It's so easy.

iGuard®

The digital video recording system

User Manual

Version 2.80

Status: December 2008

IDS Imaging Development Systems

Preface

We have taken every possible care in preparing this manual. Nevertheless, we are unable to provide any guarantee with regard to content, entirety or quality of the details contained in this manual. The contents of this manual are revised regularly and brought up to latest standards. Furthermore, we are also unable to guarantee that the product will operate fault-free even if the specifications and recommended computer configuration are observed.

Under no circumstances whatsoever are we able to guarantee that a specific application objective can be achieved with the purchase of this product.

Liability for immediate damages, subsequent damages and damages to others resulting from the purchase of this product is excluded within the terms of existing legislation. Liability under any circumstances is restricted to the product price.

Furthermore we exclude any liability for any possible increase in telephone costs due to unwanted connections during the use of *iGuard® RemoteView* and/or *iGuard®*.

Status: December 2008

Copyright

Security

We would like to remind you that the contents of this operating manual do not constitute part of any previous or existing agreement, commitment or legal relationship, or an alteration thereof. All obligations of *IDS Imaging Development Systems GmbH* result from the respective contract of sale, which also includes the complete and exclusively applicable warranty regulations. These contractual warranty regulations are neither extended nor limited by the information contained in this operating manual.
If you need further information or if you have special problems which are not mentioned in this manual, you can contact your installer or the address listed below.

The installation and maintenance must be done by qualified persons.

The correct and secure function of this system is based on careful transport, correct storing, installation and maintenance.

Data Security

You can also store data of persons. Please take care of legislative order concerning data security.

The system and any storage media as floppy-discs, CDs, removable disks etc. should also only be reachable for you or authorised persons.

Environment
Please take care of the correct use of this system. Otherwise guarantee cannot be granted.

Avoid direct sun, wetness and shock.

The following environment is necessary:

Use:
Temperature: 0° C to 60° C

Non use
Temperature: -20° C to 80° C

Installation and maintenance
The installation, maintenance and, if necessary, repairing must be done by qualified persons.

Trademarks
IDS Imaging Development Systems, *FALCON*, *DORADO* and *iGuard*® are registered trademarks of IDS Imaging Development Systems GmbH. IBM PC is a registered trademark of International Business Machines Corporation. Microsoft is a registered trademark and Windows a trademark of Microsoft Corporation. All other products or company names which are mentioned in this manual are used solely for the purpose of identification and/or description and can be the trademark or registered trademark of the respective owners.

Contacting us

Visit our web site where you will find all the latest program updates and information about our software and hardware products as well as our partners and distributors.

Internet:	http://www.iguard.de	
	http://www.ids-imaging.de	
Address:	IDS Imaging Development Systems GmbH	
	Dimbacher Straße 6-8 D-74182 Obersulm	
Fax:	07134/96196-99	
Email:	Sales:	sales@iguard.de
	Support:	support@iguard.de

Contents

1 Introduction

Thank you for your decision to purchase *iGuard®*. *iGuard®* is a digital video recording system for the surveillance of rooms, premises, buildings, production workshops, critical public areas or any outdoor areas where security is important.
Beside an audio channel there can be recorded up to 40 analogue and 16 further IP cameras at the same time. A simultaneous display of all cameras for live surveillance is possible at the same time as recording. Basically the system allows two different operational recording modes which may also be combined with each other:

- **Long-time recording** analogous to the operation of a standard video recorder, which however has an option for recording only motion pictures.
- **event-triggered recording** that is the recording of alarms with their pre-history via a ring buffer.

In case of event-triggered recording the system is controlled through digital inputs which can be connected with any form of event triggering sensors. In addition, the system allows a logical operation of external sensors with an internal generated digital input. Motion detection with the connected cameras which then operate as video sensors is already integrated into the software.

This means that the system is fully customisable and allows all forms of configurations according to date, time, connected periphery, ambient conditions and plausibility routines. External reactions to occurring alarms are controlled by digital outputs.

iGuard® therefore offers the best possible customisation to your application, both with regard to your various different alarm triggers such as for instance cameras, light barriers etc., and also in case of alarms to control your various external devices such as for instance sirens, alarm systems, lighting etc.. By defining different alarm configurations, you also have the possibility to adjust the video recording to the actual surveillance task in question and thereby maximise the performance of your system.

In addition, *iGuard®* possesses a well-planned user administration. By the assignment of up to 13 different user rights and 3 individual camera rights, it allows for each user to have access to certain functions on an individual basis according to his range of tasks. Such access may also be denied to others. This enables you to make the best possible adjustment to your particular requirements.

Finally, *iGuard®* is developed in terms of clarity and comprehensibility of the windows and dialogs. Most buttons are provided with easy to understand symbols that are placed at suitable points within the window. This allows an intuitive operation of the program. However, if questions do arise, the online help is available at any time.

The delivery includes, free of charge, the *iGuard® RemoteView* and *iGuard® Player* programs in addition to the *iGuard®* program itself. Using *iGuard® RemoteView*, you have the possibility to remote access (via LAN or ISDN/DSL) the system in order to revise the recorded videos and to watch camera-pictures live. Here *iGuard® RemoteView* functions as a client accessing *iGuard®* as a server. When operating *iGuard®* with separate hard discs, *iGuard® RemoteView* enables you to carry out local playback on an external PC. The *iGuard® Player* allows you to replay video recordings or exported AVI sequences.

We would like to wish you a lot of success with this product. Please do not hesitate to contact your individual installer at any time if you have any further questions.

1.1 What is new in version 2.80

Software version 2.80 of *iGuard®* and *iGuard® RemoteView* contains numerous new functions and improvements. Further information on the new features can be found in the specified chapters in the manual.

	iGuard	*iGuard RemoteView*
Multi-monitor support Up to four monitors can be configured for displaying camera images and other functions (see also *3.1.23 Multi-Monitor-Mode).*	☑	☑
Support of 16:10 monitors New split displays for widescreen monitors (see also V*iew menu* in chapter *3.2.3 Menus in display mode*).	☑	☑
System can go to multiple PTZ positions on the basis of alarm triggers (see also *3.1.13 Camera PTZ control*).	☑	
Use of network alarm inputs (see also *3.3.4 Configuration of the alarm sensors (detectors)*).	☑	
User management for *iGuard® RemoteView* (see also).		☑
Audio recording for LAN cameras (see also *3.3.3 Configuration of the LAN cameras*)	☑	
Live image zoom (also possible via the software without PTZ cameras, see *also 3.2.7 Windows*).	☑	☑
Cash box search spanning multiple servers (see also *4.11 Cash box data search*).		☑
Script-based integration of IP cameras IP cameras for which *iGuard®* does not supply a complete script for integration can be integrated using user's own scripts (see also *3.1.11 Network cameras*).	☑	

2 Prerequisites

2.1 Operating system

iGuard® was developed for operation with Microsoft Windows 2000®, Windows XP® and Windows Vista®. It only supports 32-bit systems. The desktop resolution must be at least 1024x768 pixel with 15/16-bit colour resolution. We recommend a resolution of at least 1280x1024 with 15/16-bit colour resolution.
The additional programs *iGuard® RemoteView* and *iGuard® Player* can be operated in Windows 2000®, Windows XP® and Windows Vista®.
The operating systems Windows 95/98®, Windows ME®, Windows NT® and Windows 2003 Server® are not supported.
The functionality of iGuard® cannot be guaranteed if remote control software (pcAnywhere, VNC, ...) is in use.

2.2 Hardware

In *iGuard®* the following video compression boards or frame grabbers from *IDS Imaging Development Systems GmbH* are used, depending on model design:

- *FALCONplus* with 1 to 4 board operation (4 to16 video inputs)
- *FALCONquattro* (4 to 16 video inputs, 4-chanel with 100/120 fps)
- *DORADOquattro* with 1- to 4 board operation (4 to 20 video inputs and max. 50 to 100 fps each board)

The video data is stored on local hard disks. The use of removable hard discs is possible, too. Saving to optical drives such as DVD-RAM, DVD-/+R, DVD-/+RW, CD-R/W is possible direct from *iGuard®* with the writer program NERO 6.0 or higher installed (see *3.4.16 Export to CD/DVD*).
Recording on network drives is also possible. Further Information can be found at *Using network disc drives* (cf. *3.3.1 System configuration*).

FALCON attributes
The following restrictions apply for the operation of a *FALCONplus* or a *FALCONquattro*:

- Setting the compression factor is possible, though it cannot be met exactly. Fluctuations in image size > 100 % are possible.
- Camera signal failures are detected. A test whether the signal is present again, however, is only carried out for technical reasons on the *FALCON* cards in conjunction with a camera test. A camera test is carried out every 10 minutes or at the start of *iGuard®*.

2.2.1 Important note on connecting video monitors

Order of connection
An analogue video monitor can be connected to the video output of *FALCON*- and *DORADO* cards. When you connect the monitor to the card, please always proceed in the following order:

1) Make sure that the monitor is switched off.
2) Make sure that intermediate video devices (e.g. video splitters) are switched off.
3) Make sure that the PC where the card is installed is switched off.
4) Connect the monitor to the video output of the card with a suitable cable.
5) Switch on the PC.
6) Switch on the monitor and if necessary video splitters

If you do not proceed in this order, the video output electronics of the card may be destroyed. This danger is significantly greater for monitors that have a power plug with no protective earth contact.

•

2.3 Resolution and file format

The files stored by *iGuard®* have the extension .IGD.

Resolution at setting *normal resolution*
- 384x288 pixel (FALCONplus/FALCONquattro)
- 352x288 pixel (DORADOquattro)

Resolution at setting *high resolution*
- 768x288 pixel (FALCONplus/ FALCONquattro)
- 704x288 pixel (DORADOquattro)

Resolution at setting *maximum resolution*
- 768x576 pixel (FALCONplus/ FALCONquattro)
- 704x576 pixel (DORADOquattro)

The possible *maximum resolution* (768x576 pixel) depends strongly on the main board used.

2.4 Conversion

As of version 2.35, *iGuard®* automatically converts the configurations of the preceding version to the current version. Nevertheless, we would like to emphasise that you should check your configuration without fail after an update.

A conversion of older versions (earlier than version 2.35) is not possible. It is also not possible to take over settings for ring recordings and scenarios from the preceding versions (earlier than version 2.50). These are deleted during the conversion.

3 iGuard®

3.1 Operation

3.1.1 iGuard® as demo version

You can also run *iGuard®* without video capture hardware and configure all dialogs. Recording is not possible without the video capture hardware. A special hardware simulation enables you though to test the functional capabilities of *iGuard®* despite the lack of hardware.
Four saved video sequences are played back as camera images. All the functions of a real system can be applied to these dummy camera images.

3.1.2 Licensing

With your user‘s manual you will find a registration card with your personal licensing number, the product-key. This number forms a part of the license agreement. The product-key is needed to install *iGuard®*.

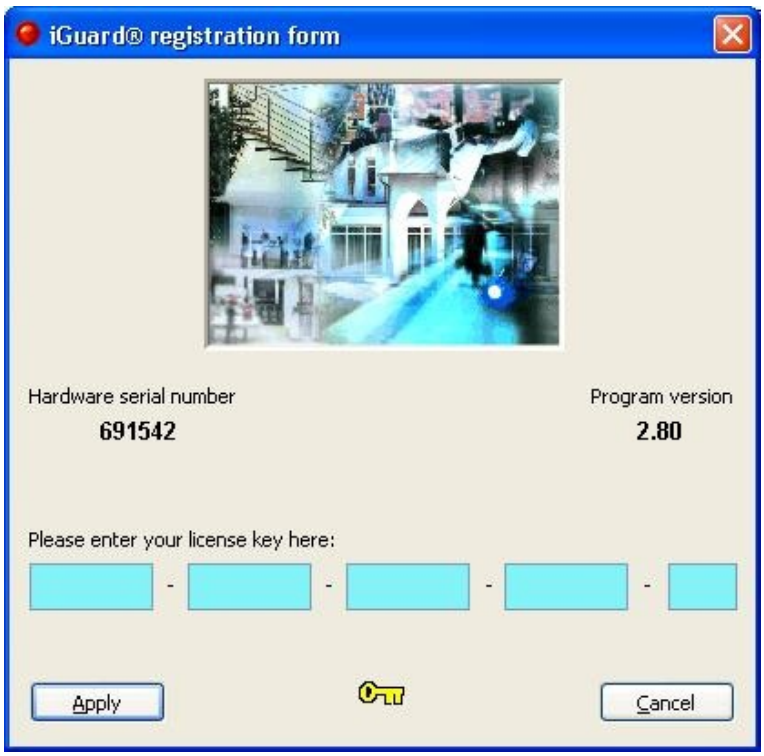


Figure 1: iGuard® registration form

Please keep your licensing numbers in a safe place. So we may keep you informed about further developments and new versions. Please send your carefully completed registration card back to the indicated address. You will then be entered into our customer database.

If a Dongle is contained in the scope of delivery, this must be plugged in at a USB slot. With the plugged in Dongle the input of the licensing number in the registration dialogue is not required any longer.

iGuard® extensions must be licenced. In case of a dongle system, the serial number of the dongle must be transmitted to the *IDS GmbH*. The serial number is noted on the dongle. Alternatively it can be readout from the *Information* page in the section *Licence information* while in *Configuration mode*.
After receiving the serial number, an updated licence file will be generated and transmitted to the customer. The licence file is named *<serial number>.liz*. Updating the licence on the customer's system is performed by the program *iGuard_Dongle_Tool.exe*. This program can be found in the iGuard® installation directory.

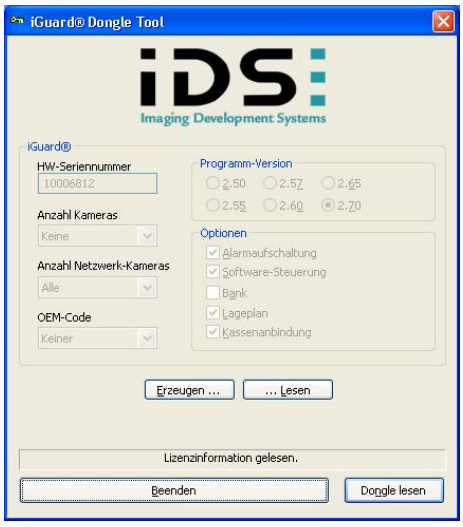


Figure 2: iGuard®-Dongle tool

With the ... Lesen button, Windows' *Open file* dialog will be opened. In this dialog the licence file has to be selected and the procedure has to be completed by clicking the button *open*. Subsequently the data will be copied from the licence file into the dongle.

3.1.3 Starting *iGuard*® (full version)

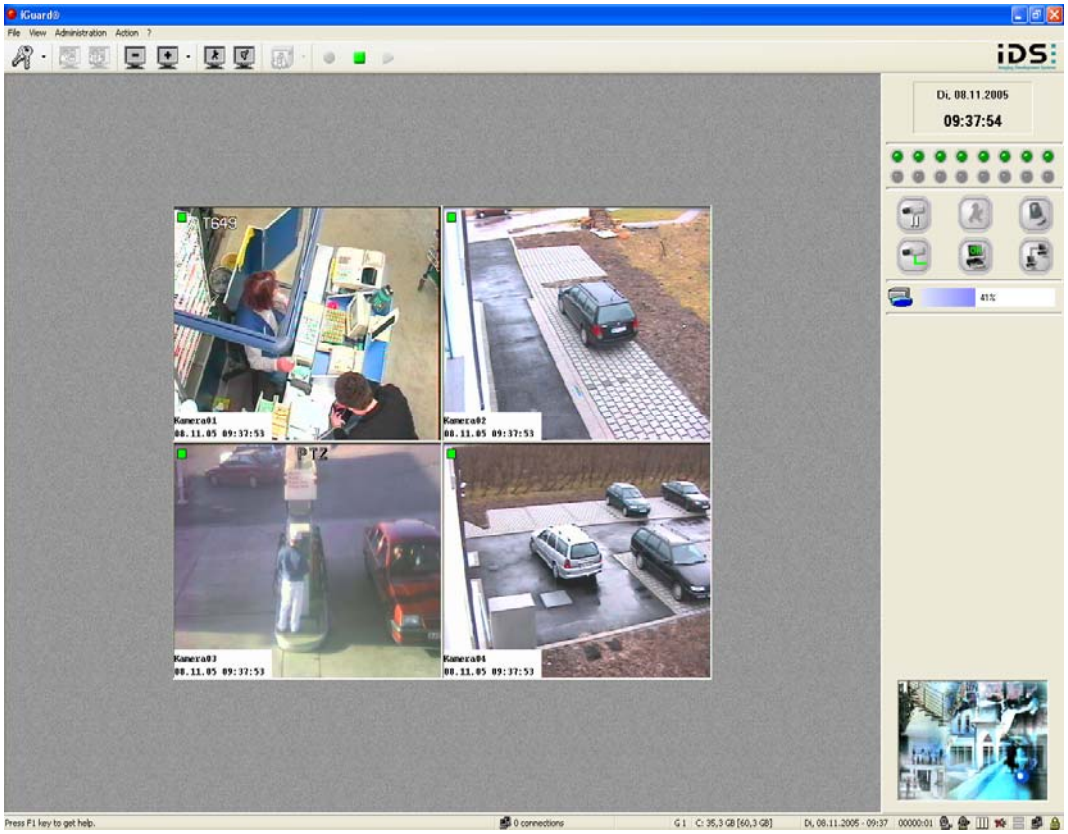


Figure 3: iGuard®-Start dialog

The registered full version of iGuard® can be called up via the **menu** *Start → Programs* of Windows or using the link on your desktop which was created during installation. After iGuard® is started automatically the display mode (see also *3.2 Display mode*) is shown. This mode is the control centre. This is where all cameras are displayed and the output of all alarm and status signals takes place.
Following initial installation and first start, *iGuard®* enters all local hard discs on the list of the discs to be used for recording. The partition where the operating system is installed is removed from the list automatically if there is at least one further local partition. Network drives are not marked automatically as recording drives.
When starting *iGuard®* for the first time, all cameras found by an automatic check of video inputs should be displayed. If this is not the case, one of the following reasons is possible:

- an error occurred during the installation of the hardware or *iGuard®*. In this case, it is essential that the installation is repeated.
- the camera‘s connection to hardware is faulty
- the camera is not sending any signal

3.1.4 Operation using removable hard disks

iGuard® also provides the possibility for the operation using removable hard discs. The revision of video sequences on removable hard discs can then be easily done using *iGuard® RemoteView*. Therefore the path of the database files has to be indicated in the application configuration (cf. *3.3.1 System configuration*). This path **must** exist on the removable hard disc.

3.1.5 Long-time recording

Long-time recording is a recording mode where, as with a standard video recorder, videos are saved on the hard disc until this is completely full. After that, the oldest pictures will be overwritten continuously. As an option the recording of only motion pictures can be adjusted. This feature allows saving plenty of hard disc space without losing important video data and/or events.
With this operating mode, the set lead time does not apply for alarm events (movement, contacts with normal or raid priority). This means that continuous recording (long-term) takes place during periods for example where long-term recording and alarm sensor are active.
An event-controlled interruption of long-term recording is available through configuration of recording parameters of the configured cameras (see *3.3.8 Configuration of the recording*).
Within the configuration it will be defined which cameras shall be recorded, the priority with which this is to happen, and the resolution of the recording. The length of the recording is limited only by the amount of available memory on the hard disc and/or the track length limitation.
If a defined event occurs, long-term recording is interrupted, event-controlled recording is carried out according to configuration and long-term recording restarts again upon completion.

3.1.6 Ring recording

The configured cameras continue operating in ring recording mode until a configured event occurs. Ring in this case means that the recording is been carried out within a loop, therefore the recorded videos will permanently be overwritten (first in/first out principle). The recording duration is determined by the size of a ring buffer. The oldest pictures will be overwritten at the end of a defined period. Therefore, there are always only as many pictures saved as defined by the size of the ring buffer, irrespective of the period during which the ring recording is active. If no ring recording is to be carried out, this can be set by entering a duration of 0 when defining the duration of the pre-trigger (see *3.3.8 Configuration of the recording*).
If an alarm occurs, ring recording stops immediately and alarm recording according to configuration is started so that the data recorded before the alarm is attached to the start of the ring recording and saved. So the pictures of the ring recording always show the history of an alarm (pre-trigger).

3.1.7 Event-triggered recording

In this operation mode in which the system records according to previously defined events. The triggers for such events could be for instance previously configured alarm sensors and/or the video sensors (cameras with enabled motion detection).
A combination of long-time recording and event triggered recording is possible. With choice of the long-time recording additional one or more event triggered recordings ca be defined. Long-term recording is then interrupted if an event occurs during this period.
In the case of event-triggered recording, the duration of a ring recording will also have to be define within the configuration (cf. *3.3.8 Configuration of the recording*). If the recording duration of ring recording is set to 0, recording only takes place in the event of an alarm. There is then no possibility of investigating the pre-history of an alarm.
An event is always triggered by at least one alarm input. As long as no alarm occurs, the system is operating in ring recording. If an alarm occurs, the ring recording is aborted and the appropriate alarm recording is started. A new ring recording is started at the end of the alarm recording. In cases where long-time recording has been selected, the recording continues after the recording of an alarm has been terminated.

3.1.8 Alarm sensor (detector)

An alarm sensor is typically a trigger input of the hardware (opto coupler board). An alarm sensor is being triggered by an external signal on which a record can be started.

Each camera is available as a further alarm detector in conjunction with the motion detection of a camera. See also *3.3.4 Configuration of the alarm sensors (detectors)*.

Referring to the configuration, alarm sensors as for example light barriers, or cameras with activated motion detection can also be understood as alarm detectors.

3.1.9 Switch output (actuator)

A switch output is a digital output of the hardware (opto coupler board) which can be used in order to control an external device (e.g. siren, alarm system, door opener, lights). See also *3.3.5 Configuration of the alarm outputs*.

3.1.10 Digital inputs

Depending upon assigned hardware, up to 8 digital inputs are available. These can be used individual for alarm release or occupied with one of 6 special functions (see *3.3.6 Configuration of the digital input*). Using the opto coupler card Opto I/O III only 4 digital inputs are available for the alarm release.

3.1.11 Network cameras

Parallel to recording from analogue cameras that are connected to the frame grabber of the *IDS Imaging Development Systems GmbH*, it is also possible to record images from specific LAN cameras (see also *3.3.3 Configuration of the LAN cameras*).
Combined operation (different LAN cameras) and hybrid operation (analogue cameras and parallel network cameras) is possible. A maximum of 16 other network cameras are supported in addition to the analogue cameras.

The number of supported network cameras depends on the license that has been purchased.

iGuard® treats network cameras as locally connected analogue cameras.
Sole restriction: Network cameras cannot connect with analogue video outputs (e.g. VOUT with *FALCONplus)*.

Access to images (live images or stored recordings) from network cameras is possible via *iGuard® RemoteView*. *iGuard® RemoteView* is also able to display analogue and network cameras parallel.
The following should be taken into consideration if using network cameras:

- Network cameras require per camera considerably more computer capacity than local analogue cameras. The frame rates required by the network cameras are decisive for the processor workload.
- The frame rate depends on a large number of factors and cannot be guaranteed. Catchphrase: Network overloading, multiple simultaneous accesses.
- The picture quality of the network cameras is stated in per cent. Precise details are not possible as each network camera recognises different quality levels and/or interprets the data differently. Consequently, it is very difficult to make a clear statement of required hard disc capacity per recording day for network cameras.
  The image quality is poorer than with analogue cameras as a result of the compression prior to transmission. As a result of this, motion detection can repeatedly trigger false alarms or fail to recognise movements.
- Several users can gain access to network cameras at the same time. In this respect, *iGuard®* is just one other user for the camera. The frame rate usually sinks as a result of access by several users. In addition, users can often change image parameters (e.g. brightness, compression) via browsers. The changes then apply for all users, in other words for *iGuard®* as well. For example: a user lowers the image brightness to 0, *iGuard®* now only receives a black image and can therefore no longer carry out any motion detection.
- Access to network cameras takes place with much greater delay time than with access to local (analogue) cameras.
  The reason for this is the increased complexity of the communication between *iGuard®* and the network cameras, the network and the partly slow network cameras with lower internal computing capacity.
  Starting and stopping recording, changing to configuration mode and configuration of the network cameras is slower than one is used to with analogue cameras.

Script-based integration of IP cameras

To enable use of network cameras in *iGuard*, a camera script must be provided for each camera type. For many camera models, scripts are already supplied in *iGuard*. If other cameras are to be integrated, a script can be generated for this camera by the user and integrated into *iGuard*.
The scripts are generated in the free script language PAWN using a simple text editor. The existing scripts can be used as a basis for developing your own camera scripts. The parameters for the camera in question must be as stated in the product description supplied by the manufacturer.

Further information on script-based integration of IP cameras can be found in the PDF document "IP Camera Integration“ which is available on request from the *iGuard*® support.

3.1.12 Motion detection (camera as video sensor)

The last picture of a camera is constantly being compared with the current picture of the same camera. If there is a change in the picture content in a pre-set manner, *iGuard*® recognises a movement in the picture. This process is called Motion Detection and can be activated for each individual camera.
Motion detection can be used to activate an alarm record and/or record the picture from a camera only if there is a change in the picture's content. In the first case the camera itself is being used as an alarm detector also. Considerably less storage space is required in the case of the latter because only those pictures are saved where there has been a change in the content of the picture.
Parameters for the motion detection have to be adjusted separately for each camera. In addition, it is also possible to define sections of the video picture where motion detection should not or should only be carried out. This enables movements to be ignored, e.g. movement of trees caused by wind and particular attention to be given to areas of special interest.

3.1.13 Camera PTZ control

Cameras with pan-tilt-zoom control that are connected to a serial interface (RS232 or RS485 via converter) or via the network can be controlled by *iGuard*®.
Several PTZ cameras can be connected as long as the following conditions have been fulfilled:

- All cameras connected to a serial interface (COM-Port) must use the same protocol
- All cameras connected to a serial interface (COM-Port) must have its own RS-485 address

The user can control the camera using the keyboard, the mouse (see *PTZ speed control with the mouse*), a commercially available PC joystick or with graphic control elements that are displayed in the dialog bar at the bottom right.
The system can also store and go to PTZ positions subject to the triggering alarm input (see also *3.3.8 Configuration of the recording*).

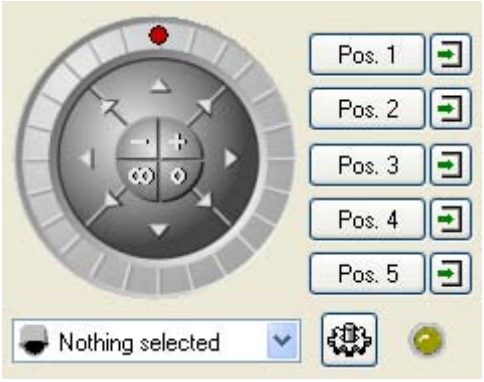


Figure 4: Camera control (PTZ and focus)

These control elements only appear if a PTZ camera is configured (see *3.3.2 Configuration of the cameras* and *3.3.3 Configuration of the LAN cameras*) and initialised correctly (COM-Port free). The control elements are no guarantee that the camera itself is functioning.
In order to display the control elements, a user must be registered and have the camera rights *Display* and *PTZ control*.
The PTZ control has eight control buttons (arrows), two buttons each for zoom (- and +) and manual focus (O and OO) and a speed control.
The auto-focus mode is activated again automatically with a pan-tilt command.
Under the PTZ control element, there is a selection list Pos. 4 where all configured positions (maximal 32) are listed with position names. The system goes to a position if it has been selected.
Movement to the first 5 stored set positions is possible using the control elements Pos. 1 to Pos. 5. The position names are also displayed with these control elements. With the button it is possible to save the current camera position to the according control.
Pushing the button , the PTZ camera will move to the stored position automatically.
The PTZ symbol is bordered in yellow in the live image of the camera currently being operated by the control system and the window is given a yellow surround. Non-active PTZ cameras, on the other hand, are marked with a grey PTZ symbol. If several cameras can be controlled, a click with the left mouse button in the window of a camera activates the PTZ control for that camera.
The following key commands are available for PTZ control:

Action:	Cursor keys	left, right, up, down can be used with the number pad switched off (Num Lock off):
	7	up-left
	8	up
	9	up-right
	4	left
	5	centre
	6	right

	1	down-left
	2	down
	3	down-right
Zoom range:	+	nearer
	-	farther
Focus control:	0 (Ins)	Focus far
	, (Del)	Focus near

Along with the graphic control elements, the keyboard control and/or mouse control, the cameras can also be controlled using a joystick.
The aforementioned control possibilities are also available in *iGuard® RemoteView*.

Multi user PTZ control
Users with the right for the PTZ control of a camera, get the camera picture with a grey frame and the grey signature PTZ displayed. To activate the control the user clicks into the camera window. Afterwards frame and signature are displayed in yellow and the user has control of the PTZ control.
If another user has the camera in this moment in access, a message box is displayed.

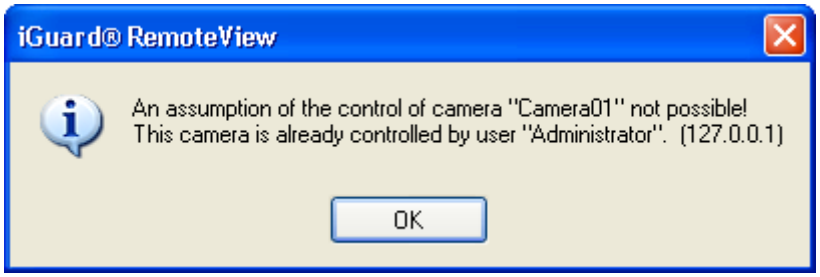


Figure 5: Multi user PTZ control - messagebox

The message box informs about the currently user access of the PTZ control. If a user has a camera in access, this camera is blocked for other users. The blocking is cancelled if

- the user has logged out
- an adjusted time elapsed, since that the last PTZ control command was sent to the camera (see also 3.3.1 System configuration)
- the automatic circulation of the stored camera positions has been started

Users, who do not have control of the PTZ control, see the graphic controls, however these are inactive.

Click-To-Pos
A special function is available for some LAN-PTZ cameras: *Click to Position*. A click on the left mouse button in the camera's live image and the camera drives to the required point and positions it centrally in the image.
This is a special function of some LAN cameras and cannot be used by other pan-tilt cameras.

The mouse pointer changes when positioned over a camera window with Click-To-Pos capability. This function must be activated over the context menu.

PTZ speed control with the mouse

Figure 6: PTZ speed control with the mouse

The driving speed of the PTZ camera can be adjusted variable by mouse and keyboard. For this the user must click the red point of the PTZ control with the mouse, keep left mouse button pressed and move the red point semicircular like a controller. The left stop (position 270 degrees) is highest the driving speed, the right stop (position 90 degrees) the smallest. In the position shown the middle speed is selected.

3.1.14 Sabotage detection

With the help of the automatic sabotage detection, which is possible with analogue cameras and network cameras (see *3.3.2 Configuration of the cameras* and *3.3.3 Configuration of the LAN cameras*), it is possible to detect turning, dazzling and covering. If sabotage is detected, *iGuard®* reports the sabotage on the screen and makes an entry in the logbook. In addition, an e-mail can be sent and a switch output activated.
Sabotage by blinding is only recognised if a large part of the image is affected. Momentary blinding by vehicle headlights, which is within normal operating conditions for example at petrol stations, is therefore not recognised as sabotage. The same applies to the recognition of sabotage by obscuring. Here too, a large part of the image must be obscured.

Imperative for the best possible recognition of sabotage is optimal illumination at all times.

Highlights of sabotage detection are the following features:

- Self-learning
- Vibration-resistant
- Can be used indoors and outside
- Relatively weather-proof

- Can also be used under normal street lighting at night
- Optimised algorithm requiring little processing power; therefore all connected cameras can be monitored
- Can be used with colour and b/w cameras
-

Sabotage detection fails:

- If unsuitable cameras are used (e.g. without AGC)
- If lighting conditions change suddenly (except abrupt transitions between light and darkness ==> false alarm)
- If too large areas of the image change in a short time ==> false alarm
- If the camera is turned only very slightly ==> no alarm
- If the camera is turned very slowly ==> no alarm
- If turning the camera does not result in sufficient changes to the image (e.g. if it is pointed at a monochrome wall or a field) ==> no alarm

The quality of sabotage detection depends on the quality of the image content

3.1.15 In the event of an alarm

iGuard® checks whether there is a recording configuration for a camera for the signalled event. If this is the case, recording is started in accordance with the stored configuration.
If several events occur at the same time which would result in recording with the same camera, *iGuard*® decides on the further procedure according to the stored recording configuration. The following rules apply in this case:

- for recordings in the same recording mode (e.g. motion recordings), current recording continues until all events have been processed;
- long-term recordings are interrupted by a movement or alarm contact;
- motion recordings are interrupted by an alarm contact;
- alarm recordings with normal priority are interrupted by an alarm contact with suspicion priority (3.3.4 Configuration of the alarm sensors (detectors)). This function is available only in the optional banking mode.
- alarm recordings with suspicion priority are interrupted by an alarm contact with raid priority (3.3.4 Configuration of the alarm sensors (detectors)).

Recordings are protocol led in the log book and stored in a database if the option *log book entry* has been activated (*3.3.8 Configuration of the recording*). The log book is integrated into the user interface of the replay mode (cf. *3.4 Playback mode*) and can be displayed or hidden per option. Only the abbreviated version with the last events to have occurred are shown in display mode (cf. *3.2 Display mode*). An acoustic alarm can also be sounded parallel to this.

3.1.16 Alarm messages

In the event of an alarm, an alarm text can be specified using recording configuration (*3.3.8 Configuration of the recording*) for each camera and each alarm type (movement, contact with normal priority, contact with suspicion priority, contact with raid priority).
In display and replay mode, this alarm message is shown at the lower edge of the live or replay images together with the alarm image from the triggering camera.
A user should confirm this message. The message and confirmation are recorded in the log book.
If no confirmation is received within 15 minutes, the message disappears. An entry is then made in the log book that the message was not confirmed.
If several messages occur that are not confirmed, only the first message is displayed and registered for each camera.
With alarm messages it is possible to give the user instructions about what further action should be taken by the user in the event of any such alarm.

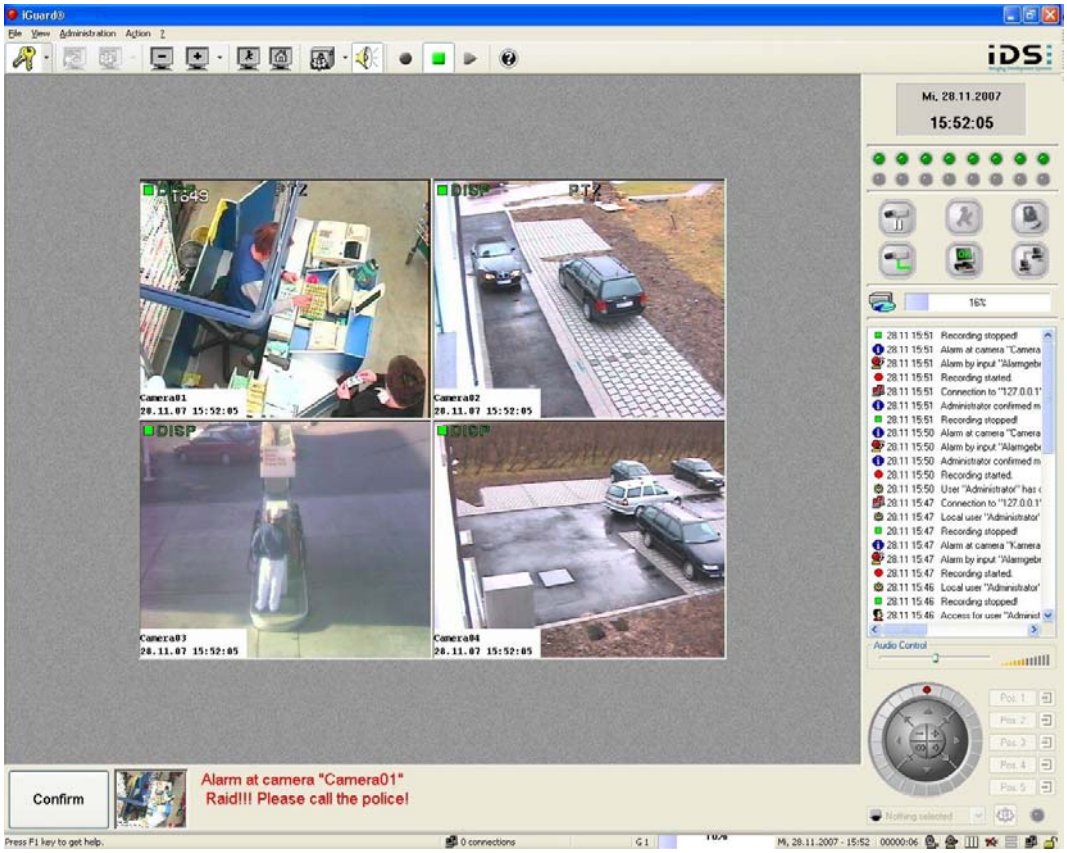


Figure 7: Alarm messages in playback mode

3.1.17 Alarm connection (optional)

As special function a connection to a client is set up if an alarm occurs. The alarm connection takes place with the events:

- Alarm event
- Motion event
- Camera loss
- Sabotage

The login at the client is carried out automatically. The live image of the camera that had detected the motion, that had triggered the alarm, is displayed immediately. Switching on the alarm can be time controlled. This means that setting up a connection can only take place at specific times, e.g. outside of business hours. The time restrictions are global, i.e. irrespective of the type of occurrence that leads to a connection being set up.
5 different addressees van be specified. A time schedule can be set up for each addressee. In the event of an alarm, the system attempts to call the first addressee. If the first addressee is not available, an attempt is made to call the second addressee and so on.

3.1.18 E-Mail/SMS messages

iGuard® can send e-mails or SMS messages event-triggered. With the email dispatch an alarm image of the alarm camera can be attached. MMS messages cannot be dispatched. Forwarding takes place automatically if a specific event or a malfunction occurs or at one of the following failures:

- Camera loss
- camera signal again available
- UPS announces: power failure
- UPS announces: power supply again available
- *iGuard®* incorrectly terminated (e.g. Watchdog, power failure), E-Mail at the next restart
- Relevant data overwritten (attitude from database configuration dialog)
- Recording could not be started
- Fatal recording error
- Hard disk full, recording is stopped
- Loss of a hard disk
- Hard disk online again (after a loss)

Sending these messages can either be via a network or an installed internal or external modem. An SMTP mail server must be available in the network for the network version.
The event-controlled activation of the E-Mail/SMS dispatch takes place within the configuration of the recording (cf. *3.3.8 Configuration of the recording*)

3.1.19 Databases

iGuard® uses databases in order to save messages and information about the recorded video data. The dBASE format is being used as database. This format is widespread and suitable for industrial use. The *iGuard®* databases that are used have the file ending *.VDB* for **V**ideo **D**ata**b**ase.
A second database (message database) is being used in order to save the received messages. When *iGuard®* is started, the database is read out and the entries written in the logbook. This ensures the latest messages to be seen after re-starting *iGuard®*.
Various user-defined data is stored in the ext. database.
It is also possible to use various functions in the databases within the *playback mode* using the **menu** *Database* or by pressing the right mouse button (see *Menu Database* in *3.4 Playback mode*).

3.1.20 Please-wait-dialog

A progress dialog is automatically displayed (also applies for *iGuard® RemoteView*) after a certain time from the start of an action. These shows:

- the expected (= estimated) remaining duration of an action in min. and sec. (with precision to 5 sec.)
- a light to dark progress bar symbol for the previously completed part of the action (relative to the overall process) as well as the corresponding percentage data
- a switch button for aborting the action
- The remaining time display always relates to the remaining time for all parallel running activities. Fluctuations in the display are possible because the estimated remaining time is calculated from the already existing elapsed time and the progress achieved within that period of time. The calculated time can vary from the actual time particularly in the case of changing transmission speeds of data transmission (ISDN) connections.

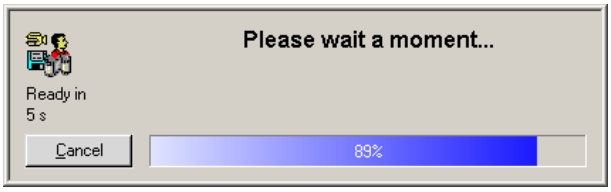


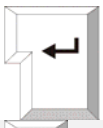
Figure 8: Remaining time display iGuard®/iGuard® RemoteView

3.1.21 Short cuts in *iGuard®*

	Function in display mode	Function in playback mode	Function in *iGuard®* Player
Ctrl + Alt + 1	PTZ Pos 1	Play backwards	
Ctrl + Alt + 2	PTZ Pos 2	One frame back	
Ctrl + Alt + 3	PTZ Pos 3	Stop	
Ctrl + Alt + 4	PTZ Pos 4	One frame forwards	
Ctrl + Alt + 5	PTZ Pos 5	Playback forwards	
Ctrl + Alt + 6	Next PTZ-Cam.	Go to start	
Ctrl + Alt + 7	PTZ patrol mode	Timeline Zoom In	
Ctrl + Alt + 8	Next group	Timeline Zoom Out	
Ctrl + Alt + 9	Split	Go to end	

Ctrl + Alt + ←	PTZ left	Slower	
Ctrl + Alt + →	PTZ right	Faster	
Ctrl + Alt + ↑	PTZ speed +	Frame forwards	
Ctrl + Alt + ↓	PTZ speed -	Frame back	
Ctrl + Alt + R	Show server version (only RemoteView)		
Ctrl + ⇧ + Alt + 1	Start PTZ Zoom In	Speed x0,1	0,5 frames/second
Ctrl + ⇧ + Alt + 2	Start PTZ Zoom In	Speed x0,5	2 frames/second
Ctrl + ⇧ + Alt + 3	Start PTZ Zoom In	Speed x1	10 frames/second
Ctrl + ⇧ + Alt + 4	Start PTZ Zoom In	Speed x3	15 frames/second
Ctrl + ⇧ + Alt + 5	Start PTZ Zoom In	Speed x7,5	25 frames/second
Ctrl + ⇧ + Alt + 6	Start PTZ Zoom In	Speed x20	50 frames/second
Ctrl + ⇧ + Alt + 7	Start PTZ Zoom In	Geschw. x50	200 frames/second
Ctrl + ⇧ + Alt + ←		Playback backwards	
Ctrl + ⇧ + Alt + →		Playback forwards	
Ctrl + ⇧ + Alt + A	PTZ up	More quietly	
Ctrl + ⇧ + Alt + B	PTZ down	Triplex mode	
Ctrl + ⇧ + Alt + C	Full screen	Louder	
Ctrl + ⇧ + Alt + D	Go to revision	Go to live mode	
Ctrl + ⇧ + Alt + E	Stop PTZ Zoom In/ Zoom Out	Stop	
Ctrl + ⇧ + Alt + S	Signal state		
Ctrl + ⇧ + 1	Start PTZ Zoom Out	Speed x0,1	
Ctrl + ⇧ + 2	Start PTZ Zoom Out	Speed x0,5	
Ctrl + ⇧ + 3	Start PTZ Zoom Out	Speed x1	
Ctrl + ⇧ + 4	Start PTZ Zoom Out	Speed x3	
Ctrl + ⇧ + 5	Start PTZ Zoom Out	Speed x7,5	
Ctrl + ⇧ + 6	Start PTZ Zoom Out	Speed x20	
Ctrl + ⇧ + 7	Start PTZ Zoom Out	Speed x50	
Ctrl + ⇧ + M		Mark time	
Ctrl + ←			Frames forwards

Ctrl + →			Frames backwards
Ctrl + F	Full screen		Full screen
Ctrl + G	Next group		
Ctrl + Space			Playback backwards
Space			Playback forwards
Alt + 1	Change split display		
Alt + 2	Change split display		
Alt + 3	Change split display		
Alt + 4	Change split display		
Alt + 5	Change split display		
Alt + 6	Change split display		
Alt + 7	Change split display		
Alt + 8	Change split display		
Alt + 9	Change split display		
Alt + L	Logbook comment		
Alt + X	End		
1 ... 9	Go to PTZ Position 1 ... 9		
↑	PTZ up		Faster
↓	PTZ down		Slower
←	PTZ left		Frames forwards
→	PTZ right		Frames backwards
+		Faster	
-		Slower	
A			Audio playback
S			Stop
F1	Help	Help	
Pos 1			Go to start
End			Go to end
Page up			Louder
Page down			More quietly

		Playback/break
		Louder
		More quietly
		Mute
		One image forwards
		On image backwards
		Playback/break
 (numeric pad)	PTZ left bottom	
 (numeric pad)	PTZ right bottom	
 (numeric pad)	PTZ center	
 (numeric pad)	PTZ top left	
 (numeric pad)	PTZ top right	
 (numeric pad)	PTZ focus near	
 (numeric pad)	PTZ Zoom in	
 (numeric pad)	PTZ Zoom out	
 (numeric pad)	PTZ Focus near	
 (numeric pad)	PTZ Focus far	
 (numeric pad)	PTZ Focus far	

3.1.22 Multimedia Control Panel

The multimedia control panel is no product of *IDS Imaging Development Systems GmbH*. It can be purchased under the product name ShuttlePRO^2 over the company Contour Design Ltd. (www.contourdesign.com).

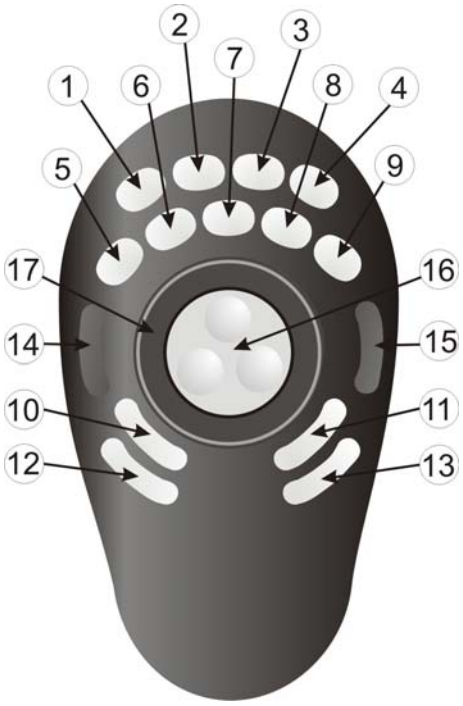
The multimedia control panel was integrated and tested in *iGuard*®. *IDS Imaging Development Systems GmbH* cannot guarantee an error free operating of the multimedia control panel. It is not supported by *IDS Imaging Development Systems GmbH*. Please contact the manufactuer for problems with this product.

The multimedia control panel offers the following possibilities:

- Controlling of the *iGuard*® recording functions
- Controlling of the *iGuard*® player
- Controlling of different functions in *iGuard*® live mode

The Multimedia control panel simulates keyboard entries. If the necessary keyboard codes are known, the device can be configured freely. Further information for the configuration of the control device you can find in the manufacturers operating manual.

The keys of the multimedia control panel are mapped as shown below.



Taste	Function in Displaymodus	Function with playback	Function in iGuard® Player
1	Next PTZ camera	Go to start	Go to start
2	PTZ patrol mode	Timeline zoom in	-
3	Next group	Timeline zoom out	-
4	Split display	Go to end	Go to end
5	PTZ Pos 1	Playback backwards	Playback backwards
6	PTZ Pos 2	One frame backwards	-
7	PTZ Pos 3	Stop	Stop
8	PTZ Pos 4	One frame forwards	-
9	PTZ Pos 5	Playback forwards	Playback forwards
10	PTZ up	Volume down	Volume down
11	Full screen	Volume up	Volume up
12	PTZ down	Triplex	Full screen
13	Change to revision	Change to live mode	Close
14	PTZ left	Slower	Slower
15	PTZ right	Faster	Faster
16	PTZ speed	Single frames	Single frames
17	PTZ zoom	Fast-forward/rewind	Fast-forward/rewind

Figure 9: Multimedia control panel – keyboard layout

In order to be able to use the multimedia control panel in *iGuard*®, the necessary configuration files

- igdPlay.pref
- iGuard®.RemoteView.pref
- iGuard®.pref

which are stored in the *iGuard*® program directory must be loaded. The configuration files will be loaded with the program Contour Shuttle Device Configuration which is available after installation of the multimedia control panel.

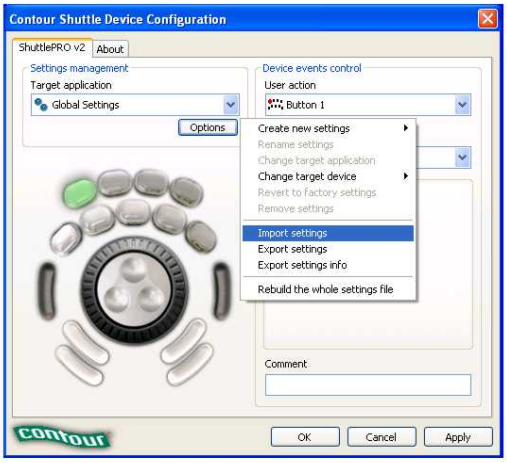


Figure 10: Multimedia Control Panel – configuration program

With *Options → Import settings* the configuration files must be loaded successively. Loading the configuration files is necessarily only once.

3.1.23 Multi-Monitor-Mode

In multi-monitor mode, *iGuard*® and *iGuard*® *RemoteView* support up to four monitors. The distribution of the monitors is configurable (see also *3.3.19 Configuration of the multi-monitor mode (iGuard®)* and *4.2.4 Configuration of the multi-monitor mode (iGuard® RemoteView*). When *iGuard*® is run as demo version the multi-monitor-mode is partially available (see also *3.1.1 iGuard® as demo version*).
In multi-monitor mode, the main monitor retains the same functionality as in single-monitor mode.
Additional monitors can be assigned the following functions:

- Display monitor
- Event monitor
- Sequence monitor
- Map monitor
- Message dialog monitor

3.2 Display mode

3.2.1 Starting dialog

The *display mode* represents the start surface of *iGuard®*. It is displayed automatically after starting the program and is used simultaneously as surface for live monitoring of camera images.

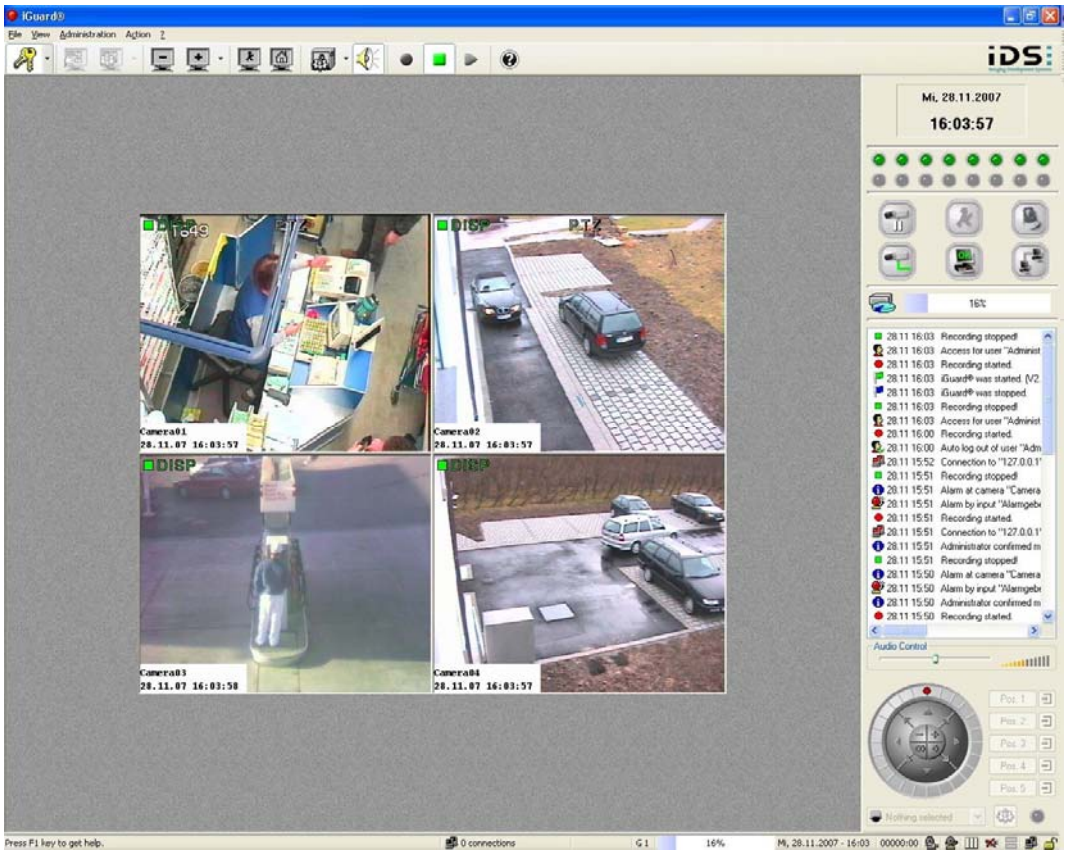


Figure 11: iGuard® display mode

3.2.2 Login

The login takes place via the **menu** *File → Login* or click on the corresponding button in the symbol bar.
Alternatively over a drop-down menu which can be opened using an arrow symbol to the right of the log-in button the user names of the last 5 successful registrations can be displayed and user name selected.
This function is not available during first log-in as the list only shows a history. The list is empty if nobody has registered yet. In this case, the below shown *iGuard®* log-in dialogue box, where the user name and password has to be entered is opened. Entering user name is not required if using the drop-down

menu. The password, however, still has to be entered manually. This function is not available in *iGuard® RemoteView*.

When first starting *iGuard®*, the input of the following entrance data is necessary:

- User name: Administrator
- Password: Administrator (displayed as ***)

Capitalisation is to be considered.

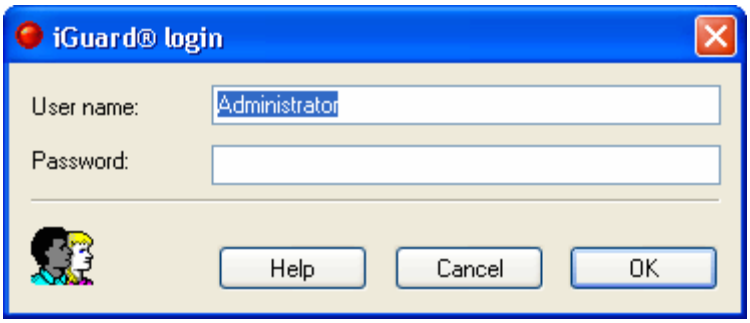


Figure 12: iGuard®-Login

The user name *Administrator* cannot be deleted. We advice to change the password.
The user manager needed to alter the password can be found in the *configuration mode*. This can be achieved by two manners:

- **menu** *File → User manager*. Therefore the authorisation *User management* is necessary.
- **menu** *Administration → Configuration*. Therefore the authorisation *Configuration* is necessary. The *user manager* is opened via the corresponding register.

More about the *User management* can be found in corresponding chapter (cp. *3.3.16 User management*).

4-eyes login for replay
For access to stored recordings (replay), *iGuard*® can be configured (cp. *3.3.1 System configuration*) so that the change to replay has to be confirmed by a further user. This also applies for replay via *iGuard*® *RemoteView*.
All actions are carried out under the name of the main user. The main user is the user who has logged into the system. If switching to replay, the procedure has to be confirmed by another user who also has replay authorisation. An entry is made in the log book.

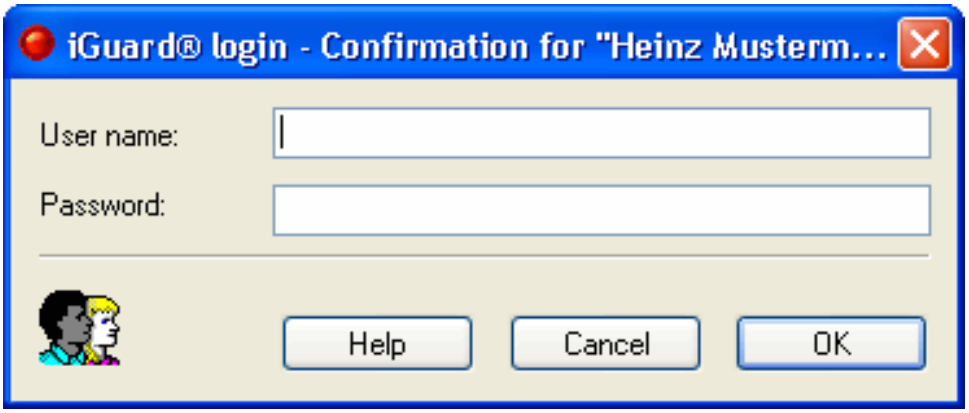


Figure 13: iGuard® login confirmation

The user *Administrator* is the sole exception to this. This user has direct access to stored recordings even without confirmation from another user.

3.2.3 Menus in display mode

Menu File

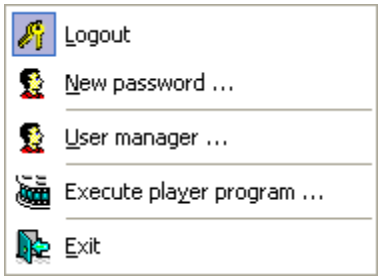


Figure 14: Display mode – menu File

- Logout/Login
  Logout/Login current user.
- New password
  For the change of the password the option *User can change password* must be activated for the appropriate user in the user administration (see *3.3.16 User management*). This option can be set by an administrator or a user with user administration authority.

The change of the password takes place in the dialog *Password modification*. Here first the old password must be entered and in the field under it the new password. The new password must be entered for confirmation again in the field *Confirmation*.
After input of all fields the dialog will be left through pressing the button OK.

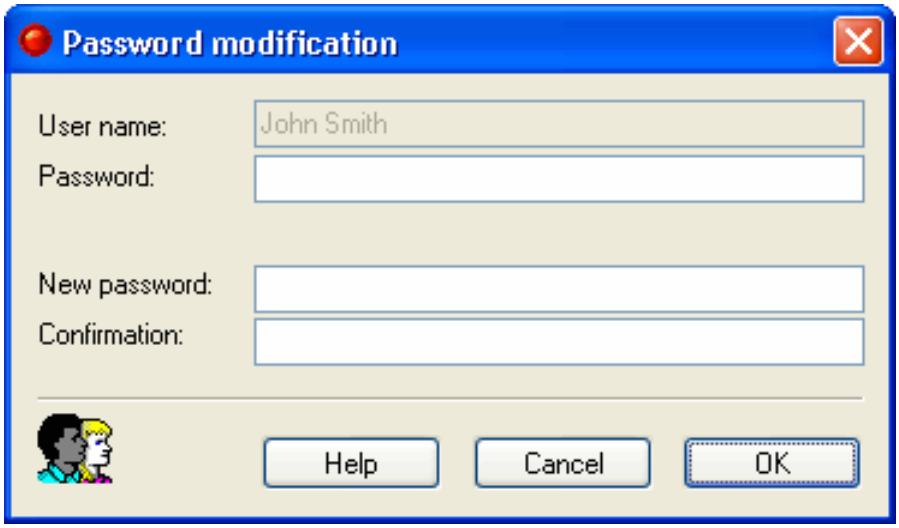


Figure 15: New password

- User manager
  The configuration dialog for the user management is opened (see also 3.3.16 User management).
- Execute player program
  Start oft the *iGuard® Player*. With this the AVI files produced of *iGuard®* in the MJPEG format can be opened and played(see also *5 iGuard® Player*).
- Exit
  iGuard® is terminated after the confirmation of a security check.

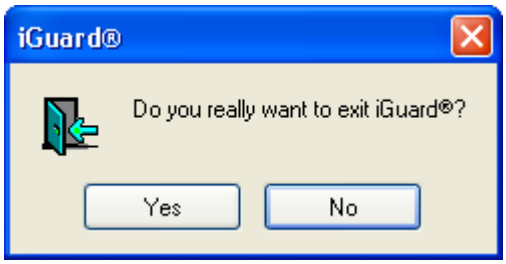


Figure 16: Exit iGuard®

Menu View

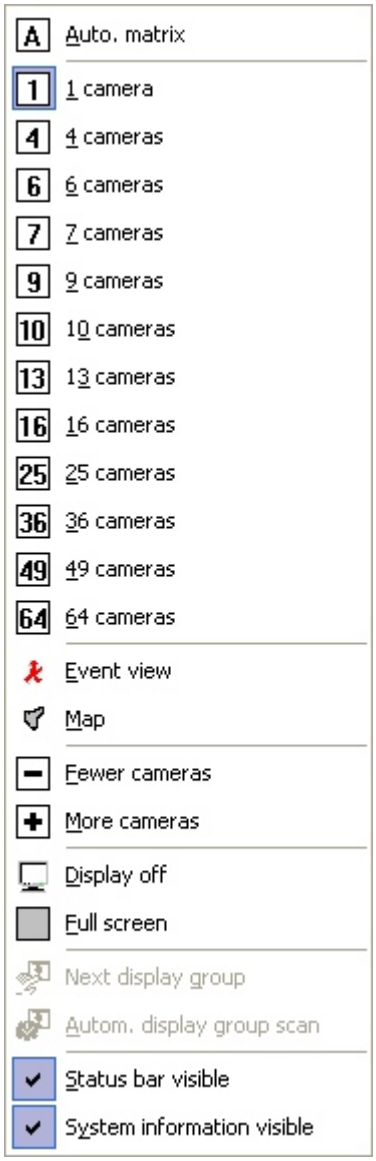


Figure 17: Display mode – menu View

- Auto. matrix
  All configured cameras are displayed (see also 3.3.1 System configuration).
- Camera split
  Adjustment of the multiple split display. The camera windows can be displayed equally in a 1-, 4-, 9-, 16-, 25- 36- or 48--split (there are adjustments possible depending on the respective hardware being used, so in the 9 camera split only 8 cameras are displayed if e.g. two *FALCONplus* are installed). Using the 6-, 7-, 10- and 13-split the windows are displayed in different sizes. If a monitor is available with the display aspect ratio 16:10, additional display modes adapted for the 16:10 format are displayed. These include e.g. a distribution for 6 x 4 cameras and a wide-format distribution for 6

cameras. The window split which is automatically active after starting *iGuard*® is defined in the configuration mode (*3.3.1 System configuration*).

- Event view
  Open/closed the event view (see 3.2.9 Event Window)
- Map
  Open/close the optional map (see 3.2.10 Map)
- Less/more cameras
  Multiple split view is increased/reduced by one step at a time until the maximum/minimum number of displayable windows is reached.
- Display off
  The whole camera image representation is switched off, even if a user is announced.
- Full screen
  The full-frame mode shows the camera images without status, menu and title bars and can also be activated with the key combination *CTRL-F* as well as by selection in the **menu** *View → Full-frame*. The full-frame mode can be terminated using the middle mouse button or *ESC*.
  If the mouse is moved to the border of the screen a menu bar will appear. In this the full-frame mode can be left with the option *Normal view*.

Figure 18: Activate border menu in full screen mode

In the dialog of the configuration of the application it can be defined whether *iGuard*® *appears in the* full frame mode when starting.

- Start camera scan
  Activates/deactivates the sequential output of the images of the configured cameras on the video exit.
- Next display group
  Manual switch to the next group of cameras. See also Camera groups in 3.2.7 Windows.
- Automatic scan
  Automatically switch to the next camera group. See also Camera groups in 3.2.7 Windows.

- Status bar visible
  Activates/deactivates the status bar (see also 3.2.6 Status bar).
- System information visible
  Activates/deactivates the system information with announcement of the time, the switch outputs and status messages as well as the PTZ control (see also *3.2.5 System information*).

Menu Administration

Figure 19: Display mode – menu Administration

- Configuration
  Change to the configuration mode (see also 3.3 Configuration mode).
- Playback
  Change to the playback mode (see also 3.4 Playback mode).

Menu Action

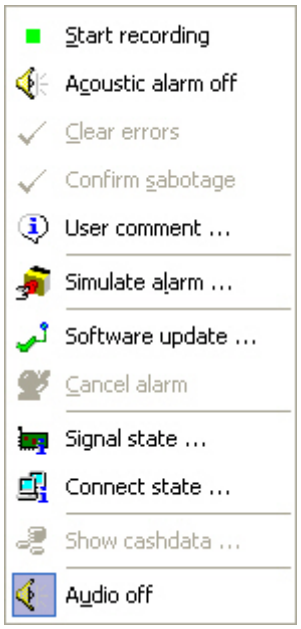


Figure 20: Display mode – menu Action

Start/Stop recording
Starting and stopping of the recording is carried out either via the **menu** *Action → Start/Stop Recording* or directly by selecting the appropriate button from the symbol bar. The recording action is identified by *REC* in the picture of the camera in question. When a camera is defined as video sensor (motion detector), movement is displayed by *DET* in the picture of the camera in question. If cameras are not recording but are nonetheless displayed, this is indicated by *DISP* within the picture. Displaying the camera condition as a symbol or as text must be activated in the system configuration (*3.3.1 System configuration*).

- Acoustic alarm off
  With this menu option it can be specified whether *iGuard®* sends a short acoustic signal in the case of an occurring alarm (see also *3.3.1 System configuration*).
- Clear errors
  Acknowledges a pending warning and resets the system status display .
- Confirm sabotage
  Acknowledges a pending sabotage and resets the sabotage status display Sabotage detection is re-initialised.
- User comment
  A user can record own comments at any time. These are saved in the log book together with the user's name. Log book comments can be inserted also by using the key combination *ALT-L*. This function is also available in *iGuard® RemoteView*.

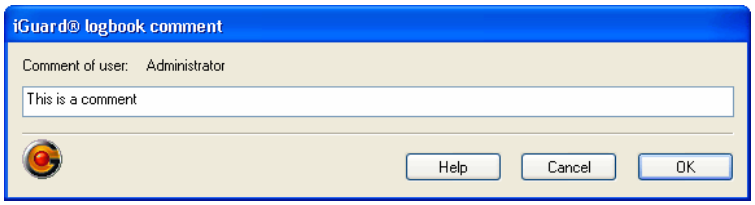


Figure 21: iGuard® logbook comment

- Simulate alarm
  For test and/or practice purposes alarms can be simulated purposefully. Thus exact adjusting of alarm-releasing events is possible. This function may only be called up if it has been released in the configuration mode (*3.3.1 System configuration*).
- Test alarm
  Trial recording can be triggered with activated bank operation in the recording mode. As a result, all cameras record image sequences of 5 frames. Triggering trial recordings is recorded in the log book so that it is possible to search selectively for trial recordings at a later date.
  As the recordings must be available permanently, they are not deleted if the recording capacity has been used up completely. A deletion only takes place if the number of pre-set recordings has been exceeded (see *3.3.14 Banking (optional)*).
- Software update
  See 4.20 Accomplish software updates.
- Cancel alarm
  With this option pending alarms can be cancelled manually. If an alarm is cancelled manually, this is documented in the logbook. This function is also available in *iGuard® RemoteView*.
- Signal State
  Signal states of the cameras, alarm sensors, switch outputs and digital inputs can be displayed at the server. The following symbols are used:
  movement detected
  lost signal

	sabotage detected
(LED light red)	active alarm sensor
(LED light green)	active switch output
(LED light blue)	active digital input

With a double click on a switch output LED the switch output can be switched, if it is configured as remote controllable switch output.

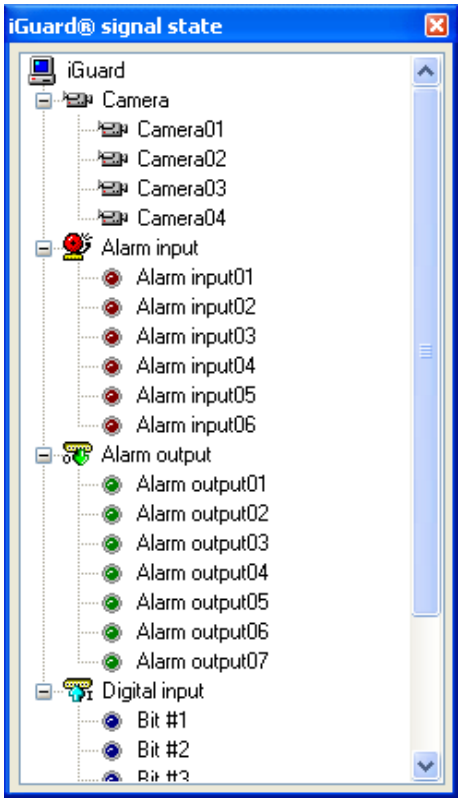


Figure 22: Signal state

- Connect state
  Connect state informs about the current connections of RemoteView clients to the server.
  An active connection can be closed with one double click on it. Thus it is possible to terminate a selective connection at the server.

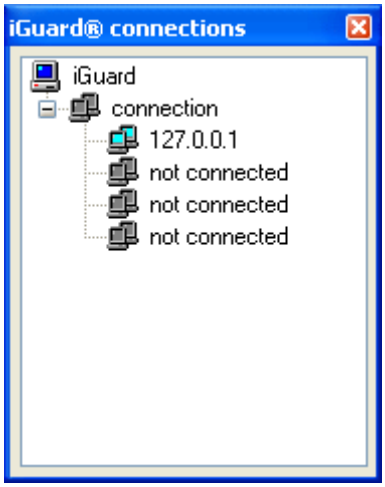


Figure 23: Connect state

- Show cash data

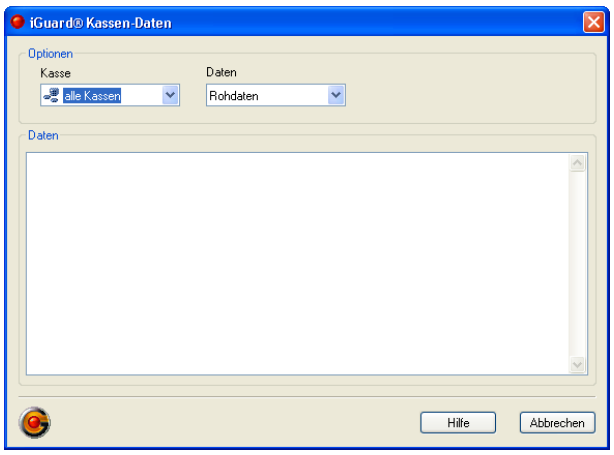


Figure 24: Show cahs data

Opens a further dialogue in which the transmitted cash box data are displayed. The following options are available:

- Cash
  - all cash boxes
  - selection of one cash box
- Data
  - Raw
  - Codepage
  - Filtered

Changes at the filter settings become visible with the next incoming data.
Audio on/off
Activates/deactivates audio output in display mode.

Menu Help (?)

Figure 25: Display mode – menu Help

- Help
  By selection of the *Help* option the *iGuard*® help is opened.
- Technical support (optional)
  This menu item opens a window with advices for the technical support.
- About *iGuard*®
  With this option the dialog *About iGuard*® is opened.

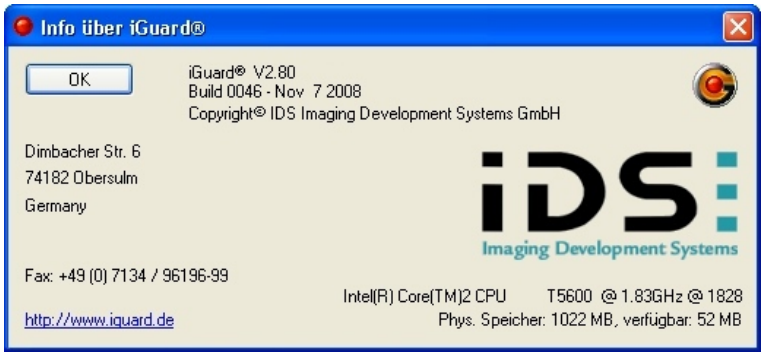


Figure 26: About iGuard® dialog

3.2.4 Symbol bar in display mode

Symbol	Description
	Authority of the user (see also *3.2.2 Login*).
	Next display group. Manual switch to the next group of cameras. See also *Camera groups* in *3.2.7 Windows*.
	Automatic scan Automatic switch to the next group of cameras. See also *Camera groups* in *3.2.7 Windows*.
	Less cameras.
	More cameras. A click on the arrow symbol opens a window, in which the possible splits are indicated.
	Open/close the event view (see *3.2.9 Event Window*)
	Open/close the map (see *3.2.10 Map*)

Cameras on monitor. A click on the arrow symbol opens a window, in which the configured and released cameras are indicated.

Activates/deactivates audio output

Start the recording.

Stop the recording.

Change into the playback mode (see also *3.4 Playback mode*).

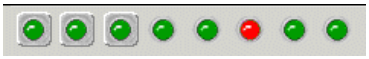
Opens the *iGuard*® help (this symbol appears only, if the Acrobat Reader is installed).

3.2.5 System information

System Date and Time

These data are stored in the database together with the video and audio recordings. If necessary, you can synchronise them according to DCF77 standard using external products.

Status indication of the digital switch outputs



A status display is entered for the first 16 switch outputs at the monitor level. Form and colour of the display have a special meaning:

Grey:	switch output not configured, not being used
Green:	switch output inactive
Red:	switch output active
Green/Red surrounded by a rectangular field:	This switch output can be activated or deactivated by the user manually. The colour of the display (red, green) shows the active/non-active status.

If the mouse indicator rests on a status LED, a popup tool-tip shows the name of the switch output.

System status


No recording at the moment


Min. one camera is recording


Min. one error detected


No movement


Movement detected


No alarm


Alarm


Camera connection ok


Camera breakdown


Sabotage detected


Sabotage and camera breakdown detected

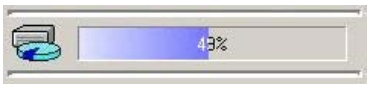
System condition ok


System error


No active connection to an *iGuard®* client


Connection to an *iGuard®* client is online

Hard disk capacity



This display shows the used hard disk capacity, for video- and audio data. This means:

0% hard disk empty
100% hard disk full

Logbook (see also *3.4.4 Logbook*)

The logbook is visible in the display mode only if a user is logged in. In the logbook the newest messages are displayed. Extended functions like filtering or printing the displayed data is not possible.

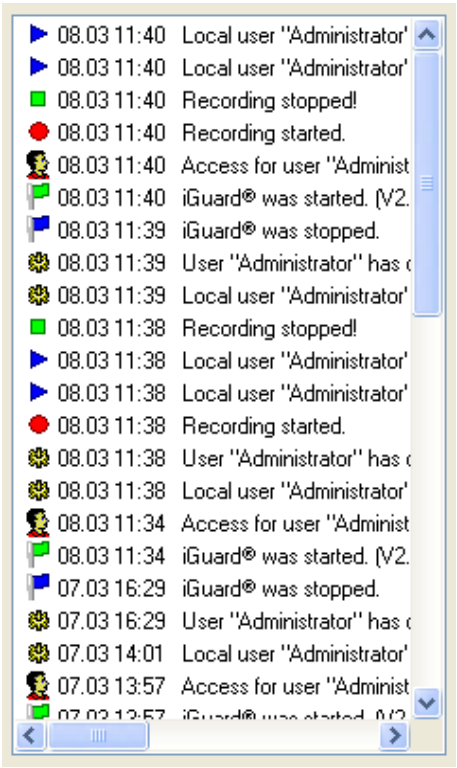


Figure 27: Logbook window

3.2.6 Status bar

Figure 28: Status bar

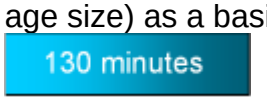
At the bottom of the screen a status bar can be found. This can be switched on or off with the help of the menu *View → Status bar*. A part of the information is also displayed in the system information. The status bar is divided into 14 fields. The meaning of the fields from left to right is as following:

- Brief help text to the menus (Windows-standard)
- Messages of the application (instructions, errors)
- Connecting speed
- Currently displayed camera group
- Free storage space of drive(s) being used and the minimum required free space (see below in this chapter)
- Date and time
- Application running time in hours and minutes
- Symbol showing whether a camera has detected a motion
- Symbol showing whether i*Guard®* is currently recording an alarm
- Status indication of the sabotage detection
  - ♦  Sabotage detection is active – no sabotage detected.
  - ♦  Min. 1 camera has detected sabotage.
  - ♦  Min. 1 camera is not ready.
  - ♦  Advance warning
- Symbol showing an activity or a fault in hardware
- ISDN-Connection
  - ♦  Channel 1 and Channel 2 are not busy
  - ♦  Channel 1/ Channel 2 is busy, connection is built-on.
  - ♦  Dial-up of Channel 1/ Channel 2
- Symbol showing there is an active connection with a *iGuard® RemoteView* client.
- Login/logout symbol showing the user status

The available disk capacity is shown in 4 stages in the status line, 2 of these are shown as a graph display. The switching takes over through a click with the left mouse button in the status field.

Stage 1: The disc capacity which is already occupied is shown as a percentage in the form of a blue bar.

Stage 2: As stage 1, but showing the estimated remaining recording time. This is an estimate because the system does not display the actual remaining recording time but, instead, measures the data volume that can still be saved and displays it as an estimated available remaining recording time. The system uses the actual settings (frame rate, image size) as a basis for this estimate.



Stage 3: Shows in text form the designation of the hard disc where current recording is taking place, the disc's available capacity and its maximum capacity.

Stage 4: Shows in text form the available capacity and the maximum capacity of all hard discs authorised for recording.

The display form set last is stored and used automatically again when *iGuard®* is restarted. This does not apply to *iGuard® RemoteView*.

3.2.7 Windows

In display mode all camera pictures are each located within one window. Each window has a pre-set size and position. The number of visible camera windows depends on the configuration and the chosen order of the windows. Only those cameras are displayed which have been configured in the configuration mode (see *3.3.2 Configuration of the cameras*) and released for display. The name of the camera, date and time may also be displayed within the camera picture. Position and colour for these text titles can be set in the configuration mode (*3.3.2 Configuration of the cameras*).

Camera information
If the mouse is moved to the upper left corner of a camera window, information on the camera supplying the current image in that window is displayed. Depending on configuration and user rights, the following information can be displayed:

- Camera name
- Sabotage status (only if sabotage recognition is configured for that camera).
- Input (only for users with configuration rights)
- IP address (only for LAN cameras and users with configuration rights)
- Camera model (only for LAN cameras and users with configuration rights)

Live image zoom
For all cameras, a section can be freely selected from the live image and displayed enlarged. To do this, click the live image with the left mouse button while holding down the CTRL key and draw a rectangle. When the mouse button is released, the selected section will be enlarged to the image size. By clicking on the image you can return to the full-screen display.

Display camera in another window
To display a camera in a different window, hold down the left mouse button and drag the image from this camera to the desired window. When you release the mouse button in the desired output window, the output windows for these camera images are swapped. This allows you to easily regroup cameras.

Insertion of the operation modes
Several acronyms are displayed in the video frame to identify the mode of operation:

DISP	Camera image is only displayed
DET	Motion detection is activated
REC	Camera is recording
PLAY	The last rcord is shown.
PTZ	Camera has pan-tilt-zoom function
PTZ yellow	The camera has pan/tilt and zoom functions and is currently active. The window of an active PTZ camera has yellow edging.
PTZ grey	The camera has PTZ function, but is not active, i.e. the PTZ function is not being applied to this camera.

Camera groups

If more cameras are released for display than can be displayed simultaneously in a multiple split screen, all cameras are divided into groups. *iGuard®* defines these groups independently. The first n camera windows are located in Group 1, the last camera windows to be displayed are in the last group. The groups may be switched through either manually or in an automatic sequence. The groups are shown in order, with the first group being shown again after the last group. The selection of either manual or automatic switching through is carried out via the menu *View → Next Display Group* or *Automatic Scan*, or directly by selecting the appropriate button in the symbol bar. During the enlarged display of a window, switching through camera groups is not possible. (see also *3.2.3 Menus in display mode* and *3.2.4 Symbol bar in display mode*).

3.2.8 Pop-up Menu in the Display Window

Clicking the right mouse button opens the pop-up menu for the respective camera window. The pop-up menu provides additional functionalities.

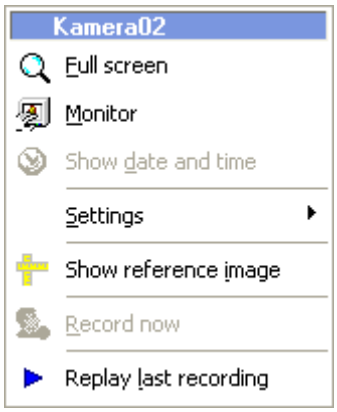


Figure 29: Pop-up Menu in the Display Window

Full screen

Each camera window can be enlarged and centred. To do this, double-click the left mouse button on the respective image or select the *Full screen* **menu item** on the pop-up menu. Return to the normal view by the same process.
The size of the full screen image is limited to the size of the display window. If the image from the camera is larger than the display window, the camera image is scaled down so that it fits into the display window.
Only one camera window can be enlarged at any one time.

In multi-monitor mode, the enlarged camera window is displayed in full-format view on the second monitor if neither the map nor the event window have been activated. If it cannot be displayed on the second monitor, it is shown on the first monitor as usual.

Monitor
Display of the camera picture on an attached analog monitor.

Show date and time
If more windows are displayed than cameras are connected, you have the option of displaying the date and time in one of the unused windows. To do this, select the *Show date and time* **menu item** in the corresponding camera window.

Settings
The *Settings* **menu item** calls up the dialogue for setting the camera parameters.

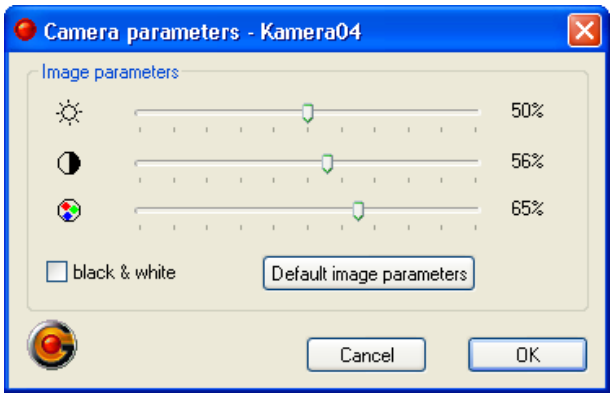


Figure 30: Setting camera parameters in display mode

These parameters allow you to control how live images are displayed and recorded.

Show reference image
A reference image documents the setting of a camera (frame cut-out) at the time when a reference frame was generated. Following installation and alignment of the camera, the displayed reference frame section can be held and compared at any time with the camera's current display locally on the server or by remote access with *iGuard® RemoteView*.
Reference images are generated in the configuration dialog of the camera (see *3.3.2 Configuration of the cameras*). The system automatically generates a camera image and saves this under a pre-set name. The images are stored in the application's main directory (e.g. C:\Program files\IDS\iGuard®). They are named camref*x*.jpg, whereby *x* represents the number of the camera.

Displaying a saved reference frame is possible both on the server (monitor level) as well as with *iGuard® RemoteView*. The user must have *Playback* and *Display* authorisation for this.
With *iGuard®* displaying the reference image is achieved by using the **menu item** *Show reference image* in the context menu.
The display of a reference frame by *iGuard® RemoteView* is virtually identical. A connection with a server must exist, the live image of the camera must be visible. A click with the right mouse button in the image of the required camera opens up the context menu in this case as well. The menu option *Display reference image*, however, is always enabled in this case if the user has authorisation to display a reference image. An appropriate notifying message is displayed if no reference frame is stored on the server for the selected camera.

Figure 31: Display reference image

Record now
Cameras can be switched by the user from live image to record mode using the **menu item** *Record now*. To do so, the user requires *Start/Stop* authorisation. Manual triggering uses the same settings for recording as set for motion recording. If no motion recording is installed, the camera records for 10 seconds at the maximally frame rate.

Replay last recording
During recording, the last recorded sequence can be played back via the pop-up menu for the camera. To do this, open the pop-up menu in the corresponding camera window with the right mouse button and then select the *Replay last recording* function. With regard to this function, please note the following:

- This function can only be activated for one camera at a time. As soon as the function is activated for a second camera, playback from the first camera stops.

- A maximum of 10 seconds are played back.
- You can end playback by calling up the function again.
- If the last recording was made more than 10 minutes ago, you cannot play it back.
- During playback, recording continues in the background.

3.2.9 Event Window

In multi-monitor mode, the event window can be displayed in full-format view on the second monitor (see also *3.1.23 Multi-Monitor-Mode*). The main monitor continues to display live images.

When the Event window option is activated, the display window is divided according to a preset layout. The large event window is displayed at top left, and twelve smaller camera windows to the right and below it.

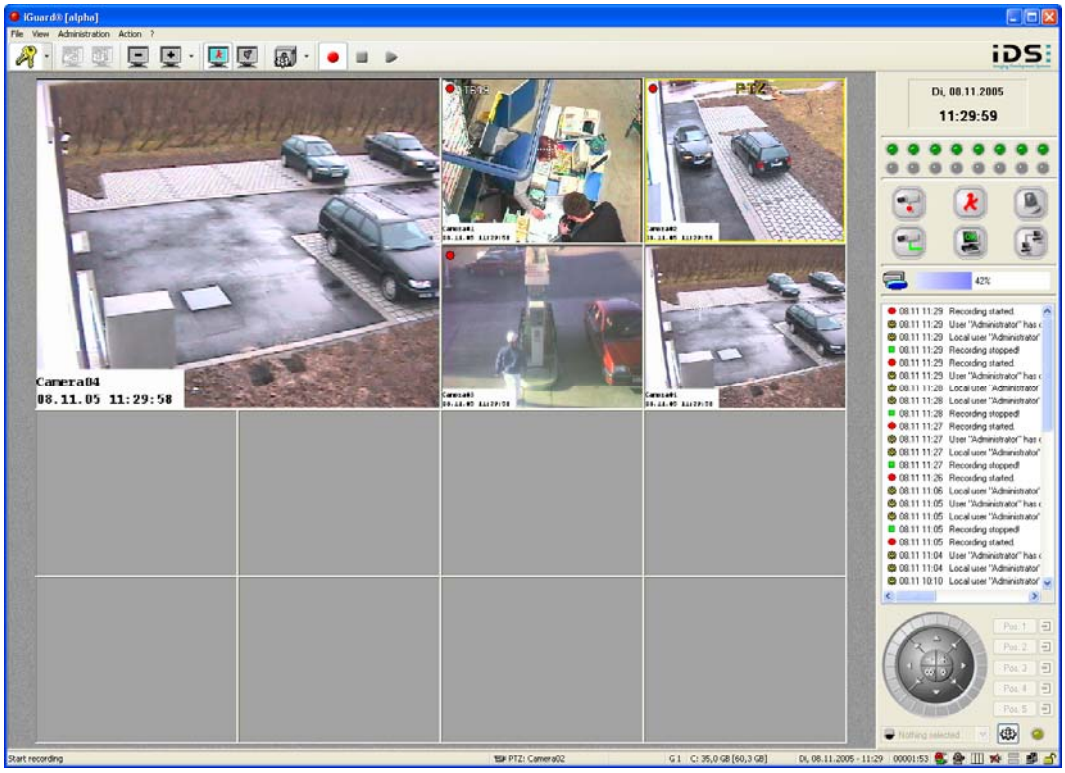


Figure 32: Event window

When an event occurs, the current camera image is additionally displayed in the event window. If several events occur, the camera image of the event that occurred first is always displayed. The display switches to the next event after a preset time. This time is preset in the control panel in the Show event on video monitor at least ... second(s) field (see 3.3.1 System configuration).

3.2.10 Map (optional)

In multi-monitor mode, the event window is displayed in full-format view on the second monitor (see also 3.1.23 Multi-Monitor-Mode). The first monitor continues to display live images.

View in single-monitor mode
When the optional map is active, the display window is divided horizontally. In the upper part, one large and four small windows are displayed. This layout is preset and cannot be changed. In the lower part, the map is displayed as configured (see *3.3.17 Configuring the Map*).
The Event window option (see *3.2.9 Event Window*) can additionally be activated at any time.

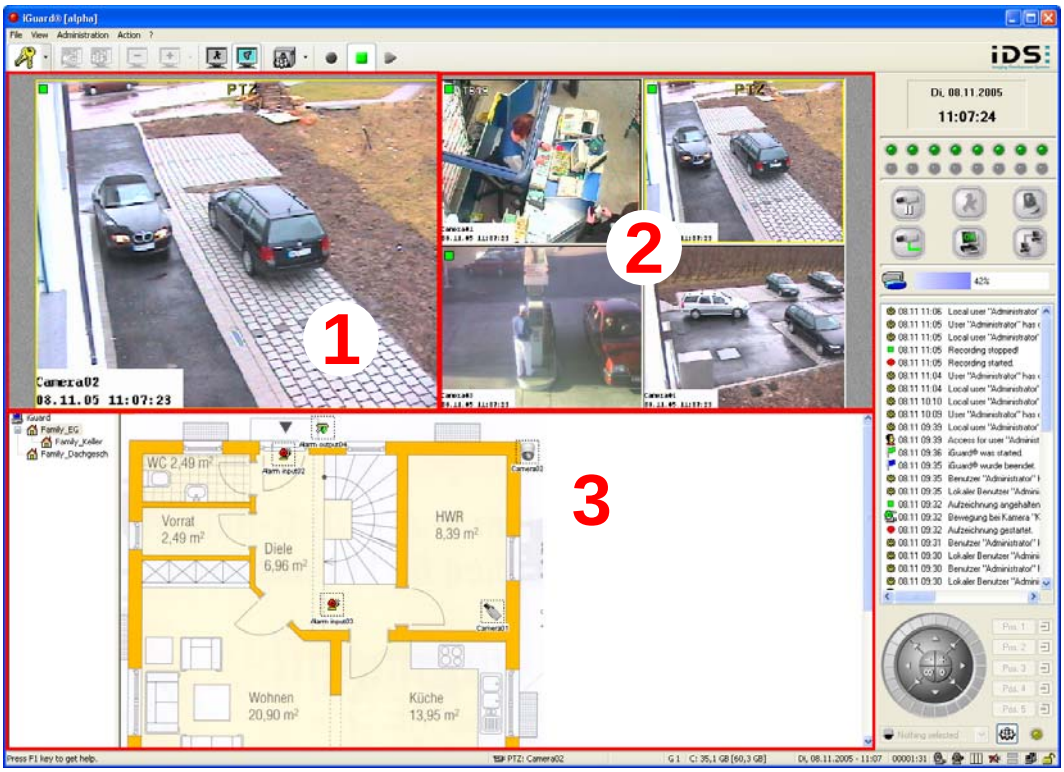


Figure 33: Map

- The image from the camera you have selected by clicking on the map is displayed in this window.
- Four live images are displayed here. Depending on how many cameras are configured (see *3.3.2 Configuration of the cameras*), the next four cameras can be displayed via the button Next Group.

- In section 3, the map is displayed as configured (see 3.3.17 Configuring the Map).

Actions on the map

- When a camera has been selected by clicking, the live image from this camera is displayed in window 1. If the camera in question is a pan-tilt-zoom camera, the PTZ controls are automatically assigned to this camera.
- The pop-up menu of a camera is opened by clicking the corresponding camera symbol with the right mouse button. The pop-up menu allows you to start recording manually. Apart from the option Show date and time, the pop-up menu is the same as that in the display window (see also *3.2.8 Pop-up Menu in the Display Window*).
- Double-clicking an output line sets/deletes this output if it is remotely controllable (see 3.3.5 Configuration of the alarm outputs).

Display modes on the map

- Green flashing border around a camera.
  This camera is currently recording motion.
- Red flashing border around a camera.
  This camera is currently recording an alarm.
- Red flashing border around an alarm input.
  This alarm input has been triggered.
- Green border around an output line.
  This output line has been activated.
- If any of these actions occurs on a layer that is not currently visible, the name of that layer is shown in red and flashes in the menu tree.

After activating the optional map this can be used also with *iGuard® RemoteView*. See *4.2.3 Configuring the Map* and *4.5 iGuard® RemoteView Map (optional)* for more information on the *Map* function.

3.3 Configuration mode

In the configuration mode, you can setup the display, functionality and operation of the application. Furthermore, this is where the hardware and event configuration takes place specifying the complete process for the recording and reaction to occurring alarms. In addition, all users to work with the system can be setup within the configuration mode with their individual authorisations and passwords.

Changes can only be made in the configuration dialogue when no recording is taking place.

During a recording, the data in the configuration dialogue can be viewed, but not changed.

If you switch to configuration mode while recording, the following message appears:

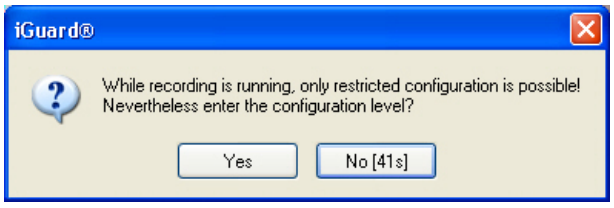


Figure 34: Alert when switching to configuration mode

If you click the Yes button, you are taken to the non-editable configuration dialogue. If you click No, *iGuard*® returns to recording mode.
To make changes to the configuration, you must switch the recorder to *Stop* before accessing the configuration dialogue. Then no recording can take place. In order to resume recording after changing the configuration, the recorder must be reactivated by clicking *Record* .

The configuration dialog, which can be called up in the display mode via the **menu** *Administration → Configuration,* consists of different pages. The page turning is done by clicking the tabs. The number of pages to be seen depends on the authorisations of the logged in user and the hardware upgrading of the system.

The parameters and their effects on *iGuard®* are described as follows. The description bases on the assumption of a user with administrator authorisation. The number of visible configuration points depends on the issued authorisation rights.

3.3.1 System configuration

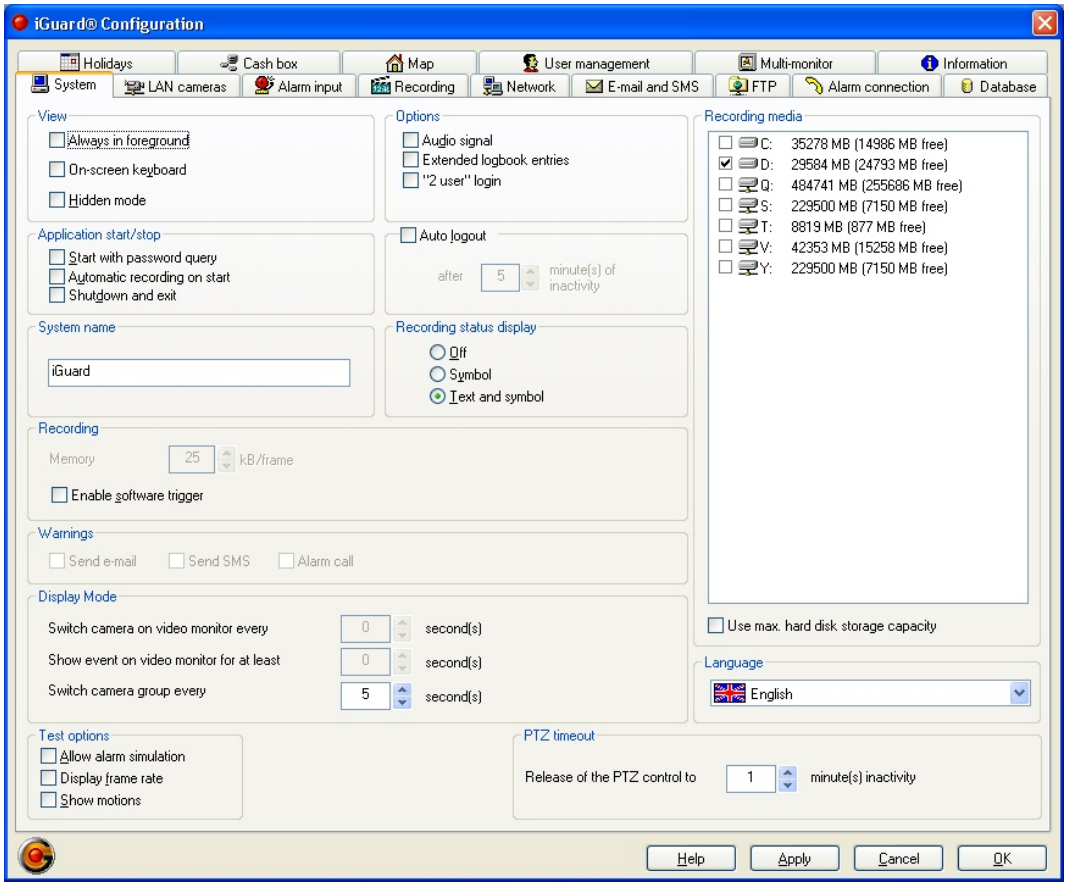


Figure 35: System configuration

View

- Always in foreground
  Selecting *iGuard® always in foreground* has the effect that the application will always be displayed in the foreground and cannot be overlaid by any other Windows application program. Thus a user can start no other program.
- On-screen-keyboard
  The *On-screen keyboard* option creates a virtual keyboard on the screen. Its keys are strikable via mouse click. This possibility is foreseen for systems with no externally connected keyboard.

Figure 36: Virtual keyboard

- Hidden mode
- If the *Hidden mode* option is activated and no user is logged on, the screen is blacked out and the keyboard will not respond to input. Click the left mouse button to open the *iGuard*® logon dialogue. When you have successfully logged on, the blackout is deactivated and the *iGuard*® display mode appears.
- Multi-monitor mode

  In multi-monitor mode, the first monitor retains the same functionality as in single-monitor mode. The map, the event window or a zoomed view of a video frame can be displayed in full-format view on the second monitor.

Options

- Audio signal

  If audio signals are allowed when new messages arrive, these can be activated with the option *Audio signals*. Afterwards the emission of audio signals can be switched on and/or off in the display mode using the **menu** *Action → Acoustic Alarm*.
- Extended log book entries

  If extended entries are activated, an entry is made in the log book when printing and storing individual images or when exporting sequences.
- 4-eyes login for replay

  For access to stored recordings (replay), *iGuard*® can be configured so that the change to replay has to be confirmed by a further user. This also applies for replay via *iGuard*® *RemoteView*.

  All actions are carried out under the name of the main user. The main user is the user who has logged into the system. If switching to replay, the procedure has to be confirmed by another user who also has replay authorisation. An entry is made in the log book.

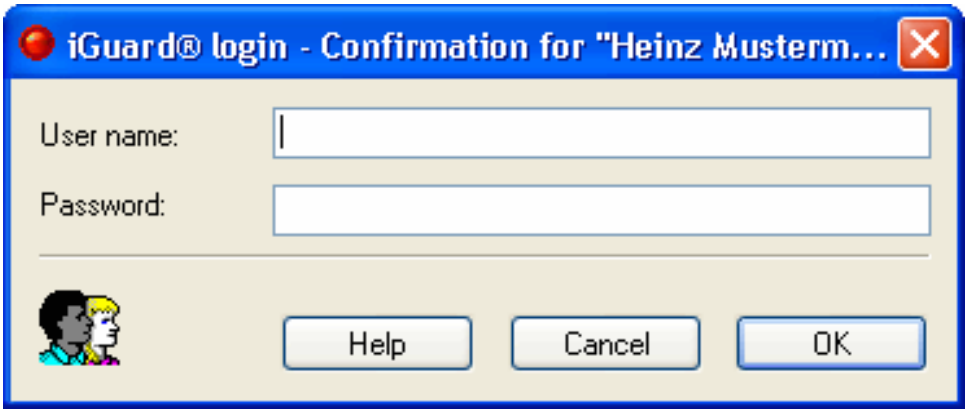


Figure 37: iGuard® login-confirmation

The user *Administrator* is the sole exception to this. This user has direct access to stored recordings even without confirmation from another user.

- Banking mode (optional)
  The banking mode is activated by selecting this option. If the banking mode is activated/deactivated, a window is displayed to notify the user that it is necessary to restart *iGuard®*.

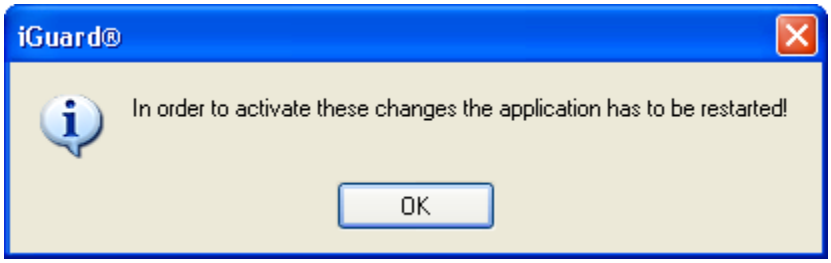
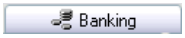


Figure 38: Restart after activating the banking mode

When *iGuard®* is restarted

- ♦ The Banks' tab is loaded/unloaded 
- ♦ The configuration for the banking mode is loaded/unloaded.

Recording media

- Definition of the drives
  All available drives (inclusive network drives) are indicated in a window .This is used to specify the disc drives where video data is to be recorded. *iGuard®* supports both recording on separate hard discs as well as hard disc partitions. We recommend, however, a physical separation of the operating system and the application from the recorded video data, i.e. the recording on physically separated hard discs. The directory structure and data file names are pre-set and cannot be changed.
- Using network disc drives
  Network disc drives also appear on the list of the available disc drives for recording. If a network disc drive is selected for recording, that drive is given priority over local disc drives. Local disc drives are then only used for recording if all network disc drives have failed. Therefore, if at least one network disc drive has been selected, local disc drives that have been enabled

for recording are only used as backup drives.
As soon as failed network drives are available again, the system switches the recording drive from a local drive to a network disc drive when the next file change takes place.
If using network disc drives, make sure that they are sufficiently fast and check for adequate broad-band capability of the network connection in order to ensure recording and replay as well as other disc access (e.g. deleting old recordings) within the required time.
We recommend connecting network disc drives via own LAN card and own sub-network. This ensures that access to the network drives is not handicapped by other network traffic such as access from *iGuard® RemoteView*.

Network disc drives have to be mapped, i.e. access to a network disc drive is only possible via a disc drive letter and not via an share name.

- Use hard-disc capacity to maximum
  In order to ensure the stability of the system, 15 % of the hard-disc capacity is reserved for the resources required by the operating system. This restriction can be deactivated to allow the hard-disc capacity to be used to its maximum. This, however, can result in the system becoming unstable and unusable.

This option is not set as standard in the case of new installations. If updating an older installation, this option is activated following the update and has to be deactivated by the user.

We do not recommend activating this option.

Application start/stop

- Start with password query
  It is possible, in this dialog field, to stipulate whether authorisation of the users is or is not required to start *iGuard®*.
- Automatic recording on start
  In addition it is specified whether *iGuard®* begins immediately with the recording or whether the recording of the camera pictures must be started manually. Manual control is carried out in display mode via the corresponding buttons, *Rec* or *Stop* on the symbol bar or via the **menu** *Action → Start/Stop Recording* (see *3.2.3 Menus in display mode* and *3.2.4 Symbol bar in display mode*).
- Shutdown and exit
  If this option is marked, *iGuard®* shuts down the operating system when the application is terminated.

Auto Logout
With the activation of the option *Auto Logout* an automatic logout takes place at longer inactivity of the user. The period of time for the inactivity must also set within the range of 1 ... 300 minutes.
An imminent auto-logout is indicated for about 1 minute by a flashing lock symbol in the status bar. If a user action takes place during this period, the auto logout is extended and the symbol does not flash anymore.

If *iGuard®* currently is operated in the *playback mode* the auto logout function is active, the playback then will be ended and the user will be logged out because of inactivity. There will be no auto logout when the user currently operate *iGuard®* in the configuration mode.

System Name
The system name should be selected so that the system can be identified clearly if using remote access, e.g. location of the system.

Record status display
With the *Record status display* option a symbol and text overlay into the live image (DISP, REC, DET, PTZ) is possible. The following options are available:
- Off
- Symbol
- Text and Symbol

Recording
- Data compression
  iGuard® has the possibility to set the storage requirements. This is made by the field *Data compression*. The data compression size is, at the same time, a measure for the image quality. The greater the compression the poorer becomes the picture quality.
  The definition of the storage requirement per image has to be accurately considered, because the two most important criterions
  ♦ resolution/compression of the images
  ♦ the existing hard disc capacity
  should be optimised. Compression settings can be carried out step less in the range of 10 ... 40 kB/image (normal resolution), 20 ... 80 kB/image (high resolution) or 40 … 160 kB/image (max. resolution).
- Normal/high/max. resolution
  Image size and resolution (pixel) are in direct linear relationship to each other. This is why the compression stage always shows a value that is dependent on the selected resolution. If the resolution is increased with adjusted compression, the value of the compression rises likewise

  The set resolution always applies for all analogue cameras. The resolution

of the network cameras must be set individually (see 3.3.3 *Configuration of the LAN cameras*).

The possible *maximum resolution* (768x576 pixel) depends strongly on the main board used.

Warnings

- Send E-Mail/Send SMS
  With *Send E-Mail* and/or *Send SMS* an e-mail or SMS can be sent in case of a fault (e.g. camera missing). The respective sending function must be set (see 3.3.10 *Configuration of E-Mail/SMS messages*).

Warnings will only be sent to a main user.

- Alarm forwarding
  There is the possibility of carrying out a connection to a *iGuard® RemoteView* client in the event of a fault. The latter then displays the fault message.

Display Mode

- Switch camera on video monitor every
  If an analogue video monitor is connected parallel to the VGA monitor it is only possible to display one camera on this at a time. In the field *Switch camera on video monitor every* the time interval after which the system will switch to the next camera can be entered. A camera will only be displayed if it is activated in the *Configuration of the cameras* (cp. 3.3.10 *Configuration of E-Mail/SMS messages*).
- Show event on monitor at least
  Timing for displaying the images on the monitor if a motion or an alarm is detected.
- Switch camera group every
  A *camera group* is a group of cameras which can be displayed simultaneously on the VGA screen. A quad-split display, for example, shows four cameras. If, however, a total of 10 cameras are connected, there are three camera groups whereby the last group contains only two cameras. These three camera groups are displayed in series when the automatic camera group change is activated in the display mode. The required group change interval time in the field for the change of the camera group

You can select switching times of between 2 and 600 seconds for these settings.

Language
This is where the language is defined in which *iGuard®* is to operate. *iGuard®* finds all installed languages and lists them in a combo box. Other languages can be installed at any time. A specific language can be selected or the automatic language selection can be used. If using the automatic language selection option, *iGuard®* starts in the language specified as local language. The automatic option usually provides the best results and that is why it is also set as default.
If on another language is to be used than those in the operating system defined, it is to be noted that standard dialogs (e.g. *File → Open, File → Save*) or standard interfaces ("Help", "Abort", "OK") still appear in the language which is set in the operating system. The reason for this is that these elements or dialogs are displayed by the operating system itself, i.e. they cannot be influenced by *iGuard®*.

Test options

- Enable alarm simulation
  Manual alarms can be triggered for test purposes using this option. An alarm simulation dialog is provided in *iGuard®* for this purpose that can be called up within the display mode in the **menu** *Action → Simulate alarm*.
  The call of this dialog is only after activation of the option *Enable alarm simulation* possible. The reason for this is that the *iGuard®* operator should not have the possibility to trigger alarms manually.
  For enabling the alarm-simulation-dialog configuration rights are necessary. Enabling this dialog can only be cancelled again in the configuration mode.
- Display frame rate
  By using this option this option it is possible to indicate the frame rate for the various different cameras within the pictures. For activating the option *Display frame rate* the Configuration authorisation is necessary in each case.
  The function is according to standard deactivated after logging in.
  This function serves for control of the frame rate, which are calculated with the configuration of the recording for each camera (see 3.3.8 *Configuration of the recording*). The Display should agree approximately with the actual displayed frame rate.

Figure 39: Display frame rate

When the function is activated, the frame rate is being displayed within the picture from the corresponding camera, but in contrast to the camera name or the date and time it is not saved. The frame rate does not immediately appear within the camera picture, but only does so after 10 pictures have been recorded, as the value can only then be calculated. For a slow frame rate this may take some time.

- Marking movements
  This option makes possible it to mark the focal point of an image change with a cross as overlay in the live images. This is not stored in contrast to the name of the camera or the date and the time.
  For users, there are no changes in the configuration of motion detection. In the configuration dialog of the live image, the areas that have changed are marked with a surrounding rectangle (no cross). As only rectangles are overlaid, the surrounding area is larger than the area that has actually changed. Several crosses or rectangles are overlaid if several areas change.

PTZ-Timeout
The PTZ Timeout affects the PTZ control of a camera. As long as a user a PTZ camera steers this is blocked for other users. If the time interval between two control commands for a camera is greater than the PTZ Timeout configured, the PTZ control of a camera is released.
The timeout applies global to all PTZ cameras and can be adjusted in minute steps (smallest time is 1 minute).

Figure 40: PTZ-Timeout

3.3.2 Configuration of the cameras

This dialog represents the link between the physical camera input on the video capture hardware and a name used within *iGuard®*. During the operation of *iGuard®* only the camera name is used (typically a description of the installation place or the field of vision of the camera).

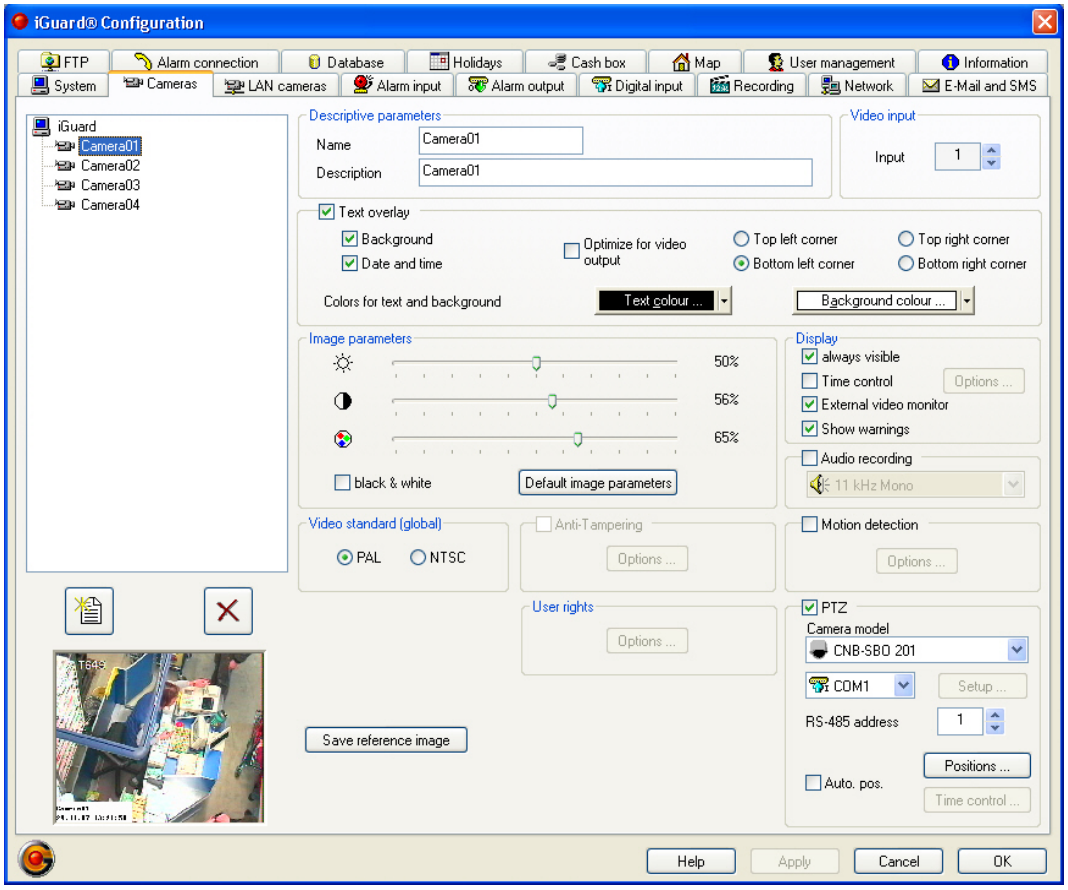


Figure 41: Configuration of the cameras

Tree structure

The available cameras are indicated in a tree structure. Over the button  further cameras can be added to this list, depending upon license. With the button  cameras are removed. After the selection of a camera their configuration data are displayed. Below the buttons the live image of the selected camera is shown.

Descriptive Parameters

- Name
  A name for the camera can be entered here. A maximum length of 16 characters is permitted. The name is being used both in the tree structure as well as being displayed in the camera picture. A precondition for its display in the respective camera picture is that the function has been enabled in the field *Text overlay*.
- Description
  It may be desirable to save additional information besides the camera name. For this purpose, up to 64 characters can be entered in the input field *Description*. This additional information only serves for a more detailed description and for documentation.

Video input

Selection of the physical video input where the respective camera is connected to the video capture hardware.

Text overlay

Here it is specified whether the camera name as well as the time and the date are to be displayed in into the video picture.

- Background
  Activates/deactivates the background of the text field.
- Date and time
  Activates/deactivates the display of date and time.
- Colours for text and background
  The colour of the text background and the text for each connected camera can also be changed. The default setting is black lettering on a white background.
- Top left corner, Bottom left corner, Top right corner, Bottom right corner
  The text is either displayed in one of the four corners of the screen. We recommend putting the text field of each camera image into the same corner, providing no decisive details then would be concealed.

Image parameters

- Brightness, contrast and colour saturation
  These settings can be set separately for each camera in the range of 0 ... 100%. The colour saturation is only advisable in combination with connected colour cameras.
- Default image parameters
  Using this option the settings of the cameras concerned are re-set to standard settings.

- Black & white
  The option *black & white* has to be activated if b/w cameras are connected The value for colour saturation is then set to 0 and the regulator can no longer be moved. As with the other image parameters, this control box can also be activated separately for each camera.

The aforementioned settings can also be carried out using a context menu on the monitor level. This is reached by clicking on the image of the required camera with the right mouse button. Via the **menu** *Settings* → *Image Parameters*, the corresponding dialog opens up.

Display

- Always visible
  The option *always visibly* affects the display of the live pictures. If this option is deactivated no live image is displayed, if no local user is logged in. With activated option however the live pictures of the camera are always displayed.
- Time control
  The *Timer* option activates the *Options* button, which opens the timer dialogue. It can be used to control the visibility of the live images of a camera. Timer control relates only to the display of live images. Functionalities, such as recording, motion detection etc. are not affected.

Marking the time

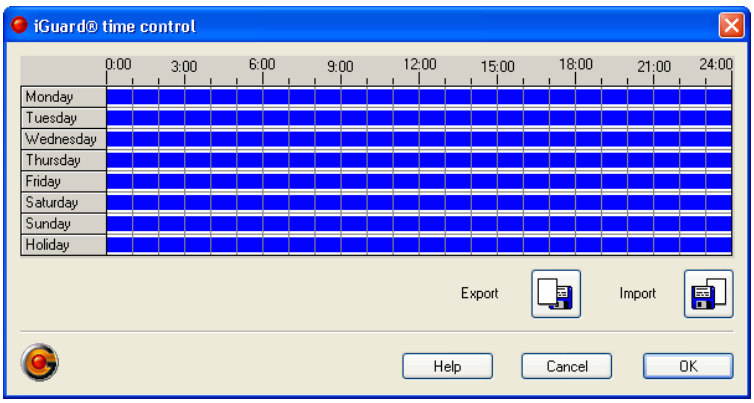


Figure 42: Time control – marking the time

- ♦ Left mouse button
  Active times (blue) are set.
- ♦ Right mouse button
  Active times (white) are deleted. For the definition of the times the mouse button can be pressed and pulled with the mouse.

- ♦ Double click in a field with the left mouse button
  The field is marked totally. A field covers the period 1 hour and is divided into 4 parts a 15 minutes. Thus only time steps from 15 minutes are possible.
- ♦ Double click in a field with the right mouse button
  The marking of the complete field is deleted.
- ♦ Click on a weekday with the left mouse button
  The complete day is marked.
- ♦ Click on a weekday with the right mouse button
  The marking of the complete day is deleted
- ♦ Click in the field over the weekdays
  All entries set (link mouse button) or deleted (right mouse button)
- ♦ Click at the top of a column
  The complete hour is set active (left mouse button)/inactive (right mouse button) on all days.

- External video monitor
  For each camera it is specified whether this is to be displayed on an analogue video monitor. In some cases it may be desirable that the operators does not all recorded cameras get displayed on the screen. For instance, if the cameras are used to record thefts committed by the staff. The pictures of cameras used for such purposes are recorded, but are usually not displayed on a monitor.
- Show warnings
  This option allows you to selectively activate/deactivate warnings for each camera.

Audio recording

A condition for an audio admission is a compatible sound map and the correctly installed drivers of them. The sound card must support the selected sampling rate and the audio mixer must be set correctly via the operating system so that the recording works (recording level, selection of the correct input, e.g. line in or microphone in).

Supported functions:

- Recording in mono and stereo with different sampling rates. The audio input can be assigned only to one camera.
- Synchronous playing with local playback
- Setting playback volume

iGuard® does not install any drivers for any sound cards. The *iGuard®* CD does not include any drivers either. The audio section of our *FALCON* cards cannot be used.

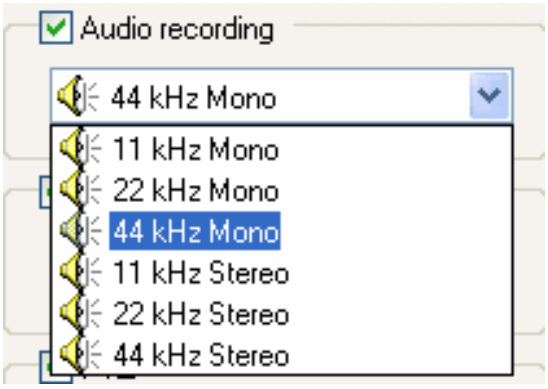


Figure 43: Audio recording settings

Video standard (global)

Figure 44: Choice of the video mode (global)

Video mode PAL/NTSC (50 Hz/60 Hz). In the European market almost exclusively the PAL video standard is used. The NTSC standard in connection with NTSC cameras is intended for the American and Asiatic market.

The choice of video mode (PAL or NTSC) is carried out globally for all cameras. It is not possible to use a mixture of PAL and NTSC cameras. Settings are carried out during configuration of the camera.

Sabotage detection

Configuration of sabotage detection is not possible if using PTZ cameras. For this reason, the configuration options sabotage detection and pan/tilt/zoom control cancel each other out.

Figure 45: Sabotage detection with PTZ cameras

Configuration of sabotage detection is carried out using a separate dialogue. This is opened after activating sabotage detection using the *Options...* button.

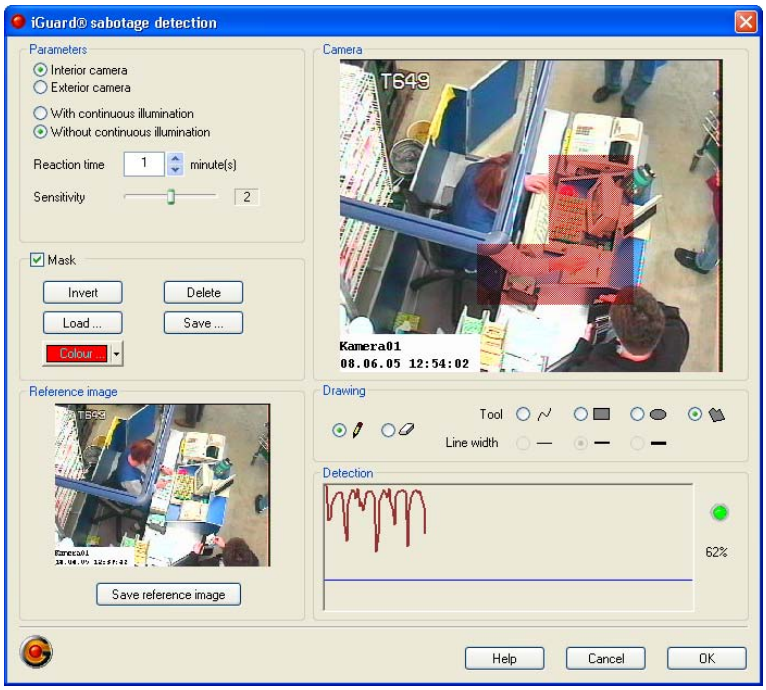


Figure 46: Configuration of sabotage detection

- Parameters
  iGuard® distinguishes between the following camera and illumination types:
  - ♦ Indoor cameras
  - ♦ Outdoor cameras
  - ♦ Continuous illumination
  - ♦ No continuous illumination

  Sabotage by obscuring cannot be detected when using a camera without continuous illumination, as the image may be darkened in normal operation, e.g. when artificial illumination is extinguished.
  The difference between indoor and outdoor cameras is mainly that with indoor cameras lighting conditions may change abruptly (artificial light), whereas with outdoor cameras other effects may be caused by weather conditions (e.g. snow, rain, wind).
  - ♦ Reaction time
    An important setting is the choice of reaction time, which can be set to between 1 and 360 minutes. A sabotage alarm is raised only after the response time has elapsed.
    To avoid possible false alarms, the recording situation must always be considered when setting a reaction time.
    If, for example, large parts of the image are suddenly covered by a parked vehicle, this may trigger a sabotage alarm. If, on the other hand, it can be expected that the vehicle will only be there for a certain time (loading zone, max. 20 minutes), false alarms can be avoided by choosing the right reaction time (e.g. only after 20 minutes). Of course, actual sabotage is then also only signalled after the reaction time has elapsed.

- ♦ Sensitivity
  Sensitivity can be set in 3 levels, where the level 2 represents the normal status. Sensitivity should be reduced if relatively large objects, taking up more than 15% of the total image and causing great differences in contrast, may change within the image during normal operation.

- Mask
  As in motion detection, masks can be used to exclude areas of the image from monitoring. All areas masked in colour are evaluated in sabotage recognition.
  When selecting masks, the following points should be considered:
  - ♦ Sky should always be masked.
  - ♦ Areas in which a lot of movement occurs should be masked.
  - ♦ Areas that are partly illuminated by bright light sources should be masked. This particularly applies to sources of light that are controlled, for example, by motion detectors.
  - ♦ The masked area should not exceed 50% of the entire image.
- Reference image
  A reference image saved at a certain time is displayed in the configuration dialogue. The reference image is not used for sabotage recognition. It merely serves to help the user to manually compare actual and target camera position. Using the button *Save reference image* the current live image of the selected camera is stored as reference image. An existing reference image will be overwritten (see also *Show reference image* in chapter *3.2.8 Pop-up Menu in the Display Window*).
- Drawing
  This field provides tools for creating/editing the mask. With the two left options it is possible to use the available tools to create or delete masks or parts of masks.
- Detection
  This diagram visualises the sabotage recognition. The lower horizontal line represents the sensitivity and can be adjusted through the *Sensitivity* parameter. Sabotage is recognised as soon as the diagram line falls below the sensitivity line.

Motion detection 

Activate or deactivating a motion detection on each camera (using the camera as a video sensor). A camera that has been activated as a video sensor camera is being marked with the symbol  within the tree structure of the system configuration. After activating motion detection the configuration takes place in a own dialog, which is to be opened over the *Options* button.

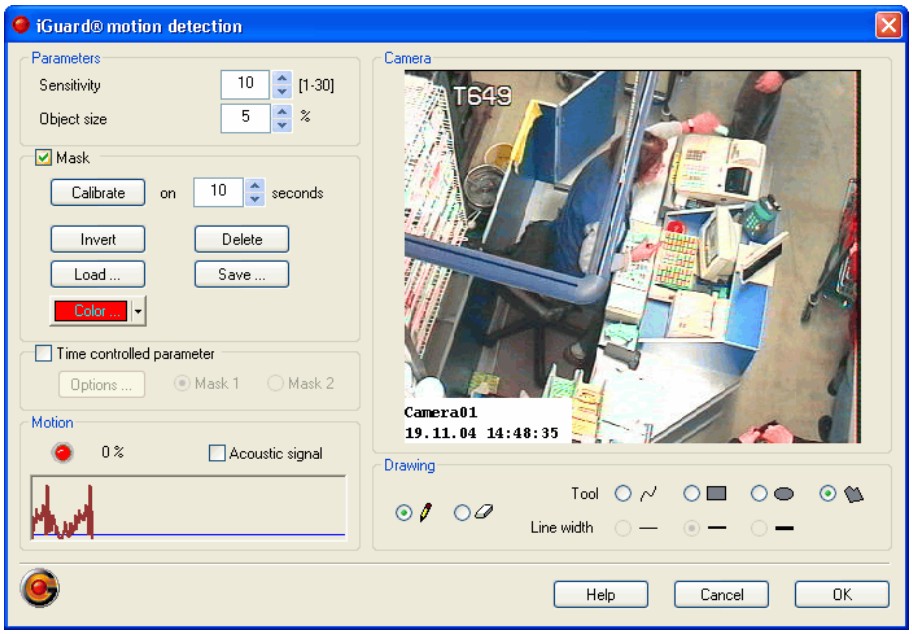


Figure 47: Configuration dialog for the motion detection

- Parameters
  Over the input fields *Sensitivity* and *Object size* the motion detection is defined. The object size refers to the percentage size in relationship to the overall image or the stipulated mask (image section).
  The system reacts more sensitively to movements the lower the threshold of the sensitivity and the lower the choice of object size.
- Mask
  In the field *Mask* is selected whether the evaluation specified above is to be accomplished for motion detection only within a defined mask, or whether the motion detection is to be accomplished over the entire picture.
  After activating the mask use masks can be created manually or automatically.
  - Calibrate
    The automatic creation of masks is activated with the button *Calibrate*. Automatic generation means that within the range of the concerned camera image a mask is drawn, in which movements in accordance with the adjusted parameters are detected. This happens for a certain duration, which will be indicated in seconds right beside the button *Calibrate*. For example: if exactly the visible section of a traffic route is to be specified for a certain camera as mask, then the mask would be the closer, the longer the calibration time would be defined, because in a larger period more vehicles, speaks more moved elements are registered and thus than as mask put on.

Selecting automatic mask generation deletes the previously defined mask.

- ♦ Invert
  With the *Invert* button the function of previously defined masks can be inverted (areas which had previously been excluded from motion detection are now relevant for motion detection while formerly relevant areas are now excluded from motion detection).
- ♦ Load/Save
  Masks can be loaded and stored over the buttons *Load* and *Save*.
- ♦ Colour
  Setting of the colour of the mask.

Defined masks are only displayed in this dialog, otherwise they are not visible.

- Time control parameters
  The dialogue for setting the timing is opened over the button *Options*. Switching over between two motion parameter datasets (mask, sensitivity, object size) is possible (e.g. day/night, weekend operation) using a time switch. All the blue marked areas in the *Time switch* dialog relate to configuration *Mask 1* and all white marked areas to *Mask 2*. *Mask 1* is used if no time switch has been activated.
  - ♦ Marking the times
    See *Marking the time*
  - ♦ Export/Import
    Via corresponding buttons there's an export/import possibility for the time control.
- Motion
  The field *Motion* serves for the support during the calibration of the video sensor. A detected movement is displayed by a red LED. Furthermore a small diagram indicates, how many pixels (in percent) over the time have been changed. They are applied over a time axis. A horizontal blue line marks the threshold value of the set object size. This analogue display allows easy assessment of the action of the video sensor system (movement, object size, time).
  Optional an acoustic signal can also be activated in addition to the display.
- Drawing
  The field *Drawing* is used for selecting tools for the above mentioned manual mask definitions. After setting the *Mask* flag, a mask can be generated manually with the help of a pen and the definition of different forms (the free-hand line, rectangle, ellipse and polygon).
  The strength of the line can be varied if using the free-hand line. Areas can be erased manually using the rubber.
  The buttons OK and Cancel close the motion detection dialog..

Camera type (optional)
The selection field *Camera type* is available if the optional banking mode has been activated.

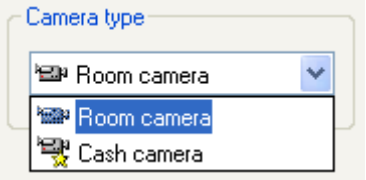


Figure 48: Selection of the camera type

Cameras of the following type can be assigned using this field:

- Room camera (default)
- Cash camera
  With this type of camera special requirements in connection with an alarm contact with hold-up priority apply. These refer e.g. to the minimum pre-trigger duration, the post-trigger duration and the minimum frame rates. For ring recording, this must be at least 1 frame per second and for raid recording at least 2 frames per second. The prescribed minimum frame rates cannot be undercut when configuring a camera of this type.

Cash cameras must not have any PTZ control.

User rights
With the button *user rights* another dialogue window is opened. In this certain rights can be assigned to the camera (see also *3.3.16 User management*).

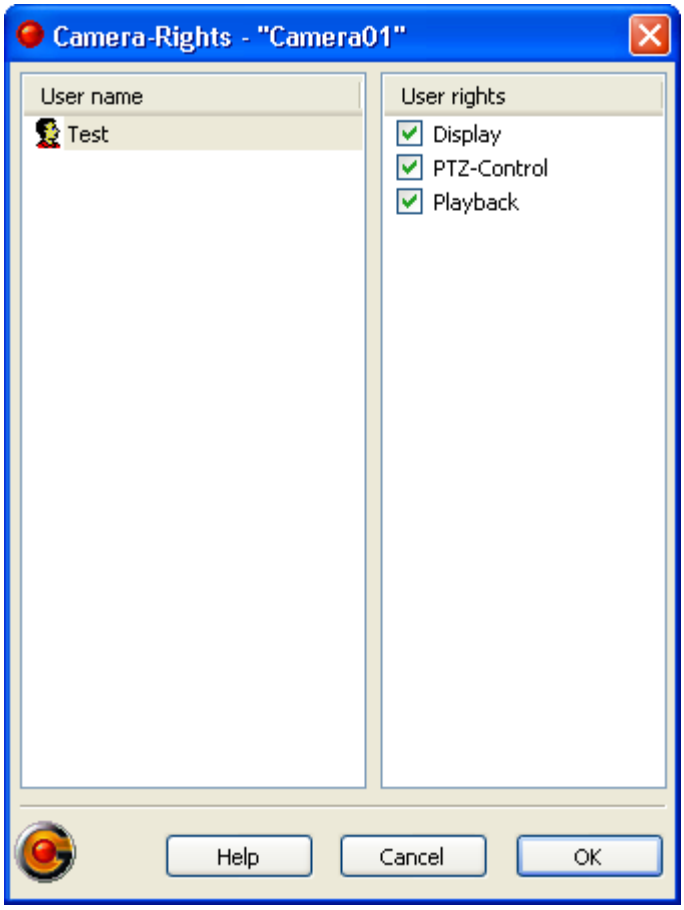


Figure 49: Camera rights

In the column *user name* of this dialogue all users are displayed and in the column *user rights* the camera-specific rights. The selected rights are assigned to the camera displayed in the header.

PTZ

The *PTZ* option must be switched on to configure the parameters for the operation of the PTZ cameras. The following PTZ functions are currently supported:

- Pan left and right
- Tilt up and down (tilt)
- Zoom in and out
- Focus
- Save set positions (32 positions)
- Automatic drive to the positions
- Event controlled drive to saved positions (patrol)
- Speed controlled drive to positions (optional, if supported by the camera)
- Remote control of the camera via *iGuard® RemoteView*
- Operation of the configuration menus

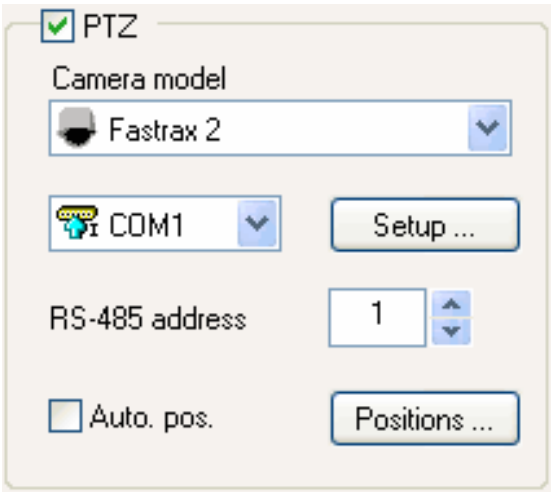


Figure 50: Configuration of the serial PTZ camera control

- Definition of camera model, serial interface and RS-485 address
  The appropriate camera protocol must be selected in the list *Camera model*.
  For the printing of the manual the following cameras are supported:

Manufacturer	Type	Baudrate
CNB Technology	SBO-201	2400
Dedicated Micros	Dennard 2060	9600
Eneo	EDC-141E	9600
	EDC-143E	9600
	EDC-144E	9600
Ernitec	BDR-510	2400
Ganz	ZC-S123P	38400
Panasonic	WV-CS570	19200
	WV-CS850	19200
	WV-CS950	19200
Pelco	Spectra III Se	2400 *
Samsung	SCC-643(P)	9600

Sanyo	VCC9300	2400
Sensomatic	SpeedDome	4800
	SpeedDome Ultra I	4800
Sony	Evi-D30/D70	9600
TRC	TP-D7720	2400
Global protocols		
Fastrax	Fastrax 2	9600
	Fastrax 2E	9600
Pelco-D	Spectra III Se	2400 *

**Versions older than V2.60 SP1 have 4800 Baud*

Further cameras can be connected rapidly if the camera protocol is known and a camera is made available by the customer for the duration of the integration. Because different cameras from one manufacturer possibly use the same protocol, it is possible that the protocols defined so far cover more cameras than are shown on the list. Thus for example many cameras support beside the own one also the "Pelco D"-protocol.
The administrator must select the correct serial interface (COM port) to which the camera is connected. It is also important to select the right RS-485 address. The address chosen must coincide with the address set for the camera.
If necessary, the camera may have to be released by adjusting some DIP switches or by configuration using a camera's own setup menu for control via a serial protocol. We must refer to the camera's manufacturer or manual in this case.

- Setup PTZ control
  A further dialog opens using the *Setup ...* button.

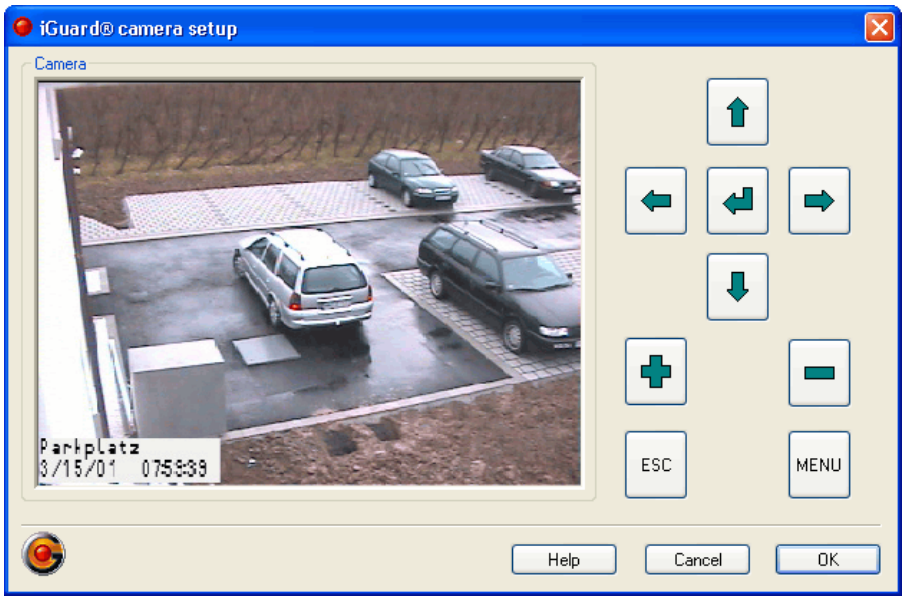


Figure 51: Setup PTZ control

At the same time, the camera's set-up menu is opened and displayed in the live image. This set-up menu is camera-related. The meaning of the set-up menu has to be requested from the manufacturer of the camera or can be found in the camera's manual.
The buttons UP, DOWN, LEFT, RIGHT, ENTER, +, -, ESC, SPEC und MENU are used for controlling the camera-related menus. Because this control is camera-related, it is possible that the marking of the button may not be perfect depending on the type of camera.
The build-up of this dialog is designed in such a way as to be able to operate all cameras or their setup menu. This is why the dialog does not necessarily match the camera being used with regard to design, construction and marking.
On some cameras, the menu can be terminated from the setup menu. The dialog does not close during this because the setup menu of the application does not provide any information.

- Positions
  The *Positions* button opens the dialogue for saving camera positions.
  Up to 32 set positions (depending on camera) can be stored for a pan-tilt camera. The positions are stored in the camera.

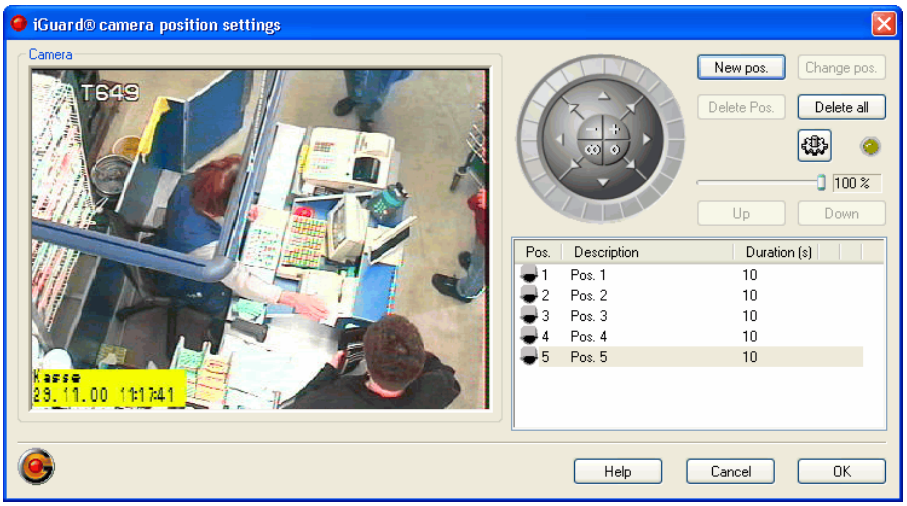


Figure 52: Saving camera positions

Cameras are controlled by the graphic control element, the mouse, the keyboard or a joystick.
By one click on the camera symbol (column 1) on the list the position can be started directly.

- ♦ New pos.
  A new position is saved after driving to a camera position. For each position a description of the position can be specified. In addition the remaining time for each position can also be specified within the range of 1 ... 360 seconds.
- ♦ Change pos.
  With the button *Change pos.* a different camera position is to be stored for a stored position marked on the list.
- ♦ Delete pos.
  The selected position is deleted.
- ♦ Delete all
  All stored positions are deleted.
- ♦ Automatic mode
  Over the button the test mode for the patrol is started.
- ♦ Status-LED
  The status LED indicates that a command is sent to the camera.
- ♦ Slide regulator
  To aid more precise positioning, the maximum speed can be set using the red marking on the operating control if the camera supports this functionality. The speed setting serves only to accurately position the camera. The speed setting has no effect on automatic mode.
- ♦ Up/down
  With the help of the buttons up and down the position of the selected camera can be shifted a position upwards or downwards.

- Auto. Pos.
  This option starts the automatic mode (patrol). In the automatic mode the positions are started in the given order. The automatic mode can be deacti-

vated temporarily by a user in the display mode. As soon as the user logs itself out of *iGuard*®, the configured automatic mode again is started.

- Time control
  The *Time control* button is activated with the function *Auto. Pos.* With the time control the active time of the function *Auto. Pos.* is given (see also *Marking the time*). As soon as the time control is active, the camera starts with their patrol. If the time control becomes inactive, the camera drives to the first position and stops there. In this condition it is not possible to start the automatic mode manually.
  During automatic mode manual starting of the saved positions is possible.

Save reference image
Using the button *Save reference image* the current live image of the selected camera is stored as reference image.

3.3.3 Configuration of the LAN cameras

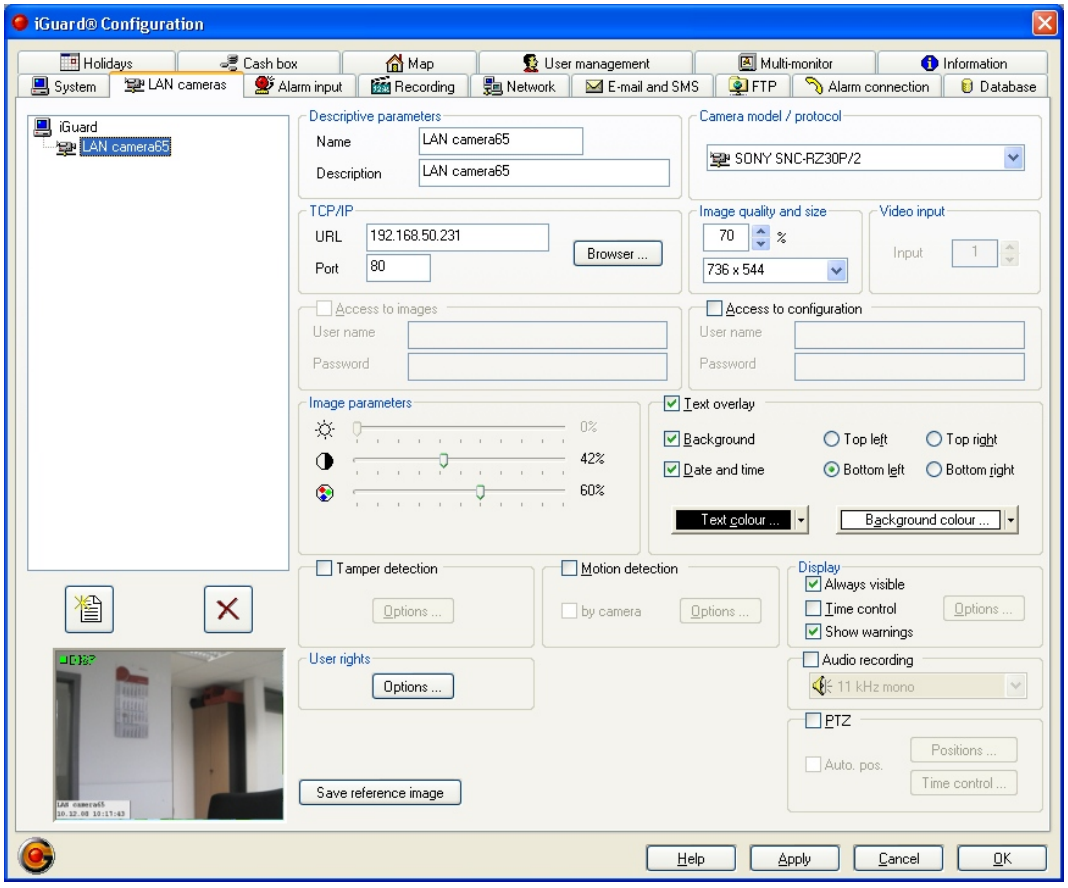


Figure 53: Configuration of the LAN cameras

Tree structure
The available cameras are displayed in a tree structure. Depending on the licence you are using, additional cameras can be added to this list via the button

 . Use the button  to remove cameras. After selecting a camera, its detailed data are displayed. The live image from the selected camera is shown below the buttons.

Descriptive parameters

- Name
  Name of the camera. See also *3.3.2 Configuration of the cameras*.
- Description
  Additional camera information. See also *3.3.2 Configuration of the cameras*.

Camera model/protocol

Selection of the camera model from the list of the available cameras. *iGuard*® currently supports the following cameras and manufacturers:

Manufacturer	Type
Arecont Vision	2100 3130 Day 3130 Night
Axis	Generic HTTP Interface v2.0 Generic HTTP Interface v1.0 205 206M 206/W 207MW 209 FD 210 211 212 PTZ 213 PTZ 216 MFD 216 FD 221 223M 231D+ 232D+ 233D 240Q 241S 241Q
CBC	MP2A MP3DN Day MP3DN Night
Eneo	ENC-1003L
iQinVision	IQ501 IQ603 IQ752
JVC	VN-C10U VN-C30U VN-C625U

	VN-C655U
Lumenera	LE175C LE275C LE375C
Mobotix	D12 M1 M10M M10D-Night M12M M12D-Night M22M-SecureCS
Panasonic	KX-HCM-280 WV-NM100/G WV-NP244 WV-NP472 WV-NS202 WV-NS320 WV-NW470
PIEPER	FK-CM-4713-2-IQ-R5
PIXORD	205
Samsung	SNC-L200
Security Center	TV7214
Siemens	TelScan CCIS1337-LP CFVA-IP CVVA-IP
Sony	Generic HTTP Interface SNC-CS11 SNC-CS3P SNC-DF40P SNC-M1/W SNC-M3/W SNC-P1 SNC-P5 SNC-RZ25P SNC-RZ30P SNC-Z20P SNT-V704
SSAM	VINWPI 2051
Vivotek	MJPEG Modelle PZ6122 VS2402

TCP/IP

- Network address of the camera
- For the access over LAN the TCP/IP port must be indicated, under which the network camera is attainable.

- Browser
  As some network cameras (e.g. Mobotix) possess a very large own function range, which cannot be shown completely by *iGuard*®, insists the possibility of opening a browser window directly out of this configuration dialog over the button *Browser* and of accessing thus on the HTML sides of the camera.

Image quality/Image size

- Image quality
  Adjustment of the image quality within the range of 0... 100%. The more highly the image quality is selected, the smaller the picture is compressed.

High image noise, twilight or darkness can result in the camera's buffer memory being too small for high-quality images. This may cause camera failure in some network cameras.
For more information please contact your camera supplier.

- Image size
  In this field you can set the image size at which the camera images are to be recorded. The available image sizes are limited by the technical capabilities of the camera you are using.

For the transmission of the image data a fast connection is necessary. An ISDN/DSL connection is not sufficient.

Video input

Selection of the physical video unit with a camera with more as one lens or with a web server with more than one input.

Access to images/Access to configuration

The options *Access to images* and *Access to configuration* are camera-specific peculiarities and are not provided from all LAN camera models. In order to be able to access the configuration options of the camera, *iGuard*® must register itself at the camera with user name and password. The access dates are deposited directly in the camera.

Image parameters

- Brightness, contrast and colour saturation
  These settings can be set separately for each camera within the range of 0 ... 100%. The colour saturation is only advisable in combination with connected colour cameras..
  See also *3.3.2 Configuration of the cameras*.

Text overlay
See *3.3.2 Configuration of the cameras*.

Anti-Tampering
Sabotage detection is possible with network cameras, too. The configuration of the sabotage detection runs as with the analogue cameras (see *3.3.2 Configuration of the cameras*.

Motion detection
Motion detection is also possible with network cameras. When the option *by camera* is activated, motion detection is performed by the network camera. In this case, motion detection can be set up like the configuration of the network alarm inputs (see Network section in Chapter *3.3.4 Configuration of the alarm sensors (detectors)*).
When the option *by camera* is deactivated, motion detection is performed by *iGuard*®. In this case, motion detection can be configured as for analogue cameras (see *3.3.2 Configuration of the cameras)*.

Display
See *3.3.2 Configuration of the cameras* (Exception: external video monitor).

User rights
See *3.3.2 Configuration of the cameras*.

Audio recording
As with analogue cameras, sound can be recorded for LAN cameras via the audio input of the sound card (see also *3.3.2 Configuration of the cameras*).
For some camera models, *iGuard*® supports audio transmission as a data stream via the network connection. The audio stream belonging to each camera can be recorded for multiple LAN cameras simultaneously. For cameras supported by *iGuard*, the entry *Camera* for feeding in an audio stream via the network appears additionally in the *Audio recording* selection list.
Audio recording is currently supported in *iGuard*® for Axis cameras that are activated via VAPIX® API. G.711 (µ-law) and G.726 with 32 kBit/s are available as recording codecs.

Camera type
See *3.3.2 Configuration of the cameras*.

Exposure window (wiht Mobotix cameras only)
Camera-specific exposure control with Mobotix cameras.

PTZ
See *3.3.2 Configuration of the cameras*.

Save reference image
Using the button *Safe reference image* the current live image of the selected camera is stored as reference picture. (see *3.3.2 Configuration of the cameras*.

3.3.4 Configuration of the alarm sensors (detectors)

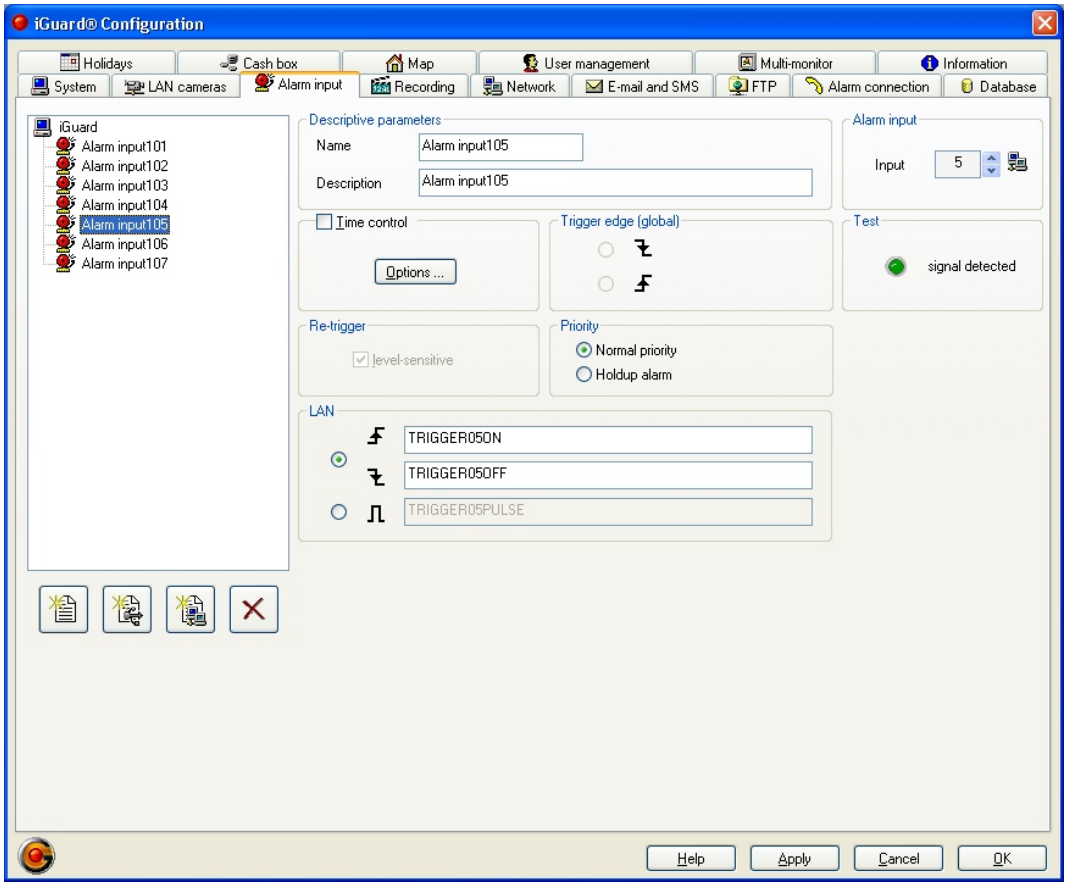


Figure 54: Configuration of the alarm sensors (detectors)

Tree structure
The available alarm inputs are listed in a tree structure. With the following buttons alarm inputs can be added to this list.

- Add alarm input connected to a frame grabber
- Add USB alarm input
- Add LAN alarm input

With the button alarm inputs are removed. After the selection of an alarm input the configuration data are displayed.

Descriptive parameters

- Name
  A name for the alarm sensor can be entered here. The names of the alarm sensors may have a maximum length of 16 characters and will be displayed in the tree structure. Alarm inputs connected to a frame grabber are allocated consecutive numbers 001…004, USB alarm inputs 065…100 and network alarm inputs 101…132.

- Description
  It may be desirable to save additional information to just the alarm sensor names. A total of 64 characters are available for this in the provided input field *Description*.

Alarm Input
In this field an actual existing physical trigger input of the video capture hardware is assigned to a selected alarm input. Available are:
- 4 alarm inputs at *FALCONplus* and *FALCONquattro*
- alarm inputs at *DORADOquattro*

If you are using USB input modules, the selected alarm input can also be assigned to an input on the USB module. In this case the USB symbol appears next to the assigned input in the display. For network alarm inputs, the network symbol appears next to the assigned input in the display.

Time control
Each alarm sensor can be activated over the definition of a timing within certain times. Outside of the fixed periods the alarm sensor is deactivated. Using the button *options* the dialog for the time control is opened (see *Marking the time* in *3.3.2 Configuration of the cameras*).

Switching edge (global)
The switching edge set here for the trigger inputs (alarm sensors) is valid for all connected alarm sensors and can consequently be changed globally. The switch edge defines whether the alarm is normally loaded with a voltage signal and drops to 0 volt in the event of an alarm (high → low) or vice versa (low → high).
Here we recommend looking up information concerning the connections of the respective hardware in the corresponding chapters of the installation manual.

Test
In the *Test* field it is possible to check whether the alarm source has been properly connected and is functioning. In the case of an alarm being triggered the little light will light up green for a brief period. This function is suitable for test purposes or when connecting a new alarm source.

Re-Trigger level sensitive
If a signal alarm is to be retained, the re-trigger of the alarm recording configuration can be set to *level control* (= active / non-active). In this case, recording is continued for as long as the level of the alarm is active. This function can be activated in particular with make and break contacts (NO and NC contacts) as well as limit switches because with these alarms recording is not only required to be "triggered" at a flank but also during a situation (level).

Priority
The following priorities are available for the configuration of the alarm sensor:
- Normal – symbol colour: red
- Suspicion (only with activated bank mode) – symbol colour: purple
- Hold-up – symbol colour: orange

From the listing it results that

- an alarm with hold-up priority ends current recording of an alarm with standard priority immediately. Motion recordings are also interrupted immediately. The alarm with raid priority, however, cannot be interrupted by a standard priority alarm or a motion.
- an alarm with suspicion priority ends an alarm with standard priority and is terminated by an alarm with hold-up priority.
- an alarm with standard priority is terminated immediately by an alarm with suspicion priority or an alarm with hold-up priority.

Various recording parameters are available for the configuration of the recording (cf. *3.3.8 Configuration of the recording*).

Alarm sensors with hold up or suspicion priority (optional banking mode) cannot be time controlled.

Network

Some network cameras can send definable messages via the SMTP or HTTP/TCP protocols. *iGuard*® responds to the text in the text fields. If this corresponds to the incoming command, an alarm signal is triggered.
To activate the inputs, *iGuard*® receives messages on the preset ports 13801 (HTTP messages and TCP data) and 13802 (SMTP, i.e. e-mail server). These ports can be changed under *3.3.9 Configuration of the network parameters* in the *Network trigger* section. All commands must be sent in capital letters and without blank spaces.

- Defines the command to activate an input (level set to High). The default command is *TRIGGER**01**ON* for the first input, *TRIGGER**02**ON* for the second input etc. up to *TRIGGER**32**ON*. Other commands can also be defined.
- Defines the command to deactivate an input (level set to Low). The default command is *TRIGGER**01**OFF* for the first input, *TRIGGER**02**OFF* for the second input etc. up to *TRIGGER**32**OFF*. Other commands can also be defined.
- Defines the command to switch an input to pulsative (Low -> High -> Low). The level is set to High for 1 sec. and then back to Low. The default command is *TRIGGER**01**PULSE* for the first input, *TRIGGER**02**PULSE* for the second input etc. up to *TRIGGER**32**PULSE*. Other commands can also be defined.

TCP data is essentially the fastest, while HTTP messages are slightly slower. E-mail messages via SMTP are slower, however not comparable with normal e-mails; the response time for these should also be under 0.5 seconds.

Examples of the configuration of TCP/HTTP and SMTP commands

- Camera type: Axis 233d Message type: TCP data
  In the camera configuration under *Setup → Event Configuration → Event Servers*, click "Add TCP...". Enter the name, IP address and port number 13801 of the iGuard® server here; confirm with OK. Then click "Add triggered..." under *Setup → Event Configuration → Event Types* and enter a name. Set "Triggered by..." to "Input ports", "Input 1" to "Active" and for "Send TCP notification to", select the previously specified server. Under "Message", enter the command defined in *iGuard®* (see above) to activate the input and confirm with OK. Then go back to "Add triggered...", but this time set "Input 1" to "Inactive" and enter the command for deactivating the input under "Message". For further inputs, enter the corresponding message (see above).
- Camera type: Axis 233d Message type: HTTP data
  In the camera configuration under *Setup → Event Configuration → Event Servers*, click "Add HTTP...", enter the name of the iGuard® server, enter http://<iguardip>:13801/ as the URL and confirm with OK. Under "Event types", then select "Send HTTP notification to" and enter the "Message" accordingly as in the example above.

3.3.5 Configuration of the alarm outputs

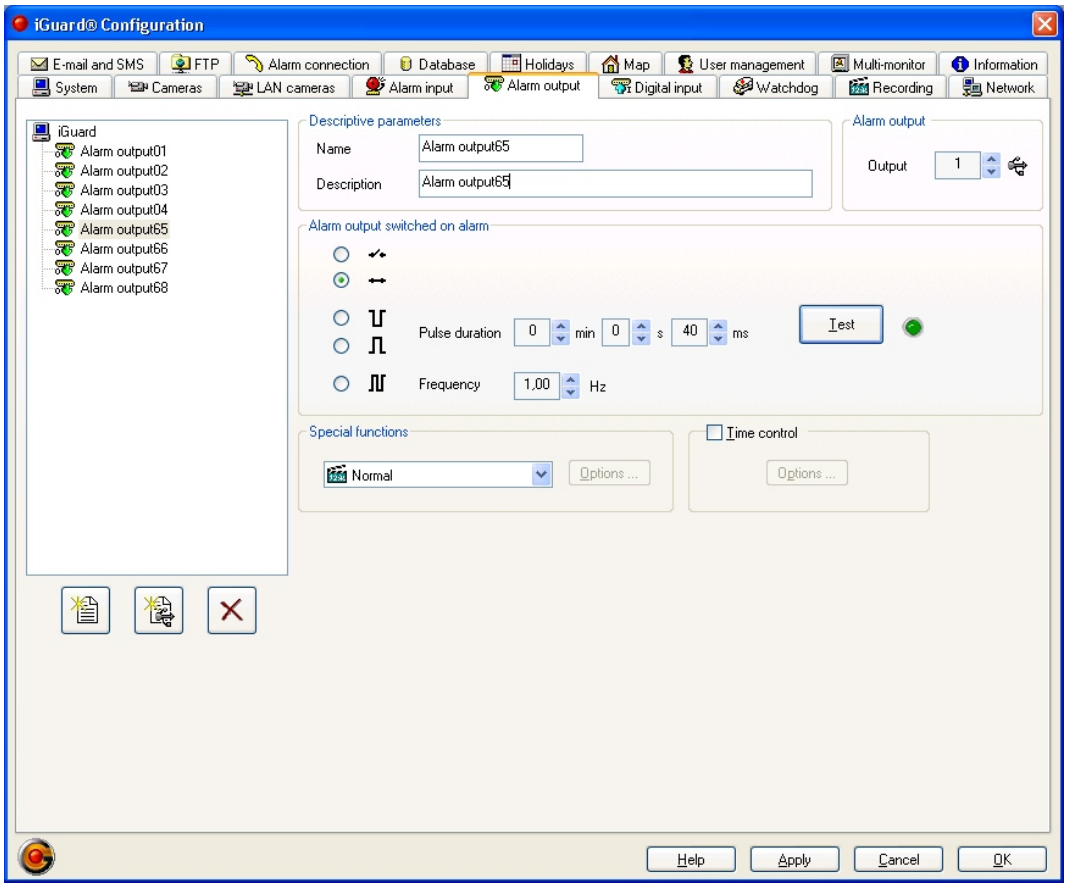


Figure 55: Configuration of the alarm outputs

Tree structure
The available alarm inputs are listed in a tree structure. With the following buttons alarm inputs can be added to this list.

- Add alarm output connected to a frame grabber
- Add USB alarm output

With the button alarm outputs are removed. After the selection of an alarm output the configuration data are displayed.

Descriptive Parameters

- Name
  A name for the alarm output can be entered here. The names of the alarm outputs may have a maximum length of 16 characters and will be displayed in the tree structure.
- Description

It may be desirable to save additional information to just the switch output names. A total of 64 characters are available for this in the provided input field *Description*.

Output line
Use this field to assign a chosen alarm output to an actual existing physical digital output on the video capture hardware. There are 8 switch outputs available. If you are using USB output modules, the selected alarm output can also be assigned to an output on the USB module. In this case the USB symbol .appears on the screen next to the assigned output.

Alarm output switch on alarm
For each switch contact can be defined how to react in the event of activation. The following options are available:

- open switch
- close switch
- switch pulse negative
- switch pulse positive
- Pulse duration
  It is possible to specify pulse duration using the *Pulse duration* field for the outputs that supply a switch pulse. Timing is set separately by minutes, seconds and milliseconds.
- Alternating
  The alarm outputs can be activated/deactivated by an adjustable frequency. With this type of wiring the green test LED is permanently on. It does not indicate the state of the output, but instead that it is active.
- Frequency
  The adjustable frequency range in *Alternating* mode is:

0.01 Hz	...	0.5 Hz:	Step width 0.01 Hz
0.5 Hz	...	1.0 Hz:	Step width 0.1 Hz
1.0 Hz	...	5.0 Hz:	Step width 1.0 Hz

- Test
  Using the button *Test* the functionality of the configured settings in case of an alarm can be tested.

Special functions
An alarm output with a special function is not available for the configuration of the recording. Remote controlled alarm outputs are not concerned.

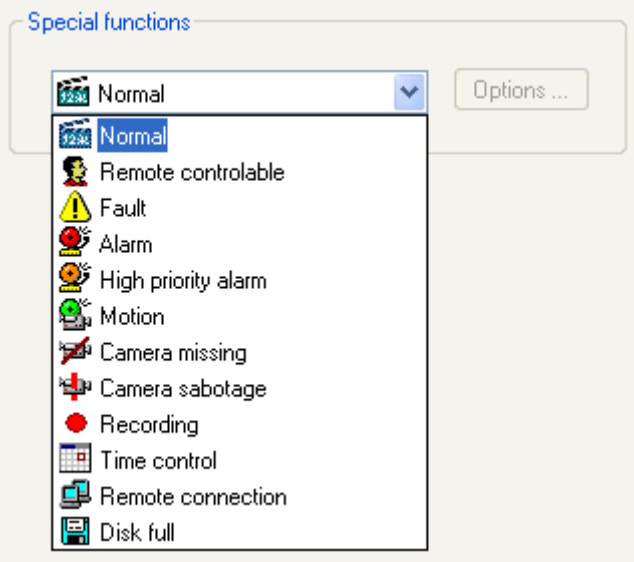


Figure 56: Configuration switch outputs special functions

- Normal
  The switch output is used for recording and does not have any special function.
- Remote controllable
  Like *Normal*, but additional remote-controlled.
  An user with *Remote control* authorisation, can activate appropriately configured switch outputs using the interactive bar in display mode. This shows a list of all switch outputs (see *3.2 Display mode*). Switch outputs which can be remote-controlled are highlighted with a grey surround.

Figure 57: Status indication of the switch outputs

  This bar is also visible in *iGuard® RemoteView*.
  Switch outputs configured with "Pulse positive/ negative" cannot be deactivated as the pulse length was stipulated during configuration and should not be changed manually.
- Error
  The switch output is activated with one of the following faults:
  - UPS (**U**ninterruptible **P**ower **S**upply) indicates a power failure
  - *iGuard®* was not duly terminated (e.g. Watchdog, power failure)
  - Recording could not be started
  - Fatal record error
  - Hard disk is full, record is stopped

  - ♦ Loss of a hard disk
  - ♦ Windows device drivers indicate errors (Event log)
- Alarm
  The switch output is activated as long as an alarm recording is being processed.
- Motion
  The switch output is activated as soon as any camera has detected a movement. It remains active for 1 second. If, within this second, it detects another movement the activation period of the switch output is extended accordingly.
  Camera missing
- Camera sabotage
  The switch output is activated if at least 1 camera signal failed.
- Recording
  The switch output is switched on while a recording is running.
- Time control
  With selection of the option *Time control* the button *Options* is activated. Over these the time control admitted from the camera and alarm sensor configuration opens. While active phases (colour blue) the switch output is activated, otherwise deactivated (colour white).
- Remote-connection
  With this special function, the switch output is activated as soon as at least one connection exists to an *iGuard® RemoteView* client.
- Disk full
  Over the option *Disk full* the alarm output is activated, if the free recording capacity sank under 20% of the available hard disk capacity.

A switch output with a special function is no longer available for the configuration of the recording (cp. *3.3.8 Configuration of the recording*).

Time control
Each switch output can be activated over the definition of a timing within certain times. Outside of the fixed periods the switch output is deactivated. Using the button *options* the dialog for the time control is opened (see *Marking the time* in *3.3.2 Configuration of the cameras*).

3.3.6 Configuration of the digital input

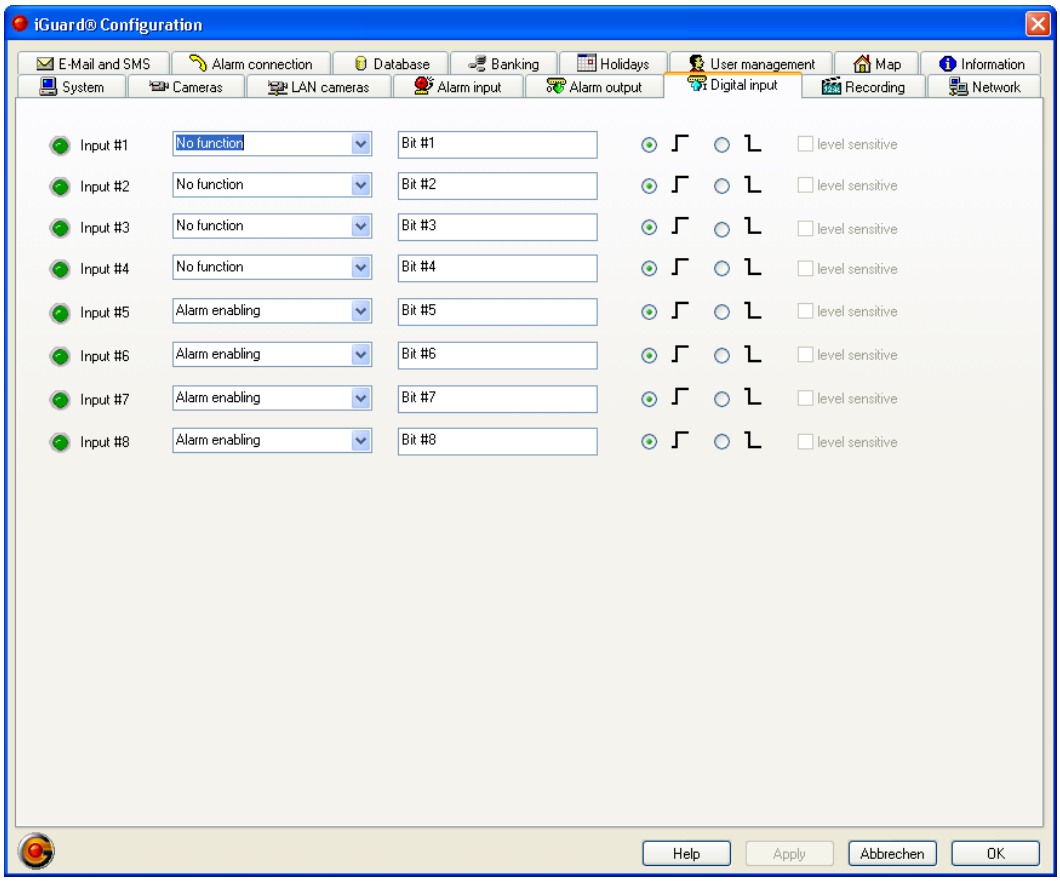


Figure 58: Configuration of the digital input

Each digital input can be assigned one of the special functions:

- Start/Stop recording
  Allows the start/stop of recording from an external signal.
- UPS power failure
  Allows a shutdown of *iGuard®* in case of power failure, if a UPS (that has this feature) has set a signal. In this case *iGuard®* terminates the recording within 60 seconds and the operating system will be shut down.
- Shutdown
  Allows a shutdown by an external signal. In this case *iGuard®* is being closed and the operating system being shut down.
- Next camera
  Allows switching cameras on an external monitor.
- Start/Stop monitor run-through
  Start/stop of the monitor run-through by external signal transmitter.
- Alarm output
  An alarm output to an *iGuard® RemoteView* client can be executed via an external signal (see also *3.3.12 Alarm connection to iGuard® RemoteView (optional)*)

- Alarm enabling
  Alarm enabling can be assigned to a maximum of four digital inputs.
  This function allows recording from the cameras to be controlled depending on the states of the assigned inputs.
  For example, a complete system may only trigger an alarm if it has been activated via an external on/off switch, a light sensor or similar.

You can determine for each input whether it is to respond to a switching edge ((⎍, ⎏) or a voltage level.
Edge or level is preset for the special functions Shutdown and UPS.
Over the selection ⎍ and/or ⎏ within the alarm release definition, the release of an alarm can be configured depending on the switching status of the respective bit. The alarm release within the alarm recording takes place in the dialogue configuration of the recording (cp. *3.3.8 Configuration of the recording*).

3.3.7 Watchdog

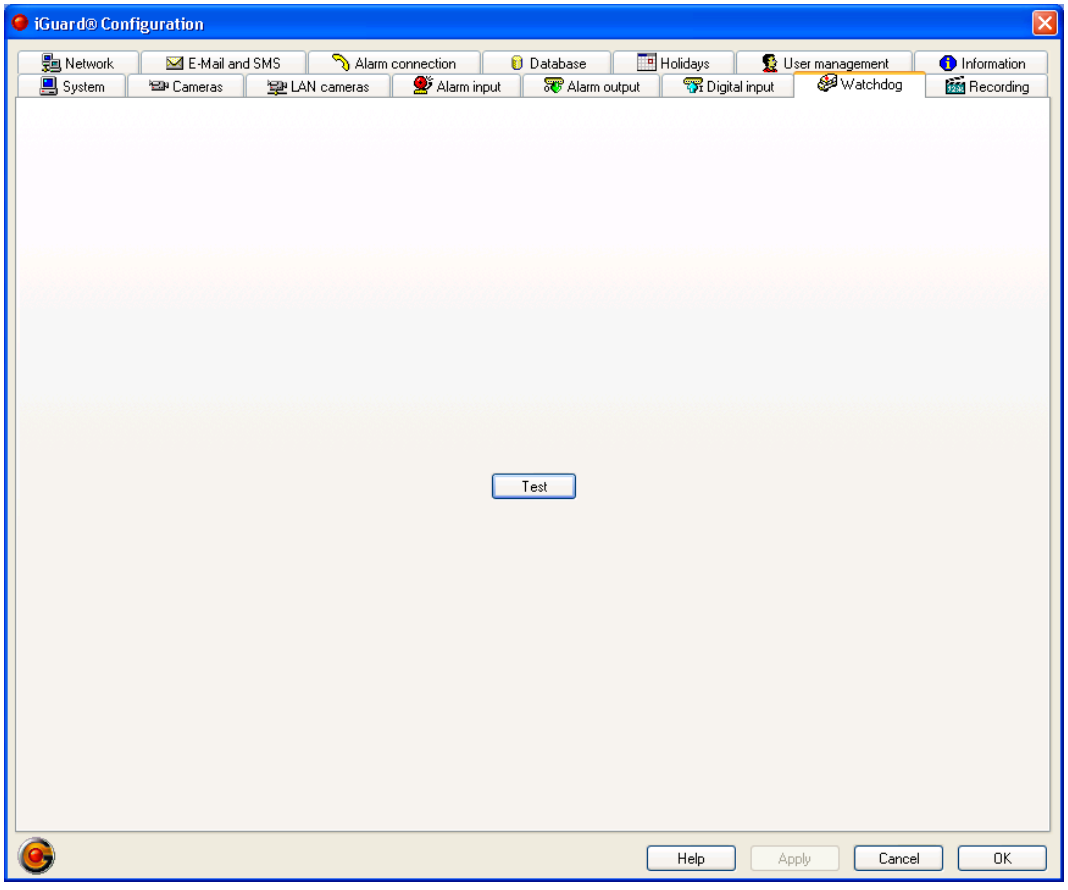


Figure 59: Configuration of the watchdog

This page is only available when a hardware watchdog exists. Here it is possible to test its correct function.

The following frame grabber and video compression board of the *IDS Imaging Development Systems GmbH* are featured with a hardware watchdog:

- *FALCONplus* as from Rev. 5.0
- *FALCONquattro* as from Rev. 2.0
- *DORADOquattro* as from Rev. 1.0

With the button *Test* the functionality of the watchdog can be tested. During the test the watchdog will not be triggered for 5 minutes, so that after the time is expired the PC will be reset.

3.3.8 Configuration of the recording

The *Configuration of the recording* is used to stipulate the recording mode with which the system should operate.
All configured cameras are always *in the ring* and provide live images. Whether the cameras record or not is determined by time settings and events.

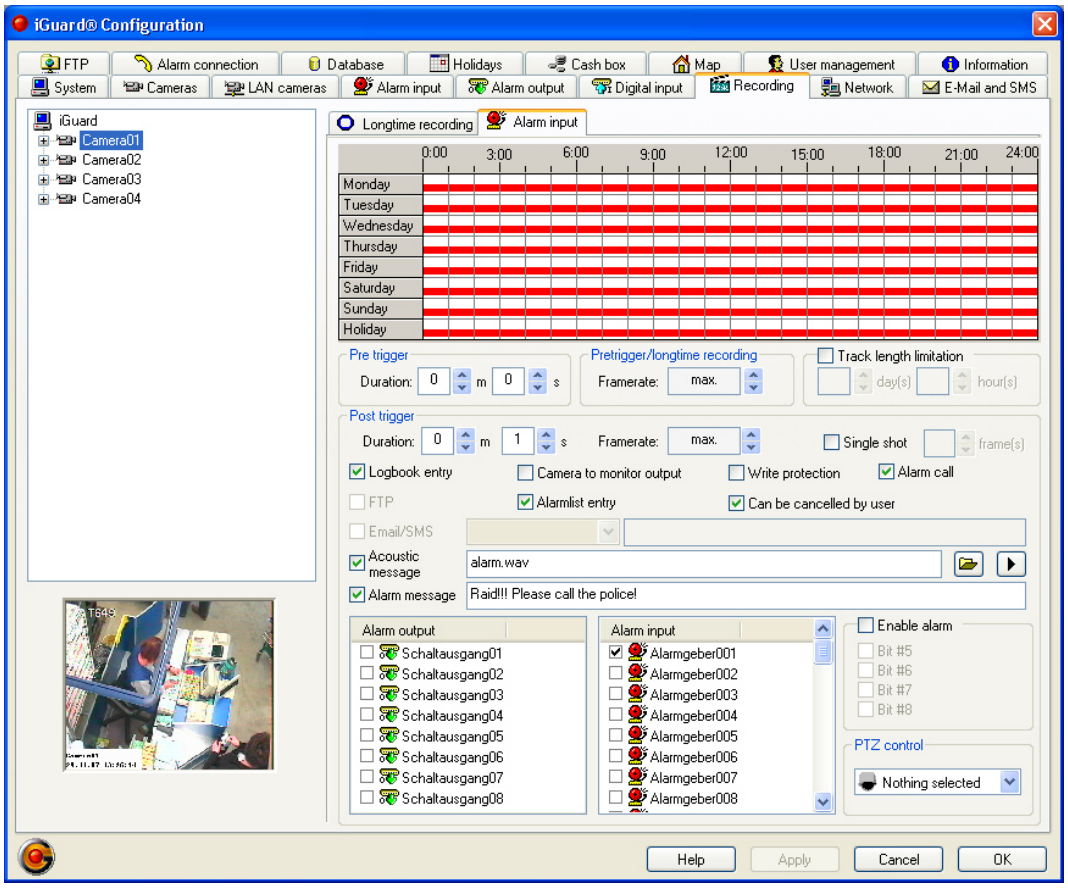


Figure 60: Configuration of the recording

Camera tree structure
All cameras already defined as part of the camera configuration are shown in a tree structure.

The elements of the camera tree can be visualized by clicking the symbols -> . This permits a quick survey of the device structure.

Graphic control element
The adjustment of time of day-dependent functions takes place here. The following operating conditions are differentiated:

- Long-term recording, colour blue
- Motion, colour green
- Alarm contact with normal priority, colour light red
- Alarm contact with suspicion priority, no colour, always active, no possibility of installing time control
- Alarm contact with hold-up priority, no colour, always active, no possibility of installing time control

The selected status (tabulator) is shown in the time graphic chart by a thick bar. Use the left mouse button to add active areas to the time chart and the right mouse button to remove them.
Tabulators are not always visible. Visibility is subject to the following rules:

- *Long-term recording* is always visible.
- *Motion recording* is only visible if the camera is configured for motion detection.
- *Alarm sensor* is only visible if there is at least one alarm sensor with normal (standard) priority.
- *Suspicion* is only visible if there is at least one alarm sensor with suspicion priority.
- *Hold-up* is only visible if there is at least one alarm sensor with hold-up priority.
- *Cash box* (optional) is visible only if a cash box is assigned to the camera. In this operating mode the system is recording if an alarm filter word is conveyed, or a data record is send by the cash box and the assigned camera does not record at this time (e.g. long-time or movement).

Controls for the definition of the behaviour when occurring appointed events

- Pre-trigger
  Each camera can be assigned an individually adjustable pre-trigger time. The variable range of the pre-trigger duration is 10 seconds up to 360 minutes (max. 6 hours). 0 seconds means: The function is inactive, the pre-trigger is not being used.
- Pretrigger/longtime recording
  The frame rate for pretrigger/longtime recording is a setting valid for all statuses. There is the possibility of setting the required frame rate direct for each camera (in predefined, rational stages) and selecting different frame rates for pre-alarm and post-alarm. The system calculates internally the max. possible frame rate to be expected (depending on the hardware and hardware configuration) and issues a warning if the required frame rate is more than 25 % above the calculated frame rate (i.e. the one that can be achieved during operation).
  Put another way: A frame rate can be specified for a camera but may not be achieved in all situations during operation.

The system attempts to bring the performance offered by the hardware as close as possible to the pre-set requirement (default). This is not always possible. Above all when different frame rates are set for different statuses it is possible for different frame rates to occur during operation - depending on the respective status of the cameras.

- Track length limitation
  A track length can be set in day/hour stages for each camera. Every 10 minutes, the system checks whether more recordings by the camera have been saved than stipulated by the max. track length. If this is the case, the system immediately deletes all old recordings that go beyond the max. track length. Write-protected recordings are not taken into account for the track length calculation, i.e. under certain circumstances the camera occupies more memory than stipulated by track length specification in the case of write-protected recordings.
  The reason for this function is that with track length restriction, "less important" cameras provide "important" cameras with more hard disc capacity than would be possible without a limitation to the track length.
- Post-trigger
  A random number of different actions can be stipulated for each status.
  - ♦ Duration
    The post-trigger duration can be set between 1 second and 360 minutes (max. 6 hours). So, when a detected movement took place, the camera switches over to continuous recording for the set time (seconds, but at least 10 pictures) taking into account switching over by other cameras.
    If a camera detects a further movement during the post-alarm duration, the post-alarm duration is extended by the set time from the moment when the new movement occurred.
  - ♦ Framerate
    Setting the frame rate [1 … 25 frames per second] or with the maximal available frame rate. The available frame rate depends on the hardware and hardware circuits.
  - ♦ Single shot/frames
    As an exception, a camera can also be operated in single-frame mode. A lead time is not possible in single-frame mode. In the event of an alarm in single-frame mode, the camera records in one go (i.e. directly one after another at 25 frames per sec. with PAL) the set number of frames (1 - 5 frames). No frames are recorded by any of the other cameras during this recording. This is why the number of frames is restricted to 5 (represents a duration of 200 ms).
    Individual frame cameras do not play a role for the calculation of frame rates of cameras as they only record for a max. of 200 ms in alarm cases.
  - ♦ Log book entries
    This option is available for movement recording and alarm sensors. An entry is made in the log book as soon as one of the aforementioned recording types is activated.
  - ♦ Switching to monitor
    This option is only available if the camera can be switched to an external monitor. Network cameras cannot generally be switched to a video moni-

tor. If an event occurs, the camera image will be displayed on an external monitor.

- Write protect
  Recordings can be provided with write protection with this option. This is only available with an alarm and/or cash box recording.
- Alarm call
  With the option Alarm connection to *iGuard® RemoteView* the possibility exists to realise a connection to a client in case of a failure (e.g. camera loss). The client then shows the error message and the image of the camera.
- FTP
  This option must be activated in order to store a picture can be stored on the ftp server in case of an alarm. This option is only available if a FTP server is configured (cp. *3.3.11 Configuration of a FTP access*).
- Alarmlist entry
  When an alarm event occurs, a message can be sent to *iGuard® RemoteView* which is then displayed in the alarm list there.
- Can be cancelled by user
  If this option is activated, an incoming alarm can be cancelled via the **menu** *Action → Cancel alarm*.
- E-mail/SMS
  Is only available if appropriate details have been provided in the e-mail configuration dialogue for sending e-mails or SMS's.
  The user can enter any random text. The system recognises some variables that can be updated before sending the mail:
  ⇒ %C Name of the camera
  ⇒ %X Current time (date, time)
- Acoustic signal
  Selection of a sound file which is played back if an alarm or an event occurs. This function is only available if the computer is fitted with a compatible, operating sound card.
- Alarm messages
  See chapter *3.1.16 Alarm messages*
- Switch output
  The allocation of the switch outputs to a selected camera is made by the check boxes left beside the switch outputs. Each camera can be linked with one or several switch outputs. That means that in the case of recording the linked output is set active. This happens so long, as the recording takes place and/or the linked output is activated by the concerned signal (cf. *3.3.5 Configuration of the alarm outputs*).
- Alarm sensor
  The allocation of the alarm sensors to a selected camera is made by the check boxes left beside the specified alarm sensors. Each camera, also motion camera (= video sensors, see *3.1.12 Motion detection (camera as video sensor)*), can be linked with an alarm sensor. Thereby a recording with the camera concerned takes place depending on the configuration of the recording (cf. *3.3.4 Configuration of the alarm sensors (detectors)*).

- Alarm release
  The recording of cameras working with sensors can be released by the digital input (see *3.3.6 Configuration of the digital input*).
  The release of an camera can be set dependant on the condition of the digital input bit 5...8 (we recommend to name these inputs corresponding to the devices connected, e.g. “key-operated switch” or “motion detector”).
  The release will occur only if an AND-logic of the digital inputs is true. With this function alarm releases (e.g. siren on/off) can be steered exactly in order to avoid false alarms. We could call this a “series connection” of alarm release.The assignment of the alarm sensor and switch outputs to a selected camera is carried out using check boxes that are located alongside the elements shown in the lists "Alarm sensors" and "Switch outputs".
- PTZ control
  In the event of an alarm (trigger with normal priority, trigger with assault priority), the system can go to stored PTZ fixed positions depending on the alarm input. All set positions that have been saved for the selected camera are recorded on a list with names. The option is only available if the camera is a pan/tilt camera and at least one set position has been saved for the camera. See chapter: "*PTZ – Saving positions*" and "*PTZ - Driving to positions in alarm cases*" (see *3.3.2 Configuration of the cameras*).

Banking mode (optional)

The possibilities of recording configuration are restricted depending on assigned camera type when banking mode is activated. The maximum recording speed (frame rate) is 12 frames per second under all circumstances.

- Room cameras
  Long-term, motion and/or alarm recording can be configured. The minimum frame rate for recordings is 1 frame per second.
- Cash cameras
  The configuration possibilities correspond to those of a room camera with the exception of long-term recording, pre-alarm duration and post-alarm
  - Long-term recordings are not possible.
  - Pre- and post-alarm periods of less than 15 minutes cannot be selected in the case of raid recording.
  - Setting a leader time is not possible for contact, motion and suspicion recordings.
  - The minimum frame rate for suspicion and raid recordings is 2 frames per second.

3.3.9 Configuration of the network parameters

The option *Remote access* must be switched on in order to enable remote access (whether via LAN or ISDN).

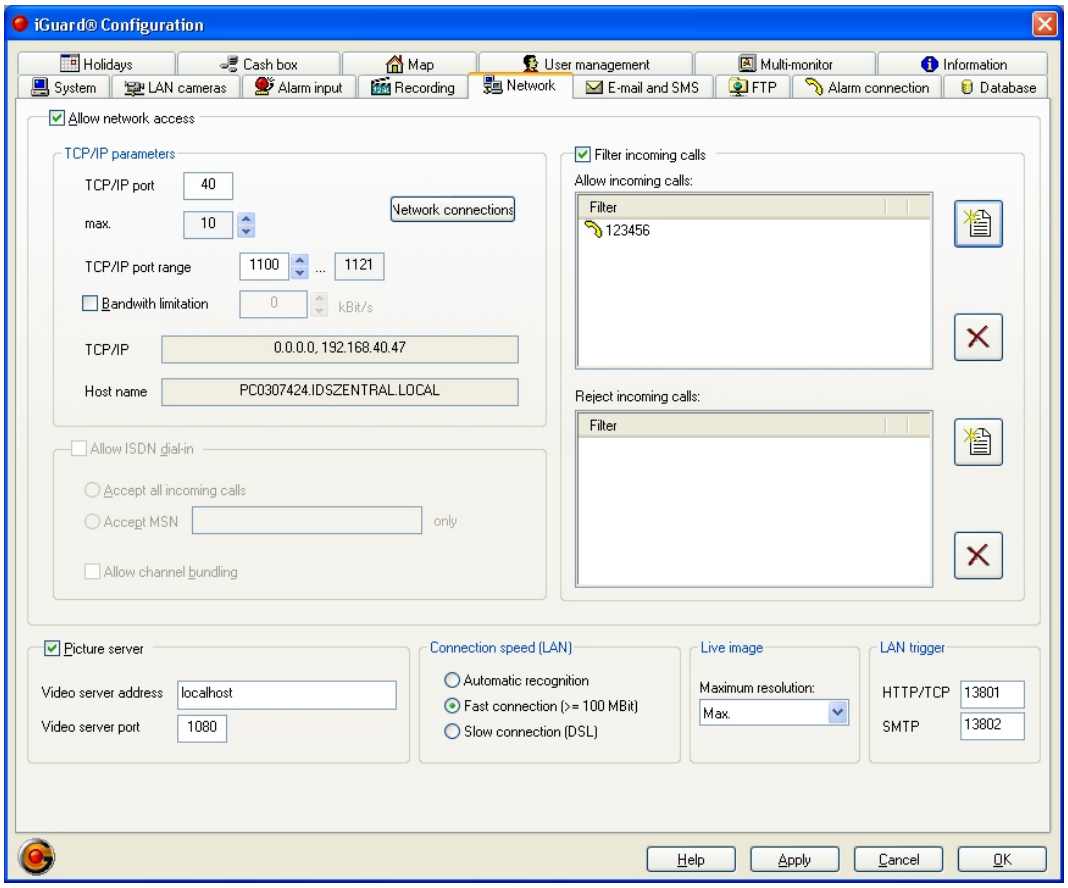


Figure 61: Configuration of the network parameters

TCP/IP Parameter

- TCP/IP Port
  The TCP/IP port (accessible under *iGuard®*) must be specified for access by LAN. Port 40 is usually used.
- Max. Clients
  Maximally 16 Clients can register simultaneously with *iGuard® RemoteView* at one server. Maximally one ISDN connection can be handled.
  In the case of an update of an older version (V2.35 or earlier) the max. number of clients is always set to 1. The administrator must increase the permitted number of clients using the network configuration dialog.
  All clients that register through a LAN connection receive exclusively JPEG images in set quality from the server. LAN clients do not have any further possibility to change the picture quality of live or recorded images. Clients of previous versions (V2.35 or earlier) continue to show control elements and menus for selecting picture quality, a change in the setting however does not

lead to a change in picture quality with a V2.40 server.
All registered clients as well as the local user operating on the server can view simultaneously live images, replay recordings and control switch outputs as well as PTZ cameras. Playing in a new configuration via *iGuard® RemoteView* or changing to the configuration level on the server disconnects automatically all existing connections. The connected clients are sent an appropriate message prior to the connection being disconnected.
The following restrictions are known due to parallel replay:

- ♦ The error message *Cannot find file* may be displayed during replay if another user has deleted recordings. The time-line is not automatically updated at a client's. The same effect can also occur if the system automatically deletes old recordings in overwrite mode.
- ♦ An AVI export can only be carried out by a client or locally from a server
- ♦ A raw data removal can only be removed by a client or locally from a server
- ♦ An iSearch search can only be carried out by a client or locally from a server

- IP port range for firewalls
  If *iGuard®* or *iGuard® RemoteView* are being operated behind a firewall but access still needs to be available from external systems (e.g. from the Internet), it must be possible for all the ports used by *iGuard®* or *iGuard® RemoteView* to be opened at the firewall. The number of ports used by *iGuard®* is related to the max. number of clients that can be registered with the server simultaneously. Each client requires 2 data ports.
  With the firewall the adjusted IP ports must be open for the in and outgoing data traffic.
- Bandwidth limitation
  The bandwidth approved for a LAN connection for the server can be set between 20 kBit per second and 100.000 kBit per second (100 MBit per second). The bandwidth restriction can be switched off.
  A restriction of the bandwidth can result in a LAN connection with *iGuard® RemoteView* only running slowly. The reaction time of the server to a command of an *iGuard® RemoteView* user can also be unbearably long.
  For this reason, the bandwidth restriction should not be activated if possible.
- TCP/IP address / host name
  The TCP/IP address is set at the operating system level during configuration of the network board. *iGuard®* displays the TCP/IP address and the host name of the computer in a non-edit field. If there is more than one network board in a computer, it is possible that this field does not show the TCP/IP address of the LAN network board but that of another network board. The host name is shown for information purposes but is not used for any further purpose by *iGuard®*.

Allow ISDN dial-in

The *Allow ISDN dial-in* option has to be activated if *iGuard®* is also to be available via an ISDN connection.
The service indicator of an ISDN call must always be *Data*. Calls with a different service indicator will be ignored. This enables *iGuard®* to be operated on an ISDN connection parallel to a telephone because the telephone only signals a

call if it bears the service indicator *Telephony*. The following options are available:

- Accept all incoming calls
- Accept MSN only
  iGuard® makes it possible to only react to calls from a specific MSN.
- Allow channel bundling
  If two channels are to be authorised for an ISDN connection, the *Allow channel bundling* option also is to activate.

This option must not be activated if one channel has to be kept free for a separate line (e.g. alarm system)!

We recommend using ISDN cards from:

- AVM FRITZ! PCI , FRITZ! USB v2.0
- HST Saphir III PCI

The communication interface between *iGuard®* and *iGuard® RemoteView* has changed because of the direct CAPI-support in many areas. That is why *iGuard®* and *iGuard® RemoteView* are not compatible downwards as of version 2.2.
Because there are differences in the CAPI drives from different manufacturers – and in some cases even between CAPI drive versions from the same manufacturer – it is possible that *iGuard®* does not function with CAPI drives or ISDN cards other than those already tested.

Filtering incoming calls
Filters can be defined for incoming network or ISDN connections. The filters enable selective exclusion of particular callers from connection with an *iGuard®* server or only allow connection to specific callers. A connection request from unauthorised callers is rejected without comment.
Setting wildcards (*) at the end of a telephone number or IP address is possible. In the event of compliance, the list of authorised callers has priority over the list of unauthorised callers. Consequently, it is possible for access to be granted to the caller with the IP address 192.168.30.100 whereas all other callers from the sub-net 192.168.30* are rejected.
When setting up filters that relate to telephone numbers (ISDN, MSN), it should be noted that MSN's are transmitted differently according to the telephone system. The specification of a filter must conform exactly with the type of MSN transfer.
With the buttons and the filter lists further entries are added or existing entries are deleted.

Connection speed (LAN)
With this option the speed of a LAN connection can be given. With *Automatic recognition iGuard®* accomplishes a recognition of the connecting speed. With *Fast connection* and *Slow connection* the connecting speed is given by the user.

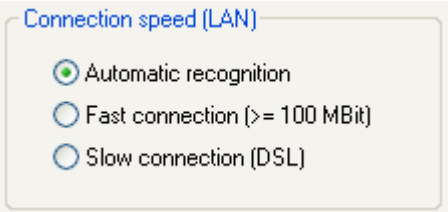


Figure 62: PictureServer

Live image
To reduce server CPU load and network load when transferring images from megapixel LAN cameras, the resolution of the images to be transferred can be set in the *Maximum resolution* field. If you select the *Max.* option, images are always transferred at full resolution.

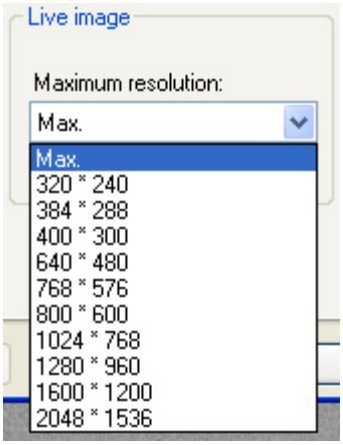


Figure 63: Live image

LAN trigger

iGuard® receives messages from LAN cameras via HTTP/TCP and SMTP on the ports specified here (see also *3.3.4 Configuration of the alarm sensors (detectors)*).

3.3.10 Configuration of E-Mail/SMS messages

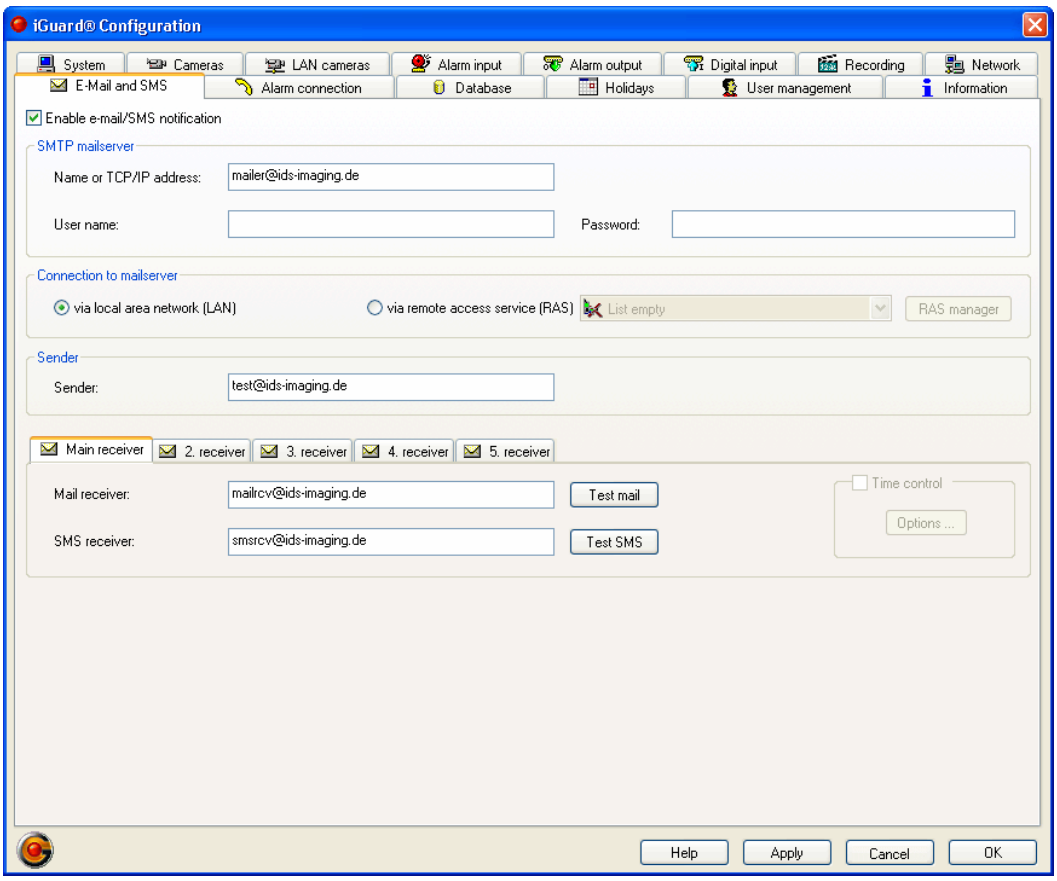


Figure 64: Configuration of email/sms

The option *Enable e-mail/SMS notification* must be switched on in order to use the e-mail and SMS functions.

SMTP Mail server

- Name or TCP/IP address
  Input of the name or the IP address of the post output server. This can be either the address of the Mail server available in a network or the address and/or the name of a SMTP server of a service providers, which is called up direct via a connected modem.
  Examples: 123.45.67.8 or mail.providername.de.
- User name/password
  iGuard® also supports ESMTP servers. These servers expect an independent registration with user name and password. Both of these have to be entered in the appropriate fields.

Connection to Mail server

Connection to the SMTP server is possible in two different ways. The mail server can be accessed in the local network either direct or via a router, or it can be dialled in with a dial-in link (RAS). In order to be able to use an RAS link, it has to be configured in the operating system first. This configuration is carried

out in exactly the same way as setting up an Internet connection, e.g. to T-Online, AOL or other suppliers. If a configured Internet connection already exists, it can be used by *iGuard®*. All RAS links configured in the system are listed. The link that is to be used by *iGuard®* has to be selected on this list. The button *RAS Manager* calls up the RAS manager of the operating system so that a new link or a change of an existing link can set up as easily as possible.

If an RAS server service has been started on your system, please note that this service is not using the same ISDN unit as *iGuard®* otherwise it is possible that no connection to *iGuard®* can be achieved.
Because *iGuard®* does not receive any information from the operating system when an RAS link has been changed, the use has to close the network configuration dialog and open it again after adding or renaming an RAS link. Only then does the system display the new or re-named RAS link for selection.
Please note as well that sending e-mails is impossible if the selected RAS link has been deleted or renamed because *iGuard®* identifies the RAS link according to its name.
If a configuration has been transferred from one computer to another, e-mail despatch only functions on the computer receiving the configuration if there is also an RAS link with the same name in that computer.

Sender

- Sender
  The name of the sender, e.g. the object or the *iGuard®* server name, should be entered here in e-mail address format. Example: site@company.com
  It can be strongly necessary that the sender name is known at the e-Mail-provider.

Receiver

- Mail receiver
  The e-mail receiver should be entered here in e-mail address format (this is essential). Example: peter.exampleman@callcenter.com
  Along with the main addressee for receiving fault messages, 4 further addressees can also be defined that can only receive alarm messages. Each mail receiver can be assigned several e-mail addresses each separated by semicolon. Additional an individual time control can be installed for each addressee, i.e. the addressee only receives a message at specific times. An exception to this is the main addressee where time control is not possible.
- SMS receiver
  The receiver of SMS messages should be entered here in e-mail address format (this is essential).
  Example:
  - ♦ D1-Net : < phonenumber >@t-d1-sms.de
  - ♦ D2-Net: < phonenumber >@d2-message.de
  - ♦ E-Net: < phonenumber >@smsmail.eplus.de

SMS messages are sent to mobile phones via the provider‘s e-mail function, which is why this first must be activated from the service provider in order to receive e-mails via SMS. Receiving these SMS generally means that the mobile phone user will have to pay charges.

- Test Mail / Test SMS
  When these buttons are clicked, a corresponding test e-mail or test SMS is sent directly from the configuration dialog.
- Time control
  Using the button *Options* the dialogue for the configuration of the time schedule can be reached. See also *Marking the time* in *3.3.2 Configuration of the cameras*.

3.3.11 Configuration of a FTP access

This dialogue is used for the configuration of a FTP access. As soon as an alarm occurs or a movement is recognized with activated option *FTP enabled*, the alarm image of the appropriate event is stored in the JPG format in the given root directory of the selected FTP server.

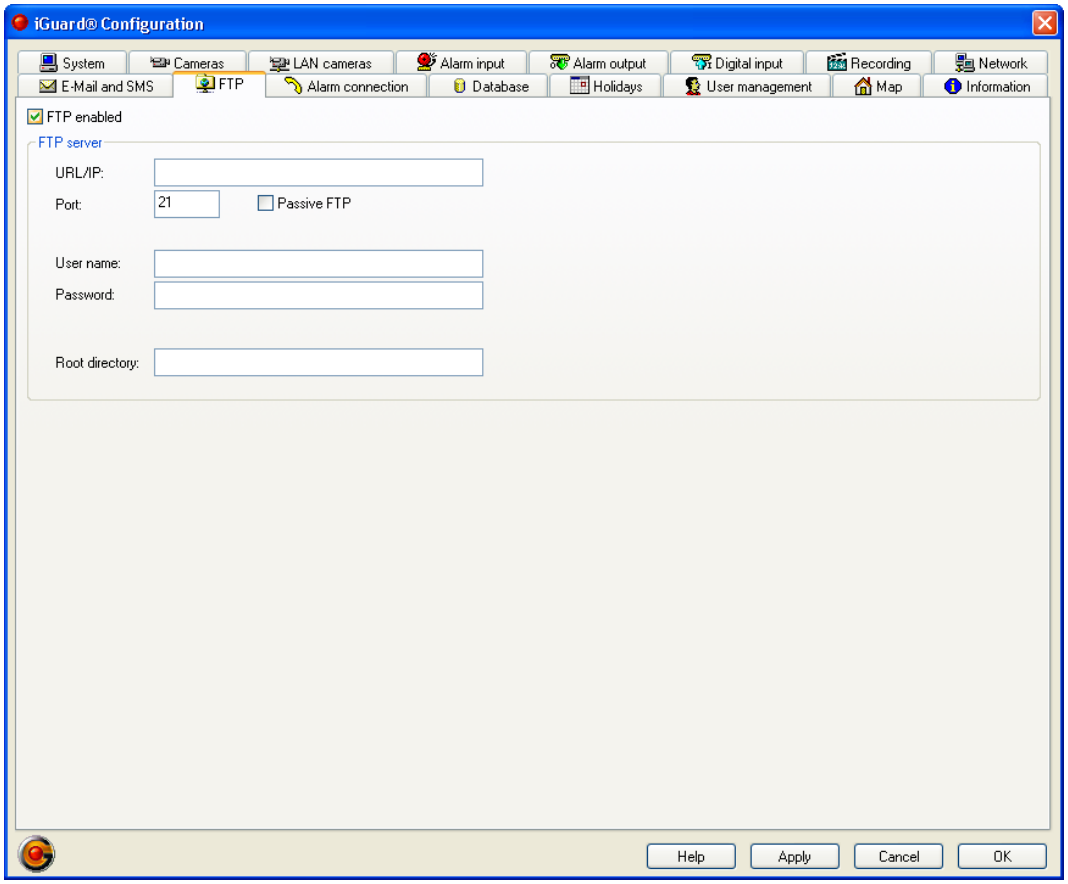


Figure 65: Configuration of a FTP access

The following name convention applies to the alarm picture: yyyymmddhhmmssxxx.jpg. For this the file name 20060223091209024.jpg is classified as follows:

yyyy	Jahr	e.g. 2006
mm	Monat	e.g. 02
dd	Tag	e.g. 23
hh	Stunde	e.g. 09
mm	Minute	e.g. 12
ss	Sekunde	e.g. 09
xxx	Millisekunde	e.g. 024

If an alarm message is configured for the occurred alarm, this is stored as text file in the same directory, in which the alarm picture is stored. The file name of

the text file corresponds to the name of the image file, up to the ending. This reads with the text file msg.

FTP Server

- URL/IP
  Address of the server
- Port
  Interface of the FTP server (usually 21)
- Passive FTP
  The dial-up of the data communication is initiated by the Client.
- User name/Password. Passive FTP must usually be used, if a firewall is in the network.
  Login information for the FTP server. The user must be configured at the FTP server.
- Root directory
  Beneath this directory, the alarm images and alarm messages are stored.

iGuard® deletes no files on the FTP server. Thus the possibility exists that the capacity of the FTP server is exhausted by-and-by.

In order to store a picture on the FTP server in case of an alarm the option *FTP* must be activated in the configuration of the recording (cp. *3.3.8 Configuration of the recording*).

iGuard® needs the following authorizations on the FTP server:

- write permission for files
- permission to create directories

3.3.12 Alarm connection to iGuard® RemoteView (optional)

In the configuration of the recording (see *3.3.8 Configuration of the recording*) the call to the *iGuard® RemoteView* Client can be assigned as a special function.

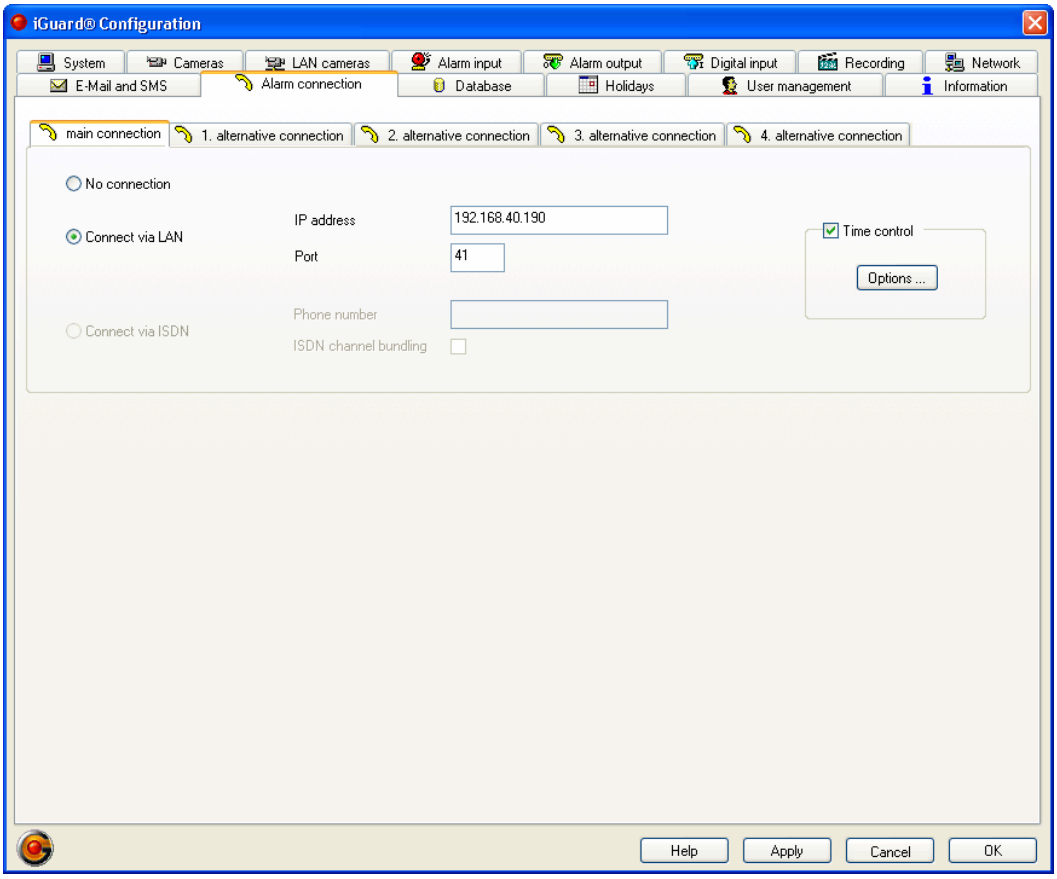


Figure 66: Configuration of the alarm connection

Following options are available for the alarm connection:

- No Connection
  No alarm connection takes place.
- Connect via LAN
  The connection to the *iGuard® RemoteView* client is made over a LAN connection. The input of the IP address and the port under which the client is reachable is necessary.
- Connect via ISDN
  Connection to the *iGuard® RemoteView* client is made over a ISDN connection. In this case the call number of the client must be entered. Further it is to be decided whether a channelling is to be accomplished.
- Time control
  The alarm connection can also be time controlled. Over the button *Option* the dialog for setting the time scheme is opened. See also *Marking the time* in *3.3.2 Configuration of the cameras*.

-

The alarm connection is only carried out if the application *iGuard® RemoteView* has been started. In addition, the option *Allow alarm connection* must be activated in the configuration of *iGuard® RemoteView* (cf. *4.2 Configuration*).

One main connection and four alternative connections are available for configuration. If one of these connections cannot be established the subsequent connection will be used. In case none of these connections can be established, no alarm connection takes place.

3.3.13 Configuration of the database

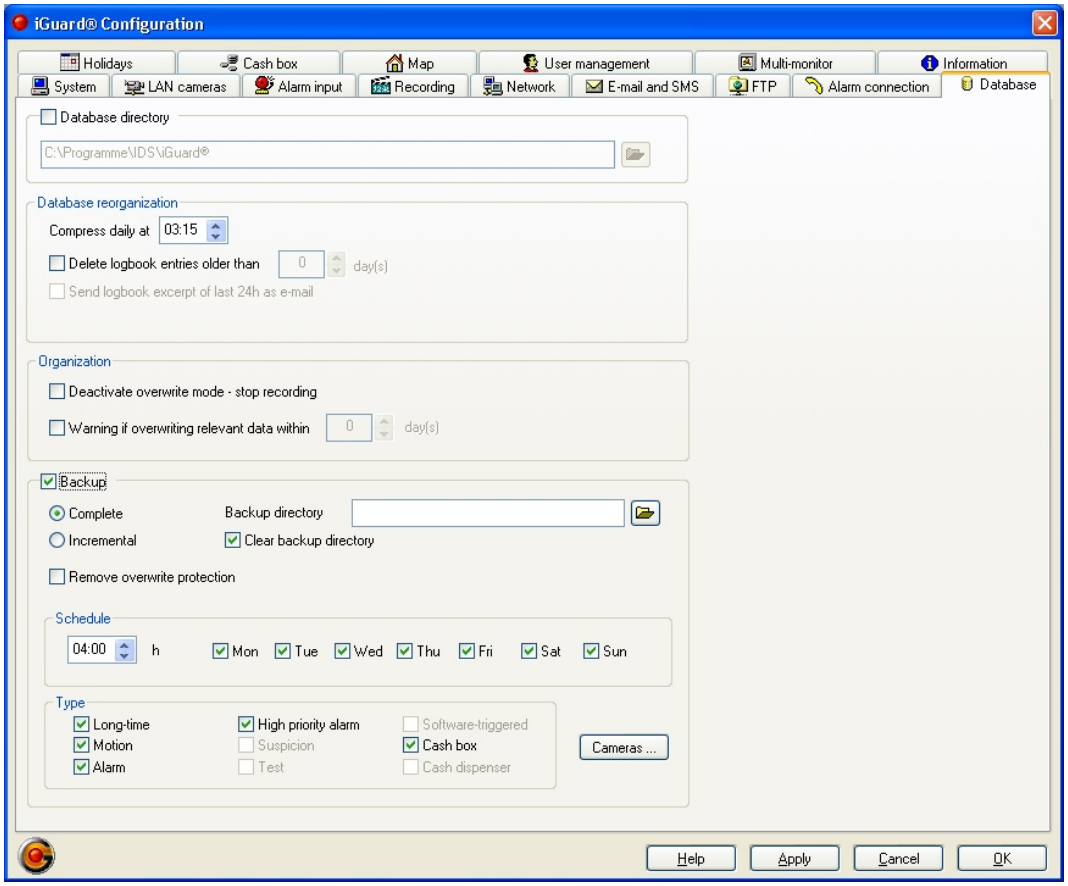


Figure 67: Configuration of the database

Database directory
If the database is to be stored in another directory than the main directory of *iGuard®*, the directory can be determined here. This is especially important, if using removable hard discs.

The local analysis of recordings on removable hard discs by using *iGuard® RemoteView* is only possible if the database files were stored on the removable hard disc before.

Database reorganisation

- Compress daily
  iGuard® will, at a pre-set time, carry out an automatic daily scan of its databases and reorganise these to the best possible condition. This routine serves to continuously maintain the database.
  The time of the daily reorganisation should be put on one calm time period which can be expected, in order to ensure that the efficiency of the system is not reduced by the write/ read activities of the hard disk drive during continuous operation. The check of the data bases can take some time depending on the complexity.
- Delete logbook entries
  Specified period in days, after which log file entries are deleted automatically.
- Send logbook except of last 24h as e-mail
  Following a database reorganisation, *iGuard®* is able to send the main receiver an extract of the logbook for the last 24 hours per e-mail insofar as e-mail despatch is correctly configured under network settings.

Organisation

- Deactivate overwrite mode
  iGuard® stops recording as soon as this option has been activated if the hard disc capacity has been completely used up. This means it is not possible to delete any data on the hard disc to make room for further recordings. In this case, a message is shown on the screen and an entry is made in the logbook.
  This option is not available if banking mode has been activated.
- Warning if overwriting relevant data
  A warning message is issued if the system automatically deletes recordings that are within the specified period (1 ... 365 days). This notifies the user if a minimum storage duration can no longer be guaranteed by the system. In this way, the system points out that more hard-disc capacity or a higher image compression is required in order to be able to guarantee the requirement storage duration.
  A warning message is not issued in the event of manual deletion (user action), not even if the deleted recordings lie within the relevant range.

Backup

iGuard® can store video and audio recordings complete or partially on an external drive. CD/DVD recorders are not supported thereby.

- Complete/Incremental
  The user can select between a complete and an incremental backup. An incremental backup saves all files, which were created since the last backup.
- Backup directory
  iGuard® provides a new subdirectory below the displayed backup directory

with each backup. The name of the directory consists of the starting time of the backup.
YYYY-MM-DD-HH-MM-SS
YYYY Year
MM Month
DD Day
HH Hour
MM Minute
SS Second
Below this directory data base copies are stored and for each camera a separate subdirectory is created.

- Clear directory before
  The user must care for enough free memory on the target drive at the beginning of a backup. *iGuard®* does not administrate the storage capacity of the target drive. However using the option *Clear directory before iGuard®* can delete all files and directories below the backup directory before a new backup.
- Remove overwrite protection
- When this option is checked and recordings that are write-protected are backed up (see *3.3.8 Configuration of the recording*), write protection is automatically removed after backup. These recordings can then be deleted/overwritten. When this option is deactivated, write protection is not removed after backup.
- Schedule
  With this option it can be configured, when a Backup is to be accomplished. The configuration of the time and the weekday is possible.
- Type
  To provide that not all recordings become stored, the user can specify, which kind of recordings and which cameras has to be stored. The following types of recordings can be selected:
  - ♦ Long-time
  - ♦ Motion
  - ♦ Alarm
  - ♦ High priority alarm
  - ♦ Suspicion
  - ♦ Test
  - ♦ Software triggered (if software trigger is activated, not possible in banking mode)
  - ♦ Cash box (not possible in banking mode)

  The cameras to be stored are selected in a separate dialogue. This is opened over the button *Cameras*.

In order to prevent that all data become stored with the setup of an automatic incremental backup, the administrator can mark all past recordings as saved. This happens in playback mode by the ***menu*** *Database → Service → Mark all recordings as backuped*. The next incremental backup then stores all files which were created after this command.

To prevent that a backup slow down the system performance too much, its system priority is smaller than the priority of other procedures. Otherwise a parallel recording and playback would not be possible. The smaller priority has the disadvantage that the backup lasts longer. An incremental backup should always be closed within 24 hours. A progress bar for backups is not designated.

When backing up recordings that are write-protected (see *3.3.8 Configuration of the recording*), write protection is automatically removed after backup. These recordings can therefore be deleted/overwritten.

3.3.14 Banking (optional)

The *Banking* register is only available when banking mode has been activated.

Banking mode and cash mode are mutually exclusive. It is only possible to run one module.

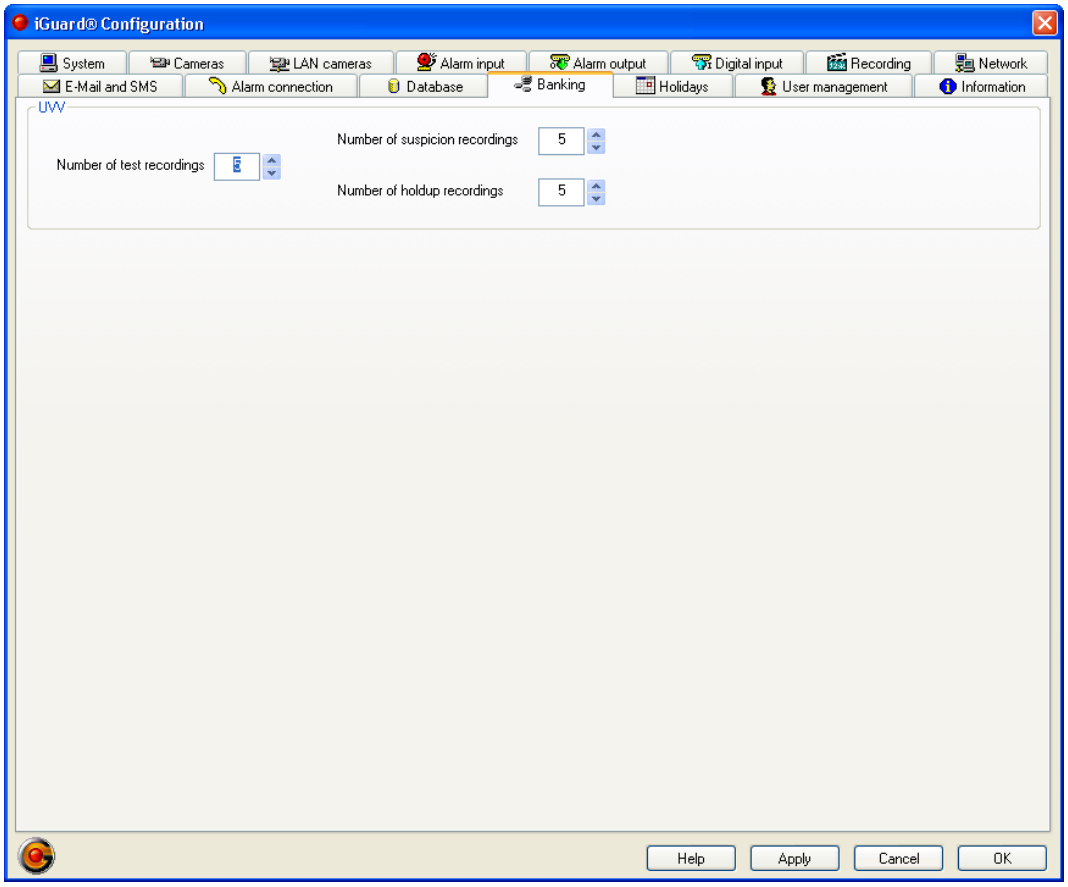


Figure 68: Configuration of the banking mode

UVV

- Number of test recordings
- Number of suspicion recordings
- Number of hold up recordings

According to UVV guidelines, test, suspicion and hold up recordings must be stored permanently.
As these recordings have to be available permanently, they may not be deleted if the capacity of the recording medium has been completely used up. In this case, older recordings will have to be deleted from normal operation in order to create room for new recordings. Deleting is only then possible if the pre-set number of recordings has been exceeded.

3.3.15 Holidays

Along with the usual weekdays (Mon. - Sun.) there is also an extra day: the holiday. Holidays are configured for the whole system. They cannot be different for one object separately (e.g. a camera).

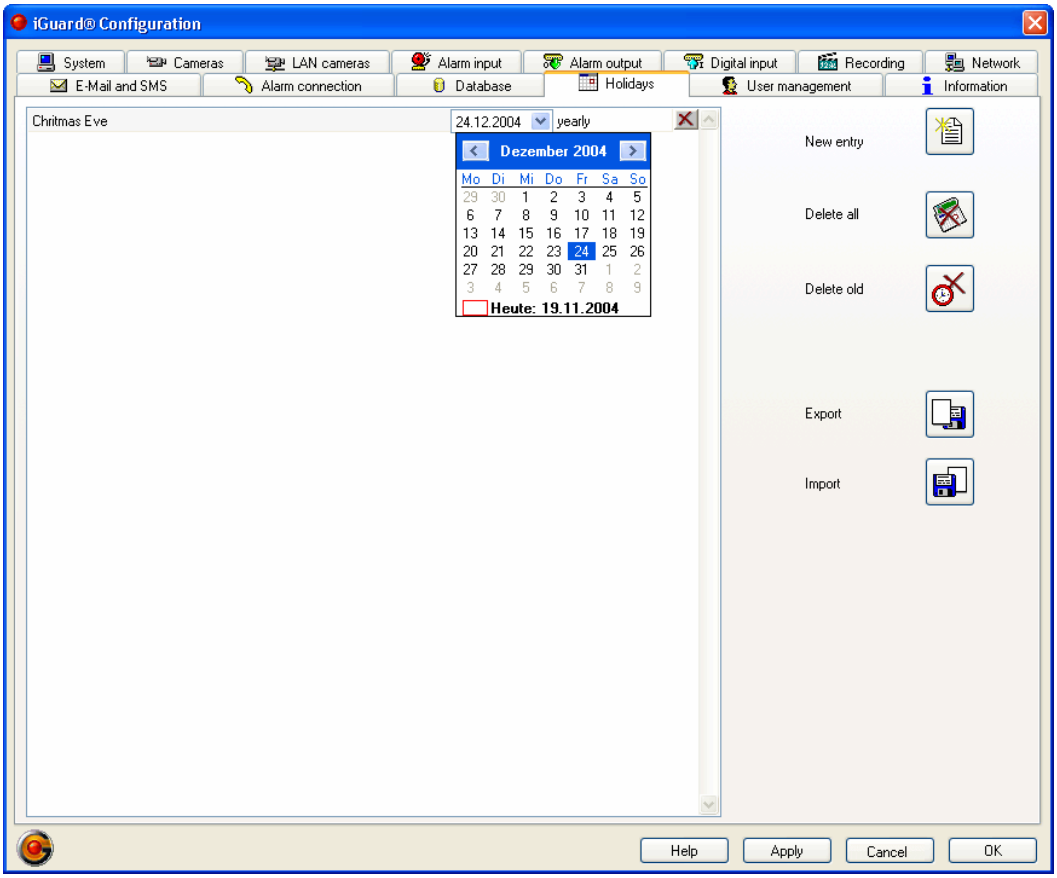


Figure 69: Configuration of the holidays

- List of the holidays
  The holidays are shown in a list. For each holiday 3 values can be deposited:
  - ♦ Name or comment
  - ♦ date

- repetition of the date

Through a click in the fields the entry of the concerned field can be changed. Marked days/weeks/years can be changed with the cursor keys or entered directly. Optionally a graphic calendar for selection can be faded in.
The preset of the repetitions takes place in a selection field. The following options are available:

- single
  Unique date, no repetition.
- monthly
  Monthly recurring date. The adjusted month and year is not important.
- yearly
  Annually recurring date. The adjusted year is not important

The deletion of an entry is made over the context menu or by the *delete* symbol in the fourth column. This appears, as soon as the entry was selected.

- New Entry
  Using the button *New entry* a new holiday can be added to the list. With a new entry the name field is empty, as date the current date was inscribed and as repetition uniquely. Alternatively a new entry can be added by a double-click within the empty range of the list.
- Delete all
  With this button all list entries can be deleted at one time.
- Delete old
  The dates already passed are deleted, if these are not repeated.
- Export/Import
  Using the appropriate buttons the holidays can be exported or imported separately.

The holidays are also stored in the configuration file *iGuard.dat*; they will also be transferred with a transfer of the entire configuration onto other systems.

3.3.16 User management

The following table informs about the user groups and the assignment of the rights for these groups.

		Administrators	Installer	User-Administrators	Users
Administration	×	☑	---	---	---
Installation	×	☑	☑	---	---
Configuration		☑	☑	---	---
User management	×	☑	☑	☑	---
Database		☑	☑	☑	---
Delete		☑	☑	☑	---
Start/Stop	×	☑	☑	☑	☐
Live audio	×	☑	☑	☑	☐
Remote control	×	☑	☑	☑	☐
Remote access	×	☑	☑	☑	☐
Playback	×	☑	☑	☑	☐
Audio playback	×	☑	☑	☑	☐
Cash box search	×	☑	☑	☑	☐
Export	×	☑	☑	☑	☐
Display *(cam)*	×	☑	☑	☑	☐
PTZ *(cam)*	×	☑	☑	☑	☐
Playback *(cam)*	×	☑	☑	☑	☐

☑: User has the right always
---: User has the right never
☐: User can get the right
×: right can be configured individually
(cam): right obtaining to a camera

The table represented above shows that the user groups *administrators*, *installer* and user administrators have dedicated rights. Individual rights can only be assigned to the user group *user*.
The user groups and rights are assigned in the user administration to the *iGuard®* users. In its supplied state, there two users defined:

- the Administrator with the password Administrator
- the Installer with the password Installer

These users cannot be deleted. The password, however, can be changed.

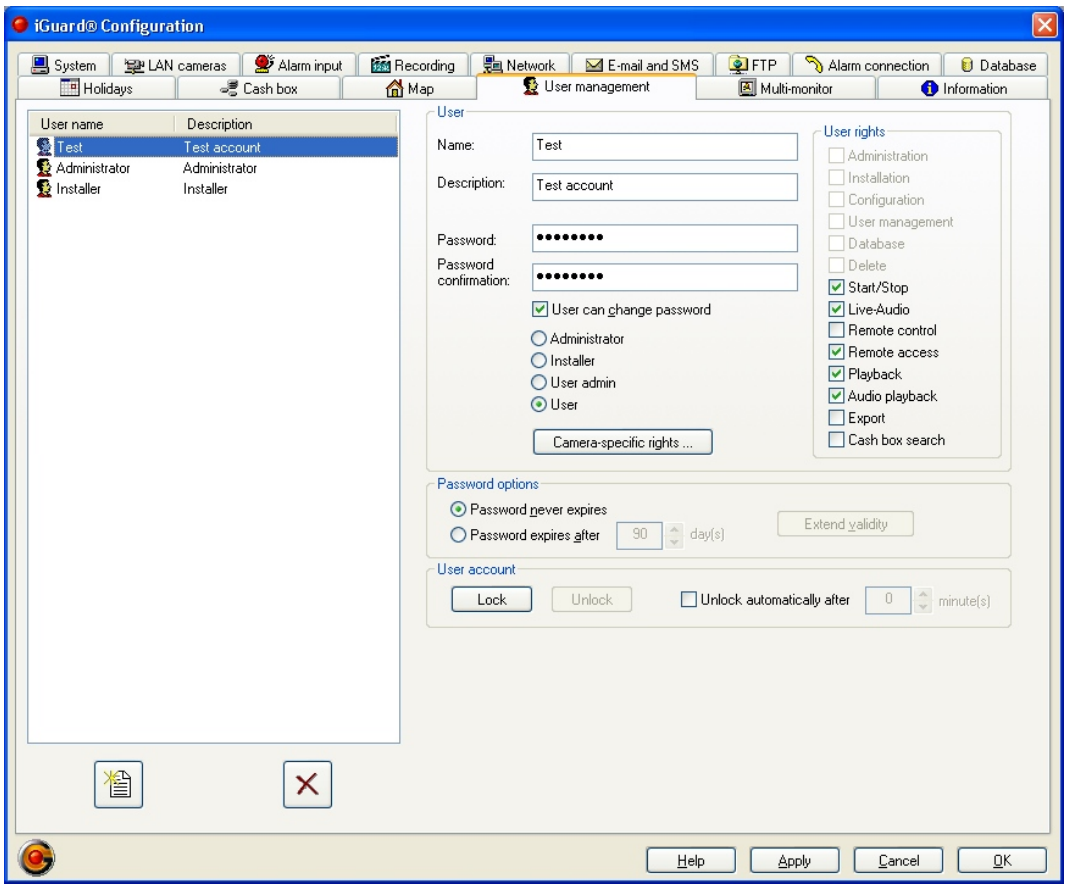


Figure 70: Configuration of the user management

User list

The dialog for the User management shows a list of all known users with user name and description. After the selection of a user its detailed information is shown and can be changed. A pre-condition for this are administrator or user administration authority.

By choosing the buttons and/or additional users can be defined or deleted.

User data can only be added, deleted or updated with the right *user administration*.

User

A user must have been appointed by the administrator before he can access the system. Therefore administration or user management authority is necessary

- Name/Description
  Name and description of the user

- Password/Password confirmation
  The allegation of a password is compellingly necessary.
- User can change password
  This option is activated by default. Thus it is possible for a user to generate a own password.
- User group
  Allocation of one of the following user groups:
  - ♦ Administrator
    All rights are assigned to the user group *administrator*.
  - ♦ Installer
    Installers have also all rights except the right administration. Thus this user group can not configure all system settings.
  - ♦ User administrator
    The user group *user administration* can add new users, delete existing users or change their rights. Opposite the user group *Installer* this user group is missing the right configuration.
  - ♦ User
    Individual rights must be assigned to this user group.
- Camera-referred rights

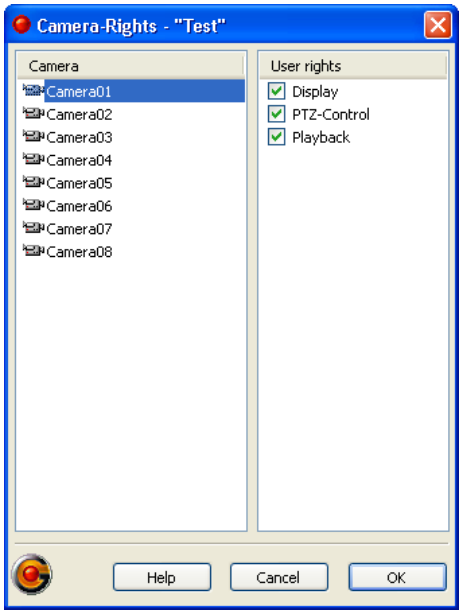


Figure 71: Camera-referred rights

Special rights for individual cameras can be assigned to users in this user group. This takes place in the dialogue camera rights, which is opened over the button Camera rights ... . The following rights can be assigned:

- ♦ Display
  Users with the right *display* may see live pictures of this camera. Without the camera-referred right *playback* and the global right *playback* the recordings of the camera can not be shown.

- ♦ PTZ-Control
  The right PTZ-Control is necessary for cameras with pan-tilt-zoom-control. In addition the camera-referred right display is essential.
- ♦ Playback
  To playback recordings of a camera the user needs the global right *playback* and also the camera-referred right *playback*. In the time line only the cameras are shown for which the users have the right camera playback. The right camera playback has only for all non-cash cameras a meaning. To cash cameras only the global right cash playback applies.

- User rights
  The assignment of individual user rights is possible only at the user group *user*. All other user groups have dedicated user rights.

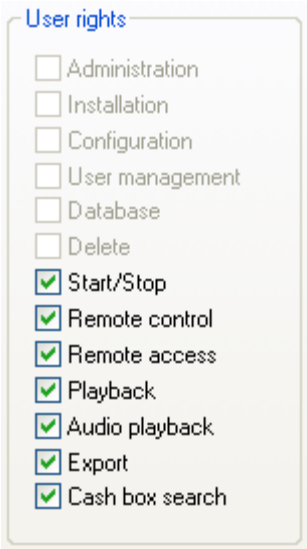


Figure 72: User rights

- ♦ Administration
  The *Administration* right is the highest of all rights. Users with *Administraton* right have control of the system.
- ♦ Installation
  With the right *Installer* less system configurations can be done as with the right *Admininistration*.
- ♦ Configuration
  Allows the configuration of the application, the hardware configuration and the access to the configuration mode.
- ♦ User management
  Installation and administration of users.
- ♦ Database
  Users with the right *Database* can start data base functions in playback mode. Database functions are:
  - database dump
  - create database
  - proof and repair database
  - indicate database

The right *Database* requires the right *Playback*. The right *Database* can not be assigned individually. Only users with *Administration*, *Installation* or *User administration* right have the right *Database*.

- Delete
  Messages and recordings can be deleted. User with the right *Delete* must have also the right *Playback*. The right *Delete* can not be assigned individually. Only users with *Administrator*, *Installation* or *User administration* right have automatically the right to delete recordings.
- Start/Stop
  This right permit to start and terminate recordings and to terminate *iGuard®*.
- Remote control
  Switch outputs can be activated and/or deactivated and PTZ cameras can be controlled (cf. *4.16 Remote control of switch outputs*).
- Remote access
  Enables remote maintenance, remote surveillance and/or remote playback. This can be done using *iGuard® RemoteView*. In order to be able to login at the system over *iGuard® RemoteView* the user needs the right remote access.See also *4 iGuard® RemoteView*.
- Playback
  This right enables to change into playback mode. In order to be able to show recordings of certain cameras, the user needs the camera right *Playback* additionally for each camera. The *Playback* right is required also for the *Audio playback*.
- Audio replay
  For users with the right *Audio playback* the right *Playback* is required.
- Export
  This right allows to export recordings in any form. In addition for this the right Playback is needed. Export refers to the production of AVIs, storing frames (bmp or jpg) or printing the images.
- Cash box search
  With this right the cash box search can be started at systems with cash boxes. Therefore the right *Playback* is not necessary. User which have the right *Cash box search* and do not have the right *Playback* can change to the playback mode. However they can only execute cash functions. They see e.g. no logbook.
  The right *Cash box* search is not offered in the user configuration for systems without cash licence and/or banking system.

Password options

The user needs a password and the deallocation for the respective system level. The indication of a password is compellingly necessary.
In addition the validity of the password can be limited temporally or however be granted for unrestricted time validity. The extension of a temporally limited password is at any time possible thereby from a user with user administration rights.

User account
The user account is blocked automatically if a password is entered incorrectly three times in a row. A user account is re-enabled either automatically after an adjustable pre-set time or manually by a user with admin. authorisation. The user account of an *Administrator* cannot be blocked.
Example: If a value of 15 minutes has been entered for the automatic release of a user account, the 3-times rule starts from beginning again at the end of 15 minutes after the last password input, i.e. if a wrong password was entered for a user account 3 times in a row within 15 minutes.

With the 3-times rule it is irrelevant whether the input was local or remote via *iGuard® RemoteView*.

Chip card scanner support
iGuard® recognizes Chip card scanner of the company SCM Microsystems (USB or serially) automatically, if these are correctly installed. The only supported chip cards are memory chip cards. Processor chip cards, magnetic strip cards or devices by other manufacturers are currently not supported.
iGuard® can save encoded user data (name, password) on a chip card. For the registration at the system then only the smart card is necessary. The user does not need to know user name and password. Because only the name and password are stored on the chip card, the server's user configuration decides which rights the user has and whether the user name is valid or whether the user is barred.
The chip card can be used both for server as well as the *iGuard® RemoteView* client.
Generation of a chip card is carried out from the user configuration. If a chip card scanner is connected, a *Generate chip card* button appears on the dialog page of the user configuration. If this button is pressed, the data of the selected user is written onto a chip card.

- Using the chip card on the server
  If a user is registered and a correctly written chip card is inserted into the card scanner, the user is automatically registered with the system with the user name stored on the card. De-registration is only possible by removing the card.
  If a user is already registered without using a chip card, inserting a chip card in the card scanner is ignored.
- Using the chip card with the client
  No log-in dialog is displayed when setting up a connection with a server if a correctly written chip card has been inserted in the card scanner at the time of setting up the connection. The log-in process on the server is then carried out with the name saved on the card.
  Removing the card from the card scanner leads simultaneously to an immediate disconnection of the connection insofar as the connection was established using a chip card.

3.3.17 Configuring the Map (optional)

In map configuration mode, maps available as bmp files can be combined and linked with objects. The following restrictions apply:

- No more than 32 maps in total can be displayed.
- Maps can be displayed in a maximum of two hierarchy layers.
- A maximum of 192 objects can be positioned.
- The minimum map size is 256 x 256 pixels.
- The maximum map size is 2048 x 2048 pixels.
- The colour depth must be 24 bits/pixel.

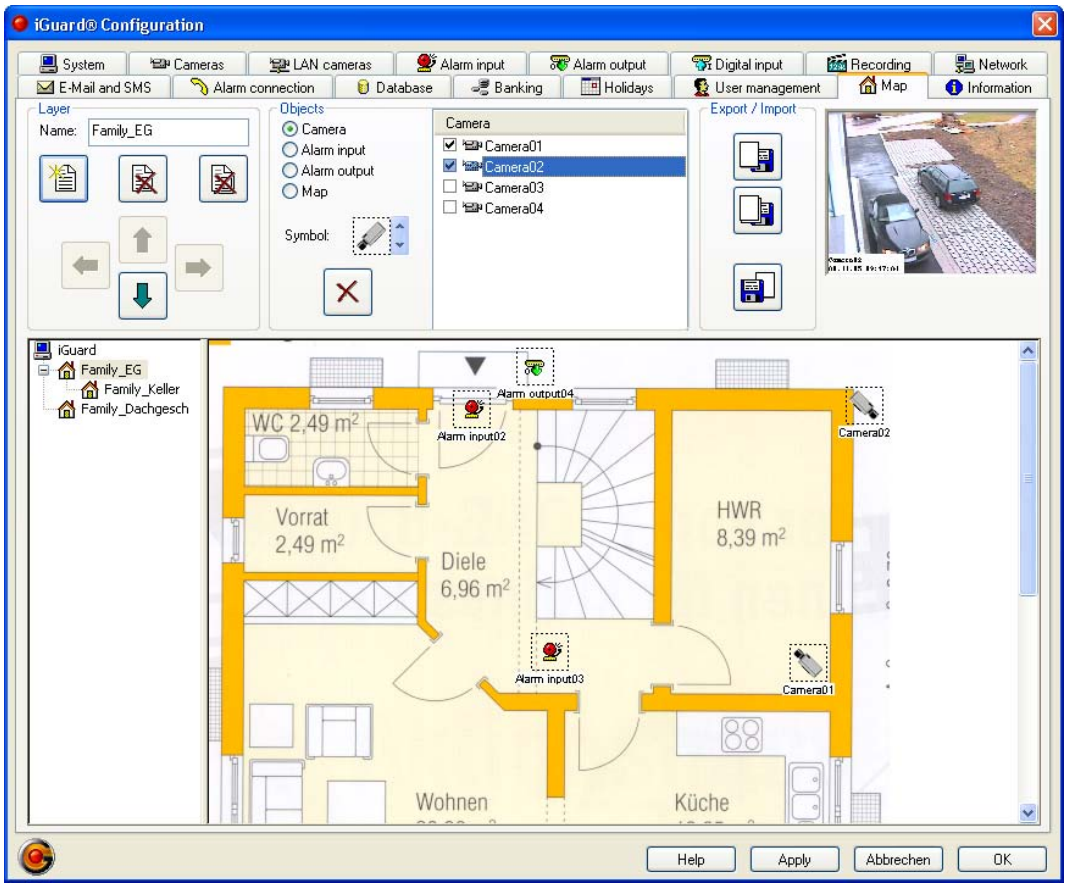


Figure 73: Configuring the Map

Layer

Name — Map name
The map is displayed in the tree structure under the name entered here.


Add map to tree structure (see also *Adding maps*).


Delete map highlighted in tree structure.


Delete all maps.

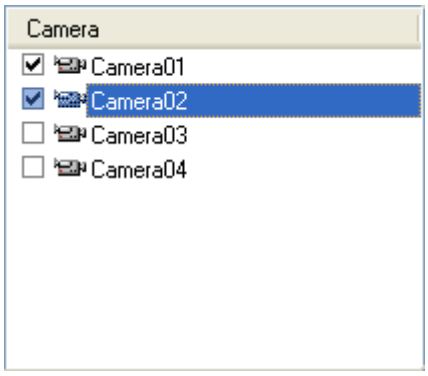

Move map one step up/down.


Move map one hierarchy layer up/down. A maximum of two hierarchy layers can be set up (main layers and one subordinate layer per main layer).

Objects

The following object types can be positioned on the currently selected map (see also *Adding and deleting objects*):

-  *Camera*
  For the *Camera* object you can use an appropriate symbol to indicate how the object is aligned. The following symbols are available for this purpose:
   (Dom cameras)
-  Alarm input
-  Alarm output
-  Switching to a different map listed in the tree structure
-  Delete all objects on the selected layer
- Selection list



Depending on the selected object type, the available elements for this object type are displayed in a selection list. Available means that e.g. cameras must have been set up in the camera configuration.
There is a special feature when selecting the cameras. As soon as a camera

is highlighted in the selection window, its live image is displayed in the window on the far right.

Export/Import
The following export and import functions are available (see also *Importing and exporting layers*):


Export current layer


Export all layers


Import layer

Tree structure
The tree structure displays all active maps (ground plans) hierarchically. Up to two hierarchy layers can be created.

Display window
The display window shows the currently selected map with the objects positioned on it. If the graphic for the map you want to display is too large to fit into the display window, scroll bars appear.

The graphic of the map to be displayed is not scaled.

For single monitor operation with a screen size of 1280 x 1024 pixels the size of the map to be displayed should not exceed 800 x 600 pixels.

Adding maps
The *Add new layer* button  calls up an *Open file* dialogue. Use this dialogue to select the map file you want to add.

The map file you want to display must be available in jpg format. Maps must be at least 256 x 256 pixels and no more than 2048 x 2048 pixels in size. The colour depth must be 8 or 24 bits/pixel.

The selected map is shown in the display window.

Adding and deleting objects

In order to add an object to the map, you must first select its object type. Then all available elements of this object type are shown in the selection list. In the next step, select an object from the selection list (highlight it) and position it on the map with the mouse. The selected object is added at the current cursor position by clicking with the left mouse button. Confirm placing the object by ticking the checkbox in the selection list.

The positions of previously placed objects can be edited at a later date. To do this, click the respective object with the left mouse button. Then you can drag the object by holding down the left mouse button.

The same object can be created on several layers, but only once on each layer.

Cameras are displayed by the selected symbol. This too can be edited after it has been positioned. Open the pop-up menu for camera objects by clicking the corresponding camera symbol with the right mouse button.

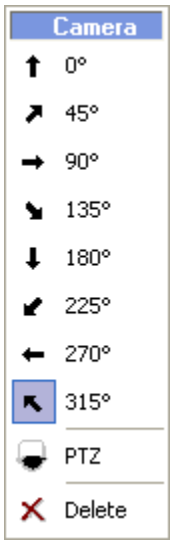


Figure 74: Pop-up menu for camera objects

You can replace a current symbol by clicking the desired symbol in this menu. You can also delete objects here.

Previously added objects can be replaced by objects of the same or a different object type. To do this, select the new object in the selection list and then click the object you want to replace with the left mouse button. Reply *Yes* to the prompt that appears.

To remove an object from the map, you must delete it. There are several ways to delete an object

- Uncheck the box before the corresponding object in the selection list
- Double-click the corresponding object with the left mouse button

- Use the pop-up menu (as described above)

As opposed to these methods, which only delete a single object, the button allows you to delete all objects on a layer.

Importing and exporting layers

You can export configured maps, for example for use in *iGuard® RemoteView*. If the current configuration consists of several layers, you can choose to export only a certain layer or all layers of the current configuration. When you have selected one of the export functions (*Export current layer*, *Export all layers*), a *Save as* dialogue opens. The layers are saved as *.map files.

You can import one or more layers with the *Import layer* button. When you press the button, an *Open file* dialogue appears in which you can select the *.map file you want to import.

3.3.18 Configuration of cash boxes

Cash mode and Banking mode are mutually exclusive. It is only possible to run one module.

Up to 10 different cash boxes can be connected over a RS-232 Interface.

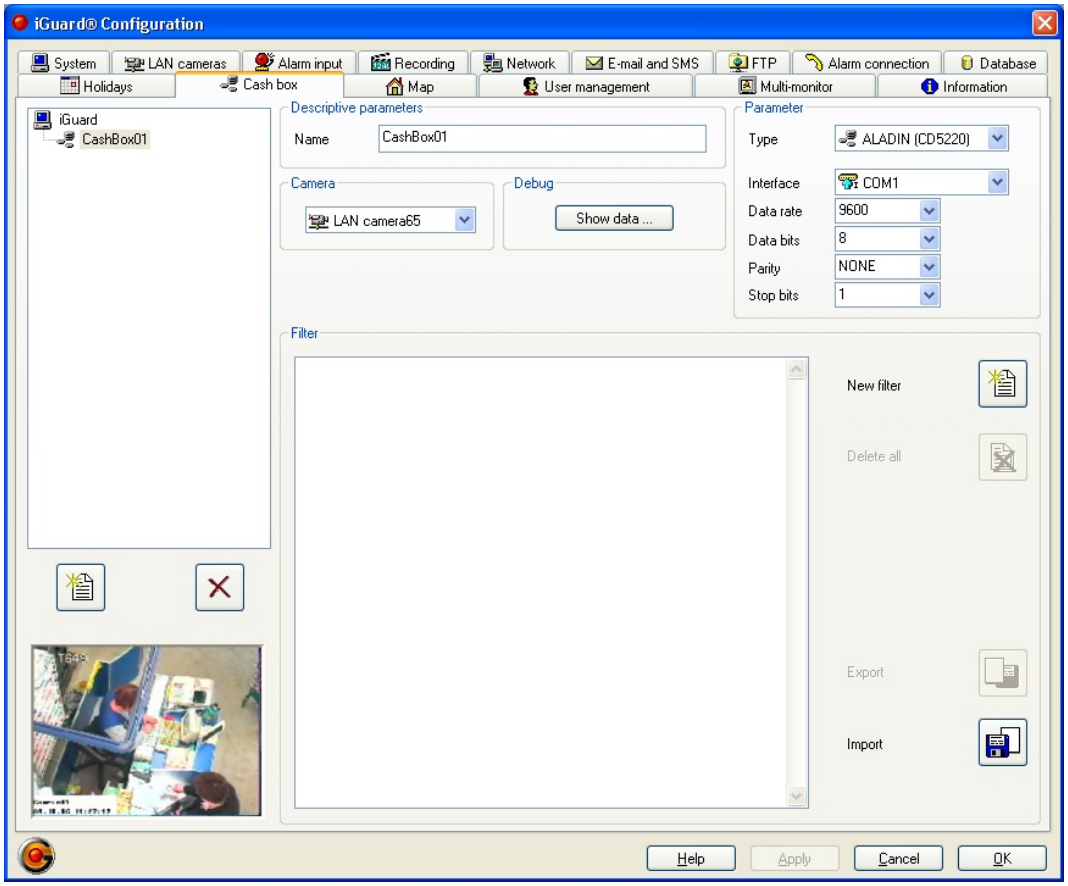


Figure 75: Configuration of cash boxes

Tree structure

The configured cash boxes are displayed in the tree structure. With the button further cash boxes can be added, depending on the licence. Cash boxes will be deleted with the button . After the selection of a cash box the configuration data of this are displayed. Below the buttons the current image of the camera assigned to this cash box is displayed.

Descriptive parameters

- Name
  Name of the camera. The camera is displayed in all dialogues with this name.
- Camera
  A camera can be assigned to several cash boxes but each cash box can only be assigned to one camera.

The recording frame rate of a cash-box camera should be set to a fixed value to ensure synchronisation of the cash-box and image data.
Please ensure that the relevant camera is able to reach the frame rate set.

- Debug
  With the button 

a further dialogue is opened displaying the cash box data. The following options are possible:
  - Cash
    - all cash boxes
    - selection of one cash box
  - Data
    - Raw
    - Codepage
    - Filtered

Changes at the filter settings become visible with the next incoming data.

Parameter

- Type
  Setting the type of cash box and/or printer.
- Interface
  Selection of the COM port to which the cash box or printer is connected. The following interface parameters can be set:
  - COM
  - Data rate
  - Data bits
  - Parity
  - Stop bits

Filter

New filters can be added to the filter list and/or all filters can be deleted with the buttons  and  . Individual filters are deleted in the filter list. Possible filter options:

- inactive

- Word filter/Line filter
  With the defined word- and/or line filters uninteresting data can be deleted from the data stream sent by the cash box.
  With a word filter all words are filtered, in which the filter occurs as sub stringer. A line filter removes a completely received line.
- Alarm trigger
  A defined alarm filter, generates an alarm, if the filter word occurs as sub-string in the received line. The filter is case sensitive.

3.3.19 Configuration of the multi-monitor mode

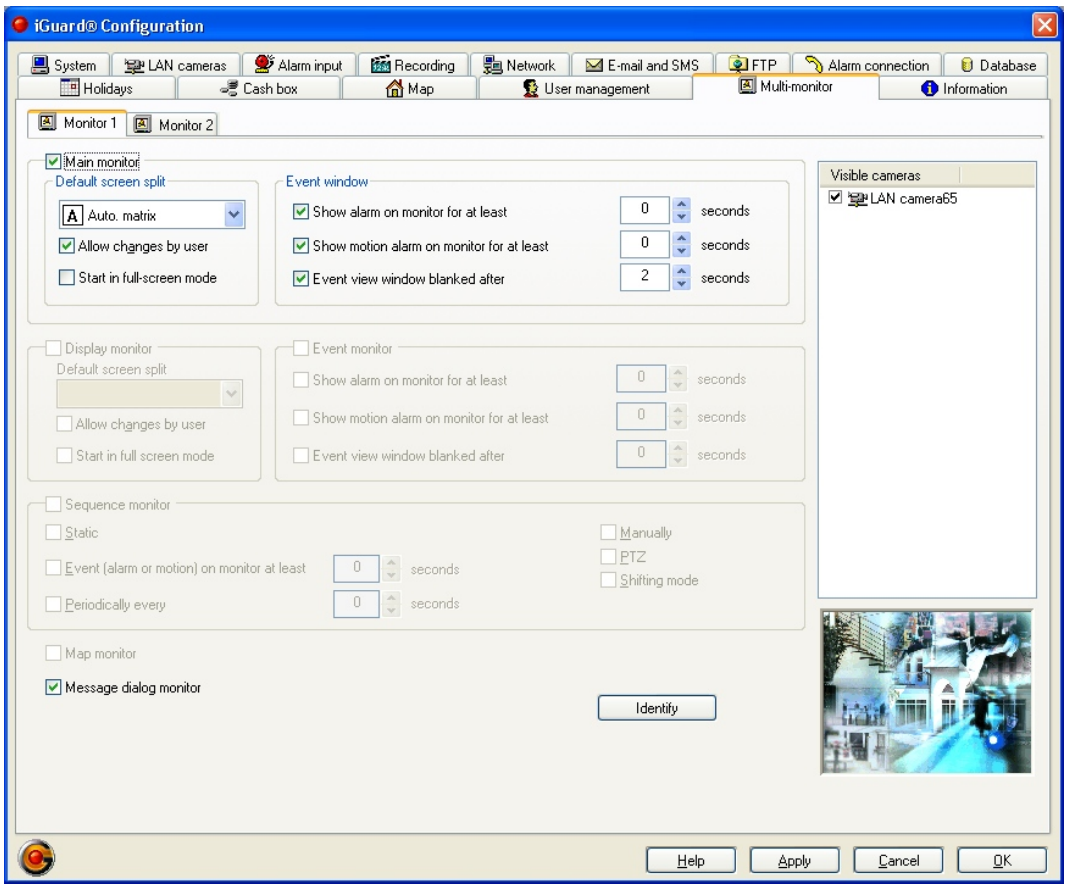


Figure 1: Configuration of the multi-monitor mode

In multi-monitor mode, *iGuard*® supports up to four monitors. The distribution of the monitors is configurable. In multi-monitor mode, the main monitor retains the same functionality as in single-monitor mode. Additional monitors can be configured for displaying camera images, map, event messages or as a sequence monitor for the event-dependent output of camera images.

Changes to *Default screen split* only become effective when *iGuard*® and *iGuard*® *RemoteView* are restarted.

Main monitor

The main monitor always shows the *iGuard*® menus, the login dialog, the rendering view and the task bar. The *iGuard*® configuration settings are implemented via this monitor. One monitor must be defined as the main monitor; other monitors are optional.

Default screen split 

A list box enables the user to specify the arrangement and number of camera windows to be displayed on the main monitor when the program starts up. If the option *Auto. matrix* is selected, all the configured cameras are displayed. If the option *No display* is used, no cameras are displayed as long as no login takes place.

- Allow changes by user
  If you wish to be able to change the window arrangement in split screen mode, the *Allow changes by user* option underneath must be checked. The corresponding buttons for switching between the different views are then active or inactive in split screen mode.
- Start in full-screen mode
  With this option you can specify whether *iGuard*® is to be started up in full-screen mode. You can also switch over to full-screen mode using the *CTRL and F* keys, the pop-up menu or *View → Full screen*. In this mode, the camera images are displayed without status bar, logbook and headline.

Event window
If one or multiple options are checked, the corresponding events are displayed as a window on the main monitor.

- Show alarm on monitor for at least … seconds
  Minimum duration for display of an alarm event. Alarm messages that come in during this time are not displayed. You can set a time of between 0 and 60 seconds. 0 seconds means that an alarm event window is immediately hidden when a new alarm comes in.
- Show motion alarm on monitor for … seconds
  Same setting option as for alarm event (see above).
- Event view window blackout … seconds
  Period of time after which the display of an event is blacked out. You can set a time of between 2 and 300 seconds.

Visible cameras
In the list of visible cameras, connected cameras can be selected for output to the relevant monitor.

Display monitor
Configuration of a monitor as the display monitor for the split display of live camera images. This selection option is only available when the monitor is not selected as the main monitor.
The setting options are identical to those for the main monitor (see above).

Event monitor
When selecting a monitor as the event monitor, this monitor is only used to display events.
The setting options are identical to those for the Event window (see above).

The Event window and Event monitor functions cannot be used simultaneously.

Sequence monitor
Configuration of a monitor as the sequence monitor for the event-dependent output of camera images.
This selection option is only available when the monitor is not selected as the main monitor.

- Static
  In this mode, one camera from the visible cameras list is permanently assigned to one monitor. It is therefore not possible to display another camera image on the connected monitor.
- Manually
  Checking this option enables the static assignment to be cancelled. In the display mode it is then possible to output another camera to this monitor via a pop-up menu. The pop-up menu is opened by clicking the corresponding camera window with the right-hand mouse button.
  If there is no manual assignment, the image of the configured camera is displayed.

Figure 76: Sequence monitor pop-up menu

- Event
  In this mode, no cameras can be assigned from the list of visible cameras. The system outputs the camera that has identified motion or the one for which the linked alarm input has been activated.
  The camera continues to be output for a certain period of time, even if another camera signals motion during this time. The output duration can be set using the parameter *Event view window blackout ... seconds* (see above).
- PTZ
  This option is used to output a camera to the monitor as soon as it is moved using PTZ control.
- Periodically every … seconds
  In the list of visible cameras, the user can select cameras to be output periodically. You can set a time of between 2 and 300 seconds for the camera to remain in the individual positions.
- Shifting mode
  In shifting mode, the current alarm is always shown on the first sequence monitor if several sequence monitors are connected. If a new alarm occurs, the alarm previously displayed on the first sequence monitor is shifted to the

second sequence monitor, and the new alarm is displayed on the first sequence monitor.
If this option is deactivated, alarms are shown on all connected sequence monitors simultaneously in the order of their occurrence.

Map monitor
This option is used to activate the relevant monitor for full-screen view of the map. Only one monitor can be used as the map monitor.

Message dialog monitor
This option is used to define the relevant monitor for displaying the message dialogs.

3.3.20 Information

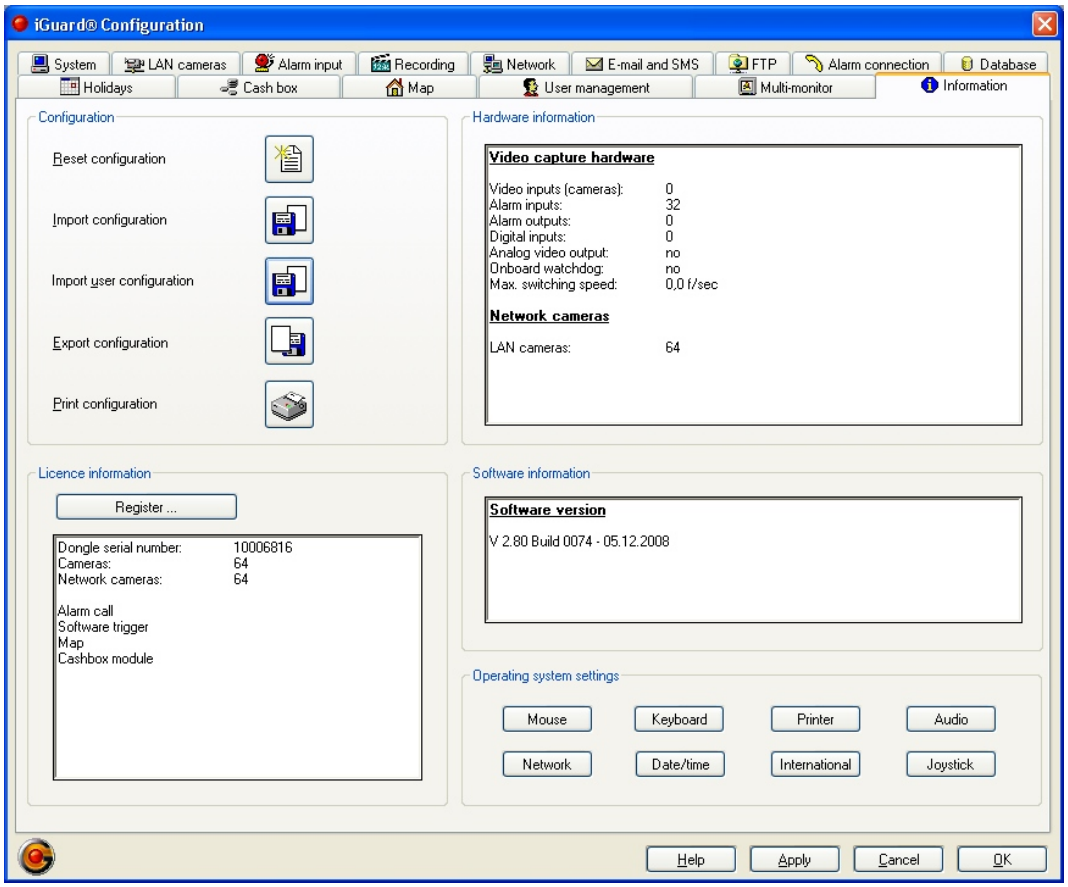


Figure 77: information

Configuration

- Reset configuration
  With this option the configuration of *iGuard*® is put back to the default parameters. Thereby all camera entrances are tested on applied video signals. If attached cameras are found, these are taken up to the configuration with standard parameters.
- Export configuration
  Save the *iGuard*® system configuration and the user configuration.
- Import configuration
  Load the *iGuard*® system settings.
- Import user configuration
  Load the user configuration. The current user configuration will be deleted and replaced by the new configuration. Because camera-referred rights are oriented at the system configuration imported users first get all camera-referred rights. Afterwards the user administrator must proof the rights.
- Print configuration
  The configuration can be printed out via the *Print configuration* button, e.g.

for purposes of archive entry or for plant documentation, on paper. The printout takes place in formatted text form without diagrams. It can contain several sides depending upon size of the configuration and the selected detailedness.

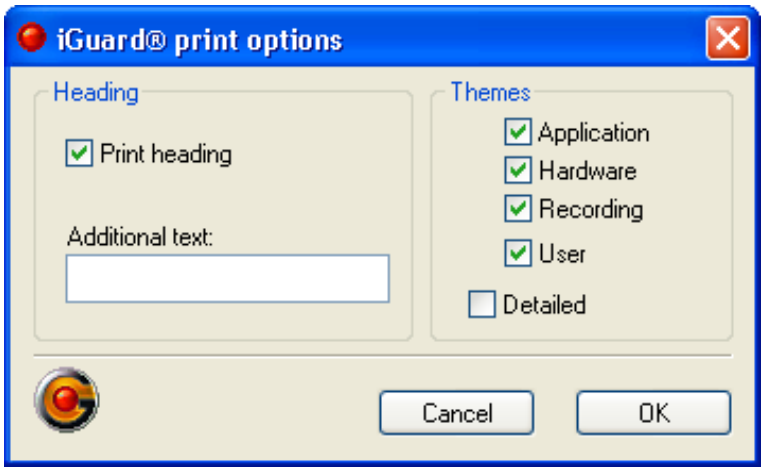


Figure 78: Printing options

- Heading
  A title page can be printed with an additional optional text of choice. The length of the text is limited on 64 characters.
- Themes
  Information to the specified topics can be printed out.
  ⇒ Application
  ⇒ Hardware
  ⇒ Recording
  ⇒ User
  ⇒ Detailed
  The printed parameters correspond to the associated configuration dialogs. With this option it is specified whether everything or only the most important information is to be printed.

Licence information
Information about the current activated licences. Using the button *Register* the licence dialog is opened (cp. *3.1.2 Licensing*).

Hardware information
In this field the technical details of the currently installed video capture hardware are listed.

Software information
The version information is stored in the configuration file. This means that *i-Guard® RemoteView* can also show the saved software version (server) of the saved configuration.

If you change the configuration of *iGuard®* by adding or removing from hard and/or software options, you receive a new enabling code, which you have to enter in the *iGuard®* registration dialog (see *3.1.2 Licensing*). Thus the new and/or changed options are enabled for the use in *iGuard®*.

Operating system settings
Over the buttons
- Mouse
- Keyboard
- Printer
- Audio
- Network
- Date/time
- International
- Joystick

the appropriate dialogues in the Windows systems management are opened. There attitudes and changes on system level can be made.

3.4 Playback mode

Analysis of the recorded video data is possible within the *playback mode*. It is based on an extremely powerful database and allows a quick and comfortable playback of occurred alarms or recorded events. Recorded video sequences or individual images can be searched by various methods. The search can be carried out using *iSearch*, the logbook (this contains all recorded incidents from the handling and current operation of *iGuard®*), the timeline display (see *3.4.8 Timeline*) or presetting of date and time.

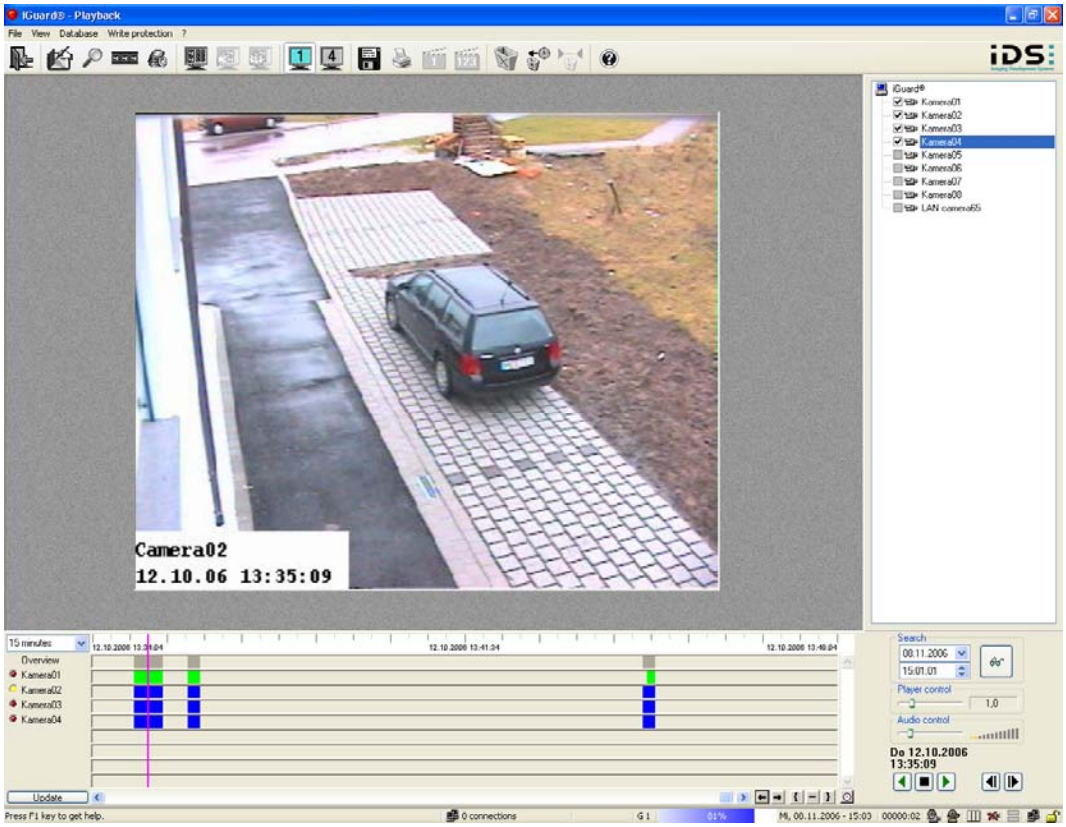


Figure 79: Playback mode

Playback mode can be started regardless of whether recording is running or not. Recording remains active even if *iGuard®* is in playback mode. Playback is possible both in *iGuard®* as well as per remote control using the *iGuard® RemoteView*.
The playback mode can be achieved in the display mode over **menu** *Administration → Playback* or the button in the symbol bar. For access to the playback mode *Playback* authorisation is necessary.

3.4.1 Menus in the playback mode

Pop-up menu

Figure 80: Rendering mode pop-up menu

In rendering mode, the "Rendering" pop-up menu can be called up by right-clicking the image:

- Play
  Starts the rendering.
- Play backwards
  Starts the rendering; the recording is played backwards.
- Stop
  Stops the rendering.
- Next image
  Jumps forward one frame in the recording.
- Previous image
  Jumps back one frame in the recording.
- Store position
  Stores the current rendering position.
- Jump to position
  Jumps to the stored rendering position.

- Set start position
  Stores the position as the start of a film sequence.
- Set end position
  Stores the position as the end of a film sequence.
- Print scene
  Opens the print dialog for printing the image currently displayed with additional information.
- Save scene
  Opens the save dialog for saving the image currently displayed in JPEG or BMP format (see also 3.4.14 Export of pictures).
- Save as video
  Opens the save dialog for saving the sequence marked using Set start position and Set end position as an AVI file (see also 3.4.15 Export of AVI-Files).
- Zoom interpolation
  Activates image interpolation for edge smoothing in scaled display.
- Hide frame information
  Shows/hides a status bar showing frame information underneath the frame.
- Hide frame data
  If cash box data on the current recording is available, this is shown/hidden in the frame.
- Show reference image
  Shows the reference image of the camera for which the recording is currently being rendered. A reference image can be created by clicking *Save reference image* in the dialogue *3.3.2 Configuration of the cameras*).

Menu File

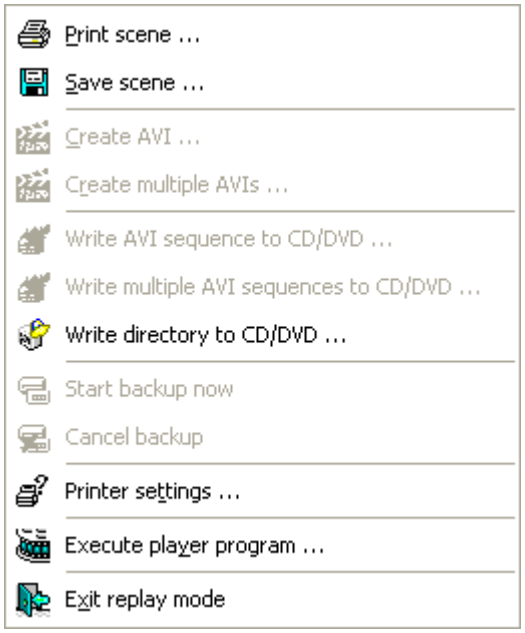


Figure 81: Playback mode – menu File

- Print scene
  In playback mode individual pictures can be printed out with *iGuard*® for further processing. Here always the picture is printed out, which is displayed in

the current window. The printout of a picture from the active camera window is started via the button  in the symbol bar.
The usual Windows® printer dialog only appears when *iGuard®* is started for the first time. Once the printer has been selected and printing has been confirmed the picture in question is then printed. Additional information is printed depending on the printing alignment. With upright format, the additional information is printed as text underneath the image. With horizontal format, the image is printed without additional information.
If changes are to be made later within the printer dialog, these can be carried out via the menu *Printer Set Up*.

- Save scene
  See 3.4.14 Export of pictures.
- Create AVI
  See 3.4.15 Export of AVI-Files.
- Create multiple AVIs
  See 3.4.15 Export of AVI-Files.
- Write AVI sequence to CD/DVD
  See 3.4.16 Export to CD/DVD.
- Write multiple AVI sequence to CD/DVD
  See 3.4.16 Export to CD/DVD.
- Write directory to CD/DVD
  See 3.4.16 Export to CD/DVD.
- Start backup now
  Usually a backup starts automatically at the preset time. With the option Start *backup now* an administrator can start a backup independently. This menu option is available only, if a backup is configured and currently no backup is running.
  The beginning and the end of a backup are logged. Errors, which arose during a backup (e.g. target drive is full) become also logged there.
- Cancel backup
  With this option an administrator can cancel a running backup. This option is only available if a backup is running.
- Printer settings
  Open dialog box *printer settings* for changes in the printer settings.
- Execute player program
  Start of the *iGuard® Player*. With this AVI files produced by *iGuard®* in the MJPEG format can be opened and played (see also *5 iGuard® Player*).
- Exit replay mode
  Exit playback mode, return to display mode.

Menu View

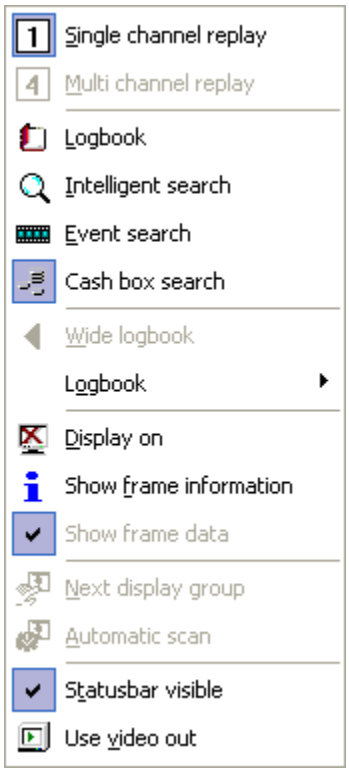


Figure 82: Playback mode – menu View

- Single channel replay
  Activate the single channel replay. Only one playback window is displayed.
- Multi channel replay
  Activate the multi channel replay (see also 3.4.12 Multi-channel playback). Display of 4 playback windows.
- Logbook
  Activate/deactivate the logbook.
- Intelligent search
  Activate/deactivate the intelligent search (see also 3.4.5 Search for changes in videos with iSearch).
- Event search
  Activate/deactivate the event search (see also 3.4.6 Event search).
- Cash box search
  Activate/deactivate the search mask (see also 3.4.7 Search cash box data).
- Wide/small logbook
  Change the width of the logbook display.
- Logbook
  Under this menu option a further menu opens which can also be opened over the context menu of the logbook.

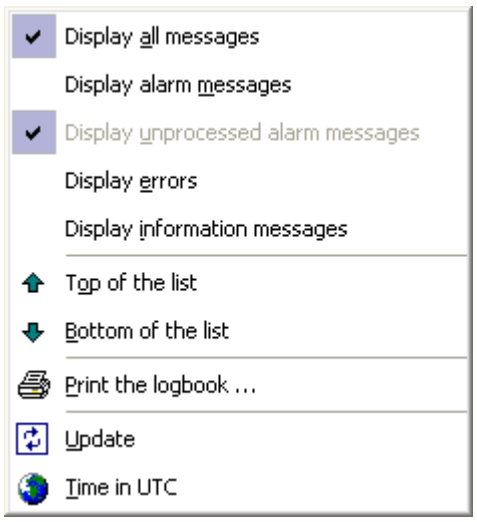


Figure 83: submenu Logbook

- ♦ Display all messages
  Log file entries are displayed non-filtered.
- ♦ Display alarm messages
  Only the entries of the alarm messages are displayed.
- ♦ Display unprocessed alarm messages
  Only unprocessed alarm messages from the logbook are displayed.
- ♦ Display errors
- ♦ Display information messages
- ♦ Top of the list
- ♦ Bottom of the list
- ♦ Print the logbook
- ♦ Update
- ♦ Local time/time in UTC

- Display on
  Change-over into triplex mode (see 3.4.13 Triplex mode).
- Show/Hide frame information
  The playback windows get an additional line at the lower image border, in which the file name and the frame number are shown. This additional line can be switched on/off global for all playback windows. The default setting is switched off.
  Alternatively the picture information can be switched on via the context menu of the playback windows.
- Show/Hide frame data
  If cashbox data are available, they can be displayed.
- Next display group
  Manual switch to the next group of cameras. See also Camera groups in chapter *3.2.7 Windows*.
- Automatic scan
  Automatic switch to the next group of cameras. See also Camera groups in chapter *3.2.7 Windows*.

- Status bar visible
  Switch on/off of the status bar.
- Use video out

Menu Database

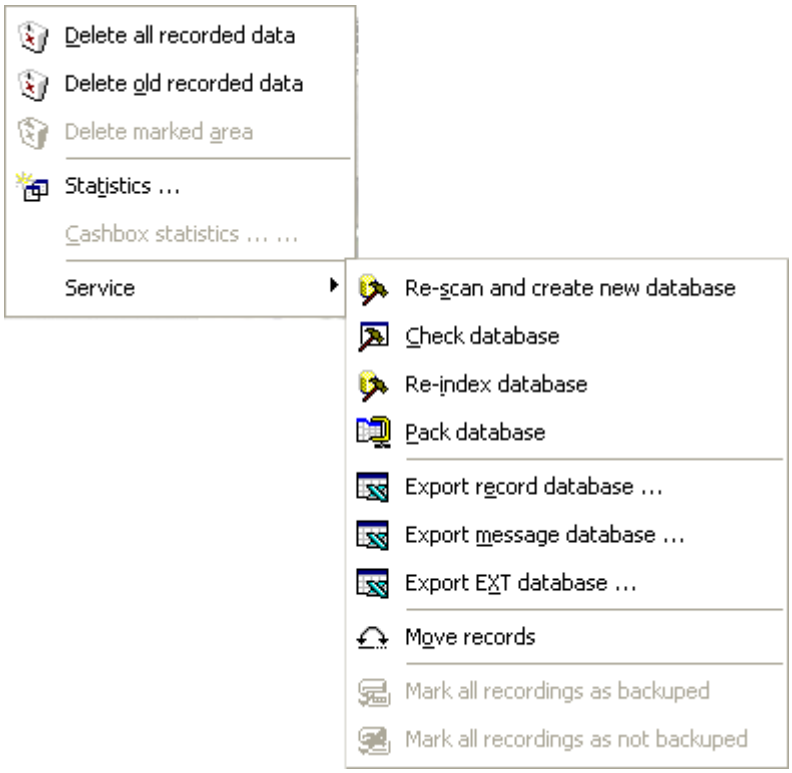


Figure 84: Playback mode – menu Database

- Delete all recorded data
  With this function all recordings are deleted. For this, like also with the other delete functions the right *Delete* is necessary.

The function *Delete All Recordings* is only possible when recording is stopped.

- Statistics

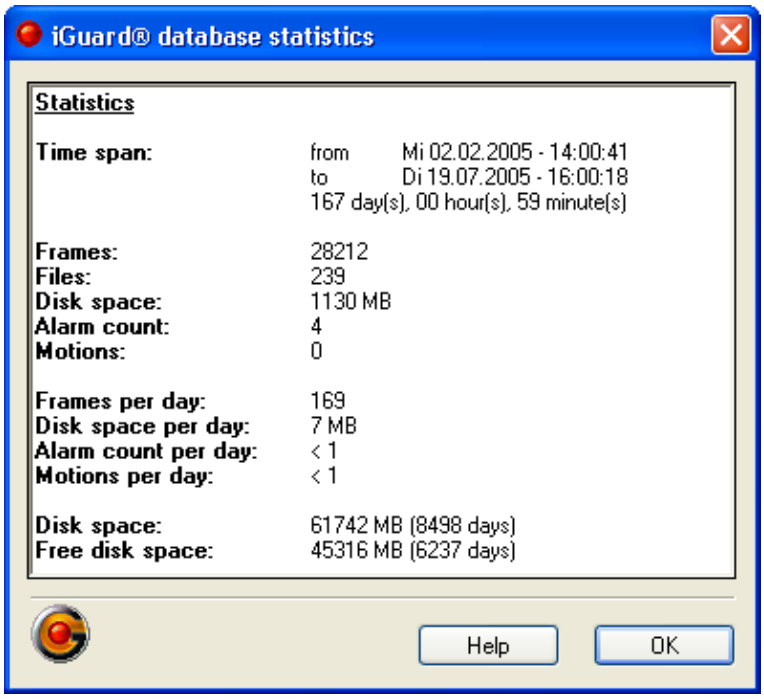


Figure 85: Database statistics

With the **menu** *Database → Statistics* the statistic of the database can be called. The following data ca be listed:

- Period of stored recordings. The point of start and end is displayed in days/hours/minutes.
- Number of stored images.
- Number of stored files.
- Hard disk space of all stored files. The actual space on the hard disk varies (it is larger) from this value. That is because:
  ⇒ in the image files is stored more than the pure images.
  ⇒ the configured size of the images will not be reached exactly.
  ⇒ the hard disk is divided into sections with a fixed size.
- Number of alarms which occurred in the defined period.
- Average number of images per day. If the period is < 1 day, a computer forecast takes place.
- Average amount of hard disk space per day. If the period is < 1 day, a computer forecast takes place. Limits as for all fields in common.
- Average amount of motions per day. If the period is < 1 day, a computer forecast takes place.
- Average amount of alarms per day. If the period is < 1 day, a computer forecast takes place.
- Complete estimated time for recording. Basis for the calculation is the daily amount of hard disk space and the amount of all hard disk space, which is available for recording.

- Cashbox statistics
  With this menu item a further dialog field is opened, in which the statistics of the cashbox database can be called up.

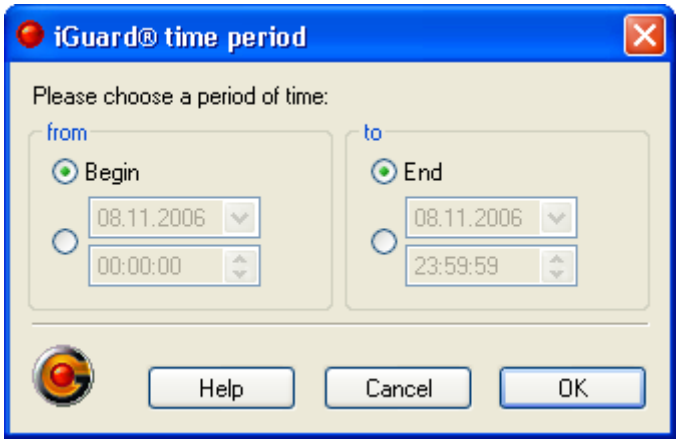


Figure 86: Cashbox statistics

- Service
  Under this menu item, users with administrator rights also have other processing functions at their disposal:
  - ♦ Re-scan and create new database
    Deletes the existing data base and provides on the basis of the available recordings a new data base.
  - ♦ Check database
    Check that entries are in place. With a negative result, the respective entries are deleted
  - ♦ Re-index database
  - ♦ Pack database
    Deletes physically previously deleted entries and thereby gains more space on the hard disc.
  - ♦ Export record database
    Exports video database as CSV-file.
  - ♦ Export message database
    Exports logbook as CSV-file.
  - ♦ Export ext. database
    Exports the database with user definied datas as CSV-file.
  - ♦ Move records
  - ♦ Mark all recordings as backuped
    See *Backup* in *3.3.13 Configuration of the database*.
  - ♦ Mark all recordings as not backuped

Menu Write protection

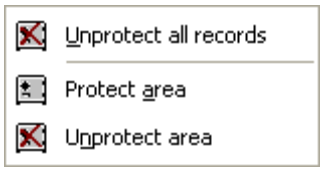


Figure 87: Playback mode – menu Write protection

Over the **menu** *Write protection* or the context menu of the timeline recordings can purposefully be provided with a writing protection and/or the protection can purposefully be waived again.

- Unprotect all records
- Protect area
  In order to protect an area, this must be marked in the timeline (see *3.4.8 Timeline*). A protected range is represented in the timeline with an additional yellow bar.
  This function is available in *iGuard® RemoteView* too.

If an event occurred, the concerned recordings can be protected remotely, so that these are not automatically deleted or overwritten, if the evaluation of the recordings can not take place immediately.

- Unprotect area
  Release protected and marked area.

Help (?)

Figure 88: Playback mode – menu Help

- Help
  By selection of the menu item *Help iGuard®* help is opened.
- Technical support (optional)
  This menu item opens a window with notes for the technical support.
- Info about *iGuard®*
  Over this menu item the *iGuard®* info dialog is opened

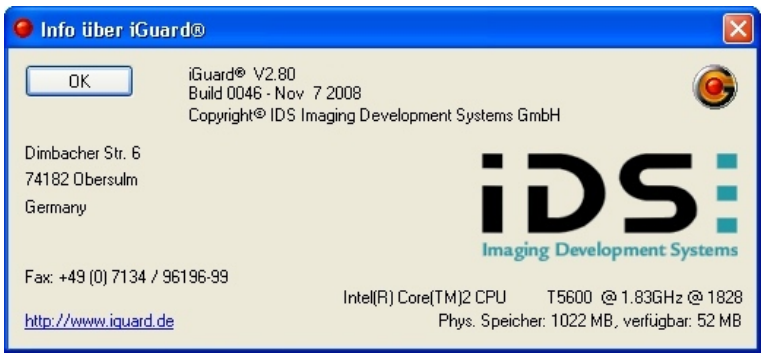


Figure 89: iGuard® Info

3.4.2 Symbol bar in playback mode

Symbol	Description
	Exit playback mode, return to display mode
	Activate/deactivate logbook
	Activate/deactivate intelligent search
	Activate/deactivate event search
	Display cash box search controls
	Activate/deactivate live image
	Next group
	Automatic cycle of the groups
	Single playback mode
	Multi playback mode
	Save scene
	Print scene
	Export video sequence of the marked camera from the indicated range.
	Export video sequence of all cameras from the indicated range.
	Delete all entries


Delete all oder entries


Delete recordings of the marked area


Open *iGuard*® help

3.4.3 Status bar in playback mode

The status bar in the playback mode corresponds to the status bar in the display mode (see *3.2.6 Status bar*).

3.4.4 Logbook

All relevant messages arising from operation such as for instance alarm messages, starting and stopping of recording, user login/logout, errors etc. are recorded in a logbook. The logbook can be activated or deactivated via the button  or the by the **menu** *Display → Logbook*. The Display is at the bottom right of the screen.
When the logbook is displayed, all messages are displayed, with the most recent of all always at the top of the list. All messages are always given with date and time (hh:mm). Small symbols in front of the messages indicate the message type.


Alarm info


Alarm input


User error


User logout


User


Application terminated


Record deleted


Crawled alarm


Crawled motion alarm


Crawled hold-up alarm


User message


Motion alarm


Disk error


Disk ok


Disk


Printing


End of the record


Error


Export


Info


Loss camera


Sabotage


Camera OK/Sabotage OK


Configuration


Long-time recording


Mail/SMS error


Mail/SMS


Manual recording


Test alarm


Fatal error


Start of the application


Stop of the application


Hold-up alarm


Connection error


Connection terminated


Connection


Suspicion alarm


Playback

All alarms are recorded insofar as the option *Log book entry* has been selected during configuration of the recording (cp. *3.3.8 Configuration of the recording*). To simplify the revision, different entries may be combined by a filter according to the message type and/or period. Filtering according to the message type is carried out by selecting a type of messages from a list shown in the context-menu of the logbook. The default setting is that when the playback dialog is called up all alarm messages from the entire period of the saved recordings are displayed.

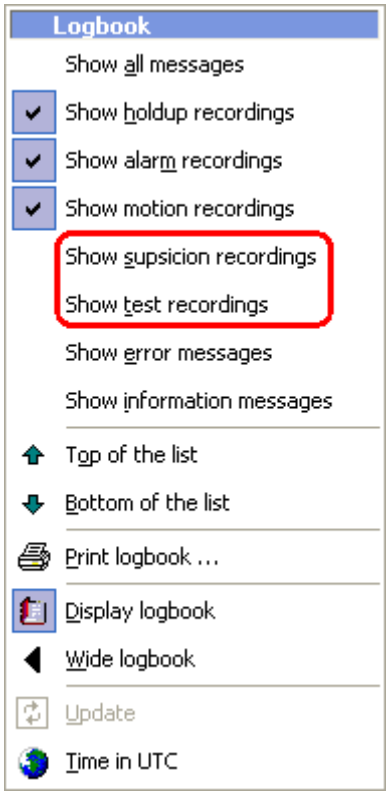


Figure 90: Logbook – context menu

In the banking mode the filtering options are supplemented about two further:

- Show suspicion recordings
- Show test recordings

Having selected a period or time interval for messages, it is now possible to access the respective video data directly. This is done by selecting entries within the *logbook* field using the mouse or the keyboard. *iGuard®* then automatically shows all involved cameras for the selected entry in the *cameras* field. Having selected the required camera, its camera picture is shown in the display field at the start of a ring recording or the respective alarm image at the start of an alarm recording.

Log book-based searching is a further aid to finding one's way round. Double click the left mouse button on an alarm entry in the log book or in a track of the timeline and the current window allocation in multi-replay is cancelled and the alarm (double click in log book) or the time line track-related camera is set in the upper left window.

As soon as a user has called up an image of an alarm sequence, this alarm is marked as sighted. Sighted alarms are marked in the log book by a separate symbol. Using an appropriate log book filter, it is possible to only display the non-sighted alarms.

Further functions of the context menu
Beside the filter functions still further functionalities are available over the context menu:

- Top of the list
- Bottom of the list
- Print logbook
- Display logbook
  Activates/deactivates the logbook display
- Wide/small logbook
  Change the width of the logbook display
- Update
- Local time/time in UTC

3.4.5 Search for changes in videos with iSearch

The iSearch dialog is opened over the **menu** *View → Intelligent search* or the button  in the symbol bar.
With iSearch can be purposefully searched for frame changes in stored recordings. The search relates to the marked camera with multi-channel reproduction and/or to the displayed camera with single camera reproduction.
In *iSearch* a small picture of the active camera is displayed (copy). Using the mouse and the draw functions known from the configuration of motion detection, the user can now draw a mask. *Rectangle* and *polygon* are available as draw functions. In addition, there is a button for deleting the mask.
If no mask is defined, the complete frame is called up for the search.

Figure 91: iSearch dialog

The sensitivity of the search can defined as well as the step-width (speed) of the search. The step-width stipulates whether each frame is to be scanned during the search or whether frames should be skipped. Because frames have to be read out of the video file and decompressed before evaluation can take place, a fine search can take a very great deal of time. With the normal step-width, not every frame is evaluated. The search is faster but short movements may be overlooked.

A click on the button  starts the search. A search always takes place in forward direction, i.e. from an older to a newer point in time. A reverse (backwards) search is not possible. The search can only be started if play is not running and if a starting point has already been entered (a recording frame is displayed in the active window).
A progress display provides information about search status. The progress bar can make a large jump at the start of the search depending on the type of system. A display of the expected remaining time for the search is not possible.

If the search was successful, the frame found is displayed. The respective point in time is marked in the timeline (see *3.4.8 Timeline*). With multi channel replay, the other cameras show their frames closest to that point in time.
If no frame change is found, the message *No frame found* is displayed at bottom right.
The search is always carried out at the server. This is why a search can also be carried out without problem via an ISDN connection using *iGuard® RemoteView*. The search, however, is a burden on the server.
As the server can only carry out one search at a time, in multi client operating mode the search will not start if another user is already carrying out a search. An error message is displayed.

3.4.6 Event search

The event search is activated over the **menu** *View* → *Event search* or the switching surface in the symbol border.

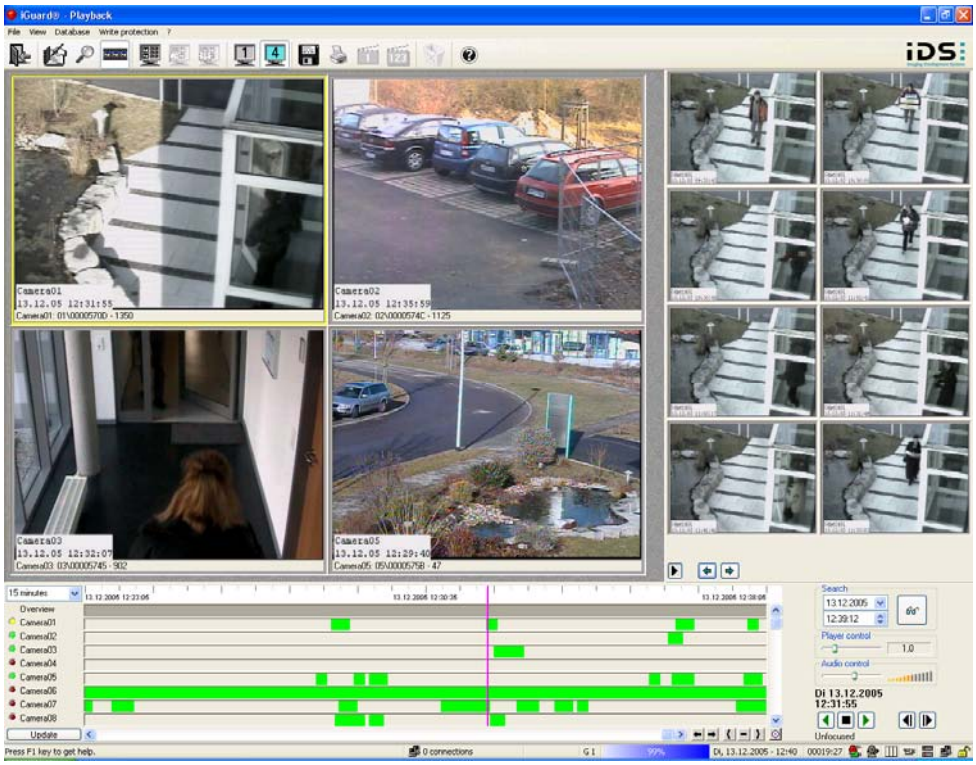


Figure 92: Event search

As soon as the event search was activated, the events are displayed in small preview pictures. Over the context menu of the event search displaying the events can be filtered.

Figure 93: Context menu of the event search

The selection of an event effected through clicking the appropriate preview picture. The time line is set automatically on the correct time. With the buttons and can be navigated within the events.

3.4.7 Search cash box data

The search for cash box data is activated over the menu View → Cash box search or the button in the symbol bar.

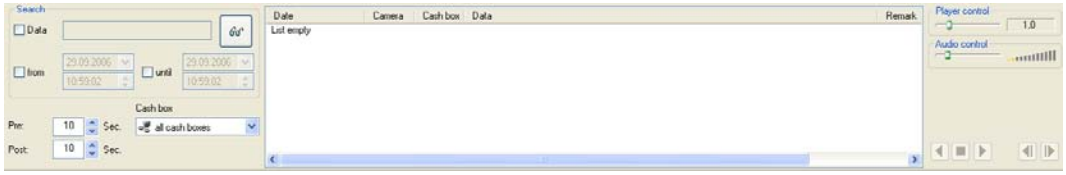


Figure 94: Search mask cash box data

The following options are possible for the search and playback of cash box data:

- Specification of a period, in which is to be searched for (from, to). Open beginning and open end are possible.
- Specification of search criteria as freely definable text (substring search). The search is case insensitive. An indication of 2 search words separated by a comma is permissible. In this case only such search results are displayed, in which both substrings occur. A search with wildcards is possible.
- Specification of the cash box from which the data must come. The option *all* or an individual cash box specified by name is possible.

The search result is listed in a table and can be selected. A selected entry will be played back minus an adjustable offset and an adjustable post-trigger duration. At the end of the post-trigger duration the next entry of the table will be opened and the pictures with consideration of the pre-trigger will be replayed. The current shown table entry is marked.
The data, which were stored to a picture, are displayed in the picture.
Frames can be exported as jpg or bmp files. The associated cash data are exported in a text file (ASCII), which has the same file name and the ending .txt.
Further the possibility exists of printing out a picture with text below the picture.

3.4.8 Timeline

The timeline display is a graphic display of the recorded images per camera over a time axis.
A maximum of one overview track plus 8 further tracks can be viewed simultaneously. The overview track shows all stored recordings of each camera within the time line. The overview track makes it possible to see whether a recording exists from a camera that is not currently supplying an image. The camera names are ordered alphabetical.

The display is scaled over the set time period. Periods themselves can be set in several stages (see popup-menu above camera list). With the setting *Overall duration* the complete period of all stored recordings is shown.

Figure 95: Timeline – setting of the periods

Each field of the diagram describes a time window of greater or smaller size depending on the set time range. Clicking with the left mouse key on a field provides the corresponding image. In this case, *iGuard®* seeks an image that was recorded at the start of the time period described by the selected field. If no image has been stored at that time, *iGuard®* searches for an image that is as close as possible to the required time (marking *out of focus* at bottom right edge). Slight inaccuracies are possible when clicking on a field depending on the resolution and selected time range.
The actual displayed time is marked in the diagram by a vertical line (colour: magenta). The configuration of the current display can be rearranged using the button *Update* at bottom left.
The corresponding fields of the diagram are also marked in colour during recording (no marking = no recording). Colour marking is differentiated as follows:

- **Blue:** image recording (at least 1 image) has taken place in the time window defined by this field / Pre-trigger phase (cf. *3.3.8 Configuration of the recording*)
- **Green:** as blue, though with movement detection instead / Post-trigger phase (cf. *3.3.8 Configuration of the recording*)
- **Red:** at least 1 alarm image has been recorded
- **Orange:** Hold-up (cf. *3.3.8 Configuration of the recording*)
- **Light blue:** Test recording (only with activated banking mode, see also *3.3.14 Banking (optional)*)
- **Purple:** Suspicion recording (only with activated banking mode, see also *3.3.14 Banking (optional)*)
- **Dark grey:** Cash box data
- **Yellow:** Write protected records (shown as additional line)
- **Dark green:** Audio data (shown as additional line)
- **Black:** User data (shown as additional line)

A click with the left mouse key and dragging the mouse to the right or left while holding the mouse key pressed causes so-called "scratching". This means that during the movement, the display always shows the image corresponding to the actual mouse position and therefore to the current moment in time.

Scratching is only possible locally on the *iGuard®* recording computer (server), not using *iGuard® RemoteView*.

If the right mouse button is clicked in the timeline, a square opens up. The size of this square can be altered with the mouse while holding the right mouse button pressed. This square is used to mark a time range. A context-menu is displayed when the right mouse button is released. With this menu, the user can define which functions are applied to the marked range.

Figure 96: Timeline – context menu

For a already marked range the following functions are available for selection:

- Enlarge section
  The option *Enlarge section* is only possible if the finest setting *3 minutes* has not already been selected.
- Mark range
- Create AVI sequence (relating to the selected camera)
- Create multiple AVI sequences (related to all selected cameras)
- Write AVI sequence to CD/DVD (relating to the selected camera)
- Write multiple AVI sequences to CD/DVD (relating to all selected cameras)
- Protect area
- Unprotect area)

When zooming (enlarge section) in the timeline, *iGuard®* selects the appropriate time range which is the iterative closest to the selected time range from the available stages. The selected range is displayed centrally.

Marking

Marking in the timeline is also possible with the following buttons: **{** **-** **}**
Click in the timeline the starting point of the range to be chosen and then **{**, afterwards the final point of the area and then **}**. The margins are removed with the button **-**.

Leaping

Using the button on the right alongside you can leap to the current time (which is marked by the magenta-coloured vertical line). This button is only active if it is possible to scroll horizontally in the timeline, i.e. if the time range cur-

rently being displayed according to the setting stage (see above) does not comply completely with the length of the time range which had actually been saved. Furthermore, you can use the arrow buttons alongside ⬅ ➡ to leap to the beginning/end of the recording.

Capturing
Click on a moment in the timeline where there are no recordings and the marking leaps to a point with existing recordings which is as close as possible to the required moment in time. The set views then show accordingly the images from that point in time.

Deleting
The symbol bar offers three options for deleting recordings shown in the timeline:


All recordings displayed in the timeline will be deleted (only possible with stopped recording).


Only the range before a point of time clicked in the timeline will be deleted.


Only a marked range will be deleted.

Deletion of ranges and traces is not possible in the timeline if the optional banking mode is activated.

3.4.9 Database scan

To the right of the timeline you can start a database query by specifying a date and time. *iGuard*® then shows from the selected camera the image which is the closed to the specified time.
With inserted logbook (see *3.4.4 Logbook*), the corresponding event is marked for each displayed image. If an entry is selected in the logbook, the system shows from the selected camera the first image that belongs to the selected event.

3.4.10 Audio playback

Audio playback is only possible locally on the server or when evaluating exchangeable discs with *iGuard*® RemoteView as well. Audio playback take place automatically when the following conditions have been fulfilled:

- Only one camera channel is displayed. Multi-channel playback (more than 1 camera at the same time) is not possible with audio
- The playback speed is set to 1.
- Playback is forwards (not reverse).
- The computer has a compatible sound system (sound card) installed for playback and the drivers of the sound card are correctly installed.
- A *FALCONquattro* frame grabber must not run in recording mode (recording stopped)

If an audio playback is taking place, a loudspeaker symbol is displayed between the playback control elements to signal this.

Figure 97: Playback symbol bar with speaker symbol

The following should be checked if there is no sound despite the loudspeaker symbol being displayed:

- Are the system's volume regulator (mixer) and possibly the hardware (loudspeaker, amplifier) turned up?
- Is the mixer for playback set correctly?
- Cable connections (sound card to loudspeaker or headphones) OK?
- Was anything audible during recording?

The timeline shows an dark green line in the lower section of the camera track if audio is being recorded along with images. Sound reproduction is synchronised to video playback to a certain extent. Absolute synchronisation is never possible because the sound card and the frame grabber record separately from each other.
Extreme system operating conditions can also result in serious image-sound displacement or not all frames are shown (dropped frames) during playback.
The volume during the rendition is adjustable over the sliding control in the field *Audio control*.

Figure 98: Adjust the volume

3.4.11 Recorder control

After from the timeline (see) a date or from the logbook (see *3.4.4 Logbook*) an event and a pertinent camera was selected with the mouse, the video sequence can be played back with the help of various playback keys.
After a date have been selected with the mouse from the timeline or an occurrence from the logbook and a corresponding camera, a video sequence can be played back using various playback keys. Possible functions are:

 Forward

 Reverse

 Stop playback

 Frame forward

 Frame back

The playback speed can set by the sliding control in the field *Player control*.

Figure 99: Adjust the playback speed

3.4.12 Multi-channel playback

Images from several individually selectable cameras can be displayed at the same time using multi channel playback. A maximum of 4 cameras can be viewed parallel.
Cameras are assigned to playback windows by clicking a window, which is then highlighted. Then assign a camera from the list of cameras shown in the time-line to the selected window by clicking. You cannot assign one camera to sev-eral playback windows. If a camera is already assigned to a different playback window, it is reassigned to the newly selected window.

Figure 100: Camera overview in the timeline

If no camera has been assigned to a window at the start of playback, *iGuard®* will automatically assign the first 4 cameras to the playback windows.

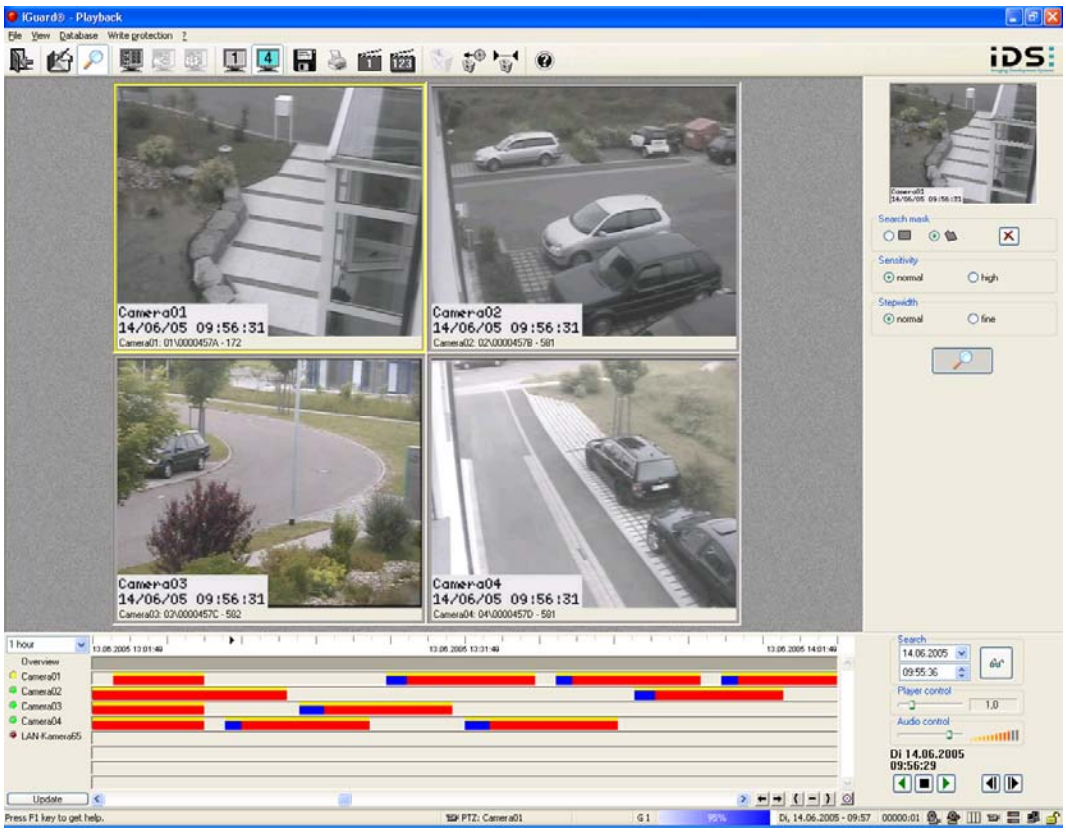


Figure 101: Multi-channel playback with activated iSearch

There is always one active playback window which is highlighted by marking (yellow surround). The following commands only relate to the marked playback window:

- Print
- Save
- Generate AVI sequence
- Assign a camera
- iSearch

When switching multi-channel to single channel playback the marked window is displayed in the single channel playback.
The settings and assignments are saved so that the cameras are assigned again to the already designated windows the next time playback is selected. This does not apply, however, to *iGuard® RemoteView* because in this case a different server and therefore a different camera configuration could exist with each connection.

3.4.13 Triplex mode

Triplex mode means that recording, playback and display of live images is possible simultaneously.

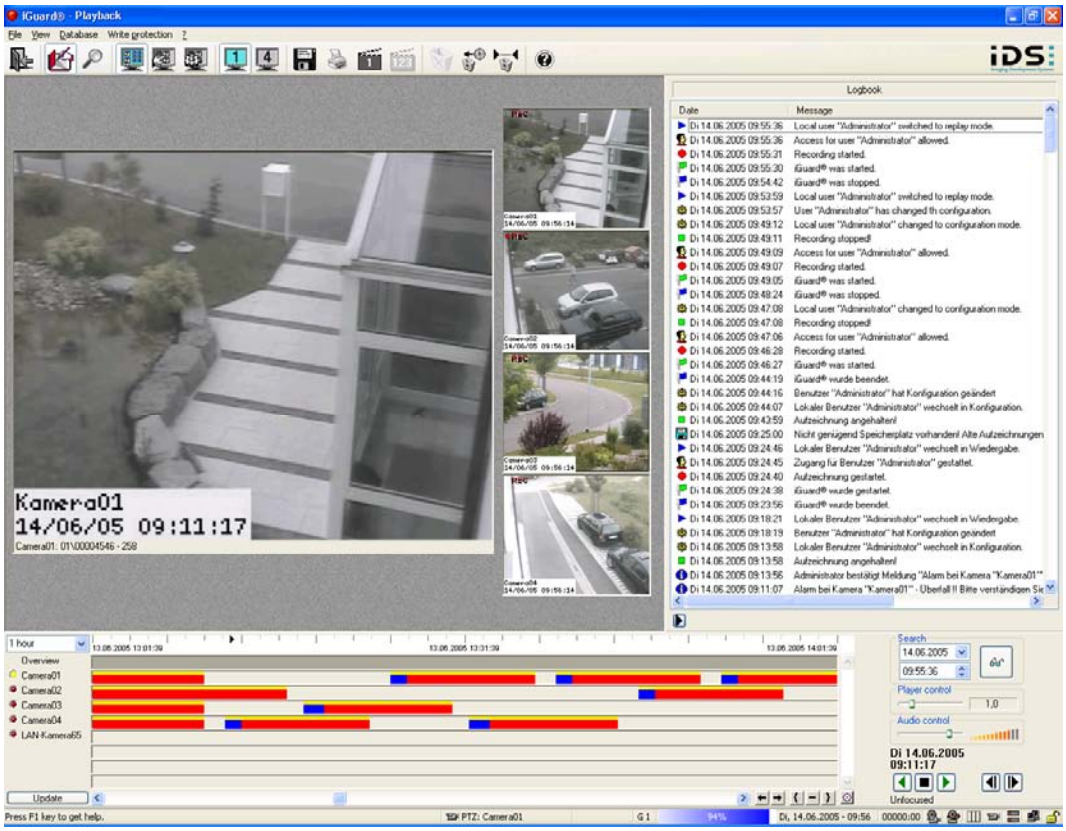


Figure 102: Triplex mode at playback level

The display of live images at playback level mode must be switched on over the *menu View → Display on.* The setting is stored (though not user-related). Live images are displayed flush left of the logbook in a column. Image size is restricted to QCIF format and cannot be changed. Zooming (cf. *3.4.17 Zooming*) is not possible. The number of displayed cameras depends on the VGA resolution of the system and the unblanked area of the logbook. With a resolution of 1024x768, 3 cameras are displayed (without logbook 6 cameras), with a resolution of 1600x1200 6 cameras (without logbook 12 cameras). If there are more cameras than can be displayed, cameras groups are formed as on the monitor level. Switching over from one camera group to another is then carried out manually or automatically in the same way as on the monitor level (**menu** *View → Next display group*; *View → Start camera scan).*

3.4.14 Export of pictures

Further opportunities for processing the video recordings are provided by saving the pictures under another name. For this export of pictures the button has to be pressed in the *Output* field.
iGuard® also offers the opportunity to save the picture in JPG as well as BMP format. As it is the case when pictures are printed out, it is the picture currently being displayed which is exported.

Exporting one picture requires considerably more storage space than this needs within recording of picture sequences. This is because the picture is saved as a complete picture (768 x 576 pixels (PAL)) - and not as a ¼ picture (384 x 288 pixels) in case of normal resolution or a ½ picture (768 x 288 pixels) in case of high resolution.

3.4.15 Export of AVI-Files

An export of linked video sequences is also possible as AVI file with *iGuard®*. The export is activated over the **menu** *File → Create AVI or File → Create multiple AVIs* (see *3.4.1 Menus in the playback mode*). Alternatively the export can be activated also over the Symbol bar (see *3.4.2 Symbol bar in playback mode*).
For the AVI export a time range must be marked in the timeline (Cut In and Cut Out at the bottom right edge of the timeline) display and a camera must be selected.
Exported AVI files are provided with a signature (watermark). This allows an appraisal of the exported data with regard to existing manipulation. The signature is evaluated when the video data is played using the iGuard® Player (see *5.8 Checking signature file*).

Generating individual film sequences
Using the menu *File → Generate film sequence* function in the or corresponding symbol in the symbol bar, the user can enter a file name and a directory where the film sequence is to be written.

Generating multiple film sequences
In multiple export, the AVI sequences of the currently displayed cameras (up to four) can be exported simultaneously. With multiple export, the user selects a directory where the exported AVI sequences are to be stored, specifies the max. permitted file size and stipulates a base file name.
The base file name is automatically extended by "_xxxxxxxx" by the system, whereby "xxxxxxxx" stands for the name of the camera.
A multiple export via *iGuard® RemoteView* is also possible insofar as the connected server supports multiple export (i.e. as of server version 2.45). If not, *iGuard® RemoteView* does not offer the option of *Generate multiple film sequences*.
It is also possible to generate a CD/DVD with all exported sequences (see *3.4.16 Export to CD/DVD*).

With the export of AVI files the corresponding sound tracks are exported likewise. Video recordings with sound are characterized in the timeline by an additional dark-green bar (see also *3.4.8 Timeline*).

3.4.16 Export to CD/DVD

Exported image sequences can now also be stored direct on a CD-R, CD-RW, DVD-R, DVD-RW, DVD+R, DVD+RW or DVD-RAM.
A precondition for this is that the user has suitable hardware (writer) and the appropriate Nero Version 6.0 software. *iGuard®* makes direct use of the functions of the Nero 6.0 writer software. Writer support by *iGuard®* is not possible without the installation of Nero 6.0, even though appropriate hardware has been installed.
Appropriate menus are displayed at the replay level if *iGuard®* has detected a CD or DVD writer through Nero 6.0 (see *3.4.1 Menus in the playback mode*).
As *iGuard®* uses Nero 6.0 as writer software, all other writers supported by Nero are also included. If the writer being used is not supported, appropriate updates for Nero should be obtained from the manufacturer via the website *www.ahead.de*. Please send any queries you may have regarding the support of specific writers to that address as well.
An important feature of the *iGuard®* is the possibility of automatically requesting several blank discs one after the other if more image sequences are to be written to disc than would fit on one blank. When generating AVI sequences, *iGuard®* does not check whether the generated sequence fit onto one disc. We recommend always having an adequate number of CD/DVD blank discs available.

RW blank discs must not be formatted. *iGuard®* does not use any packet writing. It is possible to delete RW media with *iGuard®*.

For safety reasons, *iGuard®* generally writes at max. 8x CD speed. If the writing speed is too high, the CD writer requires too many system resources which can lead to a breakdown in the recording frame rate with *iGuard®* or in extreme cases to watchdog errors of the recording hardware.
iGuard® supports writing of several sessions. For this reason, iGuard® writes exclusively in multi-session format and never closes sessions. There is a possibility of errors in reading the media if using older CD-ROM drives that are not able to support this format.
If there are already files on the CD or DVD with the same name as the those to be added, *iGuard®* will not overwrite the existing files. Instead, the new files will be provided with a name suffix "_$xxx" whereby "xxx" stands for a serial number commencing with "000".
iGuard® automatically writes the *iGuard® Player* (igdplay.exe) onto each CD or DVD. This cannot be prevented by the user. The iGuard® player enables exported sequences to be played back on any Windows®-PC. *iGuard®* offers 2 possibilities for writing files to CD/DVD:

- Write all files of a directory to CD/DVD
- Export film sequences direct to CD/DVD

The **menu** *File* in the playback mode contains three entries, which have to do with CD/DVD drives (see *3.4.1 Menus in the playback mode*). These menus are only visible if the above-named points are fulfilled.

- Write AVI sequence to CD/DVD
- Write multiple AVI sequences to CD/DVD
- Write directory to CD/DVD

Writing film sequences to CD/DVD
The operation of this function corresponds with the previous export of a film sequence with the difference that following the export of the files (which are always written to the hard-disc first), the files are written to disc and then deleted. The period marked in the timeline is exported from the active camera (yellow surround). This function can also be called up using the context menu of the timeline.
iGuard® automatically requests additional discs if the exported film sequence is too large to fit on one disc.
This function is not available with *iGuard® RemoteView* with an online connection. This function is possible with *iGuard® RemoteView* if replaying from an interchangeable hard-disc.

Writing multiple film sequences to CD/DVD
Several film sequences from all marked cameras (max. 4 cameras) are generated and written to CD/DVD immediately. *iGuard®* automatically requests additional discs if the exported film sequence is too large to fit on one disc.

This function can also be called up using the context menu of the timeline.
This function is not available with *iGuard® RemoteView* with an online connection. This function is possible with *iGuard® RemoteView* if replaying from an interchangeable hard-disk.

Writing directory to CD/DVD
The user has to select a directory. All files that are in that directory are written to disc. Further discs are automatically requested if the size of the medium is not large enough.
The user can stipulate whether the written files should be deleted after being written to disc.
A special dialog is visible during the writing process. This prompts the user for further action or displays the progress of the writing process:

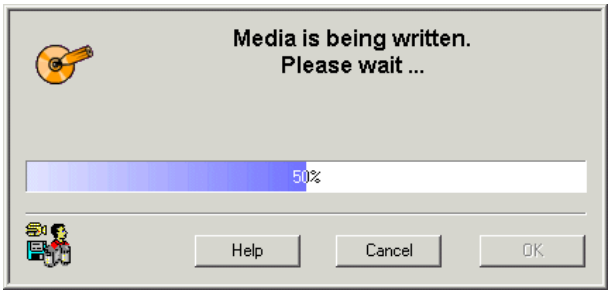


Figure 103: CD/DVD writing process

The function *Write directory to CD/DVD* can be used, for example, if several AVI exports are necessary from one directory (exporting several cameras or different periods).
This function is also available with *iGuard® RemoteView*.

3.4.17 Zooming

In order to recognise details better in cases of doubt when revising the images, it is possible to zoom in within a displayed picture. This is done by drawing a window with the left mouse button around the area to be enlarged (Zoom In). The pictured area will then appear within the window. There is also the additional option of pressing the right mouse button in the picture window to switch into or out of the *Zoom-interpolation* function (context-menu). For strong zoom, this improves the picture quality. Zooming is also possible during the playback of a video sequence. By clicking the left mouse button within the window the image will return to its original size (Zoom Out).

The level of detail available when zooming depends on the recorded image size, as the area to be enlarged is always relative to the original image size.

3.4.18 Reference image on replay

In all playback modes the reference image of the appropriate camera can be opened during the playback. Thus the display window of the recorded scene can be compared with that of the reference image. Through a click to the right mouse button in the playback image the context menu is displayed. Over the menu entry *Reference image* the reference image will be displayed in a new window opened.

Figure 104: Context menu in playback mode

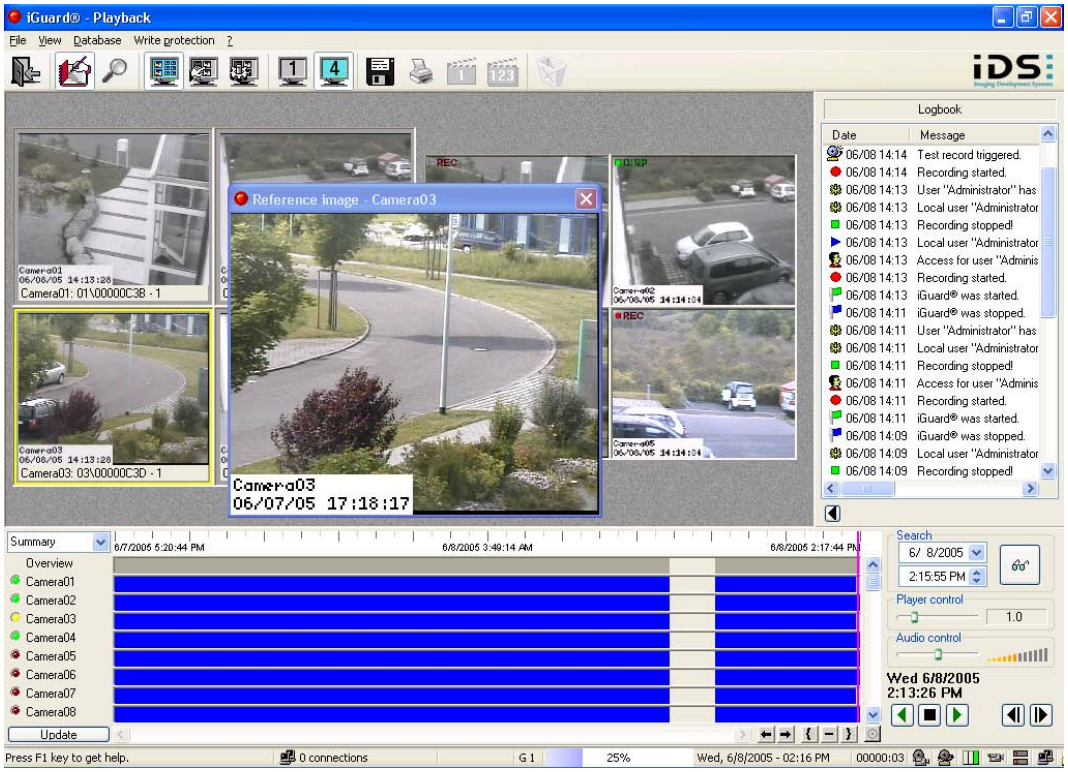


Figure 105: Reference image at replay

4 iGuard® RemoteView

4.1 Functionality

iGuard® RemoteView offers the opportunity for easy revision of video sequences by remote access. *iGuard®* here functions as a server, with *iGuard® RemoteView* as the client. This enables to carry out the revision independently of place, as long as the *iGuard®*-system is running and also the PC intended for the revision are networked. Finally a connection via LAN or ISDN to the *iGuard®*-system is running is then required.
Another option is to use *iGuard® RemoteView* to revise databases without the requirement for a direct connection to the *iGuard®*-system. To do so it is necessary to have the two databases, Record- and Message Database, available. This enables to operate iGuard® with removable hard discs, which can then be locally revised using iGuard® RemoteView.
This is made possible by operating *iGuard®* with removable hard disks, which then can be evaluated locally with *iGuard® RemoteView*.

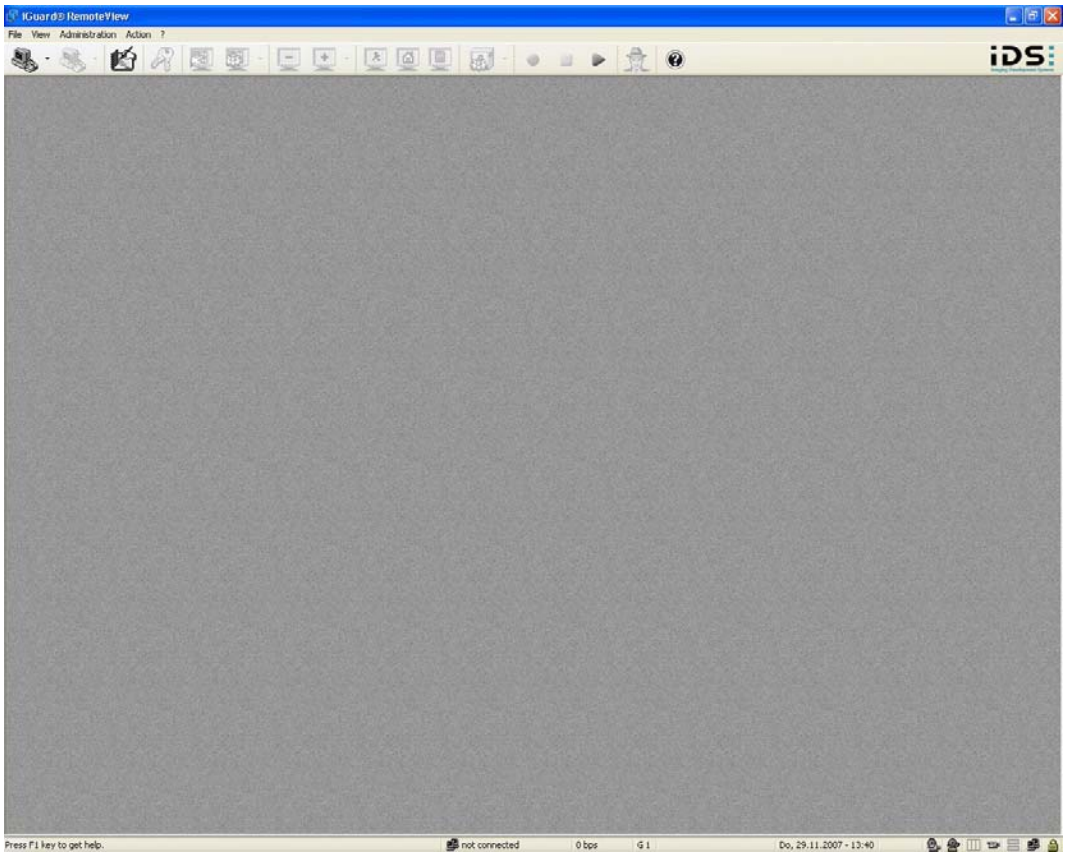


Figure 106: iGuard® RemoteView

After starting *iGuard® RemoteView*, the window displayed above will appear. This is similar in appearance and function, in reduced form, to that of i*Guard®*. Buttons with the same functions have in *iGuard® RemoteView* the same appearance as in *iGuard®*.

After starting up *iGuard® RemoteView*, you must log in in order to perform further actions or close the program.

iGuard® RemoteView can receive an alarm output even without user login.

4.1.1 Logging into the system

You can log into the system by selecting *File → Login* or using the button on the toolbar. Each login is logged in the logbook of *iGuard® RemoteView* (see also *4.3 Logbook in iGuard® RemoteView*).

When first starting up *iGuard® RemoteView*, the following access data must be input:

- User name: **Administrator**
- Password: **Administrator** (output as ***)

This data is case sensitive!

The login dialog of *iGuard® RemoteView* is identical to the login dialog of *iGuard®* (see also *3.2.2 Login*).

4.1.2 Logging out of RemoteView

You can log out of the system by selecting *File → Logout* or using the button on the toolbar. All existing connections are automatically deactivated when you log out.
After a logout, *iGuard® RemoteView* cannot be used till the next login, except to receive alarm outputs.

iGuard® RemoteView has an Auto Logout function. This is activated by default and executes a logout when there has been no connection to a server and no user action on the PC for longer than the set period of time (see also *Auto Log-out* under *3.3.1 System configuration*).

4.1.3 Menus in *iGuard® RemoteView*

Menu File

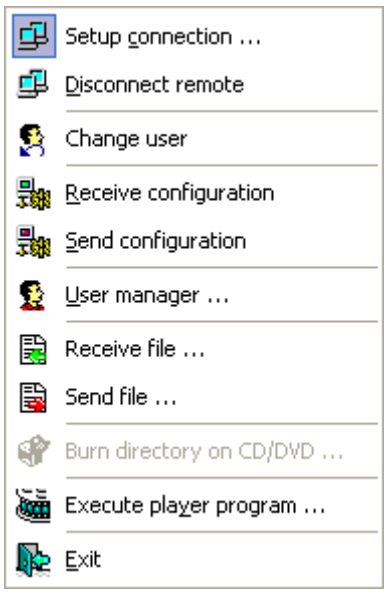


Figure 107: iGuard® RemoteView – menu File

- Setup connection
- Disconnect remote
- Logout
- New password
- Opens the dialog for assigning a new user password.
- Change user
  Login with new user name.
- Receive configuration
  Transmit configuration file *iGuard.dat* from *iGuard®* to *iGuard® RemoteView*.
- Send configuration
  Transfer configuration file iGuard.dat from *iGuard® RemoteView* to *iGuard®*.
- User management
  The configuration dialog for the user management is opened (see also 3.3.16 User management).
- Receive file
  Transfer file from iGuard® to iGuard® RemoteView (see also 4.15 Data transfer).
- Send file
  Transfer file from iGuard® RemoteView to iGuard® (see also 4.15 Data transfer).

- Execute player program
  Start oft the *iGuard® Player*. With this the AVI files produced of *iGuard®* in the MJPEG format can be opened and played(see also 5 *iGuard® Player*).
- Exit
  iGuard® RemoteView is terminated after the confirmation of a security check.

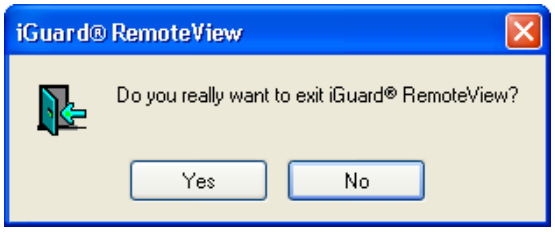


Figure 108: Exit iGuard® RemoteView

Menu View

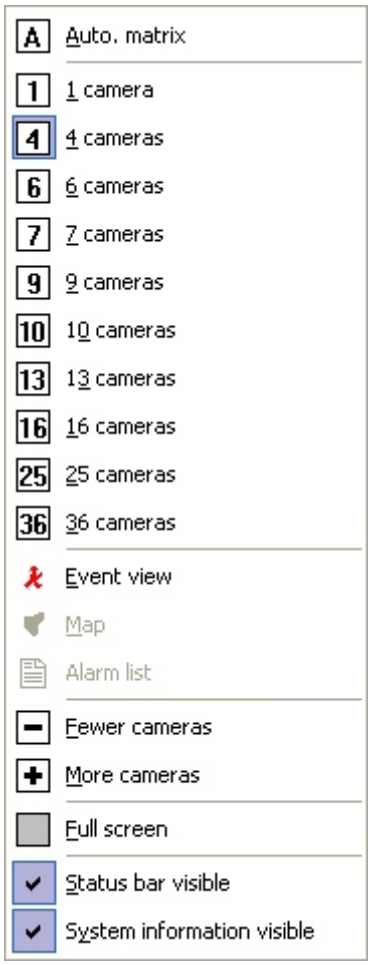


Figure 109: iGuard® RemoteView – menu View

The functionalities provided by the *View* menu correspond to the functionalities described under *Menu View* in *3.2.3 Menus in display mode*. The following additional options are available in *iGuard® RemoteView*:

- Alarm list
  Alarm events occurring during ongoing operation can be displayed in the alarm list (see also *4.6 iGuard® Remote View Alarm List (optional)*).

The options

- Map
- Statusbar visible

are also available if there is no connection to a server.

Menu Administration

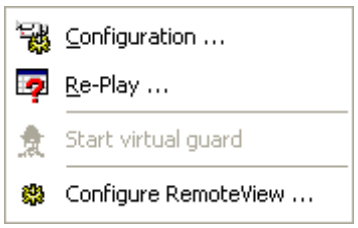


Figure 110: iGuard® RemoteView – menu Administration

- Configuration
  Edit configuration file iGuard.dat.
- Re-Play
  See 4.14 Evaluation of video sequences in playback mode.
- Start virtual guard
- Configure RemoteView
  See 4.2 Configuration.

Menu Action

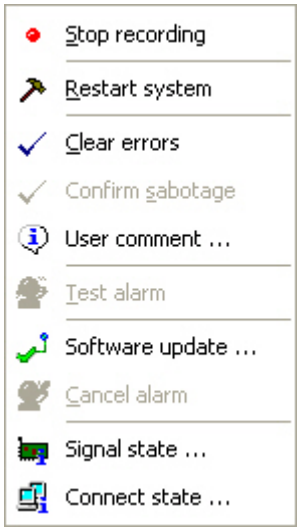


Figure 111: iGuard® RemoteView – menu Action

- Start/Stop recording
  See 4.9 Start/stop recording.
- Restart system
  See 4.18 Remote-System-Reboot.
- Clear errors
- Confirm sabotage
- User comment
  Adding from comments to logbook entries (see also Adding maps unter 3.2.3 Menus in display mod).
- Test alarm
  Activates trial recordings by activated banking mode (see also Adding maps unter 3.2.3 Menus in display mod).
- Software update
  See 4.20 Accomplish software updates.
- Cancel alarm
  This option allows you to manually cancel a pending alarm (see also *3.3.8 Configuration of the recording*). If an alarm is cancelled manually, this is documented in the logbook.

Menu Help (?)

Figure 112: iGuard® RemoteView – menu Help

- Help
  By selection of the *Help* option the *iGuard® RemoteView* help is opened.
- About *iGuard® RemoteView*
  With this option the dialog *About iGuard® RemoteView* is opened

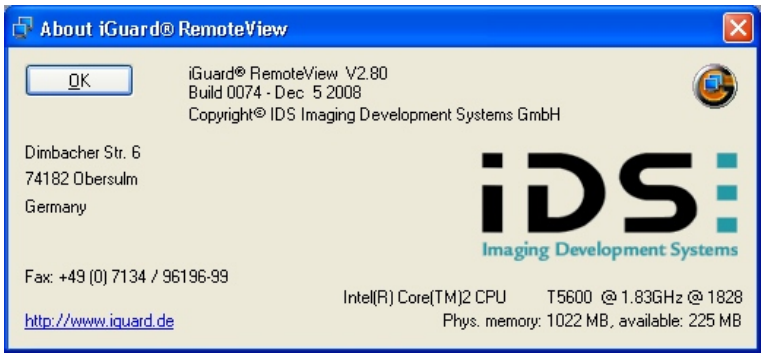


Figure 113: Information about iGuard® RemoteView

4.1.4 Symbol bar in *iGuard® RemoteView*

Symbol	Description
	Make a connection to iGuard® see *4.4 Connecting to iGuard®*
	Terminate connection to iGuard®
	Activate/deactivate logbook siehe *4.3 Logbook in iGuard® RemoteView*
	Login with new user name
	Next camera group Manual switch to the next group of cameras. See also *Camera groups* unter *3.2.7 Windows*.
	Automatic run. Automatic switch to the next group of cameras. Siehe auch *Camera groups* unter *3.2.7 Windows*.
	Less cameras.
	More cameras Clicking the arrow symbol opens a window in which the available split screen layouts are displayed.
	Open/closed the event window (see *3.2.9 Event Window*)
	Open/close the map (see *3.2.10 Map*). The map can also be displayed if there is no connection to a server.
	Opens/closes the alarm list (see *4.6 iGuard® Remote View Alarm List* (optional))
	Cameras on monitor
	Start recording See *4.9 Start/stop recording*.
	Stop recording See *4.9 Start/stop recording*.
	Start playback See *4.14 Evaluation of video sequences in playback mode*.
	Start Virtual Guard's walk arround See *4.7 Virtual guard's walk around*
	Open iGuard® RemoteView help

4.1.5 Status bar in *iGuard® RemoteView*

The status bar in *iGuard® RemoteView* corresponds to the status line in the display mode of *iGuard®* (see *3.2.6 Status bar*).

4.2 Configuration of *iGuard® RemoteView*

iGuard® RemoteView can be configured with the help of a dialog, which is accessible through the **menu** *Configure Management → RemoteView*. The parameters are stored in the file *iGuardRemoteView.dat*.

4.2.1 System configuration

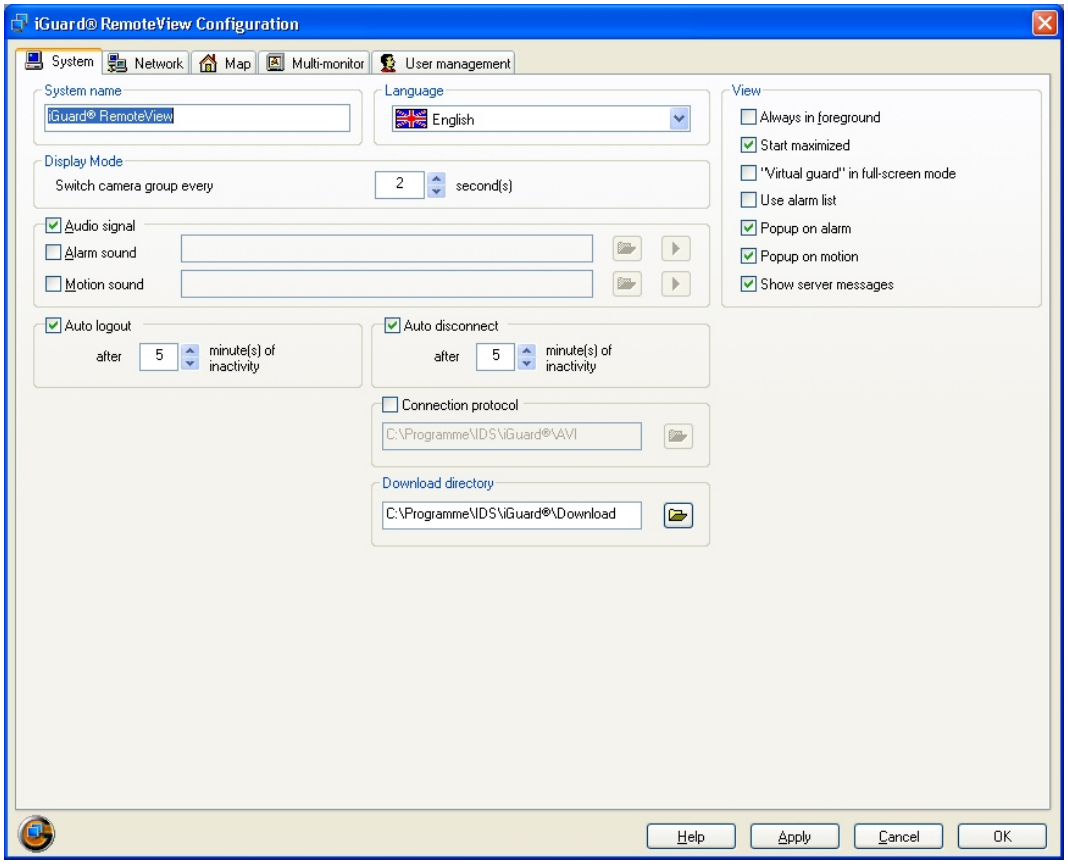


Figure 114: iGuard® RemoteView – system configuration

System name
The system name is primarily used for identifying the system if using remote access. For example, the location of the system can be entered here.

Language
Determination of the language in which *iGuard® RemoteView* is to operate. See also *Language* under *3.3.1 System configuration*.

View

- Always in foreground
  iGuard® RemoteView is always displayed in the foreground and is not overlaid by any other Windows application program.
- Start maximized
  If this option is activated, *iGuard® RemoteView* is started in a maximised window.
- Virtual Guard in full screen mode
  The virtual guard is executed in full-frame mode. Only video images are visible.
- Use alarmlist
  The alarm lists of the connected servers are displayed in *iGuard® RemoteView*.
- Popup on alarm
  iGuard® RemoteView is automatically displayed in the foreground in the event of an alarm.
- Popup on motion
  iGuard® RemoteView is automatically displayed in the foreground in the event of a movement.
- Show server messages
  Determines whether message dialog windows from the server are shown in *iGuard® RemoteView*.

Display mode

- Switch camera group every ... seconds
  A camera group is a group of cameras that is displayed simultaneously on the VGA screen. A quadsplit display, for example, shows four camera images. If, however, ten cameras are connected in total, this results in three camera groups, the last of which consists of only two cameras. These three camera groups are displayed one after the other if automatic camera group switching is activated in display mode. The desired group switching time is entered in the field for camera group switching. You can set a switchover time of between 2 and 600 seconds.

Audio signal

- Alarm Sound
  The specified wave file is played in the event of an alarm occurrence.
- Motion Sound
  The specified wave file is played if a movement is detected.

Auto logout
When the *Auto logout* option is checked, the system automatically logs the user out of *iGuard® RemoteView* in the event of long-term inactivity. The inactivity period can be set for between 1 and 300 minutes.

Auto disconnect
When the *Auto disconnect* option is checked, the system automatically disconnects the user from the *iGuard®* Server in the event of long-term inactivity. The inactivity period can be set for between 1 and 300 minutes.
See also *Auto Logout* under *3.3.1 System configuration*.

Control panel
The control panels CKA 4810 and 4820 are supported.

- COM
  Selection of the serial interface, at which the control panel is attached.
- Key delay
  If no keyboard entry takes place within the indicated time, the input is considered as final. Therefore the key delay should be adapted to the printing rate of the operator, because otherwise it can result to the fact that the control panel tries to process incomplete commands.

Connection protocol
So that a protocolling (see also *4.10 Connection protocol*) takes place, the option *connecting protocol* must be activated. The AVI files with file names stipulated by the program are then generated in the specified directory. Because of the file sizes which can be expected the specification of a floppy disc drive is not recommended. Unlike the server application *iGuard®*, in this case it is also possible to specify a network path.
Download directory
The configuration files, received for the remote configuration from the server are stored in the indicated download directory. Because these can exceed the disk space of a floppy disk, depending upon the size of the stored configuration, the allegation of such a drive is not recommendable.

Download directory
The configuration files received for remote configuration from the server are stored in the specified download directory. As these files may exceed the storage volume of a floppy disk depending on the size of the saved configuration, we do not recommend that you specify a floppy disk drive.

4.2.2 Configuring the network

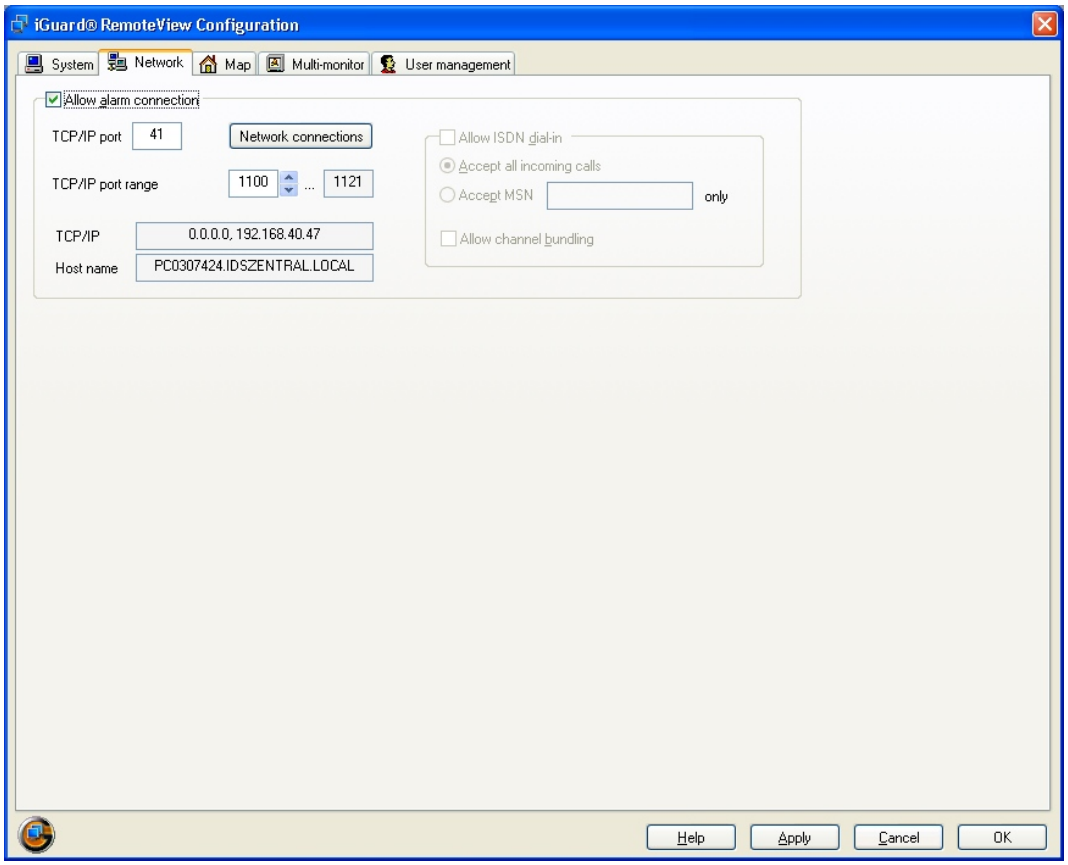


Figure 115: iGuard® RemoteView - Configuring the network

Allow alarm connection (optionally available)
The option *Allow alarm connection* must be switched on if an alarm connection (via LAN or ISDN) is to be permitted. The alarm output is activated on startup of *iGuard® RemoteView* even if no user is logged in. If no user logs in, only the live image of a camera activated by the alarm output can be viewed. For further actions, a user login is required.
The TCP/IP port where *iGuard® RemoteView* is accessible must be specified for access via LAN. Port 41 is usually used. The TCP/IP address is set at operating system level during configuration of the network board. *iGuard® RemoteView* shows the TCP/IP address and the host names of the computer in a non-editable field. If more than one network board has been installed in a computer, it is possible that the display will not show the TCP/IP address of the LAN network board but that of another network board. The host name is shown for information purposes and is not used further by *iGuard® RemoteView*.
If *iGuard® RemoteView* is operated behind a firewall but access still needs to be available from external systems (e.g. from the Internet), it must be possible for all the ports used by *iGuard® RemoteView* to be opened at the firewall. Each

client requires 2 data ports. The relevant IP ports must be opened with the firewall.

Allow ISDN dial in

The option *Allow ISDN dial in* also has to be activated if *iGuard® RemoteView* is also to be accessible via an ISDN connection. *iGuard® RemoteView* makes it possible to only react to calls from a specific MSN. The service indicator of an ISDN call must always be *Data*. Calls with a different service indicator will be ignored. This enables *iGuard® RemoteView* to be operated on an ISDN connection parallel to a telephone because the telephone only signals a call if it bears the service indicator *Telephony*.

- Accept all incoming calls
- Accept MSN only
  iGuard® makes it possible to react to calls of a specific MSN.
- Allow channel bundling
  If two channels are to be authorised for an ISDN connection, the option *Allow channel bundling* will also have to be activated.

This option must not be activated if one channel has to be kept free for a separate line (e.g. alarm system).

4.2.3 Configuring the Map (optional)

Configuring the map in *iGuard® RemoteView* is the same as configuring the map in *iGuard®* (*see* 3.3.17 Configuring the Map).

An exception are the Objects and Addresses sections. In *iGuard® RemoteView* these areas serve to display the address book on the map.

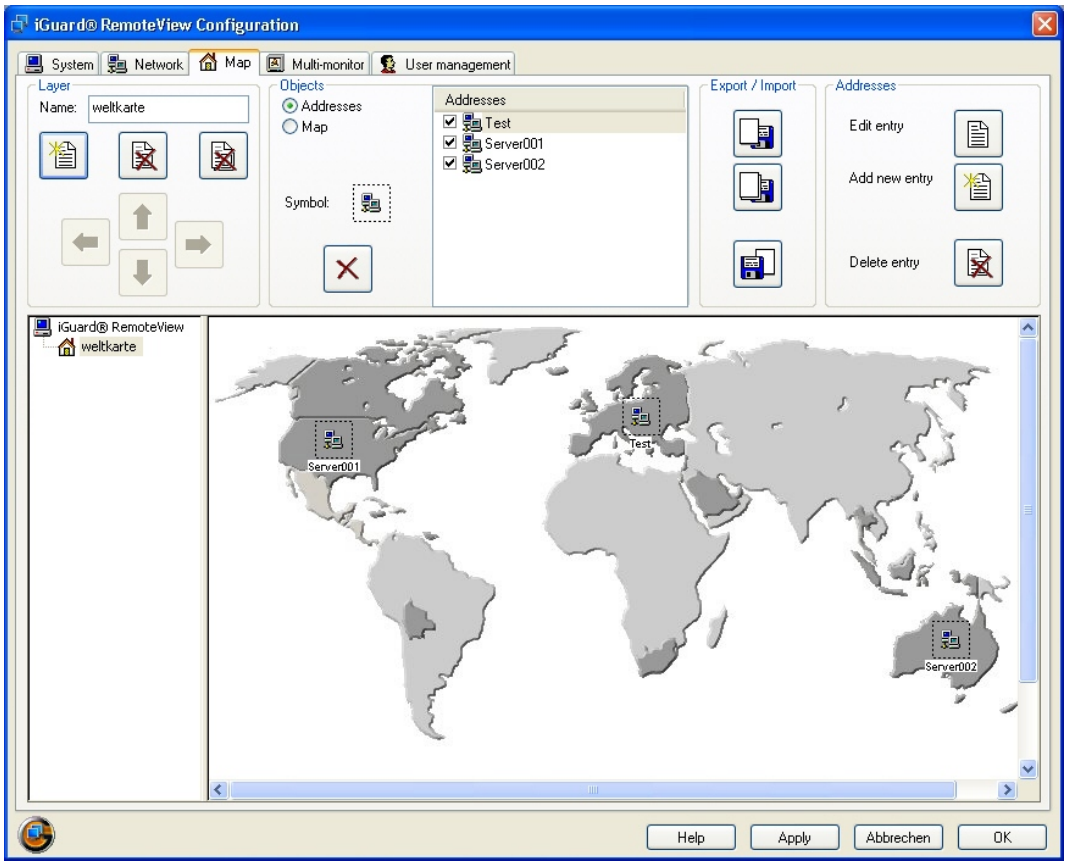


Figure 116: iGuard® RemoteView - Configuring the Map

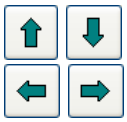
Layer

Name — Map name
The map is displayed in the tree structure under the name entered here.

Add map to tree structure

Delete map highlighted in tree structure

Delete all maps



Move map one step up/down

Move map one hierarchy layer to the left/right
A maximum of two hierarchy layers can be set up (main layers and one subordinate layer per main layer).

Objects

Addresses option	The selection list is headed “Addresses”. The addresses stored in the phone book are listed. The addresses can be positioned on the map in the same way as the objects on the server map (see also *Setting and Deleting Address Objects*).
Map option	The selection list is headed “Map". All maps stored in *iGuard® RemoteView* are displayed. This option allows you to link maps with each other (see also *Linking Maps*).

Delete all elements on the current level

Export/Import
The following export and import functions are available:

Export current layer

Export all layers

Import layer

Addresses
The buttons in the Addresses section allow you to add new entries to the address book and edit or delete existing entries (see also *4.4.3 iGuard® RemoteView Adress Book*).

Edit selected address book entry

Add new connection to address book

Delete selected entry

Tree structure
All maps configured in *iGuard® RemoteView* are displayed hierarchically in the tree structure. Up to two hierarchy layers can be created.

Display window
The display window shows the map currently selected in the tree structure together with the address objects positioned on it. If the image of the map you want to display is too large to fit into the display window, scroll bars appear.

The image of the map to be displayed is not scaled.

Adding and Deleting Adress Objects

In order to position an address object on the map, it must first be selected from the address list (Addresses option). Then it can be positioned on the map by clicking the left mouse button at the desired point on the map. Confirm the position of the address object by ticking the checkbox in the selection list.
To change the position of an address object, click it with the left mouse button. You can then reposition it on the map by holding down the left mouse button and dragging.

An address object can be set up on more than one map, but only once on each map.

There are several ways of removing an address object from the map:

- Uncheck the box before the object in the selection list
- Double-click the object with the left mouse button
- Use the pop-up menu (as described above)

The button deletes all objects from a layer.

Linking maps

If the map option is selected, all currently set up maps are displayed in the selection list. These map objects can be positioned, deleted or moved in the same way as the address objects.
If you click on a map object later on when using the programme, the corresponding map is displayed in the *iGuard® RemoteView* display window.

4.2.4 Configuration of the multi-monitor mode

Configuration of the multi-monitor mode in *iGuard® RemoteView* corresponds to the configuration in *iGuard®* (see also *3.3.19 Configuration of the multi-monitor mode*). Exceptions to this are the *Sequence monitor* functions and the configuration of the *Default split screen*.

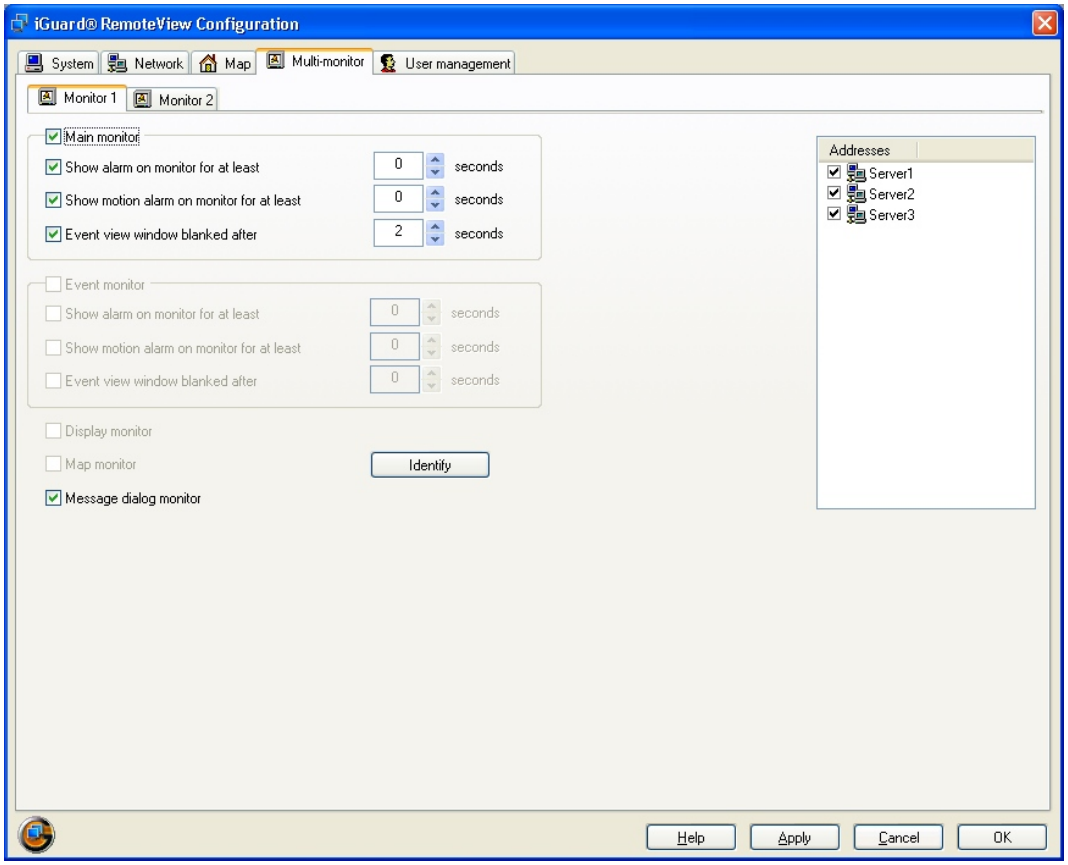


Figure 117: iGuard® RemoteView – multi-monitor configuration

In multi-monitor mode, *iGuard® RemoteView* supports up to four monitors. The distribution of the monitors is configurable. In multi-monitor mode, the main monitor retains the same functionality as in single-monitor mode. Additional monitors can be configured for displaying camera images, event messages or the map.

Main monitor
The main monitor always shows the *iGuard® RemoteView* menus, the login dialog, the rendering view and the task bar. The configuration settings are executed via this monitor. One monitor must be defined as the main monitor; other monitors are optional.

If one or several of the following options are checked, the corresponding events are displayed as a window on the main monitor.

- Show alarm on monitor for at least … seconds
  Minimum duration for display of an alarm event. Alarm messages that come in during this time are not displayed. You can set a time of between 0 and 60 seconds. 0 seconds means that an alarm event window is immediately hidden when a new alarm comes in.
- Show motion alarm on monitor for … seconds
  Same setting option as for alarm event (see above).
- Event view window blackout … seconds
  Period of time after which the display of an event is blacked out. You can set a time of between 2 and 300 seconds.

Event monitor
When selecting a display monitor as the event monitor, this monitor is only used to display event messages.
The event options are identical to those for the main monitor (see above).

The Event window and Event monitor functions cannot be used simultaneously.

Display monitor
Configuration of a monitor as the display monitor for the display of live camera images. This selection option is only available when the monitor is not selected as the main monitor.

Map monitor
This option is used to activate the relevant monitor for full-screen view of the map. Only one monitor can be used as the map monitor.

Message dialog monitor
This option is used to define the relevant monitor for displaying the message dialogs.

Addresses
In the server list, the servers entered in the address book can be assigned to the relevant monitor.

4.2.5 User management

User management in *iGuard® RemoteView* corresponds to user management in *iGuard®* (see also *3.3.16 User management*).

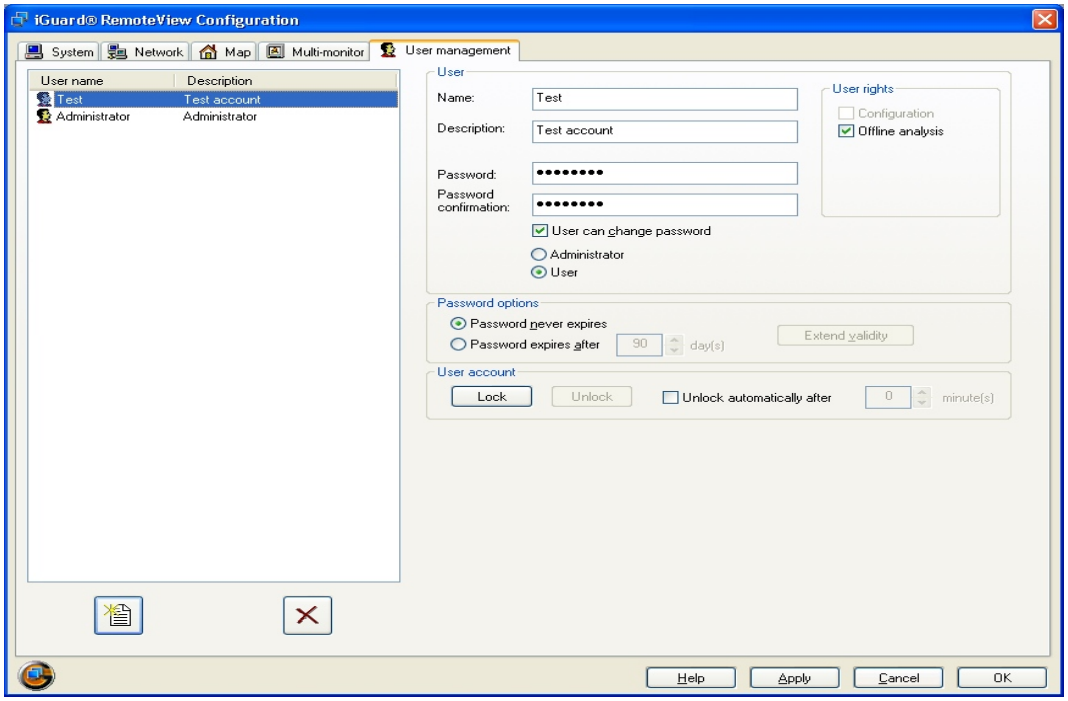


Figure 118: iGuard® RemoteView – User management

User list

The User management dialog shows a list of all known users with user name and description. When you select a user, that user's details are shown and can be changed. To do this, you must have administrator rights.

New users can be created or existing users deleted using the and buttons.

In the factory settings of *iGuard® RemoteView*, the user "Administrator" is allocated the password "Administrator". This user cannot be deleted. The password can of course be changed.

Configuration rights are assigned separately for *iGuard*® and *iGuard*® *RemoteView*.

User

- Name/Description
  Name and description of the user
- Password/Password confirmation
  A password must be entered.
- User can change password
  This option is checked by default. It allows users to create their own password. User group
  Allocation to one of the following user groups:
  - ♦ Administrator
    All rights are assigned to the *Administrator* user group.
  - ♦ User
    Individual rights must be assigned to this user group.

User rights

Assignment of individual user rights is only possible for the *User* user group.

- Configuration
  Allows the configuration of *iGuard*® *RemoteView* to be changed. Only administrators have this right.
- Offline analysis
  Allows the analysis of databases without a direct connection to the *iGuard*® server (see also *4.17 Local revision of existing databases*).

Password options

The validity of the password can be limited to a certain length of time or you can select *Password never expires*. A time-limited password can be extended by a user with administrator rights at any time.

User account

If an incorrect password is entered 3 times, the user account is automatically locked. The user account can either be unlocked automatically after a set time or manually by a user with administrator rights. The user account of the user *Administrator* cannot be locked.
For example, if a value of 15 minutes has been entered for the automatic unlocking of the user account, the 3 times rule goes back to the start when 15 minutes have elapsed since the last time a password was entered. In other words, when a password for a user account is entered incorrectly 3 times in succession within 15 minutes, that account is locked.

Chip card reader support

- *iGuard*® *RemoteView* automatically recognises chip cards from SCM Microsystems (USB or serial), provided these have been correctly installed. The only supported chip cards are memory chip cards. Processor chip cards,

magnetic strip cards or devices from other manufacturers are not currently supported.
iGuard® RemoteView can store user data (name, password) in encrypted form on a chip card. This means you only need the chip card to log into the system. The user does not need to know their user name and password.
As only the name and password are stored on the chip card, the user configuration of the server determines what rights the user has, whether the user name is valid or whether the user is locked.
A chip card is created from the user configuration on the server (see also *Chip card reader support* in Chapter *3.3.16 User management*).

4.3 Logbook in *iGuard® RemoteView*

While *iGuard® RemoteView* is running, any events that occur are recorded in a logbook. For an overview of events that have occurred, you can activate or de-activate the logbook display via the button . However, the logbook can only be activated when no connection is established.
Clicking the right mouse button opens the pop-up menu for the logbook.

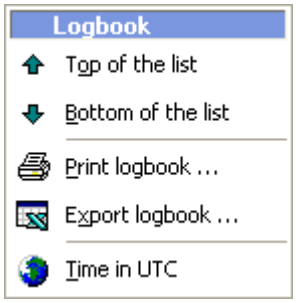


Figure 119: iGuard® RemoteView – pop-up menu for the logbook

This pop-up menu provides the following options

- Jump to the start or the end of the logbook entries
- Print the logbook
- Export the logbook

4.4 Connecting to *iGuard*®

4.4.1 Connecting Quickly

A fast way to establish a connection to *iGuard*® is to use the dropdown menu that opens when you click the arrow symbol to the right of the button  . This list is divided into two sections. The upper section lists up to ten of the *iGuard*® servers you have most recently connected to. As this list displays a connection history and is therefore initially empty, this functionality is not available when you connect for the first time.
The lower section of the list shows the first ten entries in the address book. To display your favourite connections here, sort them accordingly in the address book.

A connection can only be initiated once a user is logged into *iGuard*® *RemoteView*.

4.4.2 Automatic login while connecting

When an *iGuard*® server is contacted, *iGuard*® *RemoteView* checks whether the user currently logged in is known on the server. If the user is known, the server transmits his or her rights to *iGuard*® *RemoteView*. If the user has sufficient rights, he or she is automatically logged into the server. If the user is not known on the server or does not have sufficient rights, the login dialog box appears and the user has to log in manually.

For this function, *iGuard*® version 2.80 must be installed on the server. If an older version is installed on the server, the login dialog box appears and the user must log in manually.

4.4.3 *iGuard*® RemoteView Adress Book

Other ways of connecting to *iGuard*® are via the *File* → *Connect* **menu** or by pressing the button  . The *Address book* dialog box then appears. The address book allows you to establish a connection based on existing entries, manage the existing connection data and add entries for new connections.

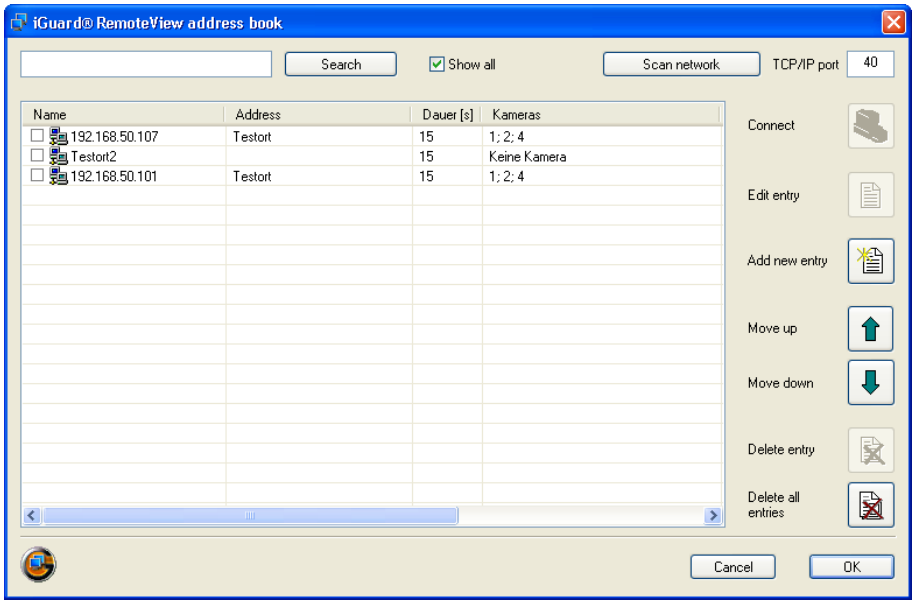
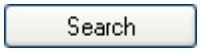
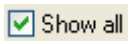
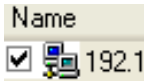


Figure 120: iGuard® *Address book*

Buttons and options in the address book

	Search connection in addressbook
	The *Show all information* option allows you to display the fields Connection, Duration, Cameras, Server name/IP address, Port, RAS und Phome number in addition to the Name and Location fields.
	ee *Automatic search for iGuard® Servers*
	The virtual guard function can be activated for the respective connection via the selection field in the name of the connection (see also *4.7 Virtual guard's walk around*)
Duration [s]	The Duration field is a function of the virtual guard. It determines how long the cameras of the selected connection are displayed when the guard function is active. The Duration can be set to a value of between 15 and 999 seconds.
	Use this button to select the cameras that are to be displayed after establishing a connection. See also *Selecting the cameras to be displayed*
	*Connect* opens the *Login* dialogue box. Enter username and password to access the *iGuard®* server.
	Edit selected address book entry.
	Add new connection to address book (see also *Adding entries to the address book*).
	The buttons *Move up* and *Move down* allow you to arrange the connections in your preferred order. This order is followed by the virtual guard and in the list for quick connecting.
	Delete selected entry/Delete all entries.

Automatic search for *iGuard® Servers*

Over the button *Search network iGuard® RemoteView* can be prompted to scan the local network and to add all *iGuard®* servers to the address book that are not already listed in it.
The search is carried out for only one specified port. If there are *iGuard®* servers in the local network with different ports, a search will have to be made for each port.
This function is currently only available for class C networks yyy.yyy.yyy.xxx (yyy are fixed, xxx variable).

In view of the restrictions of the operating system version Windows XP ServicePack 2, this procedure can take a number of minutes under certain circumstances if using Windows XP with ServicePack 2.

Selecting the cameras to be displayed

For existing connection entries, use the Cameras field to determine which cameras are to be displayed live on connecting. To do this, first select the connection you want to edit by clicking on it. The button [...] then appears in the Cameras field. Click this button to open the camera selection dialogue.

A connection to the chosen server is set up in the background for the selection of a camera. The Please wait dialog (cp. *3.1.20 Please-wait-dialog)* is displayed while this is taking place.
The dialogue for camera selection is displayed with one of two contents depending on whether it was possible to set up a connection to the server or not:

- Connected to server
  Configured cameras (with name) on the server are listed in the dialog.
- Connection to server not possible
  A numbered list is shown for selection of the cameras. It is not possible to select cameras by name without connection to the server as *iGuard® RemoteView* does not know the designated names of the cameras on the server.

On the list of camera selections without server connection, network cameras are listed as of number 65. No. 1 to 64 are reserved for analogue cameras.

The *No cameras* and *All cameras* options allow you to quickly edit the camera selection list.

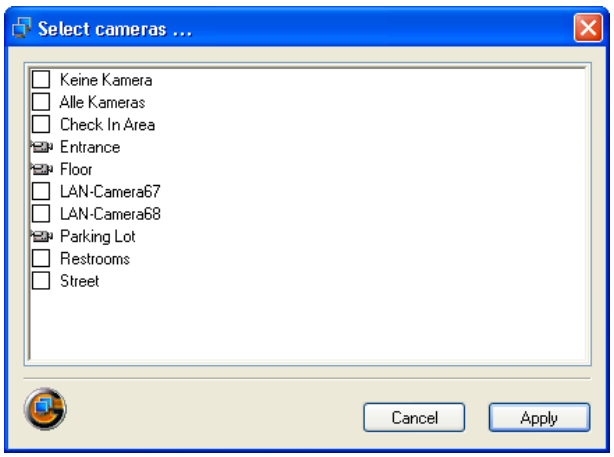


Figure 121: Virtual guard selecting cameras – with server connection

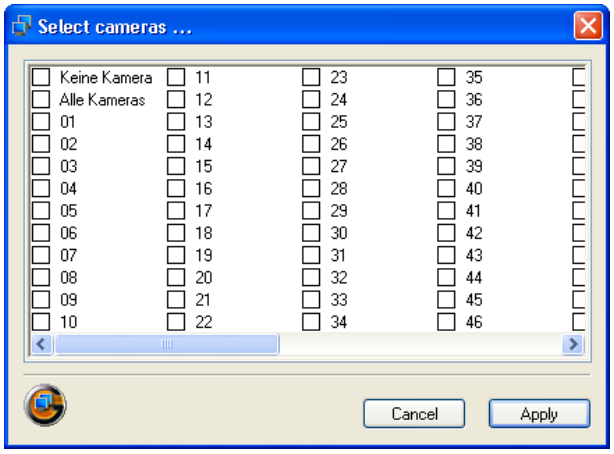


Figure 122: Virtual guard selecting cameras – without server connection

Adding entries to the address book

Click the button to open the *Address book entry* dialogue box. Of the available text fields Name, Server location, Server IP address, Server port and Server phone number, the fields Name, Server IP address, Server port and, if applicable, Server phone number must be filled in.

Several entries can be stored for an IP address in the address book. This allows you to group cameras and display them over different connections.

You can select the desired connection type in the *Connect via* field. The requirements for this connection type must be met (installed connection, see *3.3.9 Configuration of the network parameters*).
Only numbers and the characters „**(**“, „**)**“ and „**-**“ are permitted in the *Server phone number* text field. The *Server location* field is optional. Return to the *Address book* dialogue box with the button OK.

You can establish a connection instantly by clicking the button or by double-clicking the entry in the list.

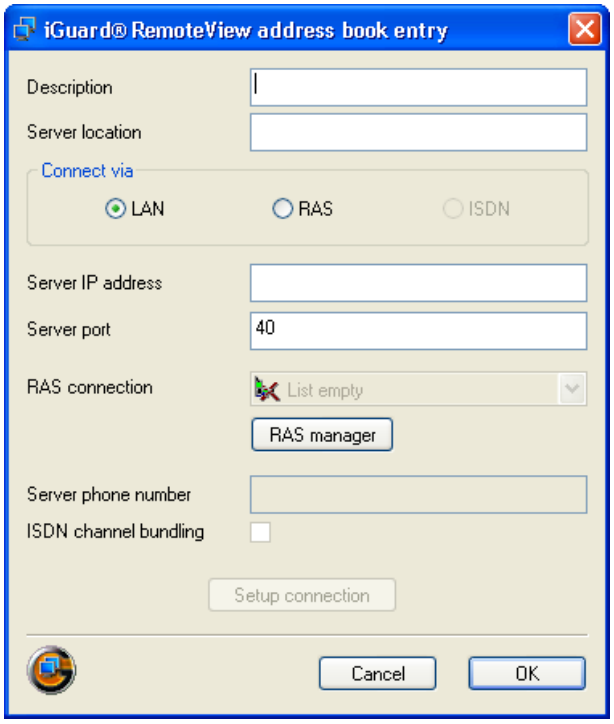


Figure 123: iGuard® RemoteView – telephone book entry

Remote access authorisation is necessary in order to be able to set up a connection. Furthermore remote access also has to be authorised in the configuration mode of iGuard® in the field *Allow network access* (cf. *3.3.9 Configuration of the network parameters*).

4.4.4 Connection with multiple servers

With *iGuard® RemoteView* up to ten servers can be connected at the same time. The connected servers and their cameras are listed in the display mode. Maximal 10 x 96 = 960 cameras can be listed.

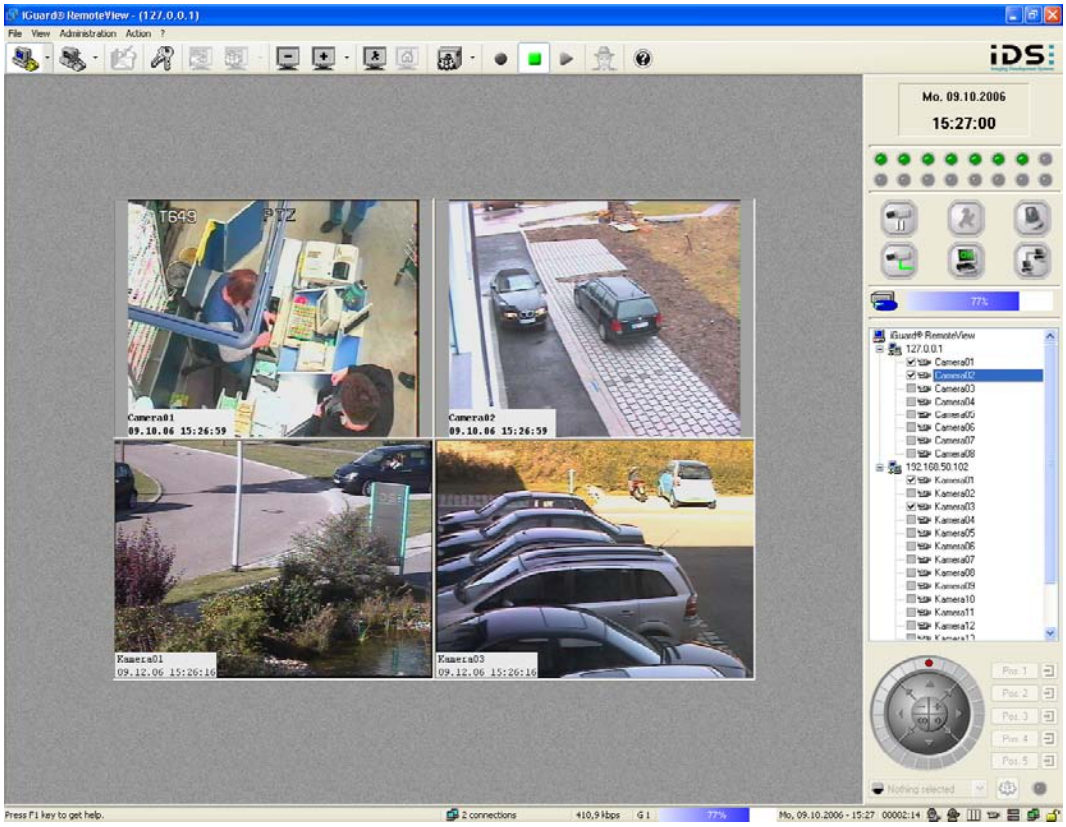


Figure 124: iGuard® RemoteView display mode

The camera list is displayed in a tree structure. Below the entries of the connected servers the available cameras of the server are displayed.

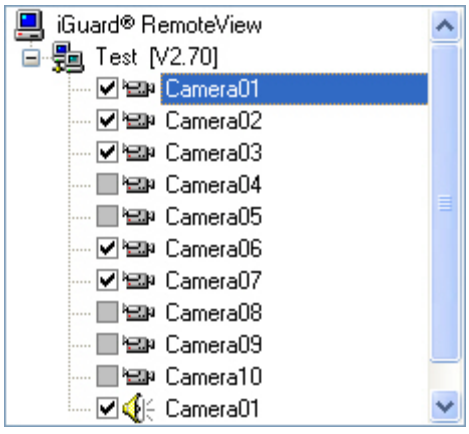


Figure 125: iGuard® RemoteView camera list

A camera is activated via the selection in the camera list. By one right-click on the camera list a context menu appears.

Figure 126: iGuard® RemoteView camera list context menu

Here can all cameras be activated at the same time and/or to be deactivated. The cameras are automatically allocated to the display windows. Maximally 36 cameras can be displayed at the same time.

Activating Audio Transmission
If a camera has an audio channel, it is displayed in the camera list in *iGuard® RemoteView*. The audio channel is identified by a loudspeaker symbol and the name of the associated camera.
You can activate/deactivate audio transmission by means of the checkbox before the speaker symbol.

iGuard® RemoteView can transmit an audio channel for analogue cameras. Both the live and the rendered sound can be transmitted.

For LAN cameras, *iGuard® RemoteView* supports transmission of the rendered sound.

Status indications
RemoteView shows different status indications of the server in the surface. With several connected servers the information of the selected server is displayed. A server is selected in the camera list. To activate the server the server or a camera of the server must be marked in the list. Afterwards all status indications and commands refer to this server. The current active server is displayed additionally in the *iGuard® RemoteView* header. To the server-referred status indications belong:

- time
- switch outputs
- hard drive capacity
- running time of the system
- recording start/stop

Beside these there is also a global status indication. The global status indication reacts, if on one of the connected servers one of the following characteristics occurs:

- motion
- alarm
- loss camera
- sabotage
- failure
- connection

Figure 127: iGuard® RemoteView global status indication

Commands

Commands (e.g. menu commands) are likewise server-referred. However the following commands are available only in single server mode:

- Configuration
- System restart
- Software update

Remote configuration is possible only if there is a single connection to a server.

Server-referred commands are:

- activate test recordings
- start monitor run-through
- start/stop recording
- change user
- logbook comment

Beside the server-referred commands there are also global commands available:

- confirm sabotage
- clear errors
- cancel alarm

Camera-referred commands can be assigned directly to the camera associated server:

- switching to monitor
- PTZ control

All delete functions and the cash search are locked, if more than one server connection exists.

Disconnect
With the button can either all connections at one time or individual connections be separated.

Playback mode

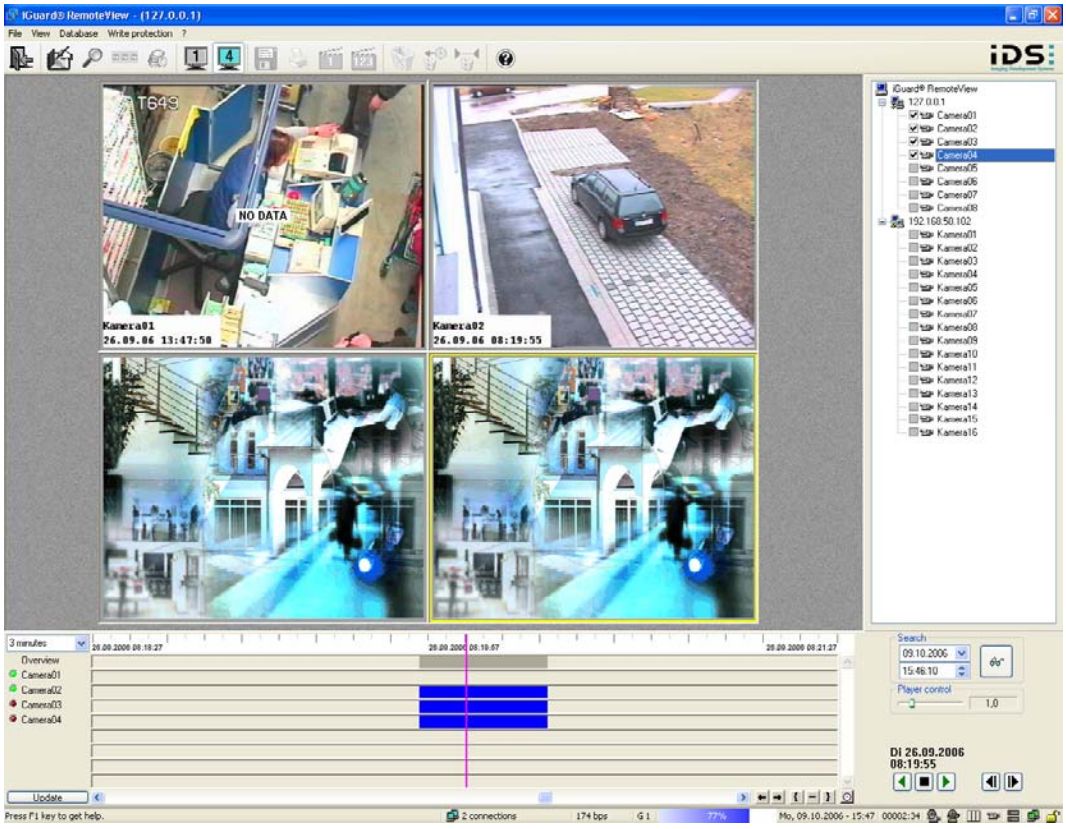


Figure 128: iGuard® RemoteView playback mode

In playback mode a camera list is displayed as in display mode. The cameras to be observed are selected in the display mode. Only the cameras marked in the time line are displayed, independently to which server the cameras belong.

Logbook display
Displaying the logbook is not possible with several connected servers. Only the logbook of one server can be displayed.

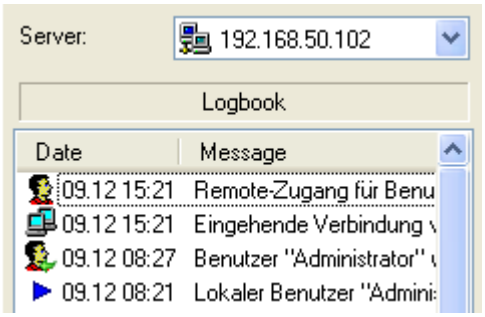


Figure 129: iGuard® RemoteView logbook display

The server is selected in a combo box, which is attached above the logbook. In this the names or IP addresses of the servers are registered, with which currently a connection exists.

4.4.5 Connecting via the Map (optional)

When the map is displayed, you can connect to a server by clicking the corresponding server symbol with the left mouse button.

4.5 *iGuard® RemoteView* Map (optional)

In multi-monitor mode, the map can be displayed in full-format view on a further monitor (see also *3.3.19 Configuration of the multi-monitor mode*).

4.5.1 View in Single-monitor Mode

In single-monitor mode, the map and the selected camera images are shown in a subdivided display window (see also *3.2.10 Map (optional)*).

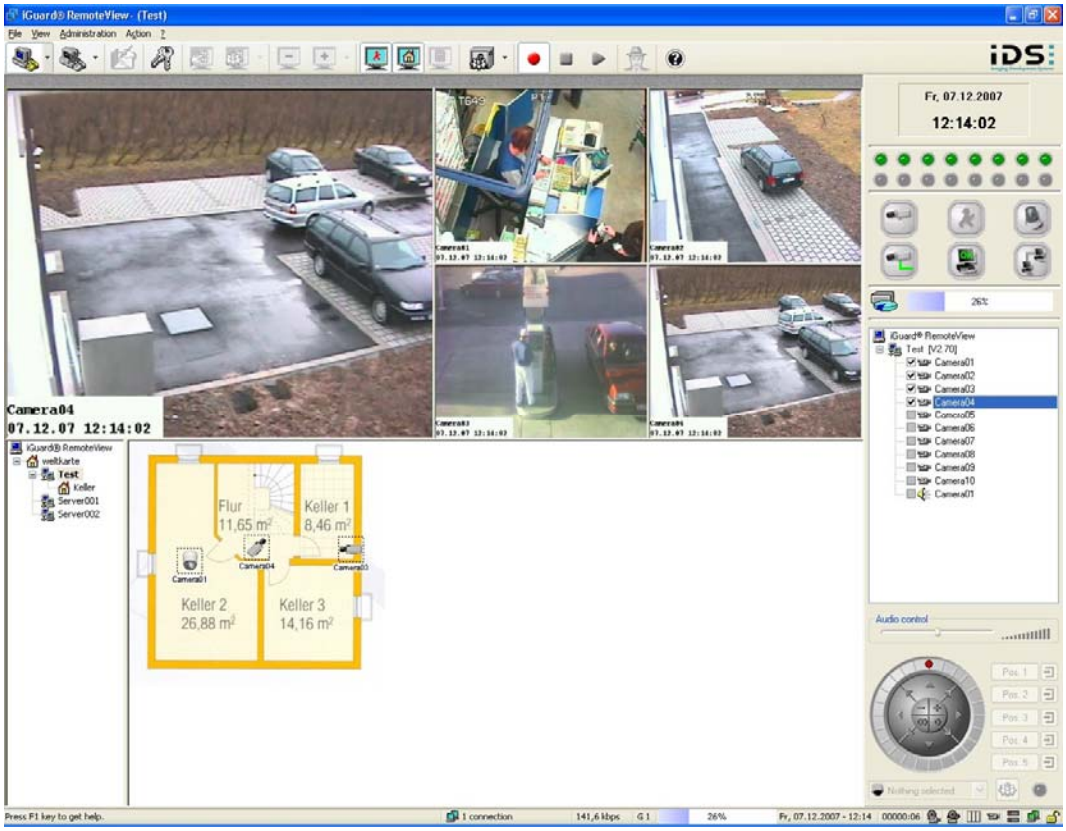


Figure 130: iGuard® RemoteView Map in Single-monitor mode

4.5.2 View in Multi-monitor Mode

The camera images are displayed on the main monitor.

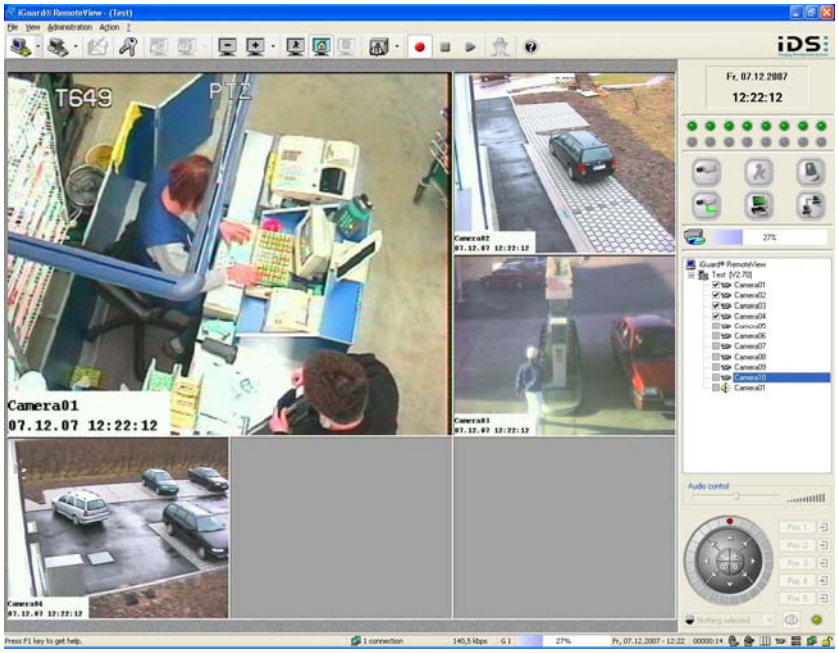


Figure 131: iGuard® RemoteView camera images in multi-monitor mode

The map is displayed on an additional monitor

Figure 132: iGuard® RemoteView Map of connected server

4.5.3 Connecting to a Server

You can connect to a server via the map. Simply click the desired server symbol with the left mouse button.
When a connection to a server has been established, the maps available on the server are transferred to *iGuard® RemoteView* and listed in the map tree structure there.

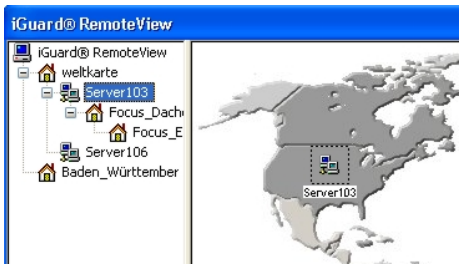


Figure 133: Server connection display

4.5.4 Displaying the Map

After selecting the desired map in the tree structure, it is shown in the display window.
If you move the mouse over an object on the map, a tool tip with the following information on the object in question appears:

- Object name and description (as configured with the server)
- IP-Address and Port of the server

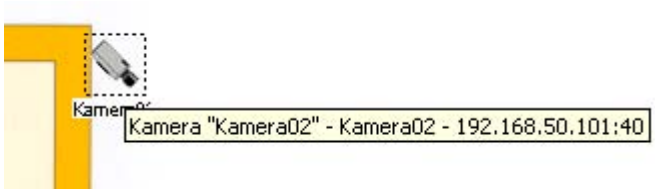


Figure 134: Tool-Tip in iGuard® RemoteView map

The status of objects can only be displayed if a connection to a server is present.

Only one connection to a server can be open at any one time!

4.6 *iGuard® Remote View* Alarm List (optional)

Alarm events occurring in ongoing operation can be displayed in the alarm list. Alarms that occurred before connecting to the server are not included in the alarm list. In order to use the alarm list entries from the connected servers in *iGuard® RemoteView*, the following settings are required:

- The option *Alarm List Entry* must be activated on the server side.
- The option Use Alarm List must be activated in the iGuard® RemoteView system configuration.

The Alarm List is only visible if there is at least one entry in the list. As soon as an alarm occurs, the alarm list automatically appears on the left-hand side of the application; the latest alarm list entry is always at the top of the list. The time sequence of the list therefore corresponds to that of the logbook. The alarm symbols before the list entries are also the same as those used in the logbook (see *3.4.4 Logbook*).

If there are entries in the alarm list and none of these entries are currently being processed, the list can be shown/hidden using the View → Alarm List **menu** or the button on the toolbar.

In order to display additional details of an alarm and process it further, an alarm entry can be opened by double-clicking with the left mouse button. The following data of the selected list entry then appear below the alarm list:

- Date and time of the alarm
- Camera that triggered the alarm
- Message text
- Server from which the alarm has come

In Edit mode, a comment can be entered which is stored in the *iGuard® Server* logbook. The logbook also automatically records when and by whom the alarm was processed.

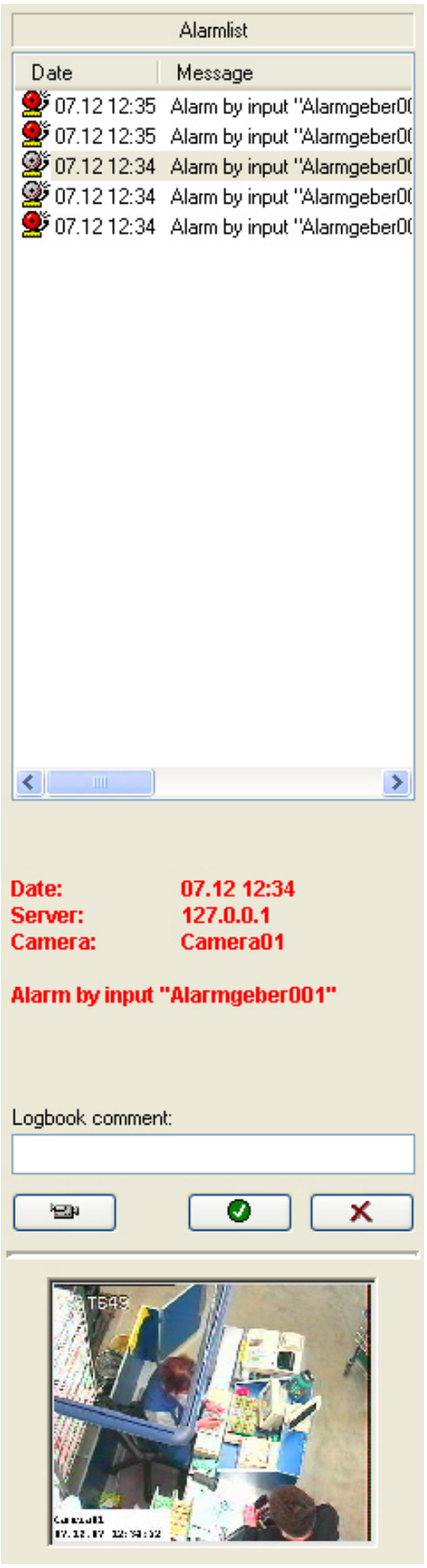


Figure 135: Alarm list

The stored alarm image (if there is one) pertaining to the open alarm is displayed at the bottom of the dialogue bar. Double-click this image to display a larger view in a separate popup window.

You can also display the live image from the camera triggering the alarm by clicking the  button. If an audio channel is assigned to the camera, the live audio of the PC sound cards audio channel is output together with the live image.

When you have finished processing the alarm and confirmed with  , the alarm is removed from the alarm list. The  button resets the alarm entry and retains it in the alarm list.

When you exit *iGuard*® ® *RemoteView,* the alarm list is deleted. When only the connection to the server is closed, the alarm list remains.

4.7 Virtual guard's walk around

This function is used for establishing in a pre-set sequence time-controlled and automatic connections to various recording systems, displaying pre-set cameras and separating these connections at the end of a pre-set time and establishing a new connection to another server.
The virtual guard uses the address book (see *4.4.3 iGuard® RemoteView Adress Book*), which can be accessed via the **menu** *File → Connect* or the button  . The connection settings are identified there by means of the address book entries. This means the user has to enter the connection settings in the address book first before the configuration of the guard can work with these settings.
The *virtual guard* can be started using the switch  of the symbol bar, the **menu** Admin → Start virtual guard or direct using a command line parameter upon calling up *iGuard® RemoteView*.
The command line parameter is:

„-vguard“ or:
iGuardRemoteView.exe –vguard

The guard is terminated again using the same functions (except command line parameters).

A login on the server takes place automatically when the user logged into *iGuard® RemoteView* is also known on the server and has the corresponding rights on the server. In this case – as with the alarm output – the user does not need to log in manually (see also Chapter *4.1.2 Logging out of RemoteView*). If the user is not known on the server or does not have the necessary rights, no connection is established to this server and no login dialog appears. A message is entered in the logbook and this server is no longer activated for subsequent security rounds, provided no new user has logged into *iGuard® RemoteView*.

4.8 Display cameras live

To display the images grabbed by a camera live the user must have *Display* authorisation. By selecting a camera in the *Cameras* field the live image of this camera will appear in the window.

A maximum of 16 cameras can be displayed simultaneously with an ISDN connection. Other than this, simultaneous display of all cameras is possible. In the live image, in contrast to *iGuard®* the titles *REC*, *STOP* or *DET* are **not** available.

By double clicking the left mouse button within the picture or by clicking the right mouse button within the picture and then selecting *Full Picture* out of the context-menu the window may also be enlarged. The image transmission for each camera can be started, stopped or switched. Thus, recorded scenes can be captured and printed or saved.

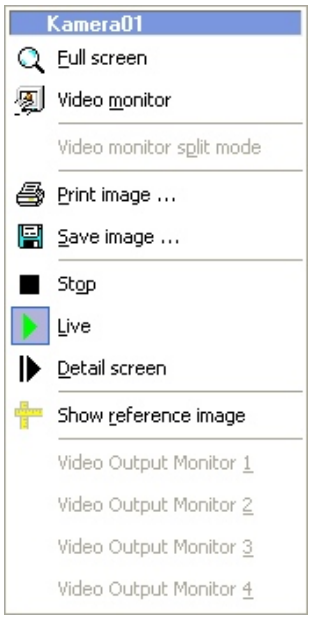


Figure 136: Context-menu of the live image

Live image zoom
For all cameras, a section can be freely selected from the live image and displayed enlarged. To do this, click the live image with the left mouse button while holding down the CTRL key and draw a rectangle. When the mouse button is released, the selected section will be enlarged to the image size. By clicking the image you can return to the full-screen display.

4.9 Start/stop recording

Using *iGuard® RemoteView*, it is also possible to start or stop the *iGuard®* server by remote access. Pre-condition therefore is beside the *Remote access* authorisation also the *Start/Stop* authorisation. Starting and stopping is carried out in the same way as in *iGuard®*, either via the **menu** *Action → Start/Stop Recording* or by pressing the buttons (*REC*) and/or (*STOP*)..

4.10 Connection protocol

All images which have been received during remote connection from an *iGuard®* recording system are stored with the help of this function. It is unimportant whether these images were requested using the preview or the playback function. The image size is 384x288 irrespective of the transmitted image size. All received images are scaled up/down to this size and stored. The quality of the stored images, naturally, cannot be better than that of the received images – the opposite, however, does apply.
The function *Connection protocol* must be enabled by the user. The directory where these AVI are to be stored can also be specified by the user (see *4.1.3 Menus in iGuard® RemoteView*).
The system generates AVI files, the names of which have the following format:

YYYY-MM-DD_hh-mm-ss_XXXXX_YYYY.AVI

Explanation:

YYYY-MM-DD_hh-mm-ss:	Date (Year, Month, Day, Hour, Minute, Second) of connection set-up
XXXXX:	Name of distant station (from the telephone directory)
YYYY:	Serial number

The AVI files can be reproduced using *iGuard® Player*.

4.11 Cash box data search

The configuration of the cash box search in *iGuard® RemoteView* corresponds to the function in *iGuard®* (see *3.4.7 Search cash box data*). *iGuard® RemoteView* also supports searching for cash box data spanning multiple servers. The results are displayed together in a server list.

For the cash box search, *iGuard® RemoteView* must be linked to one or more servers. A search for cash box data can be activated in rendering mode by selecting *View → Cash box search* or via the button on the toolbar.
To search for and render cash box data, the following options are possible:

- Entry of search criteria as freely definable text (substring search). The search is case insensitive. Two search words separated by a comma may be entered. This will find only those entries where both substrings occur. A search with wildcards is possible.
- Entry of a time period for the search (*from, to*); start and end may be left open.
- Entry of the server on which the search is to take place. You can either select *all servers* or individual server names.
  If you have entered an individual server, you can search *all cash boxes* for this server or one individual cash box.

The search results are listed in a table and can be selected. The rendering is based on an entry selected in the table, less an offset and a post-trigger time, both of which can be set. Once the post-trigger time has elapsed, the system jumps automatically to the next entry in the table and the frames are rendered taking into account the pre-trigger. The table entry currently displayed is marked.
The data that has been saved for a frame is shown within the frame.
Individual frames can be exported as JPG or BMP files. The associated cash box data is exported in a text file (ASCII) with the same file name and the ending TXT. It is also possible to print a frame with text underneath it.

4.12 AVI export

With *iGuard® RemoteView* it is possible to carry out AVI export. This AVI export runs in *iGuard® RemoteView* according to the same pattern as in the playback mode of *iGuard®* (see *3.4.15 Export of AVI-Files*). *iGuard® RemoteView* sends the command to the *iGuard®* server. The server generates film sequences locally in the *Upload* directory which is located in the work directory (usual path: "C:\Programs\IDS\iGuard\Upload“) and transmits these files to *iGuard® RemoteView* via the network and or ISDN.

Sufficient storage space must be available on the hard disc where the *iGuard®* work directory is located (usual path: "C:\Programfiles\IDS\iGuard“).

Transmission of AVI files, above all via the telephone network, can take a long time (several hours) because they are usually large and cannot be compressed any more. *iGuard® RemoteView* cannot accept any other inputs from the user during transmission. A progress display notifies the user about the progress of the transmission (see *3.1.20 Please-wait-dialog*)

4.13 Raw data removal

Along with an AVI export, using *iGuard® RemoteView* it is now also possible for *iGuard®* to generate a copy of all video recordings including the database for a preset period and transmit that to the *iGuard® RemoteView* system. Thereby all video files of all cameras are copied without change, which were generated during the defined period. An extract from the database which also corresponds with the required period is also generated.
The advantage of this process is that all known playback and search functions are available with this copy together with *iGuard® RemoteView* and a very fast and comfortable evaluation of the recordings can be accomplished offline after the raw data removal.

Procedure
During an existing connection to an *iGuard®* server, a specify range can be defined with the help of the timeline (cf. *3.4.8 Timeline*). Using the **menu** *File → Backup* the dialog is called up where the directory is specified where the data extract should be stored.

In the case of raw data extraction – unlike recording – the database and video data files are always stored in the same and always only in one directory. The database is given the name *iGuard_Backup.vdb*. There must not be any other database files with the ending .vdb in the specified directory. The directory should be empty. A network directory, however, can also be used.

Figure 137: Menu File

iGuard® now generates first of all a database extract (*iGuard_Backup.vdb*) which contains all entries for the specified period and transfers this file to the

iGuard® RemoteView client. The client evaluates the database file and orders gradually from the server the video files belonging to the database entries. The video files are transferred as direct copies of the original. This is why a slightly larger period of time may be saved in the video files than was specified by the user.
The connection to the server can be disconnected once all files have been transmitted. Using *iGuard® RemoteView* it is then possible to open the database iGuard_Backup.vdb offline (analogue to *Analysis of exchangeable hard disks*). All known analysis possibilities are now available.
If the connection to the server is interrupted while the video data is being copied or if copying is aborted by the user, it is possible to continue transfer of the missing video data at a later date. This is achieved by setting up a connection again to the same *iGuard®* Server and switching to playback. Without having to mark any range beforehand in the timeline, data extraction can be started again immediately from the **menu** *File → Data extraction* Specify the same directory where the previously aborted data extraction is saved. *iGuard® RemoteView* now analyses the database *iGuard_Backup.vdb* that is stored there and requests the missing files from the server.

Please note that the missing files can no longer be copied if they have been deleted in the meantime by the server. In addition, a connection with the same server system has to be set up as before.

4.14 Evaluation of video sequences in playback mode

Just as with *iGuard®*, it is possible within *iGuard® RemoteView* to playback and revise video sequences as being in the *playback mode* of the server. To do this, the *Playback* authorisation is necessary. The *playback mode* of *iGuard® RemoteView* is opened via the **menu** *Administration → Playback*, or by pressing the button . The dialog box which then opens corresponds almost exactly to that in *iGuard®* which is described in *3.4 Playback mode*. A difference to iGuard® is that some functions for manual reorganisation of the database are not available.
Pressing the  button will leave the *playback mode*.

4.15 Data transfer

In order to be able to transfer files from the server to RemoteView and reverse, a file transfer function was released.

This function is only available for administrators.

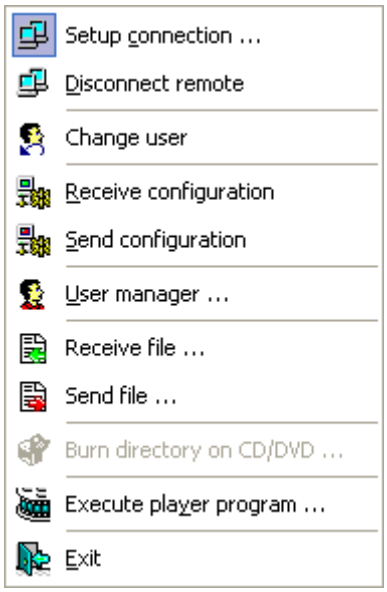


Figure 138: Menu File

To start the data transfer in *iGuard® RemoteView* click *Receive file…* or *Send file…* from the *File* menu. Data transfer in *iGuard® RemoteView* requires a connection to a server.

Send file

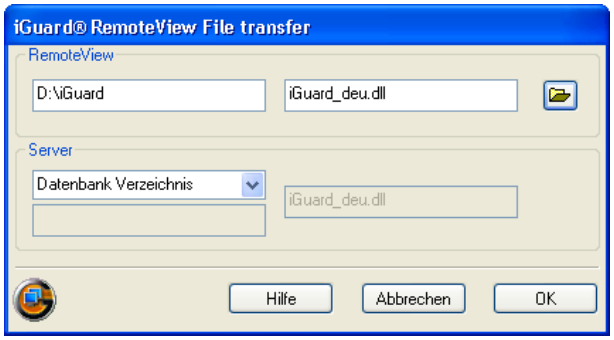


Figure 139: Send file

In order to transfer a file to the server, first the file to be transferred must be selected. Then the directory on the server must be specified. The file name of the source file and the target file is identical.
A file transmission is possible only if the selected listing on the server exists and the file to be transferred is not opened.

Receive file

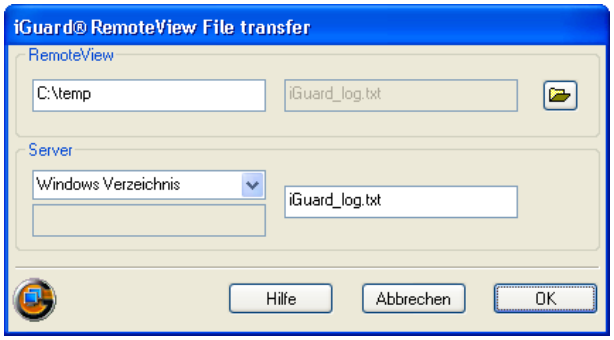


Figure 140: Receive file

The data receipt runs analogue to the data transmission.

4.16 Remote control of switch outputs

Here switch outputs can be activated the, which were configured accordingly. For this the authorisation *remote control* is necessary.

Figure 141: Remote control of Switch outputs

The switch outputs are activated by clicking onto the LED-symbol. Switch outputs which were configured with *pulse-negative/positive mode* cannot be deactivated, because the length of the pulse was determined in the configuration and should not be changed manually.

4.17 Local revision of existing databases

In iGuard® RemoteView databases may also be revised without a direct connection to the recording *iGuard®*-system. Both Message and Record Database must be available for this to take place.
This enable to operate *iGuard®* with removable hard disks also and carry out the revision locally on external PCs using *iGuard® RemoteView*. However, to do this both databases must be written to the removable hard disk. These settings are described in chapter *3.1.4 Operation using removable hard disks*.
A database is opened via the **menu** *Administration → Playback* or clicking on the button in the symbol bar. The dialog box *Select Directory* will then appear, in which the directory containing the database should be entered and the database clicked on. After confirmation using the *Select* button, the database is loaded and the same dialog box as in the *iGuard® playback mode* will appear. The revision can be carried out in the same way as in *iGuard®*, as all functions are available.

4.18 Remote-System-Reboot

Via the **menu** *Action → system* a reboot of the server system can be accomplished. For this *Administration* authorisation is necessary. In order to be able to accomplish the reboot actually, 3 safety queries must be acknowledged. So that *iGuard®* starts again automatically after a Reboot, the following conditions must be fulfilled:

- automatic login
- *iGuard®* in the Auto start file (the Setup enables this automatically)

Only after the restart a connection to *iGuard®* can take place. The restart can take quite 1 minute or more.

If *iGuard®* is not configured to begin immediately after a restart with the recording, no recording will take place after reboot. However, the recording can be started via remote-control at any time.

4.19 Configuration of *iGuard®* using *iGuard® RemoteView*

Via *iGuard® RemoteView*, It is also possible to do a remote configuration of an *iGuard®* server. *iGuard® RemoteView* contains the same dialogs for changing the configuration as are used for *iGuard®* server application (see 3.3 Configuration mode). The functions of the dialogs and dialog elements are therefore the same.

The following restrictions should be noted in this respect:

- *iGuard® RemoteView* 2.80 can be used to configure servers with *iGuard®* version 2.70. If this configuration is done online (see below), only the functionality of the offline configuration is available.
- Recording media (hard disk partitions) cannot be changed
- A database directory cannot be specified
- The language version cannot be changed
- The option *Always in foreground* cannot be changed
- The option *On-screen keyboard* cannot be changed
- Masks for motion detection by cameras cannot be changed
- Network parameters cannot be changed
- Live image display of camera signals is not possible

Changing the configuration of an *iGuard®* server is possible in 2 ways:

- Online, i.e. transmission of configuration, changing configuration, playing back configuration, starting configuration on the server.
- Offline, i.e. an existing configuration is edited without connection to the server; a connection is then established and the configuration sent to the server.

Procedure for possibility A):
Select **menu** *Administration → Configuration* during an existing connection.

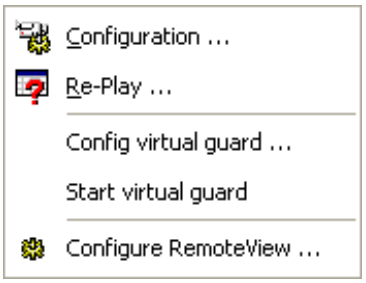


Figure 142: iGuard® RemoteView – menu Administration

Answer question with "Yes"

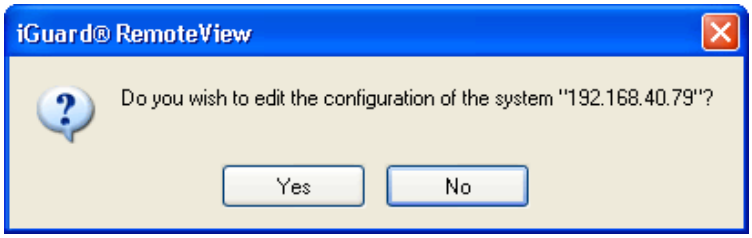


Figure 143: iGuard® RemoteView – configuration option for server

- The configuration file from the server is transmitted and stored in the download directory. *iGuard® RemoteView* then opens this file automatically and changes to the configuration level
- Changes to the configuration by the user with the aforementioned restrictions.
- Quit the configuration level
- Answer question with "yes" and send configuration to the server

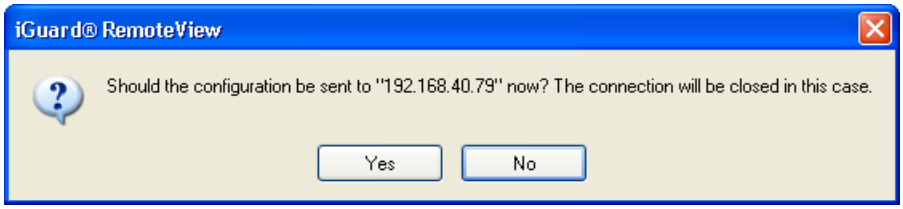


Figure 144: iGuard® RemoteView – transmission option for server configuration

- The transmission takes place. Upon receipt of the configuration, it is copied to memory by the server and then started. Recording is stopped for a few seconds for this.
- The user should now check that the server is recording again and running correctly, insofar as this can be assessed from a remote location.

The transmission of a new configuration is recorded in the server logbook as info-message. The logbook also records whether the server has accepted and started the new configuration.

If a configuration contains more cameras than are available to the recording system, only the first *n* cameras of the configuration are accepted. All other cameras are ignored. This also applies for objects that are included in a configuration but do not exist on the hardware side of the recording system (e.g. external monitor output, more than 8 trigger inputs).
Settings which are not configurable (see above) such as recording drives or network settings are not taken over by the server from the new configuration. The system continues using the existing settings for these parameters. This is aimed at avoiding malfunctions.

In the event of a server crash as a result of remote configuration, the installed watchdog can trigger a computer re-set. If the computer has been configured so that *iGuard®* starts automatically, it is possible that the malfunction will be remedied with the restart. In the event of a malfunction as a result of a remote configuration of the server, it is still accessible by telecommunication and can be re-started using *iGuard® RemoteView* (**menu** *Action → System restart*). In this case as well, the server must have been configured so that *iGuard®* starts automatically when the computer is started again.
The *Send configuration* function corresponds with the *Import configuration* function with the difference that the configuration file is sent to the server by telecommunication. Transmission errors should be detected by a checksum that is included in the configuration file. Configurations with incorrect checksum are not imported.

Procedure for possibility B):
Configuration files for offline configuration can be transmitted or received during an existing connection in the **menu** *File*.

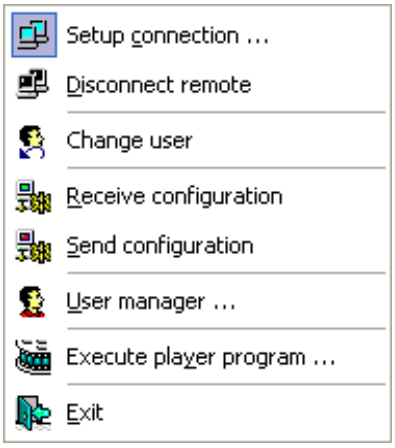


Figure 145: iGuard® RemoteView – menu File

The *Receive configuration* function enables the Administrator to receive a copy of the configuration from *iGuard®* Server and to edit this with *iGuard® RemoteView* (without actual telecommunication connection). The function *Transmit configuration* enables the Administrator to select a file and send this file to the *iGuard®* Server.
The connected user needs *configuration* authorisation for remote configuration. No authorisation is required for editing a configuration offline with *iGuard® RemoteView*. To this extent, it is possible for any user to change a configuration file. Transmitting this file to the server, however, requires the appropriate authorisation.

4.19.1 Changing user data

It is also possible to carry out remote alteration to user data as part of remote configuration. However, this is only possible *online* for security reasons. The logged in user that would like to change user data needs *Configuration*, *Remote access* and *User management* authorisation. Operation is analogue to operation on the server. The changed user data is transmitted simultaneously to the server system upon completing the user management dialog.

4.19.2 Picture output on an analogue monitor at the server

The remote configuration also permits images to be output on an analogue monitor that is connected to the server.

4.19.3 Remote configuration of the motion mask

It is possible to generate and alter camera motion masks. Drawing the mask is the same as with the server (see *3.3.2 Configuration of the cameras*). The drawing tool *Pen*, however, is not available.
Camera images are visible insofar as the server camera is currently supplying images, i.e. it has not failed.
The image quality is the same as selected at the monitor level of *iGuard® RemoteView* (ISDN) or set by the system (LAN).
If the camera does not supply any image, the mask is displayed in a grey window. In this case, the mask can also be edited, though without a camera image this leads to an extremely imprecise result.
Unlike the server system, there is no system status signal about detected movements (graphic, sound signal, signal lamps).

4.20 Accomplish software updates

Accomplishing a software update, the following requirements must be fulfilled:

- *iGuard® RemoteView* must be started.
- the *iGuard®* server to be updated must be connected before
- the *iGuard®* server to be updated must be configured in such a way, that *iGuard®* starts automatically (*iGuard®* in the autostart group) after a restart of the operating system (Auto login)
- The login on the *iGuard®* server must take place with administrator rights.
- The self extracting update file, which was provided by the *IDS Imaging Development Systems GmbH*, must be available.

The *iGuard®* server to be updated must at least have version 2.57 and the update archives must be applicable for the version of the *iGuard®* server. It is not possible to accomplish the software update of the current *iGuard®* version on an earlier *iGuard®* version (Upgrade not possible). In this case an error message appears.

Over the **menu** *Action → Software update* a *file open* dialogue is opened in the display mode. In this dialogue the self extracting update file which is to be used for the procedure is to be selected.
Thereupon *iGuard®* accomplishes the update. Afterwards the operating system (if necessarily) and *iGuard®* are re-started, if the computer is configured accordingly.
During the update all *iGuard®* actions, mainly the recordings, are stopped and the connections to *iGuard® RemoteView Clients* are disconnected.

The connections to *iGuard*® *RemoteView Clients* can only be reconnected by the user after the software update and the associated restart of the operating system (if necessarily) and *iGuard*®. This can quite take some minutes.

It cannot be guaranteed under all circumstances that the automatic update procedure is successfully implemented. In the case of a not successful accomplished update procedure it will be tried automatically to undo all changes.

This procedure can fail also.

The *IDS Imaging Development Systems GmbH* makes expressly attentive to the fact that it can be necessary that the user must start up the *iGuard*® server system manually. The user must be aware of this risk.

The *IDS Imaging Development Systems GmbH* excludes any liability for damage, which result from a not successful accomplished software update.

5 iGuard® Player

5.1 Start from iGuard®

The *iGuard® Player* can also be started from *iGuard®* or *iGuard® RemoteView* using the **menu** *File → Execute player program* insofar as it is installed in the Windows or *iGuard®* directory.

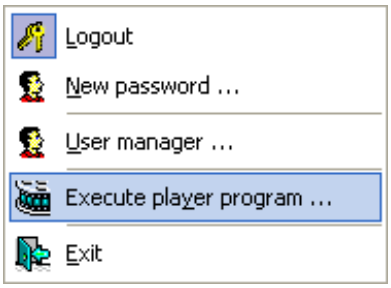


Figure 146: Menu File in - start iGuard® Player

Playback authorisation is required to start the Player.

The *iGuard® Player* can only be opened in one instance. This means that a multiple display of the Player on the screen is not possible.

5.2 Functionality

iGuard® Player is supplied free of charge with *iGuard®*. Using the *iGuard® Player* you can open and playback any AVI files created from *iGuard®* in the MJPEG format (including sound). Images, which were stored from *iGuard®* in the JPG/BMP format, can be shown likewise.
After starting the program, *iGuard® Player* will display the following dialog box:

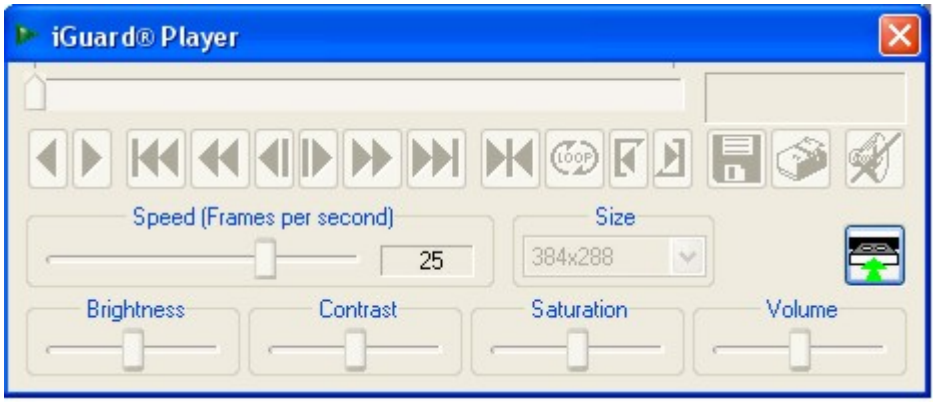


Figure 147: iGuard® Player

The language of the iGuard® Player adjusts to the language of the operating system. Only one button is active when started. This allows a video file to be loaded which is explained in more detail in the following section.

5.3 Load AVI-file

After activating the button the Windows standard dialog box for opening a file will open. Here one or more files are selected in used way. According to the used operating system, the dialog box may vary slightly from the Open dialog displayed below. With the selection of several files these are played successively in alphabetical order.
As an alternative, AVI files may also be opened and played back simply by using Drag and Drop. To do this, the files must be moved into the *iGuard® Player* dialog box by pressing the left mouse button and then the mouse button must be released.

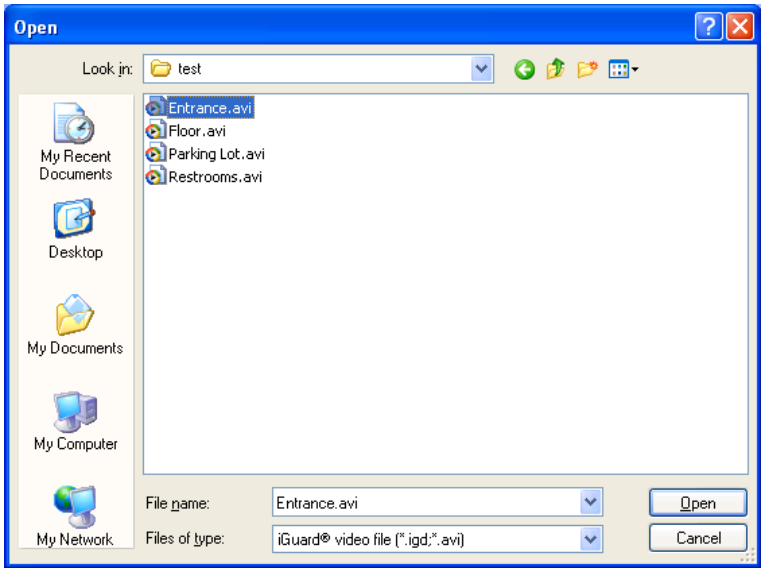


Figure 148: Playing AVI Files

Once the required file has been opened, a further window for the video film is displayed next to the dialog window. This window may be freely moved around the screen independently of the dialog window. As soon as the mouse pointer is placed within the video window it is shown as a small magnifying glass and the *iGuard® Player* **zoom function** is activated. It is now possible, by operating the left mouse button, to mark an area within the video image, also during playback, and have this displayed to fill the window (Zoom In). After double-clicking the left mouse button within the window the display will return to its original size (Zoom Out).

Figure 149: Video sequence-dialog window

5.4 Summary of operating elements

The meanings of the various buttons used to operate the *iGuard® Player* are contained in the listing below (further details see ***Fehler! Verweisquelle konnte nicht gefunden werden.***). These are for the most part self-explanatory and are based on the keys and symbols of a standard video recorder.


Rewind video


Playback video (Play)


Stop; This symbol appears after activation of the playback field to stop the video. The final picture is frozen.


Jump to start of video


Fast rewind


Individual picture backwards


Individual picture forwards


Fast forward


Jump to end of video


Go to specified picture. After activating this field a small dialog will open to enter the picture number.

Start loop mode

Stop loop mode


Start of loop


End of loop


Save current picture as BMP-file or JPEG-file


Print current picture


Sound on/off


Open video file


Close video file

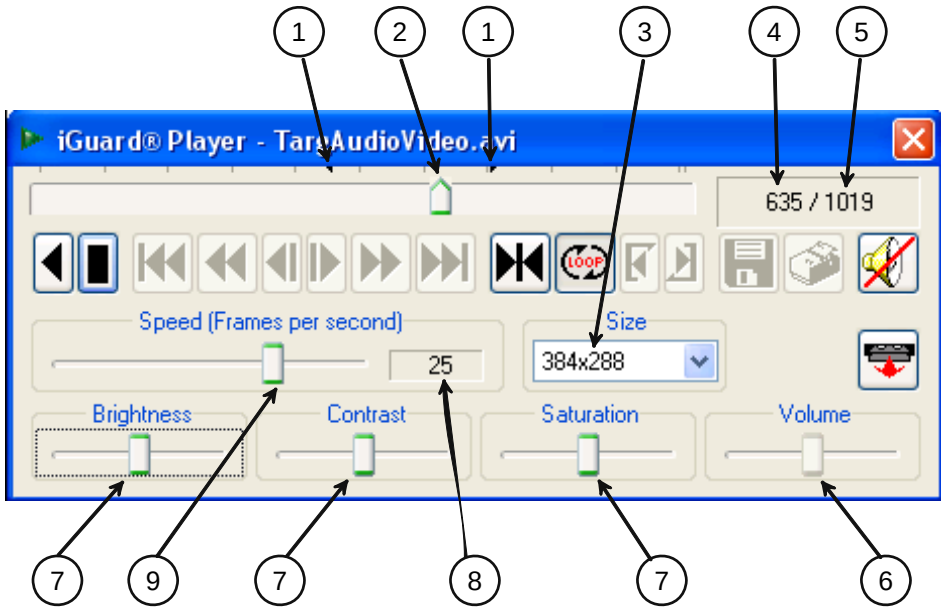


Figure 150: iGuard® Player – control elements

1 Marked range of defined loop
2 Current position in video file
3 Size of the display window in pixel
4 Current picture number
5 Number of pictures in the whole file
6 Volume control
7 Setting the image parameters. The default parameters can be reset for each slide control by clicking with the right mouse button. The settings are accepted for other files.
8 Playback speed with reference to recording speed from 0.1FPS to 200 FPS. The 25 setting means that playback is at original speed. FPS = Frames per second
9 Current playback speed setting

Using the button, it is possible to jump directly to a specified picture. To do this, enter a numerical value between 1 and the number of pictures in the video sequence.

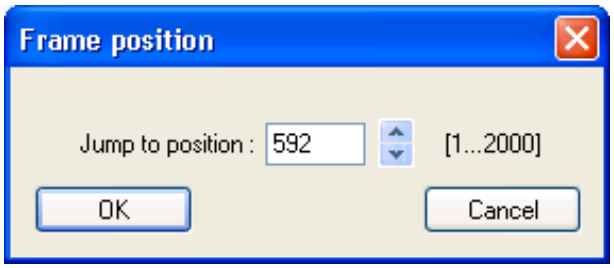


Figure 151: Jump to specified picture

5.5 Video signal window and full-frame mode

The following sizes are available for displaying the video signal window:

96	x	72	Pixel
176	x	132	Pixel
192	x	144	Pixel
320	x	240	Pixel
352	x	240	Pixel
352	x	288	Pixel
384	x	288	Pixel
576	x	432	Pixel
640	x	480	Pixel
704	x	480	Pixel
768	x	576	Pixel

Apart from these fixed resolutions further resolutions are available. These are determined from the resolution of the recording and the screen resolution.

The full-frame mode is activated by pressing the key combination *Ctrl+F*. Replay can be controlled using the keyboard in this mode. To quit this mode, press *ESC* or *Ctrl+F* again.

Key combinations in full-frame mode:

Ctrl + F	Switch full-frame mode on/off
ESC	Quit full-frame mode
Ctrl + O	Open video file
Arrow key left	One frame back
Arrow key right	One frame forwards
Space (bar)	Play video file/stop replay

5.6 Loop mode

iGuard® Player can mark certain periods of time within the sequence and play these in an endless loop. To do this the button is to be activated. The two symbols for marking the start and end of the endless loop are then activated. Marking is done by using the mouse to place the cursor on the required start position of the endless loop. The symbol should then be activated. In the next stage the cursor is placed in the same way on the end position. Activating the loop end field will end the procedure.

5.7 Show serial number

With the export of AVI files (see *3.4.15 Export of AVI-Files*) additionally the serial number of the appropriate system is stored in the AVI file. This can be displayed in *iGuard® Player*. Therefore the *iGuard®* symbol must be clicked with the right mouse button and the menu item *Properties* is to be selected.

Figure 152: Open iGuard® Player menu

The window show in the following is opened.

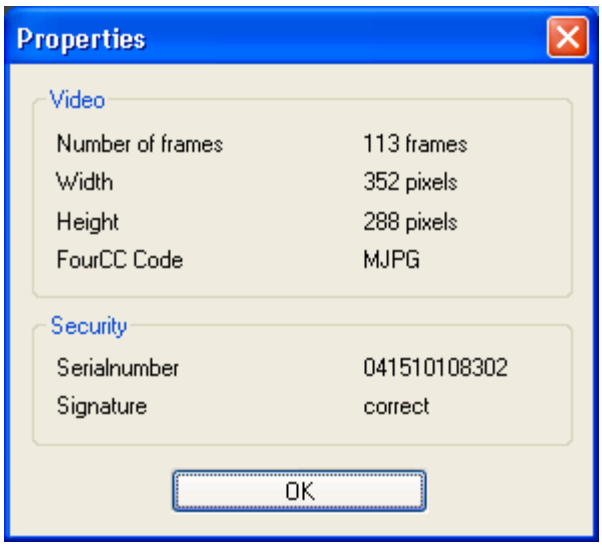


Figure 153: iGuard® Player properties

The field video informs about

- the number of pictures contained in the AVI file
- the resolution of the pictures
- the codec used with the compression (**** coded file)

In the field *Security* the serial number and the status of the signature are deposited.

5.8 Checking signature file

When a file is exported, it is always assigned a signature (see *3.4.15 Export of AVI-Files*). When the *iGuard® Player* opens a file, it checks whether that file has a signature. If so, the status of this signature is checked.
If the file is authentic, i.e. it has not been altered, a small lock icon appears after the file is opened in the program window. Otherwise the unlock icon is shown.

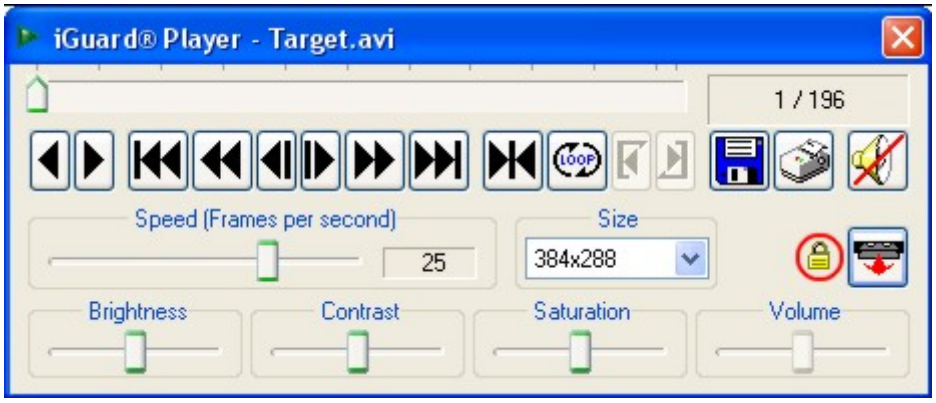


Figure 154: Opening a signatured file

Table of figures

