



**BOSCH**

# **Access Professional Edition**

Video verification

**en** Configuration manual



## Table of contents

<b>1</b>	<b>Overview</b>	<b>4</b>
1.1	Modular Design	4
1.2	Server and Client Modules	4
1.3	Client activation	5
<b>2</b>	<b>General</b>	<b>6</b>
2.1	User Login	6
<b>3</b>	<b>Video Verification</b>	<b>8</b>
3.1	General	8
3.2	Managing video devices	11
3.2.1	Opening the Configurator	11
3.2.2	Finding video devices	11
3.2.3	Adding a video device to the access control system	11
3.2.4	Changing connection data	12
3.2.5	Changing video device data	13
3.2.6	Showing live video image	14
3.2.7	Showing archive recordings	14
3.2.8	Displays and processes	15
3.3	Creating and editing entrances	17
3.4	User Rights	20
3.5	Video verification	22
3.5.1	Switching video verification on/off	24
3.6	Alarm Management	24
3.6.1	Map Viewer and Alarm Management	26
3.7	Video playback	30
3.8	Local recordings	31
3.9	Video Player	32
3.10	Displays and processes	33
<b>4</b>	<b>UL 294 Requirements</b>	<b>35</b>

# 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.

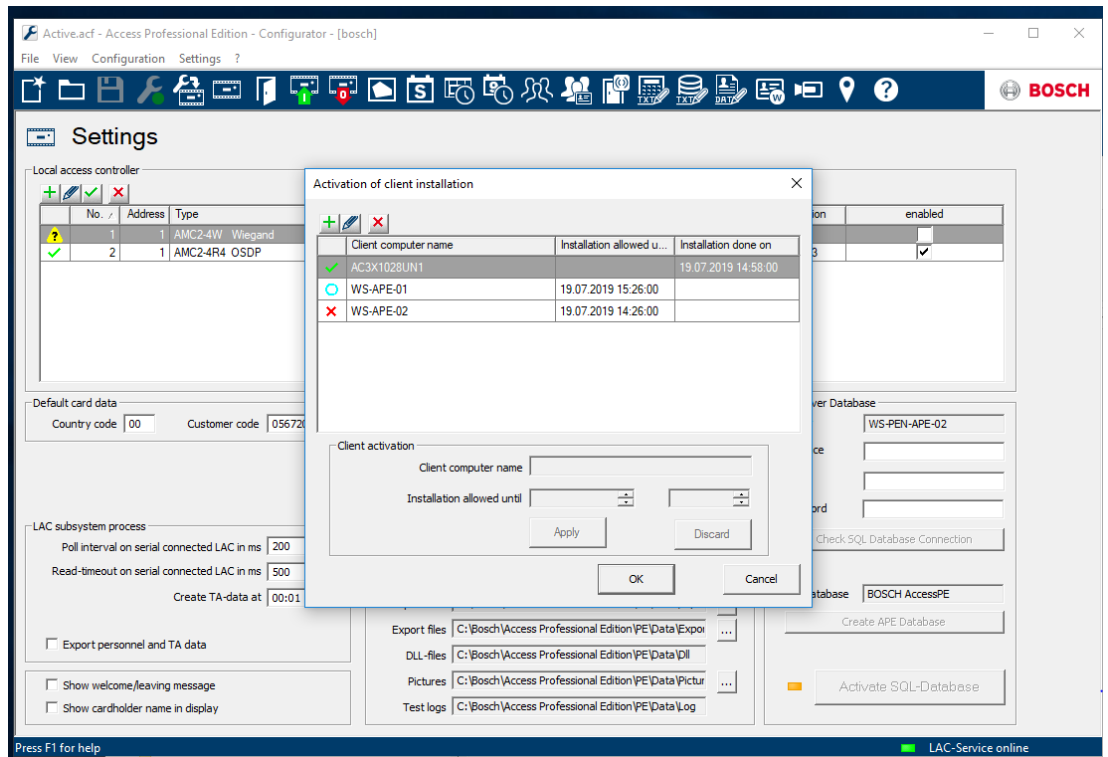
The LAC service needs to remain in constant contact with the controllers because firstly it constantly receives messages from them regarding movements, presence and absence of cardholders, secondly because it transmits data modifications, e.g. assignment of new cards, to the controllers, but mainly because 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)

### 1.3 Client activation



1. In the **Configurator**, click **Settings**.
2. Click **Client activation**.
  - A dialog box called "Activation of client installation" opens.
  - The dialog box "Activation of client installation" shows the name and the period in which the client can be installed, as well as the time of the last successful installation.

<b>Blue circle</b>	- Installation is possible
<b>Red cross</b>	- Time expired - No installation
<b>Green check mark</b>	- Successful installation

1. Enter the name and the period in which the client installation should be possible.

During the Client installation, the entries will be checked and an error message will be generated if necessary.

## 2 General

### 2.1 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 screenshot shows a standard Windows-style dialog box titled "Change password". It contains two text input fields, one labeled "New password" and one labeled "Confirmation". At the bottom of the dialog, there are two buttons: "Ok" and "Cancel".

**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!**

## 3 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.



When the video system is installed additional facilities are activated in Personnel Management, which serve to make the video system more useful and versatile.

### See also

- *Video verification, page 22*
- *Alarm Management, page 24*

### 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.
	The video display is either switched off or no camera has been selected.
	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 SDKs** (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 Managing video devices


### 3.2.1 Opening the Configurator

There are three possible ways to open the Configurator:

#### Option 1

1. On your Desktop, double-click the Configurator icon .
- The Configurator opens.

#### Option 2

1. Open the **Access PE Personnel Management** application.
2. In the menu bar of the **Access PE Personnel Management** application, click .
- The Configurator opens.


#### Option 3

1. Open the **Access PE Personnel Management** application.
2. In the menu bar, select **Tools**.
3. In the drop-down list, select **Execute Configurator**.
- The Configurator opens.

### 3.2.2 Finding video devices

Precondition:


- Install and configure all video devices.
- Open the Configurator.

1. In the menu bar of the Access Professional Edition Configurator, click .
2. Click the **Browse new devices** button to search for video devices.
  - During the search, the button name changes to **End searching** so that you can cancel the search.
  - All video devices that are supported by the Bosch Video SDK will be detected and appear in the list field at the bottom right area of the Configurator dialog.

#### See also

- *Opening the Configurator, page 11*

### 3.2.3 Adding a video device to the access control system

1. Open the Configurator.
2. In the menu bar of the Access Professional Edition Configurator, click .
3. Click the **Browse new devices** button to search for video devices.

- During the search, the button name changes to **End searching** so that you can cancel the search.
  - All video devices that are supported by the Bosch Video SDK will be detected and appear in the list field at the bottom right area of the Configurator dialog.
  - Once a video has been activated, the activation button will be disabled.
4. Select a video device from the list field at the bottom right area of the Configurator dialog.
  5. Click the **Activate device** button.
    - The selected video device moves to the list field on the left-hand side of the Configurator dialog.

**Notice!**

You can only move devices that are marked with a green check mark. Make sure to first make password-protected list entries (marked with a red cross) accessible by pressing the **Change connection** data button.


**Notice!**

The number of devices that you can transfer may be restricted by the license.

**See also**

- *Opening the Configurator, page 11*

**3.2.4****Changing connection data****Option 1**

1. Open the Configurator.
2. In the menu bar of the Access Professional Edition Configurator, click .
3. Click the **Browse new devices** button to search for video devices.
  - During the search, the button name changes to **End searching** so that you can cancel the search.
  - All video devices that are supported by the Bosch Video SDK will be detected and appear in the list field at the bottom right area of the Configurator dialog.
4. Select a video device from the list field at the bottom right area of the Configurator dialog.
5. Click the **Change connection** data button.
  - The dialog box called **Change connection parameters** opens.
6. Enter the user name and the password.
  - Make sure that you are using an authorized user account.
7. Click **OK**.

**Option 2**

1. Open the Configurator.
2. Double-click a video device in the list field on the left-hand side of the Configurator dialog.
  - To help you identify the individual video devices, see the encoder device entries (No., Name, Address, Camera, Type).
  - A dialog box called **Change video device** opens.
3. Click the **Change connection data** button.

4. Enter the user name and the password.
  - Make sure that you are using an authorized user account.
  - Note that you can only change the access data of the video device using its own software.
5. Click **OK**.

Change video device

Device: Camera 1

IP: 172 . 23 . 0 . 10

Protocol: https://

Type: Dinion5000HD

Subtype: Transmitter

Camera: 1 Change connection data

Device category used for user rights

Category 1

Category 2

Category 3

Video archive

Device is storing video archives

First video archive is track 0


OK Cancel

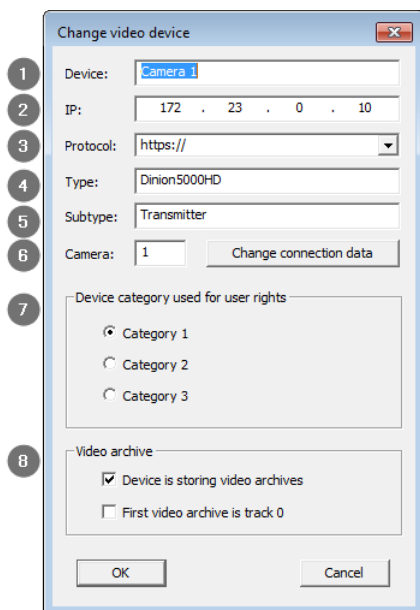
#### See also

- *Opening the Configurator, page 11*

### 3.2.5

#### Changing video device data

1. Open the Configurator.
2. In the menu bar of the Access Professional Edition Configurator, click .
3. To open the **Change video device** dialog box:
  - Double-click a video device in the list field on the left-hand side of the Configurator dialog.
  - Click the green plus icon above the list field on the left-hand side of the Configurator dialog.
4. Enter or change the video device data according to the possibilities below.
5. Click **OK**.



1	Enter or change the name of the video device.
2	Enter or change the IP address of the video device.
3	Video devices are connected through https protocol by default. If the selected video device does not support https protocol, select none, in the drop-down list.
4	Enter or change the video device type.
5	Enter or change the video device subtype.
6	Change connection data.
7	Assign one of three user right categories, so that only selected users can operate certain cameras.
8	Select or clear the check boxes depending on how you want the videos to be archived.

**See also**

- *Opening the Configurator, page 11*

**3.2.6**

**Showing live video image**

1. Open the Configurator.
2. In the menu bar of the Access Professional Edition Configurator, click .
  - Select a video device from the list field on the left-hand side of the Configurator dialog.
  - Click the **Show video** button.

**See also**

- *Opening the Configurator, page 11*

**3.2.7**

**Showing archive recordings**

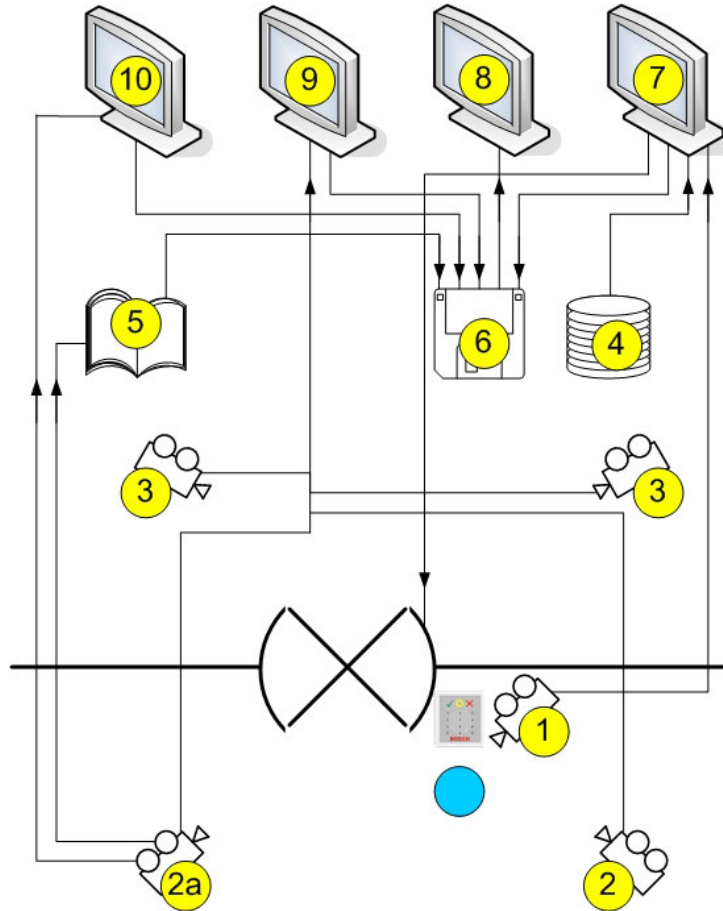
1. Open the Configurator.
2. In the menu bar of the Access Professional Edition Configurator, click .

3. Select a video device from the list field on the left-hand side of the Configurator dialog.
4. Click the Show playback button.
  - A dialog box called Start playback opens.
5. Define the point in time at which you want to begin to see the recording.
6. Click **OK**.

**See also**

- *Opening the Configurator, page 11*

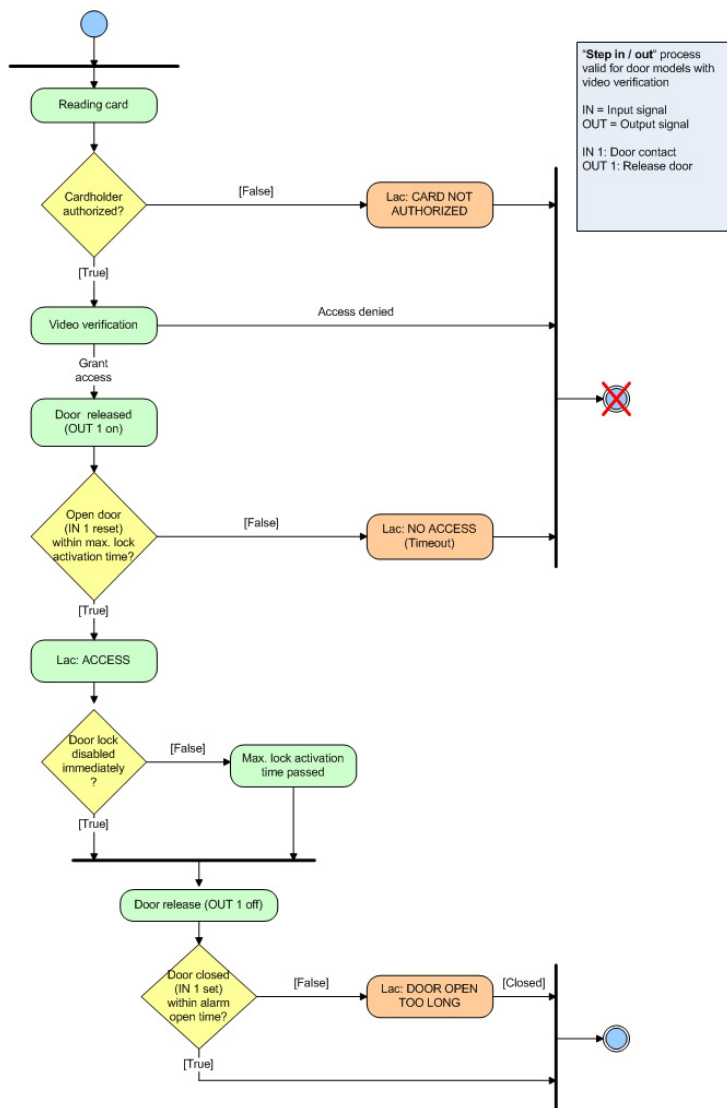
**3.2.8 Displays and processes**



1 =	<p>Identification camera</p> <p>The image from this camera is displayed in the Video verification dialog (7) when an access request is received.</p>
2 =	<p>Surveillance cameras - back area</p>
2a =	<p>Alarm and log book camera</p> <p>Choose one of the cameras 1, 2 or 3</p>
3 =	<p>Surveillance cameras - front area</p>
4 =	<p>Database</p> <p>In video verification (7), a database image is placed opposite the live image from the identification camera (1) for comparison.</p>

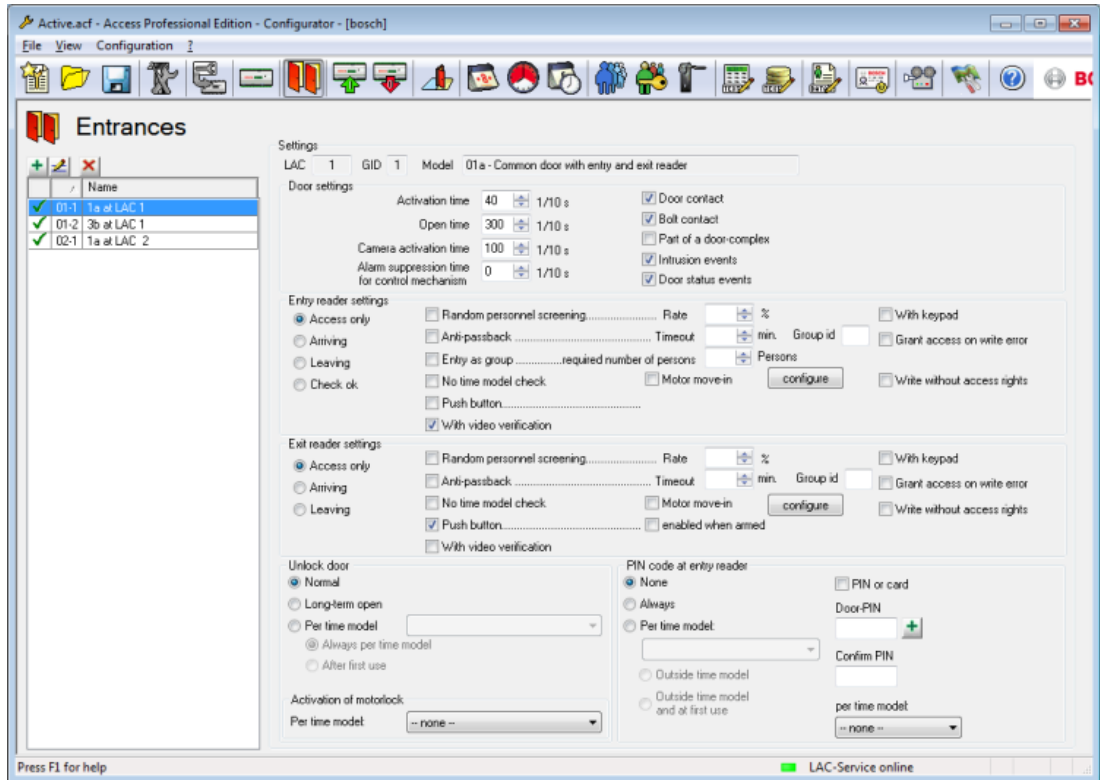
5 =	<p>Log book</p> <p>If you have configured an alarm and log book camera (2a), alarm-related images will be saved.</p>
6 =	<p>Local hard disk/storage media</p> <p>Local files can be saved from the Video verification (7), Video panel (9) and Alarm Management (10) dialogs, as well as from the images of the log book messages (5). In the case of video recordings (.vxx format), these can be displayed with the Bosch Video Player (8).</p>
7 =	<p>Video verification</p> <ul style="list-style-type: none"><li>– Image comparison between the live image from the identification camera (1) and a database image (4).</li><li>– Door release/locking via a button in the dialog.</li><li>– Local storage of displayed images (6).</li></ul>
8 =	<p>Bosch Video Player</p> <p>Locally stored .vxx recordings (6) can be displayed with this dialog.</p>
9 =	<p>Video panel</p> <ul style="list-style-type: none"><li>– You can display images from up to four cameras at the same time in this view.</li><li>– Local recordings (6) are possible for each camera.</li></ul>
10 =	<p>Alarm Management</p> <p>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).</p>





### 3.3 Creating and editing entrances

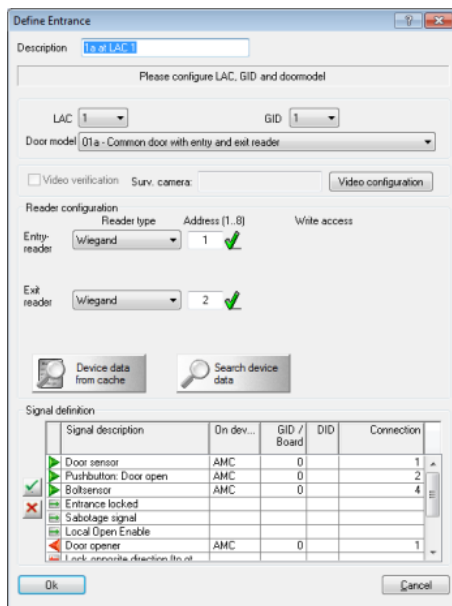
The entrance creation dialog also offers an option for setting up cameras for this entrance.



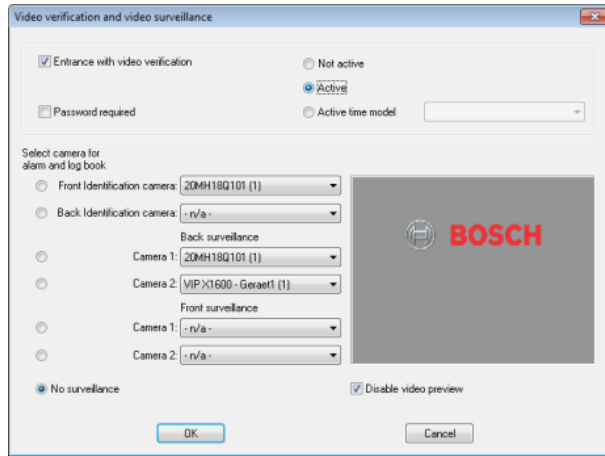
To enable and set options for **Video verification**, you can make changes and configure other settings in a special dialog that you can open by pressing the **Video configuration** button. Proceed as follows:

- 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 <b>Alarm Management</b> dialog and process incoming alarms.
Video verification	The user can access the <b>Video verification</b> dialog to compare live images of the person requesting access with the images stored in the database.
User rights for video devices	
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.

Personnel data and authorizations

**Personnel Data** | Access Authorizations | **User Rights** | Additional Data

Username

**User-administrator**

Password

Confirmation

Type of user

No rights

User

User-administrator

User rights for persons

<input checked="" type="checkbox"/> View personnel data	<input checked="" type="checkbox"/> Change authorizations
<input checked="" type="checkbox"/> Edit personnel data	<input checked="" type="checkbox"/> Alarm_Map Management
<input checked="" type="checkbox"/> Change location	<input checked="" type="checkbox"/> Video verification

User rights for configurator

Configuration of system

User rights for door management

Open / lock door (long-term)

User rights for video devices

Category 1

Category 2

Category 3

User rights for video functions

Live video

Archive

Export / record

User rights for logviewer

View own messages

View all messages without personal data

View all messages

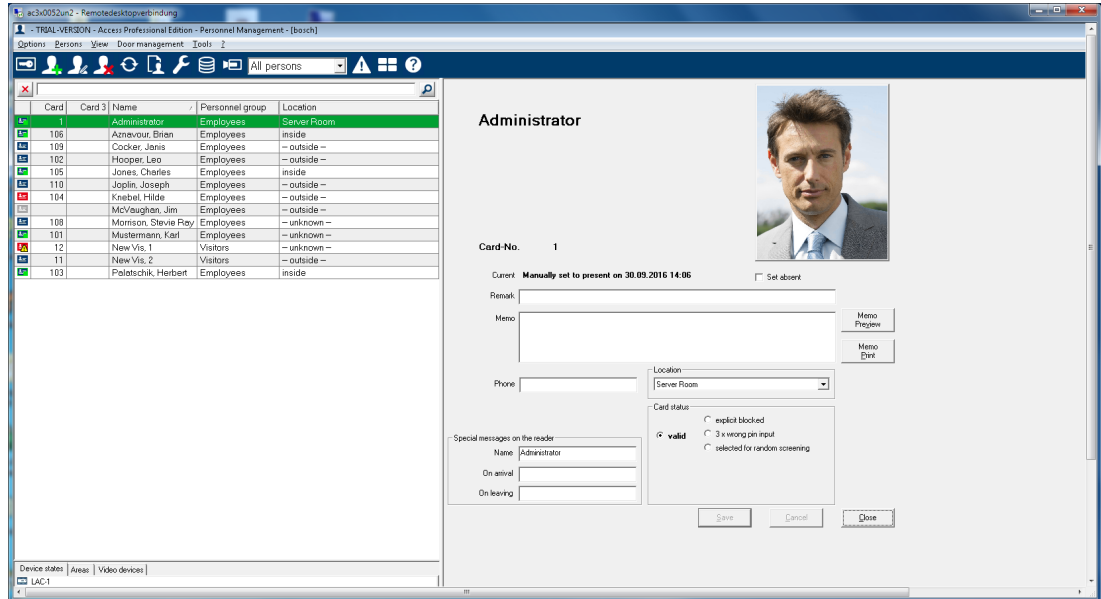
OK Abbrechen Hilfe

### 3.5 Video verification

#### Description of dialogs

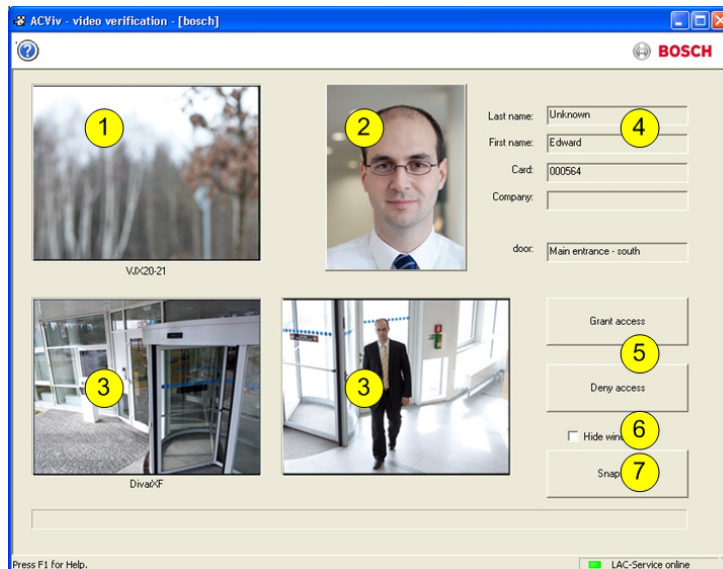


Start the application by pressing the button in Personnel Management.



If there are no current access requests, the dialog displays the default page. 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 =	<b>Identification camera</b> - transmits a live image of the person requesting access.
2 =	<b>Database image</b> - an archive image is displayed for comparison with the live image.
3 =	<b>Surveillance cameras</b> - the camera showing the back view is shown first, then when the door is unlocked, the display switches to the front view camera.

4 =	<b>Personnel data</b> - display showing the data stored in the database for the card number scanned.
5 =	<b>Grant access/Deny access</b> - buttons for releasing or locking the door in question.
6 =	<b>Hide window</b> - 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 =	<b>Snapshot</b> - 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
  - Card data checked
  - Authorizations checked
2. Video Verification application connected
 

If available and configured:

  - 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
  - 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
3. The workstation user
  - 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.
4. Video Verification application
  - 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 switches to showing the default. 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 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.

**3.5.1****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.

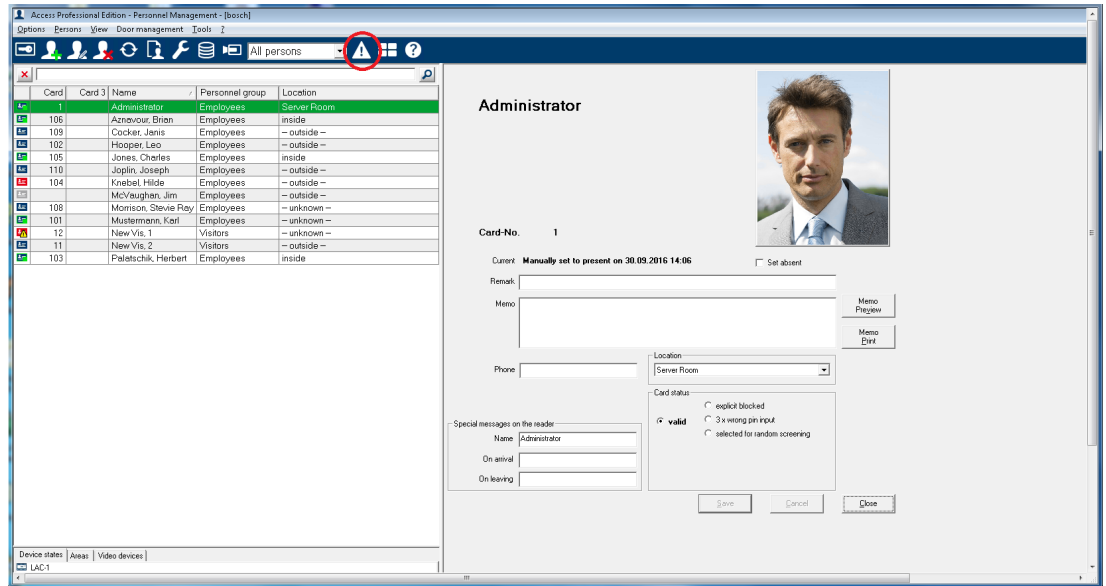
The function is only available for those entrances for which video verification has been activated in the configuration data.

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.

**3.6****Alarm Management**

You can start this dialog from the Personnel Management view by pressing the  button .






**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.

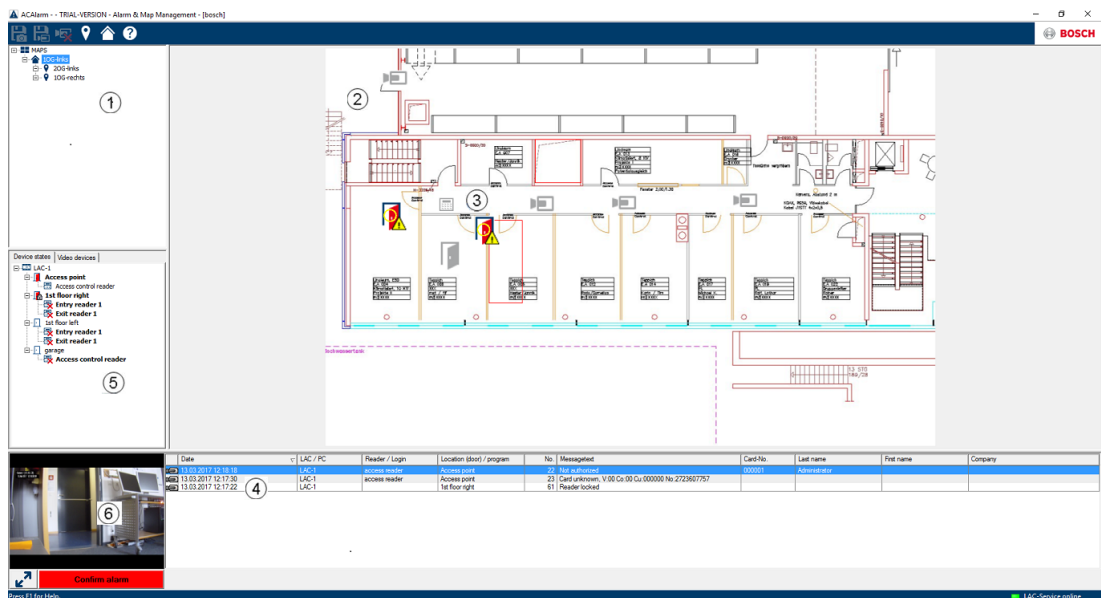
Press the buttons in the toolbar to save still images  or video recording  of these live images locally. See *Local recordings*, page 31 for details on storing and naming local copies.

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.

## 3.6.1 Map Viewer and Alarm Management



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

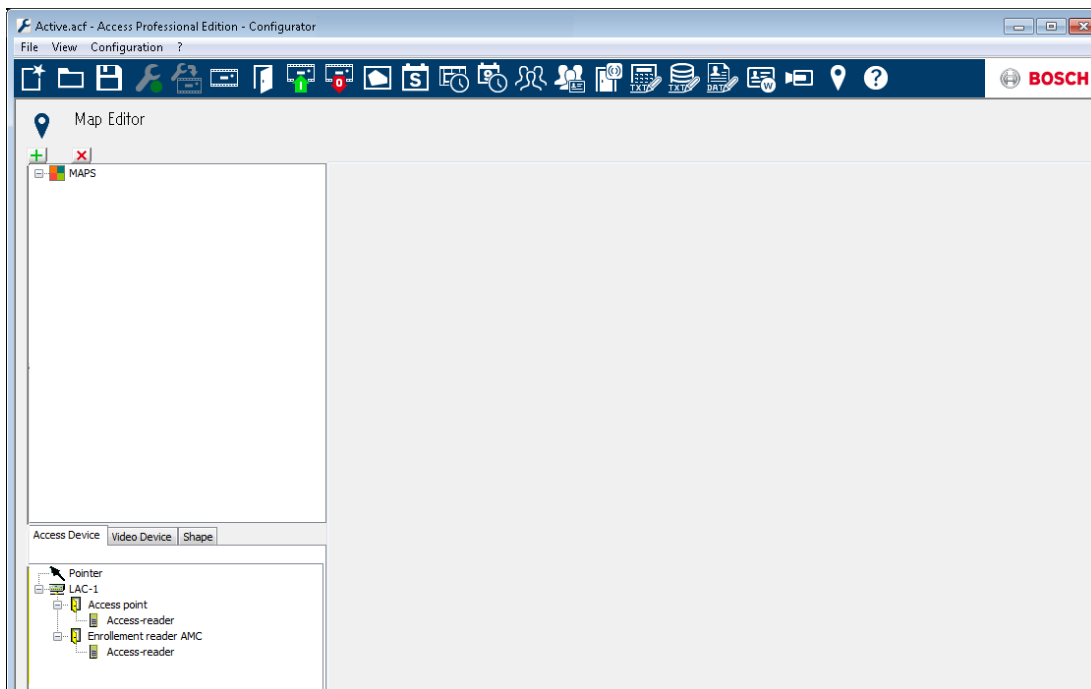
### Mapviewer features:

- Home map for easy navigation
- Navigation between photo views and floor plans via hyperlink
- Navigation via device tree structure up to three levels
- Interactive Graphical Maps for alarms with integrated alarm list
- Live view and door control from the map and device tree
- 128 maps per system
- 64 devices per map
- 64 hyperlinks per map
- Max 2 MB per map
- Map viewer use a standard image format .bmp, .jpg, .png

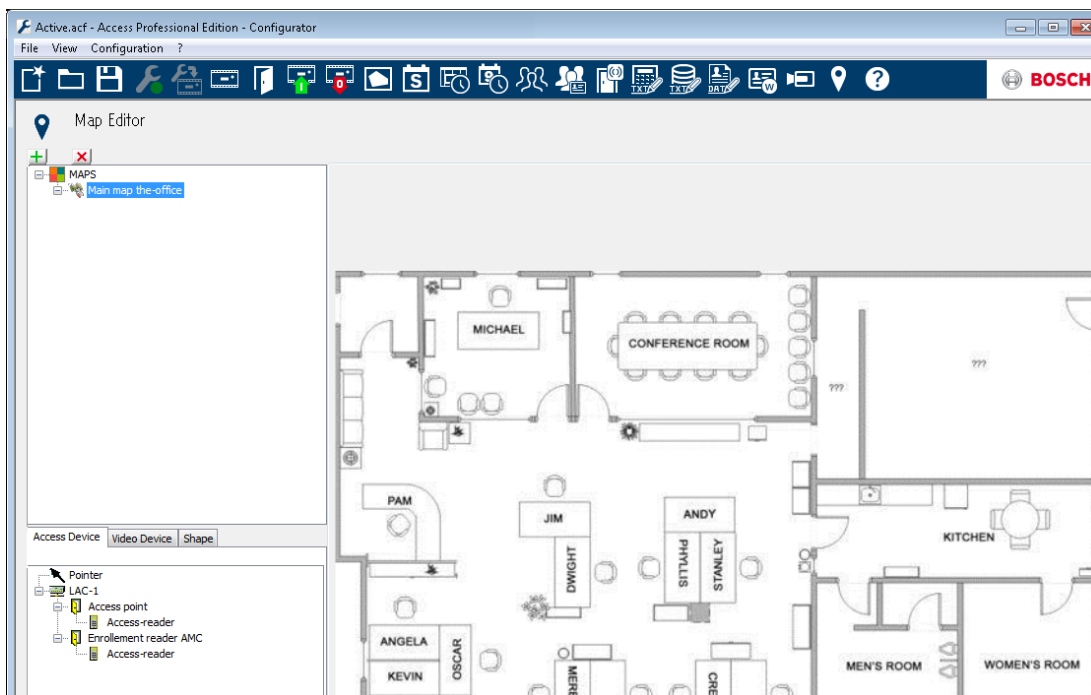
### 3.6.1.1

#### Configuring a map

Start the Map Editor

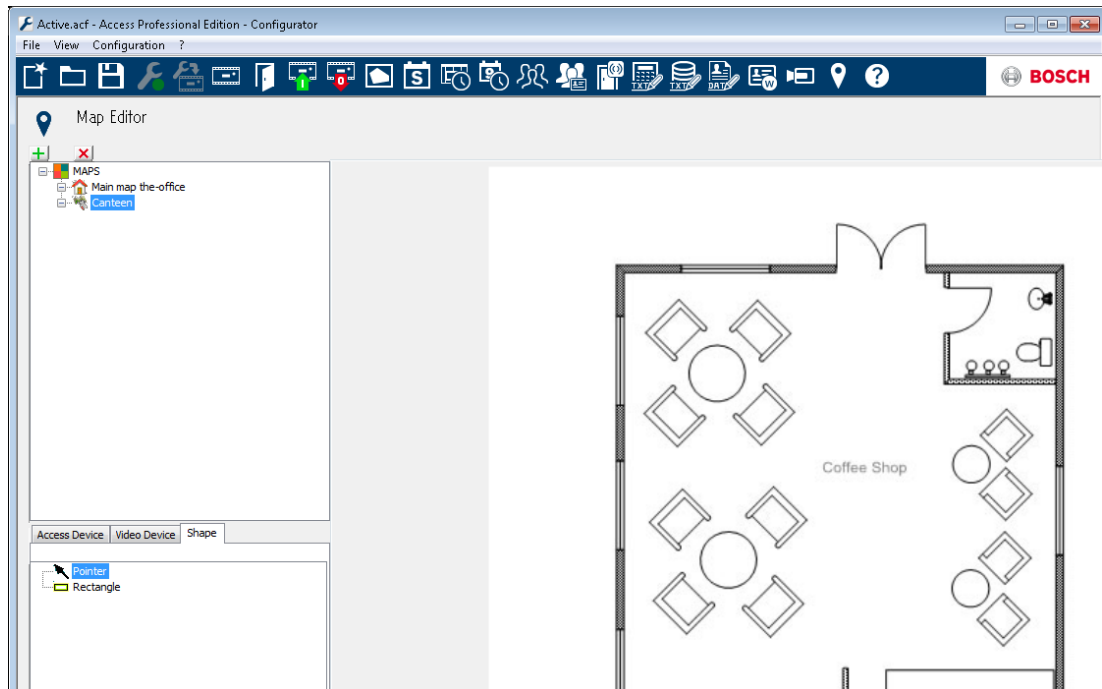


Click the  button to add a map.

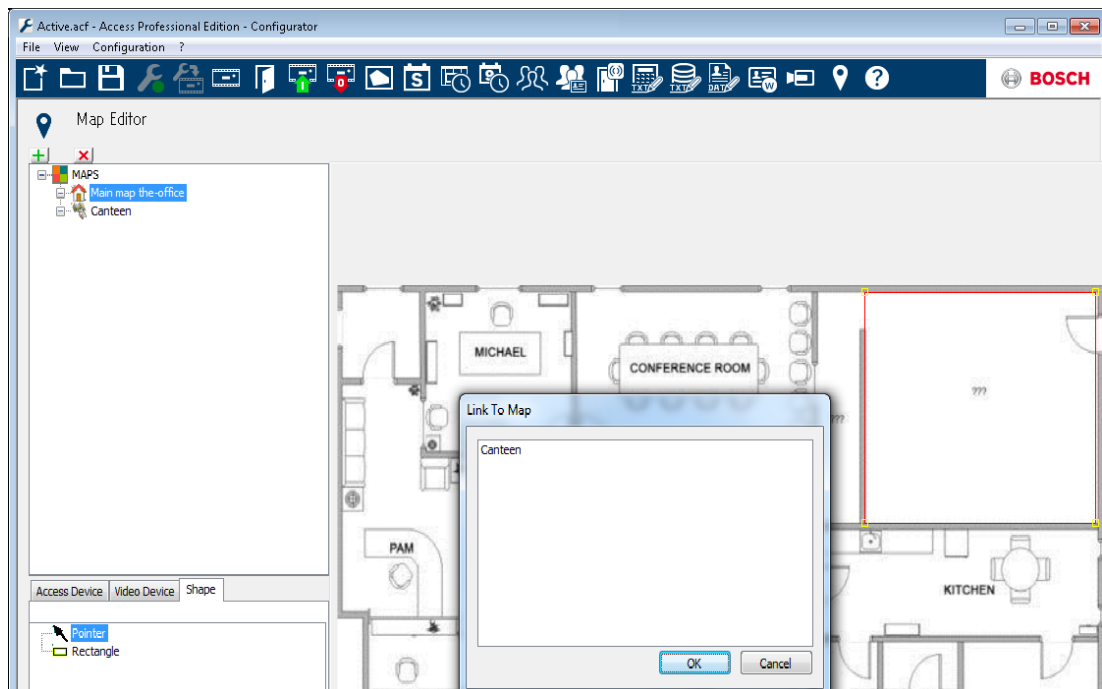


The map is shown on the dialog.

- Optionally configure this map as **Home Map**
- Add a detail view, e.g. the canteen, to the map tree.



- To connect the new **Canteen map** with the main map, go to the **Shape Tab** and select a **Rectangle**.
- Place the rectangle over the area of the main map that should be shown as a detail view (shown as a red rectangle in the example below).
- In the **Link to Map** Display select the respective detail view, which is “Canteen” in this example.



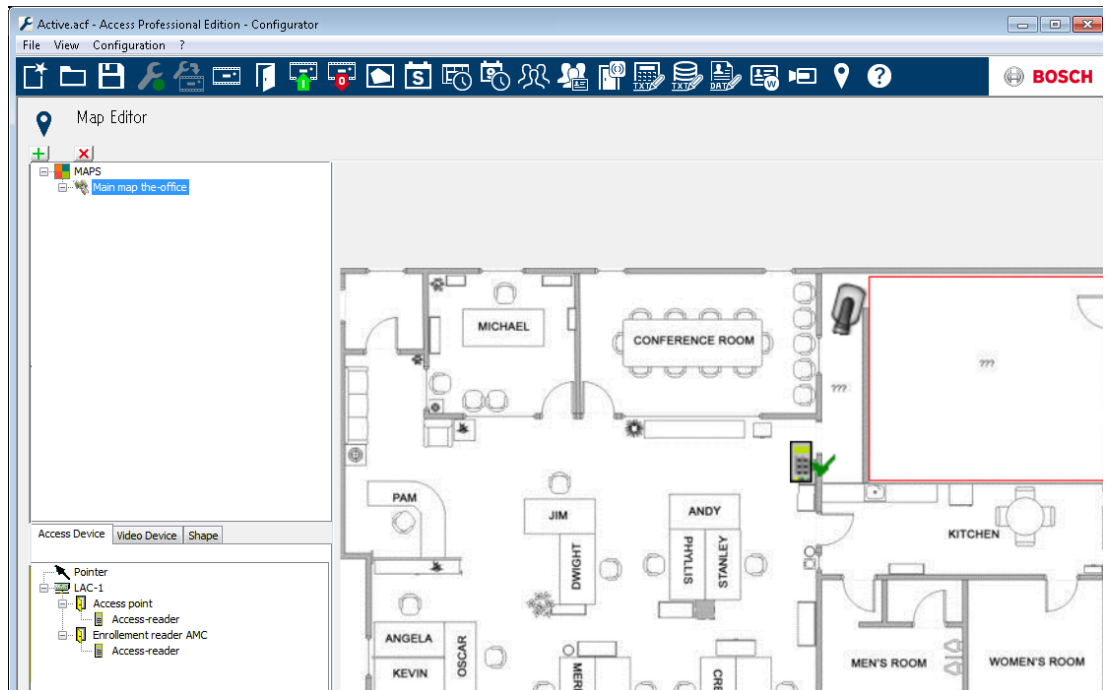
### 3.6.1.2

#### Adding a device to a map




Select the **Device Tab** and add Devices to the map by pulling them with the mouse into the map. In the example below the following devices have been added:




- One Access point

- One Reader
- Two Cameras




- Click a device in the map and resize by holding the mouse button pressed,
- Click a device and rotate as required using the scroll wheel of your mouse.


Device Types	Control elements
	Door
	Reader
	Camera

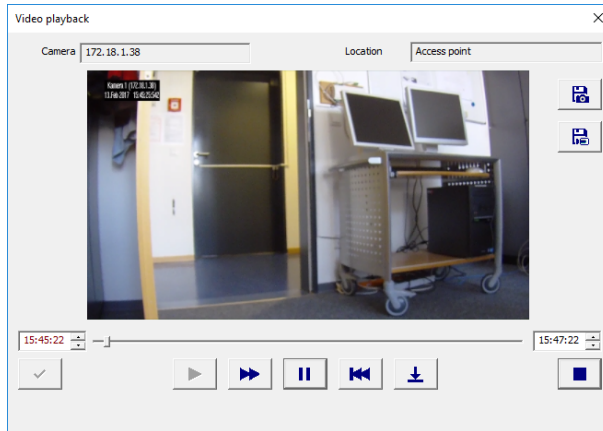
Device Types	Alarms
<b>Access Point (Entrance)</b>	
	Door opened without authorization
	Door opened too long
	(All Reader alarm also reflect as Entrance Alarm*)
<b>Reader</b>	Reader error
	
<b>Camera</b>	N.A.

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

## 3.7 Video playback

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.
-  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.

## 3.8 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.

## 3.9 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**.



### Notice!

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

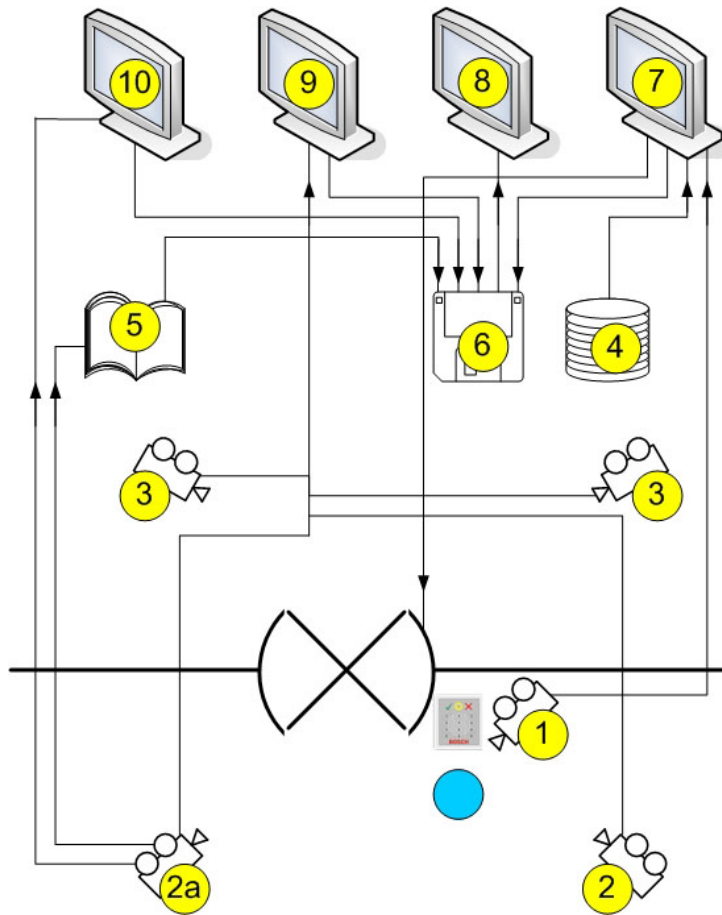
The dialog has been deliberately kept simple and only has two buttons next to the video display field, namely **open file** and **start/stop**.

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.

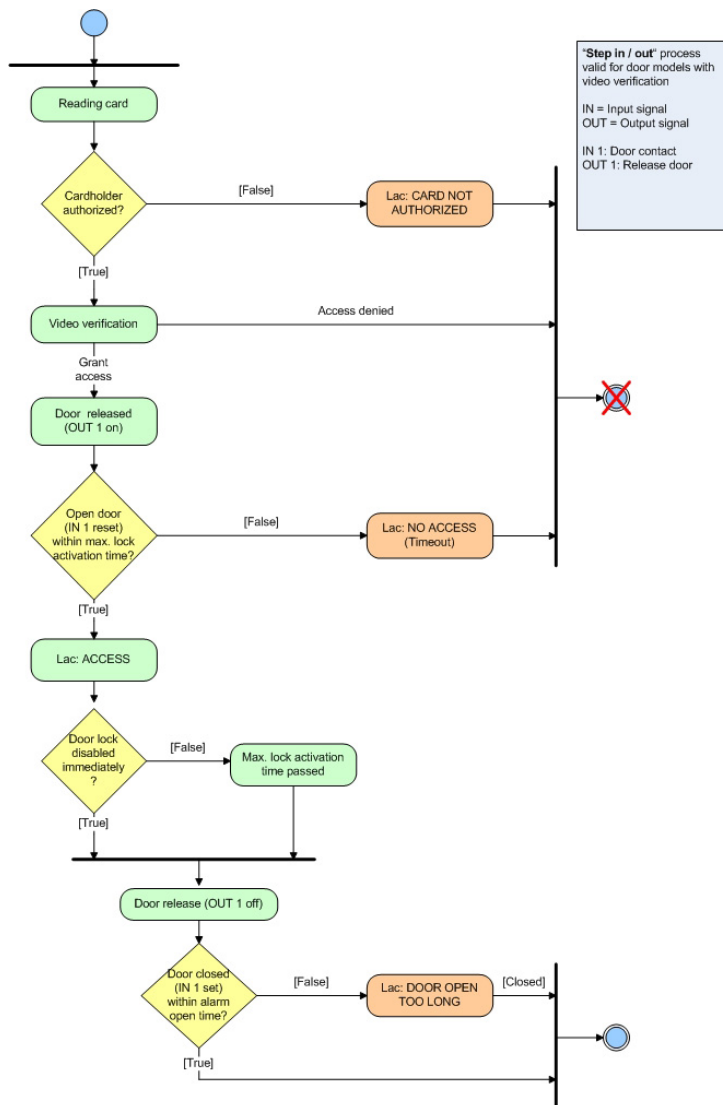


### 3.10 Displays and processes



1 =	<p>Identification camera</p> <p>The image from this camera is displayed in the Video verification dialog (7) when an access request is received.</p>
2 =	<p>Surveillance cameras - back area</p>
2a =	<p>Alarm and log book camera</p> <p>Choose one of the cameras 1, 2 or 3</p>
3 =	<p>Surveillance cameras - front area</p>
4 =	<p>Database</p> <p>In video verification (7), a database image is placed opposite the live image from the identification camera (1) for comparison.</p>
5 =	<p>Log book</p> <p>If you have configured an alarm and log book camera (2a), alarm-related images will be saved.</p>
6 =	<p>Local hard disk/storage media</p> <p>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).</p>

7 =	<p>Video verification</p> <ul style="list-style-type: none"> <li>– Image comparison between the live image from the identification camera (1) and a database image (4).</li> <li>– Door release/locking via a button in the dialog.</li> <li>– Local storage of displayed images (6).</li> </ul>
8 =	<p>Bosch Video Player</p> <p>Locally stored .vxx recordings (6) can be displayed with this dialog.</p>
9 =	<p>Video panel</p> <ul style="list-style-type: none"> <li>– You can display images from up to four cameras at the same time in this view.</li> <li>– Local recordings (6) are possible for each camera.</li> </ul>
10 =	<p>Alarm Management</p> <p>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).</p>



## 4 UL 294 Requirements

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

**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

**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
- Burglar Alarm Use







**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2019