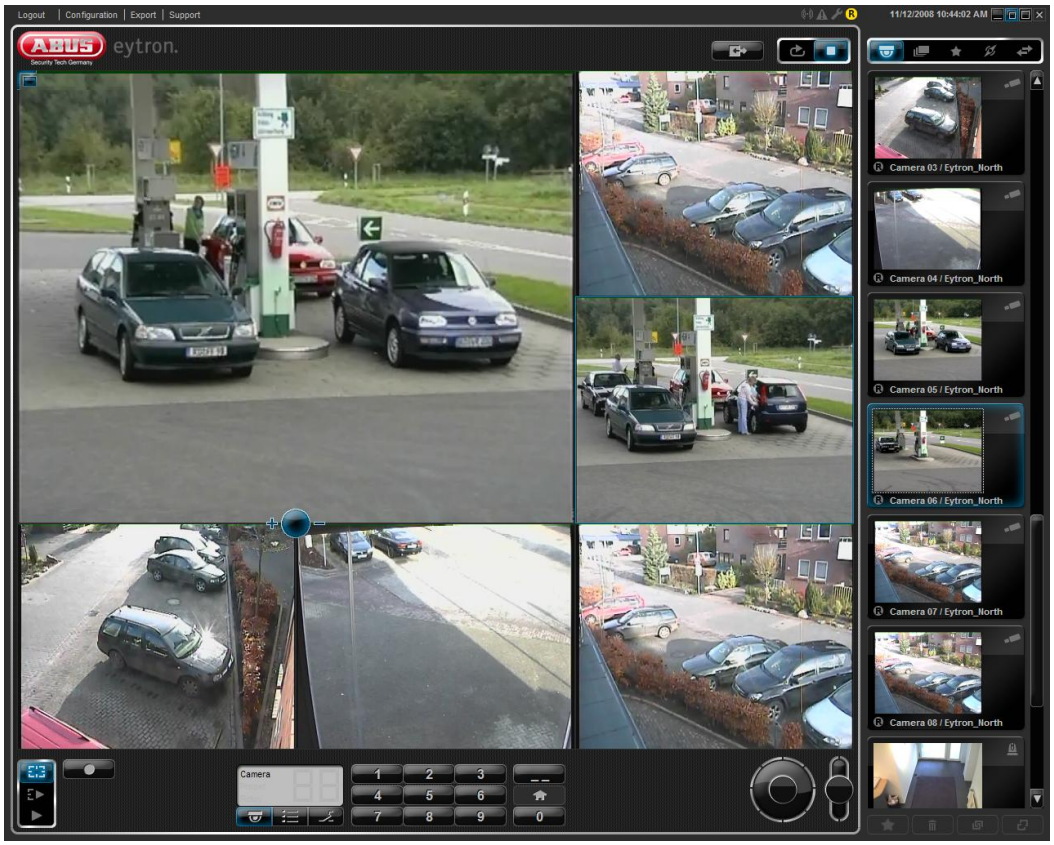
System manual

ABUS VMS

Basic, Professional, Enterprise
Web application



© 2012 ABUS Security-Center GmbH & Co. KG

Contents

Introduction **6**
Safety information **6**
Areas of application **7**
Information symbols **7**
Upgrades **8**
System requirements **8**
1. Setting up / putting into operation **9**
1.1 Starting the software 10
1.1.1 The setup wizard *10*
1.2 Log-in 13
1.3 User interface 13
1.3.1 Interface layout *13*
1.3.2 The CPU utilization indicator *15*
1.3.3 The network utilization indicator *16*
1.3.4 Logging out and exiting the software *17*
2. Software operation **17**
2.1 Switching system modes 17
2.1.1 Using the search function *22*
2.1.2 Voiding archives *23*
2.2 Switching the slide elements 24
2.3 System status indicator 26
2.4 Working with the cameras 26
2.4.1 Activating and deactivating the cameras *27*
2.4.2 Switching the image geometry *29*
2.4.3 Using the zoomstick *31*
2.4.4 Using the numeric field (keyboard) *31*
2.4.5 Saving camera positions (presets) *32*
2.4.6 Using the sequencer function *33*
2.4.7 Using manual recording (Panic Record) *33*
2.4.8 Using the alarm lists *34*
2.5 Creating backups 36
2.5.1 Local backup (database export) *36*
2.5.2 Local backup (AVI export) *37*
2.5.3 Remote backup *38*
2.5.4 Single frame export (storage, printing, e-mailing) *38*
2.6 Creating favourites 41
2.6.1 Deleting favourites *43*
2.7 Connecting to a host 44
2.7.1 Automatically redialing hosts after the connection is interrupted *45*

2.8 Reference image comparison 46
2.9 Shell mode (safe mode) 48
2.9.1 Activating the shell mode 48
2.9.2 Deactivating the shell mode 48
3. System configuration 49
3.1 Opening the system configuration 50
3.2 Camera configuration 51
3.2.1 Setting up an analogue camera 51
3.2.2 Setting up a pan/tilt camera 54
3.2.3 Setting up an network camera 55
3.2.4 Setting up the camera anti-swivel protection 58
3.2.5 Monitoring the camera focus 59
3.2.6 Displaying a camera name in the live image 60
3.2.7 Saving reference images 60
3.2.8 The mask dialog 61
3.2.8.1 Setting a permanent mask 63
3.2.8.2 Setting a privacy mask 64
3.2.8.3 Activating the adaptive mask 65
3.2.8.4 Configuring the sensitivity of activity detection 65
3.2.8.5 Using multiple-zone alarms 66
3.2.9 Setting up camera groups 67
3.3 Database settings (Database / Storage) 68
3.3.1 Setting the storage drives (drive settings) 69
3.3.2 Creating database fields 70
3.3.3 Setting up the archives 70
3.3.4 Backing up individual archives (automatic database backup) 72
3.4 Processes (actions) 74
3.4.1 Creating storage processes 74
3.4.2 Setting up a continuous recording or recording using activity detection 77
3.4.3 Alarm dialling 80
3.4.3.1 Setting up a "Guard Tour" 82
3.4.3.2 Setting up alarm dialling 86
3.4.4 Using the check call process 89
3.4.5 Setting up the FTP upload 90
3.4.6 Creating a video output process 93
3.4.7 Playing user-defined audio files in the event of an alarm 94
3.4.8 Using timers 96
3.4.9 Activations (process links) 98
3.5 Configuring the inputs and outputs (Digital I/O) 102
3.5.1 Virtual alarm detectors 103
3.5.2 Activating the external detectors 106
3.5.3 Activating the external relays 107
3.5.4 Using the SimUnit 108
3.5.5 ABUS serial alarm 109

3.5.6 CASA10010 ... 110
3.6 Security settings ... 110
3.6.1 Creating a new permission level ... 111
3.6.2 Creating a new user ... 115
3.6.3 Security guidelines ... 116
3.6.4 Automatic logging in and logging out of users ... 117
3.6.5 Windows login ... 118
3.7 Network configuration ... 119
3.7.1 Configuration of the network module (TCP/IP) ... 119
3.7.2 Activating the RTSP server ... 120
3.7.3 Creating a new host ... 121
3.7.4 Changing the network port ... 123
3.7.5 Using notifications ... 124
3.7.6 Sending/receiving configurations from a host ... 127
3.8 Miscellaneous settings ... 128
3.8.1 Multi-monitor operation ... 128
3.8.2 Language settings ... 129
3.8.3 Maintenance ... 131
3.8.4 Connection of a standard joystick ... 131
3.8.5 Miscellaneous ... 132
3.8.6 Activating and deactivating voice output ... 132
3.9 Importing / exporting the system configuration ... 132
3.10 POS operation (point of sale) ... 134
3.10.1 Setting up a camera for POS operation ... 134
3.10.2 Using the POS function and performing a database search ... 139
3.11 “UVV Kassen” operation ... 142
3.11.1 General information ... 142
3.11.2 Guidelines ... 142
3.11.3 Setting up “UVV-Kassen” operation ... 143
3.11.4 Measures to continue recording after power failures ... 149
4. ABUS® VMS web application ... 151
4.1 System requirements ... 152
4.2 Supported web browsers ... 152
4.3 Installing the web application ... 153
4.4 Accessing the web application ... 153
4.4.1 Log-in ... 154
4.4.2 Using the ActiveX plug-in ... 155
4.5 Working on the user interface ... 156
5. Installing software updates ... 160
6. Uninstalling the software ... 161
7. FAQs ... 162
8. Frequently used terms (glossary) ... 167

9. Online support and remote configuration 168

10. Copyright information.....170

Introduction

Thank you for choosing the ABUS.® **V**ideo **M**anagement **S**oftware. This manual explains how to use the software with the TV3300-TV3310 video cards together with the TV3311 alarm card, the TVVR95000-TVVR95020 video cards, as well as how it is used with the ABUS ® HDVR.

These instructions have been produced with the greatest care. Neither the author nor ABUS Security-Center can be held liable for damage arising from these instructions.

ABUS Security-Center reserves the right to modify this manual at any time without prior notice.

Please read these instructions carefully before putting the system into operation.

You can find more information on products from ABUS Security Center GmbH & Co. KG at

http://www.abus.com

Safety information

For the hardware and software to operate smoothly, you must observe the following safety information. Otherwise, the hardware may become damaged.

Video compression cards:

1. Avoid subjecting the card to excessive physical force (e.g. dropping the card).
2. Only remove the card from the anti-static bag immediately before installation.
3. Disconnect your PC from the power supply before installation.
4. When installing the card, ensure that your body is free of electrostatic charge.
5. When installing the card, ensure that the housing is sufficiently ventilated. If necessary, use an additional fan.
6. Never carry out independent repairs to the video or alarm card. Otherwise, all guarantee claims will become invalid.

ABUS.® HDVR:

1. Always pack the device in the original box for transportation.
2. Avoid subjecting the card to excessive physical force, such as vibrations or dropping the card.
3. Never place the device near heaters, ovens or any other sources of heat.
4. Avoid contact with direct sunlight.
5. Always allow the device to acclimatise before putting it into operation.
6. Never block the air supply. Otherwise, the system could overheat.
7. Install the device in dry rooms only and do not allow moisture to enter the equipment.
8. Before opening the device, switch it off and pull out the mains plug.
9. Never carry out independent repairs to the device. Always have them performed by trained specialists.

Areas of application

The areas where the ABUS.® VMS software can be used range from small monitoring assignments through to complex applications. Along with the ABUS® HDVR, the software also offers an inexpensive and reliable alternative in sectors such as banking (ATM, BGV), parking management or shop cash desks (POS).

The VMS Express or Basic software is included free of charge with the video cards (TV3300-TV3310) and the network cameras. The VMS Professional software is included free of charge with the video cards (TVVR95000 – TVVR95020). You can acquire extensions later by purchasing upgrades. The Upgrades item in the table provides an overview.

Information symbols

In the manual, notes or dangers are indicated by the following information symbols. Always read these through carefully.

Warning – The instructions must be followed.

Note – These boxes contain valuable information for using the software.

Upgrades

The performance of the VMS software can be expanded if the appropriate upgrades are made. The following overview shows the different versions.

Module	ABUS VMS Express	ABUS VMS Basic	ABUS VMS Professional	ABUS VMS Enterprise	ABUS HDVR
Maximum number of analog cameras	9	16		64	Up to 64
Maximum number of HD-SDI cameras					Up to 16
Maximum number of network cameras					Up to 24
Maximum number of hosts	1	1	3	Unlimited	Unlimited
Number of simultaneous users	1	1	3	10	10
Maximum number of screens	1	1	2	4	2
UVV (BGV) Kassen mode	-	-	Yes	Yes	Yes
Cash desk interface (POS)	-	-	Yes (2)	Yes (8)	Yes (8)
Use of masks	-	Yes	Yes	Yes	Yes
Lost focus detection	-	-	Yes	Yes	Yes
Camera swivel detection	-	-	Yes	Yes	Yes
Maximum number of users	1	Unlimited	Unlimited	Unlimited	Unlimited

System requirements

Supported operating systems

- Windows Vista 32-bit/64-bit
- Windows 7 32-bit/64-bit
- Windows 8 32-bit/64-bit

System requirement	Minimum requirements	Recommended hardware	Optimum performance
CPU	iCore3	iCore5	iCore7
RAM	2GB RAM	2GB RAM	4GB RAM

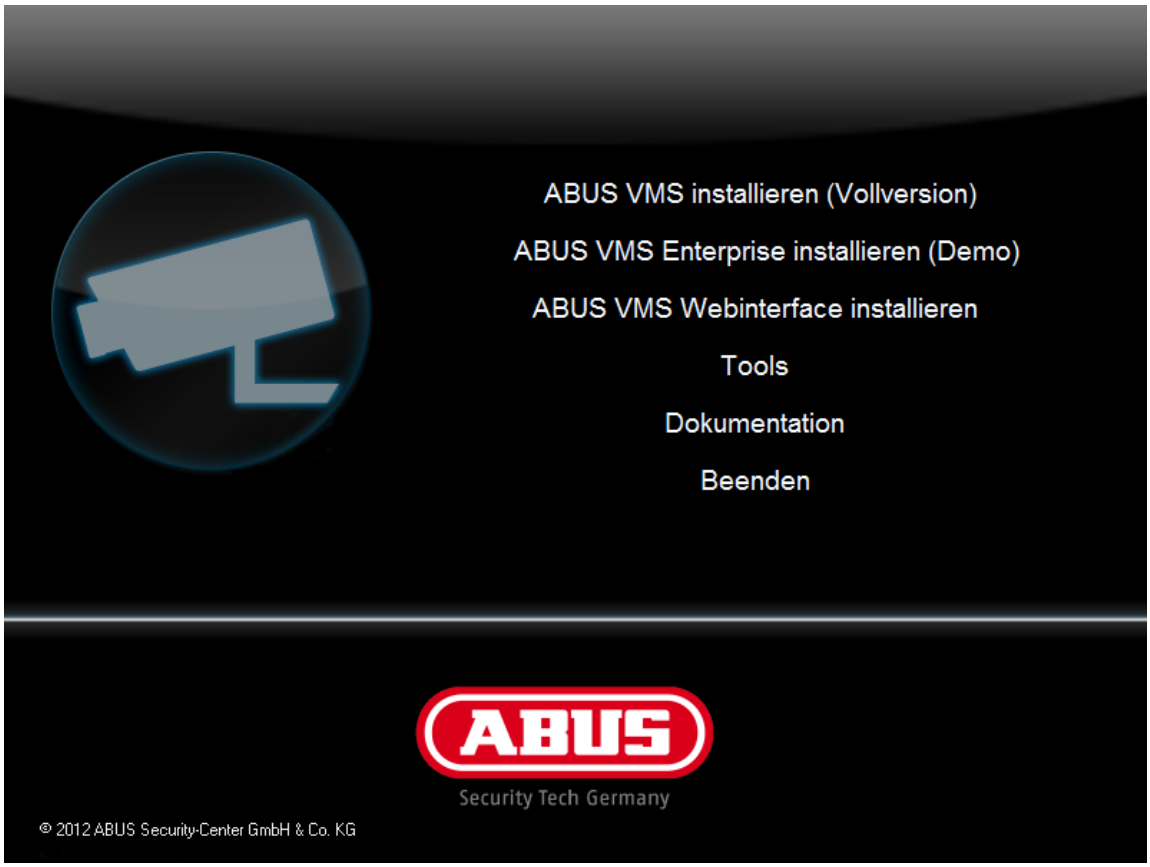
Note:

Microsoft server operating systems are not supported at present. When using a non-Intel processor, make sure it has a comparable computing speed to those stated above.

1. Setting up / putting into operation

Information on installing and putting the video hardware/recorders into operation can be found in the quick installation guide enclosed with the equipment.

To install the software, place the installation CD in the CD drive, wait until the start screen has been loaded and click *Install ABUS VMS*.



Follow the instructions in the installation wizard.

You can find technical data and documentation at http://www.abus.com

Warning: *The use of video and audio surveillance systems is subject to strict conditions. Therefore, establish which laws apply specifically to your country and, if necessary, inform your customers of these conditions before any installation is performed.*

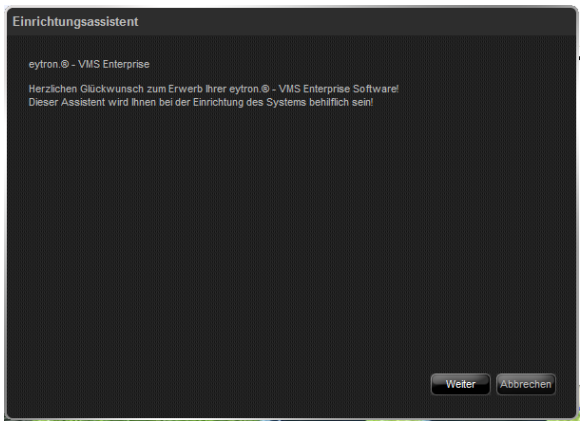
1.1 Starting the software

When the software starts, double-click the program icon on your desktop.

ABUS.® VMS

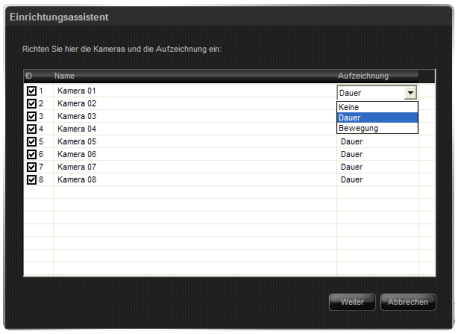
When the system first starts, it must be set up for recording.

The set-up wizard appears. This will assist you when setting up the system for the first time.



1.1.1 The setup wizard

If your system has a video grabber card installed (TV3300-3314 or TVVR95000-TVVR95020), the setup wizard first configures the analog cameras.



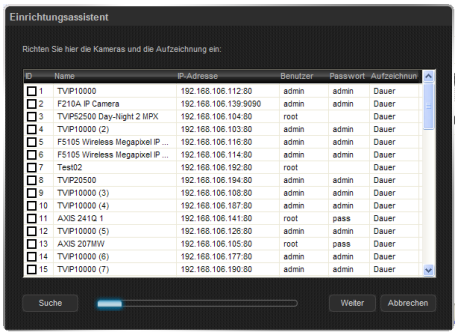
Here you have the option of choosing the cameras that will be used during operation. You can also select the camera recording mode. The options here are:

- None (the camera only shows live images)
- Permanent (the camera images are permanently recorded)
- Motion (the camera images are only recorded when motion is detected)

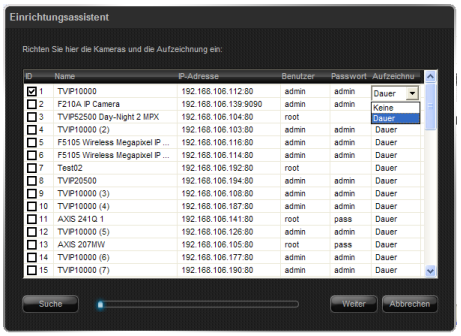
Make the settings are required and click *Next*.

The next window is for setting up IP cameras. First, the program looks for all the IP cameras in the system and lists them in a table.

If your IP camera is not listed, make sure that the camera is in the same network and has been assigned a valid IP address. If necessary, click *Search* to perform the search again.



Activate the cameras for displaying and recording by selecting the checkbox in the *ID* field of each camera.



If a user-defined password is used for the camera, you are prompted to enter the user name and password for the camera in order to activate it. There is also an audible signal.

Only when authentication is successful can the camera be used and the check mark appears in the *ID* field.

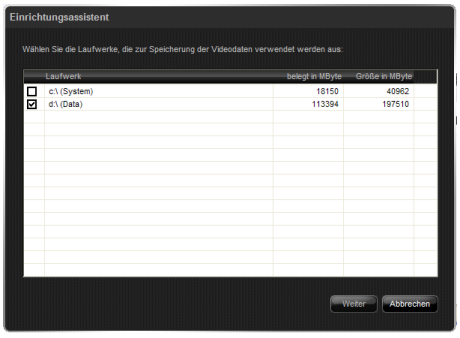
You can now define the recording mode for the camera in the Recording column. However, you can only select no recording or permanent recording here.

If you want to record after motion is detected, you must select this later in the system configuration (see section 3.2.3 on page 55), because motion detection first has to be activated using the camera's web interface. You will find more information on this in the instructions for the camera.

Once you have completed the network camera configuration, click *Next*.

Note:

Pan/tilt network cameras are detected automatically. If one of these cameras was selected during setup, the pan/tilt function is available as soon as you log in



Next, you must define the storage drives. Choose the required storage drives by clicking the checkboxes next to them.

The size of the archive is then automatically calculated for all the activated cameras. The calculation is based on the following formula:

2/3 of the configured memory space / number of configured archives

For example, if you set up 16 archives and 250 GB of memory space is available, the calculation is as follows: (2/3 * 250) / 16 = ~ 10.5 GB per archive

If you want to add more storage drives later or change the size of the archive, you can do this easily using the system configuration. Then click *Next*.

In the subsequent dialog you can create the users. However, you can only have one user for each authorization level.

The standard authorization levels *Supervisor*, *Operator* and *Guest* have the following privileges:

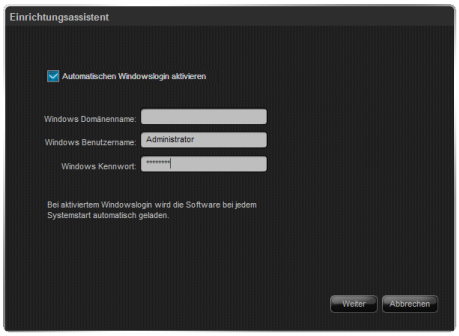
Supervisor - Full access to all parts of the system, including the system configuration

Operator - Access to the live images and recordings of all configured cameras. No access to the system configuration.

Guest - Access to the live images of all configured cameras. No access to the system configuration.

Enter the user names and passwords for the authorization levels that you use and click *Next*. You can use blank passwords.

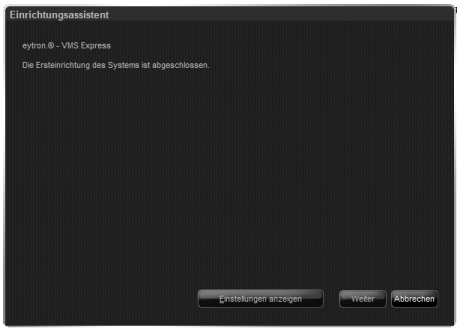
Finally, the wizard offers you the option of carrying out the user login automatically on starting Windows and then launching the program automatically.



You can disable this function in the system configuration later if you need to.

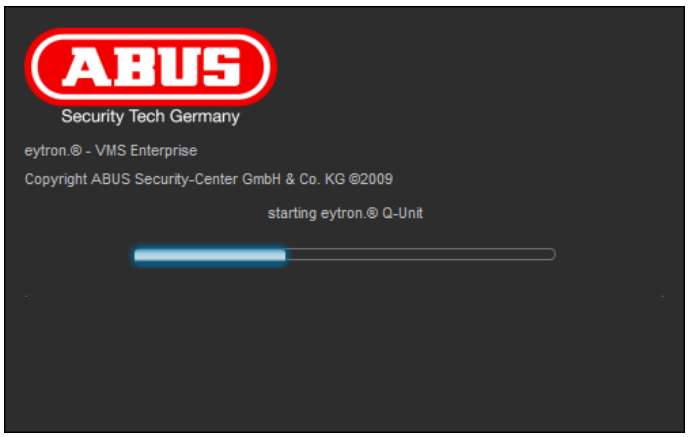
Select the checkbox to activate automatic Windows login and enter the corresponding password in the appropriate fields. Then click *Next*.

The initial setup is now complete. You can click the *Show settings* button to generate an HTML file of all the settings, which can be archived for documenting the system.



You can also create this file later in the system configuration. Section **Fehler! Verweisquelle konnte nicht gefunden werden.** on page **Fehler! Textmarke nicht definiert.** describes the procedure.

Now click *Next* to close the setup wizard and start the program.



1.2 Log-in

When the VMS software has been loaded completely the log-in window appears.

In addition to logging in, the user has the opportunity to select the language of their choice.

The available languages are: German, English, French, Dutch, Danish, Swedish and Polish.

Select a language and enter your user name and password. Then click the *Login* button (key symbol).

1.3 User interface

When the user interface for the ABUS VMS was designed, it was highly important that it should be user-friendly and intuitive. This has resulted in an interface which can be operated simply by left-clicking the mouse (clicking and dragging).

The advantage of this is that it can also be operated using a touch-screen.

Of course, alternative methods of operation are also integrated for more experienced users (e.g. context menus).

The following pages describe how the software is used and configured, thus enabling work to be carried out quickly and professionally.

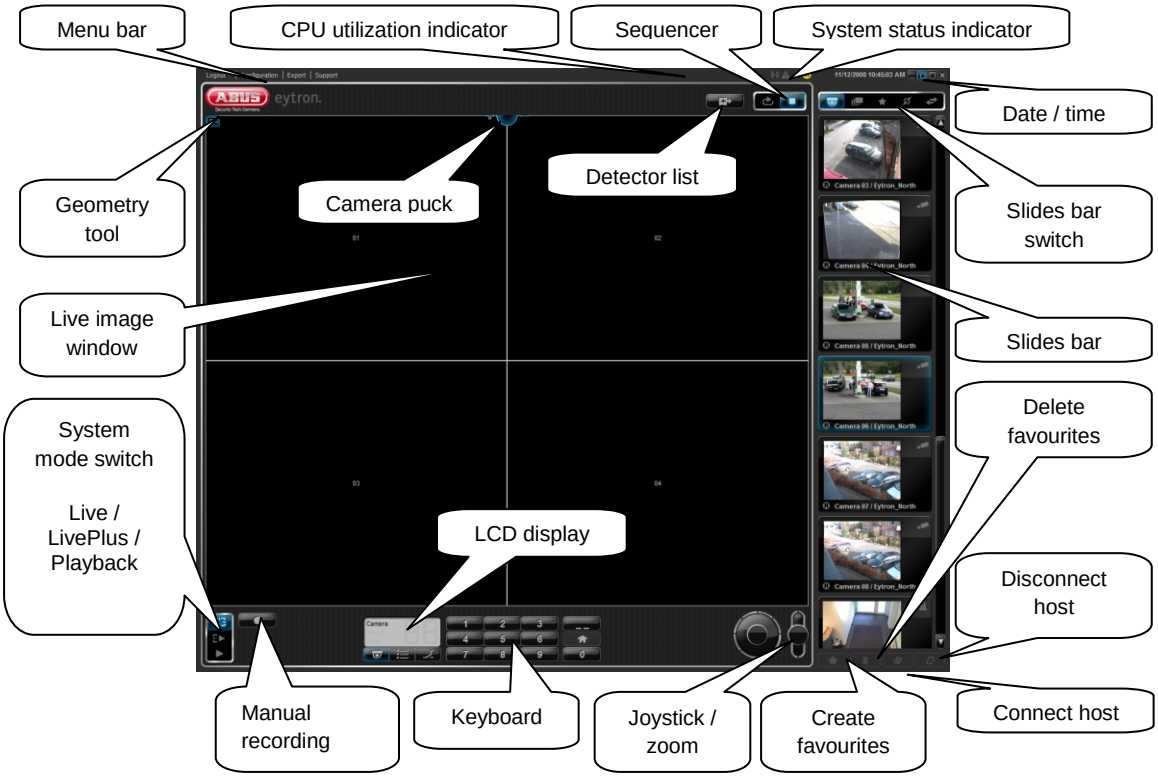
1.3.1 Interface layout

All important functions can accessed quickly with the ABUS VMS interface. By using sliders, the current view can be switched to cameras or hosts, for example. This allows the way that the interface is displayed to be customised, even when several screens are used.

Starting from the top left, you will find a menu bar with buttons for logging out/exiting the software as well as calling up the system configuration, data backup (export) and options for technical support.

Furthermore, the system status indicator and current date and time are found on the top edge of the screen.

The system status indicator is comprised of four symbols which reflect the current state of the system.



A slider is located below the date which switches the slides bar displayed underneath. This tool can be used to switch the slides bar view between the Camera, Camera group, Favourites, Connection map and Host view. This is described in more detail later in the manual.

The slider to the left of it is for activating the sequencer. After activation, the live images from all the cameras are shown in succession.

Start sequencer **Stop sequencer**

The system mode switch in the bottom left-hand corner switches the software to the desired operating mode. The modes available are Live, LivePlus or Playback mode. This is also described in more detail later in the manual.

The button for manual recording (Panic Record) can also be found next to the system mode switch. This saves a recording of all the cameras currently shown. This occurs as long as the button is activated.

The keyboard is used to select cameras, saved camera positions and to switch the set relays. The control buttons below the LCD display switch between the different operating methods. The current selection is shown directly in the LCD display.

The next controls that you will find are the joystick and the zoom controller. These controls allow you to control pan/tilt cameras or, in the case of fixed cameras (analog or network cameras), to digitally zoom into the image and move the enlarged area of the image.

The buttons on the bottom right-hand edge of the screen are used for creating and deleting camera favourites or connecting and disconnecting hosts. The function of these buttons will be described in more detail later in the manual.

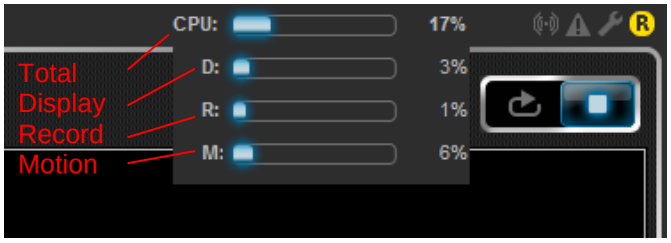
The slides bar located above is used as a recording container for cameras, camera groups and hosts, for example. The higher-level slider switches between the views.

The live image window takes up the majority of the user interface. All cameras to be displayed are located in this area. The camera puck and the geometry cross provide an innovative way of modifying the number of camera windows shown or the current image geometry of the live window. For more information, see point 2.4.2 on page 29.

When 4:3 or 16:10 screens are used, the live window display is automatically adjusted to the appropriate resolution.

1.3.2 The CPU utilization indicator

The CPU utilization indicator displays the current utilization of the processor. If you move your mouse over the display a window opens showing the overall utilization divided into three sections, providing a much more detailed view of the system utilization. As well as the overall display, the system resources required for displaying the live image (Display) for current recordings (Record) and for motion detection (Motion) are shown . This remains on the screen until you move your mouse over the indicator again.



Note:

Because other processes also utilize the system resources, the displayed total utilization (CPU) is never the sum of the values shown for Display (D), Record (R) and Motion (M).

During configuration, make sure the total utilization of the system is not too high, as otherwise it will be difficult to operate the system normally.

1.3.3 The network utilization indicator

The network utilization indicator displays the current utilization of the network adapter. If you move the mouse over the indicator, a window showing the following information opens:

Network

- **Host:**

  Displays a host's received and sent data volume in Mbits per second.

- **LAN1:**

  Displays the first network card's received and sent data volume in Mbits per second.

  Important: For systems with two network connections, the display is divided into LAN1 and LAN2.

Images

- **HD/SD:**

  Shows the compressed data volume and the number of images of the analog cameras.

- **IP:**

  Shows the compressed data volume and the number of images of the network cameras.

- **Live:**

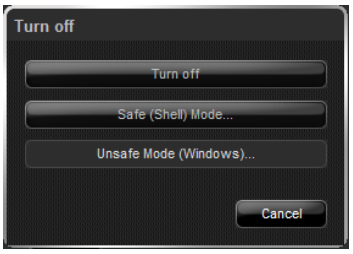
  Shows the decompressed data volume and the number of images in the live view.

Recording

- **Write:**

  Shows the data volume and number of images written to the database.

1.3.4 Logging out and exiting the software



To turn off the software, a logged-in user must first log out. This is performed using the *Logout* button located in the upper left-hand corner of the interface.

When the user has logged out, the button changes to *Exit* and another click results in a dialog where the software can be switched off.

However, to switch off the software, the user has to enter their user name and password once again to prevent the video system from being accidentally shut down.

2. Software operation

Software operation is divided into several steps. This enables the user to better understand the software and to apply it more effectively. In the following pages, you will become familiar with the software's basic operations.

2.1 Switching system modes

The slider in the lower left area of the screen determines the basic software functionality. There are three categories, each one standing for a specific operating mode. These are described in more detail further on in the manual.

When you switch to another mode, the system saves the current view in the background. This view (camera positions) is automatically restored when you return to this mode.

Live mode

Live mode is used for viewing what is currently being monitored by the system's cameras. These can be cameras at the local station or at another host.

In addition, you can create favourites, generate connection and camera maps or activate the sequencer in this mode.

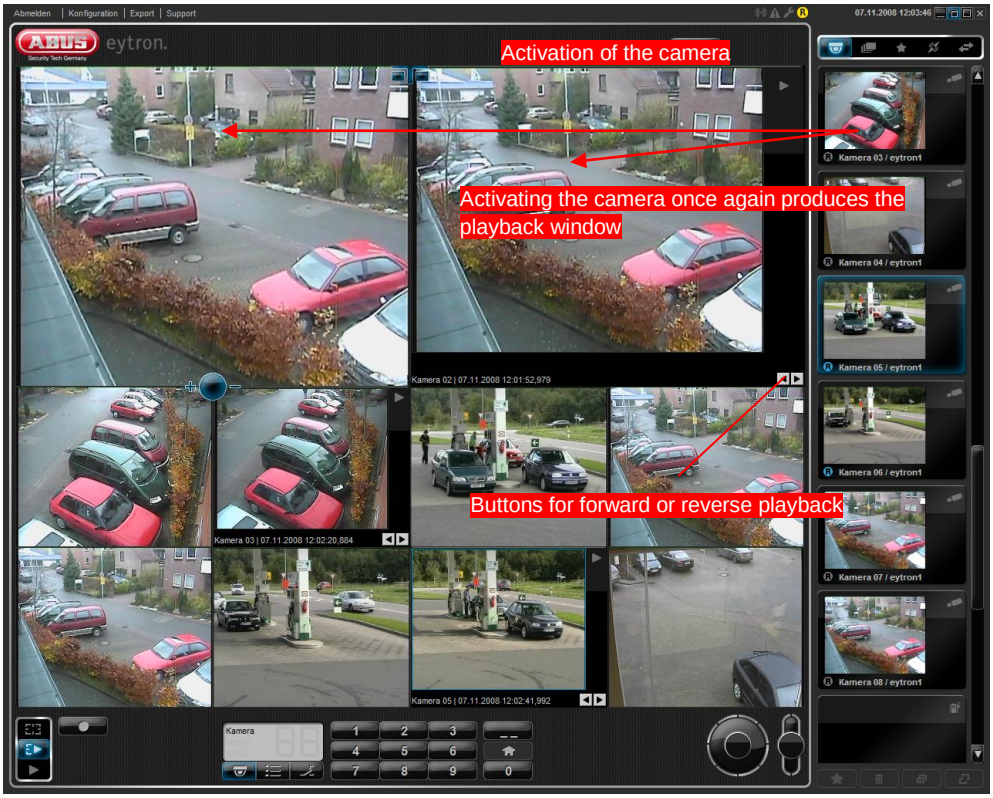
It is not possible to access the database in Live mode.

LivePlus mode

LivePlus mode is a combination of Live mode and Playback mode. Here, the user is given the opportunity to start a playback of the database in addition to showing the live cameras.

If an activated camera is placed in the live image window in this mode again, the playback window for this camera is opened.

The playback buttons in the playback window can now be used for forward or reverse playback.



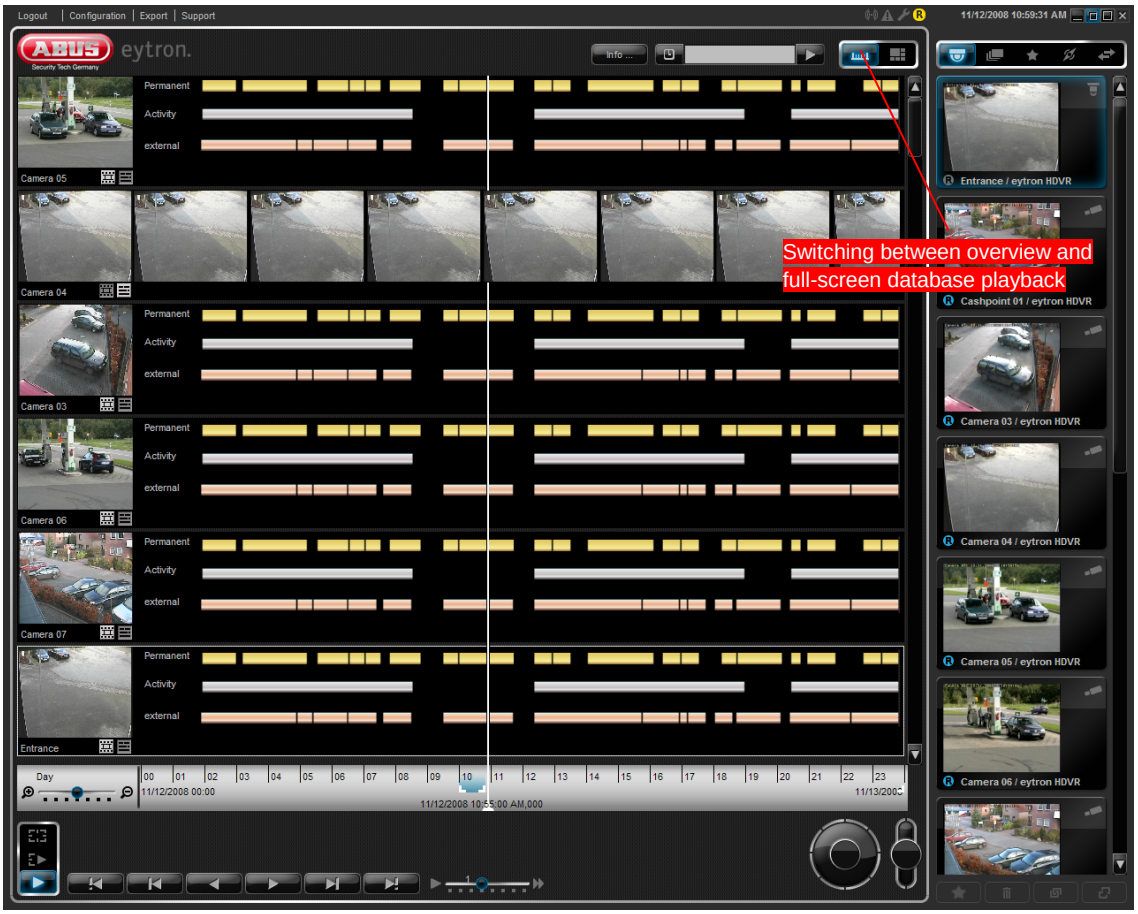
Playback mode

When switching to Playback mode, the keyboard at the lower edge of the screen is replaced by the playback controls. A time stream is also added to the interface, which is used for selecting when playback starts or defining the backup period.

All activated cameras are now transferred from Live mode to Playback mode and an overview window with the current recording statistics is displayed.

This overview can be used for showing the current recording period with permanent recording, as well as recordings with activity detection and recordings of external data (e.g. ATM).

The bar view is used to show the current recording. There is a distinction here between constant recording (yellow bar), recordings after activity detection (gray bar) and recoding of external data (copper-colored bar).



The slider for starting the sequencer also has a new function in this mode. It is no longer used here for starting the sequencer but for switching between the recording statistics (bar view) and full-screen database playback.

If any cameras are already activated when the system switches to database playback, these cameras are used for playback (synchronous playback).

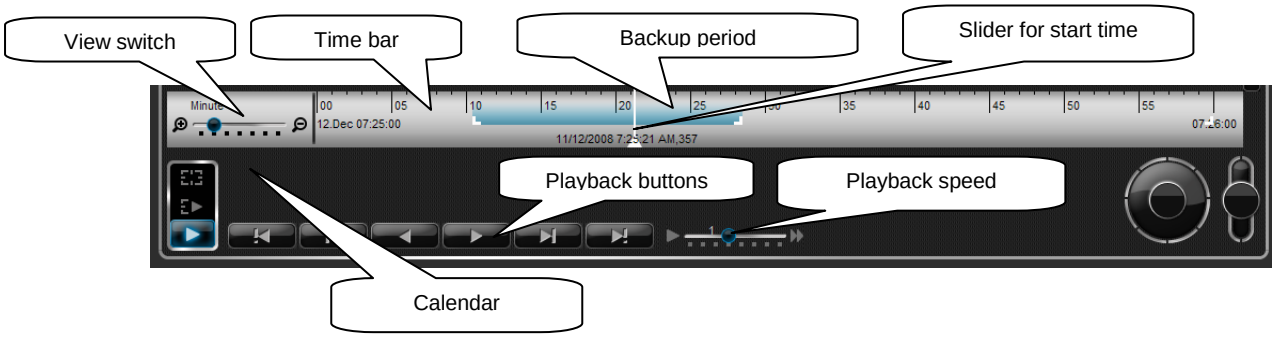
The list of cameras (slides) is replaced by the list of all existing archives. The advantage of this is that if a camera's images are saved to more than one archive, they can also be activated separately.

The view selector on the left of the timeline is for switching the current period for playback. You can switch this between *Year, Month, Week, Day, Hour* and *Minute*. The timeline caption (units) changes according to the position of the slider (see the illustration).

The start time controller defines the absolute start time. If the start time is to be a certain date or time, move the slider to the required starting position by clicking and dragging it. Note that you may have to first switch to a higher-level view (such as Month or Day) to select the starting point.

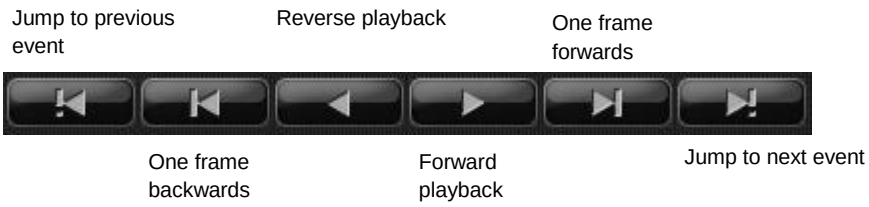
You can select the start time (date and time) directly using the calendar function. For example, if you want to go directly to the end of the current recording you only need to open the calendar and click *Today*. After you close the calendar, the slider for the start point jumps directly to the current date and time.

Open the calendar by clicking the calendar button in playback mode.

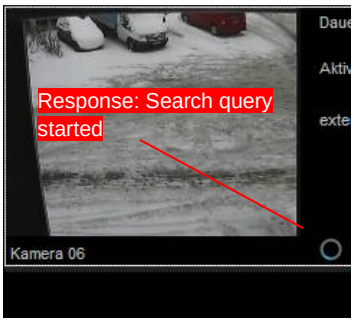


The selected cameras can now be played back using the *Forward* and *Reverse* buttons. The playback speed can also be set to between 1/20 and 40x using the speed controller.

The following graphic shows the meaning of the individual playback buttons.



When you use the *Skip to next/previous event* buttons, the search query may take a moment longer. If so, an indicator showing the current query status appears below the *List view* camera display in playback mode. Once the database query is complete, this indicator disappears again and the system skips to the next event.



Note:

If there is no recording present for the period chosen, a blue image with the caption "No video" is displayed instead of the video image.

2.1.1 Using the search function

The search function provides quick and easy access to the stored data.

Possible search criteria include the time, date, ATM data (transaction number, bank sort code, amount etc.), camera or detector name.

To carry out a database search, set the mode selector to playback.

Activate the cameras that you want to include in the search.

Use the search bar to select the search criterion (e.g. time).

Enter the time for the search in the field and click *Start search*.

Note:

When entering search criteria, no particular format is required. For example, if the search is for a particular time, then this can be entered as a time (e.g. 23.15) or as a sequence of numbers (2315).

If matching data is found, the slider for the start point jumps to the time entered.

2.1.2 Voiding archives

If the image data saved in an archive is no longer needed, it is possible to void this archive.

To do this, switch the mode switch to *Playback mode*. The *Info…* button now appears on the upper edge of the screen.

With this button, the operator can see how full the archives are in general and void individual archives.

Highlight the archive that you wish to void and click the *Empty* button. Answer “Yes” to the subsequent confirmation prompt.

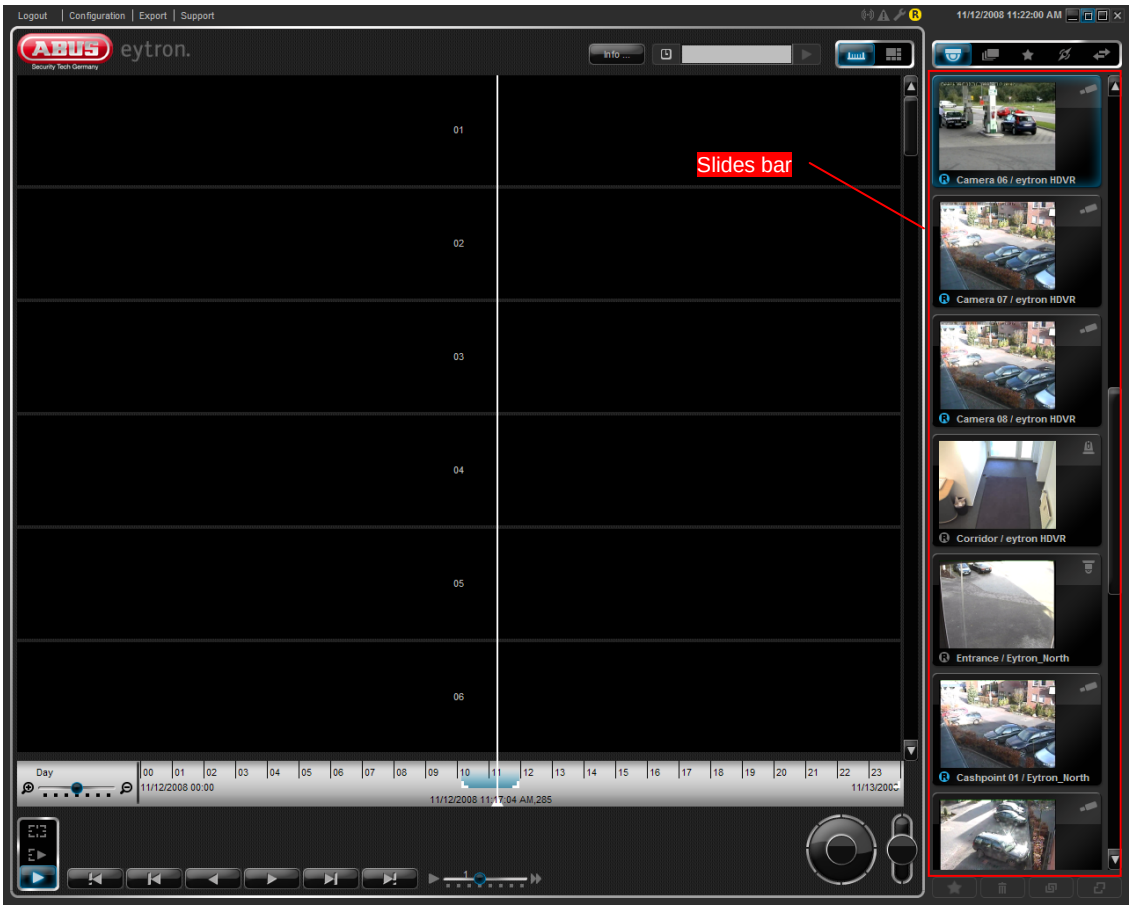
This voids the archive.

2.2 Switching the slide elements

The content of the slides bar is switched using the higher-level slider. This procedure replaces the slides currently shown on the right-hand side with slides in the category selected.

For example, if the cameras category is switched to hosts, the camera slides are replaced with slides from the available hosts.

The individual views are described in detail below.



Camera view

The “Camera” view is always the standard view for the software. All activated cameras and connected hosts are listed here. If, for example, the system is restarted or exited, this is the view that is always shown to begin with.

It is also possible to obtain additional information from the slide, such as the camera type, name and recording status.

Camera group view

In the “Camera group” view, entire sets of cameras can be activated at once. For example, if a camera group referred to as “Outdoor cameras” is set up, all the empty windows in the live image area are filled with the cameras from this group when the group is activated.

If there are more cameras in the group than can be displayed in the live image area, the remaining cameras are ignored.

Camera groups can be created in the system configuration under *Camera* → *Camera groups* (see 3.2.9 on page 73).

Favourites view

The “Favourites” view contains all the saved camera favourites. These can be created and individually named by any user with the button (on the bottom right-hand edge of the screen). This generates a user-defined list of camera sets.

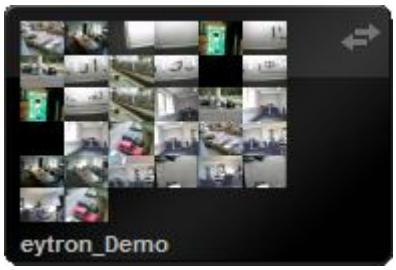
This facility is different from the camera groups because the current view and image geometry are also saved when favourites are created.

Furthermore, when a favourite is activated, the current live window view is replaced by the view saved in the favourites.

A detailed description on creating favourites can be found under 2.6 on page 41.

Host view

All the set hosts are listed in the “Host” view.



In this view, each host has its own slide showing a preview of the local cameras on the host.

This view is always used to call up a host.

You can find further information on selecting hosts under point 2.6 on page 42.

2.3 System status indicator

The current system status can be seen with the system status indicator. This is depicted by four symbols.

These symbols are also located on the front of the ABUS HDVR / NVR housing, and use LEDs to reflect the current system status.

The symbols are as follows:

Alarm (lights up as soon as an alarm is received (e.g. over an external detector))

Fault (lights up if a fault occurs (e.g. camera failure))

Maintenance (lights up when maintenance interval is reached)

Recording (lights up as soon as video data is recorded)

The system status always relates to the local system only. It is not possible to display a remote system status.

2.4 Working with the cameras

Providing they are set up in the system configuration, any cameras connected will be listed in the Camera view. Each slide shown represents a camera.

The camera type is indicated by the camera symbol on the top right-hand side of the slide. This can vary as follows:

Pan/tilt camera

Pan/tilt camera with network connection

Network camera or video server

Analogue camera

The camera name and host name are always displayed at the bottom of the slide. It is therefore very easy to assign the listed cameras to the relevant host.

If the camera is recording, the Record symbol appears in the slide.

Information on setting up further cameras can be found under 3.2 on page 51.

2.4.1 Activating and deactivating the cameras

Simply drag and drop a camera into a free live window to activate (switch on) the camera.

Switch the mode switch to *Live* mode (step 1).

Next, switch the view switch to the *Camera* view (step 2).

In the Camera view, click the slide of the camera and keep the left mouse button pressed.

Now move the mouse to a free camera window and release the left mouse button. The camera is then embedded in the window (step 3).

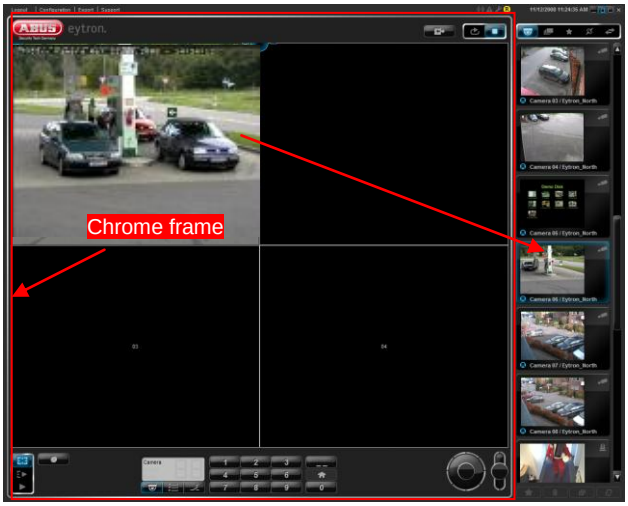
If you wish to embed the camera in another window, you can again use the drag and drop function to move the embedded live image to another window.

If an activated camera is moved to an occupied window, then the cameras swap positions on the screen.

If a camera from a camera list is released over an occupied window, the existing video image is replaced with the image from the new camera.

To deactivate (switch off) a camera, simply release the camera outside the chrome frame using drag and drop. We recommend dragging the camera back to the slides list.

Camera groups or favourites can be used to activate more than one camera at the same time.



From version 7.3 onwards, you can reposition the individual slides using the drag and drop method. Your individual user settings are saved each time you log off.

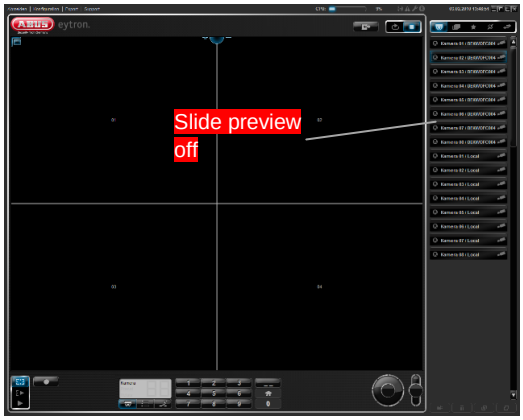
As well as this, you can activate a camera by double-clicking the corresponding slide.

Note:

Each camera can only be displayed once on the screen at all times. This applies to each screen in multi-monitor operation. Depending on your particular version, a camera can be displayed up to four times in Live mode.

If there are very many cameras in the list, the preview image on the slides may be disabled. This is to provide a better overview when one receiver. for example, is connected to several hosts.

To disable the preview image, right-click a slide in the list and select *Preview* in the context menu. You can enable or disable the preview at any time using the context menu.



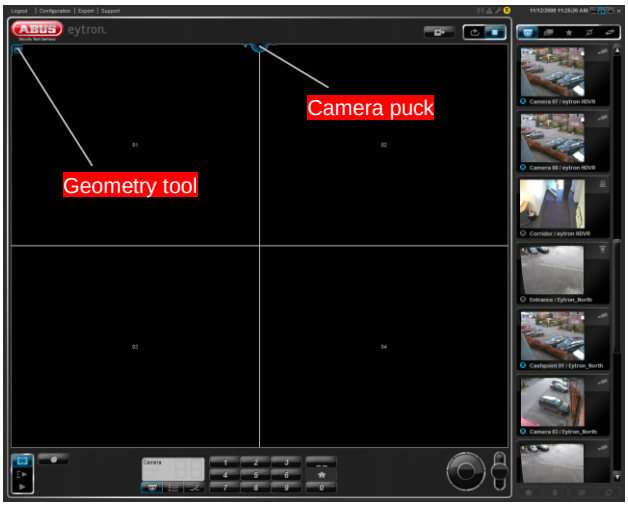
2.4.2 Switching the image geometry

The ABUS VMS software has two tools to switch between camera views. The first of these is the geometry tool and the second is the camera puck.

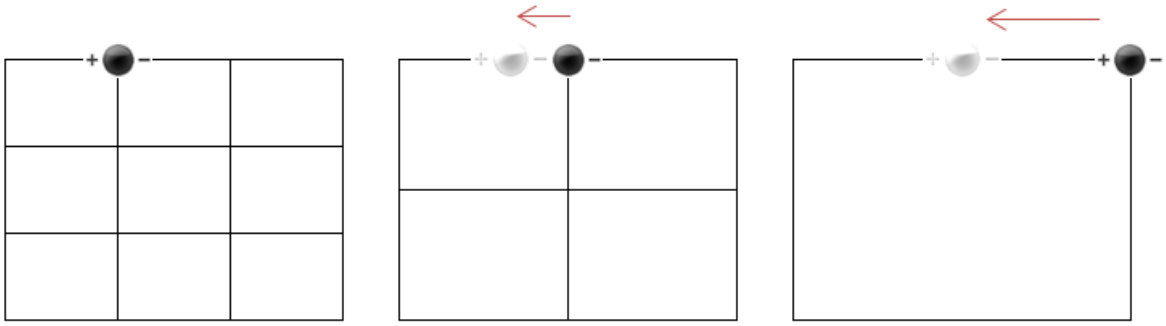
By changing the position of both tools relative to each other, a total of 72 views in 4:3 and 72 views in 16:10 can be displayed. The views are only switched once the mouse button is released.

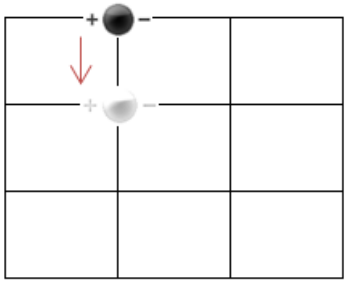
The set view is saved when you exit the software and is automatically reproduced when the software is next started.

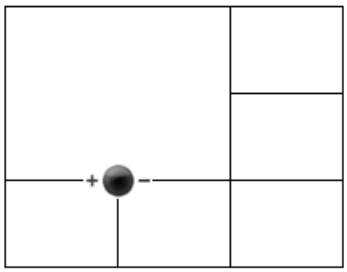
A more detailed description on how to use these tools can be found below.



Working with the camera puck:







The camera puck is used to increase and decrease the number of camera windows. For example, if more free camera places are required, the puck must be moved along the horizontal plane towards the plus sign (in quadratic view).

If the puck is moved along the vertical plane, the current view is changed to the *1Plus view*. The further the puck is now moved away from the geometry tool, the larger the *1Plus window*.

If more free windows are required again, then these can be created by moving the puck along the horizontal plane (+/-).

Working with the geometry tool:

The geometry tool is used for displaying the Quadratic, 1Plus and 2Plus views as well as reflecting the current view.

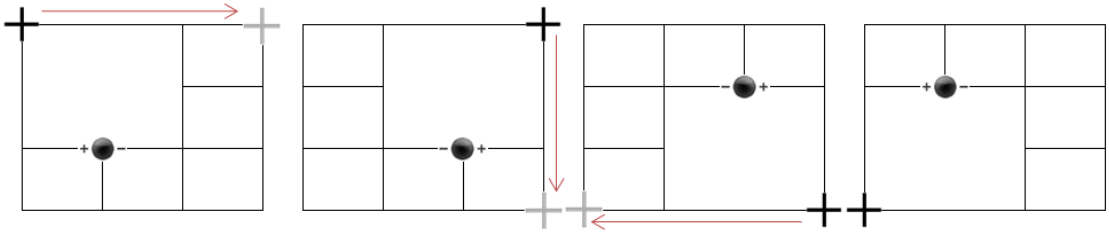
If the geometry tool is in one of the corners of the live window, the Quadratic and 1Plus views can be displayed with the camera puck.

If the tool is positioned in the centre and on the edge of the live window in the horizontal or vertical plane, then the 2Plus view is shown. However, it is not possible to switch to 2Plus mode from every view.

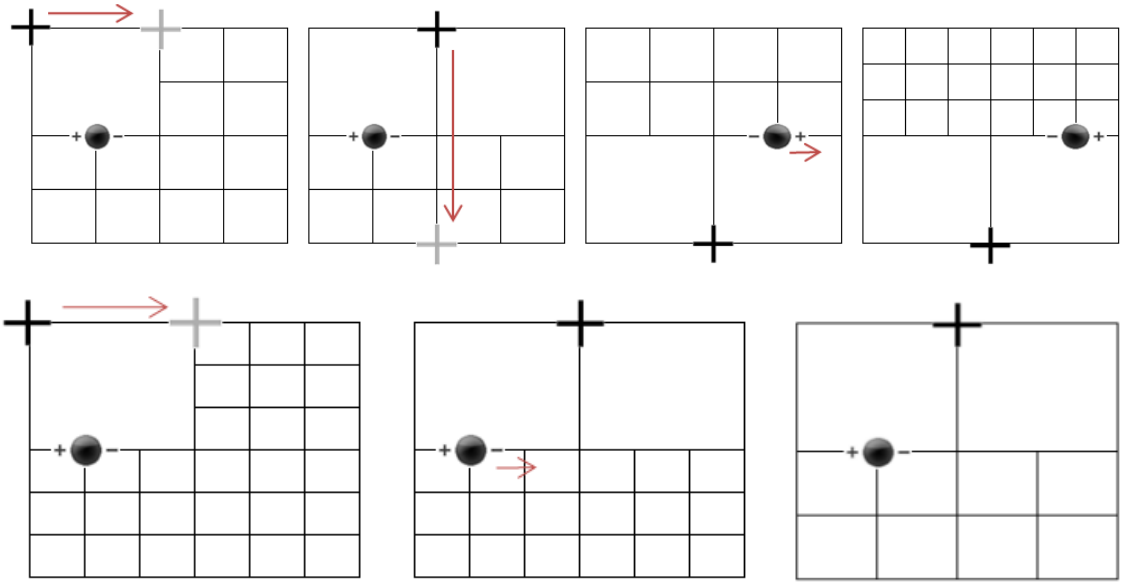
To activate the 2Plus view, proceed as shown in the illustration *Displaying the 2Plus view*.

The current view can be reflected by moving the geometry tool to the opposite side.

Reflecting the current view



Displaying the 2Plus view



The 2Plus view can only be displayed from a symmetrical 1Plus view.

This means that the system can only switch to 2Plus mode if the first 1Plus window can fit next to it again.

2.4.3 Using the zoomstick

The zoomstick on the lower right-hand edge of the screen is used to control pan/tilt cameras.

This allows the direction of the cameras to be variably adjusted (horizontally, vertically and diagonally).

However, only the camera currently selected can be directed in this way. This is shown by a red frame in the live window.

To direct another camera, left-click that camera's live image in the live window section.

Alternatively, the camera can be selected with the numeric field. To do this, the number of the camera to be activated must be entered.

The current image section can be enlarged by means of the zoom controller. If a pan/tilt camera has been selected, the camera's analogue zoom is used. With fixed cameras, the image is zoomed in on digitally.

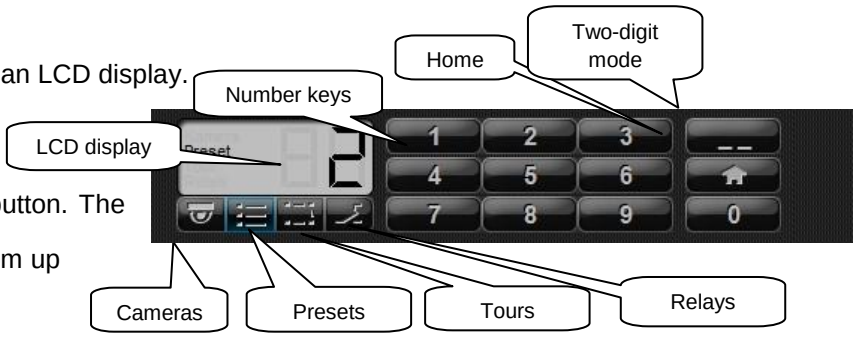
You can then move the enlarged section of the image using the arrow buttons.

2.4.4 Using the numeric field (keyboard)

The numeric field can be divided into four separate modes of operation. These are camera selection, selection of pan/tilt presets (saved camera positions), selection of tours and relay activation.

The current selection is shown in an LCD display.

The input mode can be changed to two digits using the button. The operator can therefore choose from up to 99 entries.



You can call up tours 1 to 8 of analogue cameras by clicking the button. You can also open and use the on-screen display (OSD) of each analogue camera.

The *(Home)* key moves the pan/tilt camera back to its starting position. This is particularly useful if a camera has been moved and the operator no longer knows its starting position.

2.4.5 Saving camera positions (presets)

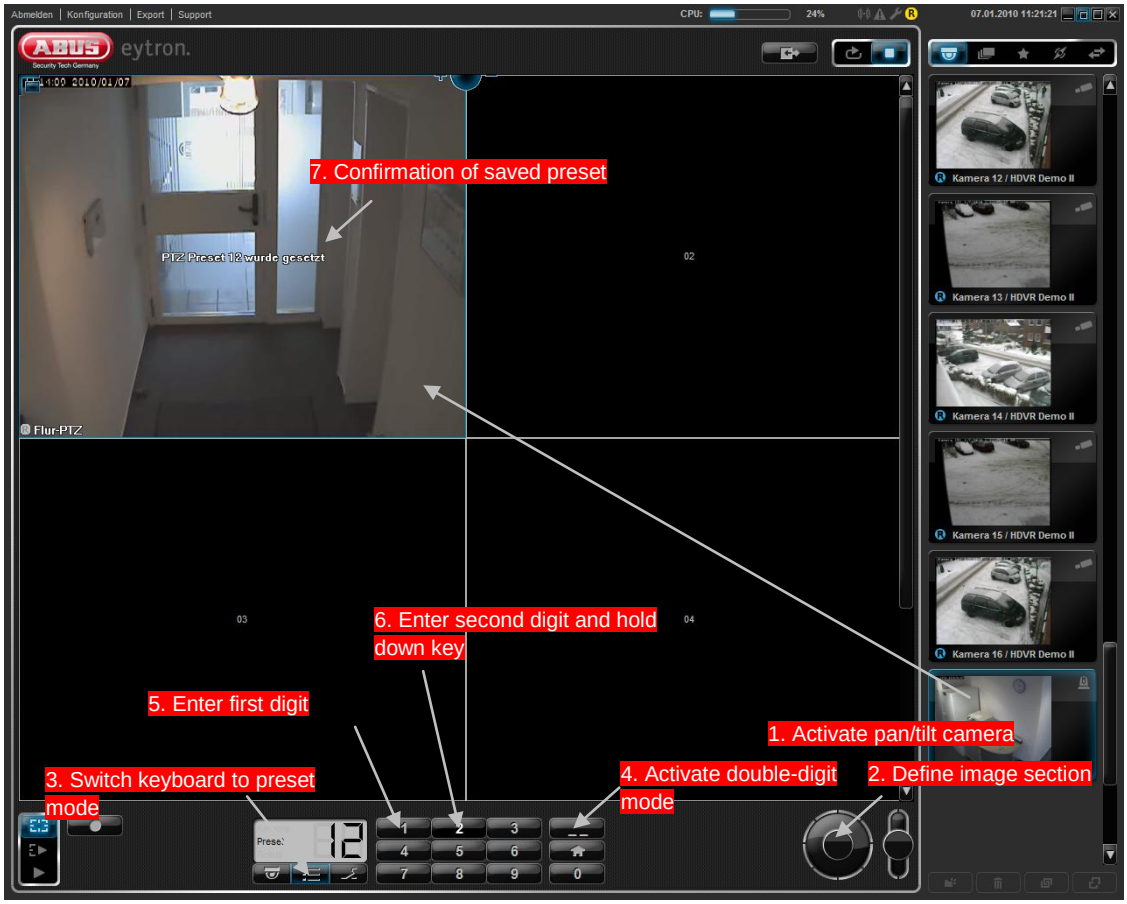
The presets can be used to save and call up specific positions for pan/tilt cameras. Presets are saved by pressing and holding down a number key while preset mode is activated (see **Fehler! Verweisquelle konnte nicht gefunden werden.**). You then receive confirmation on the live image of the camera (e.g. Preset 1 has been set).

Note:

The message that the preset has been saved does not appear until the command has been sent to the camera. This can sometimes take up to 10 seconds.

If you save more than nine presets, click the button to move to double-digit mode. Then save the preset by pressing and holding the number key after entering the **second** digit.

Example – saving present number 12:



2.4.6 Using the sequencer function

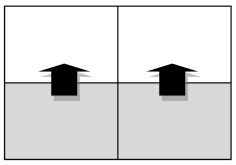
The sequencer is used to display all the cameras in the camera list one by one.

It does not matter whether the cameras are in a local or remote system in this case.

The sequencer can be influenced by changing the image geometry. For example, if you are in the quadratic view (4, 9, 16, 25 or 36 cameras), all the live image windows are moved upwards line by line (see graphic). If the height of the view has been set in such a way that all the cameras can be shown at once, the sequencer swaps the positions of the images.

If 1Plus view is activated, the cameras in the small windows are swapped in succession with the large window.

The default sequencing interval is 5 seconds.



Images moved line by line in quadratic view

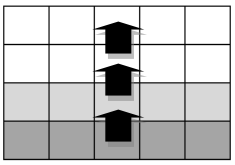


Image swap when all the cameras are displayed in a high view

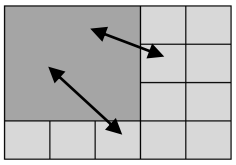


Image swap when all the cameras are displayed in 1Plus view

Note:

Sequencers can only be activated in Live and LivePlus mode. If the software is in Playback mode, the slider is used to switch between database playback and recording statistics and the sequencer is deactivated.

2.4.7 Using manual recording (Panic Record)

Activating the *Manual recording* button ensures that recordings are made from all the currently activated cameras. This occurs until the button is switched off again or Playback mode is selected.

It is then possible to watch the recordings in Playback mode.

For each camera that was active during recording, there is now a recording in that period. This is shown in the recording statistics.

Manual recording **On**

Manual recording **Off**

2.4.8 Using the alarm lists

The alarm lists help users to monitor detector activity. If an alarm list has been created in the database settings, it can be linked to any detector. Every time a detector is triggered, an entry is generated in the alarm list.

Configuration

To create an alarm list, open the system configuration and set the view selector to *Database/saving (see section 4)*.

In the list on the left, select *Archive* and click *New* to create a new archive.

Give the archive an unambiguous name and specify the required memory size.

Finally, select the archive type *Alarm list* and save the settings. The alarm list has been created.

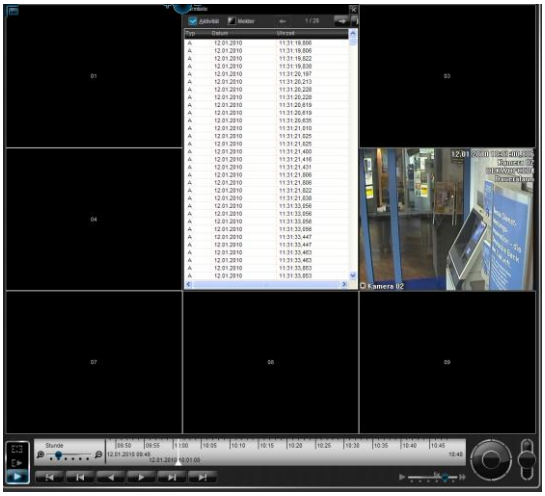
In order for entries to be generated in the alarm list, you must activate the required detectors and link them to the alarm list using the *Activations* item. For more information see section *3.5* on page *102* and section *3.4.9* on page *98*

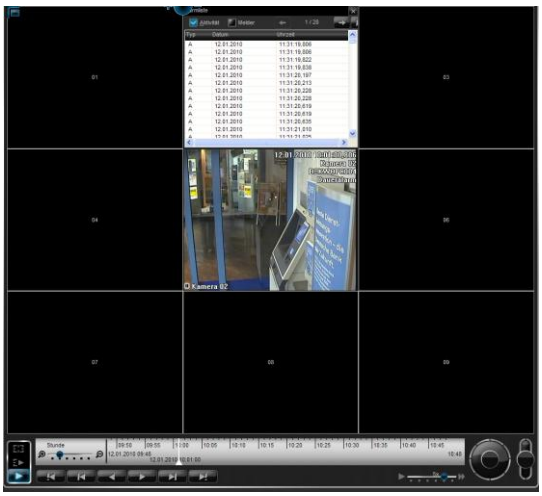
Use

If an alarm list has been configured in the system, it appears as a slide in the camera view. Like the cameras and recordings, you can activate the alarm list using your left mouse button (see section **Fehler! Verweisquelle konnte nicht gefunden werden.** on page **Fehler! Textmarke nicht definiert.**), by dragging it to a free camera window.

Note, however, that the alarm lists can only be activated in full-screen and list view playback mode.

If there is another free field below the camera window (in full-screen mode), the alarm list always occupies two windows at the same time. This gives you a clearer view for evaluating the entries. If not, it is only displayed in one window. Use the following illustrations for this.





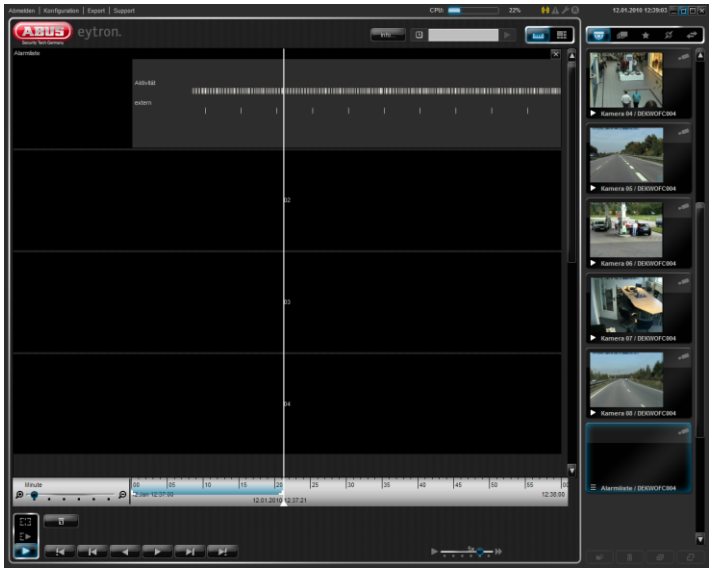
Free field available

No free field available

The alarm list also gives you the option of filtering the entries using two checkboxes. These are for the motion alarms (activities) and external alarms (detectors).

If the alarm list is activated in list view playback mode, you will see statistical summary of the alarms that have been triggered. Motion alarms are shown in gray and alarms from external detectors in copper-color.

Virtual alarms and the detector inputs on the alarm card can be used as external detectors.



Clearing alarm lists

If the entries in the alarm lists are no longer needed, you can clear them by clicking the Info button (in playback mode). However, only users with the appropriate authorization can do this. For further information on see section **Fehler! Verweisquelle konnte nicht gefunden werden.** on page **Fehler! Textmarke nicht definiert.**.

2.5 Creating backups

The backup dialog can be called up easily using the Export button on the top left-hand edge of the screen. Single-frame export, AVI export and database export are possible. In addition, you can print out individual frames or send them by e-mail.

There is a difference between local and remote backup. The variations are explained in more detail below.

2.5.1 Local backup (database export)

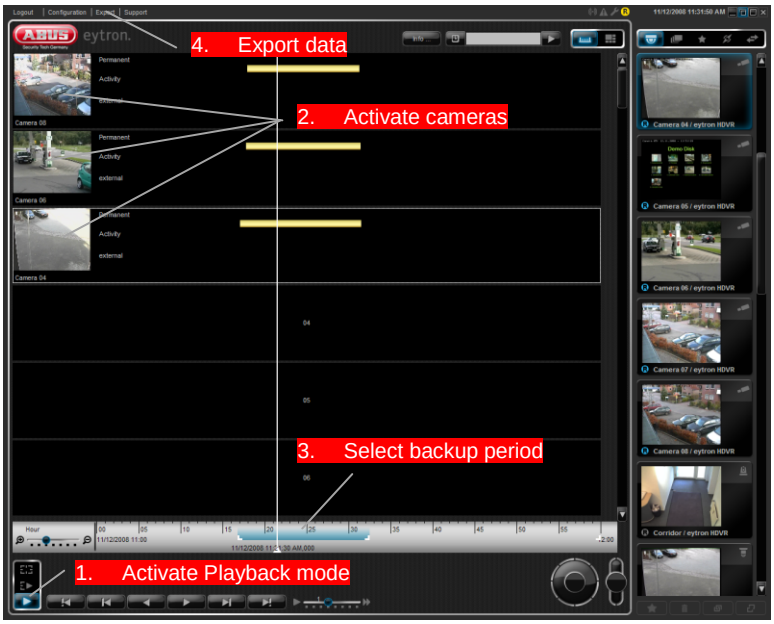
A local backup saves the recorded video data from the local system onto external media. These include USB sticks, CD/DVD or an export to a separate directory.

To export the video data, insert a disc in the DVD burner or attach a USB stick.

Change to Playback mode and activate the cameras to be used for the backup. When doing so, make sure that only the cameras to be backed up are activated, as otherwise any cameras not needed will also be backed up.

Specify the time period to be backed up using the selection tool and click the *Export* button.

The Export dialog is now started in the *Database export* view and the archives selected from the list are displayed. The selected backup period is also taken from the client and updated in the list.



If the operator wishes to use another name for the backup, this can be entered in the *Name of backup* field.

In the Export dialog, select the drive to be used for the backup. If the drive is not listed here, you must first set it up in the system configuration (*Database/Storage → Drives*) as *Backup read & write* (see point 3.3.1 on page 69).

When all the settings have been made, the backup can be started using the *Export* button.

The reader software is also automatically copied on to the storage medium at the end of the backup process (database export only). This enables the image data to be viewed on any Windows PC (Windows XP and higher).

Compared to the main software, use of the reader software is highly limited. Only the database playback functions are implemented.

If the data was backed up on CD or DVD, the reader software is automatically started immediately after the disc is inserted.

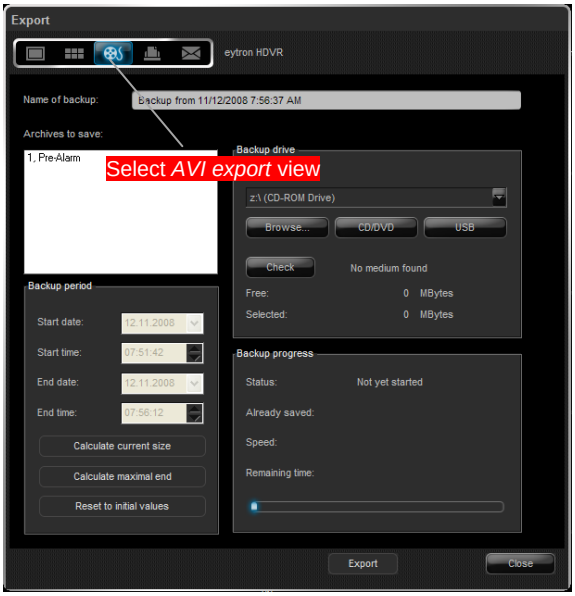
2.5.2 Local backup (AVI export)

The AVI export enables the recorded image data to be exported in a video format. This can then be played back using a normal media player. Reader software such as that used for exporting a database is not needed for playback.

If your program has difficulty playing the data, check that a corresponding codec for DivX or XVid (e.g. K-Lite codec pack) is installed. Further information can be found in the manual of the media player.

The procedure for exporting video data is the same as described under 2.5.1 except that *Database export* (point 2) is selected instead of *AVI export* (point 3) in the backup dialog.

If more than one camera is activated during backup, a separate video file is created for each of these cameras.



2.5.3 Remote backup

The remote backup enables image data from a connected host to be backed up.

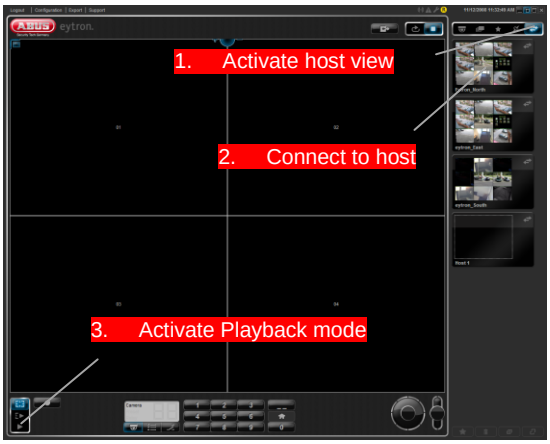
However, the host must be connected before the backup dialog is opened.

Switch the view switch on the client interface to the *Host* view and select a host (further information on selecting hosts can be found under point 2.7 on page 44).

Now change to Playback mode and activate the cameras of the host to be used for the backup. Ensure also that no other cameras are activated, otherwise they will be backed up as well.

Perform all further steps as described under point 2.5.1 (local backup).

A combination of cameras from the local station and host is also possible.



2.5.4 Single frame export (storage, printing, e-mailing)

The single frame export can be used to save, print out and e-mail single frames from the database or live image display.

If needed, the station name, camera name and date and time can be shown in the image directly.

The possible settings available here are described in more detail below.

Storing single frames:

To export single frames, open the export dialog at the top left-hand edge of the screen in the client interface and switch the export mode to *Single frame export* (point 1).

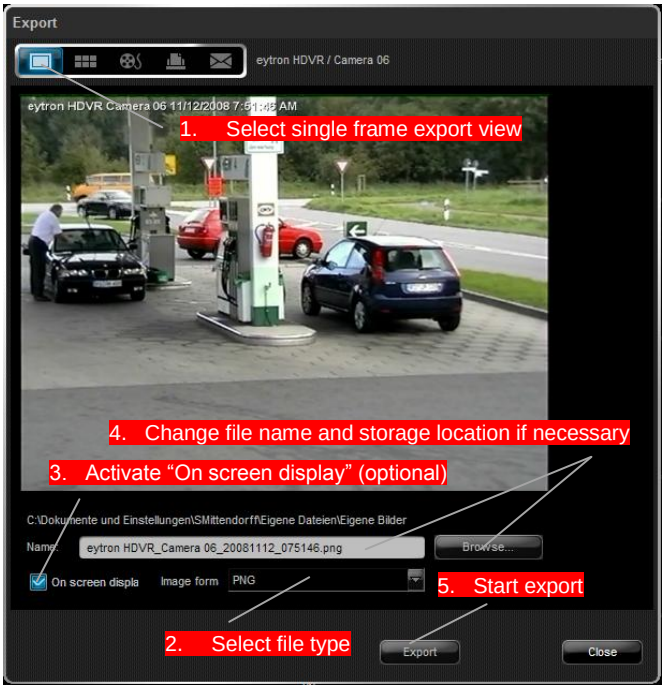
The image to be exported is now displayed as a preview.

Select the file type and check the “On screen display” box if the camera name, date and time are to be contained in the exported image.

The default folder for the images is the *My Pictures* folder. If you wish to save to another location, you can use the *Browse* button.

Click the *Export* button to start exporting. The image is now saved to the location selected and the export dialog is closed again.

Repeat the above steps to export further single frames.



Sending image data to a printer:

If you wish to send single frames to a printer, you only need to select printer export (point 4) instead of the single frame export (point 1) in the export dialog.

If necessary, the printer can be changed with the *Printer setup* button.

Click the *Export* button to send the image to the printer.

If a printer has not yet been set up, the Windows wizard appears for setting up a new printer. Follow the wizard’s instructions for adding a new printer.

Otherwise, select the printer to be used and click the *OK* button.

The image is now sent to the printer.

Note:

The operating system for the ABUS HDVR is on a CompactFlash card. The available memory on the C:\ drive is therefore greatly reduced. When adding another printer, please only install the printer drivers and not the image editing programs or printer management tools.

Sending image data by e-mail:

In addition to e-mail notification (see point 3.7.5.1 on page 124), you can now also send the image data by e-mail.

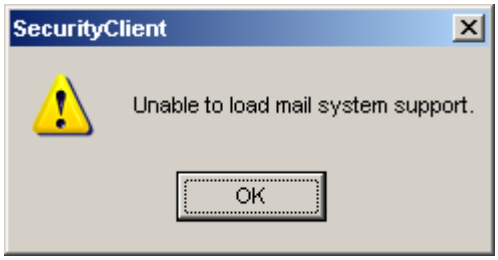
To send an e-mail, switch to Playback mode. Activate the camera to be used for the e-mail and open the export dialog.

Note:

If more than one camera is activated in Playback mode, the export only applies to the active camera. The active camera can also be selected by clicking the preview image.

Switch the option switch to E-mail Export (point 5) and click the *Export* button. However, an e-mail client (MS Outlook or Outlook Express) must be installed to send the images.

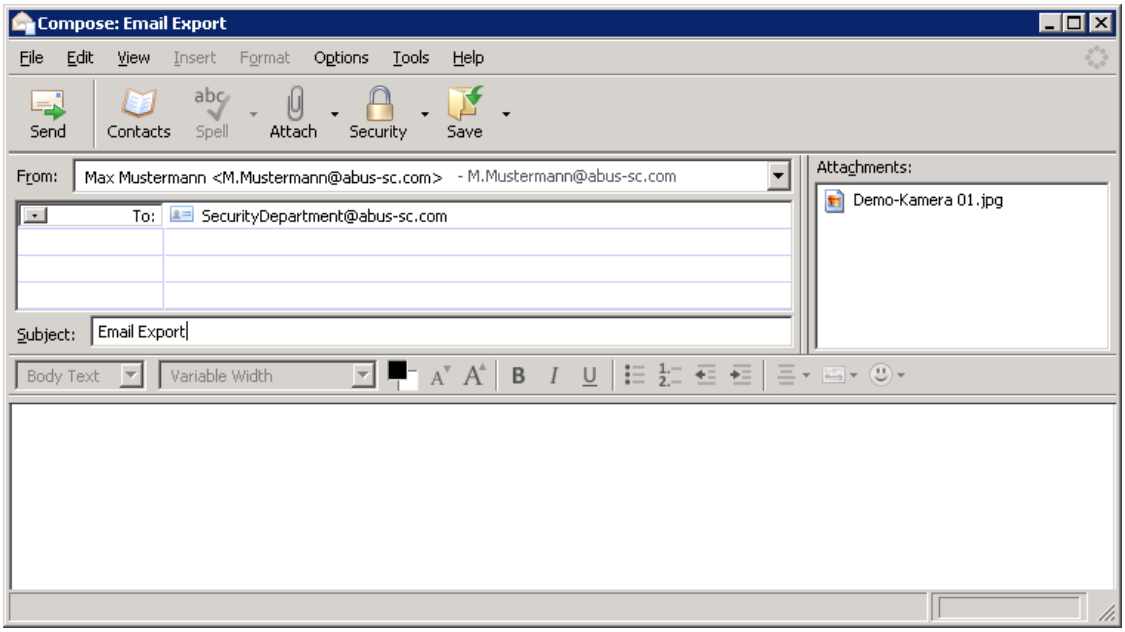
If no e-mail client is installed, the e-mail cannot be exported. You will then receive an error message stating that the mail system cannot be loaded (see graphic).



If an e-mail client is found, it is started and the individual frame is attached to the e-mail.

Complete the message by adding a recipient's address, subject and a message text (where necessary).

Click Send to send the e-mail.



2.6 Creating favourites

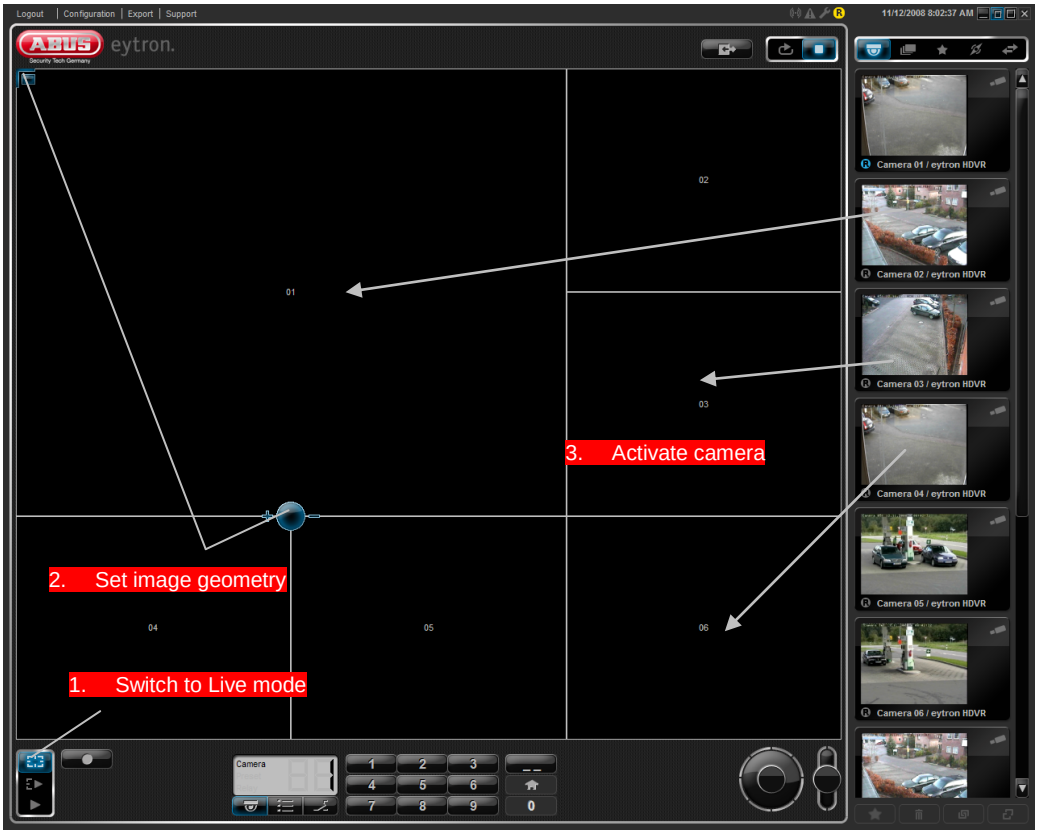
When using several cameras in the ABUS VMS software, it is recommended to save certain camera views as favourites.

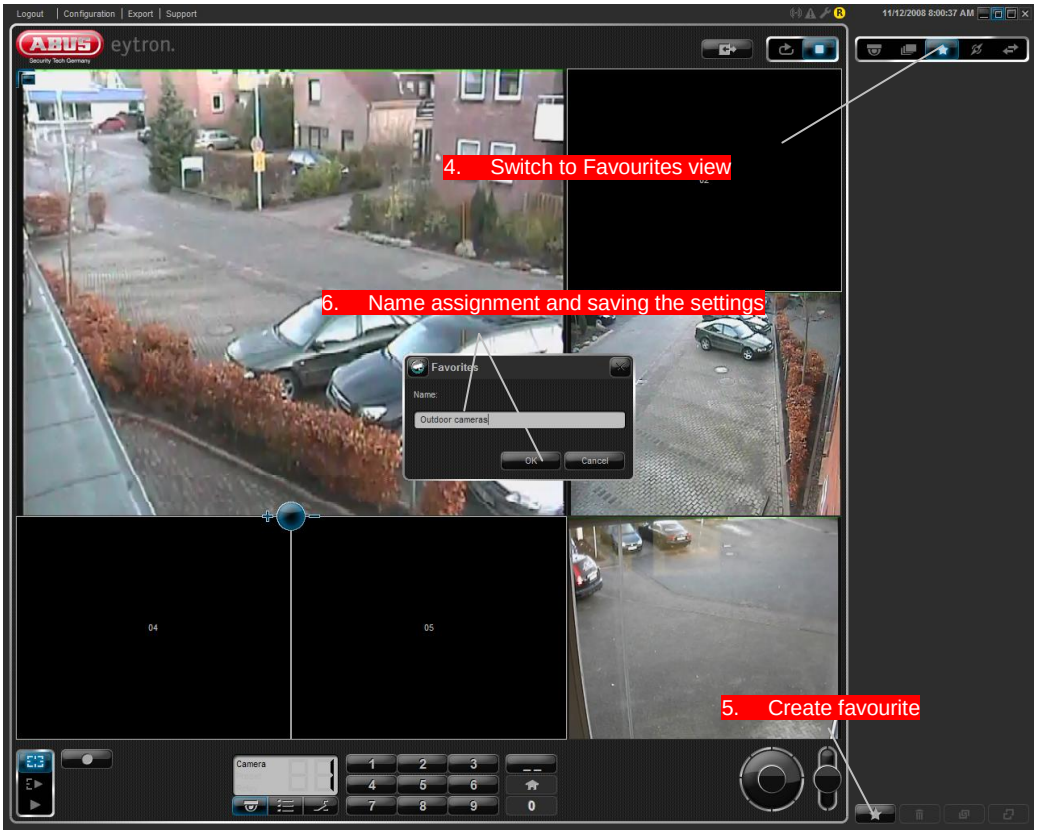
To display the camera again, only the favourite needs to be activated instead of each individual camera.

Another advantage is that the set image geometry is also saved when favourites are created.

The following steps are necessary when creating favourites:

- Switch the system to *Live* mode
- Set the desired image geometry (see point 2.4.2 on page 29: “Switching the image geometry”)
- Activate the desired cameras and define the sequence in the live window
- Switch the view switch to the *Favourites* view (point 3)
- Create the favourites using the *Create Favourites* button
- Assign a name for the favourite to be saved


3. Activate camera
2. Set image geometry
1. Switch to Live mode


4. Switch to Favourites view
6. Name assignment and saving the settings
5. Create favourite
Favorites
Name:
Outdoor cameras
OK
Cancel

After the favourite has been saved, a new slide is added to the favourites list.

When this slide is now dragged into the live window, then the image geometry is changed according to the saved view and the cameras are displayed according to the defined sequence.

In doing this, the existing cameras are replaced.

Note:

Favourites are created separately for each user. This means that favourites cannot be seen by other users when in multiple-user mode. No supervisor rights are needed for the creation of favourites.

2.6.1 Deleting favourites

If stored favourites are no longer needed, then they can be deleted using the button. Switch to the Favourites view and select the slide to be deleted, then click the *Delete* button.

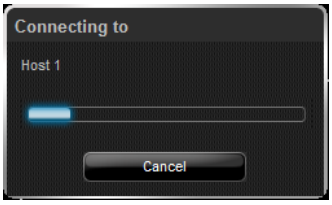
The favourite is then deleted from the list.

2.7 Connecting to a host

You can connect to hosts over the Host view in the interface when hosts have already been created in the system configuration.

To do this, switch the view switch to the *Host* view.

There are three different ways of connecting to a host. Connection is made in the following circumstances:



1. When the host slide is dragged into the live image area (drag and drop).

2. When the host slide is double-clicked.

3. When the host slide is selected and the *Connect* button is clicked.

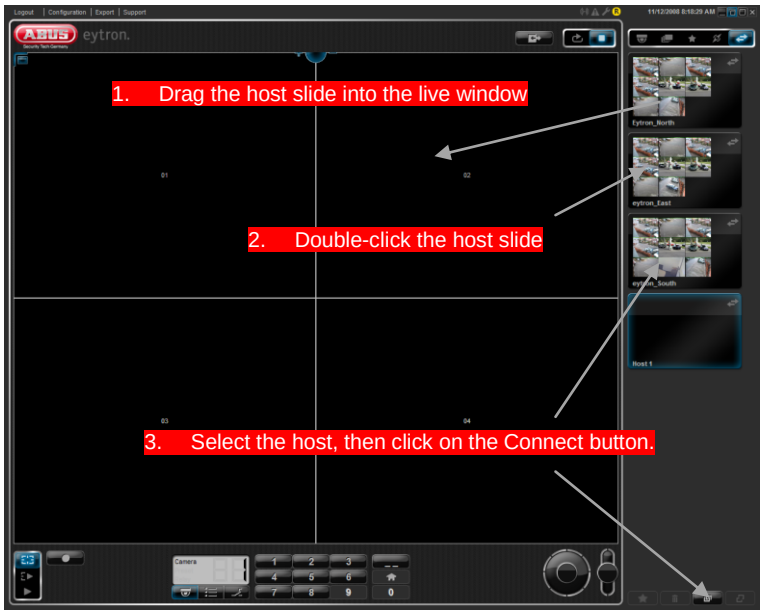
In each of these cases, the progress of the connection is shown in a dialog.

When the connection has been established correctly, the software switches from the Host view to the Camera view. The cameras of the host are now added to the list and can be activated in the same way as the local cameras.

To disconnect the host, press the button *(Disconnect)* in the Host view. To do this, first select the desired host (host slide) from the list, then click on *Disconnect*.

Information on setting up other hosts can be found under point 3.7.3 on page 121.

Possibilities of connecting hosts

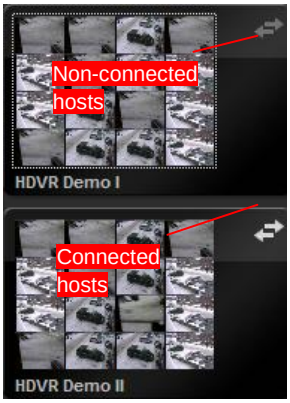


If the connection has been successfully established, the software switches from the host view to the camera view. The cameras of the host are now added to the list and can then be activated in the same way as the local cameras.

If you want to disconnect from the remote station, you can do this by clicking *(Disconnect)* in the *Host view*. To do this, first highlight the host (the slide representing it) in the list and then click *Disconnect*.

Hosts that are already connected appear on the host screen with a host icon lit up.

For more information on connecting additional hosts, see section 3.7.3 on page 121.



2.7.1 Automatically redialing hosts after the connection is interrupted

If hosts are connected via the internet or DSL, the ISP (Internet Service Provider) may sometimes automatically disconnect every 24 hours (DSL forced disconnection).

This disconnection also interrupts the connections to the hosts.

The system therefore features an automatic redial function for reconnecting to the hosts within a defined period. You can set this up in the system configuration under *Network* → *Hosts*.

Specify the number of automatic redial attempts and the intervals between them. Once you save and apply the settings, the function is activated.

Note:

Automatic redialing must be set up separately for each host.

Because the IP addresses change after every forced disconnection, they have to be updated each time in the host settings. We recommend replacing the IP addresses of the hosts with what are known as DynDNS addresses. The update then takes place automatically.

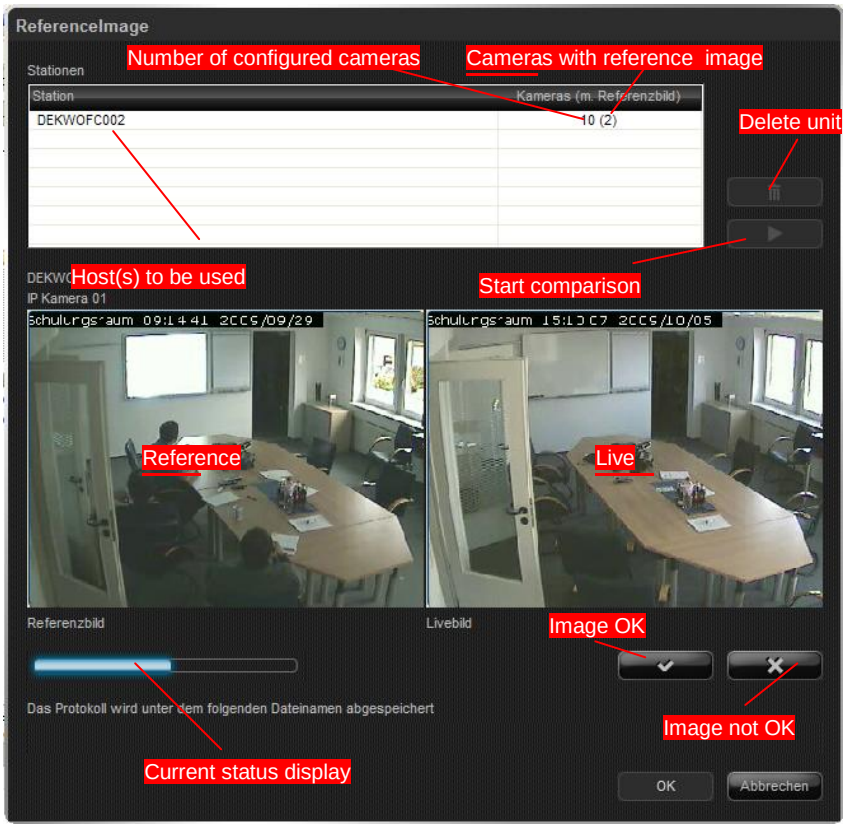
2.8 Reference image comparison

The reference image comparison allows users to compare the current camera image with a reference image stored in the system. This means that any tampering with the cameras, for example turning them around, can be quickly detected. The result of this comparison is then documented in an HTML report any saved in the *My Documents* folder of the current user.

To start the reference image comparison, first open the Info dialog by clicking *Support*. You can then start the comparison by clicking *Reference images…* .

Note:

A reference image comparison is only possible for cameras that are set up in the system for creating reference images and if reference images have been created. For more information see section 3.2.7 on page 60.



After the window has loaded, all the configured hosts are connected and the number of activated cameras, as well as the cameras with reference images created, are shown in parentheses. If a host is not reached within 60 seconds, its status is changed to *Connection failed*. This host is then no longer included in the reference image comparison and can be deleted.

If the reference image comparison is not carried out for all the listed hosts, then the hosts that are not included must be deleted. Highlight these hosts and click *Delete*.

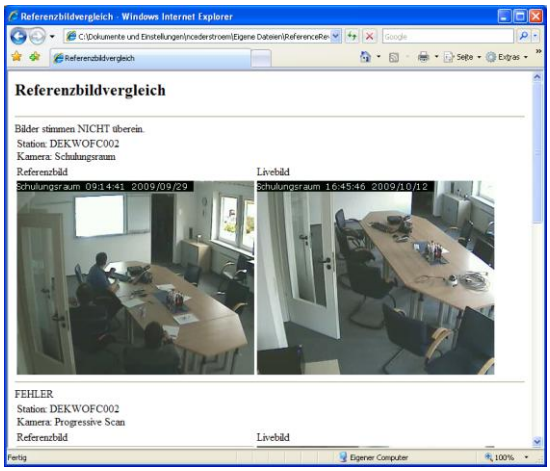
To start the comparison, click *Start.* All cameras of the hosts activated for the reference image option are shown in succession.

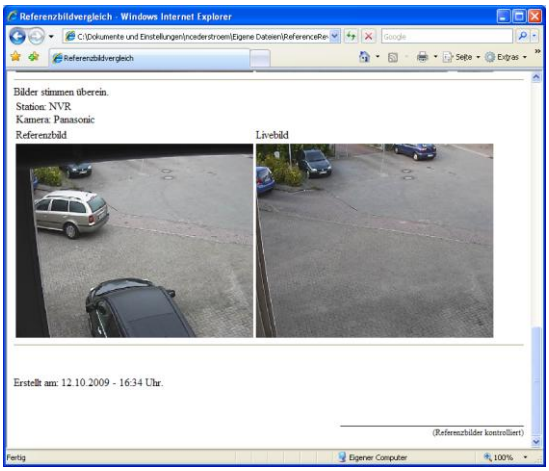
The user must then compare each image with the reference image and decide whether the two images match. If they do, click *OK* to confirm the image. If not, click *Not OK* to mark the image as incorrect. This is documented later in the report.

Once the comparison has been completed, the system generates an HTML report and displays it in the web browser. You can print the report out if required.

If several hosts are included in the reference image comparison, the overall results are summarized in a single HTML report.

The following illustration shows a finished HTML report where one camera has been evaluated as *OK* and the other camera is *Not OK*. The user making the comparison must print out and sign the document, and file it as required.





Note:

A report is saved in the My Documents folder of the current user for each reference image comparison. The folder name is "ReferenceView_(date)_(time)", (for example ReferenceView_20090101_0900). Because this generates large amounts of data, the user must manage these reports and, if necessary, delete old reports and those that are no longer required.

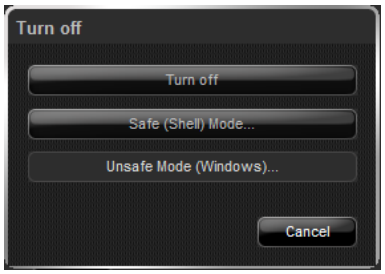
The reference image comparison is implemented in software version 6.5 and higher, and is limited to the ***VMS Enterprise*** *version.*

2.9 Shell mode (safe mode)

The shell mode prevents access to the operating system by setting the user interface modally at the front of the system. This means that the system is prevented from possible manipulation. The following points show how to activate and deactivate the shell mode.

2.9.1 Activating the shell mode

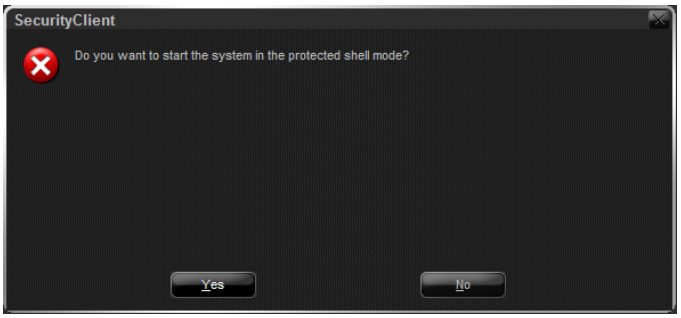
To activate the shell mode, a logged-in user must first log out. To do this, use the *Logout* button (in the menu bar at the top-left of the screen).



Click on the *Switch off* button, then select *Safe (Shell) Mode* in the switch-off dialog.

For security reasons, you are then asked whether the program should really be started in shell mode or not. Confirm this dialog by pressing *Yes*.

After entering the user name and password, the system is automatically restarted and the shell mode is activated.



2.9.2 Deactivating the shell mode

To deactivate the shell mode, proceed as described in point 2.6.1. The only difference here is that the *Unsafe Mode (Windows)* button is pressed instead of the *Safe (Shell) Mode* button.

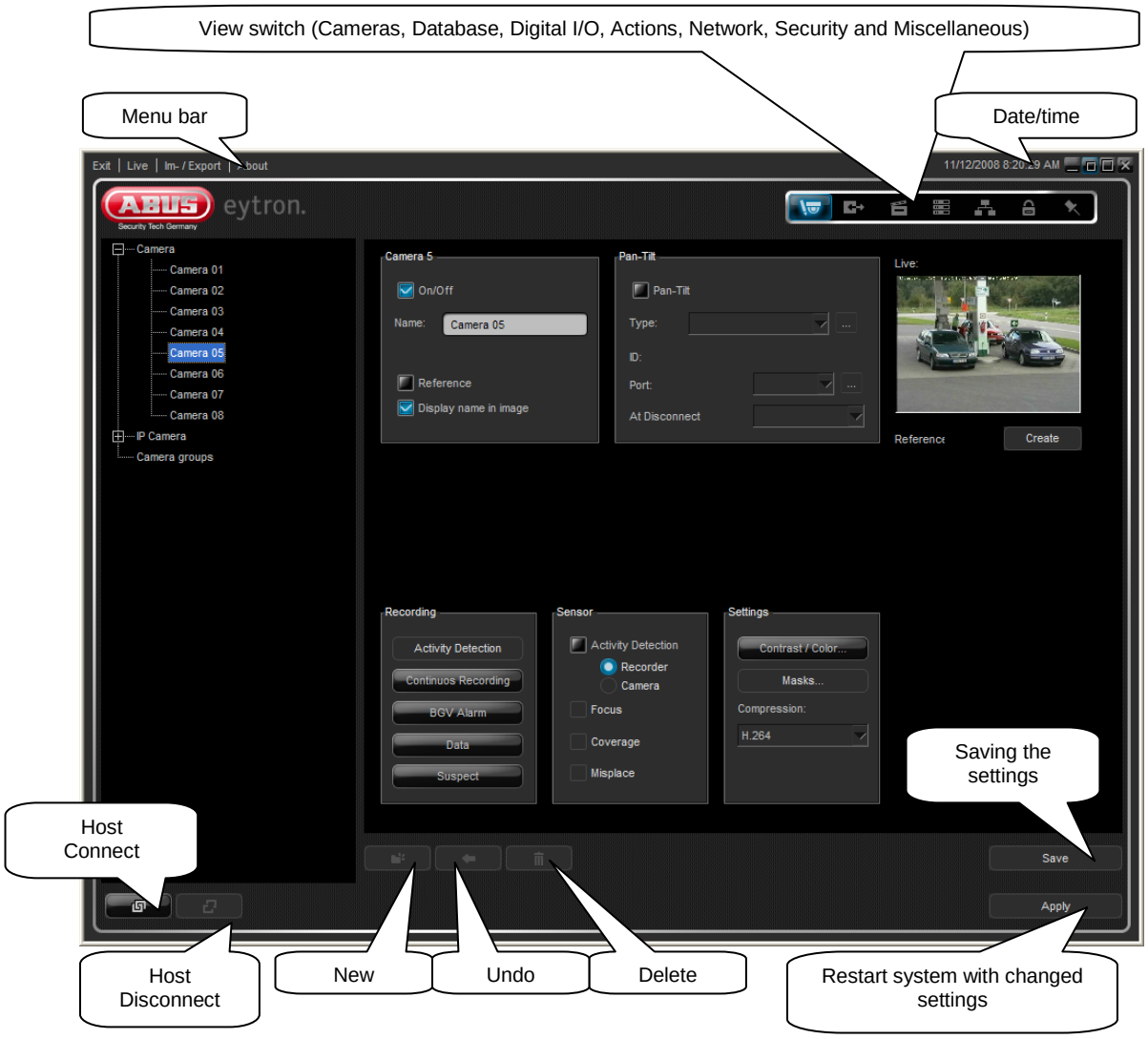
After the user data is entered, the system is restarted in unsafe mode and the Windows interface can be used again.

3. System configuration

The system configuration is used to set up the entire system. For example, you have the possibility of creating new users or configuring connected cameras here.

A more detailed description on how to use the system configuration can be found below.

When configuring the system, ensure that the individual components are set up carefully in order to prevent possible malfunctions.



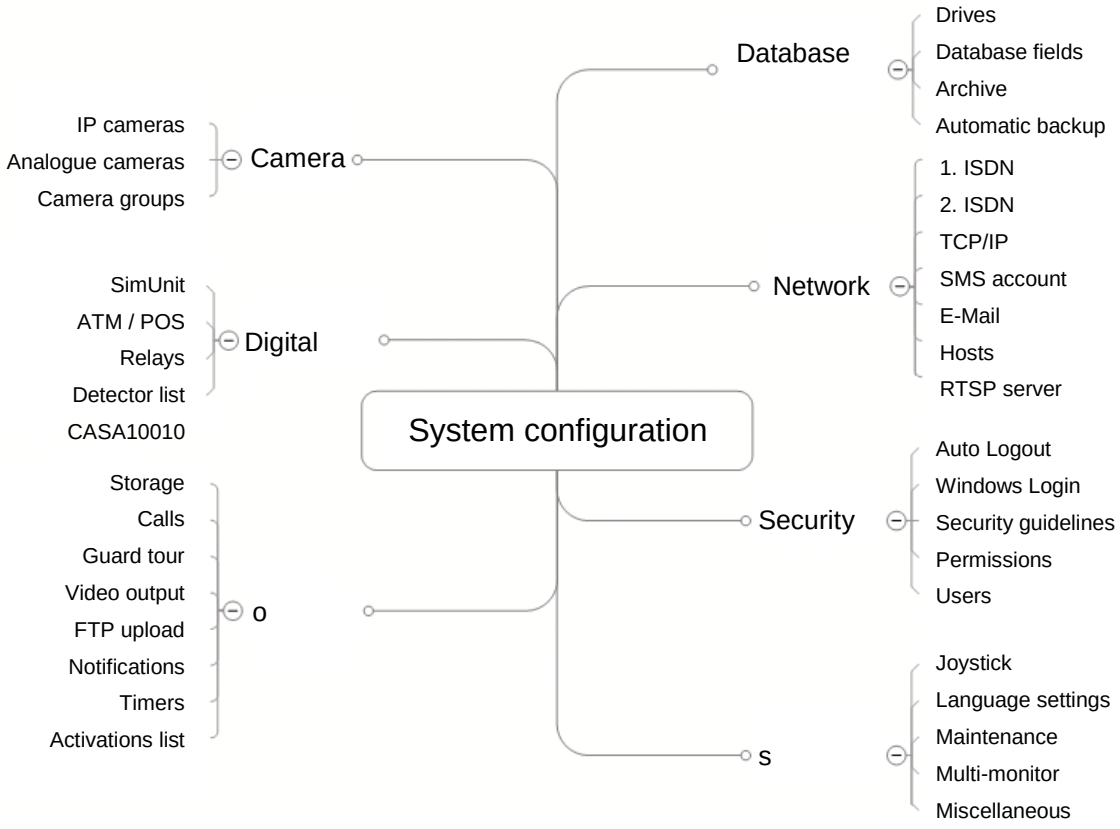
3.1 Opening the system configuration

The system configuration is opened using the *Configuration* menu point at the top-left corner of the user interface screen.

Access is only permitted for authorised users (entry of user name and password). To log in, use your existing user data.

Access to the system configuration can be adjusted for each user individually using the “Permission” levels (see point 3.6.1 on page 111).

The following graphic shows the schematic structure of the system configuration:



3.2 Camera configuration

The camera configuration is used to define the global settings of each individual camera and also to add and set up new cameras. The camera configuration can be accessed over point 1 of the view switch (slider).

Descriptions of the individual configuration methods for analogue, IP and pan/tilt cameras can be found below.

3.2.1 Setting up an analogue camera

Using the set-up wizard, the maximum available number of cameras is determined and entered in the system configuration.

To be able to use more cameras in the software, the signal must first be connected to the system using a BNC cable. The set-up can be continued if this has already been made.

Switching on the camera:

Open the system configuration and switch the view switch to the Camera view (point 1). All analogue cameras are now listed on the left-hand side under *TV33xx camera*.

Select the desired camera number and activate it using the *On/Off* field. The camera number corresponds to the number on the BNC connection cable.

If a pan/tilt camera is connected, then it must be triggered according to point 3.2.2.

Using the *On/Off* field, only connect the cameras that are physically connected to the system. Cameras which are not connected or activated can lead to unintentional errors.

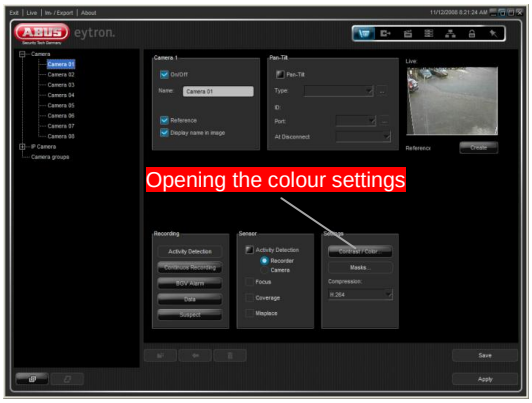
1. Choose camera view
2. Select camera
3. Activate camera

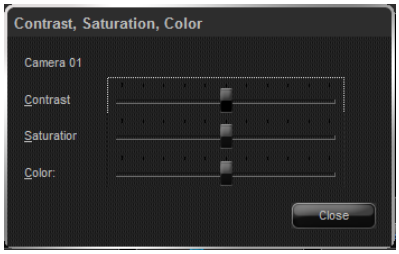
Setting up the colour settings:

Colour, brightness and contrast settings can also be set up individually for each camera using the system configuration. To change the settings, use the *Contrast / colour...* button on the camera configuration page.

The parameters can then be adjusted in the dialog which follows.

Exit the dialog by pressing *Close*.

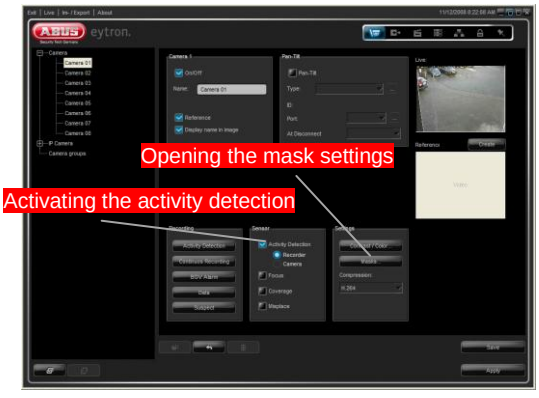




Setting an activity mask:

Press the *Masks...* button to use activity masks for the recording of individual cameras. Please note that the button is only activated when the *Activity Detection* box is checked for the camera.

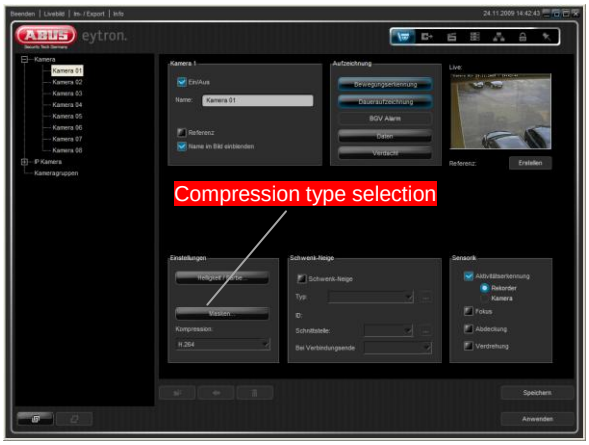
Further details on using activity masks can be found under point 3.2.8.1 ff.



Selecting the compression type

The compression type can be selected separately for each camera. The possible compression formats include .JPEG,.MPEG-4 and H.264. The image files are then saved in this format in the database.

Select the required compression type and save the settings.



Note:

The setting for the compression type only applies to analog cameras.

Defining a recording process:

After the camera has been activated, you can record the image data continuously or according to activity detection.

To do this, click on the *Activity Detection* or *Continuous Recording* buttons. With the PCIe cards (TVVR95000 – TVVR95020), you can choose between Stream 1 (high resolution and Stream 2 (low resolution). From version 7.0 onwards, you also have the option of audio recording. To do this, first activate audio in the camera setup and then in the required recording process.

All other necessary settings are then made automatically, meaning the set-up is completed.

An image rate of five images per second is used for recording image files.

Note:

The activity detection button is only enabled when you select the checkbox in the activity detection field (sensor settings).

3.2.2 Setting up a pan/tilt camera

Important!

Pan/tilt cameras are usually triggered using the RS-422 or RS-485 bus (data transfer). In this case, an additional converter is required (e.g RS-232 → RS-422/485 or USB → RS-422/485).

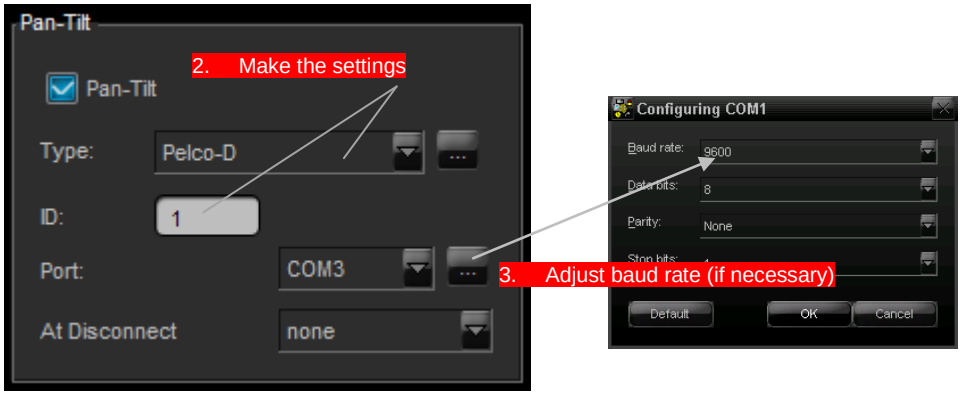
Connected cameras are always set up as fixed cameras when activated during system configuration. To add a pan/tilt function to a fixed camera, the pan/tilt support must be activated.

To do this, switch on the pan/tilt support for the desired camera in the system configuration (*Camera configuration → TV33xx camera → TV33xx camera 01 → Pan/tilt*).

Define the appropriate protocol, ID, interface and position at disconnection. The appropriate information can be found in the camera documentation.

When all settings have been made, they must be saved and then applied. Use the *Save* and *Apply* buttons to do this.

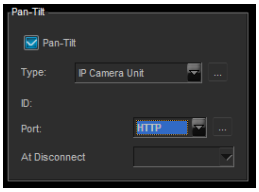
The camera can now be controlled over the user interface using the joystick.



If this is not the case, then an excessively high baud rate may be the cause. Adjust the baud rate according to your camera documentation (step 3) and then check the functionality again.

When using a pan/tilt network camera, the *IP Camera Unit* type and *HTTP* interface should be selected in the pan/tilt configuration.

The availability of this setting depends on the successful set-up of an IP camera. See the following description for more details.



3.2.3 Setting up an network camera

The ABUS VMS software supports all ABUS network cameras and is compatible with selected models from other manufacturers (see the compatibility list at www.abus.com).

Additionally, video streams (generic RTSP) and individual image requests (generic JPEG) can also be used. This means that the software can also be used with other third-party cameras.

A completely configured camera (user name, password and a valid IP address) is necessary for successfully setting up an IP camera in the ABUS VMS software.

If this is not the case, configure your camera according to the camera documentation until access over a web browser is possible.

Set-up steps:

- Open the system configuration and switch the view switch to the *Camera* view (point 1).
- Open the *IP Camera* menu point on the left-hand side.
- Select the camera number you wish to set up and activate this using the *On/Off* field.
- Select the camera manufacturer in the *Type* selection field.
- The system then searches for all available IP cameras from the selected manufacturer and displays the results in the *URL/Port* field. This process may take some time.

  Alternatively, you can enter the IP address and port of the camera manually (e.g. 192.168.0.100:80).
- Click the “Selection” button to open the ABUS IP Installer, which allows you to easily select the camera you want.
- If a user name or password has been configured for data access, then this should be entered in the *Administrator:* or *Password:* field. Click on “Detect” and wait until the camera name has been updated.
- If you enter the access data correctly, you get a positive response.
- If the network camera supports audio, select the Audio checkbox so that audio can be switched on and off in the live view.
- To apply the changes, click on the *Save* and *Apply* buttons in the last step.

Recordings can be made using activity detection or continuous recording as described under point 3.4.2 on page 77.

If the IP camera is also equipped with a pan/tilt function, then this can be activated in the pan/tilt section of the camera configuration. Proceed as detailed in point 3.3.2.

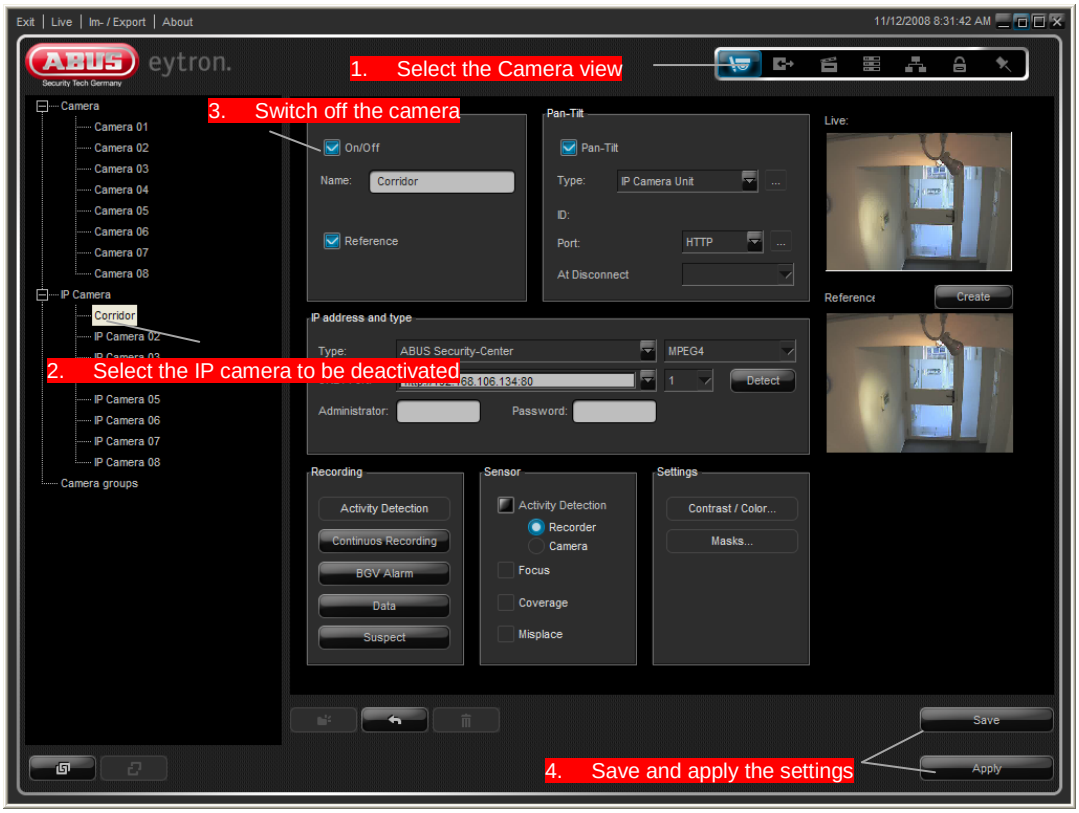
Deleting an network camera:

An network camera can be deleted over the system configuration when it is no longer needed.

Open the system configuration and switch the view switch to the Camera view.

Select *IP Camera*, then select the camera to be deactivated. Uncheck the *On/Off* field, then click on “Save” and “Apply”.

The camera name in the list should now be “IP Camera XX” and the camera is deactivated.



3.2.4 Setting up the camera anti-swivel protection

In order to prevent manipulation of the camera, an anti-swivel monitoring system is installed in the ABUS VMS software (**not** included in ABUS VMS Basic).

Using this function, the system can detect camera movements and send an alarm to another system or receiver.

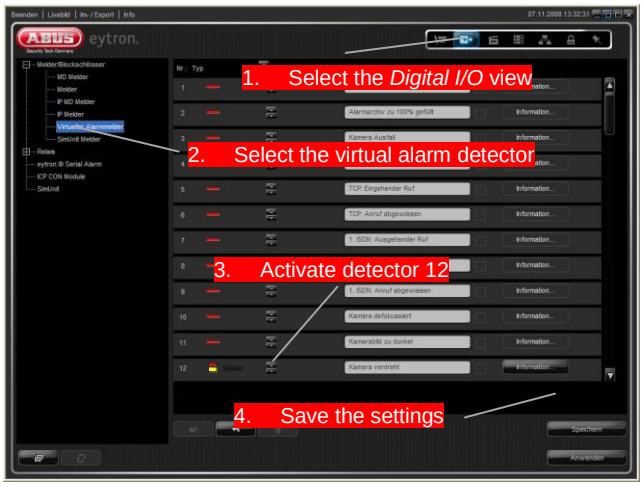
To activate the anti-swivel protection, first open the system configuration

and select the view of the camera where this function should be activated.

In the *Sensor system* area, check the *Misplace* box and save the settings. The camera is now prepared for anti-swivel protection.

In order for the system to also be able to start processes in the event of camera misplacement, these processes (notifications, alarms etc.) always have to be connected to a detector. The anti-swivel protection is equipped with a virtual alarm detector *(camera position wrong).*

This detector is always triggered when a camera with activated anti-swivel monitoring is misplaced.



To set up the detector, switch the view switch to *Digital I/O* (point 2) in the system configuration, then open the “Detector/Key switch” menu point on the left-hand side.

Select *Virtual detector* and activate detector 12 *(camera position wrong).* Save the settings.

Finally, this detector must be linked to a process. For more information on possible configurations, see point 3.4.9 on page 98.

Note:

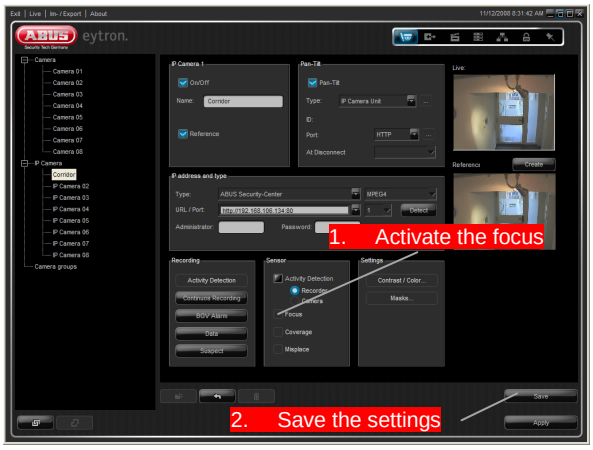
Only cameras with activated “Misplace” checkboxes can trigger an alarm over the virtual alarm detector.

3.2.5 Monitoring the camera focus

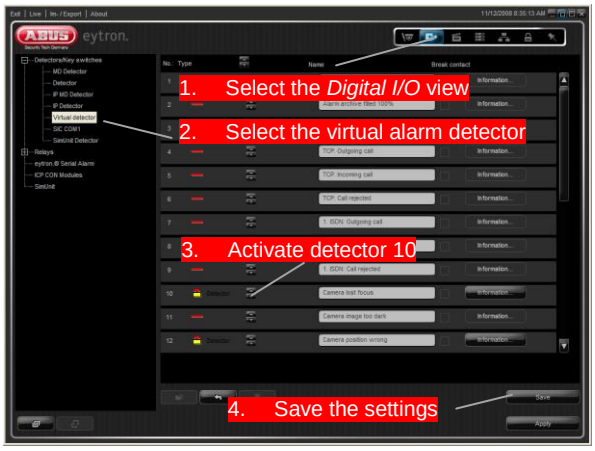
The focus on each individual camera can change from time to time. This can have a negative effect on monitoring quality.

If the current value differs significantly from the initial set value, then the system is able to detect this and notify the system operator when required.

This function can be activated on each camera in the “Sensor system” area in the system configuration on the camera configuration page (does **not** apply to ABUS VMS Basic). The *Focus* box must be checked and the changes must then be saved.



In order for the system to be able to send messages in the event of differing camera focus, the *Camera lost focus* alarm detector must be activated in the system configuration.



To do this, switch the view switch to *Digital I/O* (point 2), then open the *Detector/Key switch* menu point from the list on the left-hand side. Select *Virtual detector* and activate detector 10 *(camera lost focus)*.

Save the settings, then link the detector to a process (see point 3.4.9 on page 98).

Note:

Only cameras with activated “Focus” checkboxes can trigger an alarm over the virtual alarm detector.

3.2.6 Displaying a camera name in the live image

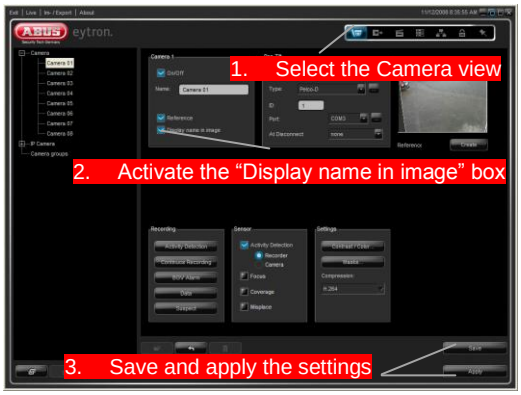
The name of the activated camera can be shown in the live image. This makes it easier to see which name is assigned to which image.

Open the system configuration and switch the view switch to the *Camera* view (point 1).

Select the desired camera and check the *Display name in image* box.

Save the settings and click on the *Apply* button.

After all settings have been loaded, the camera name is shown in the live image when the camera is activated.



3.2.7 Saving reference images

Reference images are used to compare the current image section of each camera with the image created when the camera was first put into operation (does **not** apply to ABUS VMS Basic).

In this way, alterations to the camera (manipulation, misplacement etc.) can be detected swiftly and dealt with accordingly.

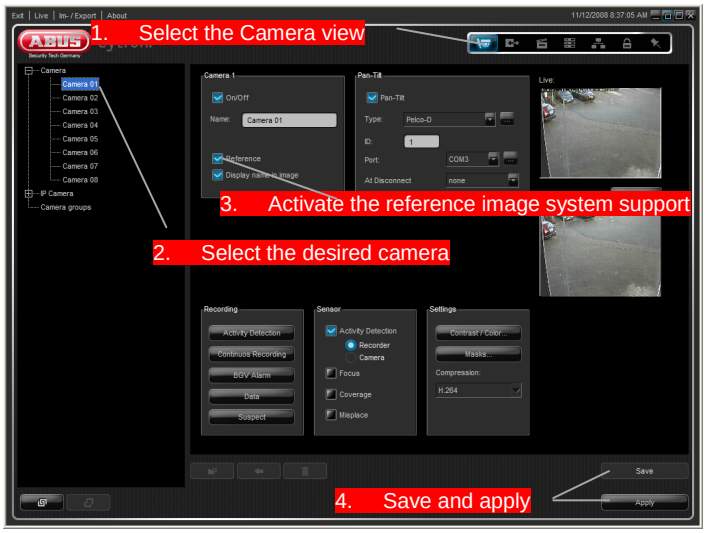
Before the camera can create a reference image, the relevant system support options must be activated. Reference images can then only be created using these cameras.

To activate the reference image system support, open the system configuration and switch the view switch to the *Camera* view.

Select the camera (analogue or IP) from the list on the left and check the *Reference* box.

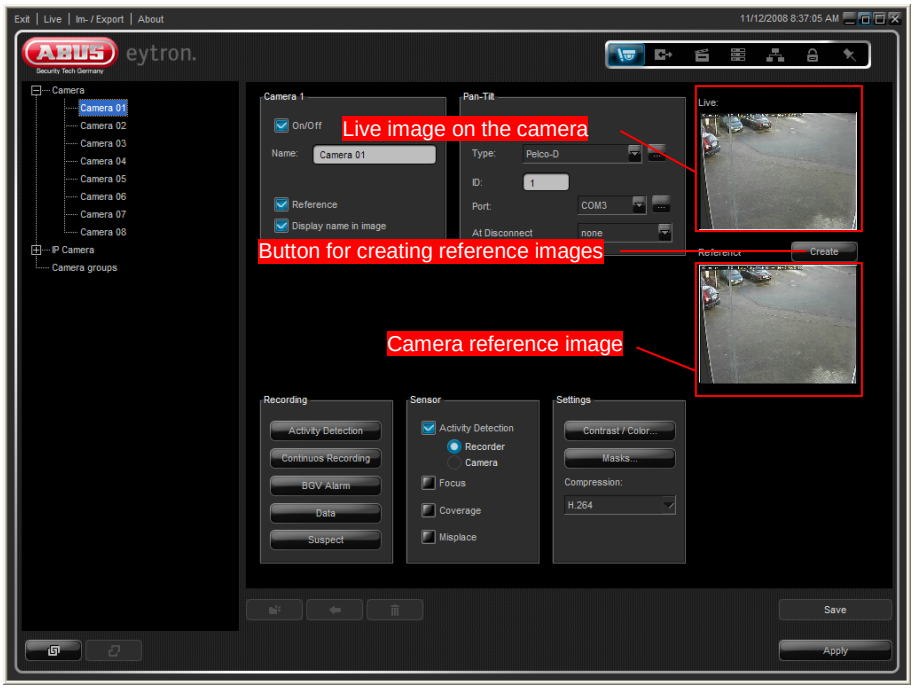
Save the settings and click on the *Apply* button.

The system shows whether a reference image has already been created by the camera on the right-hand side of the camera configuration page.



If this has not yet been made, then the reference image can be created using the *Set* button.

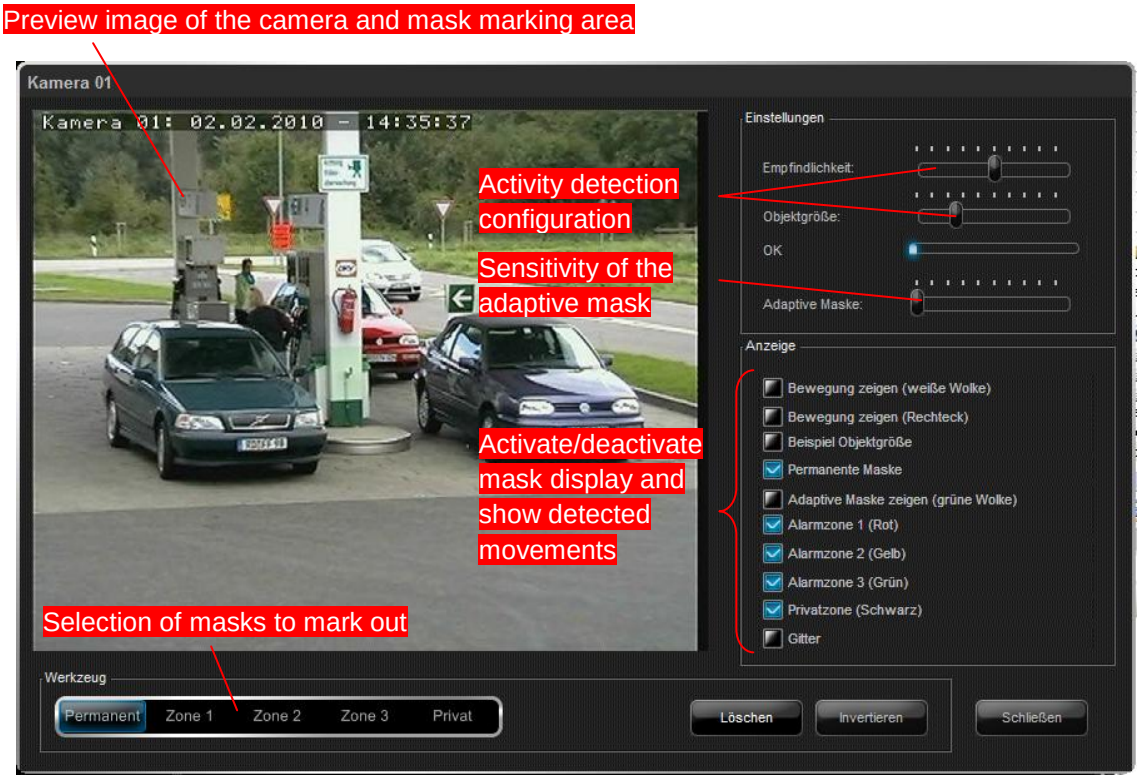
The reference image can only be checked afterwards using the system configuration.



3.2.8 The mask dialog

The mask dialog allows you to create motion masks and control their sensitivity, as well as the object size for recording after activity detection. The settings are saved according to the camera. This means the software lets you use individual parameters for each camera.

The following illustration contains a summary of the elements that can be used in the mask dialog.



Note:

Recording after activity detection only takes place if the camera has been set up for it. For further information on see section 3.4.2 on page 77.

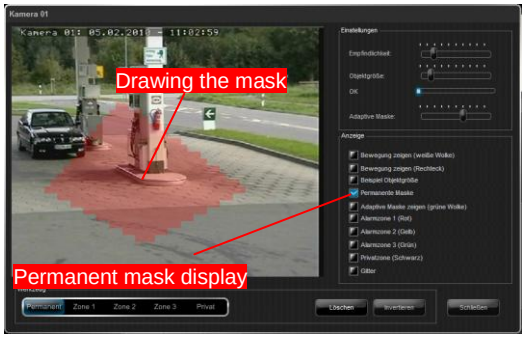
To call up the mask configuration dialog, click *Masks* on the camera configuration screen in the system configuration. However, the button is not enabled unless the checkbox in the *Activity detection (sensor settings)* field is selected.

The motion masks are the permanent mask, the private zone mask and the adaptive mask. The following sections describe these masks and how to use them.

The masks *for Zone 1, Zone 2 and Zone 3* are for multiple zone alarms and are explained in *section 3.2.8.5* onward.

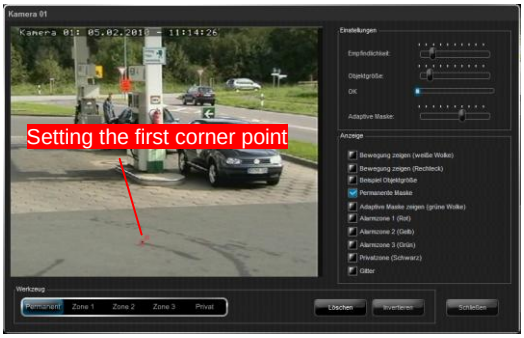
3.2.8.1 Setting a permanent mask

The permanent mask is for limiting the area analyzed by the selected camera.



Movements that occur within this area are ignored by the software and not used for recordings.

To draw a permanent mask (red mask) in the preview image, VMS version 6.8 and allows you to make the mask simply by setting the corner points. The area within these corner points is then automatically masked.

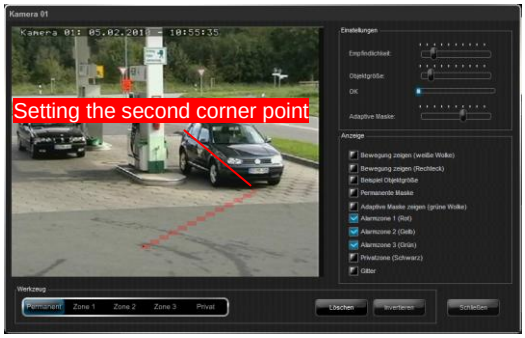


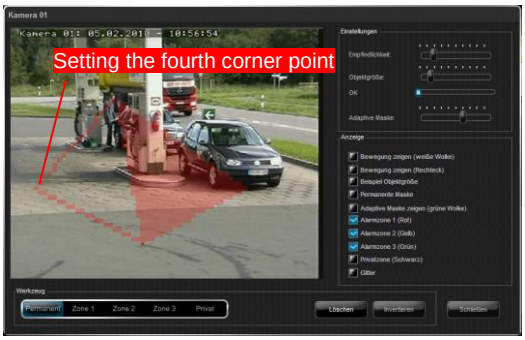
Left-click inside the preview image to set the first corner point.

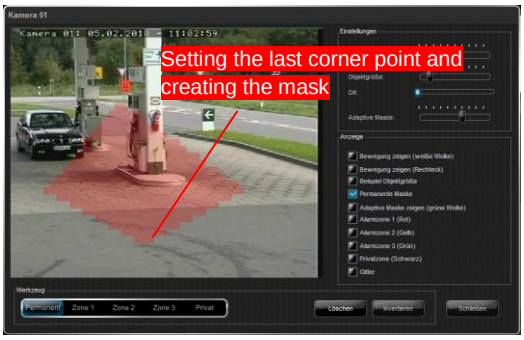
Then move your mouse to the second corner point of the mask and set it by clicking the left mouse button again. Repeat this for all the other corner points. If you set a corner point in the wrong place. simply click it to remove it. The mouse pointer changes to the following icon.

When you have set all the corner points, you must connect the last point with the first one. Only then is the mask created and saved. The mouse pointer changes to the following icon when you close the corner points.

The following illustrations show in detail how to create a mask.







Once you have created the mask, click *Close* to quit the dialog and complete the process.

You can invert the mask if necessary by clicking *Invert*. This means that the masked area is swapped with the non-masked area. Inversion always applies to the mask that is currently selected (use the *Tool* slider).

3.2.8.2 Setting a privacy mask

Using a privacy mask, a certain section of the image is masked off, meaning this area is blurred out in the live image.

The privacy mask is also created in the system configuration (does **not** apply to ABUS VMS Basic).

To create the mask, proceed as detailed above under point 3.2.8.1, but use the middle mouse key (scroll wheel) instead of the left mouse button.

In contrast to the permanent mask, a privacy mask is displayed in black. The masked section of the image is then blurred out in the live image

The following illustrations show how to set up a private zone mask.

Setting up the mask

→

Result in VMS

3.2.8.3 Activating the adaptive mask

The adaptive mask prevents false alarms from being triggered when recording is made by activity detection.

Possible examples of this are trees or flags moving in the wind.

As their movements remain constant, a mask (similar to a permanent mask) is placed over this area (does **not** apply to ABUS VMS Basic).

Recording through activity detection is then ignored for this area.

The sensitivity of the adaptive mask can be set between *"low"* and *"high"*. The more sensitive the mask setting, the bigger the adaptive mask.

Note:

The standard mask sensitivity setting is "normal". Check whether or not this setting is suitable for you, as the adaptive mask can sometimes lead to an unexpected loss of recording.

3.2.8.4 Configuring the sensitivity of activity detection

The activity detection system analyzes the entire video image for any changes. If these changes exceed a set threshold, an alarm is triggered and recording is started.

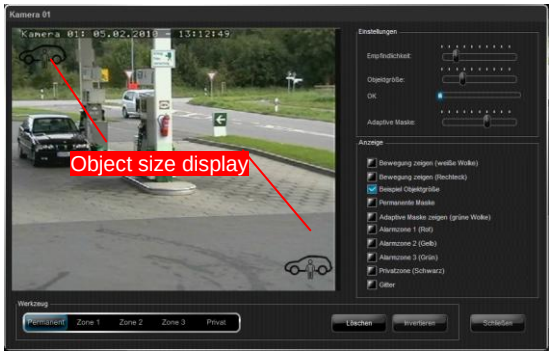
In the mask dialog on the camera configuration screen of the system configuration, you can not only create motion masks, but also adjust the activity detection threshold parameters. To do this, you can use the *Sensitivity* and *Object size* sliders.

In this case, *Sensitivity* refers to the average brightness value with which altered pixels are compared with the previous brightness. If the sensitivity is set very low, the change must differ greatly from the previous value. If the sensitivity is set very high, even slight changes trigger an alarm.

Object size is the area a change must cover. In this case: The smaller the object size, the smaller the coherent area which triggers an alarm.

You can see a graphical display during setup if you select the checkbox in the *Example object size* field.

You will then see a graphics showing the current threshold object size in top left and bottom right of the preview image. An alarm is only triggered and the associated recording process started when the actual object reaches the size of the preview object.



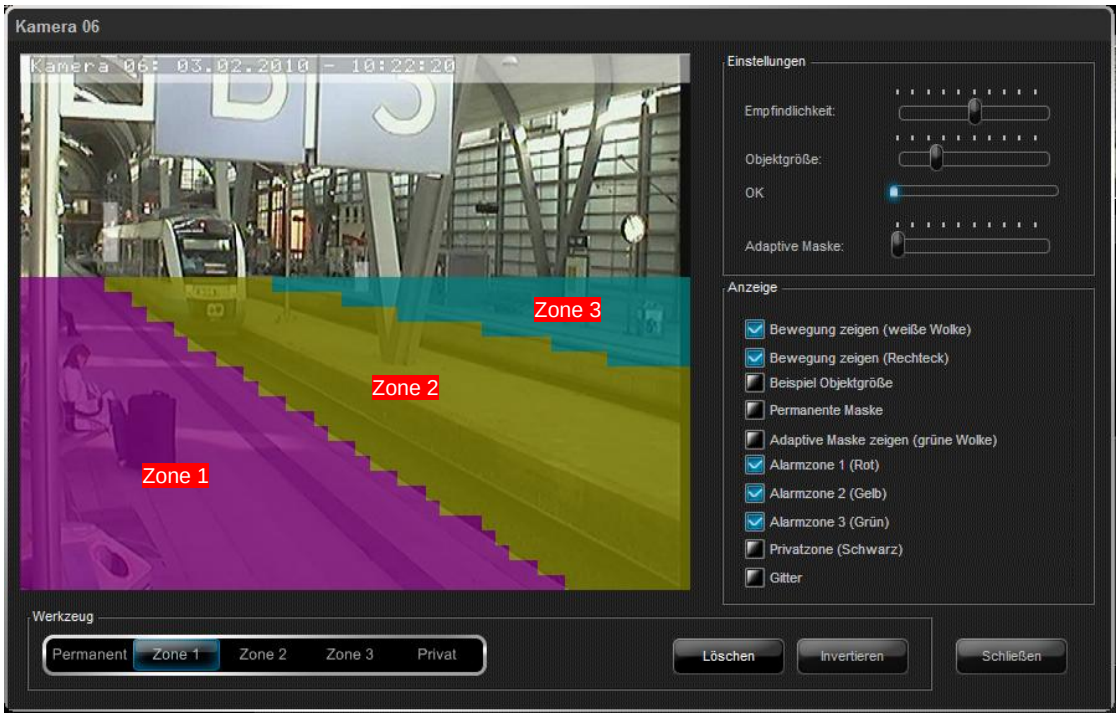
When you have finished the configuration, click *Close* to quit the mask dialog and complete the system configuration.

3.2.8.5 Using multiple-zone alarms

Multiple-zone alarms are used for starting various processes depending on the zone which activity is detected in.

The zones are also created in the mask dialog, which you can open by clicking *Masks* in the camera configuration dialog. (*See section 3.2.1 on page 51)*

The ABUS VMS software allows you to use up to three zones at the same time. The illustration below shows a configuration with three zones.



To create the first zone, move the slider in the *Tool* field to *Zone 1* and draw the zone by setting the corner points in the preview image (see section 3.2.8.1 on page 63).

Repeat these steps for *Zone 2 (yellow mask)* and *Zone 3 (green mask)*.

As soon as you have drawn the zones in the preview image, a new motion detector is created for each zone under *Digital I/O* → *Detectors/block locks* → *Motion detection* .

These detectors can then be linked to the required processes on the activation screen *(Processes*→ *Activations)*.

In order to make it easier to assign the detectors, these have been subordinated to the main motion detector (in this case Camera 06 MD).

Note:

The detectors (e.g. Camera 06 Zone 1 to Zone 3) are only triggered when motion is detected in their zone. However, the main motion detector, Camera 06 MD, is always triggered.

For the main motion detector it is unimportant whether the movement is inside or outside a zone: it always applies to the whole video image.

If, for example, an alarm is triggered in Zone 2, the detectors Camera 06 MD and Camera 06 Zone 2 are given *Alarm* status.

3.2.9 Setting up camera groups

Camera groups are used to group together cameras which belong together. This makes the addition of cameras to the live window significantly easier, as the cameras no longer have to be searched and activated individually. Instead, this can be made in one single step.

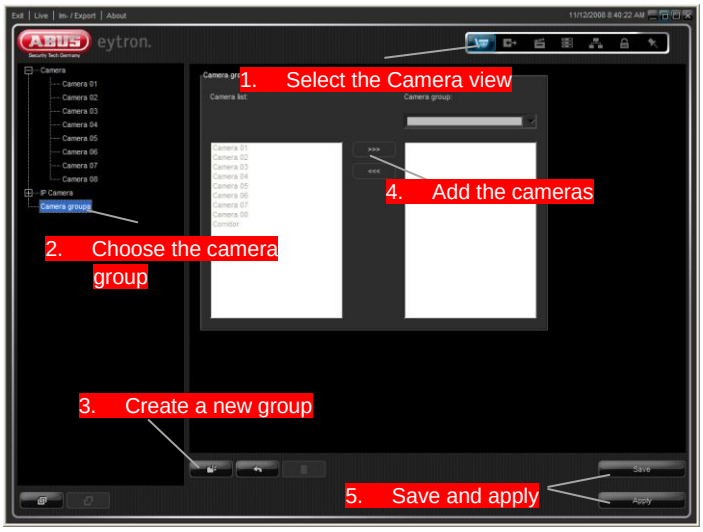
Setting up a camera group:

Open the system configuration and set the view switch to the *Camera* view.

Select *Camera group* from the list on the left and create a new group using the *New* button.

Assign a unique name for the group.

Add the cameras from the camera list (left column) to the newly created group (right column) using the Add >>> or Remove <<< buttons.



Save the settings and click on the *Apply* button.

The camera group is now available in the Camera group view on the user interface.

If one of these groups is dragged from the Camera group view on the user interface into the live window, then the vacant live windows are filled with the cameras from this group. The set image geometry is not changed here.

If more cameras are present in the group than can be displayed, then the remaining cameras are ignored.

Deleting a camera group:

To delete a camera group, proceed as described above under *Set-up*, but select the *Delete* button instead of the *New* button.

Note:

As camera groups may only be created by authorised users, they must be set up in the system configuration. Alternatively, if the logged-in user is not authorised to access the system configuration, then favourites may be used. For more details, see point 2.6 on page 41.

3.3 Database settings (Database / Storage)

The database settings are used to define the parameters for handling the available drives and create database fields and archives.

Changes to the database settings can be made in the Database view in the system configuration (point 4 - “Database / Storage”).

Read through the following points carefully to gain an overview of all available setting possibilities.

3.3.1 Setting the storage drives (drive settings)

The drive settings define how the drives connected to the system (CD writers, USB sticks or removable drives) are used. The following options are available here:

- **Operating system:** This drive contains the operating system and may not be used for storage
- **No usage:** Do not create any databases on this drive
- **Storage:** Use this drive for storage
- **Backup read & write:** Drive used for creating and reading backups
- **Backup read:** Backups may only be read on this drive
- **Removable hard disk:** This drive is run with read software when the system is shut down so that the data can also be seen on other systems

When a drive is set up as a storage drive, the entire storage space is used. If only a part of the storage space should be used, then this can be restricted using the *Size to use:* option.

Use the *New* button to add further network drives to the system.

Note:

In order to make a data backup (e.g. on CD/DVD or a USB stick), this drive must be specified as a "Backup read & write" drive. Otherwise, this drive will not appear in the drive list of the backup dialog.

3.3.2 Creating database fields

Database fields are used to save information that has been added externally. For example, this may be information from cash machines (ATM) or cash desk systems (POS).

All fields required for the connection of a cash machine are created automatically using the *Create default fields* button.

Other user-defined fields can also be created in addition to these fields, which enables the processing and storage of all incoming data.

Use the *New* button to create further database fields. Finally, assign a name, ID, type and string length (for “String” types only).

If the date or time is used as a type, then the data is saved automatically in the appropriate format (hour/minute/second hhmmss or day/month/year ddmmyy). In contrast, a string type can contain letters, figures or a combination of the two.

In order for the database fields to be filled with data, they must be linked in the Serial Alarm Unit.

The data is saved as soon as a detector on the Serial Alarm Unit is linked to a recording process.

3.3.3 Setting up the archives

Archives are used for saving image information (video data). In order to cover all possibilities, the archives have different properties.

These properties are as follows:

Ring archive:

The ring archive is the most common archive type used. Using this archive, old image data can be overwritten when required. For example, when the ring archive is completely full, the oldest video data is automatically overwritten. This means that video data is saved continuously without the need for user intervention.

Alarm archive:

An example of an alarm archive is in “BGV-Kassen” mode. The archive can only be filled with data once so that the image data is not deleted or overwritten in the event of an alarm. Further image data is then ignored until the user has manually deleted the data in the archive.

Two virtual alarm detectors are available in the system for monitoring the storage space (number 1: *Alarm archive is filled up to 60%* and number 2: *Alarm archive filled 100%*). These can be activated in the Digital I/A view under “Detector/Key switch → Virtual detector”.

Pre-ring archive:

The pre-ring archive is also required for use in “BGV-Kassen” mode. Image data which covers the time period before an upcoming alarm is saved in this archive.

When this archive is linked to an alarm or ring archive, then the image data from this archive is moved to the linked archive and the current alarm images are also saved in the alarm archive.

The pre-ring archive is only filled with video data again when the recording process for the alarm has been stopped (“Detector state OK”).

Alarm list:

The alarm list is used for monitoring detector activity. When a detector is linked to the alarm list, an entry is made in the alarm list each time this detector is triggered.

The alarm list can be linked to any available detector.

3.3.4 Backing up individual archives (automatic database backup)

The database backup function can be used to automatically transfer existing archives to other storage drives.

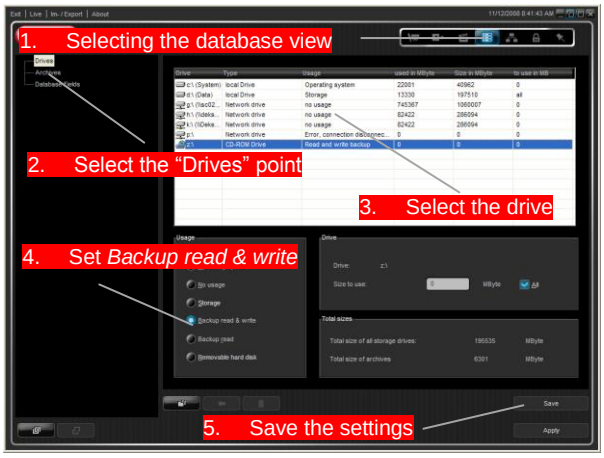
This function is useful in “BGV-Kassen” mode, for example.

As alarm archives are never overwritten automatically and need to be deleted manually, these can be transferred elsewhere using the database backup function, after which the archive can be deleted.

Please note that the database backup function is not compatible with removable media such as CD/DVD or USB sticks. A removable hard disk drive is necessary here.

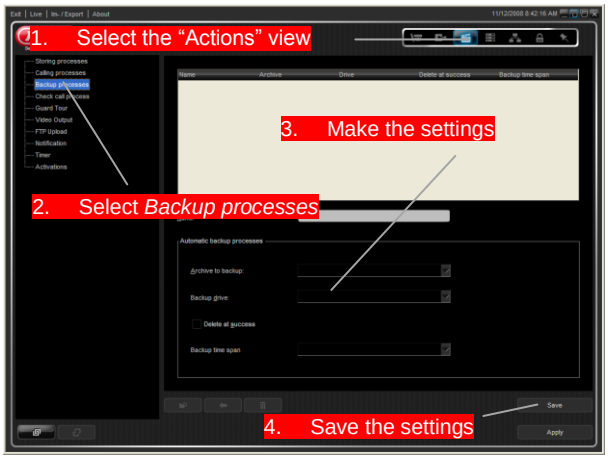
Setting up a data backup:

- Connect the external disk drive with the USB port on the video system.
- Open the system configuration and switch the view switch to the *Database / Storage* view (point 4).
- Select the *Drives* point from the list on the left.
- Select the connected storage drive (e.g. E:\) and select *Backup read & write* in the *Usage* field.
- Save your settings.



- Switch the view switch to the *Actions* view (point 3) and select *Backup processes* from the list on the left.
- Click on the *New* button and give the process a name. If the *New* button is not activated, then no storage drive could be found with the *Backup read & write* property. In this case, repeat all the steps for setting up a database backup.
- Select the archive to be backed up and the desired storage drive.
- Activate the *Delete at success* option, when required. The archive is then automatically emptied when the backup has been made successfully. Define a backup period. It is possible to either save the entire archive or only the last 24 hours.

- Save your settings.



- If you wish to control the backup using a timer, then this should be created as detailed under point 3.4.8 on page 96. The *Permanent alarm* detector is then used as the trigger. This is switched on in the system configuration under *Digital I/O* → *Detector/Key switch* → *Virtual detector* → *Detector 20*.
- Switch the view switch back to the *Actions* view (point 3) and select *Activations* from the list on the left.
- Press *New*, then create a new activation with the following data:

  Detector: Permanent alarm or other event; **Timer:** Always or user-defined; **Camera:** None; **Process:** Process created under point 7; **Archive:** None

  For more details on creating activations, see point 3.4.9 on page 98.

Repeat the steps detailed above to create further backup processes. A separate backup process must be created for each individual archive. However, these can all be started using one detector.

To make an automatic backup in “BGV-Kassen” mode, the process must be dependent on virtual alarm detector 1 *(Alarm archive is filled up to 60%)*.

Note:

As image archives can be very large and the backup process may take some time, we recommend starting the process at time where a low amount of movement is expected (for example, at night).

3.4 Processes (actions)

Processes are used to prepare the system for new tasks. For example, the storage speeds for recording can be set and notifications to external systems can be created using processes.

Any number of processes can be created in the ABUS VMS software. Ensure that the individual components are given a clear and conclusive description. This makes it easier to find existing configurations when adding new activations to the list at a later date.

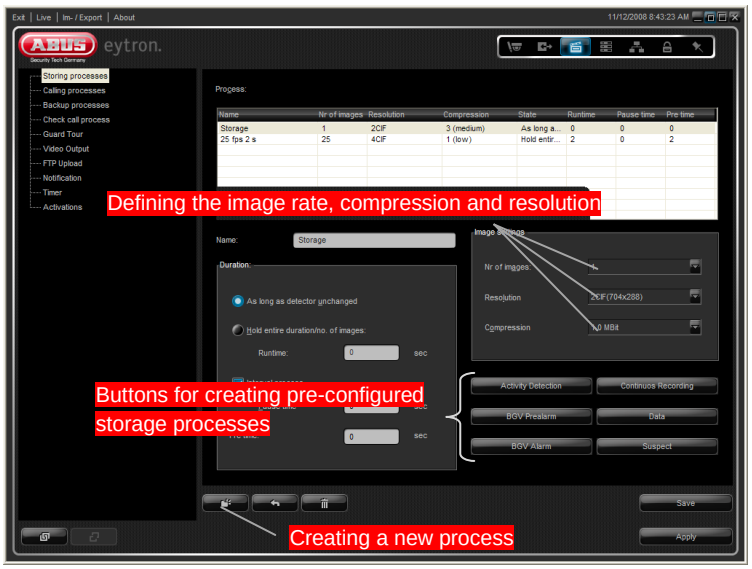
The following pages describe how to create each of the individual processes.

3.4.1 Creating storage processes

Storage processes are used to store image data from analogue or IP cameras in the linked archive. The image rate, resolution, compression or Stream1/2 can be set individually here.

To create a storage process, open the system configuration and switch the view switch to the *Actions* view (point 3).

The first point in the list on the left shows the storage processes. You can create a process manually or use pre-defined configurations here. For example, if you wish to create a process for recording using activity detection, then this can be set up by clicking on the *Activity detection* button. The image rate or resolution can then be changed as required.



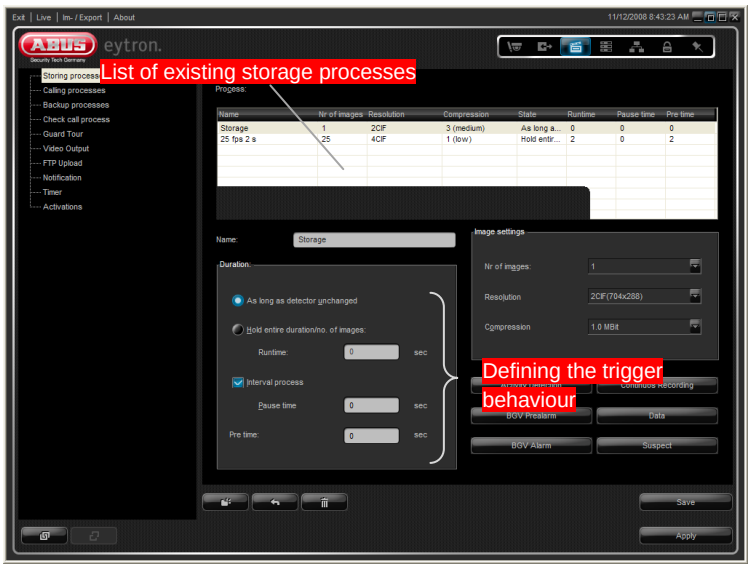
The behaviour of the storage process can also be defined here. If a connected detector triggers an alarm, then the storage process can either run until the alarm stops again (“As long as detector unchanged”) or can be processed completely (“Hold entire duration/no. of images:”).

As of version 7.0, you can choose between Stream 1 (high resolution) and Stream 2 (low resolution) for the recording.

You can also activate audio for each recording process, provided that the PCIe card or network camera supports audio.

When the storage process is set to *As long as detector unchanged*, then the process only runs as long as the connected detector has the “Alarm” status. For example, if the alarm stops after a half-second, then the storage process also ends.

When the storage process is set to *Hold entire duration/no. of images*, then the process is completed, even when the detector is only triggered briefly.



The interval process is another property of the storage process. This function is used to repeat the recording at set intervals instead of ending it after the entered run time. The process is then repeated after the set delay time.

Storage processes should always be selected according to the maximum capacity of the video card. Overloading the video card can lead to software malfunctions.

The following table illustrates the maximum recording rates:

Video card	Number of video inputs	Recording rate	Resolution
TVVR95000	4	100	4CIF (704 x 576)
TVVR95010	8	200	4CIF (704 x 576)
TVVR95020	16	400	4CIF (704 x 576)
TV3300	4	25	CIF (352x288)
TV3301	8	25	CIF (352x288)
TV3302	16	25	CIF (352x288)
TV3303	4	50	CIF (352x288)
TV3304	8	50	CIF (352x288)
TV3305	4	100	CIF (352x288)
TV3306	8	100	CIF (352x288)
TV3307	16	100	CIF (352x288)
TV3308	8	200	CIF (352x288)
TV3309	16	200	CIF (352x288)
TV3310	16	400	CIF (352x288) 2CIF (720x288)
TV3314	8	200	2CIF (720x288) D1 (720x576)

These values are guidelines only. Recording rates at higher resolutions can be determined as follows:

Recording rate	/	Number of video inputs used	=	Maximum recording rate per camera in CIF (352x288)
Recording rate per camera in CIF	/	2	=	Maximum recording rate per camera in 2CIF (720x288)
Maximum recording rate per camera in 2CIF	/	2	=	Maximum recording rate per camera in 4CIF (720x576)

For example, if you have a TV3305 video card then you can operate a maximum of four cameras on the card.

As the video card has a maximum capacity of 100 images per second in CIF resolution, then the maximum resolution rate for each camera is 25 images per second in CIF, 12 images per second in 2CIF and 6 images per second in 4CIF.

When setting manually, this value must then be used in the recording process.

Note:

The determined values are theoretical values only. They are based on continuous recording with a full system version. If recording is made using activity detection, then higher recording rates can be attained.

3.4.2 Setting up a continuous recording or recording using activity detection

The system is set up for continuous recording or recording using activity detection during the initial configuration. The following information describes the necessary steps for adding further recordings or changing an existing configuration.

Activity detection scans the video image of a camera for changes. For example, when a person appears in the video image, then this is detected by the system and the connected recording process is started.

In contrast, continuous recordings are always active. Changes in the video image have no effect on the system. This option requires a large amount of storage space.

The following components are required for the system set-up:

1. Activated camera to be recorded
2. Activated detector which starts the recording process
3. Created storage drive and archive
4. Created storage process
5. Created timer (optional)
6. Created activation

1. Activating the camera:

This point can be skipped if the camera has already been activated in the system.

Otherwise, open the system configuration and switch the view switch to the *Camera* view (point 1). Open the *TV33xx camera* point from the list on the left and select the desired camera. Activate this by checking the *On/Off* box.

To set up a recording, you only need to click on the *Activity detection* or *Continuous recording* button. The system makes all other settings automatically.

Please note that the image archive is only assigned 150 MB of storage space. Additionally, the image data is only recorded at one image per second and a 2CIF resolution. The parameters can be adjusted manually if this is insufficient (see points 3 and 4 for more details).

If special parameters are necessary for recording (recording rate, resolution, timer etc.) then the complete set-up can also be created manually. Use the steps detailed below for this.

2. Activating the detector

Switch the view switch in the system configuration to the *Digital I/O* view (point 2) and open the *Detector/Key switch* point.

If the system should record according to activity detection, then the *TV33xx MD detector* point should be selected and the detector should be activated according to the camera number in point 1 (camera 01 corresponds to MD detector 01). Switch the detector to the *Detector* state ( ) and save the settings.

If the system should record continuously, then the *Virtual alarm detector* point should be selected and detector 20 should be activated (*Permanent alarm*). Switch the detector to the *Detector* state ( ) and save the settings.

3. Creating a storage drive and archive:

Switch the view switch to the *Database / Storage* view *(point 4)* and open the *Drives* point. Ensure that at least one drive is used for storage. See point 3.4.1 for more details. Save your settings.

Create a new ring archive under *Archives* and give it a unique name and sufficient archive size *(see point 3.4.3)*. Save the settings.

4. Creating a storage process:

Switch the view switch to the *Actions* view (point 3) and open the *Storage processes* point. Create a new storage process using the *Activity monitoring* or *Continuous recording* buttons (*see point 3.5.1*). Save your settings.

5. Creating a timer:

If recording should only be made at certain times, then it can be set using a timer *(see point 3.4.8 on side 96: "Using timers")*. Otherwise, use the standard *Always* timer.

6. Creating an activation:

The final step is the creation of an activation. All components detailed above are connected to one another in this way. Only then is the system set up for recording.

Switch the view switch in the system configuration to the *Actions* view (point 3) and open the *Activations* point. Using the *New* button, create a new activation with the following data:

Detector: *Camera MD detector (activity detection) or permanent alarm (continuous recording) (see step 2)*

Camera: *As required (see step 1)*

Timer: *Always or user-defined (see step 5)*

Process: *Created storage process (see step 4)*

Archive: *Created ring archive (see step 3)*

For more details on creating activations, see point 3.4.9.

Save the settings and then click on the *Apply* button.

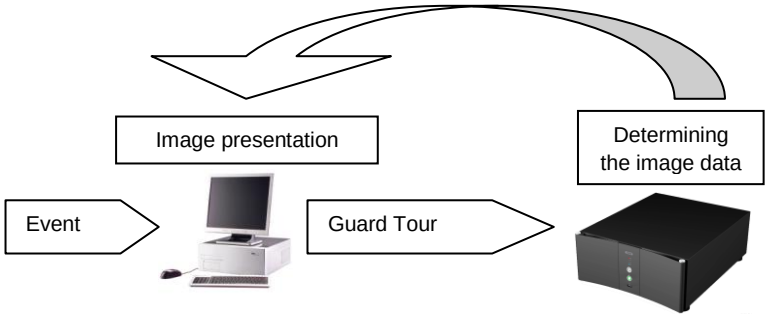
The recording is now configured. This is shown by the record display in the client or the blue LED on the front of the ABUS HDVR/NVR. The system configuration can now be closed.

3.4.3 Alarm dialling

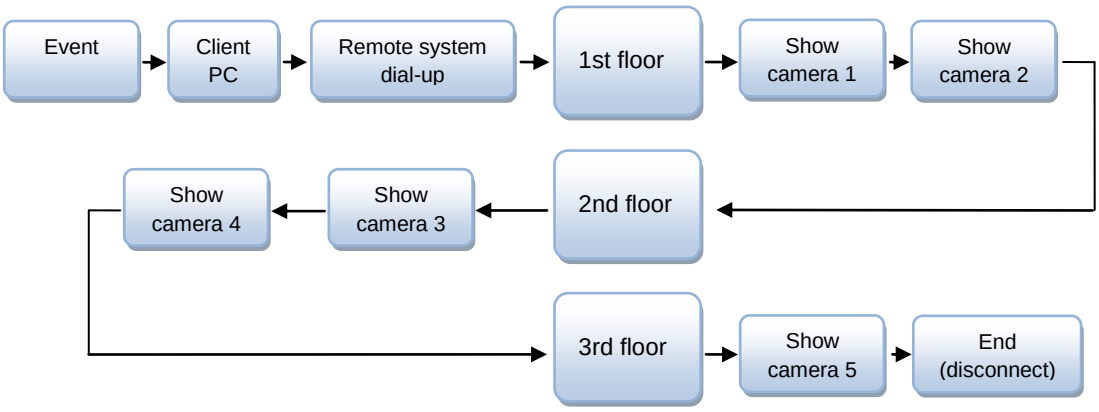
In the event of an alarm, there are two different types of image transmission in the ABUS VMS software. These are “Guard Tour” and “Alarm Dialling”.

Guard Tour:

In this mode, the client software dials into the corresponding recorder and displays the desired cameras. The process is triggered by an event on the client PC (e.g. an external alarm).

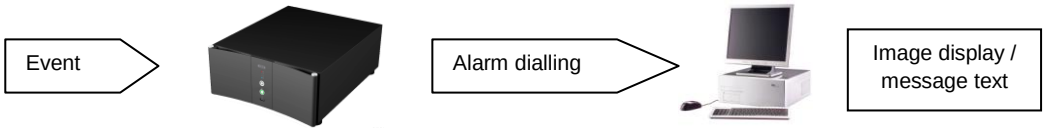


For example, if a recorder monitors a three-storey building with five cameras, then the cameras can be set up as a “virtual tour” on the client PC. Cameras 1 and 2 show the first floor, cameras 3 and 4 show the second floor and camera 5 shows the third floor. These are shown one after another before they are disconnected. The following diagram shows the functions as a flow chart.

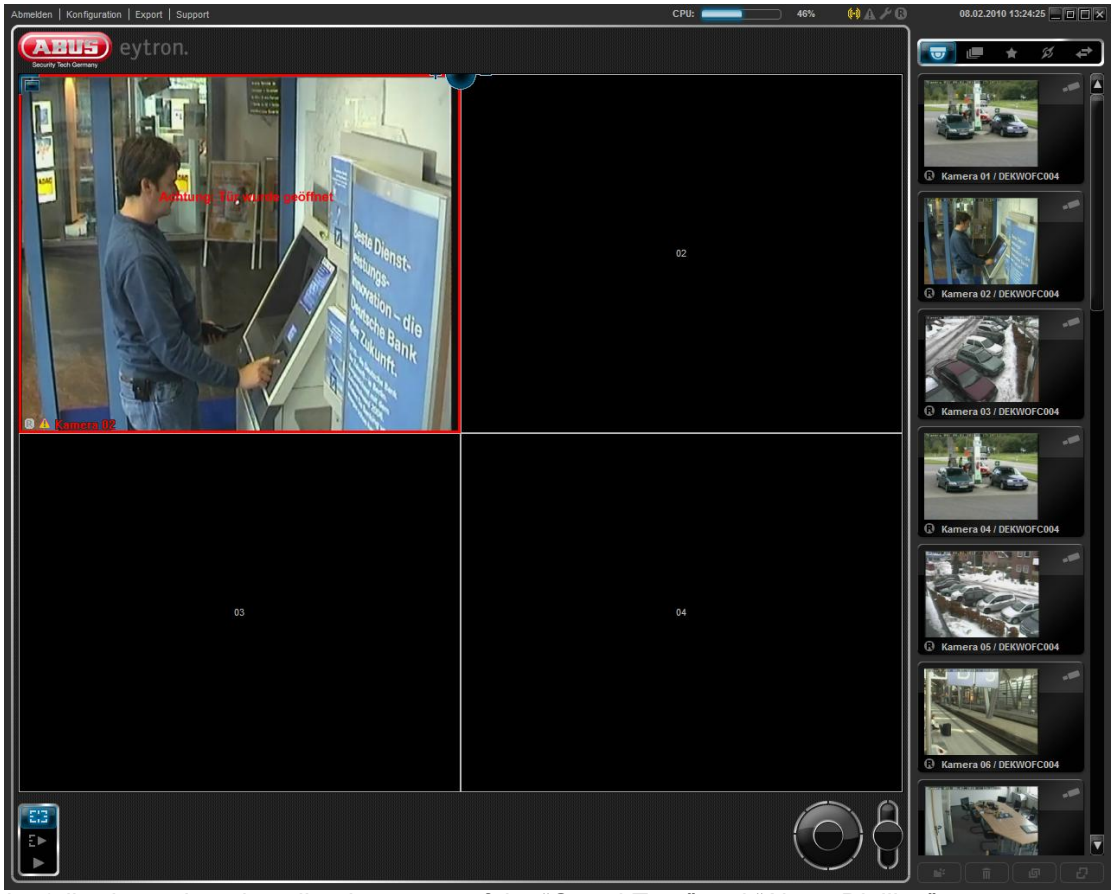


Alarm dialling:

In alarm dialling, the client is dialled from the recorder and the image data or a notification is transmitted. This is triggered by an event on the recorder.



For example, when a door is monitored in a room using a door contact, then the recorder sends information to the client PC each time the door is opened and also transmits the corresponding camera information and a corresponding text message.



The following points describe the set-up of the “Guard Tour” and “Alarm Dialling”.

3.4.3.1 Setting up a “Guard Tour”

The following components are required for manual set-up:

1. An event which triggers the action (e.g. alarm detector)
2. A host to be called
3. The appropriate permission level for accessing the remote system
4. A process used to call the host and display the desired cameras
5. An activation to connect all the components together

1. Selecting the event:

Theoretically, each alarm detector on the system can be used as the event trigger. These include external alarms, virtual alarms or simulation alarms.

Activate the desired detectors in the system configuration under *Digital I/O* (point 2) → *Detector/Key switch* and save the settings.

2. Setting up the host:

Switch the view switch in the system configuration to the *Network* view (point 5). Under *Hosts*, create a new host and save the settings. For more details on creating new hosts, see point 3.7.3.

3. Setting up the permission levels:

Switch to the *Security* view (point 6) and select *Permissions*.

Create a new permission level using *New*, then define the specific permissions. It is important that the cameras used in the guard tour are also activated under “Permissions”. For more details on permission levels, see point 3.6.1.

If you do not wish to work with permission level, then the standard “SuperVisor” level can also be used. However, please note that each user with this permission level has full access to all systems.

Save the settings.

4. Setting up a process:

Switch to the *Actions* view (point 3) and select *Guard Tour*.

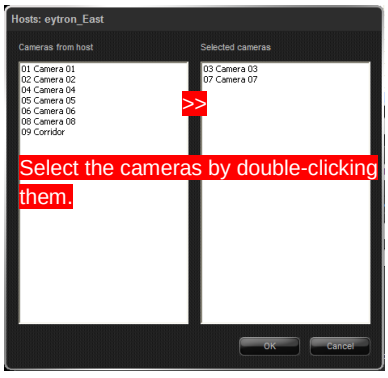
Create a new process using the *New* button and give it a unique name.

Select the host to be used by checking the box next to the host in the list. A multiple selection of hosts is also possible here.

Click on the *List* button and select the desired camera(s). These are then used later in the process. Add the cameras to the list on the right by double-clicking on them and close the window by pressing *OK.* If more than one camera has been selected, then the speed of camera display can be influenced using the *Switch time* field.

Now select the permission level. If you have set up your own permission level, then this should be selected here.

Otherwise, you can use the *SuperVisor* permission level. Please note that a user-defined permission level must also exist on the host with the same permissions and the level name on both systems must be identical. Otherwise, no connection can be established to the host.



The start behaviour of the guard tour must then be set. When this is started over an alarm detector, then the *Hold entire duration/no. of images* option must be selected so that the process is completed, even when the detector is only triggered for a short time.

When the process is started over a permanent alarm in connection with a timer, then the start behaviour must be set to *As long as detector unchanged*, as a *Permanent alarm* detector can never change its status.

“Save pictures”, “Fullscreen” and “Show camera exclusive” can also be set.

When the *Save pictures* box is checked, the host images are saved in the local archive. When no archive has been created for this purpose, it is set up automatically when an alarm occurs.

The “Show camera exclusive” option is used to display cameras individually on the local station. This means that all other activated cameras are not visible in the display.

“Fullscreen” mode disables all interface tools around the live window so that only the live images and chrome frame are visible.

The *Disconnect* option is used to disconnect the system after the camera sequence has been completed (end of process).

The completed settings should be saved before an activation is created.

5. Creating an activation:

Select the *Activations* point from the list on the left and create a new activation using the *New* button with the following data:

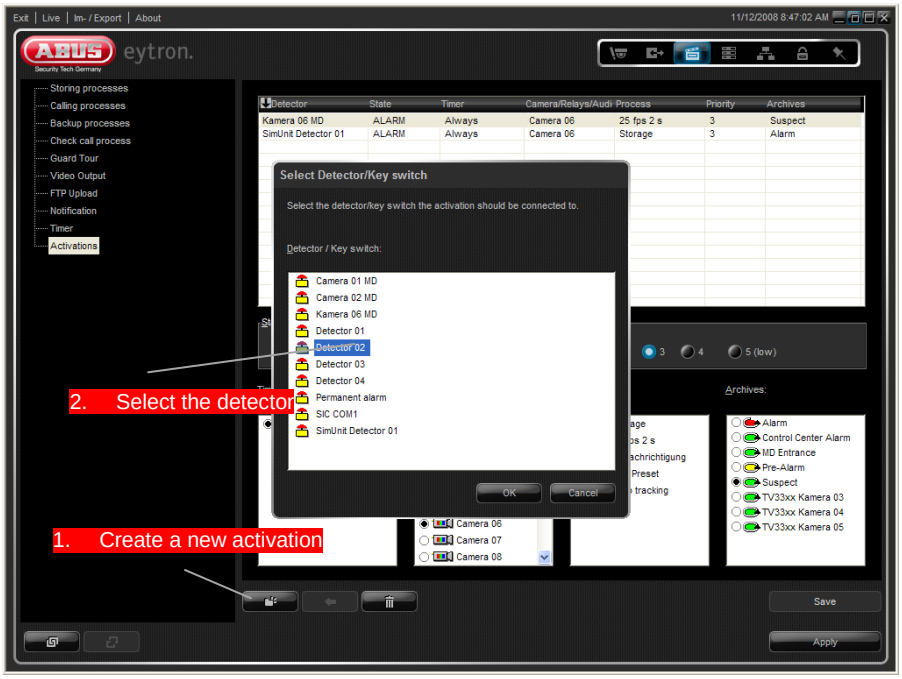
Detector: Set detector for triggering the process

Timer: Always or user-defined

Camera: None

Process: Set guard tour (point 4)

Finally, click on “Save” and “Apply”. The process is started as soon as the detector is triggered or the set time is reached.


Exit | Live | Im- / Export | About
11/12/2008 8:47:02 AM
ABUS eytron.
Storing processes
Calling processes
Backup processes
Check call process
Guard Tour
Video Output
FTP Upload
Notification
Timer
Activations
Detector | State | Timer | Camera/Relays/Audi | Process | Priority | Archives
Kamera 06 MD | ALARM | Always | Camera 06 | 25 fps 2 s | 3 | Suspect
SimUnit Detector 01 | ALARM | Always | Camera 06 | Storage | 3 | Alarm
Select Detector/Key switch
Select the detector/key switch the activation should be connected to.
Detector / Key switch:
Camera 01 MD
Camera 02 MD
Kamera 06 MD
Detector 01
Detector 02
Detector 03
Detector 04
Permanent alarm
SIC COM1
SimUnit Detector 01
OK
Cancel
2. Select the detector
1. Create a new activation
Archives:
Alarm
Control Center Alarm
MD Entrance
Pre-Alarm
Suspect
TV33xx Kamera 03
TV33xx Kamera 04
TV33xx Kamera 05
Camera 06
Camera 07
Camera 08
Save
Apply

Exit | Live | Im- / Export | About
11/12/2008 8:50:51 AM
ABUS eytron.
Storing processes
Calling processes
Backup processes
Check call process
Guard Tour
Video Output
FTP Upload
Notification
Timer
Activations
Detector | State | Timer | Camera/Relays/Audi | Process | Priority | Archives
Detector 02 | ALARM | Always | none | GT Station 1 | 3
Kamera 06 MD | ALARM | Always | Camera 06 | 25 fps 2 s | 3 | Suspect
SimUnit Detector 01 | ALARM | Always | Camera 06 | Storage | 3 | Alarm
3. Select the alarm status
State
OFF
OK
ALARM
Priority
1 (high)
2
3
4
5 (low)
Timer
Camera/Relays/Audio:
Process:
6. Link to the guide tour
Always
none
Camera 01
Camera 02
Camera 03
Camera 04
Camera 07
Camera 08
Check call process
Benachrichtigung
GT Station 1
4. Select the Always timer
5. Select no cameras
Save
Apply
7. Save and apply the settings

3.4.3.2 Setting up alarm dialling

The following components are required for the set-up:

1. An event which triggers the action (e.g. alarm detector)
2. A host where the notification is to be sent
3. The appropriate permission level for accessing the remote system
4. Activation of the camera
5. A call process used to notify the host and transmit the desired cameras
6. Creation of a message text
7. An activation to connect all the components together

1. Selecting the event:

Theoretically, each alarm detector on the system can be used as the event trigger. These include external alarms, virtual alarms or simulation alarms.

Activate the desired detectors in the system configuration under *Digital I/O* (point 2) → *Detector/Key switch* and save the settings.

2. Setting up the host:

Switch the view switch in the system configuration to the *Network* view (point 5). Under *Hosts*, create a new host and save the settings. For more details on creating new hosts, see point 3.7.3.

3. Setting up the permission levels:

Switch to the *Security* view (point 6) and select *Permissions*.

Create a new permission level using *New*, then define the specific permissions. It is important that the cameras used in the guard tour are also activated under “Permissions”. For more details on permission levels, see point 3.6.1 on page 111.

If you do not wish to work with permission level, then the standard “SuperVisor” level can also be used. However, please note that each user with this permission level has full access to all systems.

Save the settings.

4. Activation of the camera:

This point can be skipped if the camera has already been set up in the system. If the camera has not yet been set up, then switch to the Camera view and open the *TV33xx camera* point. Select the desired camera and activate it by checking the *On/Off* box. More information on configuring the camera can be found under point 3.2.

Save your settings.

5. Setting up the process:

Switch the view switch in the system configuration to the *Actions* view (point 3) and select the *Calling processes* point.

Create a new process using the *New* button and give it a unique name.

Select the host from the list of available hosts by double-clicking it. The host is then removed from the upper list and added to the lower list.

Select the permission level to be used. If no special permission level should be used, then the standard

SuperVisor level can be used. However, please note that this permission level has full access to all systems.

In order for the process to be completed, the *Hold entire duration* option must also be selected. Otherwise, the process will be interrupted when an event occurs for a short time.

From software version 6.8 onwards, you can change the receiver display when alarm notifications arrive. A new area *(Interface)* was added to the call-up process.

The functions are described in detail in the following list.

Function	Description
Full-screen mode	Activates full-screen mode of the receiver when alarms occur
Show camera in 1Plus	Switches the current view of the receivers to the 1Plus view and displays the alarm camera in the large window
Show camera exclusively	Deactivates the live cameras on the receiver and only display the alarm camera in the single-image view
Max. connection time	The number of seconds after which the alarm is automatically deactivated

6. Creating a message text

Select *Notifications* from the list on the left and create a new notification with a message text for an alarm using the *New* button. More details can be found under point 3.7.5.

7. Creating an activation:

Select the *Activations* point and create an activation using the *New* button with the following data:

Detector: Detector used for triggering the process (permanent alarm or external detector)

Timer: Always or user-defined

Camera: Camera used for alarm dialling (step 4)

Process: Set guard tour (step 5)

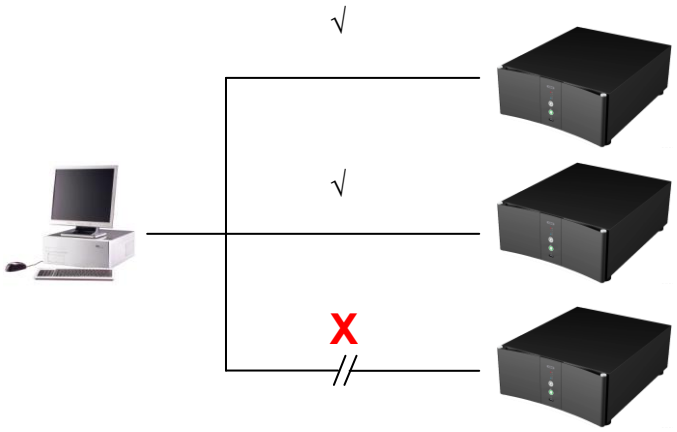
Notification: Message text from step 6 (or none)

3.4.4 Using the check call process

The check call process is used to check the connection of all hosts in the host list. For example, a system failure can then be detected quickly and relevant measures can be taken to solve the problem.

Two detectors in the virtual detector list are used for monitoring the connection. These are *Check Call Error* (detector 19) and *Check Call OK* (detector 21).

One of these detectors is triggered with every connection attempt to the hosts. For example, if the detectors are connected to the notification process, then any failure in reaching the host can be detected in good time.



The check call process is set up in the system configuration (*Check call process* point in the *Actions* view (point 3)).

You can select the permission level here and compare the time on the remote system with the local station, when necessary.

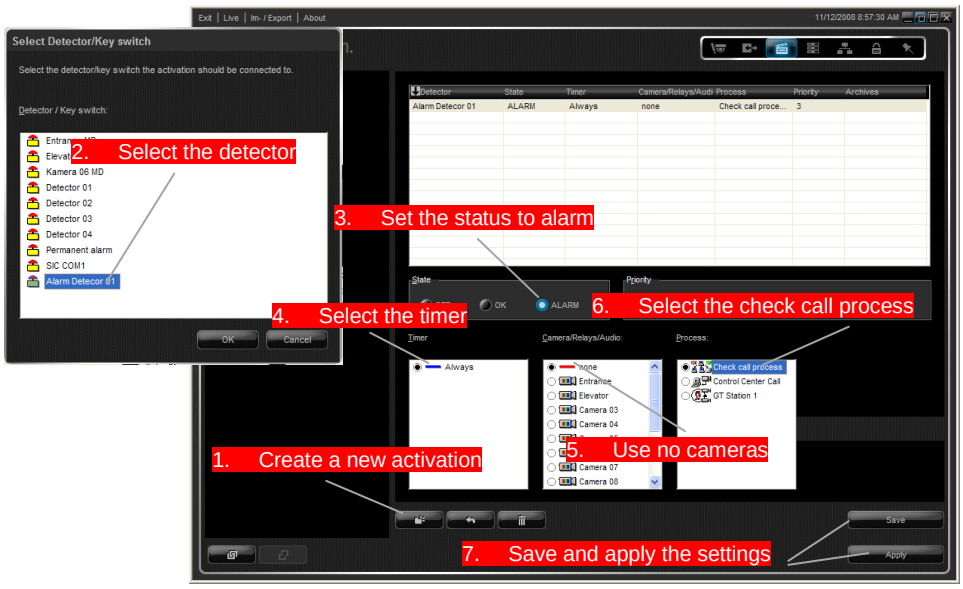
However, please note that the selected permission level must exist on the host and that this is also permitted to change the system time.

The check call process is always activated, meaning it does not need to be switched on.

Save the changes and activate virtual alarm detectors 19 and 21 under *Digital I/O* → *Detector/Key switch* → *Virtual alarm detector* (see point 3.5 for more details).

If the check call should be controlled according to the time, then it must be connected to the *Permanent alarm* detector (detector 20). When required, switch this on as well. Now create a timer with the desired times. For more details, see point 3.4.8 on page 96.

Switch the view switch back to the *Actions* view. Select *Activations* from the list on the left. Use the *New* button to create a new activation with the following data:



3.4.5 Setting up the FTP upload

Using the FTP upload, it is possible to send individual images from various cameras to an FTP server within a specific time period. These images can then be displayed on an Internet site.

The following components are required for the set-up:

1. A camera where the images should be uploaded from

2. An FTP server (Internet FTP server)
3. User authorisation for uploading the image data (log-in data)
4. A detector for event control *(e.g. permanent alarm)*
5. A timer (for time-controlled uploads)
6. A process used for uploading the image data
7. An activation for connecting all the components together

Activating the camera:

Open the system configuration and switch the view switch to the *Camera* view.

Open the *TV33xx camera* branch from the list on the left.

Select the desired camera and activate it by checking the *On/Off* box.

Save your settings.

FTP connection:

You can proceed with the upload process when storage space is available on the FTP server and you know the log-in data. Otherwise, contact your system administrator or server provider.

Activating the detector:

For a successful FTP upload, a detector is required to start the process. An external event or internal timer can be used as a trigger in this case. When using external events, activate a detector under *Detector/Key switch* → *TV33xx detector* in the *Digital I/O* view (point 2) in the system configuration.

When using a time-controlled FTP upload, the *Permanent alarm* detector must be activated under *Detector/Key switch* → *Virtual alarm detector* → *Detector 20*.

Creating the timer:

If the upload process should be started with time control, then the system must be set up with a timer.

More information on creating timers can be found under point 3.4.8 on side 96 *("Using timers")*.

Setting up the upload process:

The upload process loads the actual image data to the FTP server from the database. To create the process, switch the view switch in the system configuration to the *Actions* view (point 3).

Select *FTP Upload* from the list on the left and create a new process using the *New* button.

Assign a unique name for the process. This makes it easier to find the process when assigning the activation.

Set the time interval (in seconds) in which the image data should be uploaded to the FTP server.

Select the desired image resolution.

Enter the access data (server address, user name and password).

Enter a file name for the uploaded image.

Placeholders are entered as standard for the file name. These prevent the uploaded images from being overwritten. The following placeholders can be used:

n	Camera name
Y	Year
M	Month
D	Day

If the existing image should always be overwritten, then a file name without placeholders should be used.

Save your settings.

Creating an activation:

In the current view, select the *Activations* point from the list on the left.

Create a new activation with the following data:

Detector: Permanent alarm or external detector; **Timer:** Always or user-defined; **Camera:** As required; **Process:** Set FTP upload; **Archives:** None

You can find further information on creating activations under point 3.4.9.

3.4.6 Creating a video output process

Each video card has at least one video output. The video output can be controlled using three different modes.

These are as follows:

- **Activity detection** (camera is displayed when activity is detected)
- **Manual** (currently selected camera is displayed on video output)
- **Sequencer** (set cameras are displayed on the video output individually after a defined switching time)

Setting up a process:

Open the system configuration and switch the view switch to the *Actions* view (point 3).

Select *Video Output* from the list on the left and create a new process using the *New* button.

Assign a unique name for the process. This makes it easier to find the process when assigning the activation.

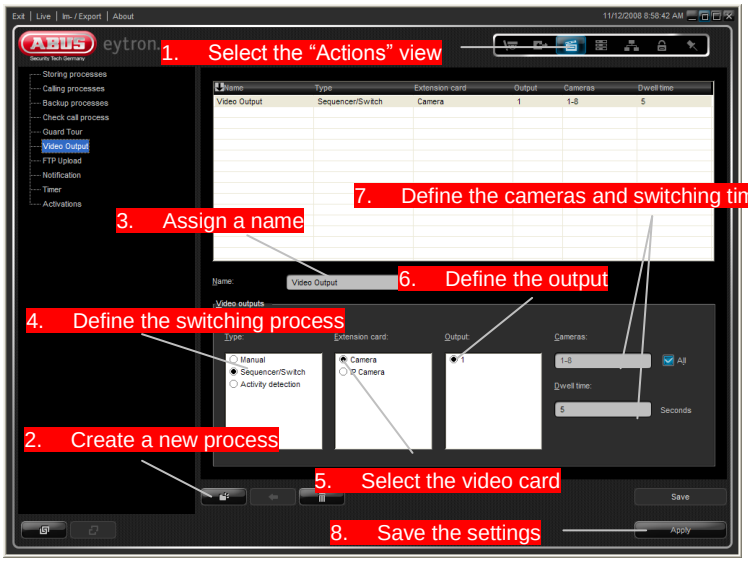
Specify the desired mode (activity detection, manual or sequencer) for the switching process on the video output.

Select a video card to be used for the process (for multi-card operation only).

Define the video output to be used.

Select the camera to be displayed. Individual cameras can be selected using semi-colons or hyphens (e.g. 1-8; 10-12 or 1;3;5;7).

Define the switching time (in sequencer mode only) and save all the settings.



Switch the view switch in the system configuration to the *Digital I/O* view (point 2) and open the *Virtual alarm detector* point.

Activate virtual alarm detector 20 *(permanent alarm)* and save the settings.

Switch the view switch back to the *Actions* view (point 3) and select *Activations* from the list on the left.

Create a new activation with the following data:

Detector: Permanent alarm; **Timer:** Always; **Camera:** None; **Process:** Video output process as specified above; **Priority:** 3

You can find further information on creating activations under point 3.4.9 on page 98.

Save the settings and click on the *Apply* button.

The video output process is now set up. To set up further video outputs, repeat the steps above for the corresponding video card.

Note:

A cross-card display of analogue video signals is possible on the ABUS HDVR. Each of the video inputs can then be displayed on a video output.

3.4.7 Playing user-defined audio files in the event of an alarm

The ABUS VMS software allows you to play user-defined audio files in the event of an alarm. Any alarm detector can be used for this.

This is of practical use when movement is detected. If an audio file is linked to the motion detector of Camera 1, the file is played whenever movement is detected.

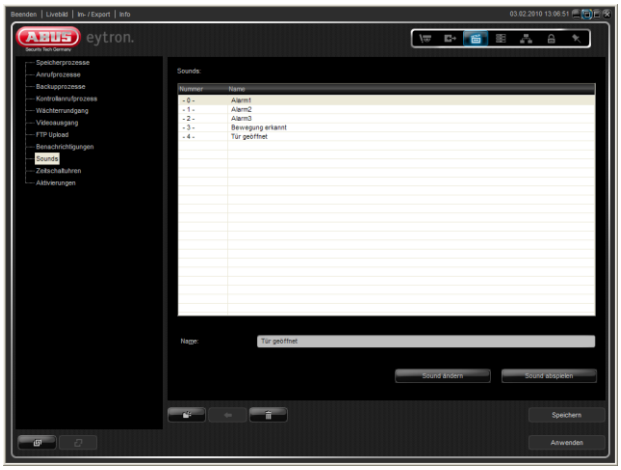
The steps required to set this up are described in more detail below.

Adding audio files

To add the audio file, open the system configuration and move the view selector to *item 3 (Processes).* Then select *Sounds* from the list on the left.

Click *New* to create a new entry and select the audio file to use.

When it is successfully imported, the message *Sound file saved* appears. The file name is used as the default name. However, to assign the sound more clearly, it is advisable to give it a name according to what it is used for.



Change the name as necessary in the *Name* field and save the settings.

You can click *Change sound* to link existing entries with new audio files.

Click *Play sound* to hear the currently selected audio file.

Note:

The maximum size of the audio file is 1 MB. For recording audio files (.wav), you can use the Windows Audio Recorder, for example.

Linking the audio file to a detector

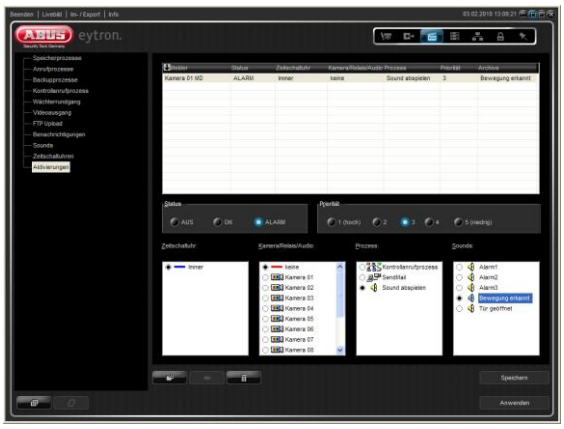
After the audio files have been imported, you can link them to the detector that is currently activated. Go from the *Sounds* item to *Activations* and click *New* to create a new activation.

Now choose the detector to be used for playing the audio file and click *OK*.

If the detector you want is not in the list, you may have to switch it on first. You can find an overview of all the detectors that can be used and how they are activated in section 3.5 on page 102.

Next go to the *Camera/relay/audio* columns and select *None* to make the *Play sound* process appear in the *Processes* column. You must select this process as the process to be used.

Finally, you must link to the audio file to be played when the process starts. You can select it in the *Sounds* column.



Save the settings and click *Apply*. The system is now configured for playing audio files.

If you want to play other sounds, repeat the above steps.

3.4.8 Using timers

In the ABUS VMS software, timers can be used to restrict the execution of a process to a set time.

For example, if recording should only be made outside of normal business hours, then this process can be restricted accordingly using a timer.

Setting up a time span

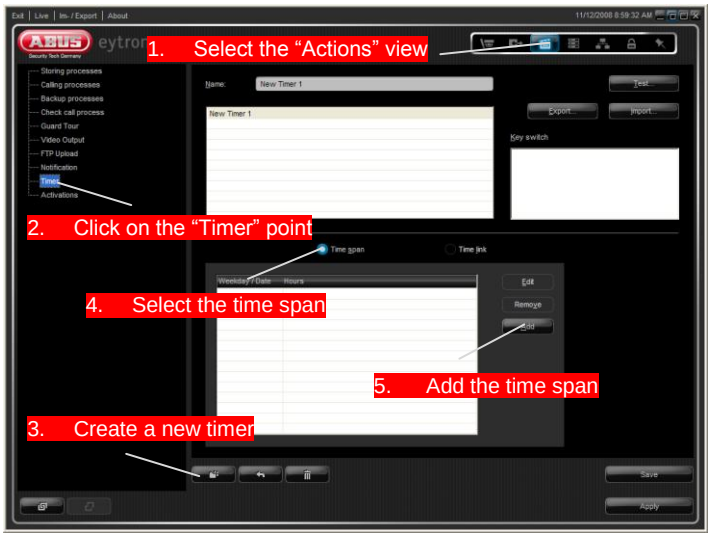
Time spans are simple time definitions used for carrying out recordings or specific actions within a defined time period. This can be a specific day of the week or a specific date. The following steps show how to set up a time span:

Open the system configuration and switch the view switch to the *Actions* view (point 3). Select *Timers* from the list on the left.

Create a new timer using the *New* button and give it a unique name (e.g. *"Outside business hours"*). Select the type of time span.

Click on the *Add* button to create a new time span.

Select the day(s) where the timer should be activated (e.g. Monday - Friday).

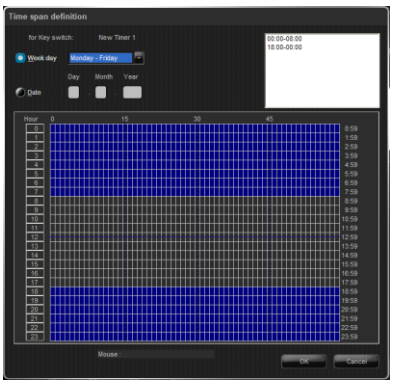


A time can be defined to the minute. Press and hold the left mouse button in the "Times" field. Select the desired time period (in this example, from 00:00 to 08:00 and 18:00 to 00:00).

Complete hours can also be selected by clicking on them.

Press *OK* to close the dialog and save your settings.

The timer is now ready for use. Switch to the *Activations* point. The timer is now added to the timer list and can be assigned to new or existing processes.



Setting up a time link

Time links are used to connect several time spans together. This is useful if you do not want to record camera images on a certain day. The following steps show the configuration of a time link with no recording on holidays and the first day of each month:

Add an *"Outside business hours"* timer (time span) (see example above *"Setting up a time span"*).

Add a second *"Start of month"* timer (time span) with the following data: **Date:** 01.01.**** to 01.12.****; **Times:** 00:00 to 00:00 (the stars here are used as wildcards for each year).

Add a third *"Holidays"* timer (time span) with the following data:

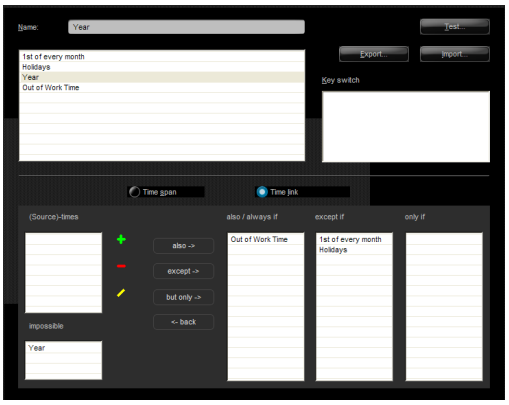
Date: 25.12.**** and 26.12.****; **Times:** 00:00 to 00:00 (a time span can be assigned to several days using the *Add* button).

Add a *Yearly recording* timer (time link).

Add the *Outside business hours* time span to the *"also / always if"* list using the

Add the *Holidays* and *Start of month* time spans to the *"except if"* list by pressing the

Linked processes are then inactive on holidays (25th and 26th December) and on the first day of each month.



Note:

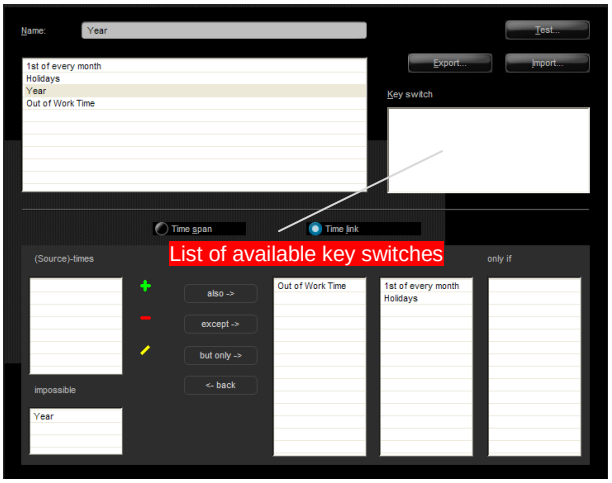
Adding time links allows the creation of extremely complex timers. For example, if you wish to activate a timer permanently on weekends and only outside business hours on workdays, then you can also do this by adding several definitions within a time span.

Connecting a timer to a key switch detector

If you have defined an alarm detector as a key switch, then you can connect it to a timer. A process is then only started when the detector is in the alarm state and the timer is within the configured time.

This function is useful when combining video systems with an alarm system, for example.

If the contact for activating the alarm system is connected to a detector on the video system (and this detector is defined as a key switch), then recording is only started when the alarm system is activated and the system time is outside business hours.



All set key switches are listed in the corresponding key switch list (timer configuration page).

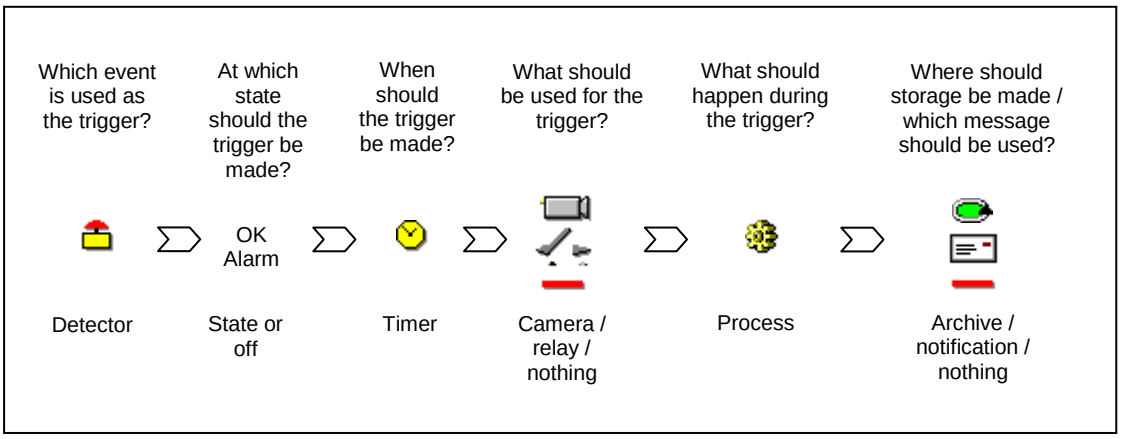
Exporting timers

The *Export* button can be used to transfer the set timers to several systems. In this way, complex time spans or time links only need to be created once, and can then be imported to other systems.

3.4.9 Activations (process links)

Activations are the most important element of the system configuration, and are used to connect the set components (processes, cameras, archives etc.) to each other. Components that are not linked here or are *Off* can never be started.

Each activity is created according to the same procedure, which is laid out as follows:

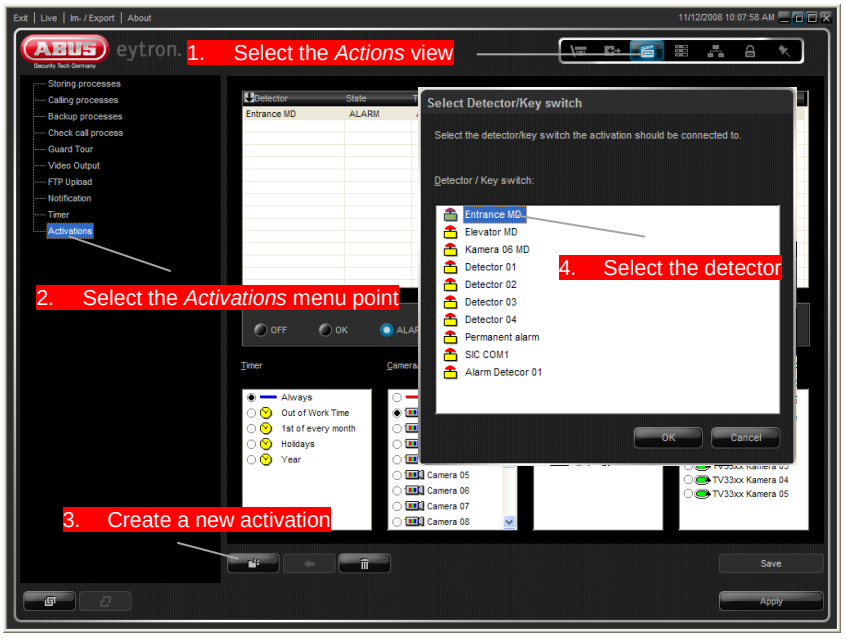


To prevent incorrect configurations, activations must always be created according to this procedure.

The following information describes the necessary steps for setting up and applying the procedure in the software in more detail. However, this information only deals with the actual creation of the activations. Consult the individual sections of this manual for more information on setting up the components (processes, notifications etc.).

1. Selecting the detector:

Open the system configuration and switch the view switch to the *Actions* view (point 3). Select *Activations* from the list on the left and create a new activation using the *New* button. Select the desired detector from the list.



If the desired detector is not listed, then it may have to be activated first. Further information on activating detectors can be found under point 3.5 on page 102.

2. Defining the start behaviour:

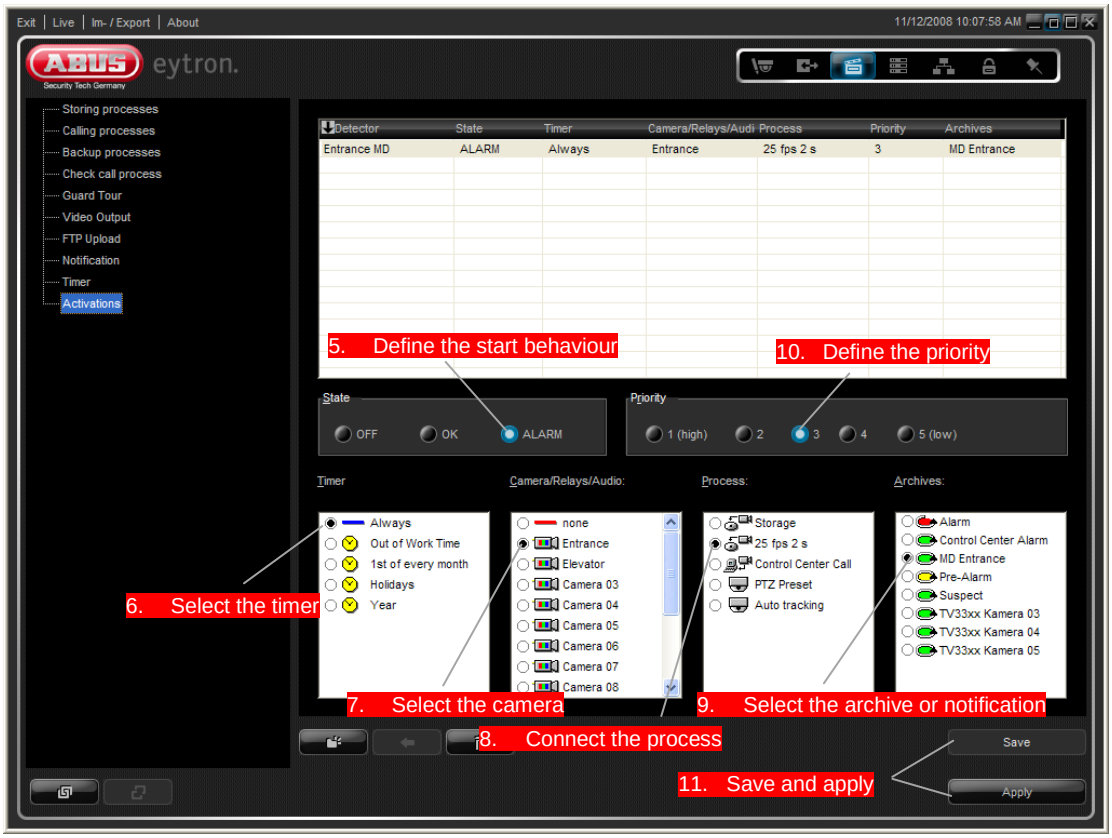
The start behaviour must be defined after selecting the detector. There are three different parameters available here:

Off (process not started when the detector is triggered)

OK (process started as soon as the detector is switched on – *"OK status"*)

Alarm (process started as soon as the detector is triggered – *"Alarm status"*)

In most cases, the "Alarm" status is used. The "OK" status is usually only used in "BGV-Kassen" mode.



3. Selecting the timer:

In the next step, select the timer. This can be used to restrict the execution of the process to a set time. If no timer should be used for the activation, then the standard *Always* entry must be used. More information on using timers can be found under point 3.4.8.

4. Selecting the camera / relay:

The input or output of the components to be used is connected in this field. This can be a camera or relay, or can also be no components. Select the desired components to be used in the activation from the list.

Note:

A camera should not be selected here when the video output or guard tour process is used, as the camera has already been defined when the process was created.

5. Connecting the process:

The process is connected to the activation in the process window. Select the process to be used for the activation here.

6. Connecting the archive / notification:

The final field is used for connecting the archive. If a storage process is selected in the process field, then the available archives are listed here. If a call process is selected, then the text messages for the notification are listed.

All components are now connected and the activation is set up.

When several entries are already present in the list of activations, it is recommended to define a priority for each entry. In this way, important processes are given higher priority when the system is under extreme load.

3.5 Configuring the inputs and outputs (Digital I/O)

The digital inputs and outputs group contains all detectors and relays connected to the system. These can originate from network cameras and video servers.

The ABUS HDVR systems are each equipped with twelve alarm contacts and four potential-free relay outputs.

Virtual alarm detectors are integrated into the system for internal system monitoring. Using these detectors, processes can be set up (e-mail, SMS etc.) and the system can send notifications in the event of malfunctions (camera failure, drive failure etc.).

All of the available inputs and outputs are described in more detail below:

SimUnit detector:

SimUnit detectors are used to simulate external alarm detectors. These detectors are only available after the SimUnit is switched on (see point 3.5.4 on page 108). The detectors switched on here can then be used as normal alarm detectors in the activations.

MD detector (MD detector or IP MD detector):

“MD” stands for Motion Detection (activity detection). A separate detector exists for each camera input (analogue or IP). When motion is detected on a camera image, the corresponding detector triggers an alarm and a connected recording process or alarm dialling is started.

Alarm detector (Detector or IP detector):

Alarm detectors can only be used when an alarm card is installed in the system (pre-installed on ABUS HDVR) or when a network camera or video server is equipped with an interface for detector inputs.

SimUnit relays:

SimUnit relays are used to simulate external relays. Four relays are added to the list when the SimUnit is activated. These can then be used like normal relays.

The current status of the relays can be seen on the SimUnit interface (see point 3.5.4 on page 108).

External relays (IP relays,relays):

External relays are listed in this group when an alarm card is installed or an IP camera / video server with a corresponding interface is connected.

3.5.1 Virtual alarm detectors

Virtual alarm detectors are integrated in the system in order to react to errors in the system or monitor network interfaces. Virtual alarm detectors are used for a variety of tasks as described below.

Alarm archive is filled up to ...

This detector is triggered as soon as a set alarm archive is filled to 60% or 100%. This detector can be used in “BGV-Kassen” mode, for example.

Camera out of order:

This detector is triggered as soon as a camera signal fails. A test picture is then displayed in the live camera image.

Camera lost focus:

This detector is used for monitoring the camera focus (image sharpness). The detector is triggered as soon as the image is not in focus or deviates too much from the reference value. This only applies to set cameras with the activated *Reference* option (see point 3.2.5).

Camera image too dark:

The brightness of the video image is monitored using this detector. The detector triggers an alarm when a sudden change in brightness is detected. This function also only applies to cameras where the *Coverage* function is activated.

Camera position wrong:

The detector for camera anti-swivel protection triggers when the current video image no longer matches the reference image. This function also only applies to cameras where the *Misplace* option is activated in the camera configuration (see point 3.2.4).

... Outgoing call:

Outgoing connections can be monitored using this detector. Activities can then be logged in an alarm list and evaluated. These detectors are available for TCP/IP, 1. ISDN and 2. ISDN.

... Incoming call:

Incoming connections can be monitored using this detector. Logging can also be made over an alarm list here. These detectors are available for TCP/IP, 1. ISDN and 2. ISDN.

... Call rejected:

This detector is triggered when a connection to a host is rejected (e.g. due to missing authorisation).

Reserved detectors:

Detectors 16, 17, 18 and 23 are reserved for additional functions and cannot be accessed by the system.

Check Call Error:

This detector is triggered when a check call to a host fails.

Check Call OK:

The *Check Call OK* detector is triggered at each successful check call. Check calls can then be logged using an alarm list.

Permanent alarm:

The *Permanent alarm* detector is used for the permanent activation of individual processes. For example, when a video output process is set up, this must be connected to the *Permanent alarm* detector. Timers can restrict the created activations despite the presence of a permanent alarm.

Error in external devices:

External devices can be monitored using this detector. For example, when a connected USB disk drive fails, then this is intercepted by this detector.

Temperature is too high:

This detector is triggered when an excessive temperature is detected on a hardware component (e.g. CPU or mainboard). This only applies when used in the ABUS HDVR / NVR.

Invalid HDD S.M.A.R.T parameter:

This detector is triggered when a HDD S.M.A.R.T error is detected.

S.M.A.R.T (**S**elf **M**onitoring, **A**nalysis and **R**eporting **T**echnology) continuously monitors all important disk drive parameters. For example, a S.M.A.R.T error is triggered when a drive runs at an excessive temperature.

Harddisk failure:

This detector is triggered when a hard disk drive is no longer available on the system.

Note:

The virtual "Harddisk failure" alarm detector does not work when connected to RAID software. In this case, use the monitoring software on the RAID controller to resolve error messages.

Fan failure:

This detector is triggered in the event of a fan failure (e.g. CPU or housing fan). This function is also only used in the ABUS HDVR / NVR, as the fan speed of each individual mainboard is different.

3.5.2 Activating the external detectors

If an alarm card is installed in the system, then the detectors can be switched on under *Digital I/O* → *Alarm detectors*.

If the card inputs should only be used as detectors, then the detector type must be selected. After doing this, assign the detector a unique name.

The “Break contact” function is used to define the detector behaviour.

When this function is not activated, the detector functions as a Normally Open contact as standard (“OK” status) and is closed in the event of an alarm (“Alarm” status). The detector functions as a Normally Closed contact when this function is activated, meaning its functions are inverted.

Using the detector as a key switch:

When a detector is defined as a key switch (), then timers can be connected to it. These are only activated when the detector has the “Alarm” status.

The following steps show the set-up of a key switch detector:

1. Open the system configuration
2. Access the *Digital I/O* menu point
3. Select the detector category to be used for the key switch function
4. Switch the status (“Off”, “Alarm”, “Key switch”) to *Key switch*
5. Save your settings

You can now link the detector to the desired timer using the *Actions* → *Timers* menu point.

3.5.3 Activating the external relays

The relays can be configured in the system configuration under *Digital I/O* → *Relays*.

The name, hold time and manual control for each relay can be configured here, as can the "Manual Reset" and "Hold" options. More details on these points can be found below.

Hold time:

The hold time specifies how long the relay should be closed when used with edge control.

Manual control:

Level:

When the relay contact is used with level control, the contact remains closed until opened manually by the user.

Edge:

When the relay contact is used with edge control, the contact remains closed until the set hold time has expired.

Manual reset:

When this option is activated, a relay which has been closed by an activation can be reopened manually by a user.

Hold:

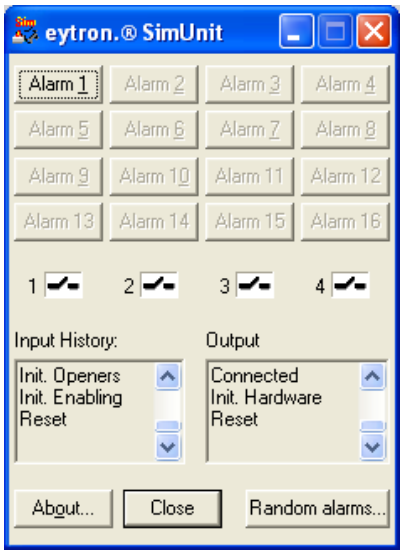
When this option is used, the relay remains closed when it has been activated by a remote user over the network and the system connection has been terminated.

Note:

The "Edge control" and "Level control" options can also be set for the relay in the activation. When creating the activation, ensure that the same control mode is used as on the relay.

3.5.4 Using the SimUnit

The SimUnit is used for the simulation of external alarm inputs and relay outputs (does **not** apply to ABUS VMS Basic).



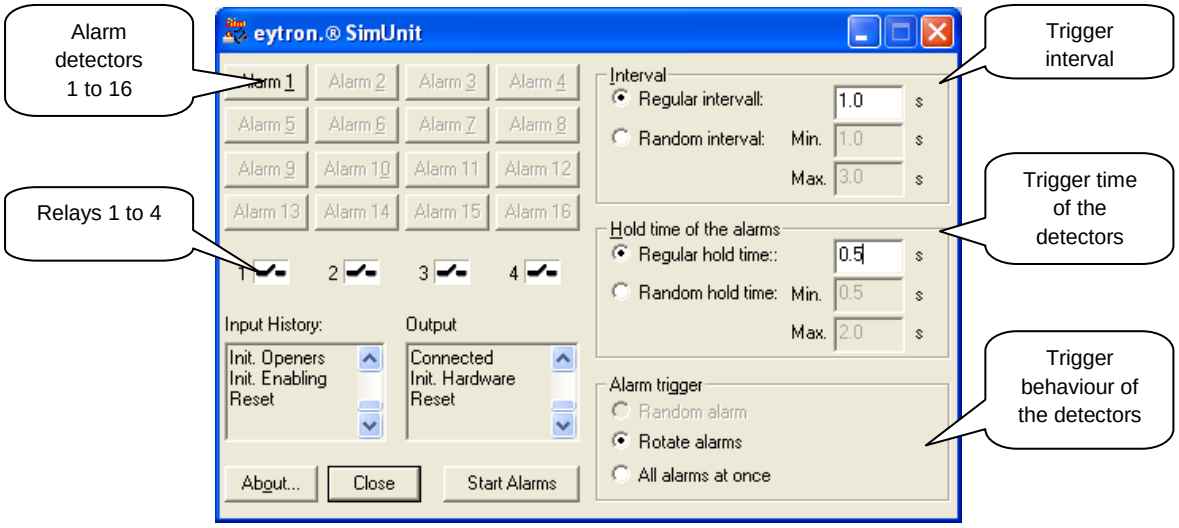
Using the SimUnit, complex application cases can be simulated in advance and any problems can be analysed.

When the SimUnit is activated, 16 detectors are added to the alarm detector list and 4 relays are added to the relay list.

The current status of the interfaces can then be changed or queried using the control panel.

Time-controlled alarm triggers can be generated using the *Random alarms...* button. The time interval, hold time and trigger behaviour can be changed here accordingly.

To switch on the SimUnit, open the system configuration and access the *Digital I/O* menu point (point 2). Select the *SimUnit* menu point from the list on the left and check the *On/Off* box. Save the settings and click on the *Apply* button.



3.5.5 ABUS serial alarm

Using the Serial Alarm Unit, external devices such as cash machines (ATMs) or cash desk systems (POS) are integrated into the software (does **not** apply to ABUS VMS Basic). Communication to the external devices is made over the serial interface.

When a system has been set up in the Serial Alarm Unit, a new detector appears under “Detector/Key switch”. This can then be connected using the activations.

If this detector is then connected to a storage process, the video data is then saved in parallel.

The necessary data (account number, item number, bank code etc.) can then be accessed over the search function and the related images can be viewed.

The optional configuration instructions should be used when setting up a cash machine or POS system.

3.5.6 CASA10010

You can connect wireless components to the VMS software using the IP alarm module (CASA10010). The following is an overview of the number of modules that can be connected to the VMS software.

Software	Basic	Professional	Enterprise
Number	1	2	4

You can use the ABUS IP Installer to identify the IP address of the IP alarm module. Set the connection in the IP alarm module to “Secvest IP” to complete the preparations for setting it up in the software.

Then click “Save + apply” to complete the setup. You can now use two alarm inputs or outputs in the software.

Make sure the wireless components have been correctly taught in the IP alarm module. To use the wireless outputs, put them into teach mode and then select output group 1 or 2 to confirm.

3.6 Security settings

New users can be added and the system access for each individual user can be configured in the security settings.

In addition, logged-in users can be automatically logged out and existing network connections can be disconnected after a specific time.

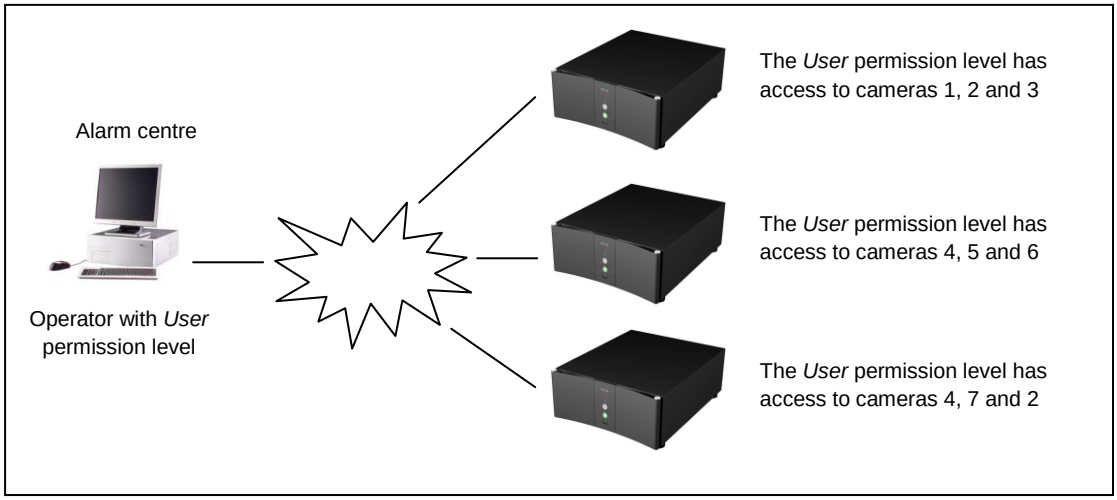
Further information on the individual configuration points can be found below.

3.6.1 Creating a new permission level

Permission levels are an important part of the ABUS VMS software.

Using these levels, database access, camera access or configuration rights in the local system configuration can be created separately for each user.

As the permission level always applies to the local system, individual permission levels can be configured for one user on several hosts. The following diagram shows a configuration example with one alarm centre and three hosts:

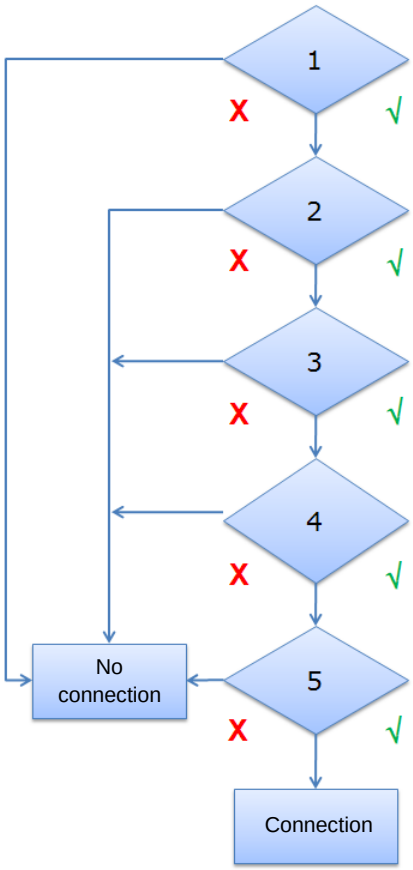


This option can no longer be seen by the user when a permission (e.g. creation of storage processes) is revoked.

Authorization level	Privilege
Supervisor	Viewing live images from all cameras Access to all recordings (archive) Opening the system configuration
Operator	Viewing live images from all cameras Access to all recordings (archive)
Guest	Viewing live images from all cameras

You can assign a password for the permission level using the corresponding *Password* option. This is necessary for security reasons when establishing a connection to hosts.

The internal access check during connection is made according to the following rules:



1. Has the password on the host permission levels been set up?

2. Does the permission level name exist on the host?

3. Does the password match the permission level?

4. Does the name in the host list on the local station match the local station name on the host?

5. Does the local station name match the host name in the host list?

To create a new authorization level, open the system administration and move the view selector to *Security (item 6)*

From the list on the left, select *Authorization levels* and click *New* to create a new authorization level.

Give it a clear name. This makes it easier to assign the level to users later.

Now define the privileges for the authorization level.

In the *Camera/relay* field, you can define the cameras or relays that the user can see or control.

In the *Playback* field, you can define access to the database. You can configure three parameters for each archive, as described below.

BI - The user is only permitted to see the recorded images (BI = images)

BD - The user is permitted to see images and image data (POS, ATM) (BD = images/data)

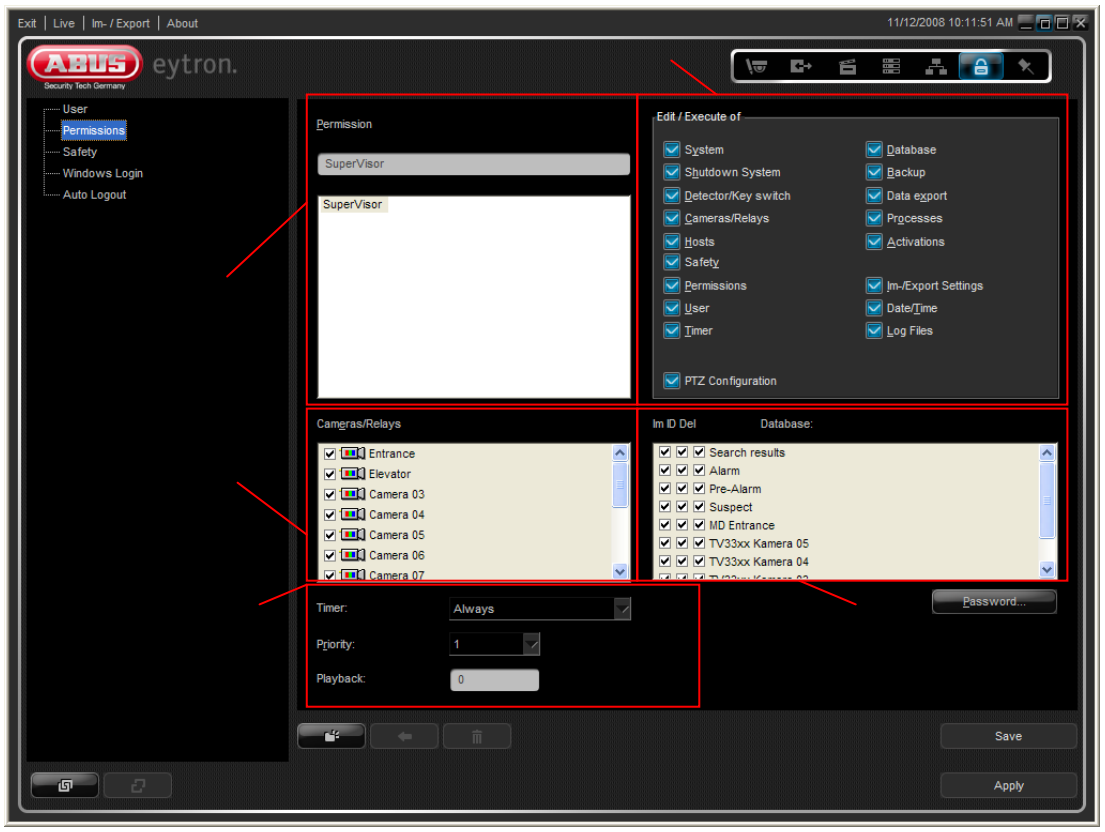
LÖ - The user is permitted to delete images in the archive (LÖ = delete)

The authorization levels can be restricted not only to camera and database access, but also to individual parts of the software. In this case, a distinction is made between authorizations in the client and the system configuration.

For example, if *Storage* permission is withdrawn from the authorization level, the system will not let these users make backups.

Users cannot see permissions that are have not been set up for them in the system configuration. For example, if *Database* authorization is not enabled, the user will not see any of the sub-items in the *Database/storage* view.

Click *Password* to issue a password for the authorization level. This is required for security when connecting to other hosts and is queried with every connection.



The permission level is now created. Save your settings and assign the permission level to a user as described in the following section (*"Creating a new user"*).

Note:

The possibility of assigning access rights depends on your own access rights as a user. Only the supervisor has full authorisation.

If you log on to a remote system, then the permission levels of the remote system apply. The connection is rejected if this permission level is not set up.

If new archives are added after the creation of the permission level, then the access authorisation must be added here. Otherwise, the user cannot access the new archives.

3.6.2 Creating a new user

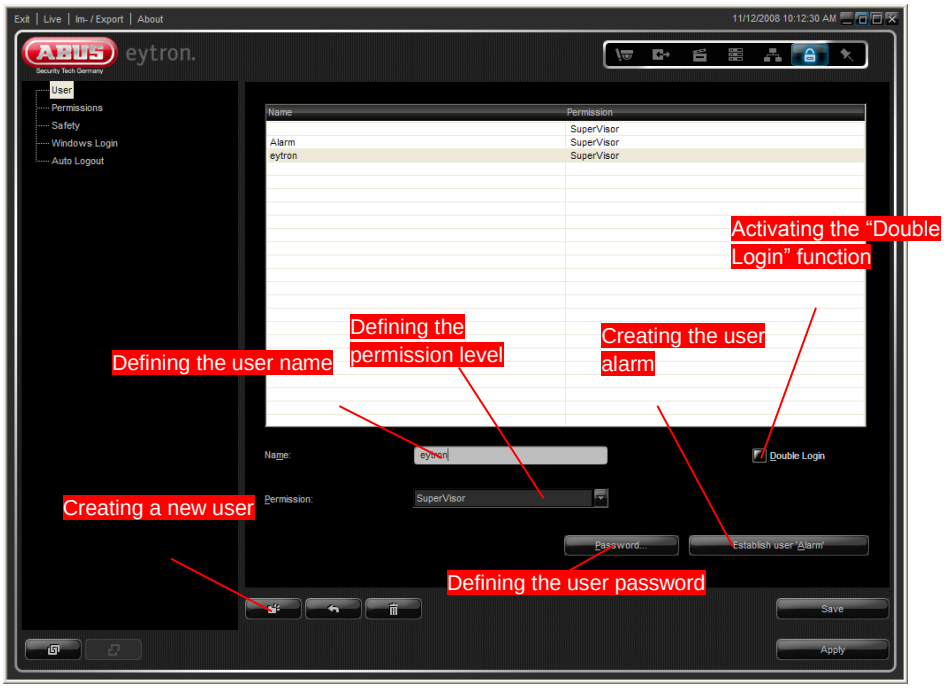
Any number of users can be created in the ABUS VMS software. After they have been created, the users must be assigned to an existing or previously created permission level.

1. The default user is **admin**; the password is **12345**. For security reasons, this user should be deleted after the initial set-up or replaced with a new user.

Ensure that at least one user with supervisor authorisation exists at all times, as complete configuration of the system can only be made by these users.

Creating a new user:

1. Open the system configuration
2. Switch the view switch to the *Security* view
3. Select *User* from the list on the left
4. Click on the *New* button
5. Assign a name for the user
6. Assign a permission level to the user (see point 3.6.1)
7. Assign a log-in password for the user. Please note the optional use of security guidelines (see point 3.6.3)
8. Activate the “Double Login” function (optional)



When the “Double Login” function is activated, the user may only log in to the system when a second user also authenticates themselves.

When the user logs in to the system and “Double Login” is activated, then the log-in dialog appears again with the prompt for a second user log-in. Any user from the local user account list can be used here.

Only then is access to the system permitted, with the guarantee that a user cannot manipulate the system without being detected.

User alarm:

The user alarm is set in the system as standard for the users. If this is not the case, it can be created using the *Establish user ‘Alarm’* button.

This is used to execute an automatic log-in and display the host images in the event of incoming alarms on a system found in the log-in window.

The user alarm has all relevant authorisations for displaying the messages. The password and permission level are specified by the system and cannot be changed.

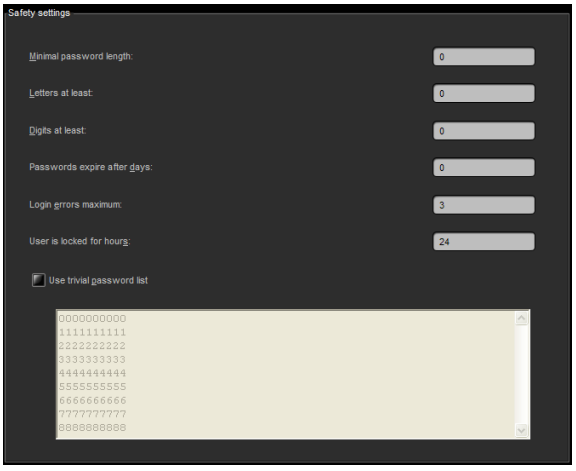
Note:

Clear guidelines for user passwords can be created in the system, which leads to increased levels of security. Examples of these guidelines are a minimum password length, a combination of figures and letters or a list of forbidden passwords (e.g. “12345” or “abcde”). A detailed description of these guidelines can be found below.

3.6.3 Security guidelines

Rules can be defined for the user log-in in the security guidelines. Examples of these rules are a minimum password length, a minimum number of figures and letters or a list of forbidden passwords (common / negative password list).

All guidelines apply to the global system. These cannot be assigned to individual users.



Configuration of the security guidelines can be found in the system configuration under the *Security* menu point.

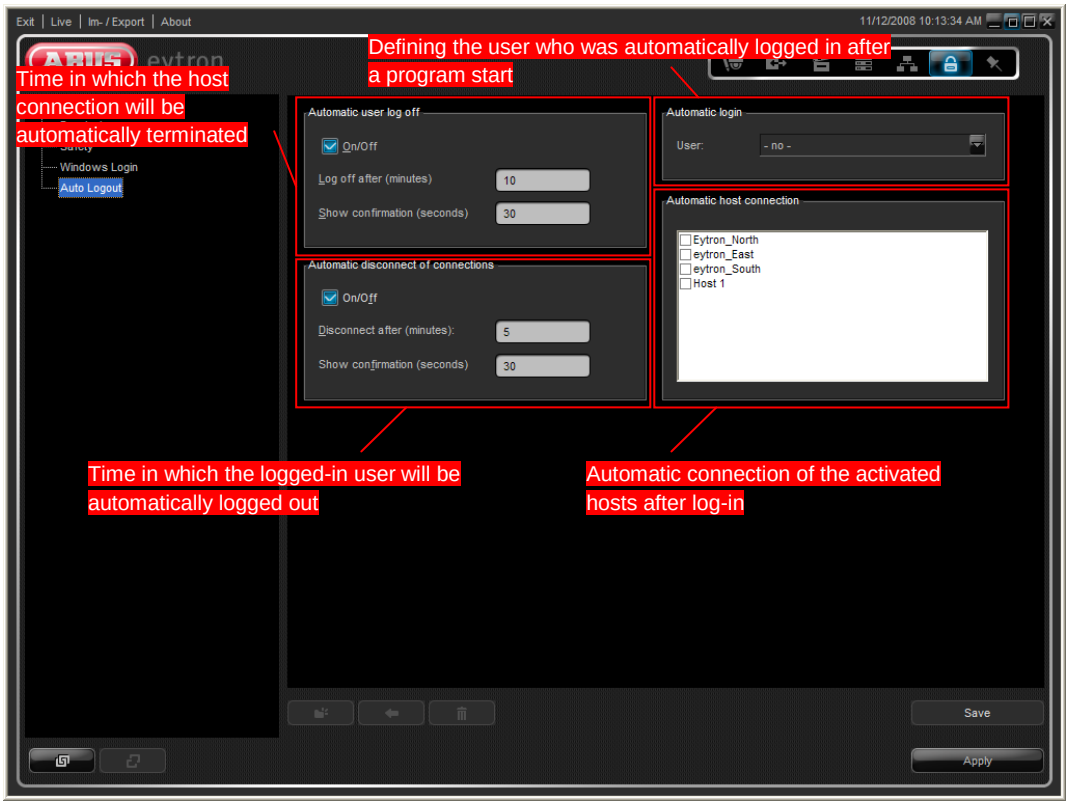
After creating or changing security guidelines, the changes must be saved and the system restarted using the *Apply* button.

Note:

If users have been created before the security guidelines came into use, then the password for these users must be assigned again. The security guidelines do not apply to existing passwords.

3.6.4 Automatic logging in and logging out of users

Using the *Auto Logout* function, users can be logged out automatically after a set time or existing connections can be terminated.



When this function is activated and one of the corresponding times has been reached, then the logged-in user is notified that the network connection will be terminated in *n* minutes or the user will be logged out in *n* minutes.

This function also provides support for automatic log-in and the subsequent automatic connection to a host. An advantage of this is that the users set here are logged on again and the connection is established again immediately (e.g. following a system reset).

Changes to these parameters are made in the system configuration under the *Auto Logout* menu point (Security view).

3.6.5 Windows login

The Windows login allows you to log in automatically on the operating system.

If this option is enabled, the configured user is automatically logged in on the operating system after Windows is restarted and the recording is resumed.

Otherwise, the system stops at the Windows login when restarted.

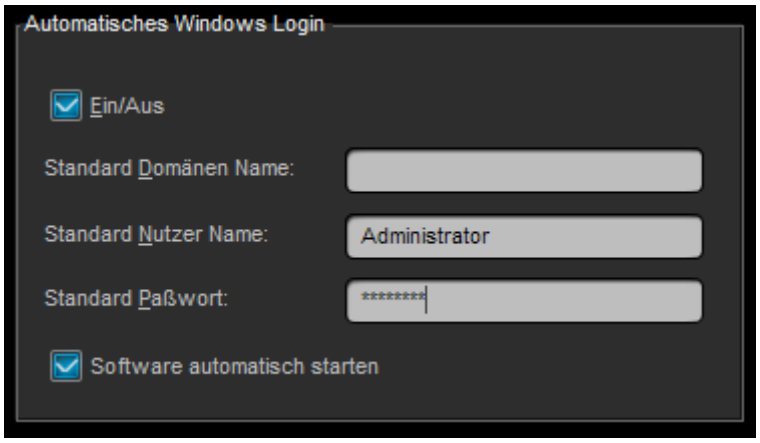
To activate the Windows login, open the system administration and move the view selector to Security *(item 6)*.

In the lift on the left, then select *Windows login* and select the checkbox in the *On/off* field.

Enter the standard domain name, the user name for logging in and the associated password. Save the settings and click the Apply button.

To run the software automatically after the user logs in, also select the checkbox in the *Start software automatically* field.

The system is now configured for automatic Windows login.



3.7 Network configuration

All settings used for incoming and outgoing communication are managed in the network configuration. This includes the configuration of networks / ISDN cards or notifications to specific recipients. All possible settings are dealt with individually below.

3.7.1 Configuration of the network module (TCP/IP)

The network module is used to transfer images to another ABUS system using the local network or the Internet.

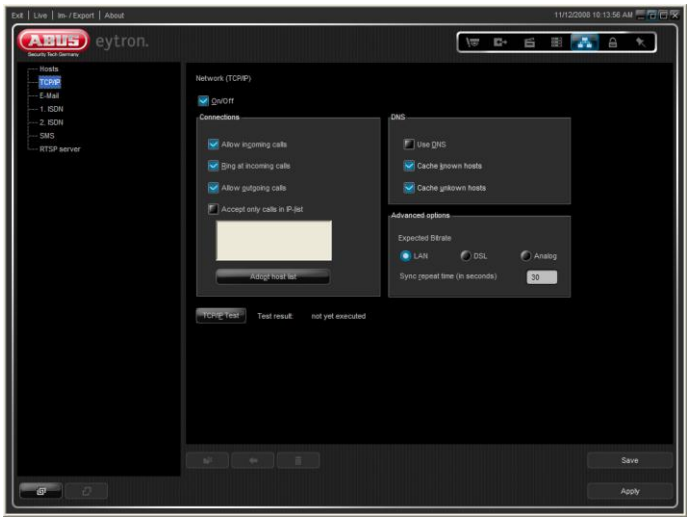
Security or bandwidth settings can be made for this module in the system configuration.

To change the settings, open the system configuration and switch the view switch to the *Network* view. Select *TCP/IP* from the list on the left.

The network module can be switched on and off here. Additionally, incoming calls can be activated or restricted to the clients in the host list.

If a remote system is connected (e.g. over DSL), then the bandwidth for image transfer can be adjusted under *Expected Bitrate*.

From version 6.6 onward, you have the option of individually configuring the network port to be used.



From version 7.0 onward, you can individually select the web interface port.

Note:

A connection to another system over the network is only possible when the network module is switched on. This also applies to access attempts from the web application.

3.7.2 Activating the RTSP server

By activating RTSP support (Real-Time Streaming Protocol), the system can be accessed using the relevant terminal devices (RTSP clients, mobile phones etc.).

The bandwidth can be configured in the server module over two separate streams. The first stream contains the video in full resolution. A bandwidth of up to 2 MB per stream is required here.

The second stream is for low-bandwidth connections, such as mobile phones. Each stream is restricted to 64 kbit. However, access using the second stream only applies to the connected analogue cameras and not to the IP cameras.

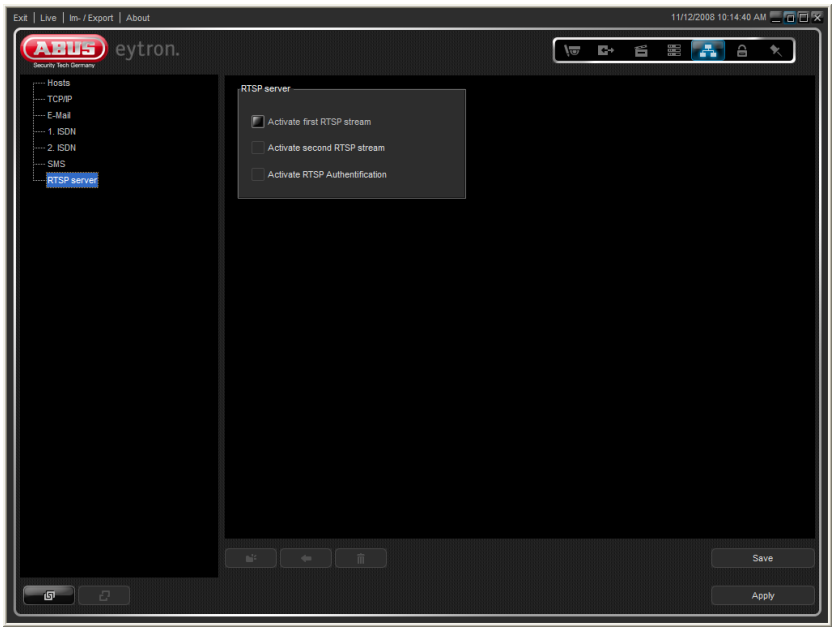
Access control is made by the entered URLs, which are made up as follows:

1st camera	=	*rtsp://Recorder-IP/camera1*	*(1st stream)*
2nd camera	=	*rtsp://Recorder-IP/camera2*	*(1st stream)*
.			
.			
10th camera	=	*rtsp://Recorder-IP/camera10*	*(1st stream)*

If the second stream should be used, then *.mobile* should be added to the URL as follows:

1st camera	=	*rtsp://Recorder-IP/camera1.mobile*	*(2nd stream)*

The recorder IP must be adjusted according to the IP address of the recorder system.

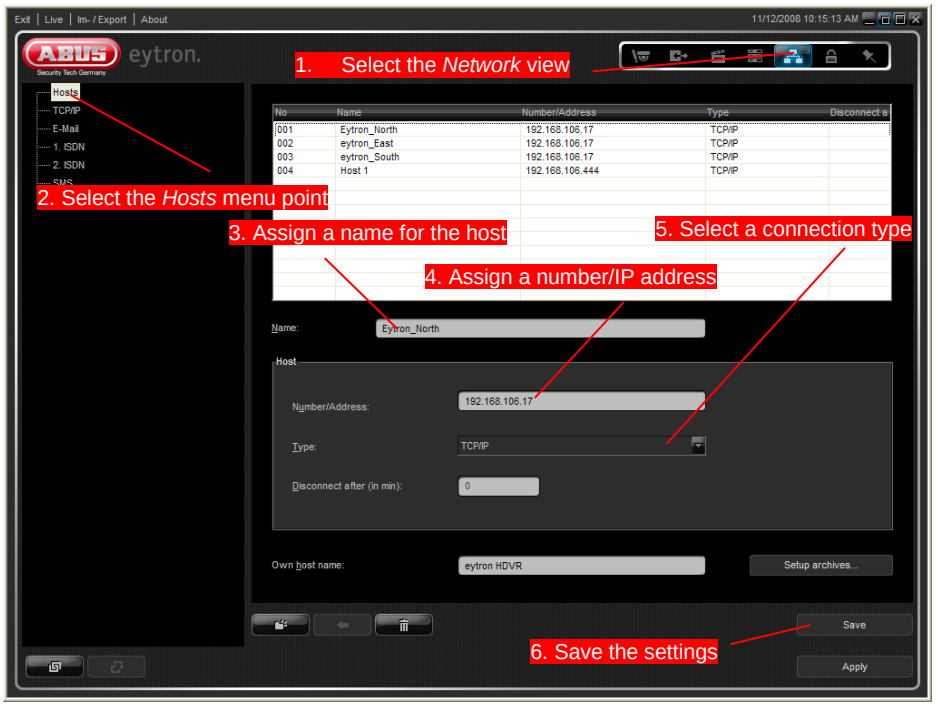


3.7.3 Creating a new host

A host must first be entered in the host list before it can be called up. The host can then be called up over LAN, DSL or ISDN.

To create a host, open the system configuration and switch the view switch to the *Network* view.

Select *Hosts* from the list on the left and create a new host using the *New* button. Assign a name to the host.



Note:

The maximum permissible number of hosts can be found in the table under "Upgrades" at the start of this manual. If more hosts are required, then an upgrade must be made to the next system version.

The call number must then be entered under *Name*. This can be a telephone number, IP address, e-mail address or mobile phone number.

Select the corresponding transmission path according to the number. This is comprised of the entered number or address.

To terminate the host connection automatically after a defined time, the desired time period in minutes can be entered under *Disconnect after:*. The connection is not terminated when "0" is entered here.

From software version 6.6 onward, you can set the connection speed for each host. The available speeds are LAN, DSL and Analog. These three options result in the following connection restrictions:

LAN	=	the full bit rate is transferred
DSL	=	each video stream is reduced to 128 Kbit
Analog	=	each video stream is reduced to 64 Kbit

If you want to automatically disconnect from a host after a certain time, select *Disconnect after:* and enter the time in minutes. If you enter a value of 0, the connection is not terminated.

The host has now been created and can be selected and connected in the *Hosts* view.

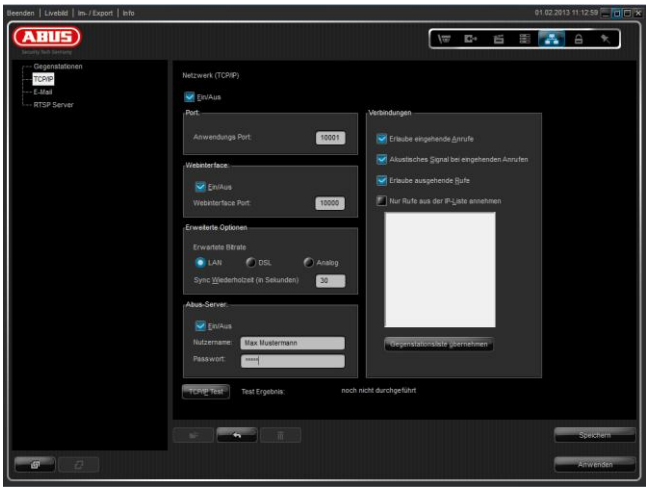
The settings must be saved after all changes have been made. As no archives exist for alarm or standard connections on this host, you will then be prompted to set these up by the system. If alarm dialling is not set up in the system, then this dialog can be closed by entering *No* or *No, all*.

The host is now created and can be dialled or connected over the Hosts view in the user interface.

Note:

Ensure a sufficient upload rate is in place when DSL connections are used, as bottlenecks can otherwise occur during the transmission of video data. For example, a DSL2000 connection (ADSL) has a download rate of 2000 kbits/sec. (ca. 250 KB/sec.) and an upload rate of 192 kbits/sec. (ca. 24 KB/sec.). This is not enough for a satisfactory transmission of image data from several cameras. A higher bandwidth (e.g. DSL 6000/16000) or a SDSL connection is recommended here.

3.7.4 Changing the network port



The network port may be changed in order to operate multiple recorders via a router (port forwarding). Because the router can only forward a network port to a single IP address, the port has to be modified in order to control several recorders.

This is done using the system configuration. To change the network port, open the system configuration and move the selector to *Network (item 5).* Select *TCP/IP* from the list on the left.

Enter the network port to be used in the *TCP Port* field and save the settings.

Then click *Apply*.

The configured network port is now used by the software.

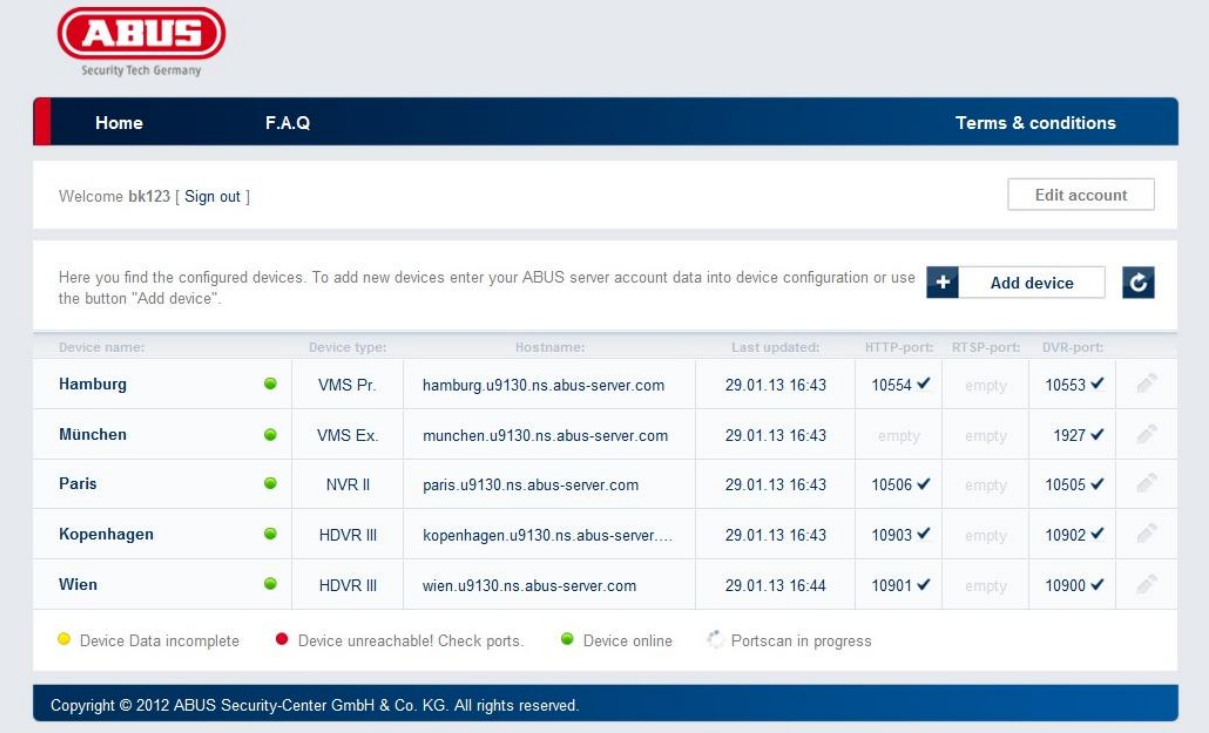
Note that you must also specify this network port when creating a new host.

For existing hosts, you must add the network port to the IP address or URL. For more information see section 3.7.3 on page 121.

From version 7.0 onward, you can configure and enable the web interface port here. By default, Port 80 is used and enabled. To enable access to the recorder system, forward the corresponding port in the router and install the VMS web interface on your recorder system.

For version 7.1 and up, you can log your VMS system onto the ABUS server. This requires a valid account on the ABUS server. Enter your user data and click Save and Apply.

In order to ensure that the VMS and web interface ports work, forward both ports in your router beforehand.



You can now edit the newly created port name and then use it in your VMS system as a host connection, for example.

3.7.5 Using notifications

In order for the system operator to react to errors or incoming alarms, the ABUS VMS software can be used to send a notification to one or more recipients in the event of an error.

This can either be an e-mail notification or a direct notification to another VMS system.

3.7.5.1 E-mail notification

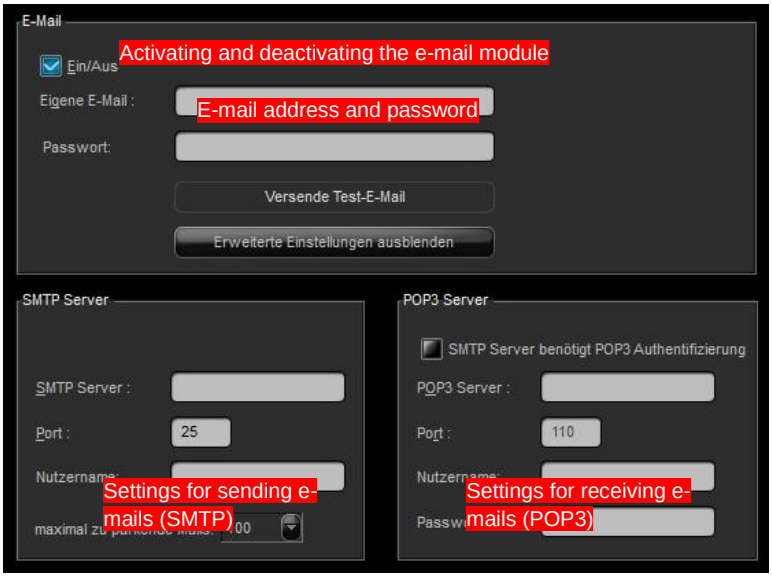
Bevor Sie Meldungen per E-Mail absetzen können, muss in der Systemkonfiguration erst ein entsprechendes Zugangskonto (Absenderadresse) eingerichtet werden. Dies wird im nachfolgenden Punkt näher beschrieben.

Einrichtung der Absenderadresse:

Öffnen Sie die Systemkonfiguration, schalten Sie den Ansichtsschalter auf die Ansicht *Netzwerk (Punkt 5)* und wählen Sie in der linksstehenden Liste den Eintrag *E-Mail* aus.

Activate the *On/Off* field and enter your e-mail address and password.

From version 7.2 onwards, the SMTP and POP3 server data is entered automatically for well-known e-mail providers. If the system does not recognise the provider, you can enter the server data manually using *Show advanced settings*.



The following settings are needed for e-mail notifications.

1. E-mail account set up correctly
2. Alarm detector activated under *Digital I/O* → *Detectors*
3. Recipient defined under *Network* → *Hosts*
4. Dialling process defined under *Actions* → *Dialling*
5. Notification text defined under *Actions* → *Notifications*
6. Timer created under *Actions* → *Timers* (optional)
7. Activations set up

1. Setting up the e-mail account

A fully set up e-mail account is needed to send e-mails. If no e-mail account has been set up, then this can be made over the Internet using a free e-mail provider. You will then receive an e-mail address, user name, password and the addresses for sending (SMTP) and receiving (POP3) e-mails. This data is then used in the software.

2. Activating the alarm detector

Switch to the *Digital I/O* → *Detector/Key switch* menu point and activate the detector used to trigger the process.

3. Creating a receiver

Select *Hosts*, then create a new host using the *New* button. Specify a name and e-mail address for the host. Select the "E-mail" connection type, then save your settings.

4. Setting up the dialling process

Access the *Actions* → *Dialling* menu point and add a new dialling process. Assign the process a unique name and select the host (e-mail recipient) created earlier. Save your settings.

5. Creating a notification text

Notification texts contain the actual message. This is then sent to the recipient by e-mail.

Access the *Notifications* point.Create a new notification with a message text, then save your settings.

6. Creating a timer (optional)

To execute the complete process according to a user-defined timer, it must first be created under *Actions* → *Timers* (see

Point 3.4.8). Alternatively, the *"Always"* timer can be used.

7. Setting the activation

Switch to *Activations* and create a new activation with the following data:

Detector: Alarm detector as required; **Timer:** Always or user-defined (step 7); **Process:** Dialling process (step 5); **Notification:** Text (step 6).

Note:

Only text messages can be sent when using e-mail notification. Use the e-mail export function to send image data (see point 3.4.9).

3.7.5.2 Direct notification

Direct notification transmits simple text messages to another ABUS system. A camera can also be transmitted in addition to the text message. The setting up of an account is not necessary in this case.

The direct notification functions are the same as those used for alarm dialling. To set them up, proceed as described under *Setting up alarm dialling* (see point 3.4.3.2 on page 86).

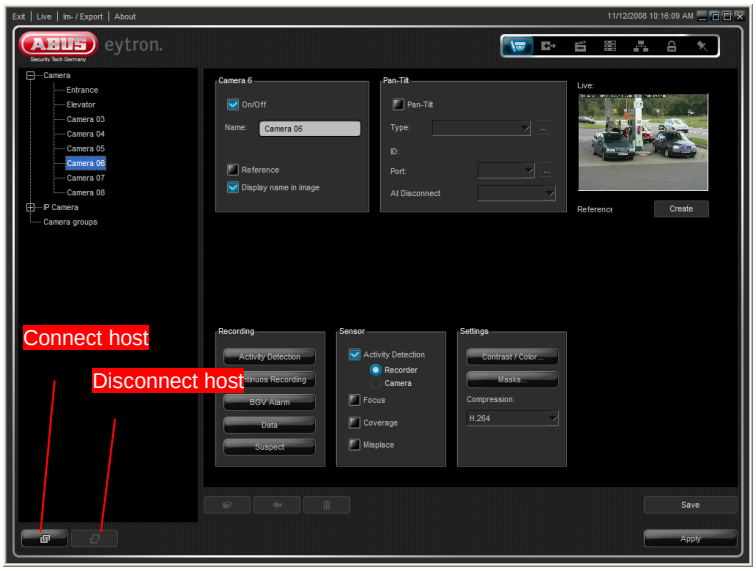
3.7.6 Sending/receiving configurations from a host

When several ABUS HDVR systems are connected together in a network, then all recorders can be managed and configured centrally (e.g. using a command centre (host)).

Examples of this can be a change to the camera name or adding/changing users and permission levels.

The current configuration of a remote host can be called up using the *Connect* button in the local system configuration.

The configuration can then be changed as desired and backed up using the *Disconnect* button. The host is then automatically initialised with the new configuration.



Note:

The remote recorder must be entered under the "Hosts" menu point in order to receive a configuration (see point 3.7.3).

3.8 Miscellaneous settings

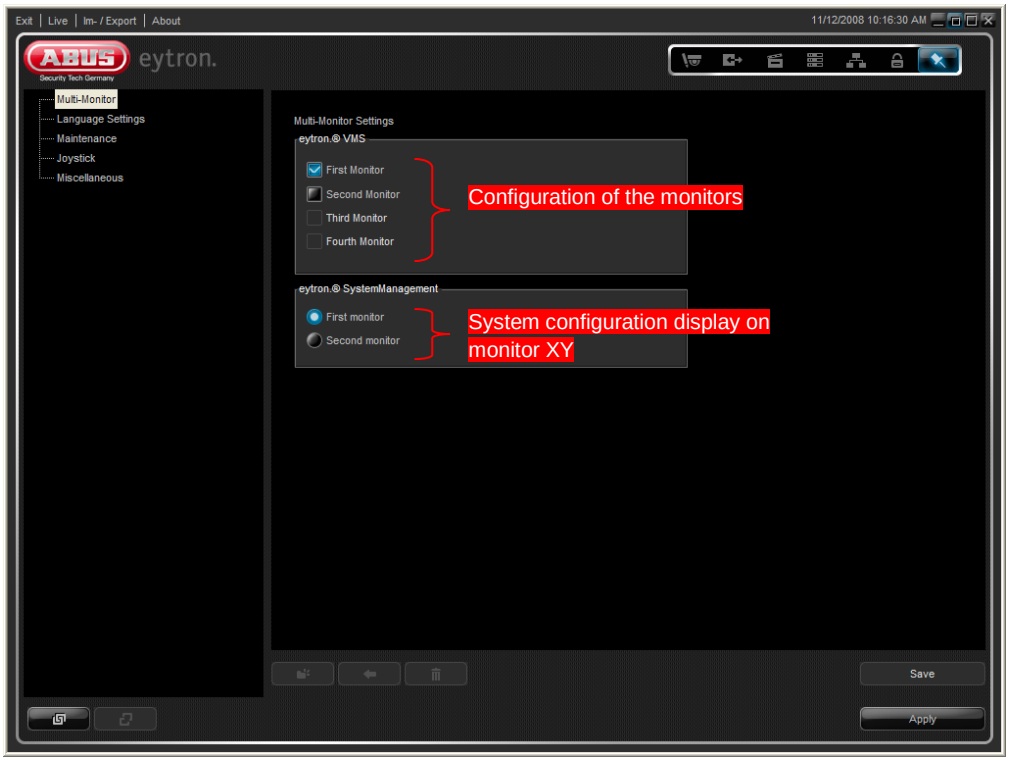
The *Miscellaneous* view contains all settings which could not be grouped under the other system views but remain important for configuring the software.

These points are described in more detail below.

3.8.1 Multi-monitor operation

The ABUS VMS software is intended for operation with up to four monitors. The use of more than one monitor is dependent on the successful configuration of the Windows display settings (dual-head, quad-head). Consult Windows Help if you experience problems during the configuration.

Multi-monitor operation can be switched on under *Miscellaneous* → *Multi-Monitor* following successful Windows set-up in the system configuration. The corresponding boxes must be checked for each of the monitors to be used. The settings must then be saved and the system restarted.



Each monitor can now be used for the following interactions:

1. Live, LivePlus or Playback mode
2. Simultaneous display of a camera on all monitors
3. Use of the joystick and keyboard
4. Use of various image geometries
5. Storage of favourites
6. Display of camera groups

Note:

The maximum permissible number of monitors can be found in the table under "Upgrades" at the start of this manual.

3.8.2 Language settings

The language settings are used to change the software to the current operating system language.

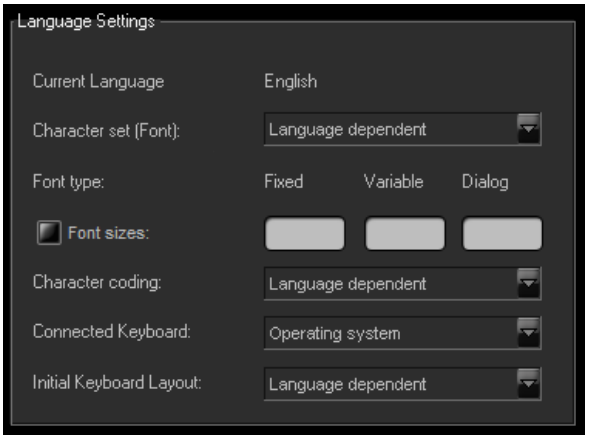
Changes to the character set or font size are only necessary when other characters (e.g. cyrillic) are displayed on the interface.

This is because the database can only save the characters in the language-specific ANSI multi-monitor character set. When archive names are specified in the database with cyrillic characters and a new language is accessed, then the character set and coding must be set to cyrillic for the characters to be saved correctly in the database.

The configuration points are described in more detail below.

Current Language — Shows the current system language (language selection following system log-in).

Character set (font) — The text font is defined here.



Font types

Fixed:	Defines the font type and size for printing and in certain texts where a uniform character width is easier to understand.
Variable:	Font size and type for window texts and headings.
Dialog:	Font size and type for text elements in dialog windows.

Character coding	Defines the character coding for storage in the database.
Connected Keyboard	The layout of the keyboard connected to the system is specified here.
Initial Keyboard Layout	The selected keyboard type for the start of a program is defined here. The keyboard layout can be switched at any time by pressing F11 (e.g. German → English, English → German).

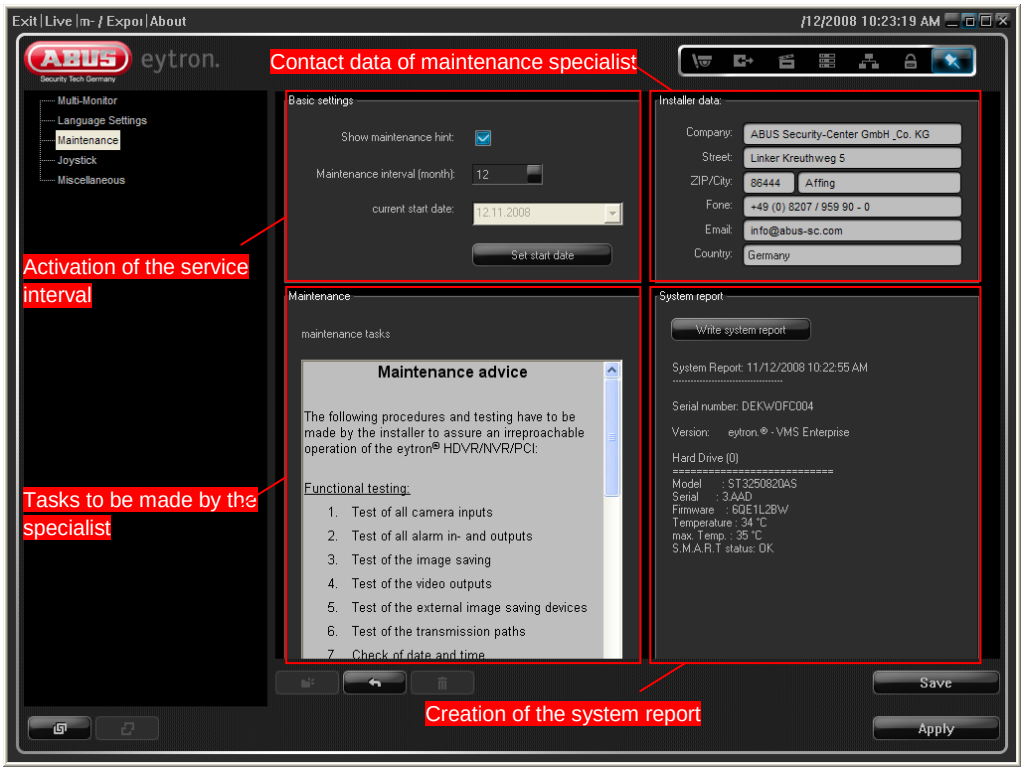
3.8.3 Maintenance

The maintenance dialog offers the possibility of defining a maintenance interval for certain operating periods. In this way, possible system failures can be actively prevented (ABUS HDVR only).

When the first maintenance period is reached, the software automatically displays a message on the monitor prompting the user to contact their maintenance specialist.

The specialist then carries out all relevant maintenance tasks (e.g. checking the fans and drives, cleaning the system) and resets the service interval.

A service report with the current system status (drive temperature etc.) can also be created in the maintenance dialog for documentation purposes.



Access to the maintenance dialog is protected by a password. For a system log-in, **“installer”** should be entered as the user name and **“installer40”** as the password.

3.8.4 Connection of a standard joystick

In the joystick dialog, you have the possibility of using a standard Windows joystick to control pan/tilt cameras.

The correct calibration of the joystick in the Windows Control Panel is a requirement for correct operation.

When calibration has been made, the various functions (e.g. zoom or focus) can be connected to the joystick buttons. To define individual functions, always click first on the desired button and then on the corresponding joystick switch to be used.

Repeat this process until all elements have been connected.

3.8.5 Miscellaneous

In this section, various settings can be made which relate to one partition of the entire system.

The line underscored in yellow shows the system partition for which the settings displayed below apply.

For example, a partition defines the possible configuration when using touch-screen monitors. The zoom function or access to the context menu (right mouse-click) can be switched off here.

To change a setting, click on the value to be changed in the “Value/Status” column and select the new value from the displayed selection box.

Save your settings, then click on *Apply* so that the software is restarted with the new settings.

3.8.6 Activating and deactivating voice output

Version 6.0 and higher of ABUS VMS features voice output. When playing voice output, there is a distinction between user and system sounds.

The user sounds are played, for example, when the software is started or the system administration is opened or closed.

The system sounds indicate malfunctions such as camera or hard drive failures.

To completely switch off the voice output, deactivate *User voice output* and *System voice output* under *Various (Miscellaneous menu view)* in the system configuration.

3.9 Importing / exporting the system configuration

The ABUS VMS software is equipped with an import / export function, which can be used to restore the system quickly in the event of errors. The current settings can then be saved or restored quickly in this way.

To export the settings, open the system configuration and select the *Im-/Export* button on the top edge of the screen.

The *Import...* and *Export...* buttons are used to load or save the current configuration.

The *Load and edit...* button is used to load an existing setting to the view and change it as required. The current active configuration is not overwritten during the load process.

When a configuration file is loaded and changed, then it must be saved in the import/export dialog *(Save and Close)*.

Note:

If motion masks (permanent or privacy masks) have been set up, these are also backed up during the export.

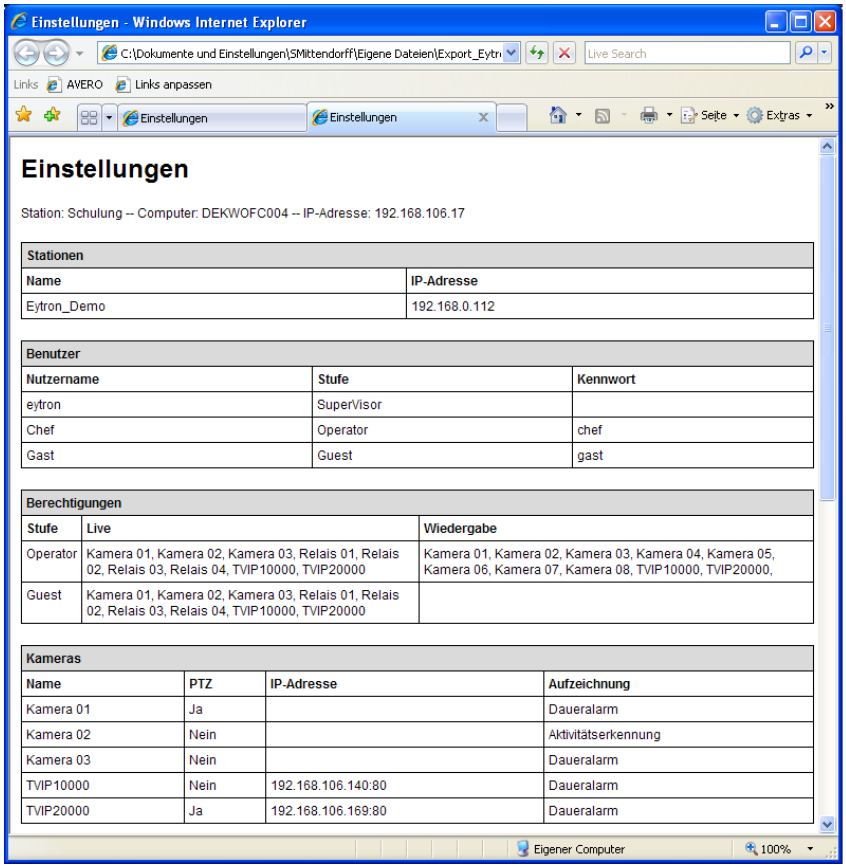
You can click *Load and edit…* to load configurations that have already been saved and edit them as required. During the loading process, the configuration that is currently active is **not** overwritten.

If a configuration file was loaded and edited, you must save it again using the import/export dialog *(Save and close).*

From version 6.6 onward, the software offers the option of exporting all settings as an HTML file. These are then written to an HTML file in the form of a table, which you can then open in an internet browser and print out for archiving.

Note, however, that only users with Supervisor authorization can create these, because the system prevents users with the standard authorization levels *Operator* and *Guest* from accessing the system administration.

The following illustration shows a finished HTML export of all system settings.



3.10 POS operation (point of sale)

Using the POS function, cash register systems can be connected to the ABUS VMS system via the RS-232 interface. The following sections describe how to set up and use the POS function.

3.10.1 Setting up a camera for POS operation

The following steps are required for setting up POS support.

1. Connecting the cash register system via RS-232 to the VMS system
2. Setting up the POS function in the system configuration
3. Activating the detector for data recording
4. Setting up a camera for POS operation

1. Connecting the cash register system to the VMS system

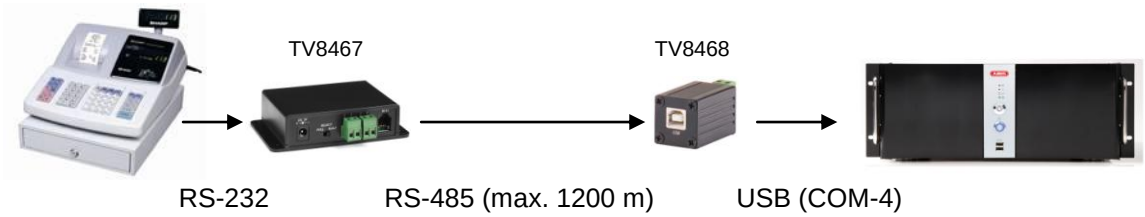
To connect a cash register system to the VMS system, you normally need a crossed RS-232 interface cable (null modem cable). However, with some manufacturers, instead of a null modem cable you need a 1:1 interface cable (RS-232 extension). For more information, see the installation instructions for your cash register system.

When using an interface cable, make sure it is not more than 15 m long.

For longer distances, use an interface converter (RS-232 ←→ RS-485 or USB ←→ RS-485).

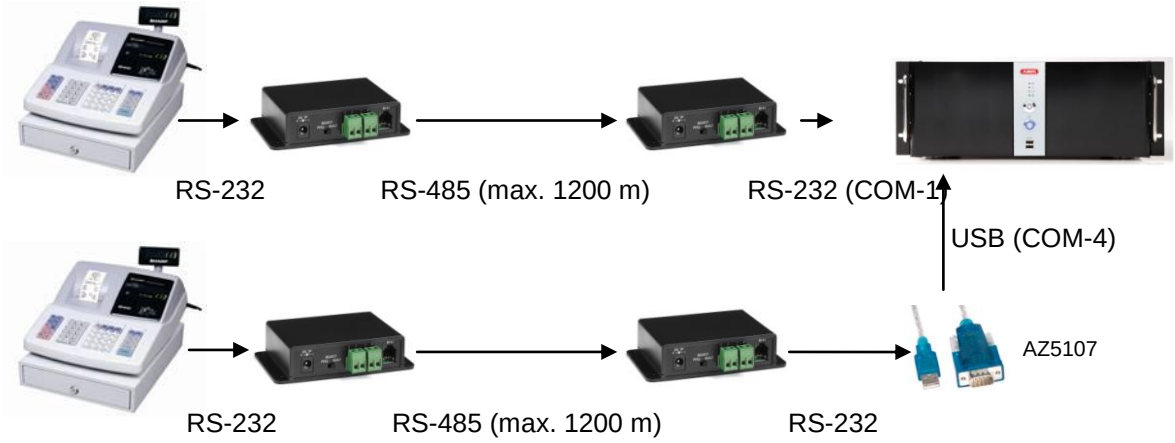
The following illustrations show the various connection options:

Example 1: Connecting a cash register system over a long distance



Instead of the USB → RS-485 converter (TV8468), you can also use the TV8467 adapter box together with the USB → RS-232 adapter cable (AZ5107). See the illustration below.

Example 2: Connecting two cash register systems over a long distance



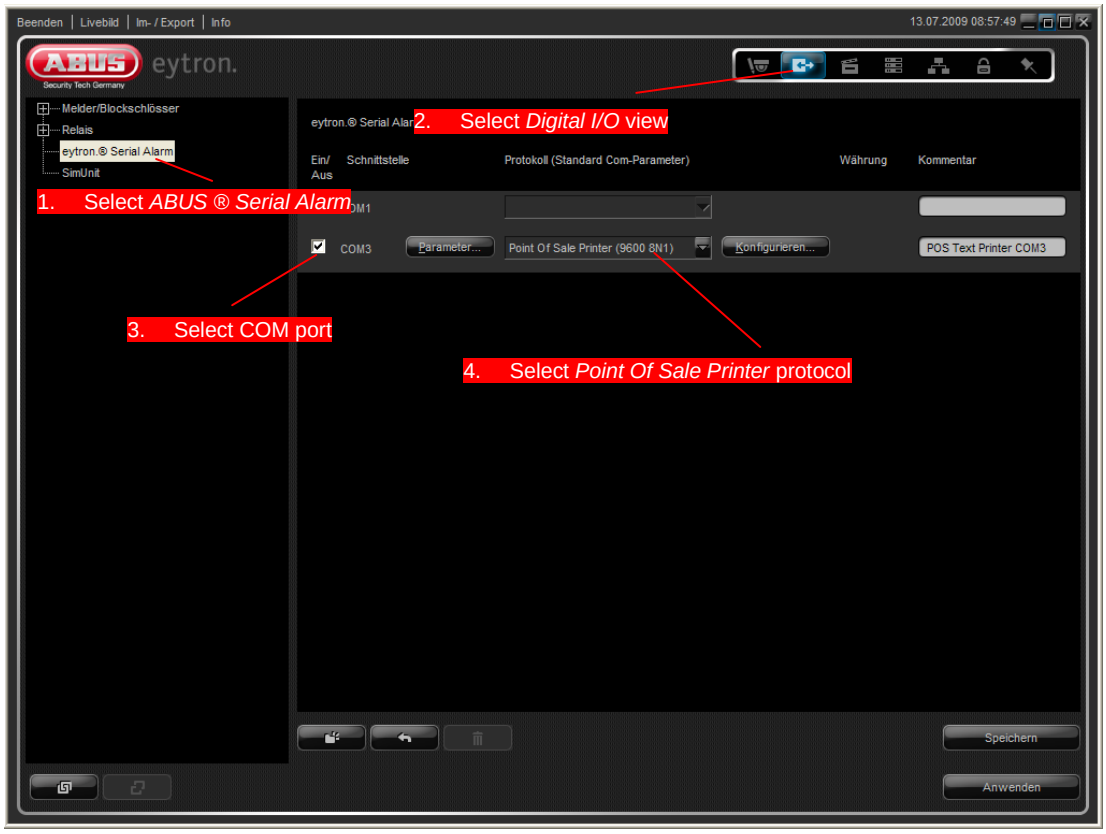
Note:

If you want to connect more than one cash register to the VMS system, you must use appropriate adapters (USB → RS-232 and RS-232 → RS-485 or USB → RS-485). Each cash register system requires its own COM port.

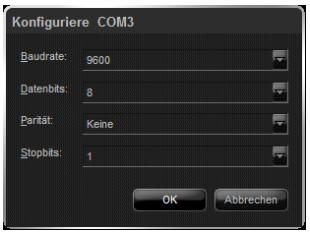
2. Setting up the POS function in the system configuration

Carry out the following steps to set up the POS functions:

- Open the system configuration and log in with your user details.
- Move the view selector to *Digital I/O (item 2).*
- Select ABUS ® *Serial Alarm* from the list on the left.
- Select the checkbox next to the COM port which the cash register system is connected to (for example COM3).
- Select *Point Of Sale Printer* as the protocol to be used.



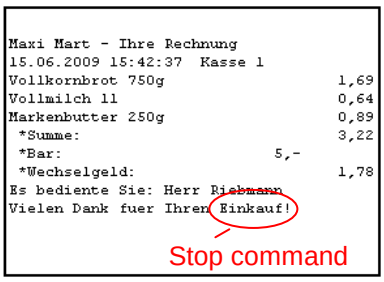
- Click the Parameters button and check the settings. The baud rate setting here must match the setting on the cash register system. For more information on configuring the baud rate on the cash register system, see the installation instructions from the manufacturer.



- Create a receipt on the cash register system and define a unique stop command. This code causes the system to stop recording data for the current cash register transaction and wait for the next one. The illustration below shows an example receipt.

  The word *Purchase!* is used here as the stop command. This is sensible, because it only appears once on each receipt. If it is not possible to use a text as the stop command, then another unambiguous command must be added to the receipt.

  You can find more information on editing receipts in the installation instructions for the cash register system.



- Click *Configure* in the system configuration and enter the code for the end of the transaction. Then click *OK*.

- Save the settings.

3. Activating the detector for data recording

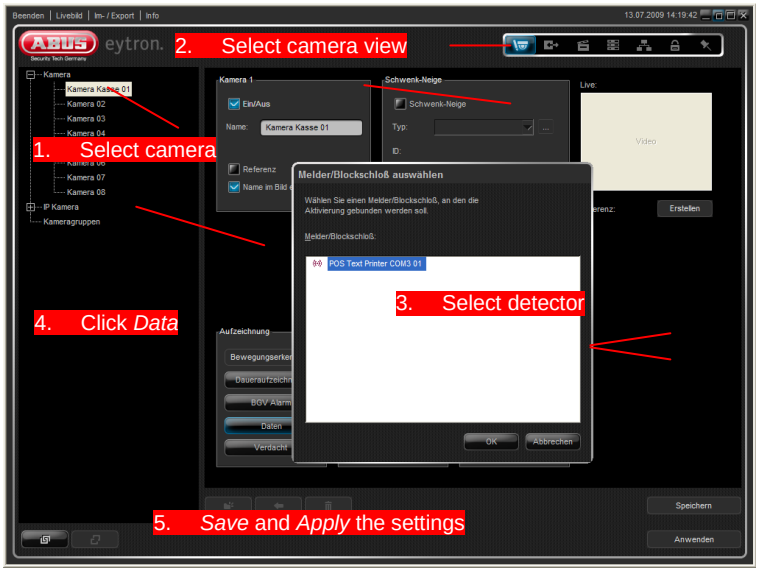
In order for data to be recorded, a detector is required, via which the recording is started. This is how to set up the detector:

- Leave the view selector on *Digital I/O* and select *Detectors / block locks* in the list on the left.
- In the subgroup, select the detectors for the *POS Text Printer* (e.g. *POS text printer COM3*)
- Activate the detector until it displays the alarm symbol .
- Save the settings.

4. Setting up a camera for POS operation

Finally, you must select the camera to use for data recording.

- To do this, move the system configuration view selector to *Camera view (item 1)* and select the camera (e.g. Cash register camera 2) on the left.
- Click *Data*. The window where you can select the detectors then appears. Select the detector you activated in step 3 (e.g. *POS Text Printer COM3 01*).
- Save the settings and click *Apply*. The system then automatically creates all the other necessary components and the POS setup is completed. You can then close the system configuration.



3.10.2 Using the POS function and performing a database search

The following sections describe how to use the POS function and search in the recorded data.

Using the POS function

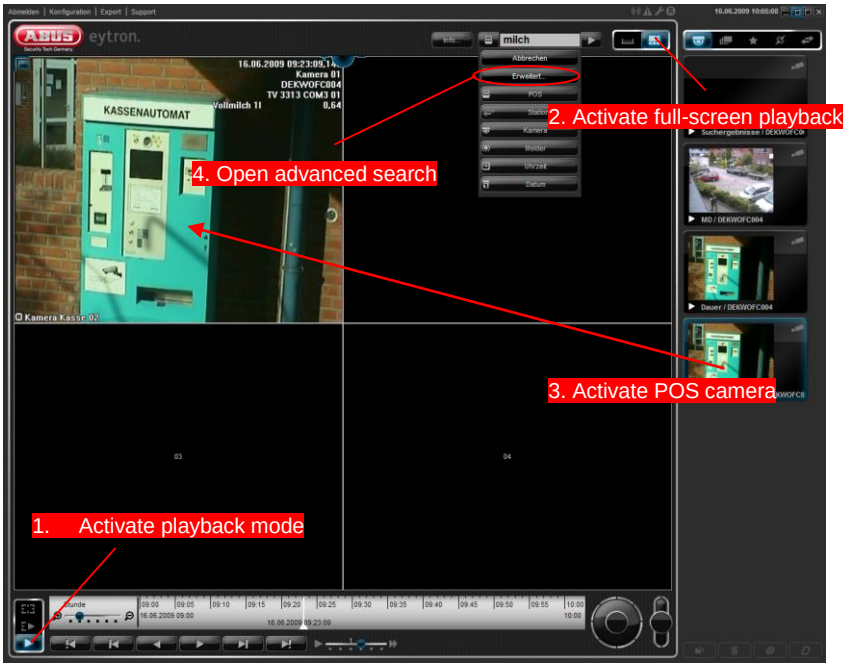
Switch the client to live mode and activate the camera that is set up for the POS function. If a transaction is now started, the cash register information is shown successively in the live image. If the transaction is finished and the end command (in this case: Purchase!) is detected, the detector data is no longer recorded and the data is no longer shown in the live image.

The system then waits for the next transaction

Performing a POS search

If you want to look for particular information, the advanced search function is a very easy way to do this.

Switch to playback mode and activate full-screen playback.



Next activate the archive where the POS data was recorded (e.g. Camera Cash Register 2).

Click the clock icon in the search bar and select *Advanced search*.

Alternatively, you can open the advanced search dialog with the shortcut *Ctrl* + *F*. Note, however, that this only works in playback mode and not in live mode.

Note:

The advanced search dialog allows you to restrict your search using appropriate criteria. These might be the start and end data, or the POS archive of the local system or a system connected via network.

If you want to search for multiple articles, you only need to enter part of the article as the search term. For example if you enter bread as the search term, the search will return results for wholemeal bread and white bread.

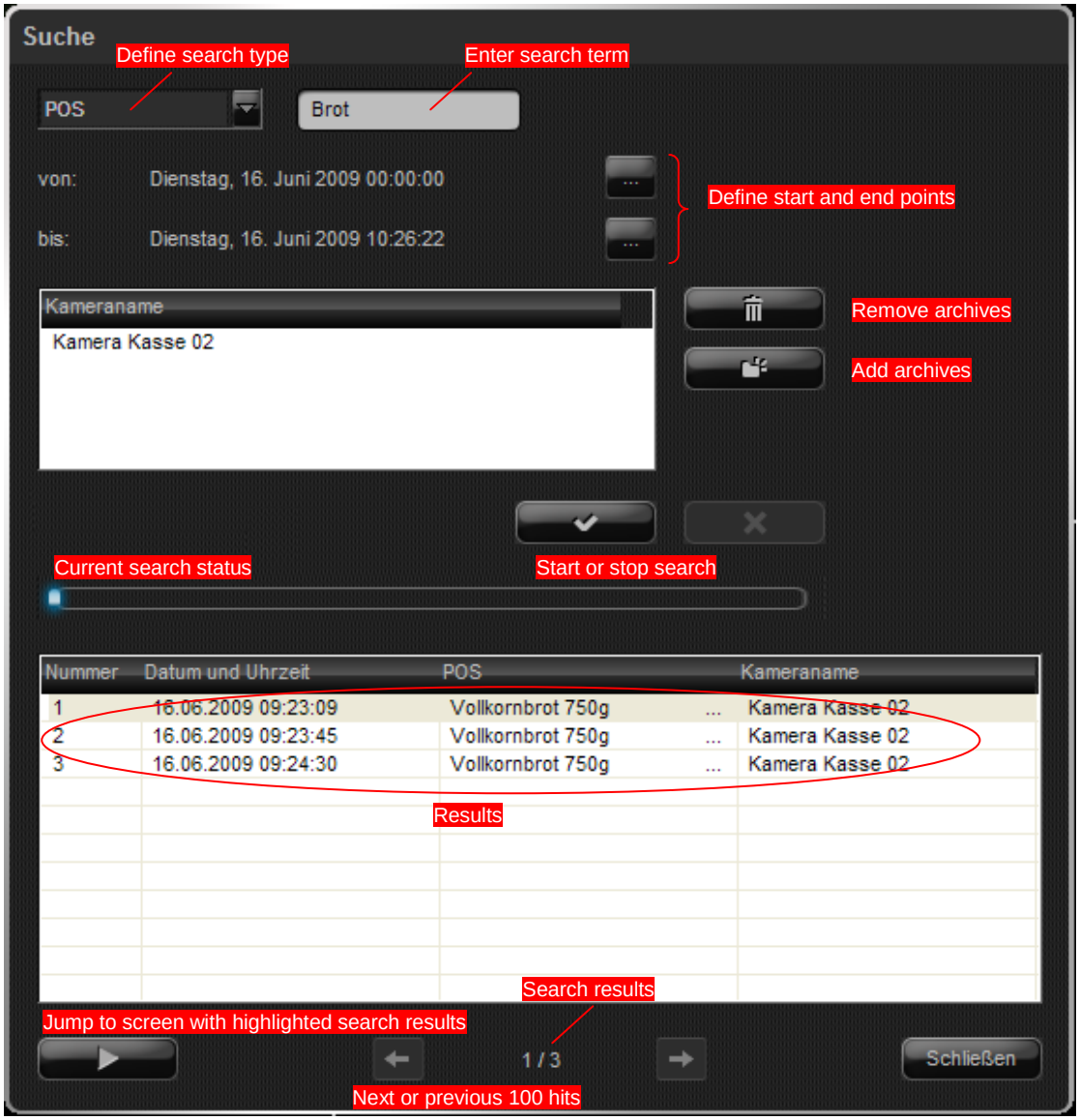
First define the type of search. If the system is solely set up for POS, only the POS option appears here.

Next enter the search term (e.g. “bread”).

Next enter the period (start and end) for the search. To do this, click the buttons and select the period.

The camera name field contains all the archives to be included in the search. By default, it lists all the archives that were activated before the dialog was opened.

You can use the and buttons to remove archives or add archives to the search.



Start the search by clicking *Start search*. ( )

While the search is in progress, the current status is displayed and the articles found so far are listed in the results window. If more than 100 hits are shown, you can scroll to the next or previous 100 hits using the and buttons.

If you want to open the recorded video for the article found, all you need to do is select the entry and click the button. The playback behind the window skips to the corresponding point in the database and can then be resumed from that point.

3.11 “UVV Kassen” operation

The following points show the system requirements and set-up of the ABUS VMS system for “UVVV-Kassen” operation.

Important!

An additional alarm card is required to fulfil the system requirements for “UVV-Kassen”. This is available separately (included in ABUS HDVR).

When selecting the camera, also pay attention to the “UVV-Kassen” certification.

3.11.1 General information

The “UVV-Kassen” (English: accident prevention regulation caches) contains guidelines on using digital recording systems for monitoring cash check-outs.

The following information details the set-up of the ABUS VMS software according to the “UVV-Kassen” guidelines.

3.11.2 Guidelines

The following guidelines must be met for “UVV-Kassen” operation:

- The cameras must be installed so that the area where a robbery may take place is monitored and usable pictures of the perpetrator can be taken (from the front or side). For more information, see “Installation Instructions for Optical Room Surveillance Equipment (ORÜA)”, SP9. 7/5.
- Cameras (especially those in the cash desk area) must not be hidden. System maintenance work that can interfere with recording must be carried out only when sales operation is inactive (i.e. outside normal business hours or immediately following a robbery).
- The camera images, time and date must be checked on a monthly basis.
- Ensure that the recording system is reset to shell mode after maintenance work. The ABUS VMS system **must** be set to the safe (shell) mode in “UVV-Kassen” operation so that direct access to the operating system is not possible.

3.11.3 Setting up “UVV-Kassen” operation

The following components are required for the system set-up:

1. Cameras (foyer and cash desk area)
2. “Alarm”, “Pre-ring” and “Ring” archives
3. Alarm and suspect detectors
4. Permission level without delete authorisation
5. User account
6. Text message used in the event of an alarm
7. Storage process (suspect, activity, alarm, pre-alarm)
8. Host(s) where the notification is to be sent
9. Dialling process for alarms
10. Connection of the processes
11. Shell mode

The following steps show an example of a “UVV-Kassen” set-up with one camera in the foyer and one in the cash desk area. The individual steps should be modified as needed if further cameras are to be installed.

1. Switching on the camera

Move the view switch to *Camera view (point 1)* and open the *Camera* item in the list on the left.

Select the number of the camera you want to use for “UVV Kassen” operation and activate it by enabling the *On/Off* field.

If you want to use IP cameras, activate them as described in section 3.2.3.

Give the camera a unique name (e.g. *POS 1*) and save the settings.

Automatic configuration:

To activate “UVV Kassen” operation for the selected camera, click the *BGV Alarm* button. You are then prompted to select a detector. Select the Alarm detector (detector from step 1). All other settings are then made automatically. Save the settings.

With HD-SDI or megapixel cameras, make sure that the archive is set large enough to save 15 minutes’ worth of data.

If you want to set the option for recording on suspicion, click the *Suspect* button in the Recording field and select the *Suspect* detector as the detector to use. Then save the settings.

Note:

The recommended setting for ""VV Kassen" operation is 25 frames per second, H.264 with 4 MBit and a resolution of 4CIF, or D1 or VGA. The automatic configuration makes these settings for data storage. For network cameras, you should enable the "Set video parameters for network cameras" option under Miscellaneous. This ensures that the video stream is correctly recorded.

To prevent any malfunctions that may arise, the cameras defined for "UVV Kassen" operation may not be used for other recording purposes (motion detection or continuous recording).

2. Creating the archives

Switch the view switch to the *Database / Storage* view (point 4). Select *Archives* from the list on the left.

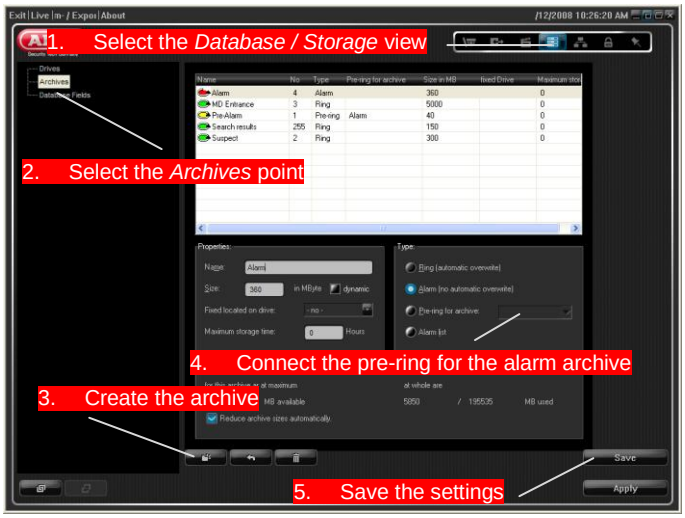
Press *New*, then create one new archive for each of the following types:

Name: POS 1 Suspect **Archive type:** Ring **Size:** min. 450 MB

Name: POS 1 Alarm **Archive type:** Alarm **Size:** min. 2700 MB

Name: POS 1 Pre-ring **Archive type:** Pre-ring **Size:** min. 450 MB **Length**:15 min

Assign the alarm archive to the pre-ring archive using the *Pre-ring for archive:* selection box and save your settings.



To use larger archives in "BGV-Kassen" mode, ensure that the pre-ring archive fits into the alarm archive at least three times and the created alarm images can be saved.

The reason for this is that the alarm archive can be filled to 60% or 100% and the *Alarm archive is filled up to 60%* and *Alarm archive filled 100%* virtual alarm detectors trigger when these levels are met.

Note:

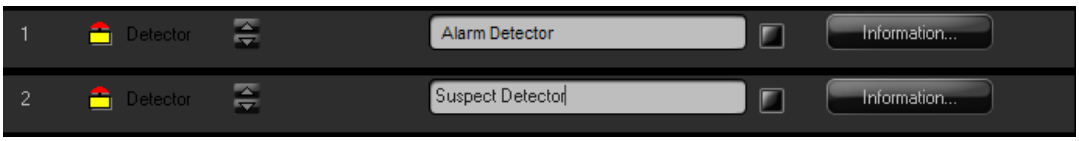
The archive sizes of 450 MB and 2700 MB are suitable for a 4 MBit video stream. To save higher bandwidths, especially HD cameras, the archive sizes must be modified accordingly. From version 7.3.xxxx onwards, you can set the length of the pre-ring archive in hours and minutes on the archive configuration page.

3. Switching the detectors

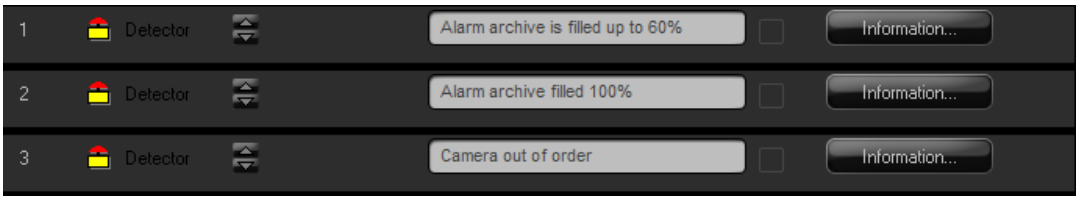
The following detectors are required for “BGV-Kassen” operation:

1. External *Suspect* detector
2. External *Alarm (robbery)* detector
3. *Archive filled up to 60%/100%* virtual alarm detectors
4. *Camera out of order* virtual alarm detector
5. Detector for activity detection

To set up the detectors, switch the view switch in the system configuration to the *Digital I/O* view (point 2) and open the *Detector/Key switch* → *TV33xx detectors* point. Activate two external detectors on the alarm card (e.g. TV3311) and designate them as “Alarm” or “Suspect” (see diagram).



Switch to the *Virtual alarm detectors* point and activate the *Alarm archive is filled up to 60%* (detector 1), *Alarm archive filled 100%* (detector 2) and *Camera out of order* (detector 3) detectors. Save the settings.



Finally, switch on the detector for activity detection. To do this, select *Detector/Key switch* → *TV33xx MD detector* and activate the detector on the corresponding camera (the camera number corresponds to the detector number).

Designate this detector as “Foyer Camera MD”, for example.

Save your settings.

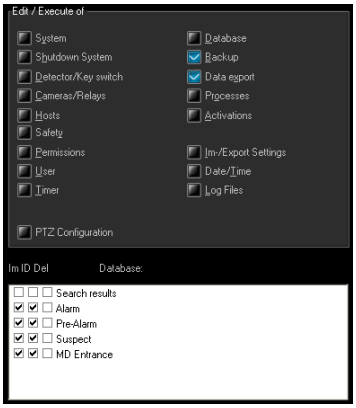
4. Creating the permission levels

Switch the view switch in the system configuration to the *Security* view (point 6) and select *Permissions* from the list on the left.

Create a new permission level and give it a name (e.g. User).

Assign the access authorisation for backups and exports, image viewing and data from the database to the permission level (see diagram).

Save your settings.



5. Creating the user

Select *User*, then create a new user using the *New* button.

Give the user a unique name, then assign the permission level as described in step 4.

Save your settings.

6. Creating text messages

Switch the view switch in the system configuration to the *Actions* view (point 3) and select the *Notifications* point. Create three text messages here with the following text:

- **Name:** *Alarm archive filled 100%*; **Text:** *The alarm archive is 100% full*.
- **Name*:*** *Alarm archive is filled up to 60%*; **Text:** *The alarm archive is 60% full.*
- **Name:** *Camera out of order*; **Text:** *Camera out of order on digital recorder xy.*

Save your settings.

7. Creating the storage process

Switch the view switch in the system configuration to the *Database / Storage* view (point 4) and open the *Storage processes* point. Using the corresponding buttons, create a process for “Activity detection”, “BGV pre-alarm”, “BGV alarm” and “Suspect”.

The images are now saved at a rate of 25 frames per second, a resolution of 4CIF and a compression of 4 Mbit.

Save the settings.

Name	Nr of images	Resolution	Compression	State	Runtime	Pause time	Pre time
BGV OK	1	4CIF	1 (low)	As long as detector unchanged	0	0	0
BGV Alarm	2	4CIF	1 (low)	Hold entire duration/no. of images:	900	0	0
Motion Detection	1	4CIF	1 (low)	Hold entire duration/no. of images:	2	0	2
Suspect	1	4CIF	1 (low)	Hold entire duration/no. of images:	10	1	10

The values set in the data saving processes are only valid as default for analogue cameras. If you also want this to apply to IP cameras, go to the configuration, select *Miscellaneous→Various* and enable the *Set video parameters for IP cameras* item. Otherwise the settings for the IP camera made via the web interface apply.

8. Creating the hosts

Switch the view switch to the *Network* view (point 5) and select *Hosts* from the list on the left.

Create a new host using the *New* button and give it a unique name. This makes it easier to find the host afterwards.

Enter the number / IP address of the system where the notification is sent in the event of an alarm and select the desired transmission path (ISDN, TCP/IP) in the *Type* field.

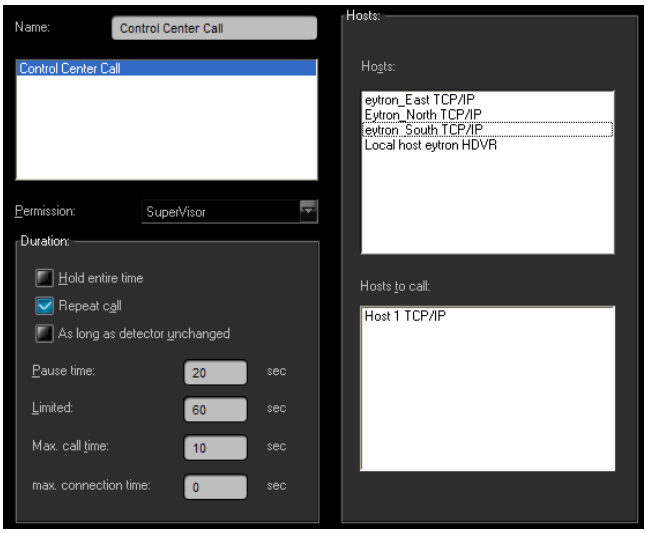
Save your settings.

9. Setting up the calling process (alarm dialling)

Switch the view switch to the *Actions* view (point 3) and select the *Calling processes* point.

Using the *New* button, create a new process according to the figure on the right and select the desired host from the host list by double clicking it.

Save the settings.



10. Setting the activation

All components must be connected to one another before they can be started.

To do this, select the *Activations* point in the Actions view and create the new activations using the *New* button with the following data:

Detector: Alarm; **Status:** OK; **Timer:** Always; **Camera:** Desk1; **Process:** BGV OK; **Priority:** 3; **Archive:** Pre-ring

Detector: Alarm; **Status:** Alarm; **Timer:** Always; **Camera:** Desk1; **Process:** BGV Alarm; **Priority:** 1; **Archive:** Alarm

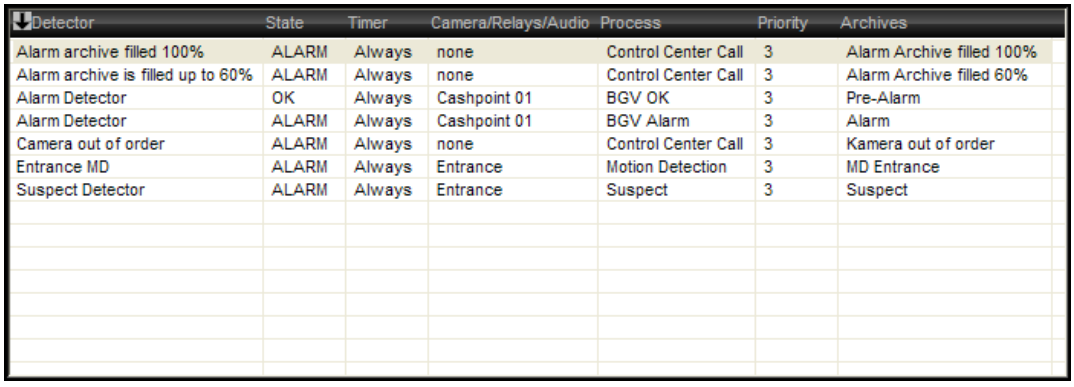
Detector: Camera out of order; **Status:** Alarm; **Timer:** Always; **Camera:** None; **Process:** Notification; **Priority:** 1; **Archive:** Camera out of order (notification text)

Detector: MD foyer; **Status:** Alarm; **Timer:** Always; **Camera:** Foyer; **Process:** Activity detection; **Priority:** 3; **Archive:** Foyer Camera MD

Detector: Suspect; **Status:** Alarm; **Timer:** Always; **Camera:** Desk1; **Process:** Suspect; **Priority:** 3; **Archive:** Suspect

Detector: Alarm archive is filled up to 60%; **Status:** Alarm; **Timer:** Always; **Camera:** None; **Process:** Notification; **Priority:** 3; **Archive:** Alarm archive is filled up to 60% (notification text)

Detector: Alarm archive is filled up to 100%; **Status:** Alarm; **Timer:** Always; **Camera:** None; **Process:** Notification; **Priority:** 3; **Archive:** Alarm archive is filled up to 100% (notification text)



Detector	State	Timer	Camera/Relays/Audio	Process	Priority	Archives
Alarm archive filled 100%	ALARM	Always	none	Control Center Call	3	Alarm Archive filled 100%
Alarm archive is filled up to 60%	ALARM	Always	none	Control Center Call	3	Alarm Archive filled 60%
Alarm Detector	OK	Always	Cashpoint 01	BGV OK	3	Pre-Alarm
Alarm Detector	ALARM	Always	Cashpoint 01	BGV Alarm	3	Alarm
Camera out of order	ALARM	Always	none	Control Center Call	3	Kamera out of order
Entrance MD	ALARM	Always	Entrance	Motion Detection	3	MD Entrance
Suspect Detector	ALARM	Always	Entrance	Suspect	3	Suspect

Save the settings and then click on the *Apply* button.

Your system is now configured for “BGV-Kassen” operation.

11. Activating the shell mode (safe mode)

Log out all users before activating the shell mode. To do this, click on the *Logout* button on the top-left edge of the screen.

Click on the *Switch off* button, then select *Safe (Shell) Mode* in the dialog which appears.

After entering the user name and password, the operating system is restarted in shell mode and access to the operating system is prevented.

Note:

“BGV-Kassen” mode is not available on the ABUS VMS Basic.

3.11.4 Measures to continue recording after power failures

To ensure that your system functions properly in the event of power failures or fluctuations, it is advisable to make and activate the following settings in the system.

1. System start-up after a power failure

Modern-day mainboards can restore the operating status after the power supply is returned. The default setting in the BIUOS is that the system remains switched off after a power failure.

In this case it is advisable to change the operating status so that the system always starts immediately the power is restored. Otherwise it is not possible to resume recording.

For more information see the mainboard manual.

2. Compensating for loss of power

If you operate your digital recorder in networks where the power often fluctuates it is advisable to use an uninterruptible power supply (UPS). This can bridge brief power interruptions.

3. Automatic login to the operating system

The VMS software runs in a Windows environment as an independent program and not as a Windows service. This means that video data can only be recorded when a user is logged into the operating system.

To make the login to the operating system automatic, activate the *Windows login* function. (See section 3.6.5 on page 118)

4. Starting the VMS automatically

To start the VMS software automatically after logging into windows, it is advisable to link it to the Autorun folder.

To do this, click Start → All Programs in your operating system and then double-click the Autorun folder. A new window appears where you can copy the *ABUS VMS* (desktop) link. The software then runs automatically when you start Windows.

Note:

If the system is running in shell mode, you do ***not*** *need to carry out this step. The software starts automatically in shell mode.*

4. ABUS® VMS web application

The ABUS VMS web application expands the ABUS VMS main software by allowing access over a web browser.

Connection to the system can then be made over the Internet or local network (LAN, Intranet). No extra installation is required on the client PC for access over a web browser.

Web access is not platform-specific. This means that the web application can be used on all common operating systems (Windows, Linux, Unix, Mac-OS).

An overview of the supported web browsers can be found under point 4.2.

4.1 System requirements

The following minimum system requirements apply for using the ABUS VMS web application:

Recorder system:

Administrator rights for installation
Windows Vista or higher

Client system:

Up-to-date web browser (IE8, Safari, Firefox, Opera etc.)
Minimum screen resolution of 1024x768 pixels

Note:

Due to currently valid licensing agreements, Internet Information Services (IIS) are not included in Windows XP Home Edition and Windows Vista Home Basic. Update your operating system to Professional (XP) or Home Premium (Vista), or use an alternative web server with ASP.Net and AJAX support.

4.2 Supported web browsers

The web application can be used in all modern, ASP.Net and AJAX-enabled web browsers. The table below shows an overview of successfully tested browsers.

Browser	Manufacturer
Firefox®	Mozilla®
Internet Explorer®	Microsoft®
Safari®	Apple®
Chrome®	Google®

4.3 Installing the web application

The web application can be installed according to the enclosed Quick Start guide. Always install the software on the system where the main software is installed (ABUS VMS Basic, Professional or Enterprise).

Insert the installation CD into the drive and wait until the start menu is loaded. Click on the *Install ABUS VMS web application* menu point and follow the instructions in the set-up wizard.

In order for the application to function properly, you need at least the ABUS VMS Basic software with a suitable video card (TVVR95000-TVVR95020) or ABUS HDVR.

For access to the web interface, you must first activate the web interface in the main software as described in section 3.4.8.

Note:

*The web application can **not** be used in combination with the ABUS VMS Express software.*

4.4 Accessing the web application

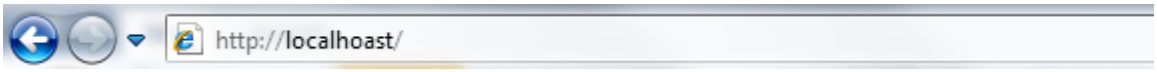
After the web application has been installed successfully, the main software can be started and the system can be accessed. Proceed as detailed in the following points.

Pay attention to the following table for later use. This gives an overview of the maximum permissible number of connections to a system.

	VMS Basic	VMS Professional	VMS Enterprise	ABUS HDVR/NVR
Maximum number of parallel connections over the web browser	1	3	3	3

Testing the local connection:

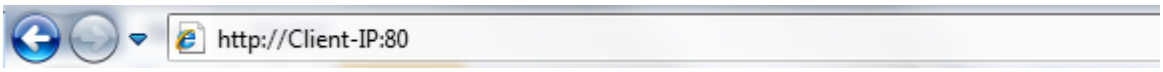
Open the web browser on the local station and enter the following URL:



The log-in window of the ABUS VMS web application should now appear when access to the system was successful.

Testing the remote connection:

Open the web browser on another PC in the network and enter the following URL:



The client IP should be replaced by the IP address or the name of the PC where the web application is installed (e.g. http://192.168.0.100:80).

The log-in window of the ABUS VMS web application should also now appear when the system connection was successful.

4.4.1 Log-in

The web application log-in is similar to the VM software log-in. You can select the system language before logging in and then use your existing user data to log in.

As server queries in the web application take longer than in the main software, the user can follow the progress of the query in the circular figure which appears (see illustration).

This is no longer seen when the query has been processed completely.

Note:

*In no other users were created in the VMS, use the default user **admin** and the password **12345** for the login.*

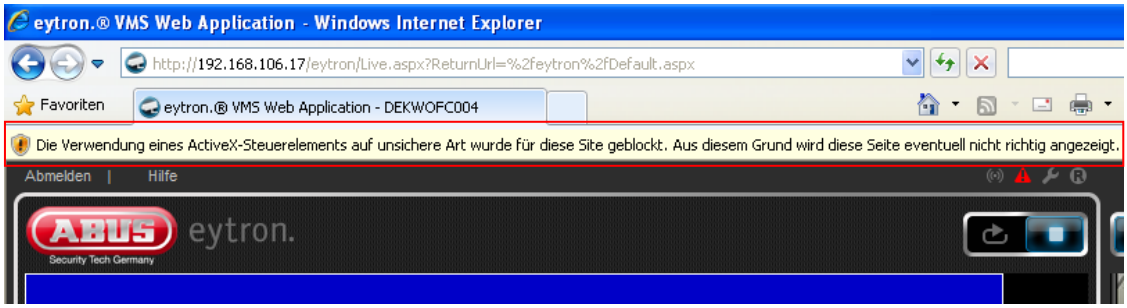
4.4.2 Using the ActiveX plug-in

The first time you access the web application you are asked to install ActiveX

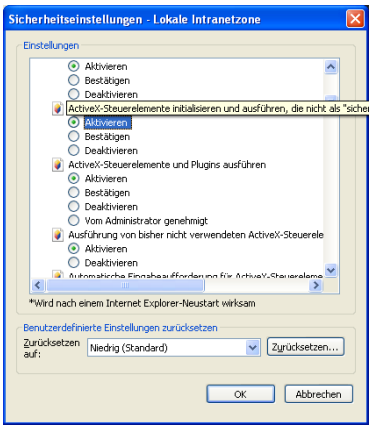
Click *Install* to start the installation of the plug-in.

Once the plug-in has been successfully installed, the camera is displayed by ActiveX.

In some cases, Internet Explorer (IE8) may block the installation of the plug-in.



If this happens, you must change the security settings in the internet options*(Tools → Internet options)*.



Select the *Security* tab and click *Change level*.

In list in the next dialog, change the setting for *"Initialize and execute ActiveX controls that are not marked "safe for scripting"* from *Disabled* to *Enabled*. Then click *OK* to close the window.

After that, close the browser and start it again. You can now use the plug-in.

Note:

If you use Firefox, Chrome or Safari, you must install ActiveX manually. To do this, download the appropriate plug-in installer from www.abus-sc.com and follow the instructions of the installation wizard.

4.5 Working on the user interface

The ABUS VMS web interface is based on the interface of the main software. The recommended minimum screen resolution for a correct display is 1024x768 pixels. If necessary, switch your web browser to full screen mode. The F11 key is used for this purpose in most web browsers.

All changes compared to the ABUS VMS are listed below.

Joystick: The joysticks are simulated by buttons in the web application, and cannot be actively pressed and moved as in the desktop application. The joystick is operated by clicking directly on the corresponding button.

Example: Camera tilt upwards and to the right

Slider: The slider is also simulated by buttons in the web application, and cannot be actively moved as in the desktop application.

Example: Show “Camera” view

System mode: The system mode selection in the web application is restricted to “Live” and “Playback” modes. “LivePlus” mode is not available here.

Live mode

Playback mode

Slide selection: The slide selection options are restricted to *Cameras* and *Favorites*.

Cameras: All available cameras are shown in the slide list. Click on the desired camera slide to incorporate it into the live window (activation).

***Note**:*

If there is no space for more cameras in the current view, then you must first select a view with more free places in order to display the cameras.

Picture geometry You can switch the picture geometry in the same way as in the main software. The maximum number of cameras that can be displayed is limited to four.

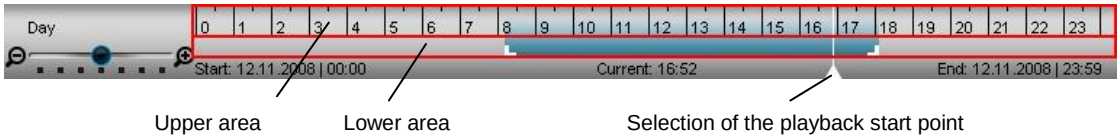
Configuration The system can be configured using the web application. Any changes to the system settings should be made in the main software.

Note:

Only use the software buttons to control the web application. Do not use the Next / Back buttons in the browser, because this may lead to unexpected results.

Using the time stream:

The time stream is divided into two sections, which are used to define the start time and select the backup time.

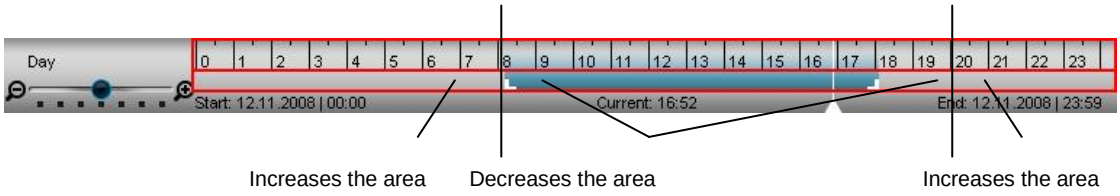


To define the playback start point, click the upper area. This enables the selection tool to move to the corresponding position.

Playback can then be started using the corresponding buttons.

To define the backup period, left-click in the lower area next to the backup selection tool. When the mouse pointer is clicked above the selected area, then the backup period is increased.

When the mouse pointer is clicked below the selected area, then the backup period is decreased.



When the corresponding area has been selected, then the data backup can be started by pressing *Export*. A video file (*.avi) is created on the recorder system and can be used after the download is complete.

Export

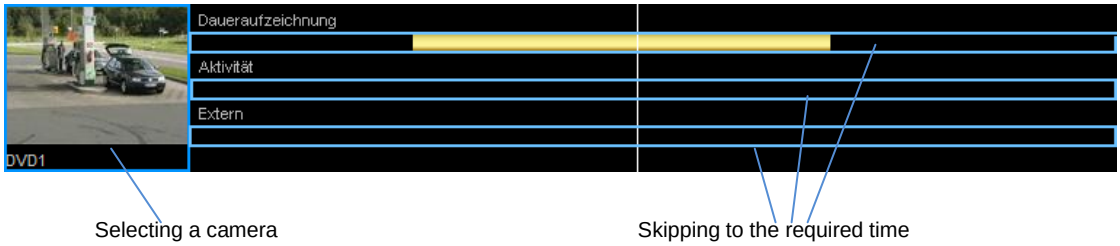
The web application allows you to export individual images and video.

Click this icon to export a single image.

Click this icon to start a video export.

Using the graphical overview of recordings

The overview is divided into several sections for each camera. Depending on the recording type, a distinction is made between permanent recording, recording via activity detection and recording via external detector.



To select an activated camera, activate the archive in the same way as the live view.

If you want to change the start time for playback, you can do this by clicking the recording bar directly. You can also select the data using the calendar function.

Playback starts from that time.

Note:

The number of playback slots in the web application is limited to four.

5. Installing software updates

We recommend installing the latest software updates, as this ensures that you always receive the latest add-ons and software improvements. The files required for software updates can be downloaded from http://www.abus-sc.com.

Software updates can also be started manually from a CD or removable media when the Internet is not available on the system.

The following steps illustrate the installation process for software updates:

- Exit the ABUS VMS software (see point 1.3.4).
- Insert the medium containing the software update.
- Using Windows Explorer, find the file path of the update.
- Start the installation by double-clicking on the *ABUS VMS-Setup.exe* or *ABUS-VMS-Webinterface.exe* file, then follow the instructions in the installation wizard.
- Restart the system after the update has been completed.
- Start the ABUS VMS software.

The software has now been updated.

Note:

Software updates are cumulative, meaning each update contains all previous versions. If some updates have not been installed previously, then you only need to use the last update. Your settings are applied in this way.

Updates can always be installed directly, meaning you do not need to uninstall the software before the update is made.

6. Uninstalling the software

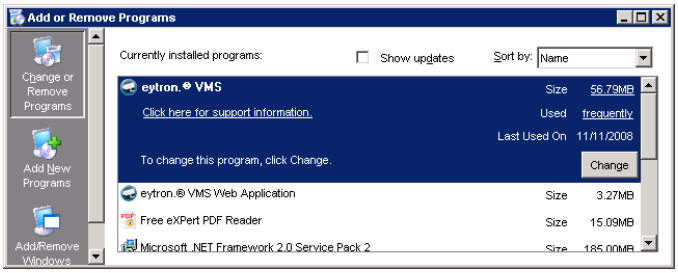
The software can be uninstalled in the Control Panel of the operating system.

Exit the ABUS VMS software and open the Control Panel. Select *Uninstall or change programs* (Windows 7).

Wait until the list of installed programs is updated.

Uninstalling ABUS VMS:

Select the ABUS VMS software from the list of installed programs.

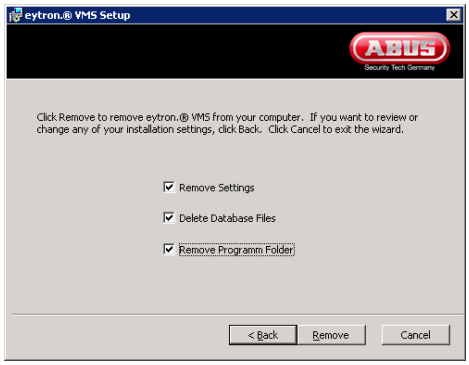


Click on the *Change* button. The installation wizard appears.

Now click on the *Remove* button.

To remove all the software, check all the boxes.

Click on *Remove*, then follow the instructions.



Uninstalling the ABUS VMS web application:

Find the *ABUS VMS web application* in the list of installed programs. Select this program, then click on the *Remove* button and follow the instructions on the screen.

7. FAQs

The following information can be used to clarify the most frequently asked questions regarding the system software.

Consult our Customer Service team if you have a question which is not listed here.

1. What is the "Double Login" procedure and how do I set it up?

The "Double Login" principle requires a second user to log in to the system.

When the user logs in to the system and "Double Login" is activated, then the log-in dialog appears again with the prompt for a second user log-in. Only then can the system be accessed. Any user from the account list can be used for the second log-in. More information on setting up the "Double Login" function can be found under point 3.6.2 on page 115.

2. What is the standard user name and password?

The standard user is **admin** and the password is **12345**. For security reasons, this user should be deleted or replaced after the system has been set up.

3. I have installed the software successfully. What do I have to do now?

After the software is started for the first time, the system is configured for recording using the set-up wizard. We recommend selecting automatic configuration here as the system is then set up without the need for any user input.

For information on making manual changes or configuring the system using the wizard, please see point 3 on page 49.

4. I have forgotten my password. What should I do now?

In this case, please contact Customer Support.

5. Which media can be used for creating a backup?

Data backups can be made on all standard media, including:

CD-R/RW, DVD-R/RW+DL, DVD+R/RW+DL, USB sticks and memory cards.

Note:

In order to make a backup on CD/DVD drives, USB sticks or removable media, these must be declared as "Backup read & write" in the system configuration. See point 3.3.1 on page 69 for more details.

6. Can the remote system settings be changed over the network/Internet? What do I have to do here?

The configuration of a remote recorder can be received, changed and sent back using the system configuration. The transmission method (LAN or ISDN) does not play a role in this case.

To receive data, open the system configuration and select the corresponding host using the *Connect* button. Using the *Disconnect* button, the configuration is sent back and the host is restarted with the changed settings.

For more details, see point 3.7.6 on page 127.

7. A user should only be allowed to access the system within a certain time. Which software options can be used in this case?

Permission levels (system administration) are used for this purpose. Permission levels always depend on a timer. Access can then be restricted in this way. The standard setting is "Always".

8. What is the shell mode?

The shell mode is used to start the system in "safe" mode. Access to the operating system is prevented here, meaning system manipulation is no longer possible.

The shell mode is used in "BGV-Kassen" operation.

9. Which IP cameras are supported?

Currently, IP cameras from ABUS Security-Center GmbH & Co. KG, Axis, Panasonic, Arecont Vision and Mobotix are supported.

However, the ABUS VMS Professional version is required for setting up these cameras. An overview of individual software packages can be found in the table under *Upgrades* at the start of this manual.

10. What is the purpose of the "Apply" button?

When changes are made to the system configuration, the server module must be restarted in order to apply the changes. The "Apply" button is used to restart the server.

11. How can I control a pan/tilt camera?

Pan/tilt cameras are controlled via RS-485 or RS-422. A special converter is needed to communicate with the camera. This can be connected to the RS-232 or the USB port.

12. Which PTZ protocols are supported by the system?

The ABUS VMS software supports the following PTZ protocols:

Baxall	Fastrax II (HID-2404)	Relais PTZ
BBV RS-422	Ganz PT	Sensormatic TT / Ultra
Bewator/Molynx	JVC TK-C676/655	Sony VISCA
CBC TOA	Meridian (Marc Mercer)	VCL Camera
CBC ZC-NAF27	Panasonic WV-RM 70	VCL MaxCom
Elbex EXC 80, 90, 1000	Pelco-D / -P	Videotec
Ernitec BDR 510	Pieper KMS 850S	Videv EC160

13. I am automatically logged out of the system after a certain time. How can I prevent this?

The "Auto Logout" function can be switched off in the system configuration. Switch the view switch to the *Security* view (point 6) and select *Auto Logout* from the list on the left. Uncheck the *Automatic User Logout* field and save your settings.

14. I have added a Video-Out process, but no signal appears on the connected monitor.

A process must always be connected to an activation – creating the process alone is not sufficient. Video-Out processes must be connected to the *Permanent alarm* virtual alarm detector. To do this, activate detector 20 in the system configuration under *Detector/Key switch* → *Virtual alarm detector* ("Digital I/O" view).

Access the activations and create a new activation with the permanent alarm and Video-Out process as described under point 3.4.9 ("Creating activations").

15. Whilst viewing database images I have received a red image with the title: "You are not authorised to view the image information". What should I do now?

This message means that a database access restriction has been added for the user.

The permitted time for viewing database images is set up in the system configuration using the permission levels (*"Security" view* → *Permissions*).

The time (in hours) must be set in the *Playback* field and the permission level must be assigned to a user. The function is deactivated when "0" is entered in the field.

Note:
The server settings always apply. The remote settings apply when a remote system is used for dialling, not the local settings.

16. When calling a host, the software always shows a system error that the connection was rejected or could not be established. What should I do now?

This may be because the network module (SocketUnit) is not switched on. Switch on the module in the system configuration *("Network" view* → *TCP/IP)*. More details on the SocketUnit can be found under point 3.7.1 on page 119.

17. The creation of reference images is not possible on all cameras. What do I have to do here?

In order to create reference images from a camera, this option must be activated for the desired camera. See point 3.2.7 on page 60 for more details.

18. I cannot play the video files from the AVI export on my media player. How can I resolve this?

Errors in the playback of video files are usually a result of a missing video codec. Install the DivX or XVid codecs to your media player. These can be found in the K-Lite codec pack, among others. For more details, consult the online help menu of your media player.

19. I am asked for a device driver when installing video cards. Where can I find this?

The video card drivers are found on the VM software CD-ROM (e.g. E:\Drivers). If you no longer have this CD, the drivers can also be found in the ABUS installation directory (e.g. C:\Program Files\ABUS Security-Center\ABUSVMS\Drivers).

20. Can I also operate a printer on the ABUS HDVR / NVR?

Yes, though only USB printers can be used. Please also note that the ABUS HDVR / NVR operating system is found on a CompactFlash memory card, meaning the storage space is restricted. Therefore, only install the device driver and not the included image editing programs or printer management tools.

21. Access to the ABUS system over RTSP does not work. What could the reason be for this?

This may be due to missing port forwarding in the router or missing entries in the firewall. In order for RTSP to work correctly, port 554 must be entered under port forwarding and in the firewall.

8. Frequently used terms (glossary)

PTZ camera	Pan, tilt and zoom camera.
CCTV	Closed Circuit Television.
RS-422 bus	4-wire bus. Used in CCTV for controlling pan/tilt cameras.
RS-485 bus	2-wire bus. Alternative to the RS-422 bus. Also used in CCTV for controlling pan/tilt cameras. Bridges distances of up to 1200 metres.
MPEG-4	Compression format for storing video files.
H.264	Compression format for storing video files.
JPEG2000	Compression format for storing video files.
RTSP	Protocol for streaming real-time video files over the network (RTSP = **R**eal **T**ime **S**treaming **P**rotocol).
fps	Frames per second.
CIF, 2CIF, 4CIF, D1	CCTV resolutions (352x288, 704x288, 704x576, 720x576)
Presets	Saved camera positions for pan/tilt cameras.
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork (digital telephone network).
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol – Regularly used protocol for transmitting data over a network.
VLC Media Player	**V**ideo**L**an**C**lient – Alternative free-to-use media player.
LCD	**L**iquid **C**rystal **D**isplay.
UPnP	Universal Plug and Play – Used for cross-company control of devices.
PAL	**P**hase **A**lternating **L**ine – Used for transmitting images on analogue TV. Used primarily in Europe.
NTSC	**N**ational **T**elevision **S**ystem **C**ommittee – Used for transmitting images on American analogue TV.
ATM	**A**utomatic **T**eller **M**achine – Bank cashpoint

9. Online support and remote configuration

Should you encounter problems, please contact our Customer Support hotline.

The hotline provides support and set-up tips for your product.

If the problem cannot be solved over the telephone, then our service team can also help by accessing your system using a remote maintenance function.

Online support only applies to the ABUS HDVR / NVR in conjunction with the ServicePlus option.

These options are not available on the ABUS VMS Basic, Professional and Enterprise software versions.

Instructions on activating online support can be obtained from our Customer Support personnel.

Have the following information on hand before contacting Customer Support:

ABUS HDVR:

- System model
- Serial number
- Installed software version
- Description of the problem

Video cards:

- Card model
- Installed software version
- Operating system used
- Description of the problem

From version 7.3 onwards, VMS has a support function which automatically generates all the relevant system information. You can save this locally or send it directly by e-mail to ABUS Security Center technical support.

Click *Support* and then *ABUS Support.*

You must fill in all the fields to use the support function. Make sure the information is correct so that your query can be efficiently dealt with.

Click Save to save the data locally. If you are connected to the internet, you can send the data directly to technical support.

Please note that we can only deal with questions if you have contacted our technical support <u>beforehand</u>.

10. Copyright information

This software used the following libraries under the LGPL:

Live555 Streaming Media (http://www.live555.com)

FFmpeg (http://ffmpeg.org)

This software uses the following libraries under the Apache license:

Framewave (http://framewave.sourceforge.net)

==========

OpenSSL *(http://www.openssl.org)*

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

HIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)All rights reserved.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

HIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

ABUS Security-Center GmbH & Co. KG
86444 Affing
Germany
www.abus-sc.com

info@abus-sc.com