PIN code

PIN code correct?

[False] — Wrong PIN code

[True]

Output "arming IDS" set (10a,b,c)

Output "arming IDS" pulsed (10d,e,f)

"IDS armed" set within timeout?

[False] — IDS is not armed
Output "arming IDS" reset (10 a,b,c)

[True] — IDS is armed
Output "arming IDS" remains set (10 a,b,c)

Door model DM10 - disarming

In = Input signal
Out = Output signal

In 1: Door contact
In 2: IDS armed
In 3: IDS ready to arm
In 4: IDS arm IDS
In 5: "Request to exit" button (DM10b or 10e)

Out 1: Release door
Out 2: Arming IDS
Out 3: Disarming IDS (DM10d,e,f)

Remarks:
In case of an iBPR reader entering "7" or a PIN code must be completed by typing "E" or "#"

Offer card to reader
(reader reads card data)

Enter
arm/disarm PIN code

PIN code correct?

[False]

Wrong PIN code.
IDS remains armed
(Output "Arming IDS" remains set – 10a,b,c)
no ACCESS (Output "Release door" remains reset)

[True]

IDS is disarmed
Output "disarming IDS" set (10a,b,c)
Output "disarming IDS" pulsed (10d,e,f)

Input "IDS armed" reset?

[False]

IDS not disarmed .
IDS remains armed
(Output "Arming IDS" remains set – 10a,b,c)
no ACCESS (Output "Release door" remains reset)

[True]

The door is opened
Output "Release door" set

Input "Door contact" reset within max. lock activation time?

[False]

NO ACCESS
(Timeout)

[True]

ACCESS

Door closed
(Input "Door contact" set)

Door model DM14 - arming

Legend box:

In = Input signal
Out = Output signal

In 1: Door contact
In 2: IDS armed
In 3: IDS ready to arm
In 4: Trigger arm IDS
In 5: "Request to exit" button (DM14b or 14e)

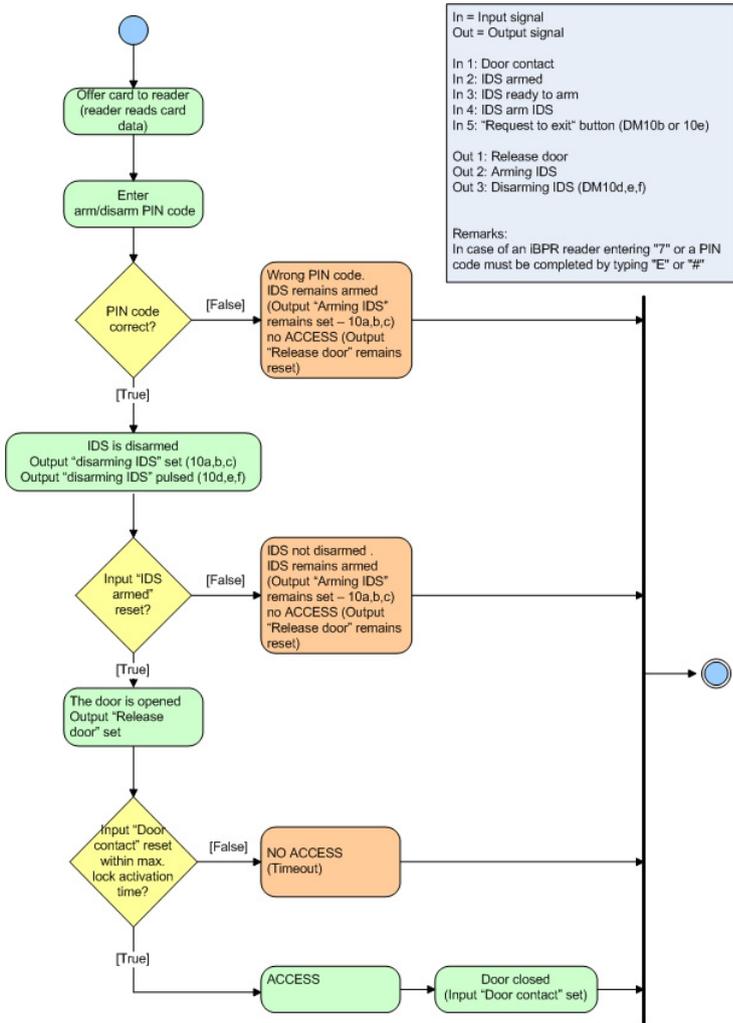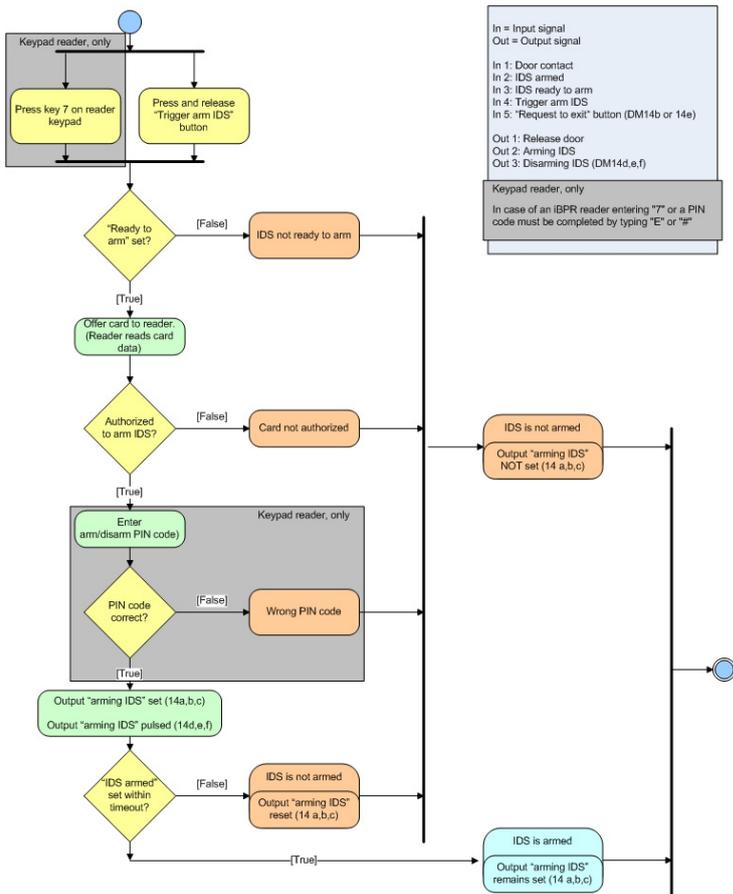Out 1: Release door
Out 2: Arming IDS
Out 3: Disarming IDS (DM14d,e,f)

Keypad reader, only

In case of an iBPR reader entering "7" or a PIN code must be completed by typing "E" or "#"

Flowchart text:

Keypad reader, only

Press key 7 on reader keypad

Press and release "Trigger arm IDS" button

"Ready to arm" set? — [False] → IDS not ready to arm

[True]

Offer card to reader. (Reader reads card data)

Authorized to arm IDS? — [False] → Card not authorized

[True]

Keypad reader, only

Enter arm/disarm PIN code)

PIN code correct? — [False] → Wrong PIN code

[True]

Output "arming IDS" set (14a,b,c)
Output "arming IDS" pulsed (14d,e,f)

"IDS armed" set within timeout? — [False] → IDS is not armed / Output "arming IDS" reset (14 a,b,c)

[True] → IDS is armed / Output "arming IDS" remains set (14 a,b,c)

IDS is not armed / Output "arming IDS" NOT set (14 a,b,c)

Door model DM14 - disarming

17.13 Access PE ports

The individual processes and applications in Access PE use the following ports.

Connection between...	Client/AMC	Server
Client - LacSp	Undefined	43434/tcp
AcPers - CP	Undefined	20005/tcp
LacSp - AMC	10001/udp	54545/udp and above

18   PIN types

Access Professional Edition provides each cardholder with up to three Personal Identification Numbers (**PIN**s) which can be used for different purposes:

– **Verification-PIN**

This PIN can be requested from cardholders as an extra security feature at special entrances. The verification PIN is compared with stored data for the cardholder to ensure that s/he is the real owner of the card presented.
Each person can choose his/her own 4-8 digit PIN in accordance with certain general rules (e.g. no numerical sequences and no palindromes). [The parameter for the length of the PIN applies equally to verification-, arming- and door-PINs]. A verification-PIN does not have to be unique in the system.
If no separate arming-PIN has been defined [i.e. as long as the check box **use separate IDS-PIN** is not selected in the dialog Configurator > Settings] then the verification PIN may also be used to arm/disarm the IDS.

– **Arming-PIN / IDS-PIN**

This special PIN is used exclusively to arm and disarm the alarm system. With door models 10 and 14 first press the 7 key or the door's push-button.
Each person can choose his/her own 4-8 digit PIN in accordance with certain general rules (e.g. no numerical sequences and no palindromes). [The parameter for the length of the PIN applies equally to verification-, arming- and door-PINs]. An arming-PIN does not have to be unique in the system.
If the cardholder wishes simply to pass through the door, and is required to enter a PIN, then the verification-PIN must be used. If the the check box **use separate IDS-PIN** is selected (Configurator > General settings) then the

verification-PIN can no longer be used to arm/disarm the IDS. It is only then that the relevant input fields become visible in the Personnel dialog.

Notice!
In order to ensure compatibility with previous Access PE versions the check box for use of separate IDS-PIN is cleared by default.

– **Identification-PIN/ ID-PIN**
This PIN identifies a person's card and must therefore be unique within the system. Once input this PIN grants access to the person in accordance with all his/her defined authorizations. To ensure uniqueness the PIN is generated by the system and assigned to the person, whereby the system adheres to the general rules (no numerical sequences and no palindromes).
Like a physical credential the Identification-PIN enforces the restrictions assigned to its owner (blocks, time models, authorizations etc.).
Depending on the reader protocol, you must enter the Identification PIN on the reader, along with the additional characters required. In the case of readers enter the pin as follows: **4 # (Enter) PIN # (Enter)**. For all other protocols, the PIN is entered immediately and followed by **# (Enter)**. The length of this PIN is configurable to between 4 and 8 digits.
[**Note:** The length of ID-PINs should bear relation to the size of the installation, in order to render active PINs harder to guess. For instance, if the installation has 1000 cardholders then the PINs should be at least 6 digits long in order to make the guessing of a valid PIN sufficiently improbable, and random guesses more likely to generate alarms.]

The PIN types described above are all person-related and therefore defined and maintained along with other personnel data. A fourth type is the so-called door-PIN.

– **Door-PIN**
The PIN belongs to an entrance (Configurator > Entrances). It must be known by all persons authorized to use it. instead of the PIN a card may also be used at such entrances (see = Function **PIN or card**).
This PIN too can be 4 to 8 digits long. If the use of the door-PIN is deactivated (e.g. by a time model) then access is only by card. An identification-PIN will not work either in this case.

Notice!
The Identification- and door-PIN-types can not be used with IDS-arming door models 10 and 14.