

Access Professional Edition

Personnel Management



BOSCH

en Operation Manual

Table of contents

1	Overview	5
1.1	Modular Design	5
1.2	Server and Client Modules	5
2	General	7
2.1	Introduction	7
2.2	User Login	11
2.3	Layout of the Personnel Management	14
2.4	Tool bar of the sub menus	15
2.5	Enrollment Configuration	19
2.5.1	Enrollment via AMC connected readers	21
3	Personnel Management	26
3.1	Persons list	26
3.2	Dialog box for personnel data	29
3.3	Device status	31
3.4	Online swipe	34
3.5	Video Management	35
3.5.1	Video panel	35
3.5.2	Live image	38
3.6	Video Management	39
3.6.1	Video panel	40
3.6.2	Live image	42
4	Personnel data	44
4.1	Personnel and card data	45
4.2	Assigning and revoking cards	50
4.3	Authorizations	53
4.4	Additional fields	56
4.5	Application of time models	57
5	Create cards	60
5.1	Creating cards	60
5.2	Taking or importing photos	62
5.3	Previewing and printing cards	67
5.4	Printing card receipts	70

6	Reports	72
6.1	Reports	72
6.2	Reports: Page view	78
7	Local recordings	82
8	User rights	84
8.1	User rights	84
8.2	Setting user access rights	88
8.3	User handover and workstation security	89
9	UL 294 Requirements	91

1 Overview

1.1 Modular Design

The Access Professional Edition System (hereunder referred to as **Access PE**) provides a self-contained access control for small and medium sized companies. It consists of several 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
- Alarm Management
- Video Verification

1.2 Server and Client Modules

The modules 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)

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-layer design: **The first layer** 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 layer 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 layer consists of card readers.

The communication between client, server, and cardholders is AES encrypted.

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. All assigned cards are active. 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 Cancellation 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

The following applications are available. See the respective User manuals for details:



Personnel Management



Configurator



Logviewer



Map and Alarm Management



Video Verification



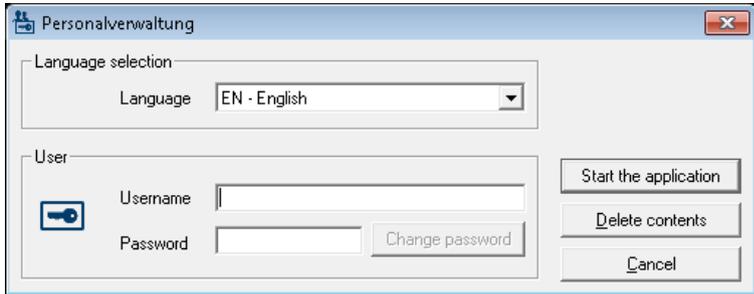
Notice!

A login from the client is only possible with the LAC service running on the server.

Client Login

The system's applications are protected from unauthorized use. The **default passwords** on first usage are:

- Username: **bosch**
- Password: **bosch**



After entering a username and password, the button **Change Password** becomes active.

After 3 wrong entries a time delay before the next logon will be the consequence. This applies for the buttons "Start the Application" and "Change Password".

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
- French
- Japanese
- 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.

After clicking the **Change Password** button enter a new user name and password in this dialog:

The image shows a standard Windows-style dialog box titled "Change password". It contains two text input fields: "New password" and "Confirmation". Below the input fields are two buttons: "Ok" and "Cancel". The dialog box has a light blue title bar and a white background.



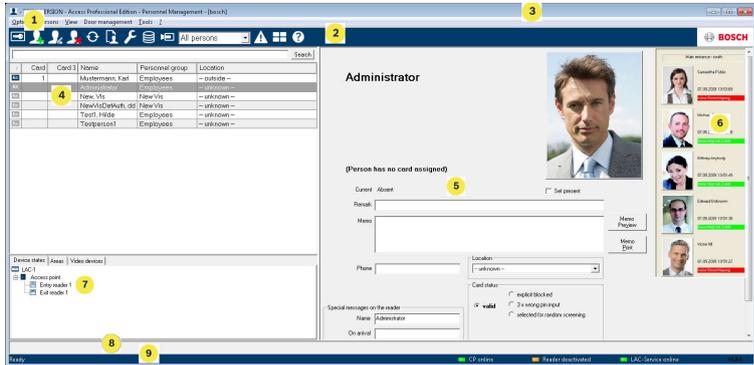
Notice!

Do not forget 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!**

2.3 Layout of the Personnel Management

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. 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.

2.4 Tool bar of the sub menus

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

Function	Icon	Description
Menu Options		
Refresh		Refreshes the Personnel list
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.

Function	Icon	Description
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.
	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.

Function	Icon	Description
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 context menu (right click on the desired door/entrance)	The entrance selected in the device list is displayed and can be opened (one-off).
Long-term open		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.

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

2.5 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



Notice!

The Delta 1200 Series and Rosslare ARD-1200EM Series were not evaluated by UL.

Consequences

- **Chip card system**

Displays the card technology – MIFARE classic and Hitag1 can be used for Access PE.

Change Configuration

Attention:
These properties will be activated immediately. This may take some time (look at the status bar).
These properties will be stored permanently and will already be activated after a restart of your computer.

Enrollment Reader Reader type: Delta 1200 RS232 Prox, iClass (WIE1)
Card type: HID 26 - Standard Wiegand 26 Bit Code
Serial: COM1:
Baud rate: 9600
Parity: none even odd
Data bits: 7 8
Stop bits: 1 2

CP system for card personalization installed

Connect to LAC service (transmit all card changes immediately to the subsystem)

Do not show dialog for edit and view internal card information

Enable THAI font for reports (use special font)

Ok Cancel

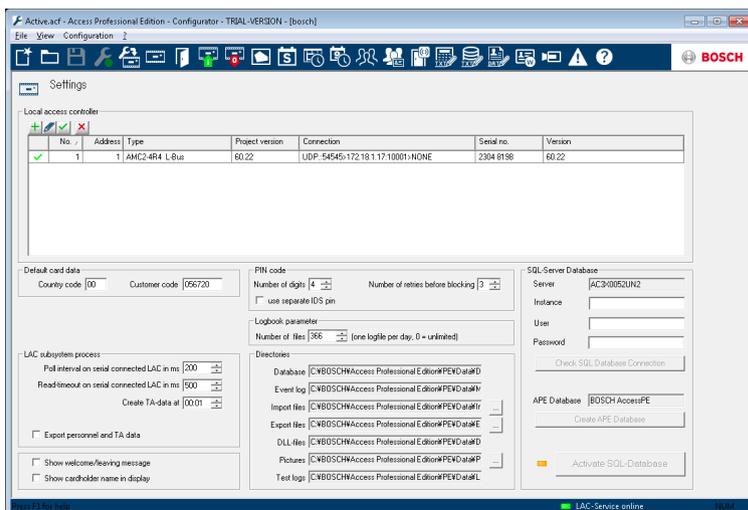
- If the system has been installed with the optional **Card Personalization** (CP) module then the corresponding check box is selected in settings. Unchecking this box blocks all functions for card design/creation.
- In addition the automatic transfer of personnel data via **Connection to the LAC Server** 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.
- Click the check box **Enable THAI fonts for report**, if reports are required in Thai language and fonts. NOTE: This works only in the English language dimension.

2.5.1 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 **Configurator** and select a **Local Access Controller (LAC)** (e.g. AMC2...)



Click the **Entrances** symbol and add a new Entrance reader:

Define Entrance ? X

Description

Please configure LAC, GID and doormodel

LAC GID

Door model

Video verification Surv. camera:

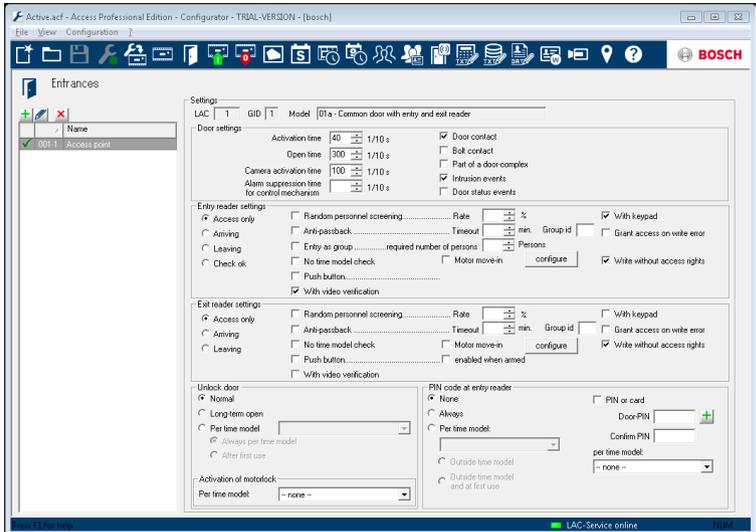
Reader configuration

	Reader type	Address	Write access
Entry-reader	<input type="text" value="RS485"/>	<input type="text" value="1"/> ✓	<input type="text" value="read only"/>
Exit reader	<input type="text" value="RS485"/>	<input type="text" value="1"/> ✓	<input type="text" value="read only"/>

Signal definition

	Signal description	On dev...	GID / Board	DID	Connection
✓	Revolving door in normal posit...				
✓	Pushbutton: Door open				
✓	Entrance locked				
✗	Sabotage signal				
✗	Open entry of revolving door				
✗	Open exit of revolving door				
✗	Lock opposite direction (to ot...				
✗	Alarm suppression				

The dialog window **Entrances** 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 to the APE client.

- Select Tool > Properties.

Change Configuration

Attention:
This properties will be activated immediately. This may take some time (look at the status bar).
This properties will be stored permanently and will already be activated after a restart of your computer.

Enrollment Reader

Reader type: Delta 1200 RS232 Prox, iClass (WIE1)

Card type: HID 26 - Standard Wiegand 26 Bit Code

Serial: COM1

Baud rate: 9600

Parity: none even odd

Data bits: 7 8

Stop bits: 1 2

CP system for card personalization installed

Connect to LAC service (transmit all card changes immediately to the subsystem)

Do not show dialog for edit and view internal card information

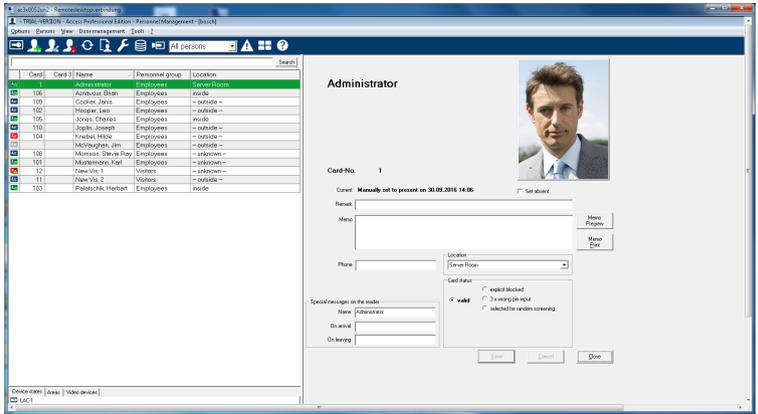
Enable THAI font for reports (use spezial font)

Ok Cancel

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 Personnel Management

This dialog is the main application of the workstations. Along with the data storage and editing facilities, this dialog also shows the locations of individual people as well as any blocks in place against them. You can also carry out system monitoring processes via the door control functions and device state displays.

3.1 Persons list

The persons list contains all persons known to the system. By default surname, first name and company or department are listed. A separate symbols column gives further details about status of the person or card as follows:



The person has no card



The person is absent



The person is present



The person is absent and blocked. The dialog shows a blinking light in addition.



The person is present and blocked. The dialog shows a blinking light in addition.

	Card	Name	Personnel group	Location
	1	Administrator	Employees	Server Room
	106	Aznavour, Brian	Employees	inside
	109	Cocker, Janis	Employees	- outside -
	102	Hooper, Leo	Employees	- outside -
	105	Jones, Charles	Employees	inside
	110	Joplin, Joseph	Employees	- outside -
	104	Knebel, Hilde	Employees	- outside -
		McVaughan, Jim	Employees	- outside -
	108	Morrison, Stevie Ray	Employees	- unknown -
	101	Mustermann, Karl	Employees	- unknown -
	12	New Vis, 1	Visitors	- outside -
	11	New Vis, 2	Visitors	- unknown -
	103	Palatschik, Herbert	Employees	inside

The default list view, with columns **Symbol, Name, Company/ Dept.**) can be customized for each workstation. The menu **View > Personnel Data** can be used to add or remove further columns. Displayed columns are marked with a tick and reselecting toggles the option on and off.

The following additional columns are available:

- card No.
- Personnel No.
- Company / Dept.
- Personnel Group
- Telephone
- Location (if **Areas** have been defined)
- Picture

Notice!



The current width of the list box may not allow all selected columns to be displayed. In this case please adjust the width and the order of the box and columns to best suit your needs. The order of columns can be changed by dragging and dropping the column headers. Increasing the width of the persons list of course impacts the width of the dialog box to its right.

The tool bar contains a combo-box to filter the persons list. By default **all persons** are displayed under **Employees** or **Visitors**.



Note: If you add an additional group (e.g. VIPs) the members of this group will be automatically listed under **Employees**.

You can add the **Picture** column to the Personnel list. You can hide or show the column via the **View > Personnel data > Picture** menu.

As this column is added to the far right, you sometimes need to scroll through the Personnel list to make it visible. Other columns may need to be hidden.

	Card	Name	
	106	Brocker, Heinz	
	109	Büsing, Gerhard	
	102	Christian, Thomas	
	105	Dabs, Andreas	
	110	Delesen, Frank	
	104	Fallmann, Inna	
		Fuhs, Wolfgang	
	108	Gilleßen, Harald	
	101	Hannewald, Joachim	
	12	hans	
	11	Herrmann, Falk	
	103	Krimmel, Thorsten	

Notice!



The images fit the height of the column, so people can be difficult to identify when the display is small. The main reason for displaying the images is therefore to enable users to quickly check which persons do not yet have a photo stored.

3.2 Dialog box for personnel data

If you select an entry in the **persons list**, that person's data are displayed in the dialog field to the right.

Victor All

Card-No. 577

Current **Present since 08.05.2009 15:50** Set absent

Remark

Memo

Phone

Location: in der Firma (anwesend)

Special messages on the reader

Name: Victor All

On arrival: Good morning

On leaving: Good bye

Card status:

- explicit blocked
- valid
- 3 x wrong pin input
- selected for random screening

Buttons: Memo preview, Memo print, Save, Cancel, Close

Apart from displaying the most important personal data various functions can be invoked from this dialog.

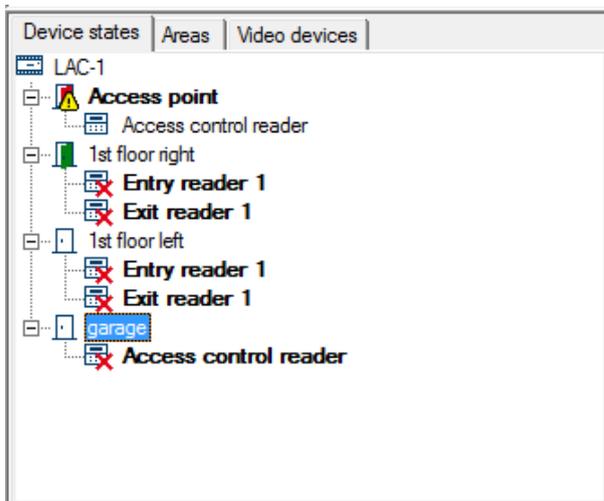
Display/Function	Description
Name (Title - First name - Last name)	Display only - modifications can be made using the modification dialog - <i>Personnel and card data, page 45.</i>
Company/Dept.	
Personnel-No.	

Display/Function	Description
Card-No.	
Photo	
Current Status	Absence / Presence display including date.
Set present, Set absent	Depending on current status the person can be set present or absent here.
Notes	Room for free text notes about this person. Max. 50 characters.
Memo	Room for free text memo to this person. Max. 300 characters.
Memo preview/ Print Memo	The memo text can be viewed or printed according to a predefined print layout.
Telephone	Telephone number or reachability of this person.
Location	Display and modification of the person's location. Any area can be selected, as well as the default value -- unknown --.
Special messages on the reader	each line of the display can contain a maximum of 20 characters
Name	Person's name as displayed by suitably equipped readers.
On arrival	Special welcome text.
On leaving	Special farewell text.

Display/Function	Description
Card status	
<ul style="list-style-type: none"> - valid - explicitly blocked - 3x wrong PIN input - Selected for random screening 	Display and modification of card status. The following card parameters can be set here.

3.3 Device status

The third area in the main personnel management dialog, situated beneath the persons list, is the device status display. Situated next to the list of log messages is the device status display.



The following symbols reflect the device status :

Device status	Symbol
Controller is online	
Controller is offline	
Connection to the controller can not be determined	
Connection to reader - OK	
Connection to reader is faulty	
Connection to reader can not be determined.	

Operation mode/ Door status	Symbol for Normal	Symbol for Permanent open	Symbol for Permanent locked
Closed			
Open normal			N.A.
Open timeout		N.A.	N.A.
Open broken		N.A.	
Unknown			
Defective			

Faulty connection are marked additionally by a bar at the bottom edge of the dialog, blinking red at the dialog start.

Connection to LAC 1, 2, 3, 4 out of order !



Notice!

The status display of Wiegand readers can be misleading. Because they are not able to respond to status requests a parameterized Wiegand reader is shown as online as long as its controller is online.

Controls

This function is only active when the user logged in has **door control rights** - *User rights, page 84*.

This function is only active when the user logged in has **door control rights**.

Selected entries in the device status list to which there is a connection can be given commands via the context menu (right click) or the menu **Door management**

Open Main entrance
Long-term open Main entrance
lock Main entrance

The name of the selected entry is read from context.

- | | |
|----------------------------------|--|
| Open <Entrance> | The selected entrance opens once (for one person). |
| Long-term open <Entrance> | The selected entrance opens for a longer period. |
| Lock <Entrance> | The selected entrance is locked. |

3.4 Online swipe

The context menu of the entries in the device states list also offers the **Online swipe** function, which opens a pane to the right of the dialog field.

In this area the function displays a history of bookings and messages for the selected entrance. The last persons to scan their cards at one of this entrance's readers are listed along with their archive images, a timestamp and the system's decision regarding access.

Additionally any messages not belonging to the categories **Message** or **Information** (except message numbers 61 to 67)



are displayed here marked with the  symbol.

The entrance in question is displayed at the top of the pane. Even after selecting a different entrance in the device states list, the online swipe view for the first entrance remains. To switch to online swipe view for another entrance, you must invoke it explicitly via the context menu for that entrance

For as long as it is active the context menu contains the line **switch off online swipe**, so that the access history can be hidden again at any time. Notes highlighted in color indicate whether access was granted (green) or denied (red) in each case.

	Administrator 06.02.2017 14:39:44 Access
	Egon Müller 06.02.2017 14:41:08 Not authorized
	06.02.2017 14:39:47 Card unknown, V.@@@

Only the last 5 messages and/or bookings are shown. While the Online swipe view is active, the display is updated constantly with new messages, the most recent appearing at the top.

The list contains only access requests for the current day and previous day. If no cards were scanned during this period the list remains empty.

3.5 Video Management

The video components integrated in the Access Professional Edition access control system can be used as an additional control facility at special entrances for the purpose of comparing live images with images stored in a database, and to check the surrounding area. It is also possible to generate special alarm responses using video recordings and to monitor specific areas, even independently of entrances.

In addition, video components can be accessed and used in Access PE in the following areas.

- Video verification: additional optical controls at entrances
- Alarm management: specially configured alarm messages and entries can be supported by recorded video sequences
- Video displays: playback of current camera images from up to four freely configurable cameras at the same time

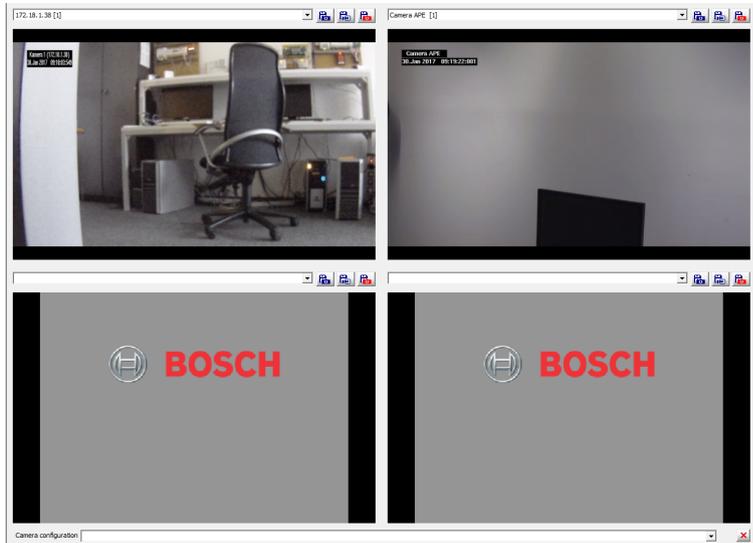
See also

- *Video panel, page 35*
- *Live image, page 38*

3.5.1 Video panel



Press the  button in the Personnel Management toolbar to replace the dialog field with a display showing four video views.



In the video panel it is possible to select up to four cameras from different entrances.

The following functions are available for each display window.

Selection list

You can select any camera loaded into the access control system and replace it at any time.



Stores a still image of the current view as **<device name>_yyyyMMddhhmmsstttt.jpg** at C:\BOSCH\Access Professional Edition\PE\Data\Video (default path).



Starts/ends a video recording of the current view and stores it as **<device name>_yyyyMMddhhmmsstttt.vxx** at C:\BOSCH\Access Professional Edition\PE\Data\Video (default path).



(= Point of Interest) Creates a still image of the current view – **POI_** is added to the start of the file name.

A log book message is also created as a marker.

Customizing views for the video display

A particular selection and ordering of cameras can be saved and then recalled by name at a later time. This saves time otherwise spent manually selecting and configuring the same view.

First manually configure the view you want by positioning the cameras in their respective windows as suits you best.

Next, give the view a meaningful name by editing in the lower combo box and save it by pressing ENTER. These views can afterwards be recalled by name from the same combo box.

In this way operators can save different camera views for different purposes, e.g. to monitor incoming personnel in the morning, and outgoing in the evenings. Saved views belong to the workstation and not to the individual operator. They can not be edited as such. To change a view first invoke it from the combo box, delete its name using the



button to the right of the combo box, modify the camera positioning as required and then save it under the same name as before using the ENTER key.

Saved views are workstation- not operator-specific, thus allowing operators to use views customized by their colleagues.

3.5.2 Live image

In addition to the door control functions, the popup menu displaying entrances and readers in the device states list also contains entries for connecting live images.



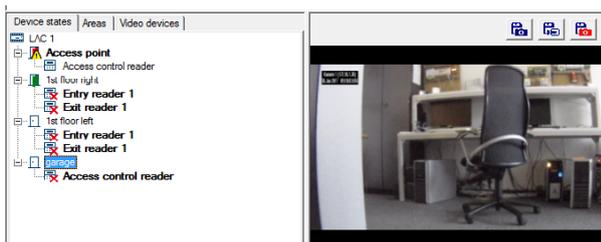
Notice!

These functions are not available in the device states list on the Logviewer.

There is a general entry for every configured camera assigned to this entrance. If the maximum number of cameras has been configured, the popup menu for live image mode appears as follows:

- Identification camera
- Back camera 1
- Back camera 2
- Front camera 1
- Front camera 2

When you select a camera, the live image is fed to the display. If you have not selected a personnel record, the live image is displayed in the dialog field (instead of the time); otherwise, it appears in a smaller format to the right of the device states list.



If you select a personnel record to edit while the large live image is displayed, the live image mode switches to a smaller format.

If the live image function for one of the cameras is active, the popup menu includes the **Video off** entry, which you can use to restore the default state.



Notice!

You can also activate live image mode via the camera list on the **Video devices** tab by selecting the list entry you require.

3.6 Video Management

The video components integrated in the Access Professional Edition access control system can be used as an additional control facility at special entrances for the purpose of comparing live images with images stored in a database, and to check the surrounding area. It is also possible to generate special alarm responses using video recordings and to monitor specific areas, even independently of entrances.

In addition, video components can be accessed and used in Access PE in the following areas.

- Video verification: additional optical controls at entrances
- Alarm management: specially configured alarm messages and entries can be supported by recorded video sequences
- Video displays: playback of current camera images from up to four freely configurable cameras at the same time

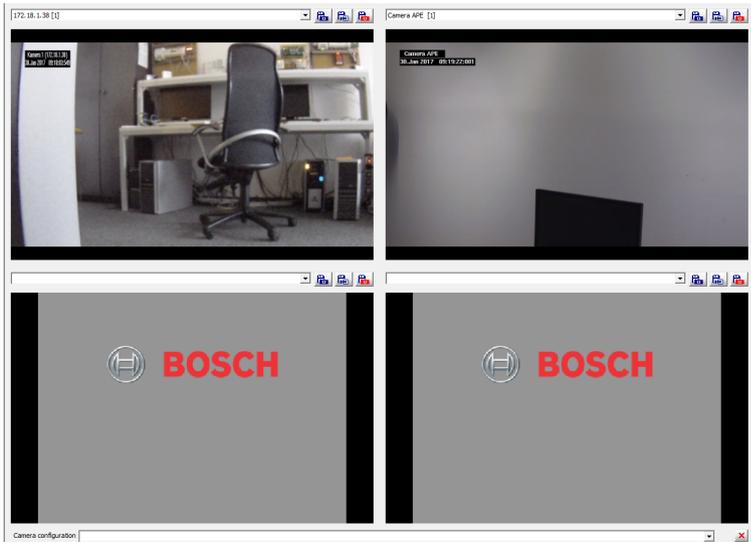
See also

- *Video panel, page 40*
- *Live image, page 42*

3.6.1 Video panel



Press the  button in the Personnel Management toolbar to replace the dialog field with a display showing four video views.



In the video panel it is possible to select up to four cameras from different entrances.

The following functions are available for each display window.

Selection list

You can select any camera loaded into the access control system and replace it at any time.



Stores a still image of the current view as **<device name>_yyyyMMddhhmmssttt.jpg** at C:\BOSCH\Access Professional Edition \PE\Data\Video (default path).



Starts/ends a video recording of the current view and stores it as **<device name>_yyyyMMddhhmmsstttt.vxx** at C:\BOSCH\Access Professional Edition\PE\Data\Video (default path).



(= Point of Interest) Creates a still image of the current view – **POI_** is added to the start of the file name.

A log book message is also created as a marker.

Customizing views for the video display

A particular selection and ordering of cameras can be saved and then recalled by name at a later time. This saves time otherwise spent manually selecting and configuring the same view.

First manually configure the view you want by positioning the cameras in their respective windows as suits you best.

Next, give the view a meaningful name by editing in the lower combo box and save it by pressing ENTER. These views can afterwards be recalled by name from the same combo box.

In this way operators can save different camera views for different purposes, e.g. to monitor incoming personnel in the morning, and outgoing in the evenings. Saved views belong to the workstation and not to the individual operator. They can not be edited as such. To change a view first invoke it from the combo box, delete its name using the



button to the right of the combo box, modify the camera positioning as required and then save it under the same name as before using the ENTER key.

Saved views are workstation- not operator-specific, thus allowing operators to use views customized by their colleagues.

3.6.2 Live image

In addition to the door control functions, the popup menu displaying entrances and readers in the device states list also contains entries for connecting live images.



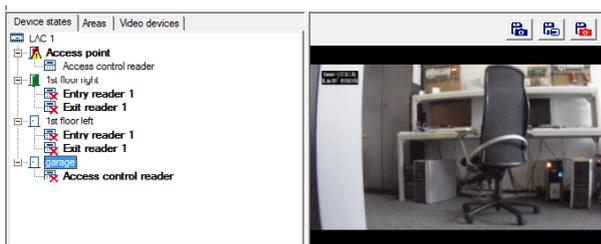
Notice!

These functions are not available in the device states list on the Logviewer.

There is a general entry for every configured camera assigned to this entrance. If the maximum number of cameras has been configured, the popup menu for live image mode appears as follows:

- Identification camera
- Back camera 1
- Back camera 2
- Front camera 1
- Front camera 2

When you select a camera, the live image is fed to the display. If you have not selected a personnel record, the live image is displayed in the dialog field (instead of the time); otherwise, it appears in a smaller format to the right of the device states list.



If you select a personnel record to edit while the large live image is displayed, the live image mode switches to a smaller format.

If the live image function for one of the cameras is active, the popup menu includes the **Video off** entry, which you can use to restore the default state.



Notice!

You can also activate live image mode via the camera list on the **Video devices** tab by selecting the list entry you require.

4 Personnel data

To create a new person open an empty dialog box using the



button or via the menu **Persons > New person**

Notice!

Note, this refers to creating a new personnel record. If instead you wish to edit existing personnel data then double click on a person in the persons list, or select a person and click the



button in the toolbar. The same dialog box will be opened, but containing the data for the selected person.

Personnel data and authorizations

Personnel Data | Access Authorizations | User Rights

Person

Title

Last name

First name

Date of birth

Company

Phone

Valid from until

Personnel group

Take picture

Preview card

Print card

Print card reverse side

Card data

Person has no card assigned

Personnel-No.

1. Card-No. Version

2. Card-No. Version

3. Card-No. Version

Import picture

Delete picture

Acknowledgement

Assign card 1

Assign card 2

Assign card 3

Delete card 1

Delete card 2

Delete card 3

Special messages on the reader

Name on display

On arrival

On leaving

Access control data

Time model

PIN Confirm PIN

Verification

Identification

OK Cancel Help

4.1 Personnel and card data

The dialog Personal data and authorizations contains all relevant personal and card data, as well as special card information. The minimum inputs for the person to be stored in the database are a **name** and a **personnel group**.

The following information can be stored:

Data field/ Input field	Description
Person	
Title	These data appear here in the order Title, First name, Last name. In the persons list the title is not displayed.
Last name	
First name	
Date of birth	The date can be entered in numbers or picked using the spin button (small up/down arrows).
Company	The company or department can be spread over 4 lines. Line feeds can be entered using Ctrl + ENTER. Max. 114 characters.
Telephone	Also appears as information about the person's availability. Max. 30 characters.
Valid from ... to ...	The validity period for access control can be specified here. Empty fields imply unlimited validity.
Personnel group	Input required. One personnel group must be chosen.
Card data	

Data field/ Input field	Description
(Display of card status)	Symbolic display of the current card status.  No card assigned  Card assigned
Personnel-No.	Enter a personnel number of max. 6 figures
1. Card-No.	Enter a card number of max. 6 figures
2. Card-No	All cards get the same access authorizations.
3. Card-No	
Special messages on the reader	
Display name	Display text for capable card readers. Default is First name, Last name. Max. 20 characters
Text on arrival	Customized display texts for arrival and departure can be entered here for TA readers. Prerequisite is that the system parameter Show welcome/leaving message is activated in the Configurator settings. Max. 20 characters.
Text on departure	
Access control data	
Time model	Select an existing duty model. The person is permitted access only during the defined periods.

Data field/ Input field	Description
PIN	Input of PINs for use with keyboard readers. PINs are not permitted to contain sequences (e.g. 1234) or palindromes (e.g. 0110). General settings for PINs are made in the Configurator > Settings dialog.
Verification + Confirmation PIN	This PIN can be generated either <ul style="list-style-type: none">– by the system automatically, or– be entered as a 4 to 8 digit PIN (default = 4) which, as an additional security measure, will be requested after presentation of card at an entrance.

Data field/ Input field	Description
Identification-PIN / ID-PIN	<p>As this PIN needs to be unique system-wide. It can be generated either</p> <ul style="list-style-type: none">– by the system automatically, or– be entered as a 4 to 8 digit PIN (default = 4) which, as an additional security measure, will be requested after presentation of card at an entrance. <p>The ID PIN is displayed in a message dialog before saving.</p>  <p>This Identification-PIN can be typed at keyboard readers instead of presenting a card. As this PIN functions virtually as a card number it also carries with it all authorizations assigned to that card number.</p>

Data field/ Input field	Description
Arming-PIN / IDS-PIN	<p>Input a 4-8 digit PIN (default = 4, the same length as the verification PIN) to arm the alarm system.</p> <p>Whether these fields are displayed or not is determined by the check box separate IDS-PIN (Configurator > Settings).</p> <p>By default the fields for arming/disarming the IDS (intrusion Detection System) are not displayed.</p> <p>If a separate arming-PIN has not been set then a verification PIN may be used to arm the IDS. However if a separate arming PIN has been set then it alone can used - the verification PIN will not then function as an arming PIN.</p>
<p>Note: A fourth variety of PIN, the Door-PIN, can be assigned separately to individual doors. This code must be known to anyone using the door.</p> <p>Door-PINs are set and activated in the configurator on the Entrances page under the function PIN or Card.</p> <p>Important: 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.</p>	
<p>Buttons on the right hand side of the dialog box</p>	
Take picture	<p>These buttons are only visible when Card Personalization (CP) (<i>Create cards, page 60</i>) is installed and running on this workstation.</p>
Preview card	
Print card	

Data field/ Input field	Description
Print card reverse side	
Acknowledgem ent	
Import picture	Pictures in .jpg or .bmp format may be imported. The picture is integrated in the personal data display.
Delete picture	Only activated if a picture has been imported.
Delete card 1	Only activated if a card has been assigned; changes the display of the card status (see above).
Delete card 2	
Delete card 3	
Assign card 1	Assigns a card number to the selected person and changes the display of the card status (see above).
Assign card 2	
Assign card 3	

**Notice!**

The identification and door PIN variants cannot be used for door models with security system arming (TM 10 and 14).

4.2 Assigning and revoking cards

Each cardholder can hold up to three cards, which can be assigned and revoked separately. Depending on the system configuration, card data can be recorded manually or via an enrollment reader, but only one of these methods can be active

at a time: once an enrollment reader has been configured (Tools > Properties) then manual methods can no longer be used in parallel.

Manual data recording supports the use of different card technologies by allowing the operator to change underlying card bit formats. Once an enrollment reader is used however, only cards of the same underlying card technology can be used.

Notice!



In Access PE a cardholder can use multiple credentials in multiple formats and technologies. Each of these however identifies the same individual with the same set of authorizations, blocks, PINs, time models and area-restrictions.

Depending on the **Properties** (*Enrollment Configuration, page 19*) cards can be checked manually or via a reader. Only one of these modes can be active at any one time. As soon as a reader has been configured the card number can no longer be checked manually.

Manual card checking

For manual card checking a card number, with a maximum of six digits in default, must be defined in addition to at least the minimum personnel data of Name and Personnel Group. **Please enter a valid card-no. for the person!**

Clicking **Assign card** initiates a verification of the uniqueness of the card number. **This card is already assigned to the following person: xxx**

The card number is now encoded based on the **default card data** shown in the **Settings** dialog of the Access PE Configurator. A successful assignment is signalled by a dialog box which needs to be confirmed with **OK** before the data are stored.

The screenshot shows a software window titled "Personnel data and authorizations". It has four tabs: "Personnel Data", "Access Authorizations", "User Rights", and "Additional Data". The "Personnel Data" tab is active. The form contains several sections:

- Person:** Title, Last name (Aznavour), First name (Brian), Date of birth, Company, Phone, Valid from, until.
- Personnel group:** Employees (dropdown).
- Card data:** A red circle highlights the "Card assigned" status with a card icon. Below it are three rows for card numbers and versions: "1. Card-No. 106 Vers. 0", "2. Card-No. Vers. 0", and "3. Card-No. Vers. 0".
- Access control data:** Time model, PIN, Confirm PIN, Verification, Identification.
- Special messages on the reader:** Name on (Brian Aznavour), On arrival, On leaving.
- Buttons on the right:** Take picture, Preview card, Print card, Print card reverse side, Acknowledgement, Import picture, Delete picture, Delete card 1, Delete card 2, Delete card 3, Assign card 1, Assign card 2, Assign card 3.
- Bottom status bar:** A green bar with the text "Card successful assigned !" is circled in red.
- Bottom buttons:** OK, Abbrechen, Hilfe.

If **Connect to LAC Service** is activated in **Personnel Management properties** (*Enrollment Configuration, page 19*) then changes or additions to personnel data are transmitted immediately to the LAC service and become valid system-wide.



Notice!

A person must be assigned not only a card number but also the **authorizations** (*Authorizations, page 53*) for all entrances required.

If the check box **Do not show dialog for editing card information** is **not** checked in **Personnel Management properties** then the button **Assign card** invokes the following dialog which provides an opportunity to override the default settings (see Access PE Configurator).

Internal Card Information

Customer code Input hexadecimal 56720

Country code Input hexadecimal 0

Card code Input hexadecimal 106 Version 0

Don't show this dialog again.
Generate card code with predefined data.

Assign card Cancel

Card checking by dialog reader.

A connected dialog reader for checking cards must be configured in **Personnel Management Properties**. Manual checking is thereby automatically deactivated.

In this case all data are read in from the card. Keyed input is therefore unnecessary and will be ignored by the system.

The user is prompted to hold his card over the dialog reader, from which he will receive either permission to enter or an error message.

4.3 Authorizations

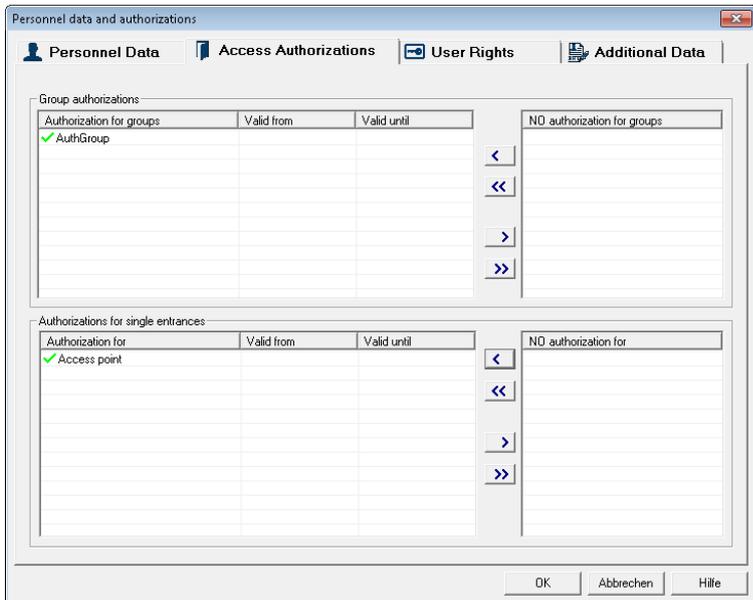
This page is only shown if the user currently logged in has administrator **rights** (*User rights, page 84*) to modify authorizations.

This tab is for the purpose of assigning authorizations to persons in the access control system. If Configurator (dialog **Authorization groups**) has already been used to assign default

authorizations to particular personnel groups, then the person will have received those authorizations by being assigned to that personnel group.



The user's authorizations can however be supplemented by use of this tab.



This dialog contains four list boxes. The right hand boxes list all configured authorization groups (upper list), and all configured individual entrances (lower list). A person's total authorizations consist of all authorization groups and all individual entrances assigned to him in this dialog.

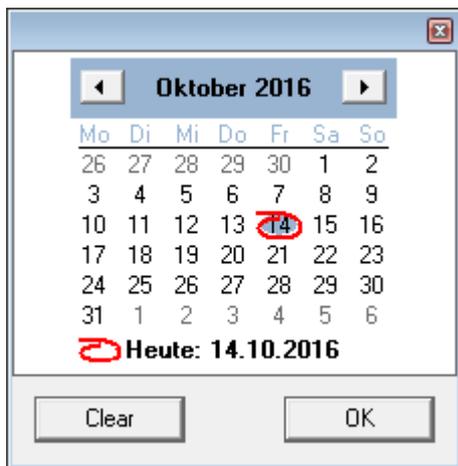
Authorizations (groups or entrances) can be transferred to a person either by double clicking on one in a right hand list box, or selecting one and clicking . The  button transfers

all available authorizations at once. Any combination of group or individual authorizations can be assigned. Conversely, assigned authorizations can be revoked by double clicking or by use of the buttons  and .

If authorization groups contain **time models** (these should be appropriately named), then the group's assigned entrances are only passable by that person during those time models. Please note the special cases in **Application of time models *** XRef ME TO Anwendung_von_Zeitmodellen.xml** in Access PE.

By default authorizations are not limited in time, however it is possible to limit both group and individual authorizations by entering dates in the columns **valid from** and **valid to**. A click in a cell in these columns invokes an in-line editor for entering dates and times: .

Dates can be entered via keyboard or mouse using the spin controls (small arrows) on the right side of the editor. The space bar moves the cursor from day to month to year etc. Furthermore, by right-clicking on an open date field the user can invoke a calendar date picker, for extra speed and comfort.



In this way, when creating a person, authorizations can be assigned which will only come into effect at a later date. Thus it is unnecessary to set a reminder to re-edit a person's authorizations because these authorizations can be set to expire automatically on a certain date. If a **valid from** date occurs later than a **valid to** date, then the authorization is deactivated upon reaching the **valid to** date and reactivated upon reaching the **valid from** date. This feature can be useful, for example, when a person takes vacation.

Changes to authorizations and other personnel data are not saved until confirmed by clicking OK. All changes are then automatically transmitted to the controllers, provided that in Settings (**Tools > Properties**) the option **Connect to LAC Service** is activated. In special cases the data can be transmitted explicitly using the menus **Persons > Transmit selected person to LAC service** or **Persons > Transmit all persons to LAC service**.

4.4 Additional fields

This tab is only visible when at least one of the 10 available additional data fields has been configured in Access PE Configurator.

Up to 10 additional data fields can be configured. These can vary both in number and in field name. The fields can contain values of up to 40 characters.

The fields are displayed in order. If one of the ten fields is skipped then a space is left as a placeholder. If that field is configured later on, then it will replace its placeholder in the ordering.

Personnel data and authorizations

Personnel Data | Access Authorizations | User Rights | Additional Data

Name of birth

Marital status

Phone - private

Phone - private (mobile)

Size

OK Abbrechen Hilfe

Caution!



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. If the use of the additional field contents does not change then the name of the field can be changed at any time.

4.5 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** 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.

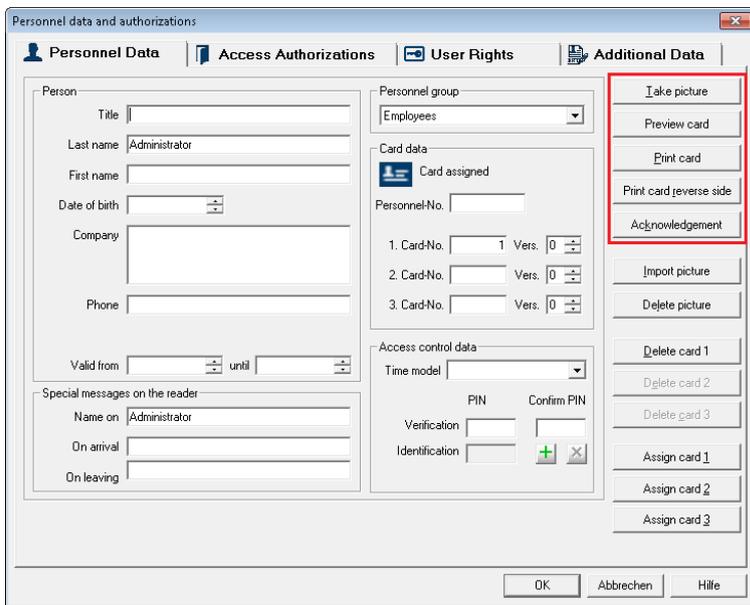
5 Create cards

Access PE is supplied with its own card personalization program. You can install this software on certain computers of your choice. To personalize cards, you will also need the appropriate hardware (camera and printer); we therefore recommend that you only install these components on the computers you will use for personalizing cards.

Please note that even the image import function, for example for displaying images in the personnel dialog, only functions on computers on which the card personalization program has been installed and started.

5.1 Creating cards

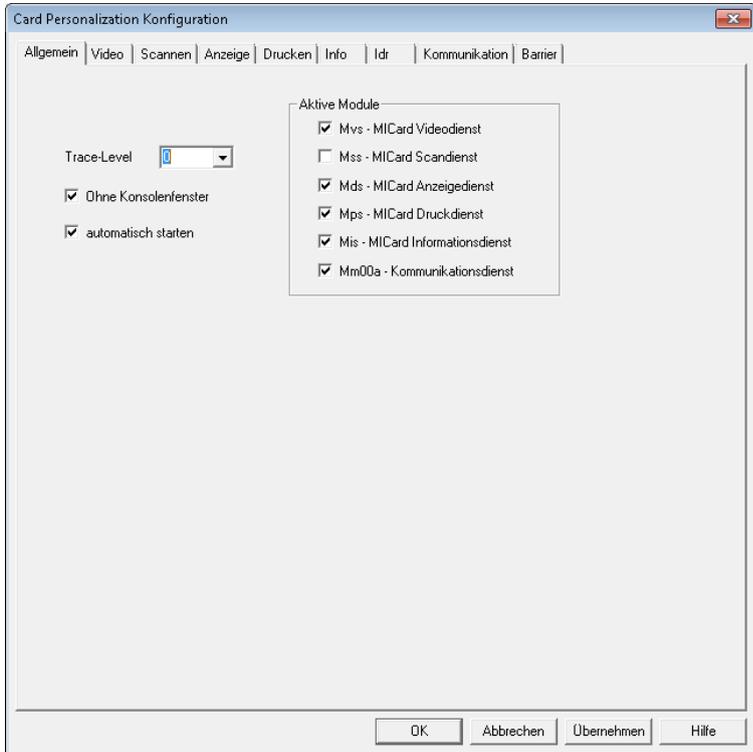
The functions required for creating cards can be executed at all workstations where the Badge Designer program is installed and running. Buttons for this purpose are found on the tab **Personnel data**.



In addition to this the workstation must be connected to the necessary equipment: a **camera** and a **card printer**.

To configure the hardware select the card personalization configurator.

Parametrize a camera or a printer with the inputs on the tab **Video** respectively **Print**. Please refer the Online Help of this tool, too.



The following steps are recommended for the creation of cards:

- **Import or take a photo**
- **Preview card** (optional)
- **Print card/reverse side**
- **Print card receipt** (optional)

5.2 Taking or importing photos

Personnel Photos, which are to be printed on cards or to appear in the personnel data dialog, can be taken with a connected camera or imported from a file, if available.

Importing photos

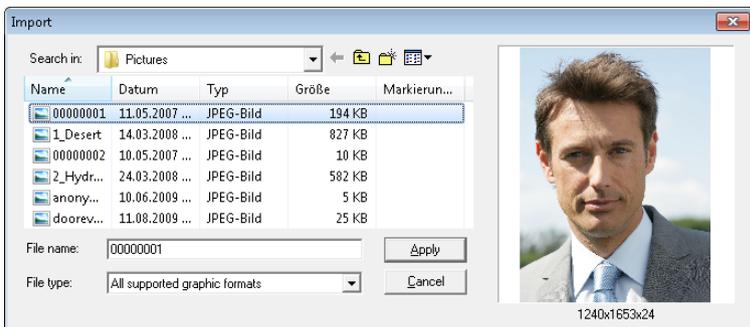
Photos of employees can be imported as files and assigned to personnel data.

Notice!

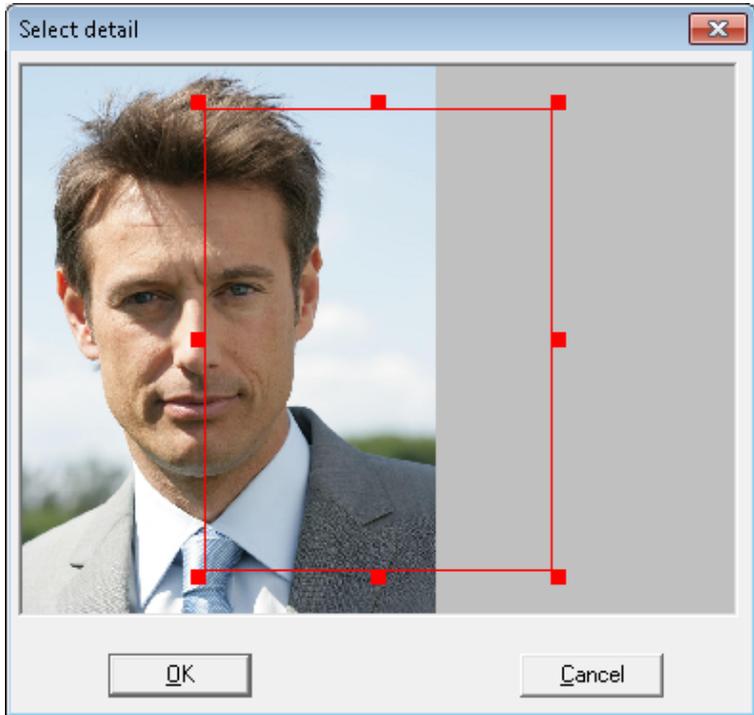


Photo import is also available at workstation where the Card Personalization application is not installed. In this case however photographs can only be imported in original size. The editing features described below are not available.

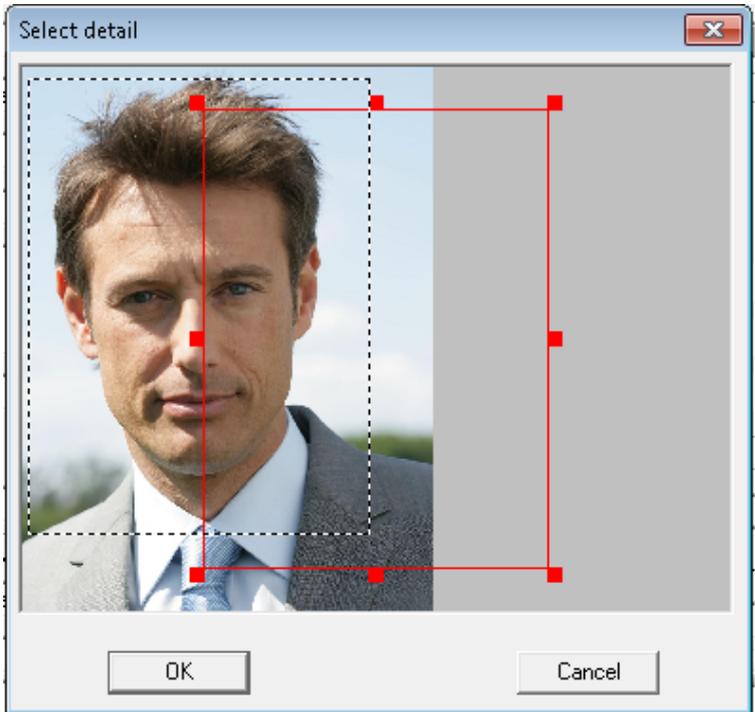
To import a photo from a file click Import picture and pick a file from the file selector dialog. The configuration settings for the Card Personalization program define a default directory for imported files, and this is the first directory opened by the import function. Nevertheless any picture file on the system can be found and selected by the file selector dialog. Once the file has been selected it is shown in the preview window to aid in finding the correct photograph.



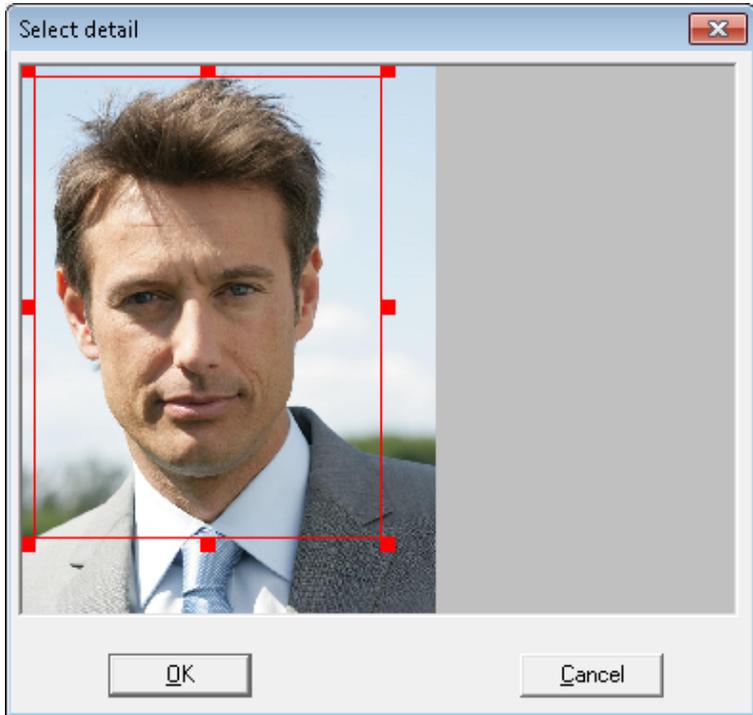
Once a picture has been chosen an editing dialog appears which allows the picture to be cropped and resized. The red frame marks that portion of the photo which will be stored in the system for that person.



The selected portion of the photo can be repositioned in the frame by dragging and dropping with the left mouse button.



The selected portion of the photo can also be enlarged by left-clicking, holding and stretching with the mouse. In this way even small portions of photos can be used for cards, provided the resolution of the photo permits the magnification. By clicking OK the selected portion of the photo is imported.



The frame size will be adapted to the size of the frame in the dialog window and/or the picture frame in the defined card layout, and previewed there immediately after confirming the import.

Taking a photo

The card creation application Card Personalization (CP) must be configured for the camera type which is attached to the workstation. This is done using the CP Configuration dialog. Please consult that application's help facility to find out more about possible settings.

The following screen shots are taken from Video for Windows and will not be the same for all camera types.

Clicking on the button **Take picture** brings up the following dialog:



If necessary the current camera settings can be checked and

modified using the  button.

If the settings and the requirements match then the image can be frozen with the Freeze button.

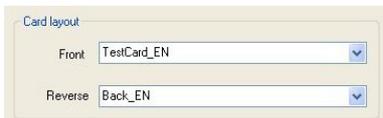
Live image mode can be activated again at any time if the frozen image is unsatisfactory. If the photograph is to be used for card and personnel data then please click Apply.

A further dialog Crop picture is displayed. Using a cropping frame you can select that part of the photograph which is to appear on the card.

Please consult the section on Importing photos above for further details about use of the cropping frame.

5.3 Previewing and printing cards

The buttons Preview card and Print card reverse side are only active if card layouts have been assigned to the respective personnel group in Access PE Configurator (dialog: Personnel Groups).



Preview card

After the picture has been taken it is automatically inserted into the predefined area in the card layout, where it can be previewed before printing. The card is previewed in the following dialog box, which is invoked by the Preview card button.



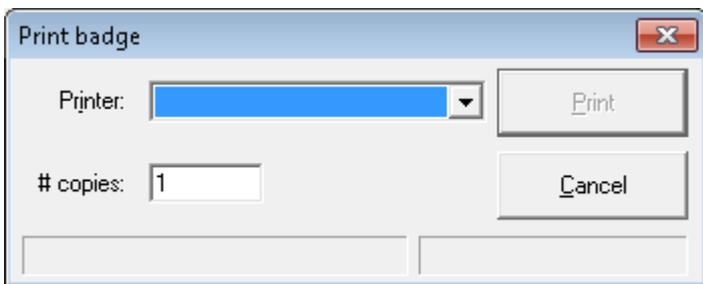
Close the dialog by clicking **OK**.

Print card

If the layout of the card is satisfactory then, in the final step, it can be printed. The Print card button invokes the following dialog which resembles the last except that it offers a print command.



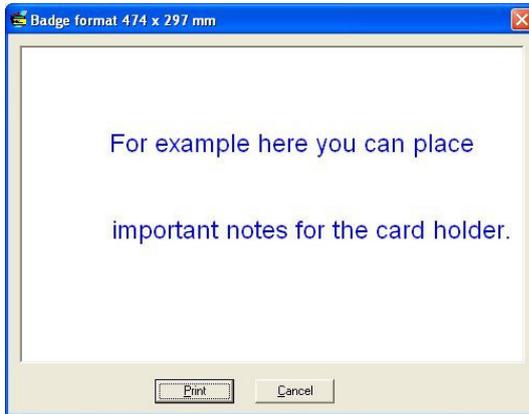
The **Print** button begins the print process by invoking a dialog to choose a printer. If a default printer has been defined in Configurator then printing proceeds immediately.



Print card reverse side

If the reverse side of the card is to be printed then special layouts and contents can be defined for the purpose.
Note: Please ensure that the cards whose fronts have been printed are uppermost in the hopper of the card printer before you give the command to print the reverse side.

Tip: We recommend that the reverse side contain only general and not person-specific data. In this case you can pre-print the reverse sides of a number of cards and hold them in stock, making it faster to create complete cards for individuals as the need arises.



5.4 Printing card receipts

Another feature of the card creation application is the ability to print a standard receipt. The receipt documents the handover of the card and the cardholder can receive information about the data stored on it.

To use this feature a template must be created and stored for the personnel group in Access PE Configurator, dialog:

Personnel Groups.



Date: 06.08.2008

Acknowledgement of identification badge

Last name: Public
First name: John B.
Company:

Reason of issue:

Please check:

- First issue
- Replacement / New issue
- Badge lost
- Badge damaged
- Return of badge (*)
- Return of damaged badge (*)
- Change of name
- Transfer
- Other:



Code of behavior:

Entering the business premises is only permitted while holding a valid badge. The badge must be shown on demand and may not be passed to other persons. Its loss must be immediately reported to the responsible issue office.

The badge has to be returned at quitting.

Charging of cost in case of loss or damage:

Check, if valid:

6 Reports

You can use the list functions in Access PE to collate the database contents in a specific way and organize them into a clear format for printing.

To filter the results so that only the data the user needs to see is shown, you can use pre-prepared layouts, which provide specific information regarding a certain aspect of access control (for example, who has what authorizations for which doors).

6.1 Reports



The  button changes the view from the personnel data view to a dialog for creating and viewing reports relevant to access control.

Reports

 Layout

Filter

Last name First name
Personnel no. Card no.
Card no. from Card no. to
Dep./Company Personnel group

Filter locations

Areas

Name
-- outside --
-- unknown --
inside

Filter additional personnel data

Field
Filter

Filter authorizations

Authorizations

Name	Type
Authorization	(G)
Access point	(E)

Valid from
Valid until

Filter devices

Type

Type
Lac
Entrance
Reader

Name

A number of reports layouts and content filters are available:

Layout	Available Filters	Description
Personnel data	Last name First name Personnel no. Card no. Card no. from ... to Dept./Company Personnel Group	Displays personnel data. Data can be filtered according to any or all of the available filters. Multiple filters function restrictively (logical AND). For example, it is possible to search for all persons whose name begins with A and whose card number is in the range 900 to 999. The * character can be used as a wildcard to stand for any or no characters.
Blocked Persons	Last name First name Personnel no.. Card no. Card no. from ... to Dept./Company Personnel Group	Displays data of personnel whose card status is anything other than valid (e.g explicitly blocked, 3x wrong PIN input, selected for random screening) in the main personnel data screen. Data can be filtered according to any or all of the available filters. Multiple filters function restrictively (logical AND). For example, it is possible to search for all persons whose name begins with A and whose card number is in the range 900 to 999.

Layout	Available Filters	Description
		<p>The * character can be used as a wildcard to stand for any or no characters.</p>
Persons - Authorizations	Last name First name Personnel no. Card no. Card no. from ... to Dept./Company Personnel Group Authorizations	<p>Report listing persons and their assigned authorizations. Group authorizations are marked with (G) and individual authorizations with (E). Duration of validity is also shown.</p> <p>It is possible to filter based on one or multiple authorizations. Each authorization can be selected or unselected with a single click.</p>
Persons - Areas	Last name First name Personnel no. Card no. Card no. from ... to Dept./Company Personnel Group Locations	<p>Based on the configured areas in the system both the names and the number of persons at the specified location are listed.</p> <p>It is possible to filter based on one or multiple areas. Each area can be selected or unselected with a single click.</p>

Layout	Available Filters	Description
Authorizations - Persons	Authorizations	<p>Report listing authorizations and their assigned persons. Group authorizations are marked with (G) and individual authorizations with (E). Duration of validity is also shown.</p> <p>It is possible to filter based on one or multiple authorizations. Each authorization can be selected or unselected with a single click.</p>
Devices	Device type Device description	<p>Report listing device types (controllers, entrances, readers).</p> <p>It is possible to filter based on one or multiple device types. Each device type can be selected or unselected with a single click.</p> <p>Devices can be filtered by text matches on their descriptions. E.g. all devices whose descriptions start with A.</p> <p>The * character can be used in the device description as a wildcard to stand for any or no characters.</p>

Layout	Available Filters	Description
Users	Last name First name Personnel no. Card no. Card no. from ... to Dept./Company Personnel Group	Report listing persons who are also users of the system and the user rights assigned to them Data can be filtered according to any or all of the available filters. Multiple filters function restrictively (logical AND). For example, it is possible to search for all persons whose name begins with A and whose card number is in the range 900 to 999. The * character can be used as a wildcard to stand for any or no characters.
Persons - Doors	Last name First name Personnel no. Card no. Card no. from ... to Dept./Company Personnel Group Authorizations	Report listing persons and their assigned doors. Group authorizations are marked with (G) and individual authorizations with (E) . Duration of validity is also shown. Persons can be filtered by text matches, e.g. all persons whose names start with A . The * character can be used in the device description as a wildcard to stand for any or no characters.

6.2 Reports: Page view

It is possible to set filters to limit the report contents to a subset. If no filter is set then all data are reported. The **Search** button triggers the collection of data and their display in a preview window.



Notice!

When changing filter criteria it is advisable to make use of the **Clear form** button to avoid unintentional filtering and hence misleading reports.

Open log files can be saved or printed. The menu item **File >**



Print or the button opens a preview.

Access Control System - Bosch Access Professional Edition

4 / 8 100%

Access Control System - Bosch Access Professional Edition

EventLog report

Date	LAC/PC	Reader/Login	Location / program	Last name, first name	Card no.	Company	Message
26.05.2009 14:19:31	LAC-1	Processor 4	Board 0				online (ready)
26.05.2009 14:19:31	LAC-1						Program downl...
26.05.2009 14:19:32	LAC-1		Main entrance - north				Door in normal...
26.05.2009 14:19:32	LAC-1		Main entrance - south				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-3				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-4				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-5				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-6				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-7				Door in normal...
26.05.2009 14:19:32	LAC-1		Entrance-8				Door in normal...
26.05.2009 14:19:40	LAC-1						Personnel data
26.05.2009 14:19:41	LAC-1						Program downl...
26.05.2009 14:38:18		LACSP					No video verifi...
26.05.2009 14:38:21		LACSP					No video verifi...
26.05.2009 14:38:23		LACSP					No video verifi...



Notice!

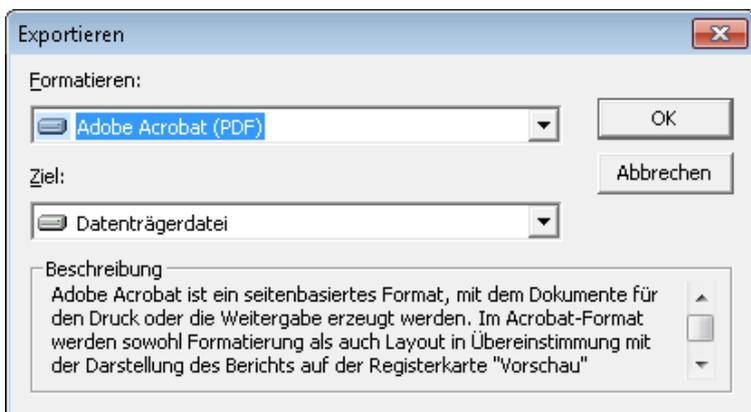
All opened log files will be printed.
Close all files which should not be printed or reduce the selection to the important messages.

The **reports page view** offers a number of tools for modifying and manipulating the display:

Button	Meaning	Description
	Export	The list can be exported to a file for further processing. The following formats are available: Acrobat Portable Document Format (PDF) Comma Separated Values (CSV)
	Print	Prints the report via a print dialog which allows the setting of a default printer.
	Select page	The arrow buttons turn to the first, previous, next or last pages of the report. The control also shows the current and the total number of pages in the report.
	No. of pages	Prompts the current page and the number of all pages.
	Zoom	The standard scale of the view (100%) can be changed as desired.

Exporting lists

Press the  button to open a dialog for defining the export criteria.



The **Format** selection list field offers the output formats .pdf (for forwarding and archiving specific search results) and .csv (for further processing data).

When exporting data to a csv file, it can be processed to some extent on the way.



As well as entering the **Delimiter** and the export **Mode**, you can also exclude or isolate **Report and Page sections** (column headers and page details) and **Group sections** (selected data) from the export.

You can select one of the following options as the **Destination**.

- **Application** – opens the file with the appropriate application. This application must also be installed on the computer. pdf files are opened with Adobe Acrobat Reader and csv files are opened with MS Excel.
- **Disk file** (default) – opens an Explorer dialog for selecting the directory you require. A name for saving the file is suggested.
- **Exchange folder** – the file can be sent directly to an MS Outlook recipient.
- **Lotus Domino Mail** – the file can be sent directly to a Lotus Mail recipient.

7 Local recordings

Recording still images and videos

The video sequences displayed via the access control dialogs are taken from the video recording devices to which the configured surveillance cameras are connected. Depending on the storage capacity of the device, the oldest recordings will be deleted as the newest recordings overwrite them (circular buffer).

To save certain sections, you can save local copies of individual images or videos. If you use the default installation path, images and videos are stored at C:\BOSCH\Access Professional Edition\PE\Data\Video.

Press the  button to store a still image in jpg format as **<device name>_yyyyMMddhhmmssttt.jpg**

[y= year, M= month, d= day, h= hour, m= minute, s= second, t= thousandth of second].

Press the  button to start recording the sequence that is currently running and press it again to end the sequence. This local copy of the video recording is named in the same way as the images and stored in **.vxx** or **.mpeg** format. The **.vxx** format cannot be viewed as video with standard market applications. To view these local copies, use the **Bosch Video Player** supplied.

Press the  button to store a still image of the current view of a Point of Interest (POI). **_POI** is added to the start of the file name: **_POI <device name>_yyyyMMddhhmmssttt.jpg**.

[y= year, M= month, d= day, h= hour, m= minute, s= second, t= thousandth of second].

A log book message is also created as a marker.

Bosch Video Player

Whilst still images can be opened with virtually any image viewer program or an Internet browser, the video recordings are in a special format and require **Bosch Video Player**.



Notice!

You can use any player to display video sequences that have been saved in .mpeg format.

The dialog has been deliberately kept simple and only has two buttons next to the video display field, namely **open file** and **start/stop**.

Press **open file** to browse the default video recording storage location (C:\) for the files you require.

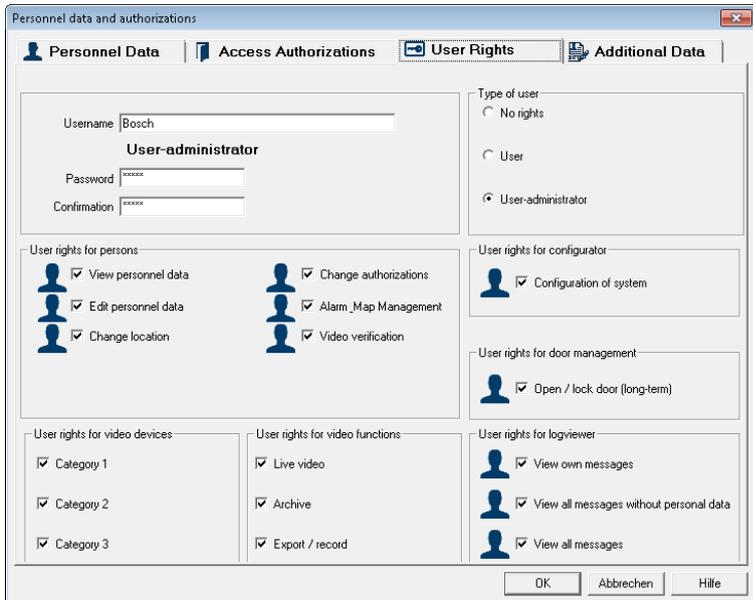
When you have selected the video file, the path is displayed in the Video Player. You can now display the selected file at any time by pressing **start**. While the video is playing, the start button changes to **stop** to allow you to interrupt the playback.

8 User rights

The rights for users of Access PE applications (as well as users of the Configurator and the Logviewer) are assigned in Personnel Management on a special personnel data tab (= User Rights).

8.1 User rights

This tab is only visible if the user currently logged in has administrator rights. Only **administrators** can set and modify their own rights and those of others.



If a person is to receive user rights for Access PE applications, then these must be explicitly assigned. By default all persons are configured **without** user rights.

User rights can be assigned by entering a user name and a password. The person's surname is suggested by default as the user name, but this is arbitrary. The password can be max. 16 characters long, is case sensitive and may contain any special characters.

Notice!



It is highly recommended that you create a separate user for each person who is to use the system. Do not create a generic user under whose name different persons will work. All data entries, modifications etc. are logged under the name of the user who carried them out, but this is only worthwhile if each user has his/her own password and **changes user settings** (*User handover and workstation security, page 89*) as necessary when sharing the workstation with another person.

The default installation contains one predefined administrator. Hence when these predefined users are logged on it is possible to create and modify any other kind of user or administrator. Administrators differ from normal users only in as far as they are able to administrate user rights. There is no difference between the user types as far as the availability of applications or access to data and log files is concerned. Each of the users can be configured with restricted or unrestricted data access. If one of the administrator options is chosen then the various groups of user rights for Access PE applications become active and can be assigned individually. In detail, the assignable user rights are the following:

Application	User right	Description
Personnel data	View personnel data	Only the dialog box with personnel data can be invoked. Locations of persons are not displayed. Modifications are not allowed.
	Edit personnel data	Personnel data can be viewed and modified. Locations of persons are not displayed.
	Change location	Can only be used in conjunction with one of the above options. If View personnel data is active then locations can be displayed only. If Edit personnel data is active then locations can be modified.
	Change authorizations	The tab Access authorizations only becomes active when this box is checked.
Configurator	Configuration of system	Activates full user rights for Configurator.
Door management	Open /lock door (long-term)	Door management is activated for the menu of the same name, and via the context menu in the device status list (in Personnel management and Log viewer).
Log viewer	View own message	Filters out all log messages except those pertaining to the user himself.

Appli- cation	User right	Description
	View all messages without personal data	Shows all log messages but masks personal data.
	View all messages	Shows all log messages uncensored.

Active user rights are marked with a tick in the check box and the  symbol next to it. The following picture shows the activation of all rights. All boxes can be checked without fear of rights conflicts, because the more comprehensive set of rights will take precedence.

8.2 Setting user access rights

The system is delivered with a pre configured User-Administrator rights.

A user with the user name and password bosch is provided by default.

Only administrators are allowed to set up other users.

Warning!



This user and his password is part of the standard delivery and not customized for each purchaser of the software. Therefore it is urgently recommended, before entering production usage, that you first use them to set up your own accounts with administrator privileges, and then delete or modify the original.

Set up further users as follows:

1. Start Access PE Personnel Management using the desktop



icon and log in with the pre-configured User-Administrator account.

2. Open the dialog for adding personnel data using the button



or the menu **Persons > New Person**

3. Add a new user by specifying at least the name and personnel group
4. Click on the User Rights tab and
 - change the **user name** if necessary
 - assign a **password**.
 - define the type of the user (**User** or **User-Administrator**).
 - assign to this user the **rights** to modify data.
 - Confirm your entries and close the dialog box by clicking **OK**.



5. Log out of Personnel Management by clicking  or the menu **Extras > Logon** and confirming the safety check by answering **Yes**.



6. Use the button  or the menu again to log on using the credentials of the user you have just created.

8.3 User handover and workstation security

User handover

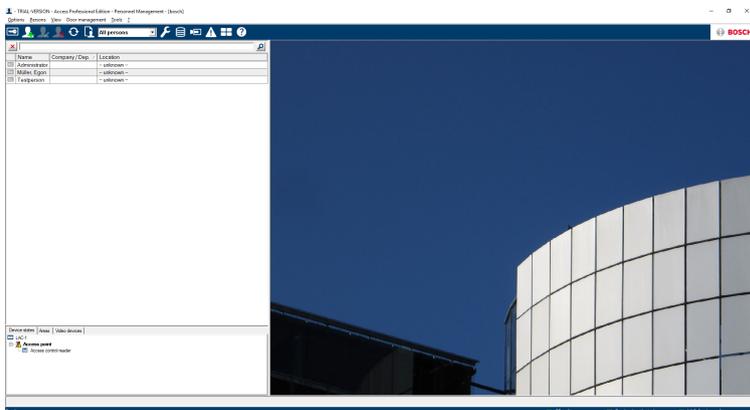
If one user relinquishes control to another at the same workstation then the handover should be made explicitly within the system. This handover can be performed with a running system - there is no need to restart Access PE.

First the current user must log out. To do this s/he clicks the



button in the tool bar. A safety check follows: **Do you want to end your work with user rights?**

After confirming the system switches back to the default view.





The new user **logs in** again using the  button.

Workstation security

In the case of temporarily unoccupied workstations in publicly accessible places it is crucial to protect personal data from unauthorized access. Several measures are available for this purpose:

- In general neither **Configurator** nor **Log Viewer** should be installed on such workstations.
- Log out of **Personnel Management** when not in use, using



the  button with safety check as described above.

The personnel list remains visible but personal data can no longer be accessed.

- **Close the application** using **File > Exit**, or the Windows **x**-button in the title bar. The application will need to be restarted to view the personnel list.
- **Lock the computer** using the standard Windows function: Press **Ctrl + Alt + Del** and choose **Lock Computer** from the system functions offered there. As this is the default function **Lock Computer** can usually be quickly achieved by simply pressing RETURN. Only the current user or a Windows system administrator can now unlock the system.

9 UL 294 Requirements

Features not evaluated by UL:

- The Video Verification System
- Map Viewer and Alarm Management with Map and Video Verification
- Video Player
- Badge Designer
- The Delta 1200 Series
- Rosslare ARD-1200EM Series
- LAC Controllers
- LACi Controllers
- APC-AMC2-4R4CF Controllers
 - BG 900 reader interface protocol
 - L-BUS reader interface protocol
- Security System IDS - Arming/Disarming
- Elevator Use
- Texts
- Logbook
- Personnel Management
- Create Cards
- Reports
- User rights
- Burglar Alarm Use

Features evaluated by UL:

- 26-bit Wiegand format readers
- AMC2 Controllers:
 - APC-AMC2-4WCF
 - API-AMC2-4WE
 - API-AMC2-8IOE
 - API-AMC2-16IOE
- APE-SW as supplementary monitoring equipment

The following Bosch model card readers were evaluated by UL for compatibility with the Bosch's APE-SW software system:

- LECTUS secure 1000 WI

- LECTUS secure 4000 WI
- LECTUS secure 5000 WI

Bosch Access Systems GmbH

Charlottenburger Allee 50

52068 Aachen

Germany

www.boschsecurity.com

© Bosch Access Systems GmbH, 2017