# Access Professional Edition

Video Integration

**BOSCH**

# 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. 512 readers
–    Max. 3 I/O extension boards (AMC2 8I-8O-EXT, AMC2 16I-16O-EXT or AMC2 16I-EXT) per Controller
–    The following restrictions apply to each controller type:

| Controller<br><br>**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. 256 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)
– The OLS functionality is only given with card No.1.

**Notice!**
USB devices which are connected at a remote desktop as e.g. enrollment readers are not supported.

## 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.
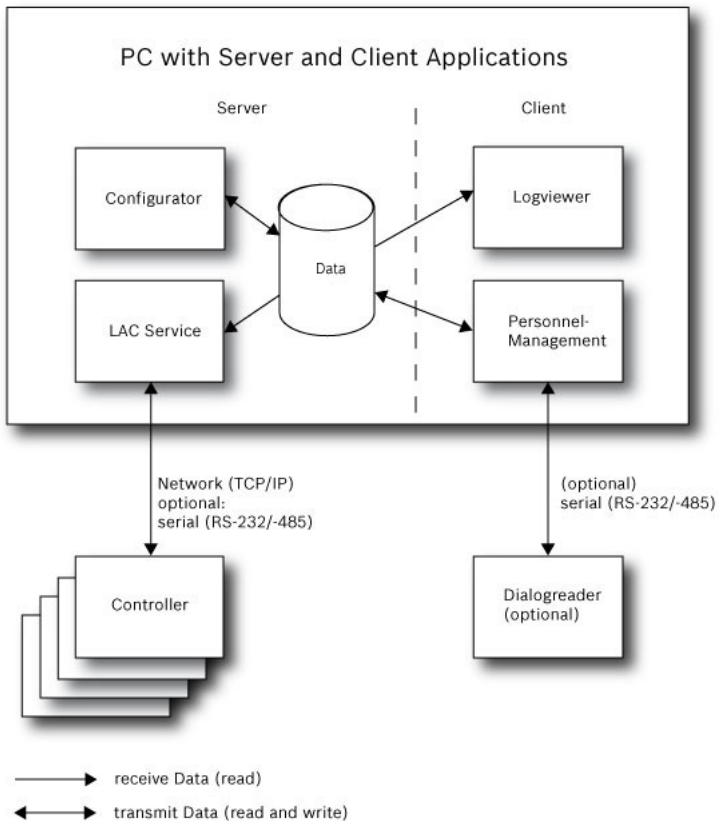


**Figure 1.1: System Overview – Single Computer Configuration**

## 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.

**Notice!**

After an **Unistall for Update** check if all files have been removed from the folder .. :\BOSCH\Access Professional Edition with the exception of the folder **SaveData**.
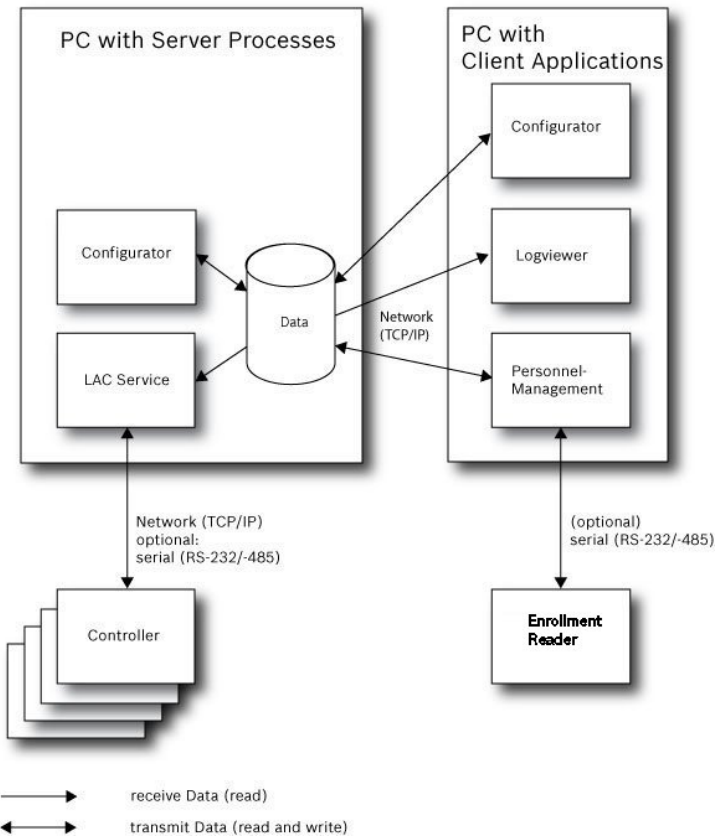
**Figure 1.2: System overview – Distributed System**

## 1.4 System Prerequisites

The installation of Access PE requires:

**Operating Systems (one of)**:

– Windows 10 X64 professional
– Windows 2008 R2
– Windows 2008 Server
– Windows 7

> **Notice!**
>
> Microsoft Windows XP of all versions is not supported by the
> Access Professional Edition from version 3.1 onwards.

### 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

## 1.5 Single-Board Computer

It is possible to run the Access Professional Edition (APE) on a **Single-Board Bomputer (SBC)**.

Basically the capacity of an **SBC** as e.g. the Intel Compute Stick STK1AW32SC or other low-end hardware may **not correspond with the system prerequisites** of the Access Professional Edition (see chapter 1.4).

**Notice!**

An SBC can only be used if LAN or WIFI and the connected hardware are permanently available.

An SBC should be configured only with a reduced feature set as specified with the **Base License** (up to 16 readers).

Due to the low hardware performance a wireless connected SBC should **not** be used with the **Alarm Management** and **Video Management**, as the network stability is critical with these features.

The APE was tested on the following device which can be used as a reference for minimum system prerequisites for operating a Base License:

**Intel Compute Stick STK1AW32SC**

| Product Name | Intel BOXSTCK1A32WFCR |
|---|---|
| Dimension | 147 x 89 x 0.7 mm |
| Processor brand | Intel Atom x5-Z8-300, 4x1.44 GHz |
| RAM size | 2 GB |
| Memory Technology | DDR3L |
| Computer Memory Type | DDR3 SDRAM |
| Hard Drive Size | 32 GB |

| Product Name | Intel BOXSTCK1A32WFCR |
|---|---|
| Voltage | 1.35 V |
| Wattage | 4 W |
| Power Source | USB |
| Operation System | Windows 10 |

**Windows Operating System preconditions**

When working with a low-end hardware as e.g. an SBC, we recommend the following hardware- and operating system-specific settings and preconditions in order to ensure seamless operation of the APE software:

– Use fixed IP addresses.
– Disable all power saving options.
    – Select a high performance power plan.
    – Disable power savings within the USB settings.
– Disable Hibernate functions.
– Disable automatic Windows operating system updates.
– Apply a USB Ethernet Adapter in case the WiFi connection is unstable.
– Ensure that the screen resolution matches the SBC hardware requirements. For the exemplarily tested device the recommended resolution is 1920x1080.
– Ensure that sufficient memory is available. We recommend a free memory of 5GB for installing and operating the APE software. Use an external hard disk or apply a microSD to the SBC in case internal memory is not sufficient.
– Create Windows recovery CDs and save entry points on a regular basis.

> **i** **Notice!**
> When using a Single Board Computer (SBC) it may not be possible to create a recovery CD or to use entry points.

# 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. 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 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.
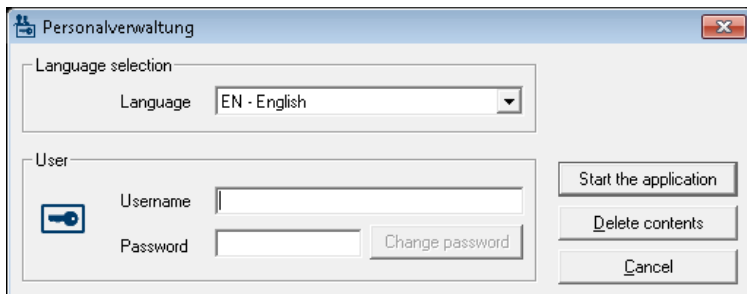
The upper drop-down list can be used to select the desired
interaction **language**. The default is that language which was
used to install the application. If there is a change of user
without restarting the application then the previous language is
retained. For this reason it is possible for a dialog 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.
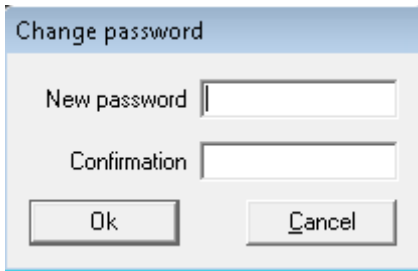


The button **Start the application** checks the user's privileges
and, based on these, starts the application. If the system is
unable to authenticate the login then the following error
message appears: **: Wrong username or password!**

**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] 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] 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] 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. |
| 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). |
| 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. |

| Function | Icon/ Shortcut | Description |
|---|---|---|
| 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. |
| 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. |

| Function | Icon/ Shortcut | Description |
|---|---|---|
| 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. |
| 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 | Description |
|---|---|---|
| Country Code | 00 | Some card data are appended to the manually entered card number. |
| Customer Code | 056720 | |
| 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 |
| Read-Timeout on serial connected LAC in ms | 500 | Possible values for read-timeout: 1 to 3000 |
| Create TA data at | 00:01 | Specification of the time at which the Time & Attendance data file should be created. |

| Parameter | Default | Description |
|-----------|---------|-------------|
| Export personnel and TA data | deactivated | When activated this option causes time & attendance data to written continuously to the export file.<br>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:<br>C:\Program Files\Bosch\Access Professional Edition\PE\Data\Export<br>Under the name **TA_<Current date YYYYMMDD>.dat** | | |
| 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.<br>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.<br>Does not apply to Wiegand readers. |

| Parameter | Default | Description |
|---|---|---|
| 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 |
| 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. |
| Number 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 |

| Parameter | Default | Description |
|---|---|---|
| Logbook parameter | 366 | Number logfiles per day Possible values: 180 to 9999. |
| 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:
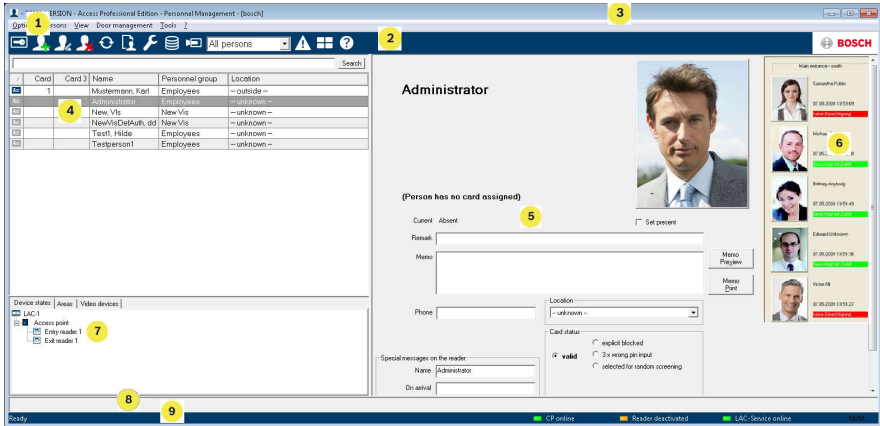
1 = **Menu bar** — contains dialog functions displayed
according to the menu order.

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,
page 70*.

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 |
| Exit | | Exits the **Access PE Personnel Management** application |
| Menu **Persons** | | |
| New person |  | Opens a blank personnel and card data dialog |

| Function | Icon | Description |
|---|---|---|
| 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. |
| | List control | Restricts the persons shown to those of the selected group. |
| Menu **View** | | |
| Symbol bar | | Toggles display of the tool bar. Default = on. |

| Function | Icon | Description |
|----------|------|-------------|
| 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 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. |

| Function | Icon | Description |
|---|---|---|
| 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 | BOSCH | 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. |

# 2.7    Layout of the main dialog
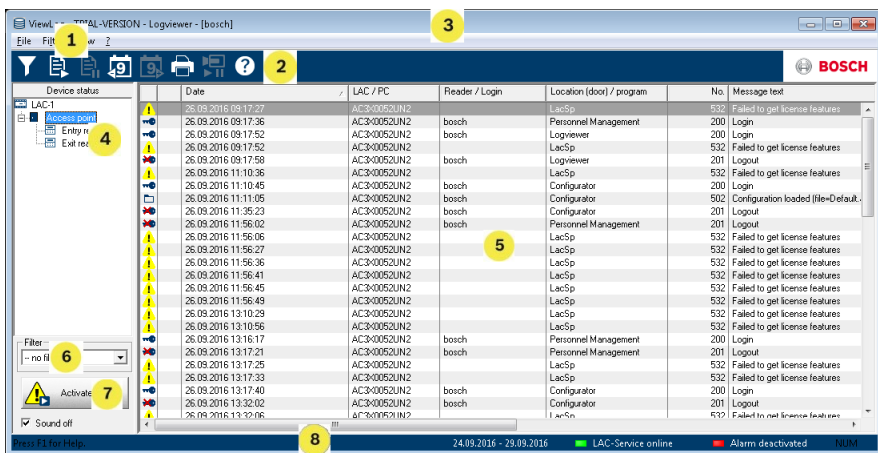


1 =    **Menu bar** - Contains all dialog functions arranged in menus.

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. |
|       | 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. |

| Menu | Function | Icon button | Description |
|------|----------|-------------|-------------|
| | 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 | | | |
| | | | |
| | | | |
| ? (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 |

**Notice!**

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

– **Chip card system**

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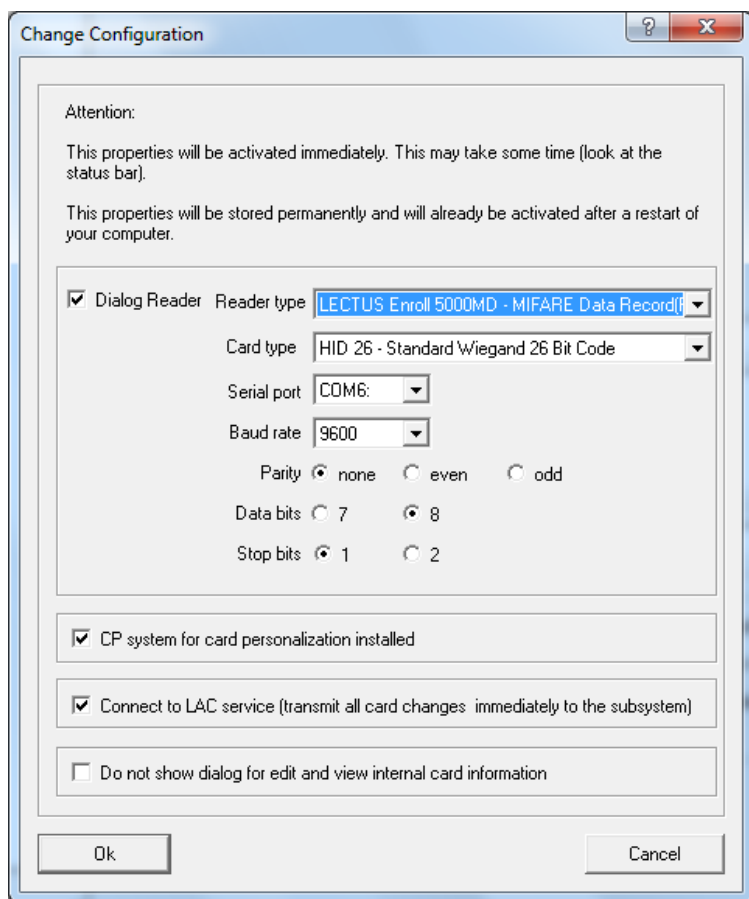


– If the system has been installed with the optional **Card Personalization** (CP) module then the corresponding check box is selected in settings. Unchecking this box blocks all functions for card design/creation.
– In addition the automatic transfer of personnel data via **Connection to the LAC Server** 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 **Configuratior** and select a **Local Access Controller (LAC)** (e.g. AMC2...)
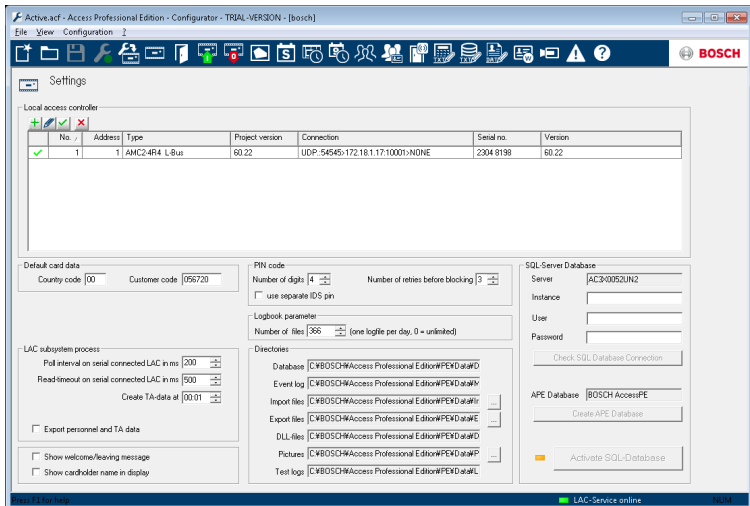


Click the **Entrances** symbol and add a new Entrance reader:
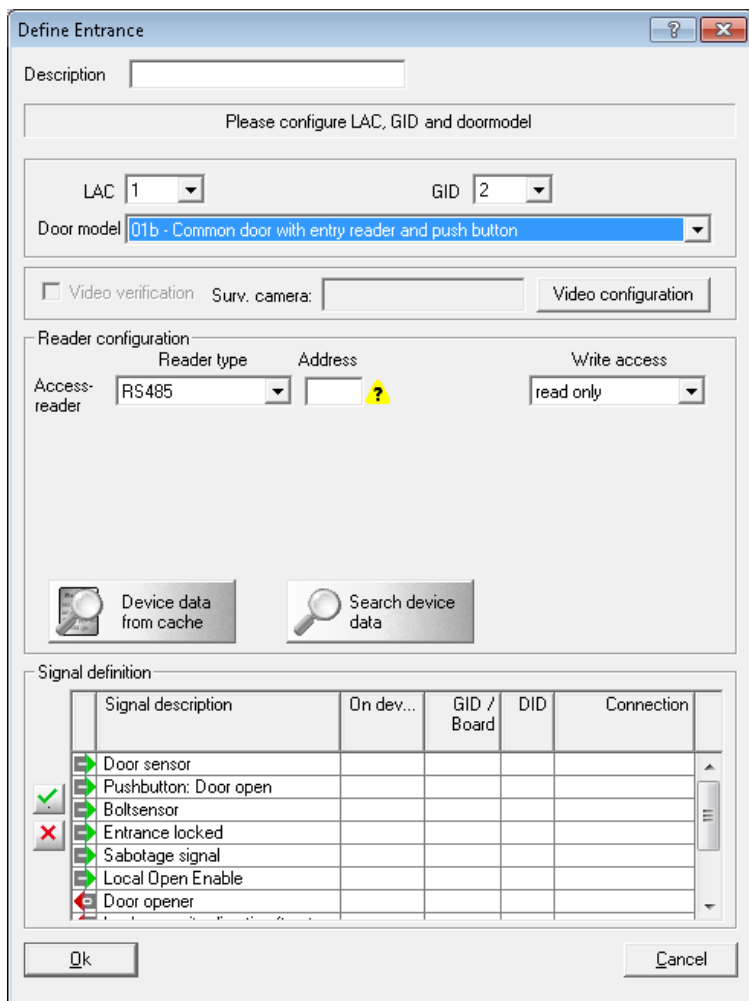
The dialog window **Define Entrance** opens:
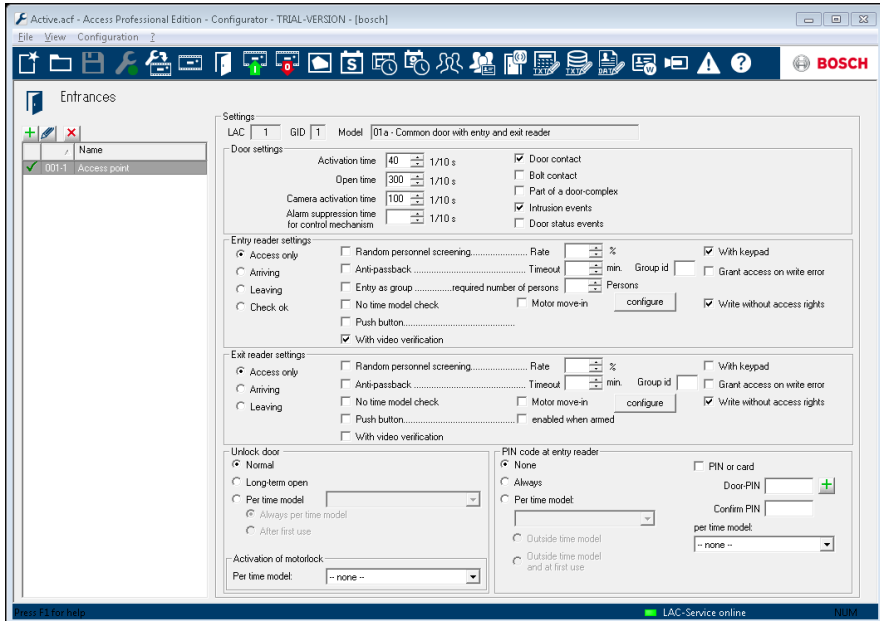
In this dialog:
– Enter a Description (e.g. Enrollment Reader AMC)
– Select a LAC and a group ID (GID)
– Select a reader type (e.g. Wiegand)
– Select a number between 1 and 8 as Access Reader
  Address
Click OK to conform the enrollment configuration.

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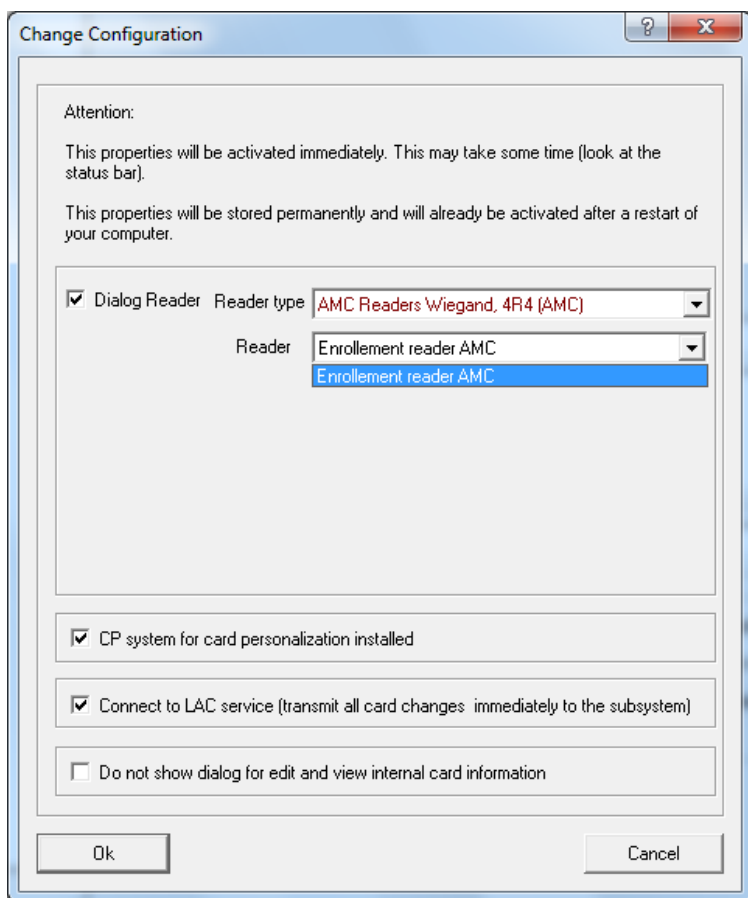
Select an available enrollment reader to activate the enrollment process.
Confirm that your enrollment reader is online.
If you don't get an immediate response, restart the Personnel Management dialog.

## 2.10 SQL Server Support

All data which are written into the event logfile, can also be stored in an SQL database. As a reference we suggest the Microsoft® SQLServer® 2014 Express, SP 1x 64 installed on Windows 10 x64 Pro.

An SQL server connection can be configured in the lower section on the right side of the **Settings** screen.

For more details refer to the installation manual.

> **Notice!**
> Make sure to install the SQL database on the same physical or virtual machine as the APE server.
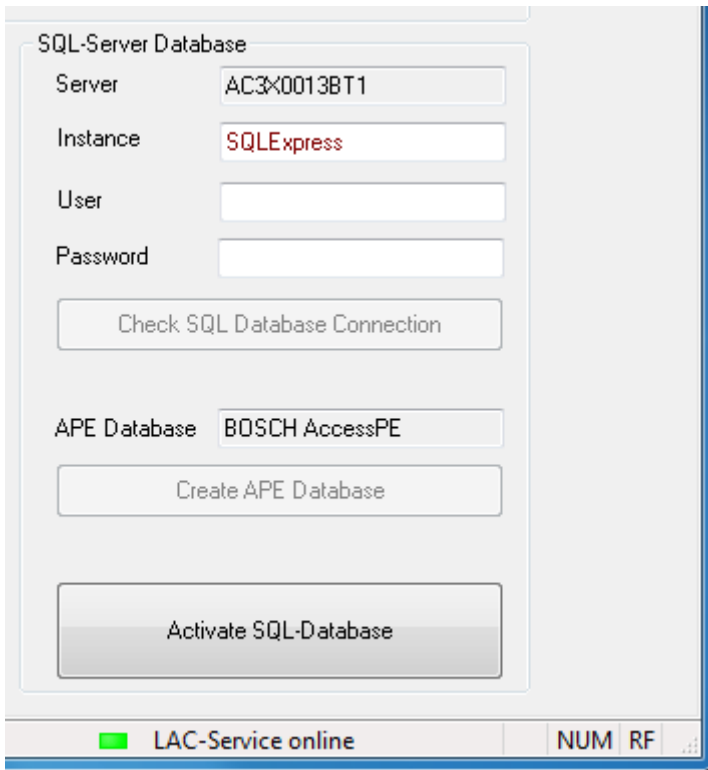
> **Notice!**
> When using the Configurator to configure the SQL database, the configurator must be started on the APE server PC.
> The Configurator must not be started on a client in this case.
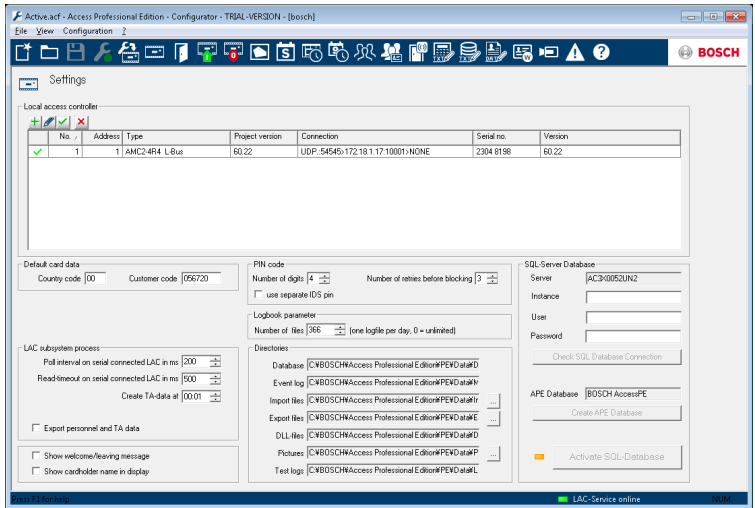
– Enter the instance ID of the database in the entry field
   **Instance**.
– If credentials are required, enter **User** and **Password.**
– Click the button Check **SQL Database Connection**.
– If no APE database server exists so far, click **Create APE
   Database**.

**Check SQL Database Connection**



Edit the name of a new valid instance ID. This causes that a new APE database is created in the specified instance.

If an APE Database exists already or after you have created one, click **Activate SQL Database**.

The system does not import existing logbook data if upgraded to an APE release with SQL database support.

If the limit of 100,000 messages is reached, the system will stop buffering events. Once the SQL service is accessible again the buffered messages are added to the SQL database. The message buffer is not included in the APE system backup.

**Notice!**
The user is responsible to maintain the database such as to erase old entries, keep the SQL installation updated etc.

**Notice!**
It is possible to enable or disable the SQL database service.
If the service is disabled, a Windows message box will warn the user.

## 2.11 Installation of SQL Database

Download the **Microsoft® SQL Server® 2014 Express Edition SP1** from the Microsoft homepage. After the start of the application the **SQL Server Installation Center** is displayed. Select **Installation**.



– Select **New SQL Server**.

Select **License Terms**.
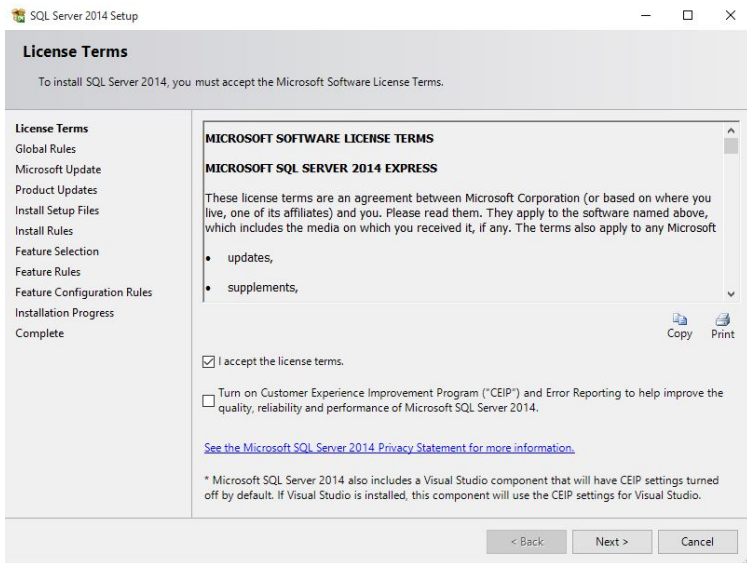
–     Accept the license terms and click **Next >** to proceed.

Select **Microsoft Update**.
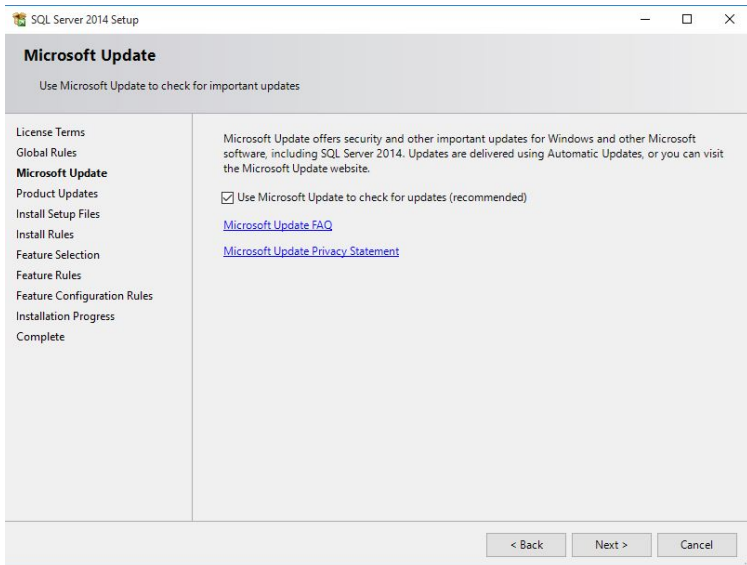
– Select **Use Microsoft Update to check for updates** and click **Next >** to proceed.

Select **Feature Selection**.
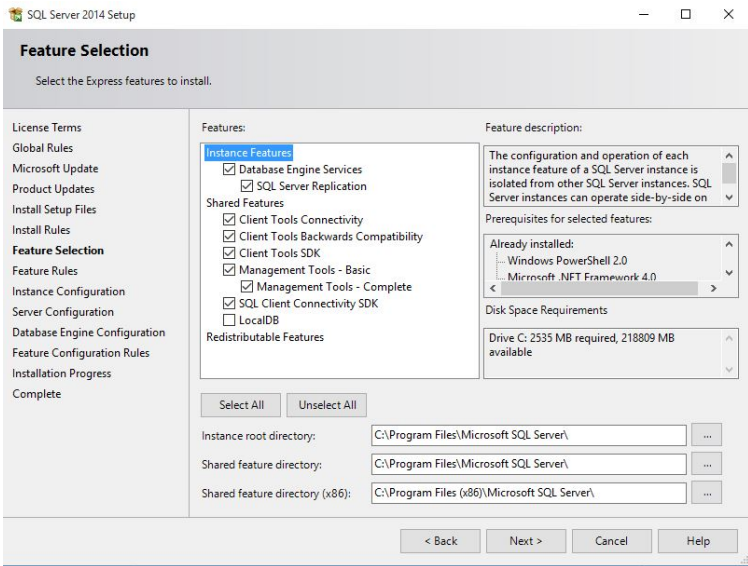


– Select the required **Features** from the list and click **Next >** to proceed.

Select **Instance Configuration**.
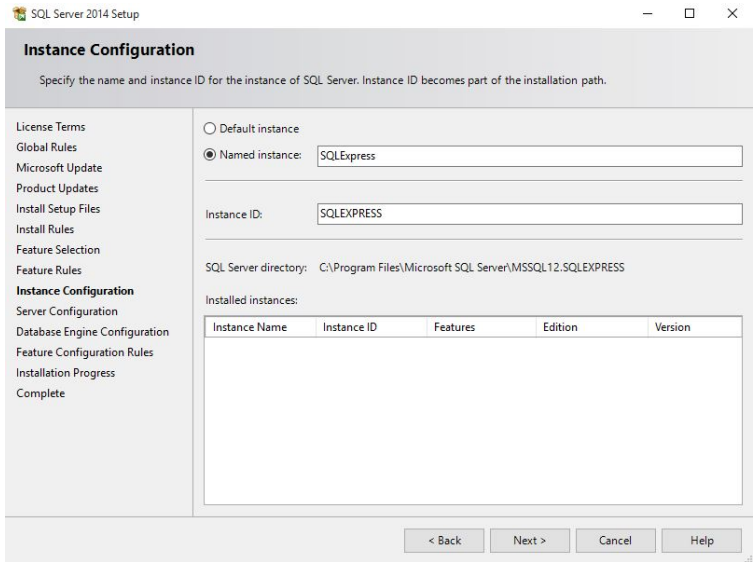
– Select one of the radio buttons **Default instance** or **Named instance**.
– Click **Next >** to proceed.
Select **Server Configuration**.
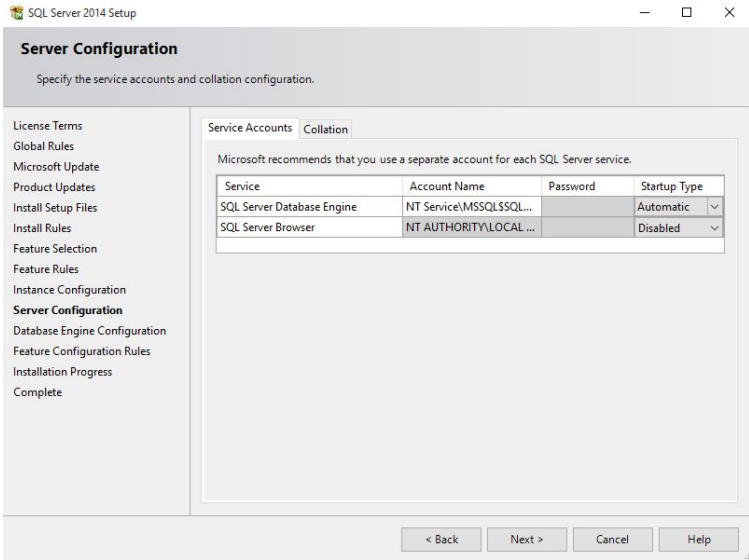
– Select the required **Service Accounts** and click **Next >** to proceed.
Select **Database Engine Configuration**.
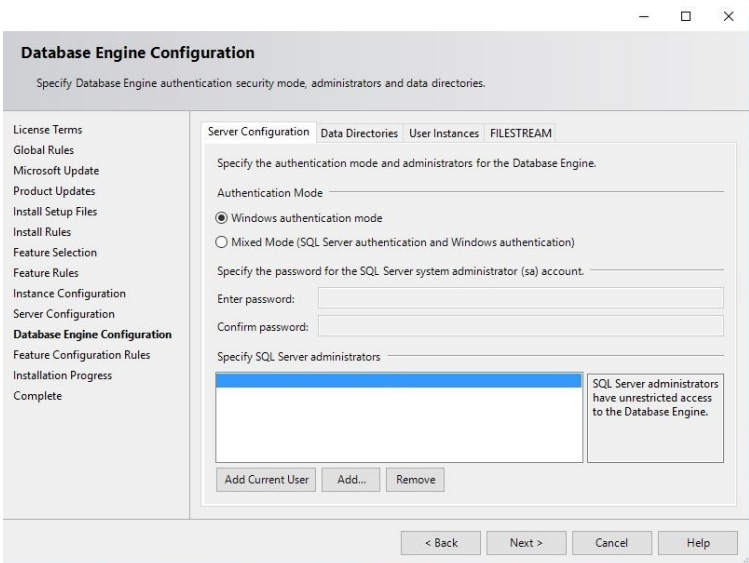
– Select the tab **Server Configuration** and activate the radio
button **Windows authenticication mode**.
– Click **Next >** to proceed.

Select **Complete** and check the **Status** column for successful
installation of all applicable features. This may take a few
minutes.
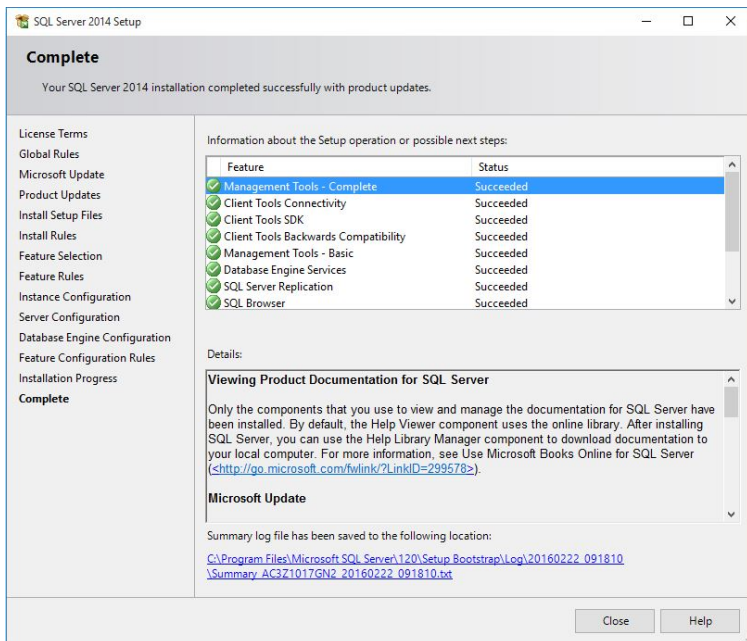


– The installation is now complete. Click **Close** to finish the
installation.

> **Notice!**
> If the installation fails, please contact the Microsoft customer
> support.

It is under the responsibility of the end-user of the SQL
database:

- To create credentials for the authorization to give access to the SQL database
- To create a backup of the SQL server, as the SQL database backup is not supported by the APE system.
- To manage the SQL security.

# 3       Video Integration

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

## 3.1      General

The video image display windows can show three different
states. (The exact appearance of the logo is partially dependent
on the software in use and can differ from the version shown
below.)

| Display | Description |
|---------|-------------|
| Live image/still image/recording | The window displays images from the selected camera. |
| BOSCH | The video display is either switched off or no camera has been selected. |
| BOSCH | There is no input signal on this video channel. |

**Explanation of terms**
– **Video verification**

A workstation user can compare an archive image associated with the card data in the database to a live image, and thus decide whether a person should be granted access.

– **Video identification** - (Access PE does not support this function)
This type of control requires the use of intelligent cameras that can compare archived grid images of a face/an eye with data from a live image and decide whether the person requesting access is known in the system.

– **Video surveillance**
In contrast to video identification and verification, here it is not the person requesting access who is checked, but the person's surroundings. This requires one or more cameras to show entire areas that can then be evaluated by workstation users via live or archive images.

**Setup**

Before the cameras can be used as additional security measures for access control, you must first install the video devices and configure them using the software supplied with the cameras. This includes configuring any digital video recorder (DVR) functions that may be present.

You will need to install the **Bosch Video SDK**s (on the CD) in order to use the video components in Access Professional Edition.

1. You can use the **Video devices** page in the Access PE Configurator to select and activate the cameras you also want to use for access control.

2. When you are configuring **entrances**, the cameras can be defined as identification or front and back surveillance cameras.
You can also configure one of these cameras as an alarm and log book camera.

3. In the Personnel Management dialog, you can allocate workstation users rights for the video devices.
4. If the video verification function is configured for at least one entrance, you must set up one workstation to show the **Video verification** dialog permanently.
5. In addition to the Logviewer, you can use the **Alarm Management** dialog to switch directly to alarm situations (with video panel, if necessary).

**Which video components can be used where and for what purpose?**

– **Video panel**

Where      Personnel Management > 

Purpose – Live image feed from up to four cameras at the same time.
– Archive function for storing images and video sequences for each camera individually.
– Marking specific images with "Points of Interest" (POIs) that also trigger log book messages.

– **Video devices**

Where      Configurator > 

Purpose – Finding and using network cameras.

– **Configuring entrances for video**

Where    Configurator >

Purpose  –    Activating/deactivating video verification
         –    Configuring identification and surveillance
              cameras
         –    Defining alarm and log book cameras

– **Playing back recorded videos**

Where    Start > Programs > Access Professional Edition
         > Bosch Video Player

Purpose  –    Playing back video recordings stored
              locally.

**Note:** You only need this application if recordings have been
saved in the special vxx format for Bosch Video SDKs. You can
use any player of your choice for recordings in MPEG format.

– **Video verification**

Where    Personnel Management >
         or
         Start > Programs > Access Professional Edition
         > Video Verification

Purpose  –    Switching to a live image from the
              identification camera.
         –    Switching to the surveillance cameras.
         –    Visual comparison with the database
              image.
         –    Granting/denying access
         –    Storing still images locally

- **Alarm application**

Where     Personnel Management >



or
Start > Programs > Access Professional Edition
> Alarm Management

Purpose  –   Special view for certain alarms.
–   With video view, if necessary
–   Archive function for storing images and
video sequences.

- **Device states**

Where     Personnel Management

Purpose  –   Switching to any configured entrance
camera for a live image.
–   Activating/deactivating the display of the
access history for the selected entrance

- **Video devices**

Where     Personnel Management

Purpose  –   Switching to any configured camera for a
live image

- **Video playback**

Where       Logviewer > ▶

Purpose   –   Displaying the video recording relating to
              an alarm at an entrance.
          –   Archive function for storing images and
              video sequences.

## 3.2      Video devices

You can use this dialog to manage devices that are to be used
for video verification, room surveillance and/or alarm
processing.
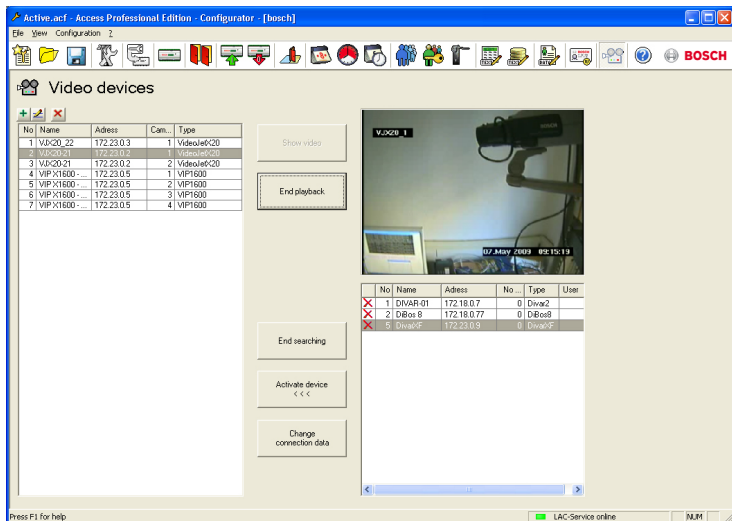


The dialog has three sections and is used for the following
functions.

1.   List field at bottom right
     You can use the buttons to the left of this list field to
     search for video devices in the network and select them for
     use in the access control system.

2.
- – **Browse new devices** button
  Press this button to search the network for new
  devices that are supported by the Bosch Video SDK
  (Software Developer Kit). Before you can do this, you
  must install all video devices and configure them
  according to the instructions supplied.
  To avoid the risk of duplicate configurations, devices
  you have already activated will not be shown again.
  During the search, the button name changes to **End
  searching** so that you can cancel the search if you wish
  to do so.
  Any new devices found will be shown in the adjoining
  list field.
  The entries in this list correspond to the encoder
  devices and not to the cameras themselves. The **No.
  cameras** column shows how many end devices are
  available according to the interfaces.
- – You can transfer selected list entries into the left-hand
  list field by pressing the **Activate device <<<** button;
  they are then available for use in the access control
  system.
  The only devices that can be loaded are those that the
  operator can access — these devices are marked with a
  ✓ . List entries marked with a ✗ must first be made
  accessible by pressing the **Change connection data**
  button.
  **Note:** The number of devices that can be loaded may
  be restricted by the license. If this is the case, devices
  are loaded according to the channel number sequence.
- – You can load password-protected devices (marked
  with a ✗) by pressing the **Change connection data**
  button.

Enter the username and password etc. in the dialog that opens. Authorized user accounts may have been set up during the configuration of the video devices. Only these accounts can be used here.

---

**Notice!**

The **Change connection data** button is only active if the device search has **not** yet finished.

---

3. List field on left
4.

– When you transfer the devices to the left-hand list field (**Activate device <<<**), a list entry is created for each video channel. The entry under **No. cameras** in the search list shows the number of entries that have been loaded.
   To help you identify the individual devices, the cameras are numbered in sequence next to the encoder device entries (Name, IP-address, Type).
   To help you select cameras in the Access PE dialogs, they appear in lists and displays along with the IP address of the connected device and with the sequential number in brackets, for example: 168.154.1.252 (2)
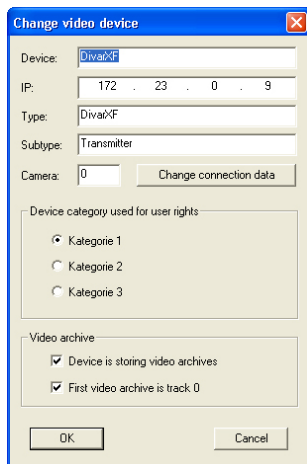
– To restrict access to the video devices, you can protect them with a username and password. You must configure the current access data to allow these devices to be used in Access PE.
   To do this, select an entry and then press the **Change connection data** button to open the edit dialog. Similarly here, you can only enter user data that is known to the video device in question. [You can only change the access data of the video device itself using its own software.]

---

As well as entering and changing user data, you can
also use this dialog to assign the cameras to one of
three **categories**. You can assign separate user rights
to each of these categories, so that only selected users
can operate certain cameras.



– **Manual device entry**
  If certain network configurations or settings prevent
  installed devices from being found by the automatic
  search function, you can also create these manually.
  The button above the list field also enables access to
  the **Change video device** dialog with empty fields,
  where you can enter the necessary connection data.

5.  Video panel at top right
    To make it easier to find the right camera, you can switch
    to a live image (**Show video** button) or an archive recording
    (**Show playback** button) from the selected list entry (left-
    hand list). To play back a recording, you must first define
    the point in time at which you wish to begin.
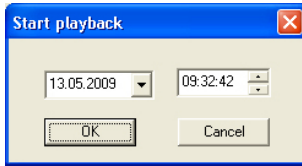
**Notice!**

You can only play back a recording if the video system has an appropriate configuration for the camera in question.

Video data is stored in a circular buffer that starts to overwrite the oldest recordings when the disk capacity limit is reached. The storage space available for this camera therefore defines how long a recording period is possible.

## 3.3 Creating and editing entrances

The entrance creation dialog also offers an option for setting up cameras for this entrance.
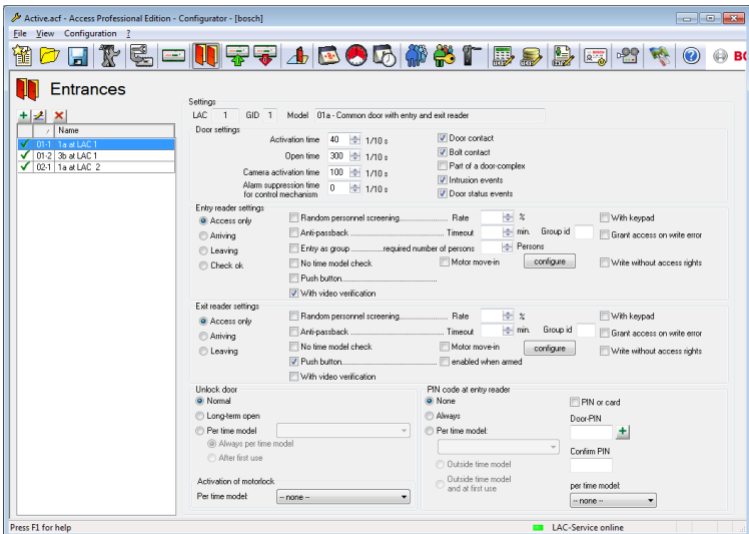
To enable and set options for **Video verification**, you can make changes and configure other settings in a special dialog that you can open by pressing the **Video configuration** button. Proceed as follows:

– Activate the checkbox **With video verification**
– Double-click the selected LAC under **Entrances**

The following screen is displayed:
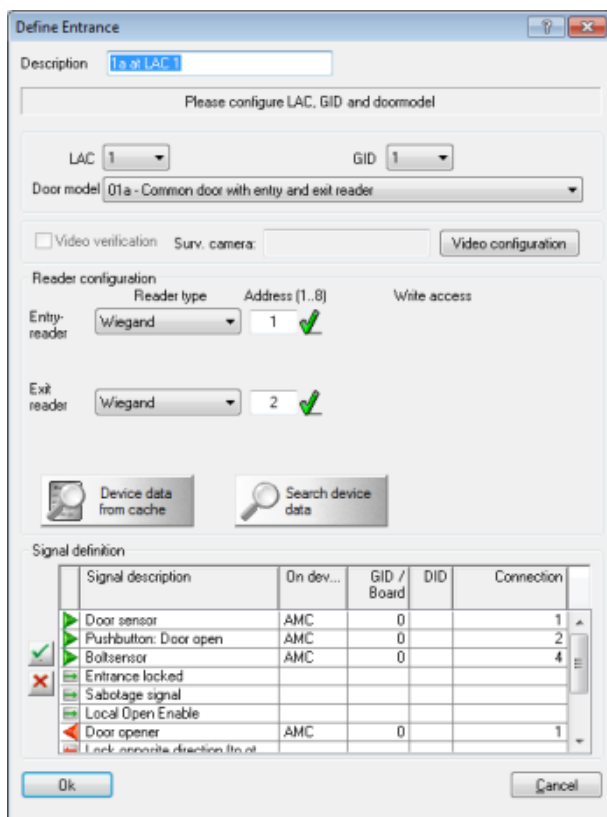


Click the button **Video configuration** to start the Configuration screen:
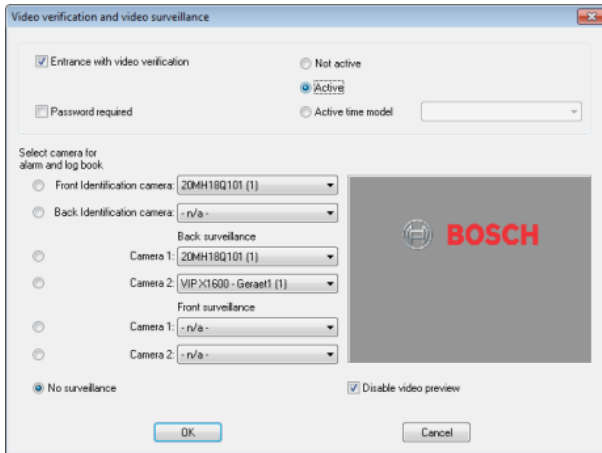
### Video verification

The top part of the dialog is for configuring video verification settings. If you want an additional check to be carried out at this entrance by way of a comparison between archive and live images, select the **Entrance with video verification** check box. This verification is carried out in a special dialog that can be protected against unauthorized access by configuring specific user rights. If you select the **Password required** check box, the **Video verification** dialog can be given special protection; when the dialog starts up, the user rights are checked as usual, but the user's password is also requested.

You can use the **Not active**, **Active** and **Active time model** options to suppress video verification for this entrance, activate it continuously or activate it part-time.

**Notice!**

If video verification is active, you must start the image

comparison dialog (Personnel Management > ) on at

least one workstation; if you do not, all access requests will be

denied.

**Camera configuration**

You can configure up to five cameras for each entrance; each of
these cameras can be set up for three different functions. You
can only select and assign cameras here that were activated in
the **Video devices** dialog.

1. **Identification camera**

    This camera is installed in such a way that it transmits a
    facial view of the person requesting access and is therefore
    generally also used for video verification purposes.
    Use the adjoining list field to assign the appropriate
    camera.
    You can only define one camera in this category.

2. **Back surveillance**

    You can configure two cameras to monitor the back area.
    This allows you to determine whether the person
    requesting access is under threat, unnoticed by the
    identification camera.

3. **Front surveillance**

    You can assign up to two devices to this camera category.
    By monitoring the area behind the door, you can ascertain
    whether someone really has gone through the door, who it
    is and, if applicable, whether anyone else has followed the
    first person in.

---

**Notice!**

To make it easier to select the right camera, you can display a live image from the selected camera in the list field in the right-hand window.

You can deactivate this function by selecting the **Disable video preview** check box.

---

You can nominate one of these cameras as the **camera for alarm and log book** by selecting this option next to the relevant camera. Images from this camera will be displayed during alarm processing and in corresponding log book messages. If this camera has a DVR recording, you can access this at a later time via the log book dialog.

If you do not want or need this facility, select the **No surveillance** option to deactivate it.

## 3.4    User Rights

User rights for the video applications can be restricted and assigned as follows.

| User right | Description |
|---|---|
| User rights for persons | |
| Alarm verification | The user can access the **Alarm Management** dialog and process incoming alarms. |
| Video verification | The user can access the **Video verification** dialog to compare live images of the person requesting access with the images stored in the database. |
| User rights for video devices | |

---

| User right | Description |
|---|---|
| Category 1 | The user can display live images from cameras in the activated category. You can select more than one category. |
| Category 2 | |
| Category 3 | |
| User rights for video functions | |
| Live video | The user can display live images. |
| Archive | The user can access stored recordings. |
| Export/record | The user can store live images or recordings locally. |
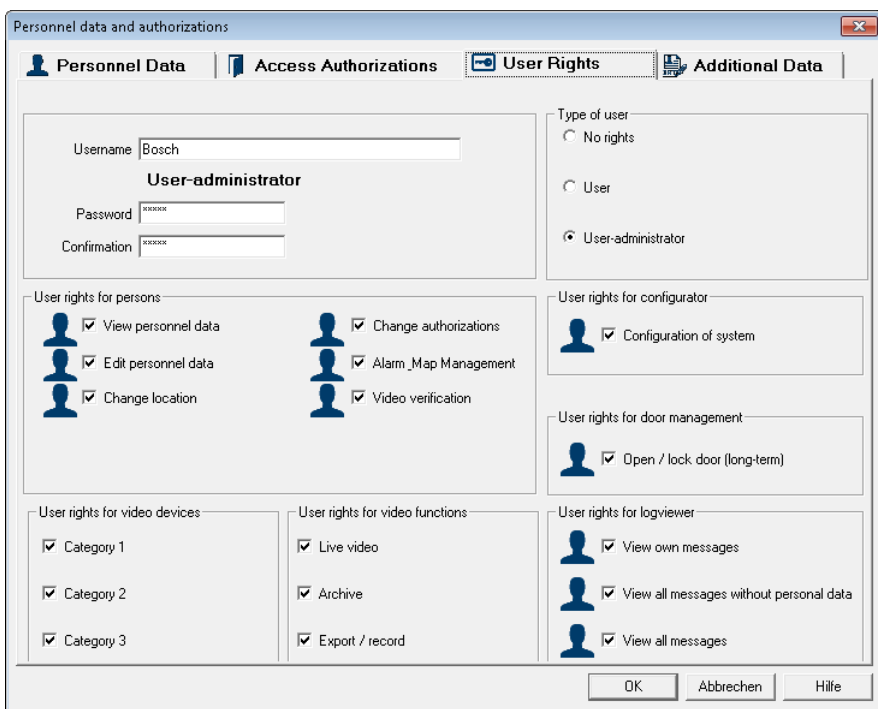
# 3.5 Personnel Management

When the video system is installed additional facilities are
activated in Personnel Management, which serve to make the
video system more useful and versatile.
The following, which shows the Personnel Management view
with the additional video elements, is intended as an overview
of the special facilities of the video system.
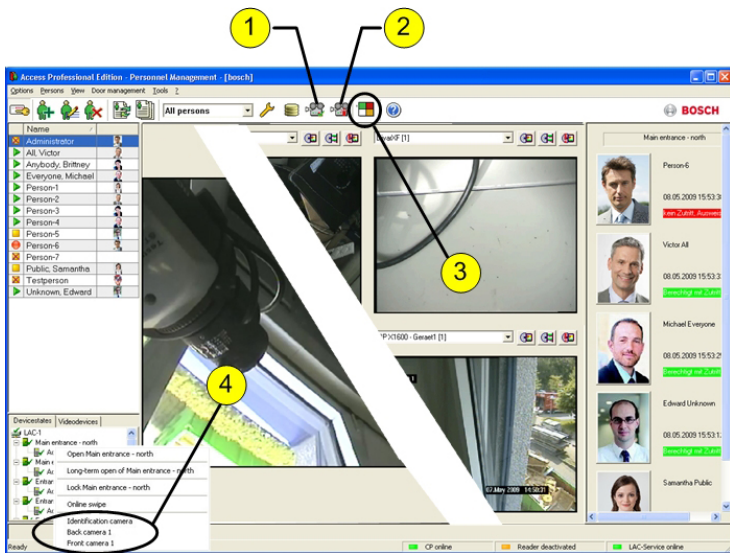
| 1 = | **Video verification** - starts the dialog for comparing images in the event of access requests. Refer to *Video verification, page 76*.<br>You must start this dialog on at least one workstation; if you do not, **all** access requests will be denied. |
|------|------|
| 2 = | **Alarm Management** - starts the dialog for processing alarms and video recordings from the alarm and log book camera. Refer to *Alarm Management, page 81*. |
| 3 = | **Video panel** - Views from up to four separate cameras can be displayed here. Still images and recordings can be stored locally for each video. Refer to *Video panel, page 72*. |
| 4 = | **Live image** - A live image can be shown from each camera at the selected entrance. This is either shown in full or as a thumbnail. Refer to *Live image, page 74*. |

In combination with the live image display, you can use the video panel to display up to five different camera positions in a single view and check them at the same time.

### 3.5.1 Video panel

Press the [icon] button in the Personnel Management toolbar to replace the dialog field with a display showing four video views.
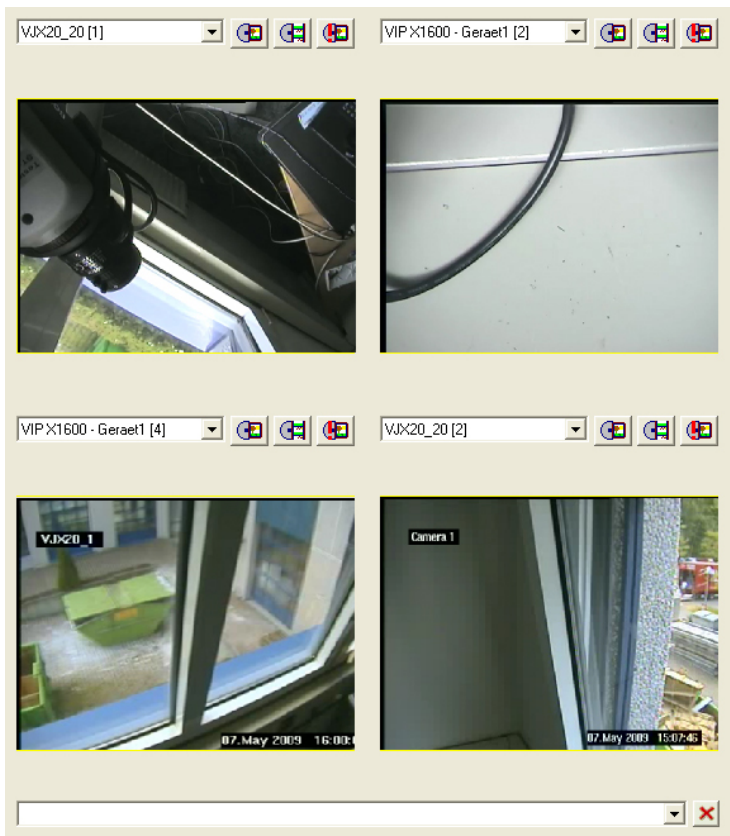
Whereas, for example in video verification, images are shown from a single entrance, here it is possible to select up to four cameras from different entrances.
The following functions are available for each display window.

| | |
|---|---|
| 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>_yyyyMMddhhmmssttt.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

![X] 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.
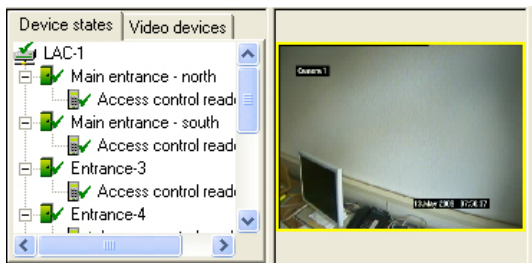
If you select a personnel record to edit while the large live image is displayed, the live image mode switches to a smaller format. If the live image function for one of the cameras is active, the popup menu includes the **Video off** entry, which you can use to restore the default state.

> **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 verification

You can use video verification to make sure that the person requesting access is actually the card holder; to do this, check the card and authorization data.

**Notice!**

If video verification is activated for at least one entrance (PE Configurator > Entrances > Select the entrance you want to edit > Video configuration), you must also start the Video verification dialog on at least one workstation; if you do not, **all** access requests will be denied.

**Description of dialogs**

Start the application by pressing the  button in Personnel Management, or go to **Start > Programs > Access Professional Edition > Video Verification**. If there are no current access requests, the dialog displays the default page (a map of the world). If an authorized person scans their card at the entrance, the dialog switches to the views from the relevant cameras. If the workstation user is currently engaged in other activities, any access requests will bring the Video verification dialog to the foreground.
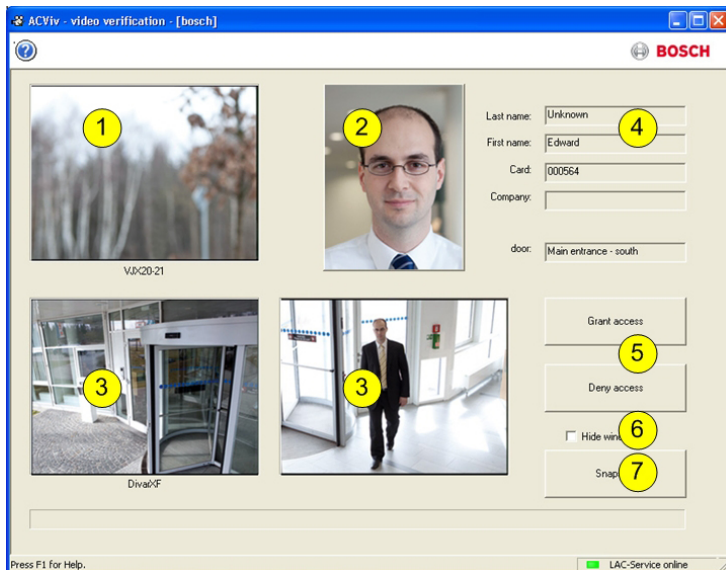
| 1 = | **Identification camera** - transmits a live image of the person requesting access. |
|---|---|
| 2 = | **Database image** - an archive image is displayed for comparison with the live image. |
| 3 = | **Surveillance cameras** - the camera showing the back view is shown first, then when the door is unlocked, the display switches to the front view camera. |
| 4 = | **Personnel data** - display showing the data stored in the database for the card number scanned. |
| 5 = | **Grant access**/**Deny access** - buttons for releasing or locking the door in question. |
| 6 = | **Hide window** - closes the dialog after video verification has been successfully completed and brings it back to the foreground the next time an access request is made. |
| 7 = | **Snapshot** - still images are stored locally from all three camera views. |

**Requirements**

The following facilities are necessary to enable this check, which is carried out by comparing a live image and an archive image.

– Images of the card holder are stored in the database.
– A camera is installed in such a way that it can create a facial view of the person requesting access.
– Up to two cameras recording the area behind the person requesting access — optional.
– Up to two cameras recording the area through the door — optional.
– Door configuration
–
   – Mark this is as an **Entrance with video verification**.
   – Set video verification to **Active**.
   – Select a device to use as the **Identification camera**.
   – Optional — other cameras to monitor the back or front area.
– At least one permanently manned workstation on which the **Video Verification** application has been installed and started.
   This can run on several workstations at the same time. However, incoming access requests are only sent to one workstation to avoid duplicate or even contradictory processing.

**Access procedure for an authorized person**

1. Person scans card
2.
   – Card data checked
   – Authorizations checked
3. Video Verification application connected
   If available and configured:
4.
   – Top left: live image from the identification camera
   – To the right of that: archive image of card holder

- To the right of that: card holder's data — Last name, First name, Card and Company, along with the entrance at which the person is waiting

5.

- Bottom left: live image from the first surveillance camera for the back area
- To the right of that: live image from the second surveillance camera for the back area

6. The workstation user...

7.

- ... makes sure that the live image matches the archive image and checks the recordings from the surveillance cameras.
- ... grants/denies access depending on the outcome of the comparison and checking activities.

8. Video Verification application

9.

- When the door is unlocked, the bottom two displays from the surveillance cameras switch to the cameras monitoring the front area. This image remains on the screen until the door closes.

---

**Notice!**

You can store any number of still images from the camera images displayed locally at any time. Press the **Snapshot** button to save an image from each video.

---

**Dialog activation**

After you have started the Video verification dialog, it defaults to showing the map of the world. You cannot edit any data or process the dialog when it is in this state. When an **authorized** person requests access at an entrance **configured** and **activated**

---

for video verification, the display shows images from the installed cameras and the corresponding data from the database.

If other applications were being used on the workstation when the request was made, thus pushing the Video verification dialog into the background, the dialog is automatically brought to the foreground at this point.

Once the access request has been processed, the dialog view switches back to the default (map of the world) but remains in the foreground.

If you do not wish to work with this setting, you can select the **Hide window** option to automatically minimize (iconify to the taskbar) the dialog after each verification process; this option also brings the dialog to the foreground each time a new request is received.

## 3.6.1    Switching video verification on/off

The context menu of entrances/readers [in the device status list] also offers the function **Deactivate video verification**. This allows, for example, a temporary shortening of the access request process, or conversely, the rapid activation of video verification without the need to change the configuration.

When video verification is switched off, the corresponding entry in the context menu is marked with a tick.

The function is only available for those entrances for which video verification has been activated in the configuration data. The activation/deactivation of video verification is controlled by the LAC-Service. This distributes the information to all workstations so that the settings can be modified from any of them.

## 3.7      Alarm Management

You can start this dialog from the Personnel Management view by pressing the ⚼ button, but you can also access it as a free-standing application via **Start > Programs > Access Professional Edition > Alarm Management**.

---

**Notice!**

To ensure that alarm processing tasks can be carried out, this dialog must be running on at least one workstation at any given time.

---

In contrast to the log book, only messages in the **Alarm** category are displayed here.

Incoming messages in the **Alarm** category bring the **Alarm Management** dialog to the foreground on the workstation where it is running, so that they can be processed quickly. The messages appear on each workstation computer on which the dialog is started, and can be processed by each of these workstations.

If the alarm message has been issued by an entrance with a surveillance camera configured as an **alarm and log book camera**, the camera's live image is displayed when you select the message concerned.

Press the buttons in the toolbar to save images ⬛ or recordings ⬛ of these live images locally. See *Local recordings, page 84* for details on storing and naming local copies.

The workstation user can respond to the alarm message for example by commissioning repair work, initiating further checks or alerting the security services himself.

You can switch off the video display for the selected message by pressing the ⬛ button in the toolbar. However, when you select another message, the video display is automatically reactivated.

You can delete alarm messages that have been processed or do not require any action from the list by pressing the **Confirm alarm** button. Confirmed messages are deleted from the lists on all workstations that have the Alarm Management dialog running.

## 3.8    Logviewer

If a surveillance camera has been configured for an entrance, all messages for this entrance are marked with a ▣ in the log book dialog. Depending on the video device configuration, this means that video sequences from the selected surveillance camera are available, and can be played back, starting at the time the message was issued.

When you select a message with camera identification, the ▣ button in the toolbar is activated. Press this button to open the Video playback dialog.

**Video playback**

When you open the Video playback dialog, the playback starts, by default, 20 seconds before the alarm was issued and ends after 120 seconds.

You can configure the starting point and duration of sequences that are set when an alarm is issued.

Notes on operating the dialog:

| | |
|---|---|
| —⊦— | Progress display showing how far through the set time period the recording currently is. |
| 11:56 ⇅ | Adjustable fields for the beginning and end of the time period for the video sequence to be shown. |
| ✓ | The beginning and end times you set are only activated when you confirm them by pressing this button. |
| ▶ | Restarts the video sequence after you have interrupted it with the pause button, or reduces the playback speed if you had fast mode activated. |
| ▶▶ | Fast mode — fast-forwards the video sequence. |
| ❚❚ | Pause — interrupts the display — produces a still image. |
| ◄◄ | Jumps to the start of the sequence and restarts the playback. |
| ⤓ | Jumps to the issue time of the alarm for which the video recording was opened. **Note:** This is only possible if the time of the alarm is within the set interval. |
| ■ | Closes the **Video playback** dialog. |

## 3.9 Local recordings

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 an image in jpg format as **<device name>_yyyyMMddhhmmsstttt.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. As with all Access PE applications, you can also open the Video Player via **Start > Programs > Access Professional Edition**.

## 3.10 Video Player

Depending on the configuration of the video devices concerned and their storage capacities, the video camera recordings are saved for a certain period of time, but then overwritten once the storage limit is reached.

To save certain sequences or images for longer periods of time, you can store still images and video recordings locally.

You can store live images and recordings locally in **.jpg** format (images) or **.vxx** [or **.mpeg**] format (video recordings) when viewing them in the Personnel Management **Video panel** (live images only), in the log book **Video playback** dialog (recordings only) and in the **Alarm Management** dialog (recordings only). 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**. As with all other Access PE applications, you can open this via **Start > Programs > Access Professional Edition**.

---

**i**

**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.

# 3.11    Displays and processes
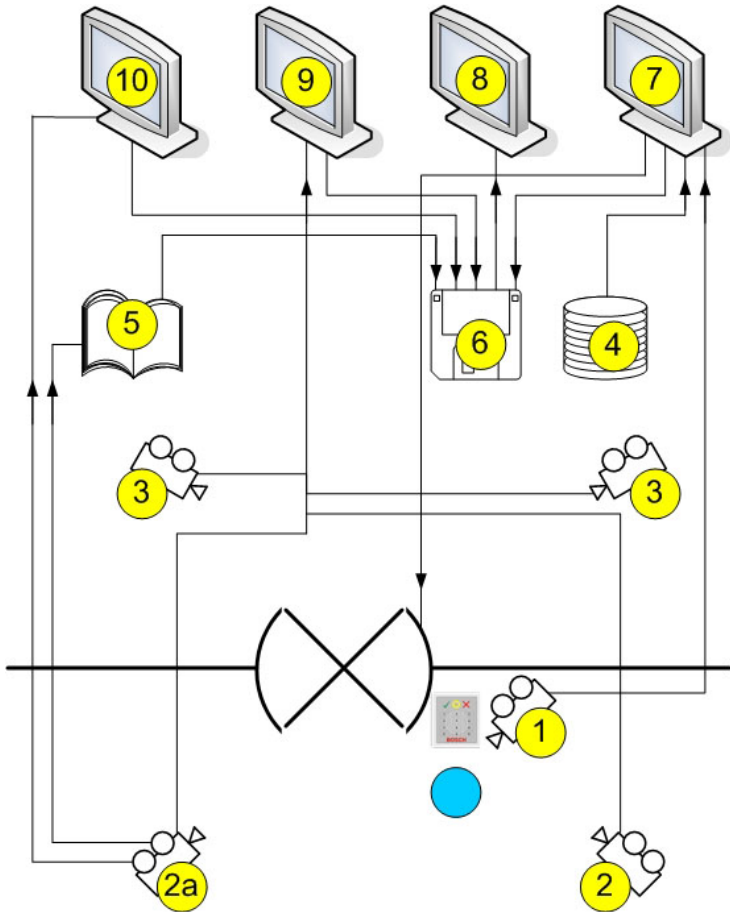


| 1 = | Identification camera |
| | The image from this camera is displayed in the Video verification dialog (7) when an access request is received. |
| 2 = | Surveillance cameras - back area |
| 2a = | Alarm and log book camera |

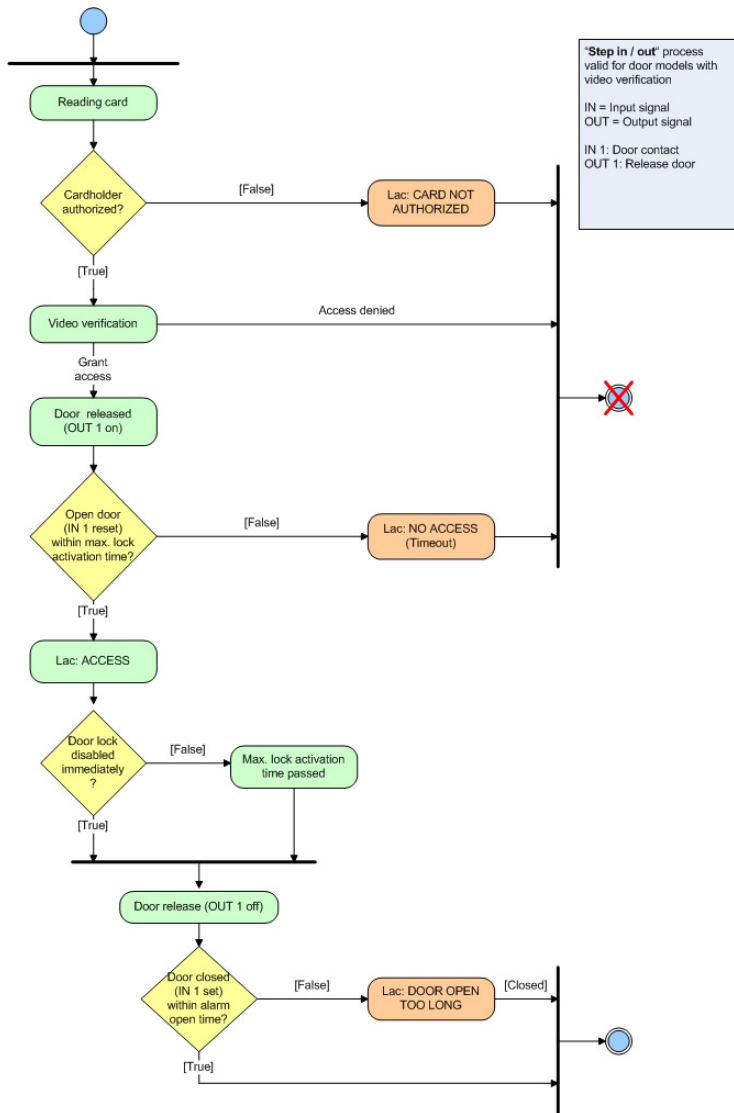|  | Choose one of the cameras 1, 2 or 3 |
|---|---|
| 3 = | Surveillance cameras - front area |
| 4 = | Database<br>In video verification (7), a database image is placed opposite the live image from the identification camera (1) for comparison. |
| 5 = | Log book<br>If you have configured an alarm and log book camera (2a), alarm-related images will be saved. |
| 6 = | Local hard disk/storage media<br>Local files can be saved from the Video verification (7), Video panel (9) and Alarm Management (10) dialogs, as well as from the images of the log book messages (5). In the case of video recordings (.vxx format), these can be displayed with the Bosch Video Player (8). |
| 7 = | Video verification<br>– Image comparison between the live image from the identification camera (1) and a database image (4).<br>– Door release/locking via a button in the dialog.<br>– Local storage of displayed images (6). |
| 8 = | Bosch Video Player<br>Locally stored .vxx recordings (6) can be displayed with this dialog. |
| 9 = | Video panel<br>– You can display images from up to four cameras at the same time in this view.<br>– Local recordings (6) are possible for each camera. |
| 10 = | Alarm Management |

If an alarm and log book camera (2a) has been configured, you can also display video images for alarm messages from the relevant entrance. You can create local copies (6) of these images and display them via Video Player (8).

"**Step in / out**" process
valid for door models with
video verification

IN = Input signal
OUT = Output signal

IN 1: Door contact
OUT 1: Release door

**Flowchart:**

- (start)
- Reading card
- Cardholder authorized?
  - [False] → Lac: CARD NOT AUTHORIZED
  - [True] ↓
- Video verification
  - Access denied →
  - Grant access ↓
- Door released (OUT 1 on)
- Open door (IN 1 reset) within max. lock activation time?
  - [False] → Lac: NO ACCESS (Timeout)
  - [True] ↓
- Lac: ACCESS
- Door lock disabled immediately?
  - [False] → Max. lock activation time passed
  - [True] ↓
- Door release (OUT 1 off)
- Door closed (IN 1 set) within alarm open time?
  - [False] → Lac: DOOR OPEN TOO LONG → [Closed]
  - [True] →
- (end)

# 4 UL 294 Requirements

**Features not evaluated by UL:**
– The Video Verification System
– Map Viewer and Alarm Management with Map and Video
   Verification
– Video Player
– Log Viewer
– User Rights
– Personnel Management
– Burglar Alarm Use

**Features evaluated by UL:**
– APE-SW as supplementary monitoring equipment