

# DiBos/DiBos Micro



**BOSCH**

en Installation Guide



# Table of Contents

<b>1</b>	<b>Safety Notes</b>	<b>7</b>
<b>2</b>	<b>Introduction</b>	<b>11</b>
2.1	System Description	11
2.2	Unpacking	11
2.3	Power	11
2.4	Environmental	11
2.5	Recommended Virus Scanners/Firewall	12
2.5.1	Virus Scanners	12
2.5.2	Firewall	12
2.6	System Overview/Technical Specifications	14
2.6.1	DiBos	14
2.6.2	DiBos micro	18
<b>3</b>	<b>Device Connections</b>	<b>21</b>
3.1	DiBos	21
3.1.1	DiBos Front View	21
3.1.2	DiBos Rear View	22
3.1.3	Grabber Card for DiBos	23
3.1.4	I/O Card for DiBos	24
3.2	DiBos micro	25
3.2.1	DiBos micro Front View	25
3.2.2	DiBos micro Rear View	26
3.2.3	Grabber Card for DiBos micro	27
3.2.4	I/O Card (for DiBos micro)	28
<b>4</b>	<b>Quick Installation</b>	<b>30</b>
<b>5</b>	<b>Quick Configuration</b>	<b>31</b>
5.1	General Settings	31
5.2	Creating a User	33
5.3	Setting up the Network	34
5.4	Specifying Cameras	36
5.5	Assigning Time Profiles	37
5.6	Setting Up Recording	38
<b>6</b>	<b>Default Configuration</b>	<b>40</b>
6.1	Configuring Drives	40
6.2	Configuring Video and Audio Connections	42
6.2.1	General Camera Settings	44
6.2.2	Setting up Dome Cameras and Pan/Tilt Cameras	46
6.2.3	Specifying Monitoring Zone for Motion Cameras	49
6.2.4	Configuring Tamper Detection	50
6.2.5	Configuring Video Monitors	52
6.2.6	Configuring camera sequence	53

6.2.7	Editing Audio Settings	54
6.2.8	Configuring JPEG IP Cameras	55
6.2.9	Configuring MPEG4 IP Cameras	58
6.3	Configuring Recording Settings	60
6.3.1	Configuring Recording Settings for Analog Cameras	60
6.3.2	Configuring Recording Settings of JPEG IP Cameras	67
6.3.3	Configuring Recording Settings of MPEG4 IP Cameras	69
6.4	Configuring Time Periods	71
6.5	Configuring Inputs and Outputs	73
6.5.1	Configuring Alarm Inputs	73
6.5.2	Configuring Relay Outputs	74
6.5.3	Configuring Alarm Simulation	75
6.5.4	Configuring Virtual Inputs	76
6.5.5	Configuring Automatic Teller Machines	77
6.5.6	Configuring Foyer Card Readers	79
6.5.7	Configuring AP Inputs	82
6.5.8	Configuring POS Inputs	86
6.5.9	Configuring ATM/POS Inputs	88
6.6	Configuring Alarm Processing	90
6.7	Configuring Remote Stations	94
6.8	Configuring Alarm Transmission	97
6.9	Configuring the Export Video Scheduler	100
6.10	Creating Authorization Levels	102
6.11	Configuring Users	107
6.12	Configuring Error Forwarding	109
6.13	Configuring Options	111
6.13.1	MIB List for SNMP	114
6.13.2	Notification via SNMP	115
6.13.3	Configuring Automatic Alarm Recording	116
6.14	Configuring Browser Access and Network Settings	117
6.15	Administration and Dongle	119
6.15.1	Activating a License	122
<b>7</b>	<b>Remote configuration</b>	<b>123</b>
<b>8</b>	<b>XP Administration</b>	<b>124</b>
8.1	Logging On as a Windows® XP User	124
8.2	Logging On as a Windows® XP Administrator	124
8.3	Changing the Administrator Password	124
<b>9</b>	<b>Connections</b>	<b>125</b>
9.1	Network Connection via DSL	125
9.2	Connecting the ISDN Controller	128
9.3	Connecting VSCom 200 H (Interface Expansion)	129
9.4	Connecting External Hard Disks	129
9.5	Connecting a Malfunction Relay	129
9.6	Connecting an ATM (Serial)	130
9.7	Connecting the MINITER RS 485 Foyer Card Reader	134
9.8	Connecting the DCF 77 Radio Clock	137

---

9.9	Connecting a Modem/ISDN Card (for Incoming Connections)	139
9.10	Connecting to AutoDome/SAE Dome	141
9.10.1	Connecting to Bosch Dome Cameras (Directly)	141
9.10.2	Connecting to Bosch Dome Cameras via Matrix Switch	141
9.10.3	Connecting to SAE Dome Cameras (Directly)	142
9.10.4	Connecting to SAE Dome Cameras with V3032 Biphase Interface	142
9.11	Connecting an AP	143
9.11.1	General	143
9.11.2	Connecting to NZ 500 (20 mA) Video System NZ 500	145
9.11.3	Connecting to BZ 500 (20 mA)	145
9.11.4	Connecting to AZ 1010/NZ 1008	146
9.11.5	Connecting to NZ 1012	147
9.11.6	Connecting to NZ 1060	148
9.11.7	Connecting to UEZ 1000 (20 mA)	149
9.11.8	Connecting to UEZ 2000 (20 mA)	149
9.11.9	Connecting to UGM 2020	150
<b>10</b>	<b>Troubleshooting and Checks</b>	<b>151</b>
10.1	Troubleshooting	151
10.2	Checking the Optional Network Connection	152
10.3	Checking the Optional ATM Connection	153
10.4	Checking the Optional Web Connection	154
<b>11</b>	<b>Notes on Service and Maintenance</b>	<b>155</b>
11.1	Maintenance Work to be Carried Out	155
11.2	Software Update	156
11.3	Troubleshooting	156

---



# 1 Safety Notes

The following safety notes must be observed:

1. **Read, follow and retain instructions**

All safety and operating instructions must be read and followed before installing the device. Retain instructions for future reference.
2. **Observe warnings**

Observe all warnings on the device and in the operating manual.
3. **Add-on devices**

Do not use add-on devices that are not recommended by the product manufacturer as these may cause hazards.
4. **Installation notes**

Do not place the device on an unstable mounting, tripod or similar. The device may fall to the ground and seriously injure the user or be damaged itself. Only use accessories that have been recommended by the manufacturer or are delivered with the device. Fit the device according to the manufacturer's instructions. Exercise extreme caution when transporting the device on a trolley. Abrupt stopping, extreme force effects and uneven surfaces may cause the device and the trolley to tip over.
5. **Cleaning**

Unplug the device from the mains power supply before cleaning. Follow all instructions for the device. Normally, cleaning can be carried out with a damp cloth. Do not use liquid cleaners or cleaners in spray cans.
6. **Service**

Do not attempt to service the device yourself. You may be exposed to high electrical voltages or other hazards if you open or remove covers. Servicing must be carried out by qualified maintenance personnel.
7. **Damage requiring service.**

Unplug the device from the mains power supply and arrange for the device to be serviced by qualified personnel if:

  - The mains cable or mains plug is damaged.
  - Liquids or foreign bodies are present in the device.
  - The device has come into contact with water and/or has been exposed to extreme environmental conditions (e.g. rain, snow etc.).
  - If the device does not work properly in spite of following the operating instructions, make changes only to those operating elements that are described in the operating instructions. Incorrect changes to other operating elements may cause damage requiring extensive repair work to be carried out by qualified service personnel.
  - The device has fallen to the ground or the housing has been damaged.
  - A noticeable change in the performance of the device has occurred. In this case, the device must be serviced.
8. **Spare parts**

If spare parts are required, service personnel must use spare parts that are recommended by the manufacturer or correspond to the original parts. Using the wrong spare parts may result in fire, electric shock or other hazards.
9. **Safety test**

When servicing or repair is complete, ask service personnel to carry out a safety test to ensure that the device is working correctly.

**10. Power source**

The device must only be operated with the power source indicated on the label. If you are not sure whether you can operate the device with a specific power source, ask the dealer from whom you bought the device or your electricity provider.

You will find more information on devices that can be operated with batteries in the operating manual.

For devices that are operated using external power units, only recommended and tested power units should be used.

For devices that are operated using power units with limited power, the power unit must conform to the EN 60950 standard. Other replacement power units may damage the device and lead to fire or electric shock.

For devices that are operated using 24 V AC, the normal input voltage is 24 V AC. The input voltage to the device should not exceed 30 V AC. The wiring provided by the customer for connecting the power source to the device (24 V AC) must conform to electrical codes (Class 2 power stages). The power source (24 V AC) must not be grounded at the connectors or the power supply connections on the device.

**11. Coax grounding**

If a cable system is connected to the device for outside use, ensure that the cable system is grounded. Only for models available in the USA: Section 810 of the National Electrical Code, ANSI/ NFPA No.70-1981, contains information on the correct grounding of the mounting, coax grounding at a discharge device, the size of the ground conductors, the location of the discharge device, connection to discharge electrodes and requirements regarding the discharge electrodes.

**12. Grounding or polarizing**

This device may have a polarized AC plug (a plug with one pin broader than the other). With this protection system, the plug can only be inserted into a socket in one way. If you are unable to insert the plug fully into the socket, rotate it and try again. If you are still unable to insert the plug, ask an electrician to replace the socket with a later model. Do not attempt to bypass the polarized plug.

Alternatively, the device may have a 3-phase ground plug with a third (grounding) pin. With this protection system, the plug can only be inserted into a grounded socket. If you are unable to insert the plug into the socket, ask an electrician to replace the socket with a later model. Do not attempt to bypass the grounded plug.

**13. Lightning**

For added protection of the device during a storm, or when it is not used for a lengthy period of time, unplug the device from the mains and disconnect the cable system. This prevents the device being damaged by lightning or a power surge.

14. The installation location should be quiet and have only **limited access**.



**Devices for inside use**

**Water and damp** – Do not use this device in the vicinity of water (e.g. in a damp cellar) or in humid locations.

**Entry of foreign bodies and liquids** – Do not insert foreign bodies into the device openings as you may touch parts that are at high-voltage or cause a short circuit, which may result in fire or electric shock. Do not spill liquids on the device.

**Mains cable and mains cable protectors** – For devices that operate at 230 V AC, 50 Hz, the input and output mains cables must conform to IEC publication 227 or IEC publication 245. Mains cables should be laid in such a way that no one can step on them and no other objects can be placed on top of them or leant against them. Particularly protect cables, plugs and sockets as well as device entry points.

**Overloading** – Do not overload sockets and extension cables as this may result in fire or electric shock.

**Rack-mounting devices**

**Ventilation** – This device should not be installed anywhere where correct ventilation cannot be ensured or the manufacturer's instructions cannot be followed. The maximum operating temperature for this device must not be exceeded.

**Mechanical load** – When installing the device in a rack, beware of hazards that may arise due to unequal mechanical load.

**WARNING!**

Interruption of mains supply:

Voltage is applied as soon as the mains plug is inserted into the mains socket.

However, for devices with a mains switch, the device is only ready for operation when the mains switch (ON/OFF) is in the ON position. When the mains plug is pulled out of the socket, the supply of power to the device is completely interrupted.

**WARNING!**

Removing the housing:

To avoid electric shock, the housing must only be removed by qualified service personnel. Before removing the housing, the plug must always be removed from the mains socket and remain disconnected while the housing is removed. Servicing must only be carried out by qualified service personnel. The user must not carry out any repairs.

**WARNING!**

Lithium battery:

Batteries that have been inserted wrongly can cause an explosion. Always replace empty batteries with batteries of the same type or a similar type recommended by the manufacturer. Dispose of empty batteries according to the manufacturer's instructions.

**CAUTION!**

Electrostatically sensitive device:

To avoid electrostatic discharges, the CMOS/MOSFET protection measures must be carried out correctly.

When handling electrostatically sensitive printed circuits, grounded anti-static wrist bands must be worn and the ESD safety precautions observed.

**NOTICE!**

Installation should only be carried out by qualified customer service personnel in accordance with the applicable electrical regulations.

---

**Disposal**

Your Bosch product has been developed and manufactured using high-quality materials and components that can be reused.

This symbol means that electronic and electrical devices that have reached the end of their working life must be disposed of separately from household waste.

In the EU, separate collecting systems are already in place for used electrical and electronic products. Please dispose of these devices at your local communal waste collection point or at a recycling center.

---

## 2 Introduction

### 2.1 System Description

The video system is a digital monitoring system that allows video images to be stored locally and transmitted and evaluated at any place determined by you independently of distance and location. The image data delivered by the video system provides additional information on the magnitude of the danger and the developments before and after the event.

### 2.2 Unpacking

Check the packaging for visible damage. If anything is damaged during transport, please inform the freight agency.

Unpack the device carefully. This is an electronic device and it must be handled carefully to avoid damage. Do not attempt to put the unit into operation if components are damaged. If parts are missing, inform your customer service representative or a Bosch Security Systems salesperson.

The shipping box is the safest transport container for the device. Retain the box and the packaging material for future use. If the device has to be returned, use the original packaging.

### 2.3 Power

Ensure that the power supply at the chosen location is stable and is within the values specified for the device.

As this is an electronic device, the video system is sensitive to sudden voltage peaks, dropoff and dropout.

**To avoid damage to the electronic components and/or loss of data and ensure trouble-free operation, we recommend installing an uninterruptible power supply (UPS).**

Depending on the stability of the mains network, the following uninterruptible power supplies are recommended:

- Mains networks with voltage peaks and voltage dropout:  
Use of an offline UPS is sufficient (e.g. Pulsar ellipse 1000 for DiBos and Pulsar ellipse 600 for DiBos Micro).
- Mains networks with voltage peaks, voltage dropout and voltage dropoff:  
Use of an online UPS is recommended.

For 1 video system, a UPS with at least 300 VA is required. If add-on devices (e.g. monitors, sub-systems) are also to be protected, the capacity of the UPS must be raised accordingly.

### 2.4 Environmental

When choosing an installation location for the device, take the ambient temperature and humidity into account.

## 2.5 Recommended Virus Scanners/Firewall

The DiBos operating system is Windows® XP Embedded.

**DiBos is not supplied with a virus scanner or firewall. It is therefore the customer's responsibility to purchase, install and update a virus scanner and firewall.**



### NOTICE!

We recommend that you install a virus scanner and firewall to protect against computer viruses, computer worms and Trojans.

### 2.5.1

#### Virus Scanners

The following virus scanners are released. The virus scanners are listed in order of suitability.

1. Norton AntiVirus 2008  
The software includes a firewall.
2. Trend Micro AntiVirus 2008  
The software does not include a firewall; this must be purchased separately.
3. McAfee VirusScan 2008  
The software includes a firewall.



### NOTICE!

- The virus scanner can affect the performance of the system.
- The real-time virus scanner must be activated to ensure sufficient protection against viruses.
- If possible, all partitions on the hard disk that contain saved images should be excluded from the scanning process.
- If possible, the C drive should be scanned at scheduled times. We recommend you carry out a scan on a weekly basis. When the C drive is scanned, the performance of the system falls significantly, along with the image refresh and storage rates.

#### **Individual images may be lost.**

- Removable drives, e. g. USB memory sticks, USB drives, CD/DVD drives and diskette drives, must be manually checked when inserted to ensure sufficient protection.
- Always use the most up-to-date virus scanner.

### 2.5.2

#### Firewall

On DiBos with Windows XP Embedded and Service Pack 2 (SP2), the Windows firewall is deactivated by default. The Windows firewall can be activated as required.

If the firewall is activated, you must add and select the following exceptions in the firewall settings:

Firewall settings	DiBos 8
Exceptions	ConnectionServer.exe
	DVR ServiceShimWrapper.exe
	DBServer.exe
	DCOM (TCP) Port 135
	DCOM (UDP) Port 135
	DiBosExplorer.exe
	DomeCameraUnit.exe
	JobServer.exe
	VCSModule.exe

---

The DiBos processes must also be activated in the firewall of the virus scanner software. The necessary ports to disable the firewall can be set in the configuration (see also *Section 6.14 Configuring Browser Access and Network Settings*).

---

**NOTICE!**

Always use the newest version of the firewall.

---

## 2.6 System Overview/Technical Specifications

### 2.6.1 DiBos

Electrical data						
Compression technique	MPEG4					
Camera inputs (analog)	6 BNC connections (DB 06 C1), 12 BNC connections (DB 12 C2), 18 BNC connections (DB 18 C3), 24 BNC connections (DB 24 C4), 30 BNC connections (DB 30 C5)					
Camera inputs (IP)	16 video/audio MPEG4 data streams from Bosch/VCS network devices or JPEG devices (DB 06 C1, DB 12 C2, DB 18 C3) 32 video/audio MPEG4 data streams from Bosch/VCS network devices or JPEG devices (DB 24 C4, DB 30 C5)					
Composite video signal	1 Vpp +/-3 dB (min. 0.7 Vpp, max. 1.4 Vpp), 75 Ohm					
Video looping out	Via connecting cable					
Recording resolution (analog inputs)	PAL: 704 x 576 (4CIF), 704 x 288 pixels (2CIF), 352 x 288 pixels (CIF) NTSC: 704 x 480 (4CIF), 704 x 240 pixels (2CIF), 352 x 240 pixels (CIF)					
Recording resolution (IP inputs/Bosch IP devices)	PAL: 704 x 576 (4CIF/D1), 704 x 288 (2CIF), 464 x 576 (2/3 D1), 352 x 576 (1/2 D1), 352 x 288 (CIF), 176 x 144 (QCIF) NTSC: 704 x 480 (4CIF/D1), 704 x 240 (2CIF), 464 x 480 (2/3 D1), 352 x 480 (1/2 D1), 352 x 240 (CIF), 176 x 120 (QCIF)					
Recording rate (analog) for DiBos models	IPS CIF (PAL)	IPS CIF (NTSC)	IPS 2CIF (PAL)	IPS 2CIF (NTSC)	IPS 4CIF PAL	IPS 4CIF NTSC
DB 06 C1 xxx R2	75	90	50	60	25	30
DB 12 C2 xxx R2	150	180	100	120	50	60
DB 18 C3 xxx R2	225	270	150	180	75	90
DB 24 C4 xxx R2	300	360	200	240	100	120
DB 30 C5 xxx R2	375	450	250	300	125	150
Recording rate per channel (analog video inputs)	PAL: 0.5; 1; 2; 3; 4; 5; 6; 8; 12.5; 25 images per second NTSC: 0.5; 1; 2; 3; 5; 6; 7.5; 10; 15; 30 images per second					
Image size (analog video inputs)	Configurable from approx. 1.5 kB to 30 kB (depending on the changes in the image)					
Maximum recording rate (analog and IP)	50 Mbit per second					

Recording rate per channel (IP video inputs)	PAL: 0.5; 1; 2; 3; 4; 5; 6; 8; 12.5; 25 images per second NTSC: 0.5; 1; 2; 3; 5; 6; 7.5; 10; 15; 30 images per second
Image size (IP video inputs)	Configurable up to 3 Mbit per camera
Supported single-channel encoder (Bosch VideoJet series and Bosch VIP series)	VideoJet 10S, VideoJet 1000 VideoJet X10 VIP X1, VIP 10
Supported multi-channel encoder (Bosch VideoJet series and Bosch VIP series)	VideoJet 8004, VideoJet 8004A, VideoJet 8008, VideoJet 8008A, VideoJet X20, VideoJet X40, VIP X2, VIP X2A, VIP X1600
Supported IP cameras from Bosch	Dinion IP, AutoDome IP, FlexiDome IP, Megapixel IP
JPEG protocol	JPEG image query via HTTP
Supported JPEG IP cameras from other manufacturers	IP cameras from Axis, Sony and Mobotix. For detailed information, please contact your local Bosch Security Systems sales office.
Audio inputs	2, 4, 6, 8, 10, cinch sockets (depending on model), line in signal, 16 kHz sampling rate
Audio outputs	1, line out signal, 1/8 inch phone jack (3.5 mm)
Alarm inputs (NO/NC)	32 Switching voltage (high): >2 VDC Switching voltage (low): <0.5 VDC Input voltage: max. 40 VDC Impedance: 22 kOhm pull up (+5 V)
Malfunction relay output (MAL)	1 Voltage range: 30 VAC - 40 VDC Switching current: max. 500 mA AC or DC Breaking capacity: max. 10 VA
Relay outputs (NO/NC)	16 Voltage range: 30 VAC - 40 VDC Switching current: max. 500 mA AC or DC Breaking capacity: max. 10 VA
Video monitor outputs	2, FBAS outputs for single image or sequence displays from connected analog cameras
Bilinx control	For AutoDome control and configuration of Dinion cameras via coax cable
PTZ control	Bilinx: via coax cable for up to 30 AutoDome devices. Biphase: up to 16 AutoDome devices. RS 232: via the console port of any Allegiant matrix switch.
Internal memory capacity	250 GB, 500 GB, 750 GB, 1000 GB, 2000 GB (the operating system and the DiBos software require 8 GB of hard disk memory space)
Video output	1x VGA
Ethernet	10/100/1000 Base-T, settable bandwidth limit

RS 232	2 (for connecting Bosch security systems and Allegiant matrix switches)
USB 2.0	5
DVD burner	Internal. Media supported: CD-R, CD-RW, DVD-R
Power	100 / 240 VAC, 50 / 60 Hz (automatic switchover)
Power consumption (typical)	Approx. 150 W
Power consumption	Max. 210 W
Operating system	Microsoft Windows XP® Embedded
Web browser	Microsoft Internet Explorer 6 or higher, under Windows 2000, Windows® XP or Windows® Vista
Export of video/audio data	DiBos or ASF format onto CD-R, CD-RW, DVD-R, USB device or network drive
Image printer	Via USB (with Windows XP drivers)
External memory capacity	Max. 16 TB
<b>Mechanical data</b>	
Dimensions (H x W x D)	17.5 cm x 48.0 cm x 54.5 cm (7 x 19 x 21.5 inch)
Weight	16–20.4 kg (25–55 lb), depending on the model
<b>Environmental</b>	
Operating temperature	5 °C to 40 °C (41 °F to 104 °F)
Storage temperature	-10 °C to 60 °C (-14 °F to 140 °F)
Relative humidity during operation	15% to 80%, non-condensing
Relative humidity when stored	8% to 80%, non-condensing
<b>Electromagnetic compatibility (EMC)</b>	
– USA	FCC Part 15, Class A
– EU	EMC Directive 89/336/EEC Interference immunity: Conformance with EN 50130-4 requires an external UPS. The product is tested in accordance with EN 50130-4, with the exception of voltage interruption as per EN 50130-4 A2: 2003 Chapter 8.3.4. To comply with EN 50130-4, an external UPS is required. The UPS is not included in the product and must be ordered separately. For information on how to connect a UPS to DiBos, please refer to the DiBos UPS installation handbook. Interference emission: EN 55022 A2, Class B Mains power fluctuations: EN 61000-3-2 Voltage fluctuations: EN 61000-3-3



<b>Safety</b>	
- USA	UL60950-1, 1st issue (2003) CAN/CSA 22.2 No.60950-1-03, 1st issue (2003)
- EU	EN 60950-1: 2003
Warranty	3 years
Released antivirus software	Norton AntiVirus McAfee VirusScan Trend Micro
<b>Order information</b>	
The current order information is contained in the datasheet. Please see: <b><a href="http://www.bosch-securitysystems.com">www.bosch-securitysystems.com</a></b> .	

## 2.6.2

## DiBos micro

Electrical data						
Compression technique	MPEG4					
Camera inputs (analog)	1 connecting cable with 6 BNC connectors (DB 06) or 2 connecting cables, each with 6 BNC connectors (DB 12)					
Camera inputs (IP)	8 video/audio MPEG4 data streams from Bosch/VCS network or JPEG units.					
Composite video signal	1 Vpp +/-3 dB (min. 0.7 Vpp, max. 1.4 Vpp), 75 Ohm					
Recording resolution (analog inputs)	PAL: 704 x 576 (4CIF), 704 x 288 pixels (2CIF), 352 x 288 pixels (CIF) NTSC: 704 x 480 (4CIF), 704 x 240 pixels (2CIF), 352 x 240 pixels (CIF)					
Recording resolution (IP inputs/Bosch IP devices)	PAL: 704 x 576 (4CIF/D1), 704 x 288 (2CIF), 464 x 576 (2/3 D1), 352 x 576 (1/2 D1), 352 x 288 (CIF), 176 x 144 (QCIF) NTSC: 704 x 480 (4CIF/D1), 704 x 240 (2CIF), 464 x 480 (2/3 D1), 352 x 480 (1/2 D1), 352 x 240 (CIF), 176 x 120 (QCIF)					
Recording rate (analog) for DiBos micro models	IPS CIF (PAL)	IPS CIF (NTSC)	IPS 2CIF (PAL)	IPS 2CIF (NTSC)	IPS 4CIF (PAL)	IPS 4CIF (NTSC)
DB 06 C1 xxx Dx	75	90	50	60	25	30
DB 12 C2 xxx Dx	150	180	100	120	50	60
Recording rate per channel (analog video inputs)	PAL: 0.5; 1; 2; 3; 4; 5; 6; 8; 12.5; 25 images per second NTSC: 0.5; 1; 2; 3; 5; 6; 7.5; 10; 15; 30 images per second					
Image size (analog video inputs)	Configurable from approx. 1.5 kB to 30 kB (depending on the changes in the image)					
Maximum data storage rate (analog and IP)	50 Mbit per second					
Recording rate per channel (IP video inputs)	PAL: 0.5; 1; 2; 3; 4; 5; 6; 8; 12.5; 25 images per second NTSC: 0.5; 1; 2; 3; 5; 6; 7.5; 10; 15; 30 images per second					
Image size (IP video inputs)	Configurable up to 3 Mbit per camera					
Supported single-channel encoder (Bosch VideoJet series and Bosch VIP series)	VideoJet 10S, VideoJet 1000 VIP X1, VIP 10, VideoJet X10					
Supported multi-channel encoder (Bosch VideoJet series and Bosch VIP series)	VideoJet 8004, VideoJet 8004A, VideoJet 8008, VideoJet 8008A VIP X2, VIP X2A, VIP X1600, VideoJet X20, VideoJet X40					
Supported IP cameras from Bosch	NWC-0455, NWC-0495, NWC-0700, NWC-0800, NWC-0900, AutoDome IP, Flexidome IP					

Supported JPEG IP cameras from other manufacturers	For detailed information, please contact your local Bosch Security Systems sales office.
Audio inputs	2 (DB06) or 4 (DB12), cinch connection, line in signal, 16 kHz sampling rate
Audio outputs	1, line out signal, 1/8 inch phone jack (3.5 mm)
Alarm inputs (NO/NC)	12 Switching voltage (high): >2 VDC Switching voltage (low): <0.5 VDC Input voltage: max. 40 VDC Impedance: 22 kOhm pull up (+5 V)
Malfunction relay output (MAL)	1 Voltage range: 30 VAC - 40 VDC Switching current: max. 500 mA AC or DC Breaking capacity: max. 10 VA
Relay outputs (NO/NC)	12 Voltage range: 30 VAC - 40 VDC Switching current: max. 500 mA AC or DC Breaking capacity: max. 10 VA
Video monitor outputs	2, FBAS outputs for single image or sequence displays from connected analog cameras
Bilinx control	For AutoDome control and configuration of Dinion cameras via coax cable
PTZ control	Bilinx: via coax cable for up to 12 AutoDome devices. Biphase: up to 12 AutoDome devices. RS 232: via the console port of any Allegiant matrix switch.
Internal memory capacity	250 GB, 500 GB (the operating system and the DiBos micro software require 8 GB hard disk memory space.)
Video output	1x VGA
Ethernet	10/100/1000 Base-T, settable bandwidth limit
RS 232	1
USB 2.0	6
DVD burner	Internal. Media supported: CD-R, CD-RW, DVD-R
Power	100 / 240 VAC, 50 / 60 Hz (automatic switchover)
Power consumption (typical)	Approx. 120 W
Power consumption	140 W
Operating system	Microsoft Windows XP® Embedded
Web browser	Microsoft Internet Explorer 6 or higher, under Windows 2000, Windows® XP or Windows® Vista
Export of video/audio data	DiBos or ASF format onto CD-R, CD-RW, DVD-R, USB device or network drive
Image printer	Via USB (with Windows XP drivers)
External memory capacity	Max. 16 TB

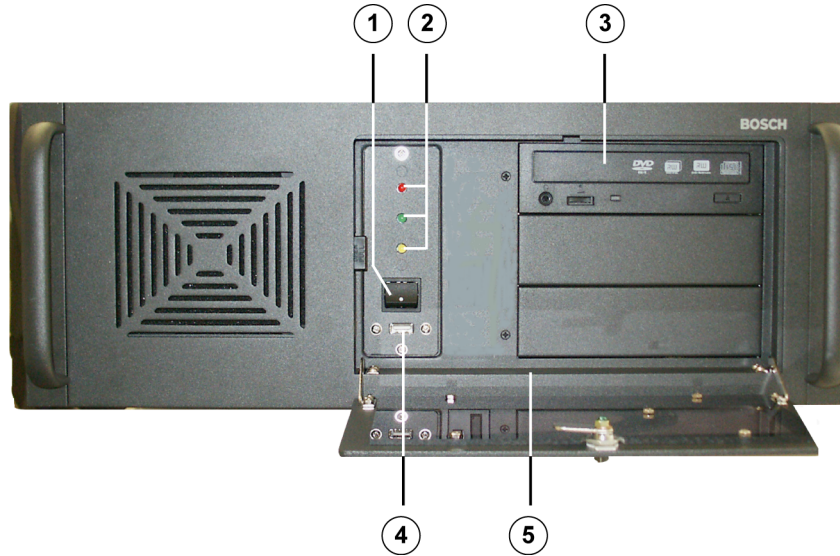
<b>Mechanical data</b>	
Dimensions (H x W x D)	11.5 x 48.0 x 43 cm (4.5 x 19 x 16.9 inches), also 19" rack installation
Weight	Approx. 11.5 kg (approx. 25 lb), depending on the model
<b>Environmental</b>	
Operating temperature	5 °C to 40 °C (41 °F to 104 °F)
Storage temperature	-10 °C to 60 °C (-14 °F to 140 °F)
Relative humidity during operation	15% to 80%, non-condensing
Relative humidity when stored	8% to 80%, non-condensing
<b>Electromagnetic compatibility (EMC)</b>	
- USA	FCC Part 15, Class B
- EU	EMC Directive 89/336/EEC Interference immunity: Conformance with EN 50130-4 requires an external UPS. The product is tested in accordance with EN 50130-4, with the exception of voltage interruption as per EN 50130-4 A2: 2003 Chapter 8.3.4. To comply with EN 50130-4, an external UPS is required. The UPS is not included in the product and must be ordered separately. For information on how to connect a UPS to DiBos, please refer to the DiBos UPS installation handbook. Interference emission: EN 55022 A2, Class B Mains power fluctuations: EN 61000-3-2 Voltage fluctuations: EN 61000-3-3
<b>Safety</b>	
- USA	UL60950-1, 1st issue (2003) CAN/CSA 22.2 No.60950-1-03, 1st issue (2003)
- EU	EN 60950-1: 2003
Warranty	3 years
Released antivirus software	Norton AntiVirus McAfee VirusScan Trend Micro
<b>Order information</b>	
The current order information is contained in the datasheet. Please see: <b><a href="http://www.bosch-securitysystems.com">www.bosch-securitysystems.com</a></b> .	

### 3 Device Connections

The video system is available as DiBos and as DiBos micro.

#### 3.1 DiBos

##### 3.1.1 DiBos Front View



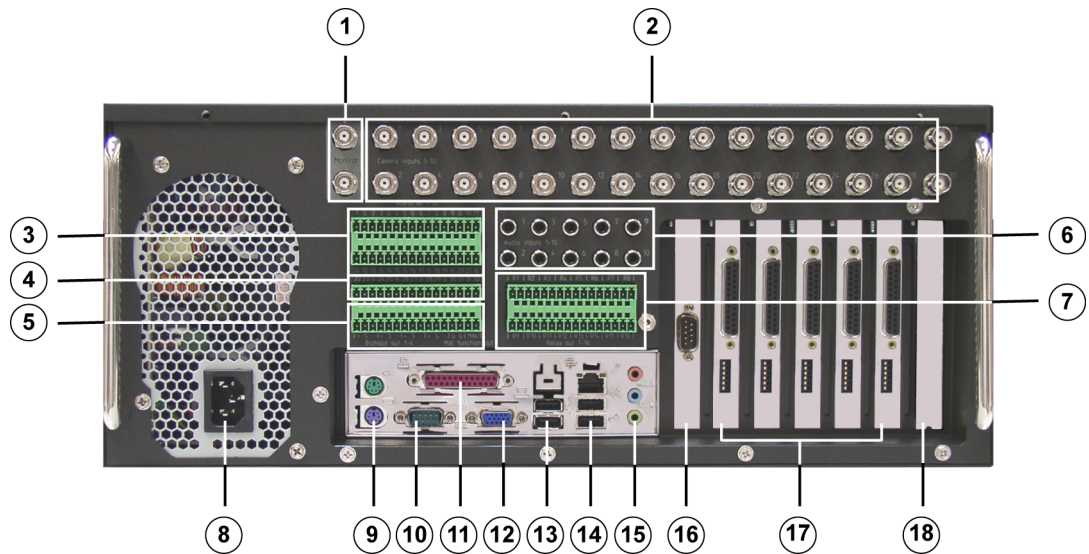
1	On/Off switch	4	USB 2.0
2	Status LEDs: Red = hard disk access Green = system is switched on Yellow = unused	5	The following are located on the device: – Windows XP Embedded license sticker – DiBos rating plate – DiBos license sticker and activation key
3	DVD-RW		

**CAUTION!**

An air filter must not be installed in the device. Installing an air filter affects the cooling of the device and can damage the device.

## 3.1.2

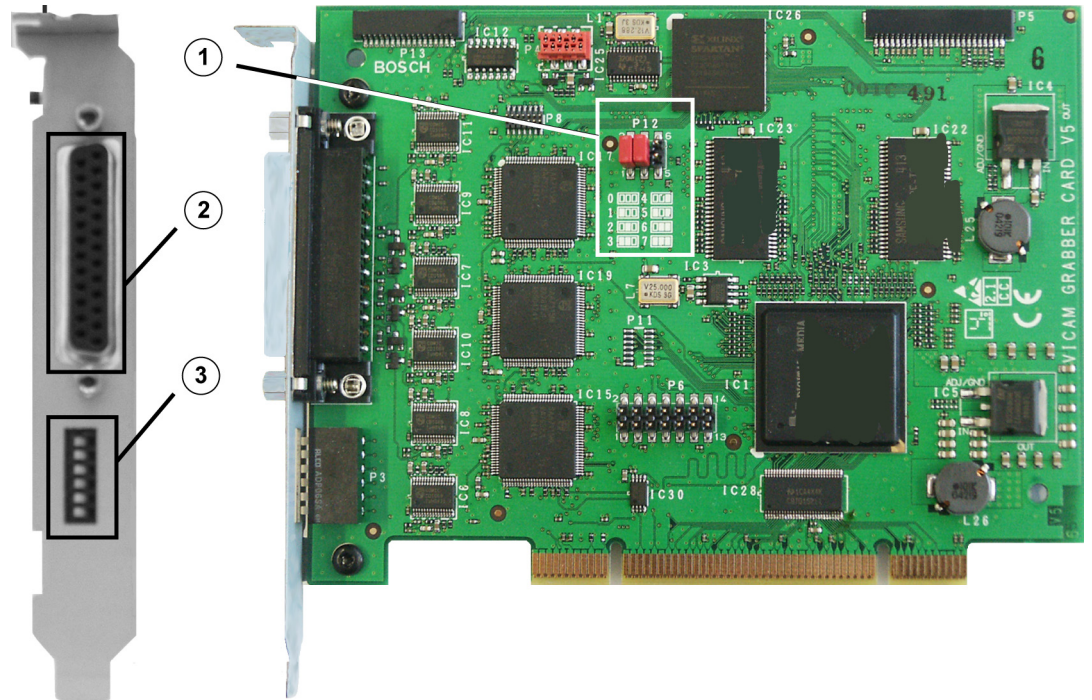
## DiBos Rear View

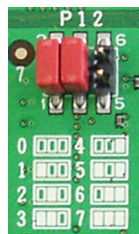
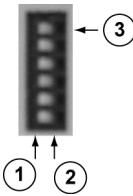


1	Video monitor A/Video monitor B	10	Serial interface COM1
2	Video inputs 1 - 30	11	Parallel interface. <b>Note:</b> The HW dongle must be connected if handling a device that has been supplied with a HW dongle.
3	Alarm inputs 1 - 21	12	VGA monitor
4	Alarm inputs 22 - 32	13	2x USB 2.0 (e.g. for mouse and keyboard with USB connection)
5	Biphase 1 - 4, malfunction outputs 1	14	1x Ethernet (RJ45) - 2x USB 2.0
6	Audio inputs 1 - 10	15	Line in (blue) Speaker out (green) Microphone in (red), mono
7	Relay outputs 1 - 16	16	Second serial interface (COM2)
8	Mains connection 100/240 VAC, 50/60 Hz (automatic switchover)	17	Grabbers 1 - 5
9	Mouse (green) - Keyboard (purple). These connections should be used if the mouse and keyboard are not connected via USB.	18	Free for optional PCI plug-in cards

### 3.1.3 Grabber Card for DiBos

Looped through inputs may not be terminated. When a grabber card is retrofitted, the grabber identification (grabber 1, grabber 2 etc.) must be set.



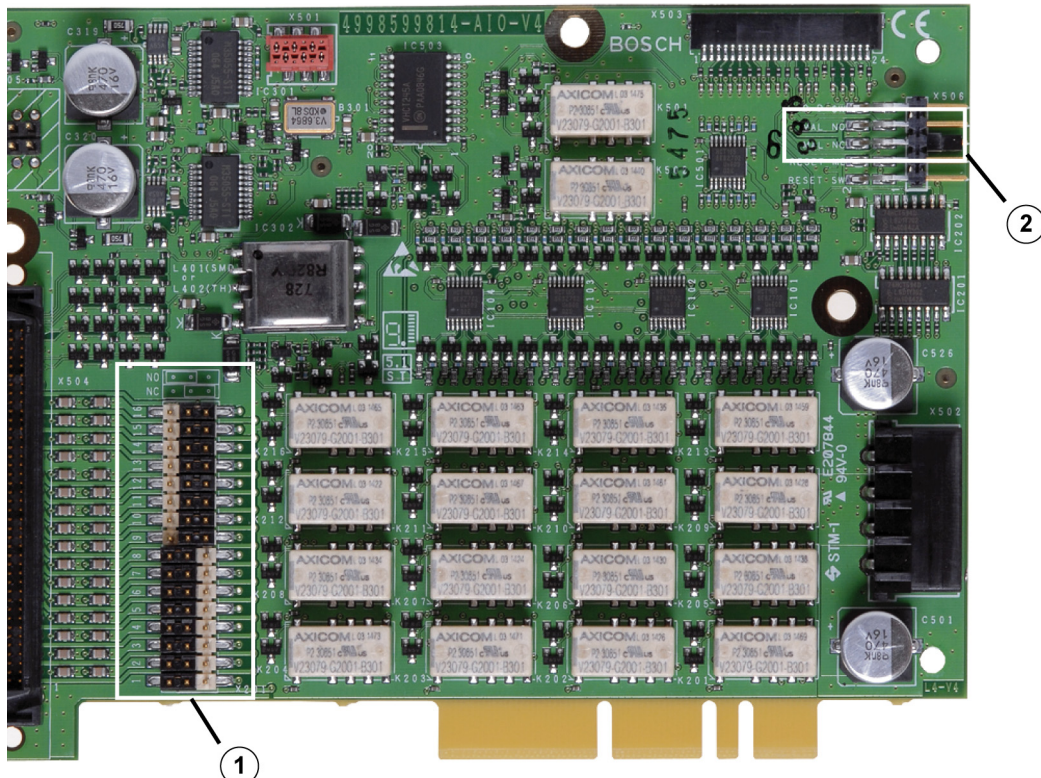
<p>1</p> 		<p>Grabber identification:                  The setting for grabbers 1 - 5 is printed on the PCB.                  0 = Grabber 1                  1 = Grabber 2                  2 = Grabber 3                  3 = Grabber 4                  4 = Grabber 5</p>
<p>2</p>		<p>Loophrough cable plug</p>
<p>3</p> 		<p>Termination when loopholethrough cable is used:                  1 = Switch position left: input terminated (position when delivered)                  2 = Switch position right: open, not terminated                  3 = Topmost switch: for camera input 1 etc.  <b>Note:</b>                  The positions relate to the illustration above.</p>

### 3.1.4

#### I/O Card for DiBos

The following can be set for the I/O card:

- the relay outputs (NO = normally open, NC = normally closed)
- the malfunction outputs (NO = normally open, NC = normally closed)



1		<p><b>Relay outputs:</b> The setting is printed on the PCB. Relay outputs 1–8: open (NO = normally open) Relay outputs 9–16: closed (NC = normally closed)</p>
2		<p><b>Malfunction output:</b> The setting is printed on the PCB. Bridge position up: Open (MAL NO = malfunction normally open) Bridge position down: Closed (MAL NC = malfunction normally closed)</p>



**NOTICE!**

The I/O card must be removed to change the bridge settings.

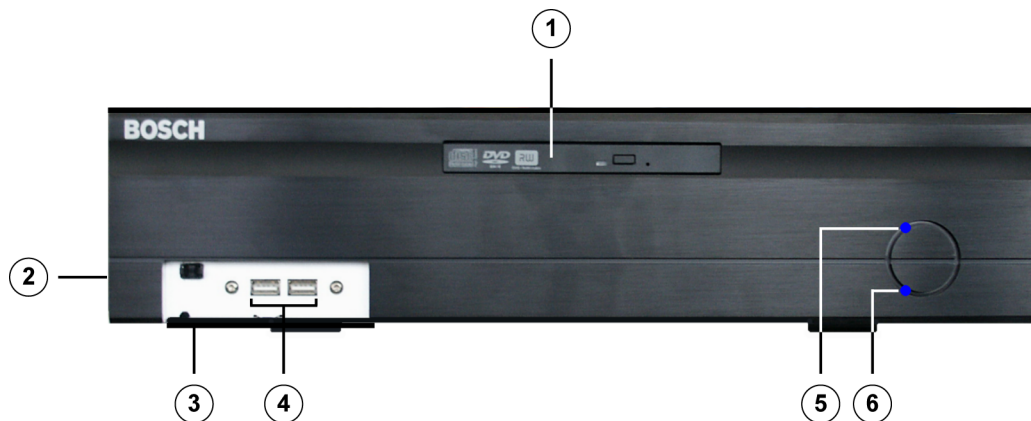


### 3.2

## DiBos micro

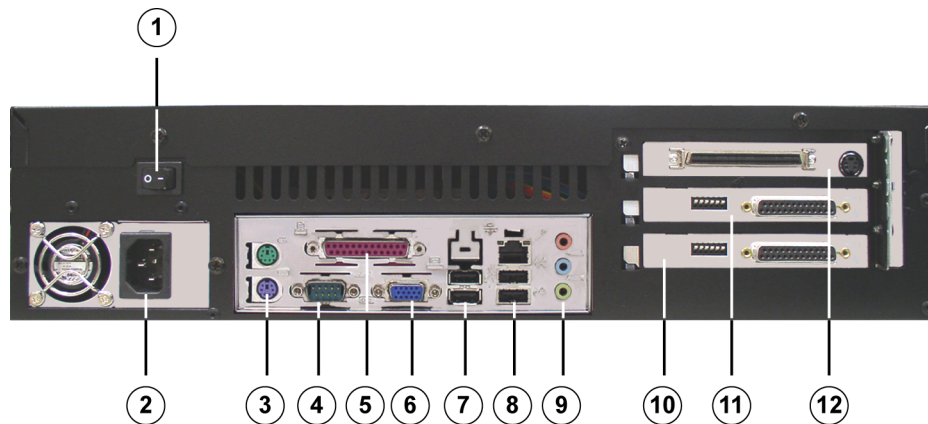
#### 3.2.1

#### DiBos micro Front View



1	DVD-RW	4	2x USB 2.0
2	The following are located on the side panel: <ul style="list-style-type: none"> <li>- DiBos rating plate</li> <li>- DiBos license sticker and activation key</li> </ul>	5	Status LED: System is switched on
3	Front cover Opened by pressing once on the cover. <b>Note:</b> The Windows XP Embedded license sticker is located on the inside of the front cover.	6	Status LED: hard disk access

### 3.2.2 DiBos micro Rear View



1	On/Off switch	7	2x USB 2.0 (e.g. for mouse and keyboard with USB connection)
2	Mains connection 100 / 240 VAC, 50 / 60 Hz (automatic switchover)	8	1x Ethernet (RJ45) - 2x USB 2.0
3	Mouse (green) - Keyboard (purple). These connections should be used if the mouse and keyboard are not connected via USB.	9	Line in (blue) Speaker out (green) Microphone in (red), mono
4	Serial interface COM1	10	Grabber 2 (camera 7 - 12)
5	Parallel interface. <b>Note:</b> The HW dongle must be connected if handling a device that has been supplied with a HW dongle.	11	Grabber 1 (camera 1 - 6)
6	VGA monitor	12	I/O card with plug for connecting the alarm inputs and relay outputs and socket for video monitor A and video monitor B



#### NOTICE!

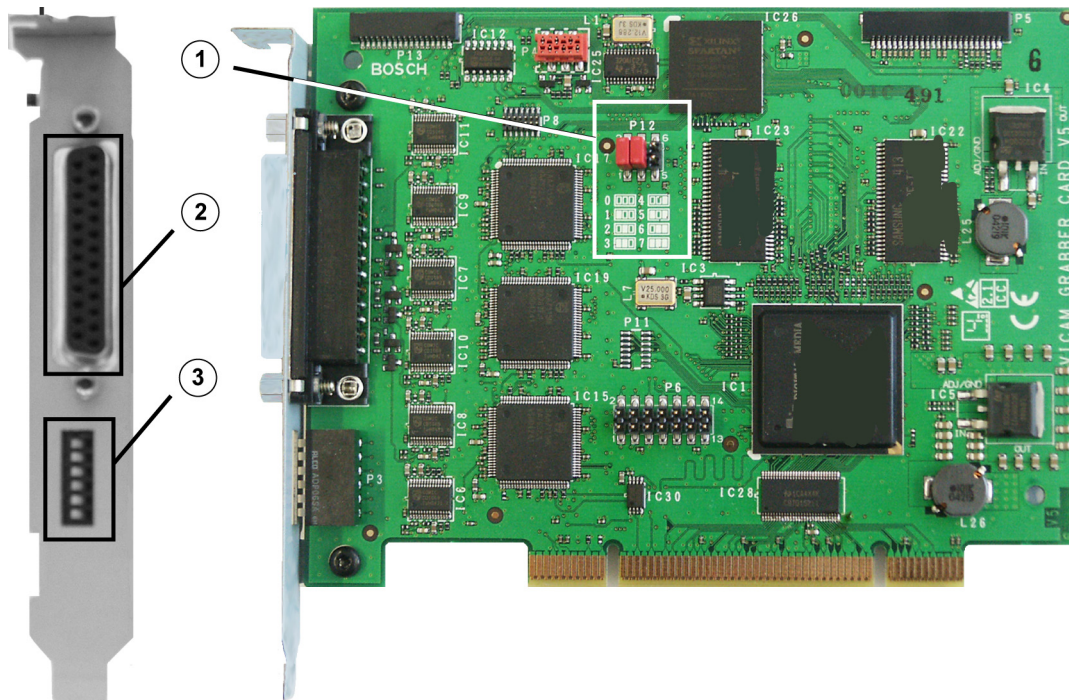
Ferrites must be fitted to the following cables:

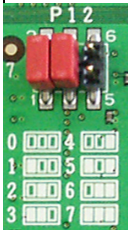
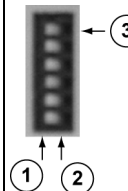
- Network cable (2 ferrites directly next to each other)
- Keyboard (1 ferrite)

The ferrites must be fitted to the cable directly next to the connections.

### 3.2.3 Grabber Card for DiBos micro

When a grabber card is retrofitted, the grabber identification (grabber 1, grabber 2 etc.) must be set.



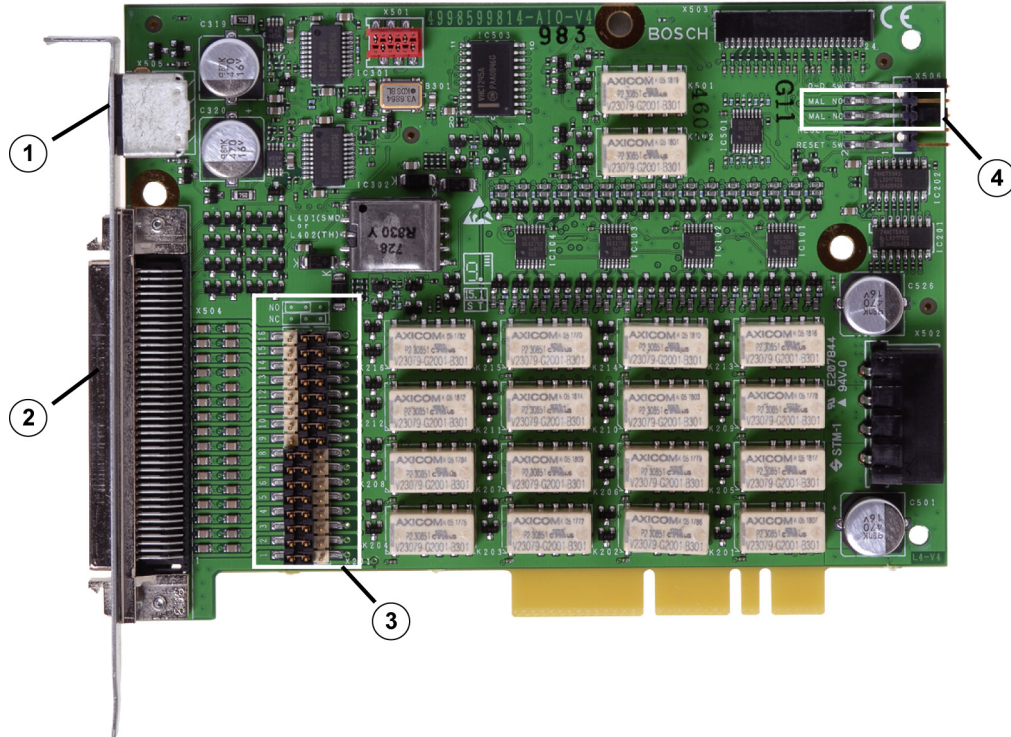
<p>1</p> 	<p>Grabber identification: The setting for grabber card 1 and grabber card 2 is printed on the PCB. 0 = Grabber 1 1 = Grabber 2</p>
<p>2</p>	<p>Plug for connecting cable with 6 video and 2 audio inputs (the cables are numbered). BNC cable number 1 (brown) = Video input 1 BNC cable number 2 (yellow) = Video input 2 BNC cable number 3 (green) = Video input 3 BNC cable number 4 (black) = Video input 4 BNC cable number 5 (white) = Video input 5 BNC cable number 6 (blue) = Video input 6 Audio cable number 1 (gray) = Audio input 1 Audio cable number 2 (red) = Audio input 2</p>
<p>3</p> 	<p>Terminating video inputs: 1 = Switch position left: input terminated (position when delivered) 2 = Switch position right: open, not terminated 3 = Topmost switch: for camera input 1 etc. <b>Note:</b> The positions relate to the illustration above.</p>



### 3.2.4 I/O Card (for DiBos micro)

The following can be set for the I/O card:

- the relay outputs (NO = normally open, NC = normally closed)
- the malfunction outputs (NO = normally open, NC = normally closed)

The I/O card must be removed to change the bridge settings.



1	Cable for monitor output A and monitor output B (the cables are numbered). Cable number 1 = Monitor A Cable number 2 = Monitor B	
2	Connecting cable for 12 alarm inputs, 12 relay outputs, 3 biphas and 1 malfunction output (for assignment, see table below)	
3		16 relay outputs: The setting is printed on the PCB. Relay outputs 1–8: open (NO = normally open) Relay outputs 9–16: closed (NC = normally closed)
4		Malfunction output: The setting is printed on the PCB. Top bridge position: Open (MAL NO = malfunction normally open) Bottom bridge position (position when delivered): Closed (MAL NC = malfunction normally closed)

**I/O card pin assignment**

<b>Connector</b>	<b>Color</b>	<b>Name</b>	<b>Connector</b>	<b>Color</b>	<b>Name</b>
1	White/tan	Relay 1	41	Tan/white	Alarm input 1
2	White/brown	Relay 1	42	Brown/white	Alarm input 2
3	White/pink	Relay 2	43	Pink/white	Alarm input 3
4	White/orange	Relay 2	44	Orange/white	Alarm input 4
5	White/yellow	Relay 3	45	Yellow/white	Alarm input 5
6	White/green	Relay 3	46	Green/white	Alarm input 6
7	White/blue	Relay 4	47	Blue/white	Alarm input 7
8	White/purple	Relay 4	48	Purple/white	Alarm input 8
9	White/gray	Ground	49	Gray/white	Ground
10	Tan/brown	Relay 5	50	Brown/tan	Alarm input 9
11	Tan/pink	Relay 5	51	Pink/tan	Alarm input 10
12	Tan/orange	Relay 6	52	Orange/tan	Alarm input 11
13	Tan/yellow	Relay 6	53	Yellow/tan	Alarm input 12
14	Tan/green	Relay 7	54	Unused	
15	Green/tan	Relay 7	55	Unused	
16	Tan/blue	Relay 8	56	Unused	
17	Blue/tan	Relay 8	57	Unused	
18	Tan/purple	Relay 9	58	Unused	
19	Purple/tan	Relay 9	59	Unused	
20	Tan/gray	Relay 10	60	Unused	
21	Gray/tan	Relay 10	61	Unused	
22	Brown/pink	Relay 11	62	Unused	
23	Pink/brown	Relay 11	63	Unused	
24	Brown/orange	Relay 12	64	Unused	
25	Orange/brown	Relay 12	65	Unused	
26	Brown/yellow	Ground	66	Yellow/brown	Ground
27	Unused		67	Unused	
28	Unused		68	Unused	
29	Unused		69	Unused	
30	Unused		70	Unused	
31	Unused		71	Unused	
32	Unused		72	Unused	
33	Unused		73	Unused	
34	Unused		74	Unused	
35	Brown/green	Malfunction output	75	Green/brown	Malfunction output
36	Brown/blue	Biphase 1-	76	Blue/brown	Biphase 1+
37	Brown/purple	Biphase 2-	77	Purple/brown	Biphase 2+
38	Brown/gray	Ground	78	Gray/brown	Ground
39	Pink/orange	Biphase 3-	79	Orange/pink	Biphase 3+
40	Unused		80	Unused	

## 4 Quick Installation

This chapter describes how to put the device into operation quickly and easily.

### Main connections

1. Connect the cameras to the video inputs.
2. Make sure that the HW dongle is connected to the parallel interface (if you are handling a device that has been supplied with a HW dongle).
3. Connect the VGA monitor.
4. Connect the mouse and keyboard.

### Optional connections

The optional connections can be added after the system is configured.

1. Connect monitor A and monitor B to connections A and B.
2. Connect up to 32 alarm inputs (for DiBos micro: 12).
3. Connect up to 16 relay outputs (for DiBos micro: 12).
4. Connect your network via the Ethernet port.
5. Connect customer-operated ATMs, foyer card reader, radio clock and alarm panel.

### Switching on

1. Switch on all connected devices.
2. Plug the power cable into the video system.
3. Switch on the video system (On/Off switch on the front). The computer boots up.

### First-time use

Once the boot routine is complete, 1 image/second is stored for every camera connected. The user interface is automatically displayed. This shows images from all connected cameras in a multi-image view. If no images are displayed for a camera, check the camera connection. You are not yet logged on as a user. You can, however, start the Configuration wizard.

### Quick configuration with the help of the Configuration wizard

1. Start the Configuration wizard in the **System** menu > **Configuration wizard**.
2. Carry out a quick configuration in the Configuration wizard or load an existing configuration onto the system.

## 5 Quick Configuration

You can create a basic system configuration with the help of the Configuration wizard in just a few mouse clicks. The system automatically recognizes the video hardware that is connected (cameras, grabbers).

The Configuration wizard consists of six dialog boxes. Each dialog box can be dealt with independently of the other dialog boxes.

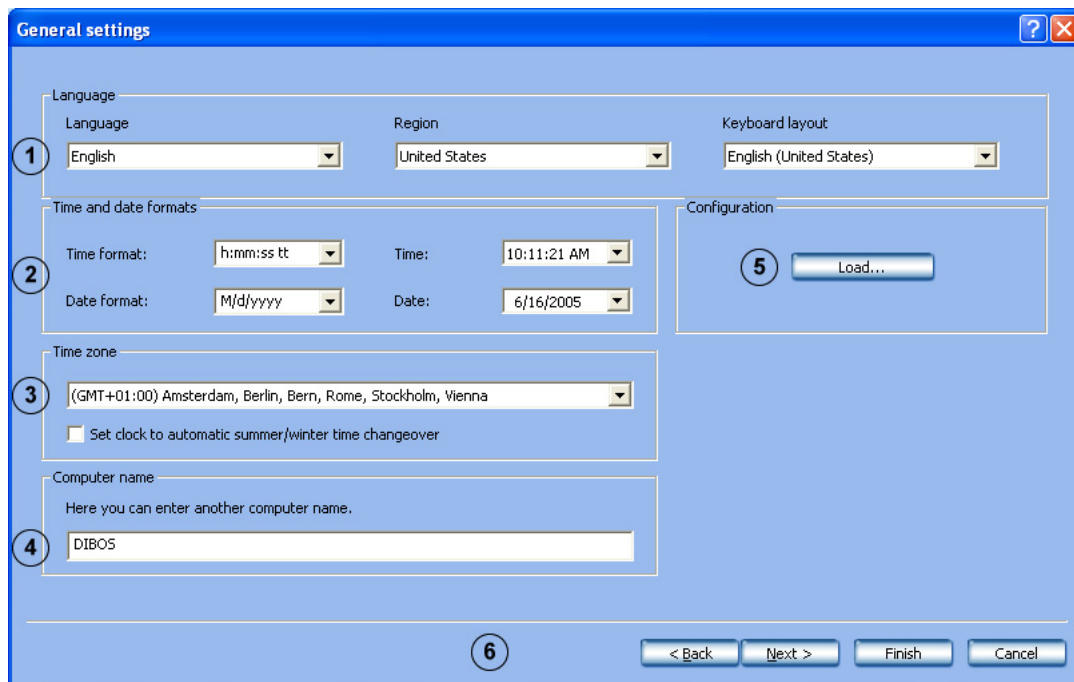
If a more complex configuration is necessary, this is carried out with the help of the standard configuration.

### CAUTION!

- The default configuration is overwritten with the last settings saved in the Configuration wizard. Overwriting settings may lead to the loss of previously configured settings (e.g. recording settings, IP cameras). We recommend only using the Configuration wizard for a newly installed system.
- For security reasons, it is advisable to save the configuration on external data carriers.

### 5.1 General Settings

System menu > Configuration wizard



In this dialog box, edit the general settings for the system.

1	Language	It is possible to set the language of the operating system and the video system software. <b>Note:</b> The format of the time and date display is determined by the language and region selected. If the language is changed, the system must be shut down and rebooted.
	Language	Lists the available languages for the operating system and the video system software.
	Region	Lists the available regions for the language selected.
	Keyboard layout	Lists the available keyboard layouts.

2	Time and date formats	Specify the time and date formats here.
	Time format:	Enter the type of time display. h = hours; m = minutes; s = seconds; t = morning/afternoon (e.g. AM/PM) h = 12 hours; H = 24 hours hh, mm, ss = representation with leading zero (representation with 2 digits) h, m, s = representation without leading zero
	Date format:	Enter the type of date display. d = day; M = month; y = year dd, MM = representation with leading zero yy = for example 05; yyyy = for example 2005
	Time:	Current time.
	Date:	Current date.
3	Time zone	Lists the available time zones.
	Set clock to automatic summer/winter time changeover	Activate this function if the system time is to change automatically to summer and winter time.
4	Computer name	Enter the name. This name identifies the video system in the network. <b>Note:</b> The computer name must not be assigned more than once. If the computer name is assigned more than once, a yellow flashing bar appears under the computer symbol in DiBos Explorer and the cameras are crossed off. If the name is changed, the system must be shut down manually when the wizard finishes. The system is then restarted automatically.
5	Configuration	Loads a previously created configuration, for example from a USB memory stick.
	Load	Click the button to load a configuration.
6	Finish	Saves the settings and finishes the wizard.
	Next	Click <b>Next</b> to continue.



## 5.2 Creating a User

System menu > Configuration wizard > Next

On an initial installation, 3 authorization levels and 3 users are automatically created. These cannot be deleted.

1	Administrator:	Possesses all rights concerning operation and configuration of the system.
2	Extended user:	Possesses all rights concerning operation of the system. He possesses no rights for configuring of the system. An exception is the right to create a <b>Normal user</b> .
3	Normal user:	Possesses all rights concerning operation of the system. He possesses no rights for configuration.
4	Finish Next	Saves the settings and finishes the wizard. Click <b>Next</b> to continue.

Proceed as follows to create a new user:

1. Create a new user by entering **Name** and **Password** in the corresponding authorization. Make a note of the name and password, as you will need it afterwards to log on.
2. Enter the same password again under **Repeat password**.
3. Click **Next** to call up the next page of the wizard or **Finish** to save the entries and exit the wizard.



### NOTICE!

By default, no password is assigned for the authorization levels.

## 5.3 Setting up the Network

System menu > Configuration wizard > Next

If integrated into a customer network, the following settings must be made:

1	Network card: Limit bandwidth	Select the network card.  Limits data transmission bandwidth to a value that the system does not exceed.
2	TCP/IP settings  Obtain IP address automatically	Specify here whether the network connection should use a fixed IP address or whether the IP address should be assigned automatically.  The IP address of this network connection is dynamically assigned by a DHCP server. <b>Note:</b> The device must be connected to the network and the available network must support this function.
3	Use following IP address:	A fixed IP address will be assigned to the network connection. In this case, the IP address and subnet mask must subsequently be entered. <b>Note:</b> You can obtain these from your system administrator or Internet service provider.
	IP address:	Enter the IP address.
	Subnet mask:	Enter the number of the subnet mask. The IP address and subnet mask determine which network your computer will use.

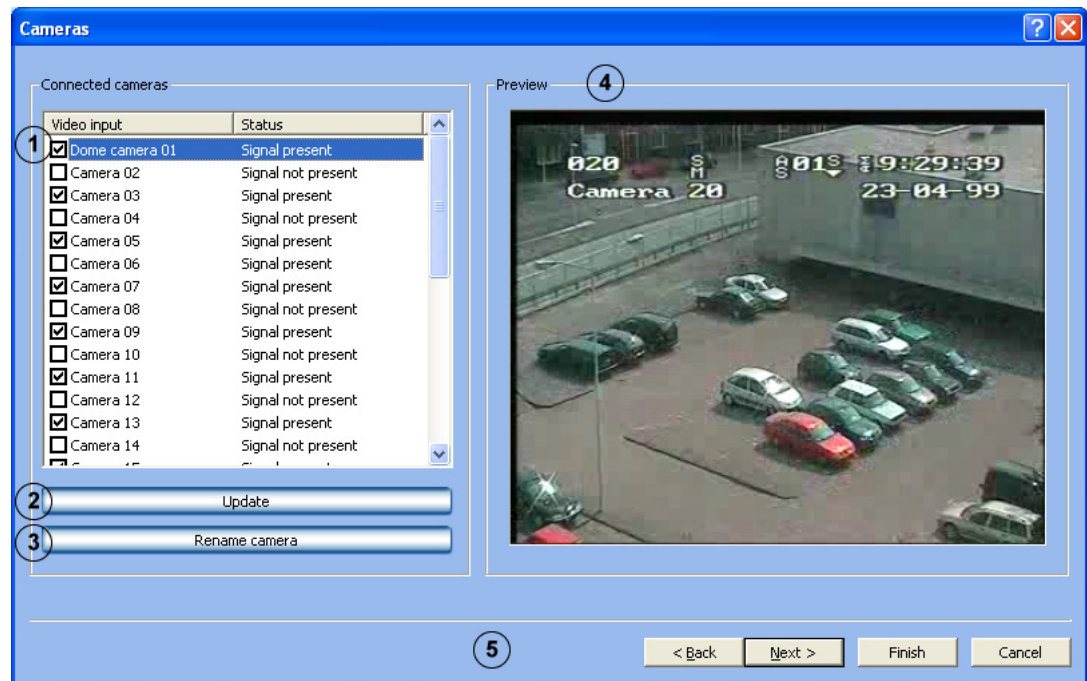
	Default gateway:	Enter the address of the default gateway you want to use. This is the address of a local gateway in the same network as the computer. It is used to forward data to a destination outside the local network. <b>Note:</b> A gateway links up separate networks. For example, the local network (LAN) needs a gateway to connect it to the Internet or WAN. Ask your system administrator for the number.
4	Obtain DNS server addresses automatically	The network addresses for DNS servers are assigned dynamically by the network.
5	Use the following DNS server addresses	The network addresses for DNS servers have fixed assignments.
	Preferred DNS server:	IP address of preferred DNS server. This server is used first.
	Alternative DNS server:	IP address of a replacement server that is to be used when the first server is unreachable.
6	Finish Next	Saves the settings and finishes the wizard. Click <b>Next</b> to continue.

**NOTICE!**

This dialog is only available when a network connection is present or a network card is fitted.

## 5.4 Specifying Cameras

System menu > Configuration wizard > Next

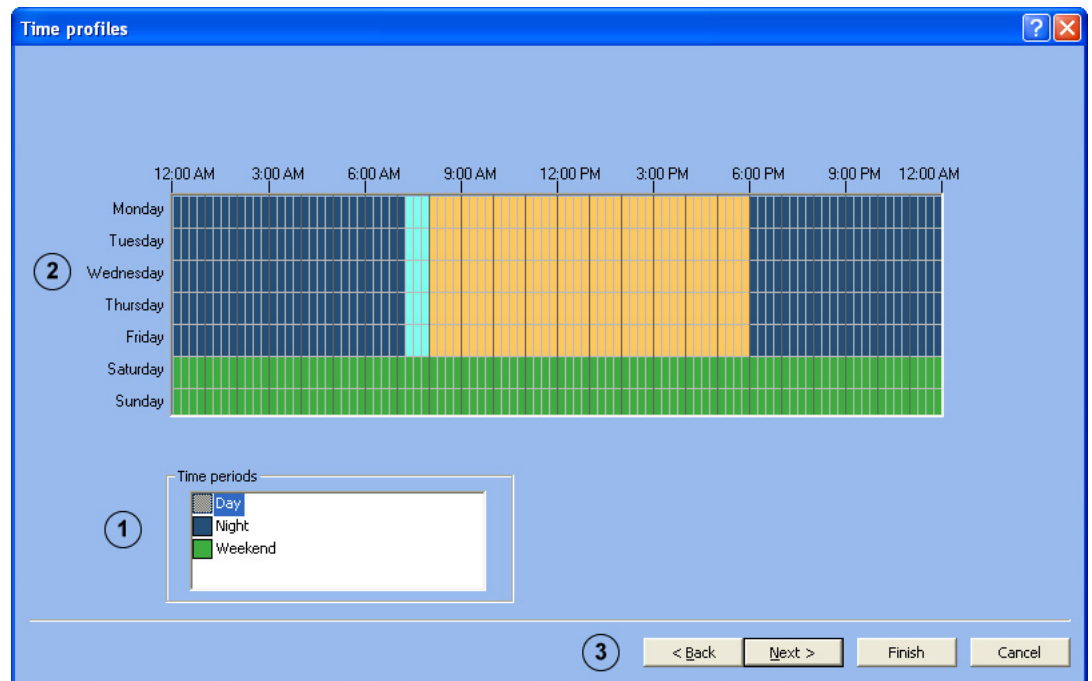


The dialog box displays all video inputs of the grabber cards present. Cameras already connected are recognized automatically.

1	Connected cameras	Activate the check box of the desired video input to add cameras that have been connected later.
2	Update	Click the button to display cameras that have been connected after the wizard has started.
3	Rename camera	Select the camera whose name you want to change and click the button. Then enter the new name.
4	Preview	Shows the image from the selected camera.
5	Finish Next	Saves the settings and finishes the wizard. Click <b>Next</b> to continue.

## 5.5 Assigning Time Profiles

System menu > Configuration wizard > Next

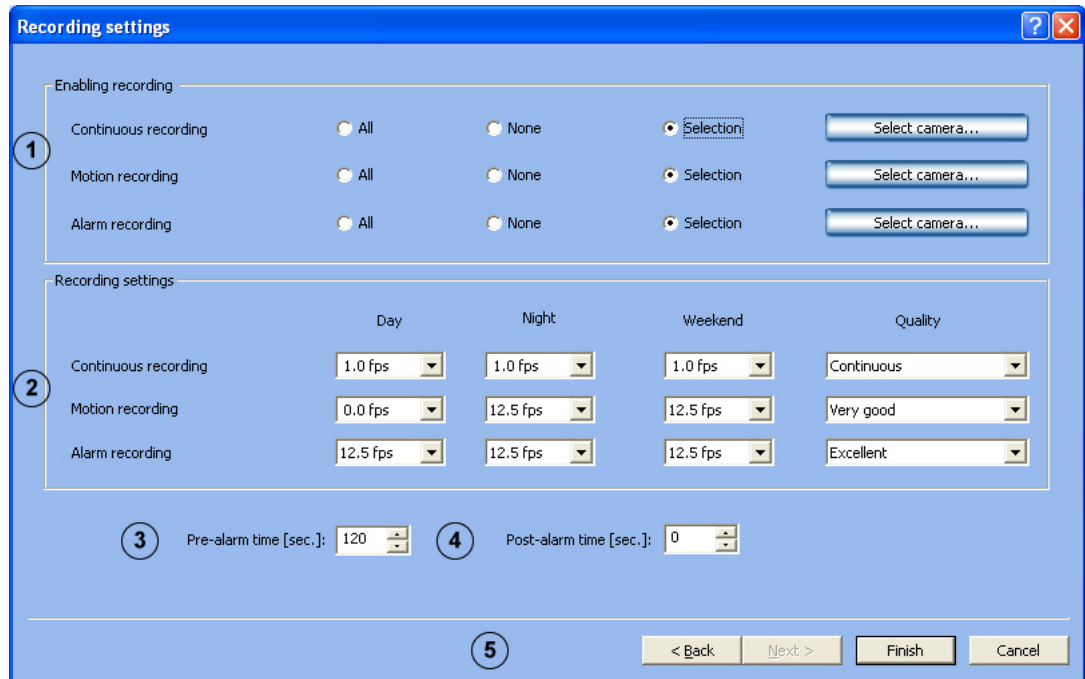


Time periods are assigned with the mouse cursor in a graphical time planner. There are three time periods available. These time periods can be assigned to any day of the week. The time periods are displayed in different colors.

1	Time periods	Select the time period that you want to assign to a day.
2	Graphical time planner	<p>Move the mouse cursor into the graphical time planner. Clicking with the left mouse button marks a cell. Dragging up a square while pressing the left mouse button marks a time period. All selected cells take the color of the selected time period.</p> <p><b>Note:</b> The 24 hours of the day are displayed on the horizontal axis of the graphical time planner. Each hour is subdivided into four cells. A cell is the smallest selectable time unit and represents 15 minutes.</p> <p>The days are shown on the vertical axis.</p> <p>To edit selected cells in the graphical time planner, select another time period and overwrite the cell already selected.</p>
3	Finish Next	<p>Saves the settings and finishes the wizard.</p> <p>Click <b>Next</b> to continue.</p>

## 5.6 Setting Up Recording

System menu > Configuration wizard > Next



In this dialog box, you determine the type of recording, recording rate, recording quality and pre- and post-alarm time.

1	<p>Enabling recording</p> <p>Continuous recording Motion recording Alarm recording</p>	<p>Here, you can select whether continuous, motion, or alarm recording for all cameras, no cameras, or for specific cameras should take place.</p> <p><b>All:</b> The type of recording is the same for all cameras, for example continuous recording on all cameras.</p> <p><b>None:</b> No camera is recording.</p> <p><b>Selection:</b> The type of recording should apply only to specific cameras. To make this setting, click <b>Select camera...</b> and choose the cameras.</p>
2	Recording settings	Specifies the recording rate and quality.
	<p>Continuous recording Motion recording Alarm recording</p>	<p>Select the recording rate and quality for each type of recording. The recording rate can be entered for each time period.</p> <p>If a column (Day, Night, Weekend) is grayed out, this means that no time periods were assigned in the <b>Time profiles</b> dialog.</p>

3	Pre-alarm time [sec.]:	<p>Enter the pre-alarm time for alarm and motion detection. Values between 0 and 1800 seconds are allowed - with a limit of 3600 images.</p> <p><b>Note:</b> The recording rate during the pre- and post-alarm time is at least 1 image per second. If the continuous recording rate is higher than 1 image per second, this value is taken.</p>
4	Post-alarm time [secs.]:	<p>Enter the post-alarm time. Values from 0 to 999 seconds are allowed.</p>
5	Finish	<p>Click the button to exit the basic configuration. The video system is then started. Log on with your user name and password. Make further configuration entries if necessary.</p> <p><b>Note:</b> When you click "Finish", the wizard automatically creates a job for each camera. In this way, the camera number and job number are the same, e.g. camera 01 - job 01, camera 02 - job 02 etc. (up to a maximum of camera 30 - job 30). When the wizard is run again, all the previous settings with the designation job 01, job 02 ... job 30 will be overwritten. If you do not want this to happen: Edit the designation of the jobs in the configuration and do not name the newly configured jobs as Job 01, Job 02 etc.</p>

## 6 Default Configuration

The default configuration allows more complex requirement or customer wishes to be catered for than the Configuration wizard.

Go through the configuration tree from top to bottom by clicking individual menu points and making the corresponding entries.

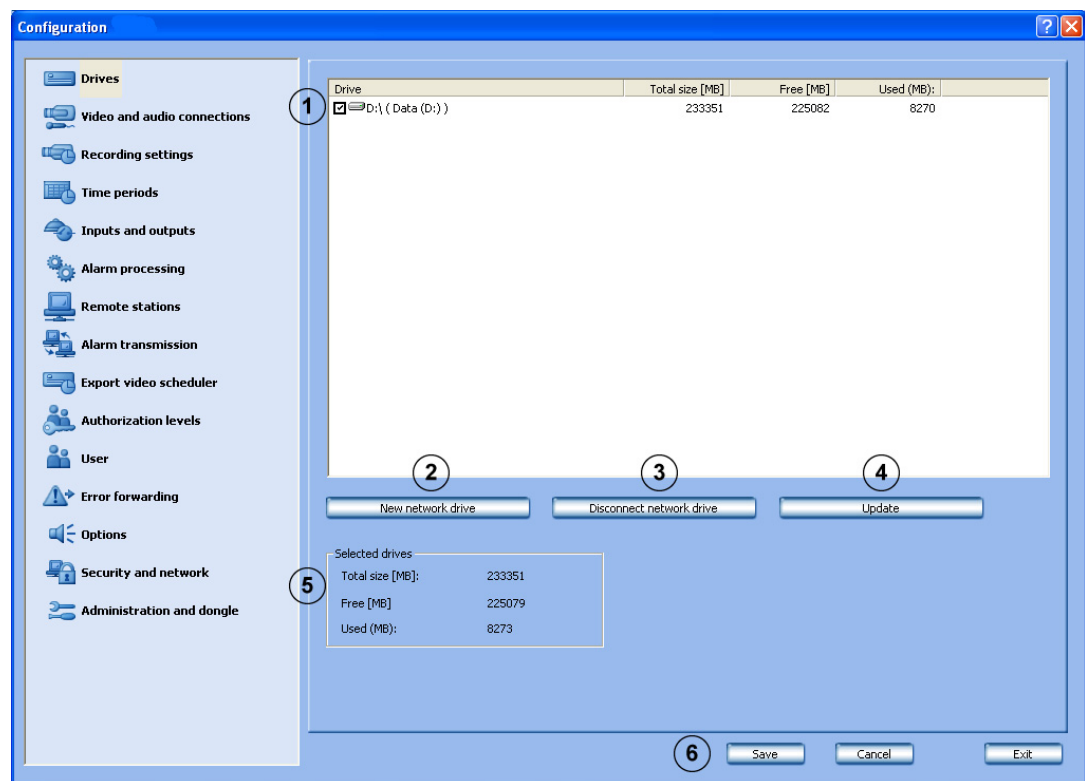
It is possible to switch to the Configuration wizard from the default configuration at any time; however, this is only recommended for a newly installed system *Section 5 Quick Configuration, page 31*.

### CAUTION!

For security reasons, it is advisable to save the configuration on external data carriers.

### 6.1 Configuring Drives

Drives menu



This dialog box gives you an overview of the hard drives and network drives available.

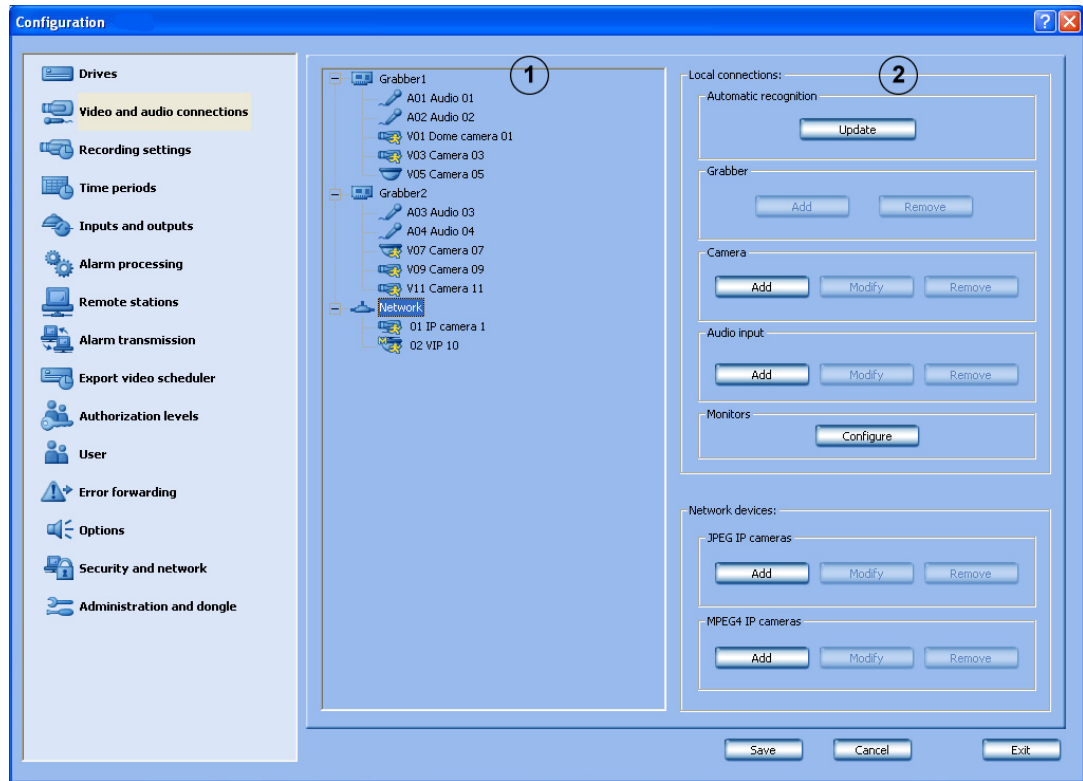
1		The list field contains all hard drives and network drives known to the system. The total size, the free storage capacity and the used storage capacity are shown in MByte. The drives listed can be activated or deactivated. Activate the drive by clicking the check box. <input checked="" type="checkbox"/> D:\ The drive is activated. <input type="checkbox"/> D:\ The drive is not activated.
2	New network drive	A new network drive can be added.
3	Disconnect network drive	Disconnects a network drive. Select the drive and click the button.



4	Update	If an additional network drive is put into operation during configuration, this can be included in the list field by clicking <b>Update</b> .
5	Selected drives	Total storage capacity, available storage capacity and used storage capacity are shown in MByte for activated network drives.
6	Save	The entries are saved.

## 6.2 Configuring Video and Audio Connections

### Video and audio connections menu



Connection overview ①	Right side of dialog box ②
<p>Gives you an overview of the local system:</p> <ul style="list-style-type: none"> <li>– Number of active grabber cards with the cameras and audio sources connected to them</li> <li>– Number of configured network devices (IP cameras)</li> </ul>	<p>Grabbers, cameras, audio sources, monitors and IP cameras can be added, edited or removed.</p>

#### Automatic recognition of locally connected components

- ▶ Click **Update** in the **Automatic recognition** section. Locally connected grabbers and analog cameras are recognized by the system and shown graphically in the connection overview.

#### Adding grabbers

1. Select a grabber in the connection overview.
2. In the **Grabber** section, click **Add**. A dialog box for grabber selection appears.

#### Adding cameras or audio inputs

1. In the selection overview, select the grabber to which you want to add cameras or audio inputs.
2. In the **Camera** or **Audio input** section, click **Add**. A dialog box for camera or audio selection appears.

**Modifying camera or audio input settings**

1. Select the camera or audio input in the connection overview.
2. In the **Camera** or **Audio input** section, click **Edit**. A dialog box for editing camera or audio settings appears.

**Removing grabbers, cameras or audio inputs**

1. Select the components in the connection overview.
2. Click **Remove** in the appropriate section. The component is removed.

**Configuring monitors**

- ▶ In the **Monitors** section, click **Configure**. A dialog box for configuring locally connected monitors appears.

**Adding network cameras**

1. Select the designation **Network** in the connection overview.
2. In the **JPEG IP cameras** or **MPEG4 IP cameras** section, click **Add**. A network camera is added.

**Modifying network camera settings**

1. Select the camera in the connection overview.
2. In the **JPEG IP cameras** or **MPEG4 IP cameras** section, click **Edit**. A dialog box for modifying camera settings appears.

**Removing network cameras**

1. Select the camera in the connection overview.
2. In the **JPEG IP cameras** or **MPEG4 IP cameras** section, click **Remove**. The camera is removed.

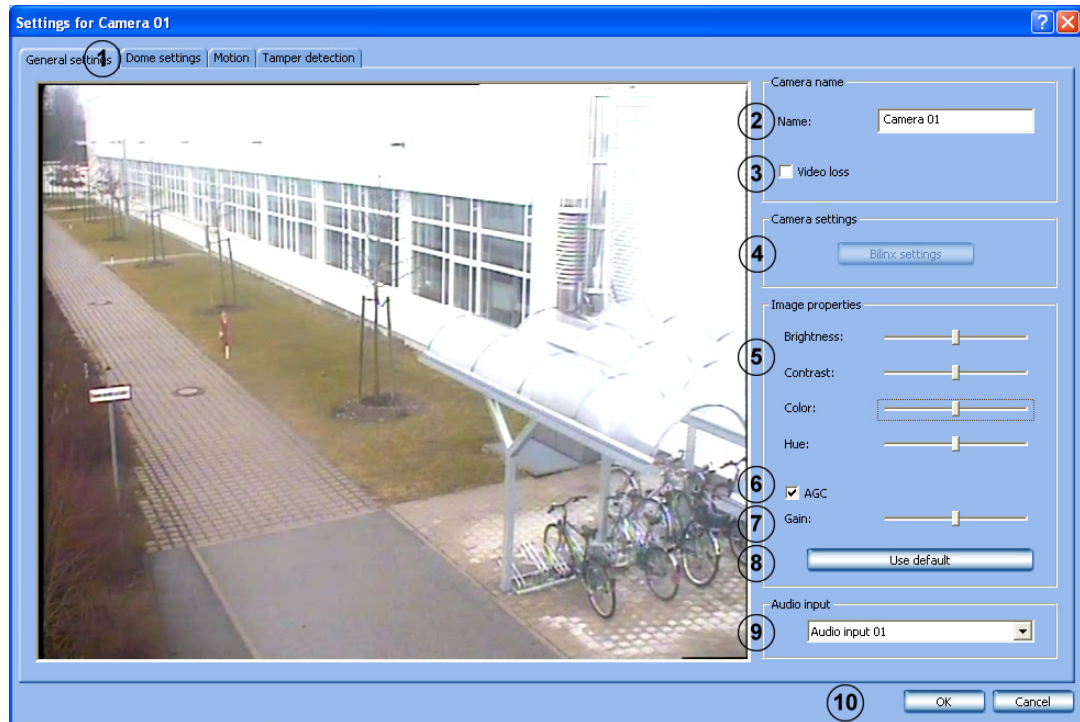
**NOTICE!**

- The system can automatically recognize built-in grabbers and directly connected cameras.
- A maximum of 5 grabbers can be built into one DiBos.
- A maximum of 2 grabbers can be built into one DiBos Micro.
- A maximum of 6 cameras and 2 audio inputs can be assigned to each grabber.
- In addition to a VGA monitor, two video monitors can be locally connected.
- The number of IP cameras depends on the extension level of the system.

## 6.2.1

## General Camera Settings

Video and audio connections menu &gt; Camera section &gt; Edit button



Make the settings for each camera as required.

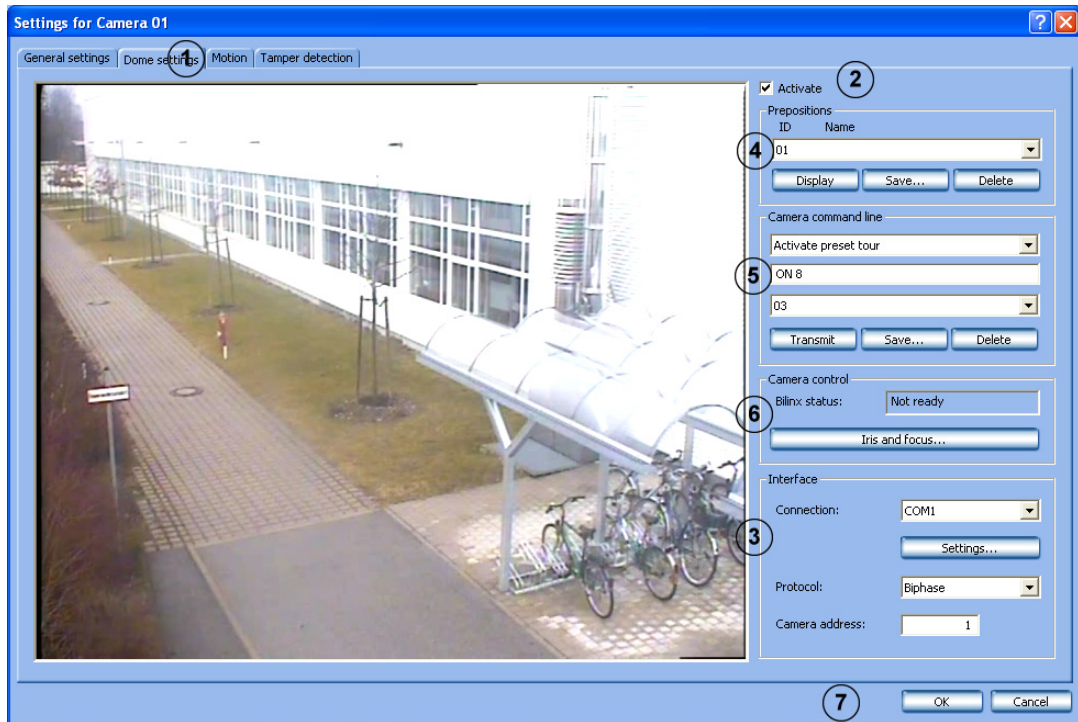
1	General settings	Click the tab.
2	Name:	Enter the name of the camera. The name must not contain any special characters or end with a space.
3	Video loss	Activate this check box if a warning should be shown on camera signal failure. <b>Note:</b> The malfunction relay is also activated if a relay output is selected as a malfunction relay in the configuration (Inputs and outputs menu, Relay tab).
4	Bilinx settings	Click the button to access the Bilinx camera navigation menu. The Bilinx camera menu is displayed in the image window. <b>Note:</b> Only selectable for Bilinx-capable cameras.
5	Image properties	Set brightness, contrast, color and hue. You can see the result of these settings in the camera image ( <b>Hue</b> is only active on NTSC cameras).
6	AGC (AGC = automatic gain control)	Activate this check box if the camera signal on the grabber should be amplified.
7	Gain:	Manually correct the input level audio level at the grabber using the slider. <b>Note:</b> Only possible when <b>AGC</b> is not activated.

8	Use default	The image properties (incl. AGC/Gain) are reset to the ex-works settings.
9	Audio input	Click the down arrow and assign the camera an audio input if necessary. <b>Note:</b> One audio input can be assigned to multiple cameras.
10	OK	The entries are saved.

## 6.2.2

## Setting up Dome Cameras and Pan/Tilt Cameras

Video and audio connections menu &gt; Camera section &gt; Edit button



Make the settings for each camera as required.

1	Dome settings	Click the tab.
2	Activate	Select the check box if the camera is a dome camera or a pan/tilt camera.

### Making interface settings

3	Interface	The interface settings must be made first. Only then can further dome settings follow.
	Connection:	Click the down arrow and select the interface (BLX = Bilinx, GBPx = Grabber Biphas port, COMx = serial RS232 port).
	Settings...	Click the button. A dialog box opens. Make the settings for the COM interface (bits per second, data bits, stop bits, parity etc.). The settings depend on the type of camera. <b>JVC:</b> 9600/8/1/even <b>Panasonic</b> 9600/8/1/none (on the Panasonic Dome, the bit rate must be set manually) <b>Pelco:</b> 2400/8/1/none <b>Bosch Domes:</b> The dome settings must be saved.


	Protocol:	Select the protocol depending on the camera connected. The following protocols are available: AllegiantProtocol, Biphas, Geutebrueck protocol, JVC TKC 676, Multisec protocol, Panasonic protocol, Pelco D protocol and Sae. Only dome functions are supported. With Biphas and Allegiant, you can choose your own command strings and pre-defined commands can be called up.
	Camera address:	Enter the address of the camera. The address is set in the camera.

### Saving camera positions

You can specify positions for dome cameras and pan/tilt cameras to which you can repeatedly pan automatically or manually. The user can quickly select these positions in the live image, assuming that these have been enabled for his level of authorization. An automatic go-to if an event occurs is also possible.

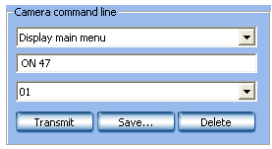
Proceed as follows to save a new position:

- Select a free ID.
- Pan the camera to the position and zoom the image as desired.
- Save the procedure.

4	Prepositions	
	ID Name	Click the down arrow beside the list field and select an unused number when you want to save a new position, or select a preposition to edit it. <b>Note:</b> When the user selects this name, the camera automatically moves to this camera position.
	This is how the camera is controlled. 	The camera is panned as follows: Move the mouse cursor around in the camera image until the directional arrow points in the direction in which you want to pan the camera. Then hold the left mouse button down. The camera pans in the direction of the arrow, the speed increasing the further you move the arrow outwards (with the left mouse button pressed). You zoom as follows: Move the mouse cursor around in the camera image window until a magnifying glass with a plus or minus sign appears. Left-click with the mouse to zoom the camera. Magnifying glass with a plus sign: Camera moves in toward the object. Magnifying glass with a minus sign: Camera moves away from the object.
	Save	Click the button to save. A dialog box opens. Enter a meaningful name and confirm the entry. A message confirms that this has been saved.
	Display	To check, select preposition and click the button. The camera moves to the preposition.
	Delete	Select a preposition and click the button.

### Entering control commands via the command line

Here, you can specify various commands for dome cameras, pan/tilt cameras or matrix switches via a command line. These commands can be called up manually or automatically. The choice of commands available can be found in the operating manual of the respective camera or matrix switch. The user can quickly select these commands in the live image, assuming that these have been enabled for his level of authorization.

5	Camera command line	
		<p>First line: The list contains preset control commands that you can select.</p> <p>Middle line (command line): The command that you selected in the first line is displayed. Alternatively, you can use this line to create a new command if you do not find a suitable command in the drop-down list for the first line.</p> <p>Bottom line: Assign the command a free number.</p>
	Save...	<p>Click the button to save. A dialog box opens. Enter a meaningful name and confirm the entry. A message confirms that this has been saved.</p> <p><b>Note:</b> The command is available on the user interface.</p>
	Transmit	Click the button to check the command.
	Delete	The saved command will be deleted.

### Camera control

The focus and iris can be set for each camera

6	Bilinx status:	The status is displayed.
	Iris and focus...	Click the button. A dialog box opens to allow you to set the iris and focus.

### Saving entries

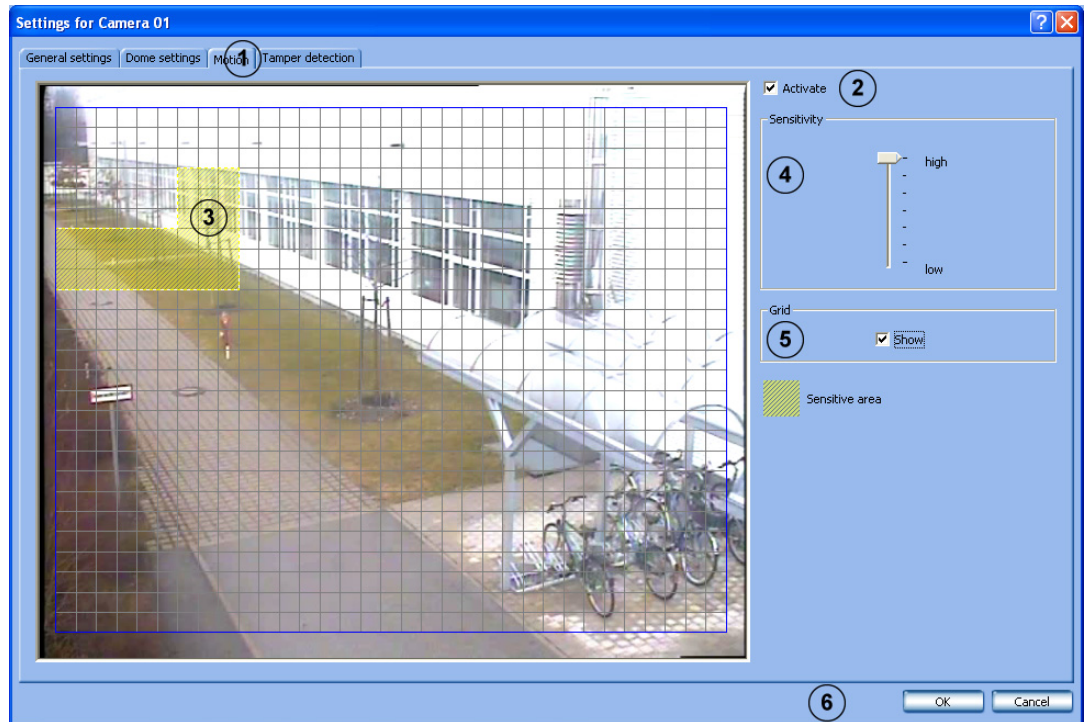
7	OK	The entries are saved.
---	----	------------------------



## 6.2.3

**Specifying Monitoring Zone for Motion Cameras**

Video and audio connections menu &gt; Camera section &gt; Edit button



Make the settings for each camera as required.

1	Motion	Click the tab. The entire image content inside the blue frame is initially sensitive, i.e. motion is monitored.
2	Activate	Select the check box to activate the motion sensor.
3	Within the blue frame (image window)	Displays the current live image and the area being monitored. The image is updated every second.
	Left-click or hold the left mouse button down and drag an area	A plus sign appears beside the mouse cursor to show that the selected area is sensitive and will be assessed during motion detection. Sensitive areas are shown shaded in yellow.
	Right-click or hold the right mouse button down and drag an area	A minus sign appears beside the mouse cursor to show that the selected area is not sensitive and will not be assessed during motion detection. Non-sensitive areas are shown unshaded.
4	Sensitivity	Change the sensitivity when the results of motion detection are not satisfactory.
	high	The sensitivity increases i.e. to trigger an alarm, smaller changes in the edges, the brightness and the motion are needed.
	low	The sensitivity decreases i.e. to trigger an alarm, larger changes in the edges, the brightness and the motion are needed.
5	Grid - Show	A grid is shown in the image when the check box is activated. The sizes of the drawn-in sensitive/insensitive areas are oriented around the grid.
6	OK	The entries are saved.

## 6.2.4

## Configuring Tamper Detection

Video and audio connections menu &gt; Camera section &gt; Edit button



Make the settings for each camera as required.

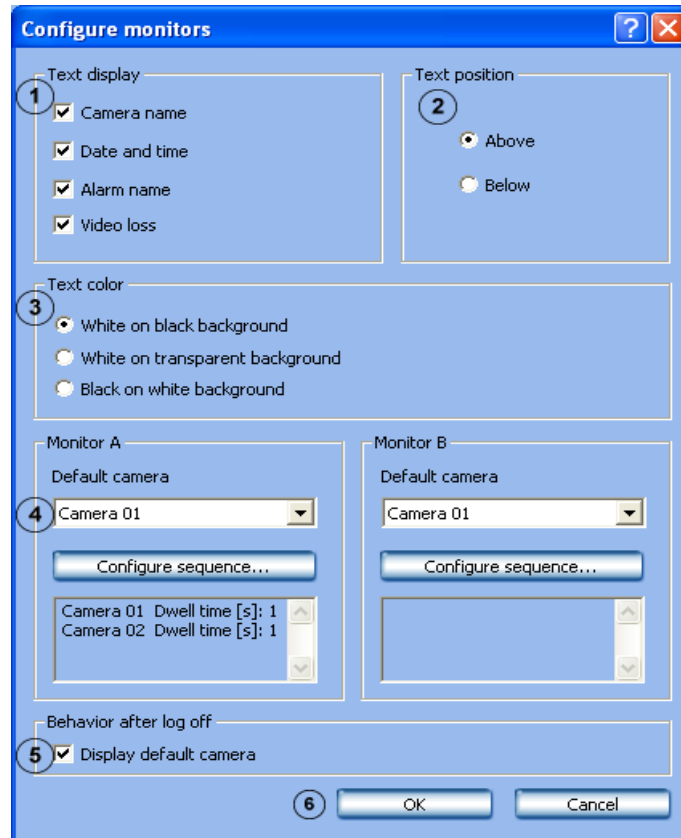
1	Tamper detection	Click the tab. The entire image content inside the blue frame is initially not selected.
2	Show camera warnings	Activate the check box if a warning is to be shown for camera problems (image too light, too dark, noisy). The values that trigger the warning are stored in the software and cannot be changed. <b>Note:</b> With pan/tilt cameras, panning the camera can cause the message "Video signal noisy" to be displayed when there is no malfunction.
3	Activate	Select the check box to activate the Reference image check.
4	Time periods	Click the arrow to display the time periods available. Select the time periods for which the reference image check is activated.
5	Within the blue frame (image window)	Displays the current live image and the area being monitored. The image is updated every second.
	Left-click or hold the left mouse button down and drag an area	A plus sign appears beside the mouse cursor to show that the area has been selected and is being monitored for tampering. Areas being monitored for tampering are shown shaded in yellow.
	Right-click or hold the right mouse button down and drag an area	A minus sign appears beside the mouse cursor to show that the area has not been selected. Unshaded areas are not being monitored.

6	Sensitivity	Change the sensitivity if the tamper detection results are not satisfactory.
	low	The sensitivity decreases, i.e. larger changes are needed for tamper detection.
	high	The sensitivity increases, i.e. smaller changes are needed for tamper detection. <b>Note:</b> Darker areas being monitored require greater sensitivity.
7	Grid - Show	A grid is shown in the image when the check box is activated. The sizes of the drawn-in areas are oriented around the grid.
8	Trigger delay	Enter the time after which an alarm is triggered. A delay of 120 to 3600 seconds can be entered.
9	Set reference image	Saves the live image displayed at this time as a reference image. This reference image is used to compare all subsequent live images.
10		Displays the reference image.
11	OK	The entries are saved.

## 6.2.5

### Configuring Video Monitors

**Video and audio connections** menu > **Monitors** section > **Configure** button



Specify the text display and the default camera sequence for the video monitors.

1	Text display	Select what should be shown on the monitors, for example camera name, date and time, etc.
2	Text position	Select where on the monitor the display should be.
3	Text color	Select what the display should look like, e.g. white on black background.
4	Monitor A/Monitor B	The default camera and sequence selected here can be started in the live image.
	Default camera	Select which camera should be displayed as standard.
	Configure sequence	Click the button if you want to specify a default camera sequence. A dialog box opens. Make your selection here (see also <i>Section 6.2.6 Configuring camera sequence</i> ).
5	Display default camera	Check box activated: After you have logged off, the camera selected under <b>Default camera</b> is displayed on monitor A/monitor B. Check box is not activated: After you have logged off, the camera sequence selected under <b>Configure sequence</b> is displayed on monitor A/monitor B. In the event of an alarm, the appropriate alarm sequence is displayed.
6	OK	The entries are saved.

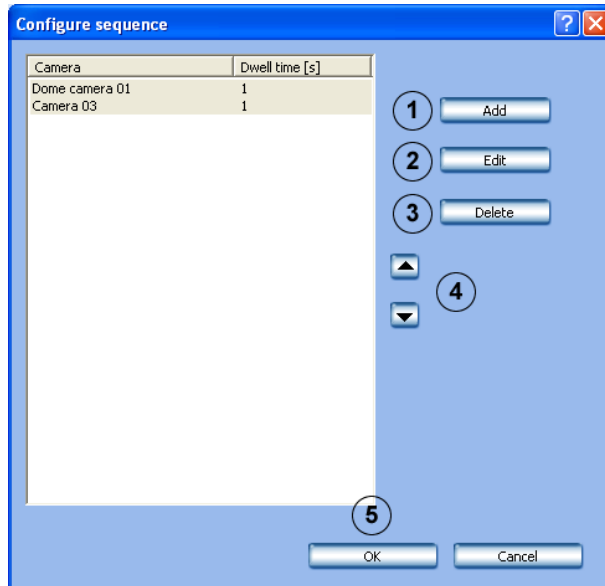
## 6.2.6 Configuring camera sequence



### Configuring default camera sequence:

**Video and audio connections** menu > **Monitors** section > **Configure** button > **Configure sequence** button

### Configuring alarm sequence:

**Alarm processing** menu > **Monitor control** section > **Edit** button

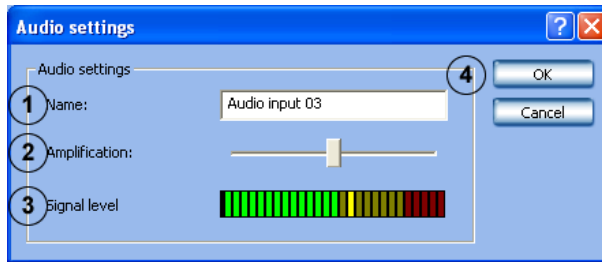


1	Add	Click the button. A dialog box opens. Select the cameras and the display duration that you want to add to the sequence. <b>Note:</b> JPEG and MPEG IP cameras cannot be selected.
2	Edit	Click the button. A dialog box opens. Make the changes here.
3	Delete	Deletes the camera from the sequence. First select the camera in the list field.
4	 	Changes the order of the cameras in the sequence. To do so, select the camera in the list field and click the up or down arrow.
5	OK	The entries are saved.

## 6.2.7

### Editing Audio Settings

**Video and audio connections** menu > **Audio input** section > **Edit** button



Here you can edit the names and the audio level of each individual audio input.

1	Name:	The name of the audio input is displayed and can be edited.
2	Audio level:	The audio level of the audio input can be changed with the slider. <b>Note:</b> Slider all the way left = minimum audio level Slider all the way right = maximum audio level
3	Signal level	Shows the signal level selected with the slider graphically. From the color, you can see if the sound is being received without distortion or if you need to change the audio level. Green = sound is too soft Yellow = sound is optimally set Red = sound is overamplified
4	OK	The entries are saved.

## 6.2.8

### Configuring JPEG IP Cameras

Video and audio connections menu > JPEG IP cameras section > Edit button

The screenshot shows the 'Settings for IP camera 1' window. It features a large empty area on the left for a camera preview. On the right, there are several configuration sections: 'Camera name' with a text field containing 'IP camera 1'; 'Image repeat rate for live images' with a checked checkbox and a spinner set to 4; 'Camera login' with 'User name' and 'Password' text fields; and 'Motion settings' with a checked checkbox and three text fields for 'Port', 'On command', and 'Off command'. The window has a blue title bar and standard window controls. Numbered callouts (1-8) highlight specific UI elements: (1) the 'Settings' tab, (2) the 'Display' button, (3) the 'Configure' button, (4) the 'Name' field, (5) the 'Max. no. of images per sec.' checkbox and spinner, (6) the 'User name' and 'Password' fields, (7) the 'Motion camera' checkbox, and (8) the 'OK' and 'Cancel' buttons.

In this menu, only those cameras from which JPEG images can be accessed via the http protocol can be configured. Depending on the model, a maximum of 32 network devices (JPEG cameras and MPEG4 devices from Bosch) can be connected.

1	Address:	<p>Enter the address (URL) of the camera and the command to access the JPEG images.</p> <p>The following syntax must be applied:</p> <p><b>Bosch BVIP devices:</b></p> <p>http://IP-Adresse/snap.jpg?JpegSize=S (for QCIF)  http://IP-Adresse/snap.jpg?JpegSize=M (for CIF)  http://IP-Adresse/snap.jpg?JpegSize=L (for 2CIF)  http://IP-Adresse/snap.jpg?JpegSize=XL (for 4CIF)</p> <p>For multi-channel devices, the channel must be selected as follows:  http://IP-Adresse/snap.jpg?JpegCam=2&amp;JpegSize=XL (e.g. for channel 2 and 4CIF)</p> <p><b>Bosch MegaPixel IP camera:</b></p> <p>http://IP-Adresse/image?res=full&amp;x0=0&amp;y0=0  &amp;x1=100%&amp;y1=100%&amp;quality=12&amp;doublescan=0</p> <p>With HTTP, motion detection occurs via port [&amp;mdn=Port number].</p> <p>tftp://IP-Adresse/  image?res=half&amp;x0=0&amp;y0=0&amp;x1=1600&amp;y1=1200&amp;quality=15</p> <p>With TFTP, the motion detection is retained in the image. It is not necessary to configure a port.</p> <p><b>Axis:</b> http://IP-Adresse/jpg/image.jpg</p> <p><b>Robotix:</b> http://IP-Adresse/record/current.jpg</p> <p><b>Note:</b></p> <p>More information can be found in the installation documents of the relevant camera.</p>
2	Display	When you click the button, you can check whether the entered URL and command are correct. If so, the camera image appears.
3	Configure	After the button is clicked, the configuration of the selected JPEG device is displayed in a browser window.
4	Name:	Enter the name of the camera.
5	Max. no. of images per sec.:	<p>Activate this check box and enter the number of images per second to be displayed. This affects the network load when viewing live images from the cameras.</p> <p><b>Note:</b></p> <p>The maximum number of displayed images depends on the camera type and the parameters set for the camera (e.g.: resolution, compression setting).</p>
6	User name:	Enter the camera user name and password needed for log-on (e.g. Robotix banking camera).
	Password:	
7	Motion camera	If the IP camera is a motion detection camera, the video system can be controlled when the sensor technology is triggered. Activate the check box for this.
	Port:	Enter the port to which the camera sends the motion information.



	On command:	Here you enter the command that the camera sends when motion detection is triggered. <b>Note:</b> The command can be found in the handbook for the camera used.
	Off command:	Here you enter the command that the camera sends when motion detection has ended.
8	OK	The entries are saved.

**NOTICE!**

When configuring JPEG IP cameras, the following limits must be observed:

**Image size and resolution limits:**

- A single JPEG image must not exceed 100 kB.
- The image resolution must be in the aspect ratio 4:3 (e.g. 2048 x 1536).
- The maximum resolution of the displayed images is limited to 2048 x 1536.

**Recording settings limits:**

- The transmission images from analog and IP cameras are limited to a total of 900 images per second.
- The recording rate is limited to 50 Mbit/second (= 6.25 MB/second).



## 6.2.9

## Configuring MPEG4 IP Cameras

Video and audio connections menu > MPEG4 IP cameras section > Edit button

In this menu, only MPEG4 units from Bosch from which MPEG4 images can be called up can be configured (e.g. VideoJet, VIP). Depending on the model, a maximum of 32 network devices (JPEG cameras and MPEG4 devices from Bosch) can be connected.

1	Camera name	
	Device type:	Select the MPEG4 device you require.
	IP address:	Enter the address (URL) of the MPEG4 device.
	Channel:	Select the channel of the MPEG4 device.
	Name:	Enter the name of the MPEG4 device. The choice of name is up to you.
	Live stream:	Select the stream of the MPEG4 device (Stream 1 or Stream 2) to be used for viewing live images.
	Motion detection	Activates the motion detection of the MPEG4 device in DiBos. <b>Note:</b> – Motion detection must also be activated on the MPEG4 device. – Under <b>Alarm processing</b> , the name of the MPEG4 device appears in the <b>Trigger</b> section. The trigger can, for example, be selected so that it controls recording. To do so, you must select the job you require.
	Reference image check	Activates the reference image check of the MPEG4 device in DiBos. <b>Note:</b> The reference image check must also be activated on the MPEG4 device.

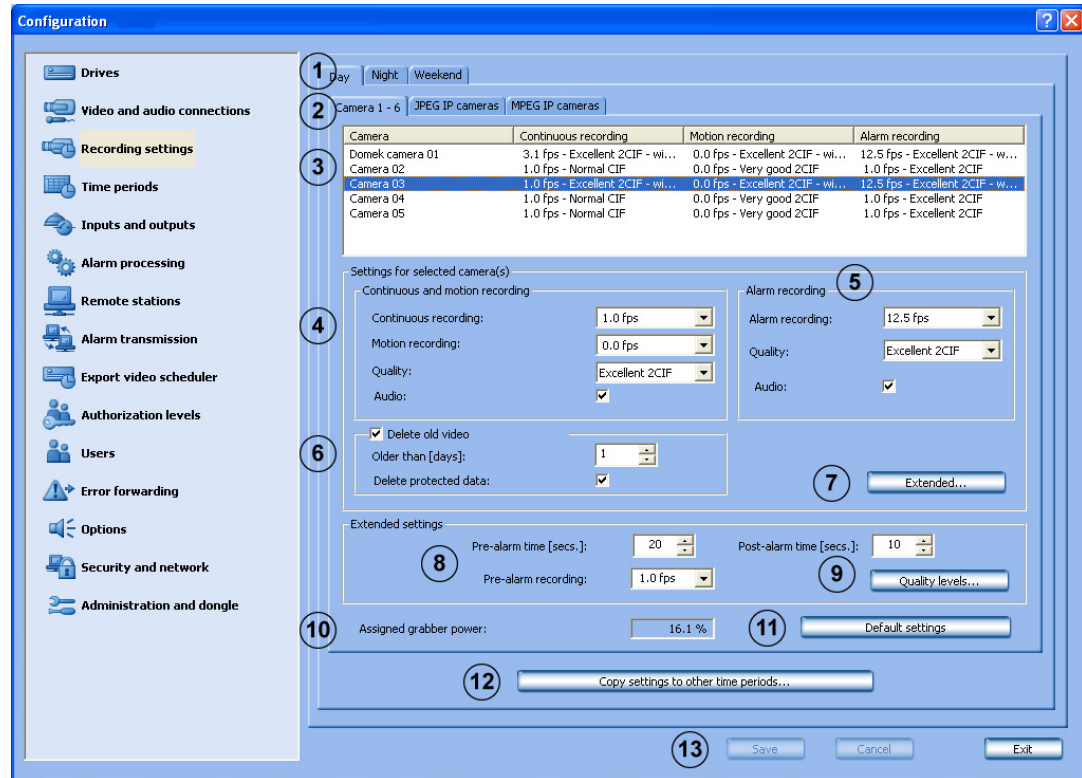
	Time periods	Select the time periods for carrying out a reference image check.
	Display	The live image from the selected MPEG4 device will be displayed if the settings were entered correctly.
	Configure	After the button is clicked, the configuration of the selected MPEG4 device is displayed in a browser window.
2	Camera login	
	User name:	Enter the user name and password for MPEG4 devices where they are needed for logging on (e.g. when a user name and password are configured in the MPEG4 device). <b>Note:</b> Select the user name <b>Service</b> , if a service password has been assigned for the MPEG4 device. The corresponding password must be entered.
	Password:	
3	Activate alarm input	Activate this check box when triggering of the input on the MPEG4 device is to be used for control of the video system. <b>Note:</b> Depending on the type of IP device (e.g. VIP X1600), more than 1 alarm input can be configured. Select the alarm input of the MPEG4 device under <b>No.</b> and activate the <b>Activate alarm input</b> check box for this alarm input.
	Name	Enter the name of the alarm input. The choice of name is up to you.
	No.:	Choose the alarm input of the selected MPEG4 device.
4	Activate relay	Activate this check box if the relay output of the MPEG4 device is to be controlled by the video system. <b>Note:</b> Depending on the type of IP device (e.g. VIP X1600), more than 1 relay output can be configured. Select the relay output of the MPEG4 device under <b>No.</b> and activate the <b>Activate relay</b> check box for this relay output.
	Name:	Enter the name of the relay output. The choice of name is up to you.
	No.:	Choose the relay output of the selected MPEG4 unit.
5	Activate audio input	Activate this check box when the audio input of the MPEG4 device is to be used.
	Name:	Enter the name of the audio input.
	No.:	Choose the audio input of the selected MPEG4 unit.
6	OK	The entries are saved.

## 6.3 Configuring Recording Settings

You can configure the recording settings of the analog cameras, JPEG IP cameras and MPEG4 IP cameras in these dialog boxes.

### 6.3.1 Configuring Recording Settings for Analog Cameras

Recording settings menu > Camera x - y tab



You can configure the recording settings of the analog cameras in this dialog box.

1	Day   Night   Weekend ...	All configured time periods are displayed as tabs. Select the time period for which the settings should apply. <b>Note:</b> Only the time periods configured under <b>Time periods</b> are displayed.
2	Camera 1 - 6   Camera 7 - 12 I...	Select the tab. Tabs with cameras are displayed for each time period. Select the tab with the camera for which you want to make settings. The corresponding list field shows all cameras connected to the same grabber card. <b>Note:</b> The number of tabs depends on the number of grabber cards and network components in the system. IP camera tabs are only shown when IP cameras are configured.
3	In the camera list field	Select the camera for which you want to edit the settings. <b>Note:</b> Multiple cameras can be selected and set up jointly. The settings in points 4 - 7 only refer to the selected cameras and the associated time periods.

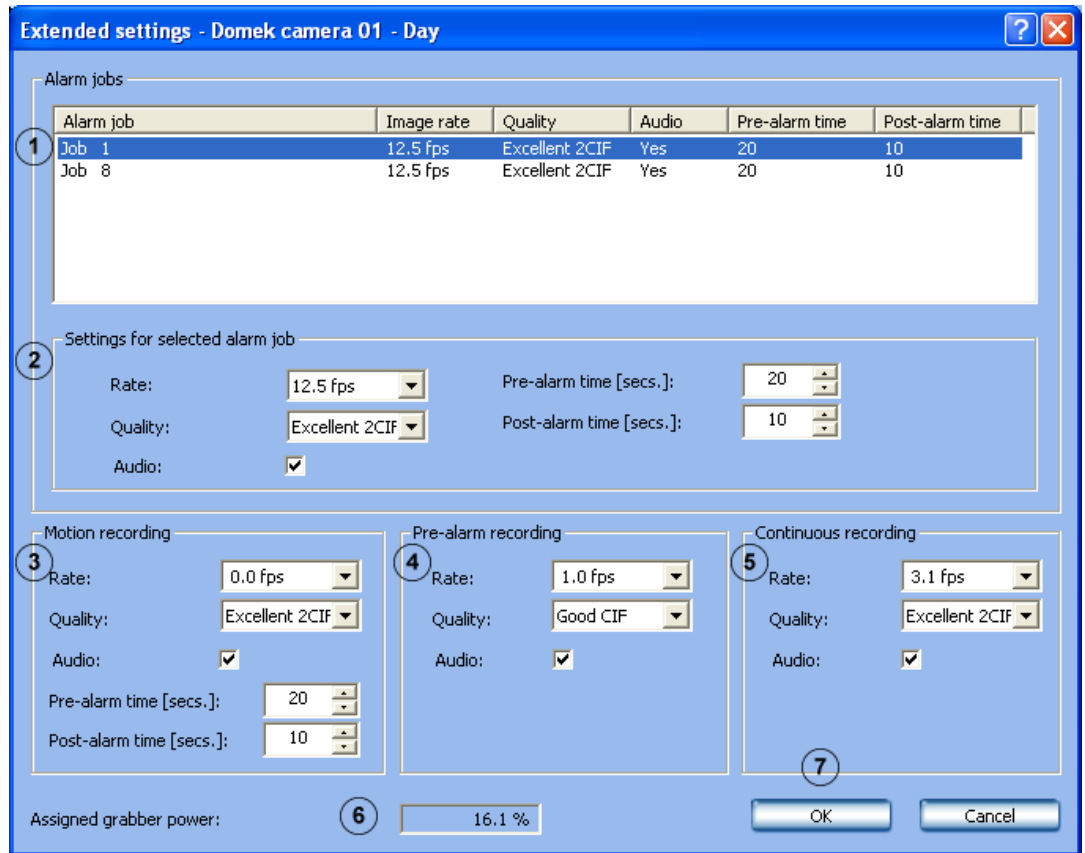
4	Continuous and motion recording	Make the settings for continuous and motion recording. <b>Note:</b> If the recording rate and the quality exceed the grabber power, the system displays a message to this effect. If the user ignores this message, recording is made at the greatest rate possible.
	Continuous recording:	Select the recording rate for continuous and motion recording.
	Motion recording:	<b>Note:</b> Recording only takes place if a value greater than <b>0 fps (images per second)</b> is selected.
	Quality:	Select the recording quality. The selection possibilities are valid for continuous and motion recording. <b>Note:</b> Six quality levels are pre-defined in the system. If the input field is empty, there are different quality levels for continuous and motion recording. Further recording qualities can be added. To do so, click <b>Quality levels...</b>
	Audio:	Activate this check box if audio is also to be recorded. <b>Note:</b> Audio can only be selected if the camera has been assigned an audio input. This is done under <b>Video and audio connections</b> → <b>Add or modify camera</b> → <b>General settings</b> → <b>Audio input</b> . An audio recording is made for continuous and/or motion recording.
5	Alarm recording	Make the settings for alarm recording.
	Alarm recording:	Select the recording rate.
	Quality:	Select the recording quality. <b>Note:</b> Six quality levels are pre-defined in the system. Further recording qualities can be added. To do so, click <b>Quality levels...</b>
	Audio:	Activate this check box if audio is also to be recorded.
6	Delete old video	Activate this check box to automatically delete data after a specified number of days.
	Older than [days]:	Enter the number of days after which data should be deleted. <b>Example:</b> 3 means that all data older than 3 days is automatically deleted.
	Delete protected data:	Check box is activated: Protected data is automatically deleted after a specified number of days. Check box is not activated: protected data is not automatically deleted.

7	Extended...	Click the button. A dialog box opens. Here you can edit the settings for each camera.
8	Extended settings	The information on pre- and post-alarm time and pre-alarm recording are valid for the selected time period and for all cameras on the camera tab. <b>Note:</b> If the cameras are assigned differing values, this is indicated by an asterisk (*).
	Pre-alarm time [sec.]:	Select the pre-alarm time for the alarm and motion recording. <b>Note:</b> The maximum pre-alarm time is 1800 seconds. The pre-alarm time depends on the recording rate of the pre-alarm recording. A maximum of 3600 images can be recorded for each pre-alarm and by each camera. <b>Example:</b> 1 image/second = 1800 seconds, 2 images/second = 900 seconds, 4 images/second = 450 seconds, 5 images/second = 360 seconds etc.
	Post-alarm time [secs.]:	Enter the post-alarm time. <b>Note:</b> The maximum post-alarm time is 999 seconds. The default setting is 0 seconds.
	Pre-alarm recording:	Select the recording rate for the pre-alarm time. The recording rate applies to alarm recording and motion recording.
9	Quality levels	Click the button. A dialog box opens. You can add or edit recording qualities (see also <i>Section Specify recording quality for analog cameras</i> ).
10	Assigned grabber power	The system calculates, per camera tab (grabber) and time period, the sum of the recording rates for continuous and motion recording. Alarms are not taken into account. <b>Note:</b> If the result exceeds the grabber power (more than 100%), the user cannot save the settings.
11	Default settings	Click the button to see the default settings.
12	Copy settings to other time periods...	Copies all tabs from the selected time period with all the settings they contain into other time periods. Click the button. A dialog box opens where you can select the time periods.
13	Save	The entries are saved.

**Extended recording settings for analog cameras**

**Recording settings** menu > **Camera x - y** tab > **Extended...** button

(see also Section 6.3 Configuring Recording Settings)



In this dialog box you can edit individual settings.

1	Alarm jobs	The list field shows all jobs where this camera is in the alarm recording list. <b>Note:</b> The alarm jobs are added to the list field according to the configuration.
2	Settings for selected alarm job	First select a job in the list field. The settings for the selected job are displayed. <b>Note:</b> If the jobs are assigned differing values, this is indicated by an asterisk (*).
	Rate:	Select the recording rate for the job.
	Quality:	Select the recording quality for the job. <b>Note:</b> Six quality levels are pre-defined in the system. Further recording qualities can be added. To do so, click <b>Quality levels...</b>

	Audio:	Activate this check box if audio is also to be recorded along with this job. <b>Note:</b> The audio input must be assigned to the camera. This is done under <b>Video and audio connections</b> → <b>Add or modify camera</b> → <b>General settings</b> → <b>Audio input</b> .
	Pre-alarm time [sec.]:	Select the pre-alarm time for the alarm and motion recording. <b>Note:</b> The maximum pre-alarm time is 1800 seconds. The pre-alarm time depends on the recording rate of the pre-alarm recording. A maximum of 3600 images can be recorded for each pre-alarm and by each camera. <b>Example:</b> 1 image/second = 1800 seconds, 2 images/second = 1800 seconds, 4 images/second = 900 seconds, 5 images/second = 720 seconds etc.
	Post-alarm time [secs.]:	Enter the post-alarm time. <b>Note:</b> The maximum post-alarm time is 999 seconds. The default setting is 0 seconds.
3	Motion recording	Make the settings for motion recording.
	Rate:	Select the recording rate.
	Quality:	Select the recording quality.
	Audio:	Activate this check box if audio is also to be recorded.
	Pre-alarm time [sec.]:	Select the pre-alarm time for the alarm and motion recording. <b>Note:</b> The maximum pre-alarm time is 1800 seconds. The pre-alarm time depends on the recording rate of the pre-alarm recording. A maximum of 3600 images can be recorded for each pre-alarm and by each camera. <b>Example:</b> 1 image/second = 1800 seconds, 2 images/second = 1800 seconds, 4 images/second = 900 seconds, 5 images/second = 720 seconds etc.
	Post-alarm time [secs.]:	Enter the post-alarm time. <b>Note:</b> The maximum post-alarm time is 999 seconds. The default setting is 0 seconds.
4	Pre-alarm recording	Make the settings for pre-alarm recording.
	Rate:	Select the recording rate for the pre-alarm time. The recording rate applies to alarm recording and motion recording.
	Quality:	Select the recording quality.
	Audio:	Activate this check box if audio is also to be recorded.



5	Continuous recording	Make the settings for continuous recording.
	Rate:	Select the recording rate. <b>Note:</b> The value 0 means no recording.
	Quality:	Select the recording quality.
	Audio:	Activate this check box if audio is also to be recorded.
6	Assigned grabber power:	The system calculates, per camera tab and time profile, the sum of the recording rates for continuous and motion recording. <b>Note:</b> If the result exceeds the grabber power (more than 100%), the user cannot save the settings.
7	OK	The entries are saved.

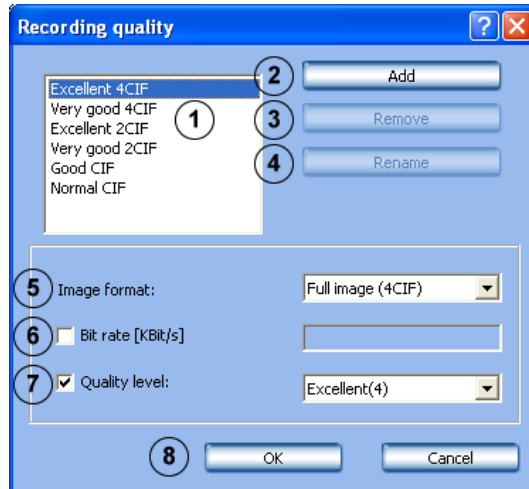
### Specify recording quality for analog cameras

**Recording settings** menu > **Camera x - y** tab > **Quality levels...** button

or

**Options** menu > **Quality levels** button

(see also *Section 6.3 Configuring Recording Settings*)



In this dialog box you can edit an existing recording quality or add a new recording quality.

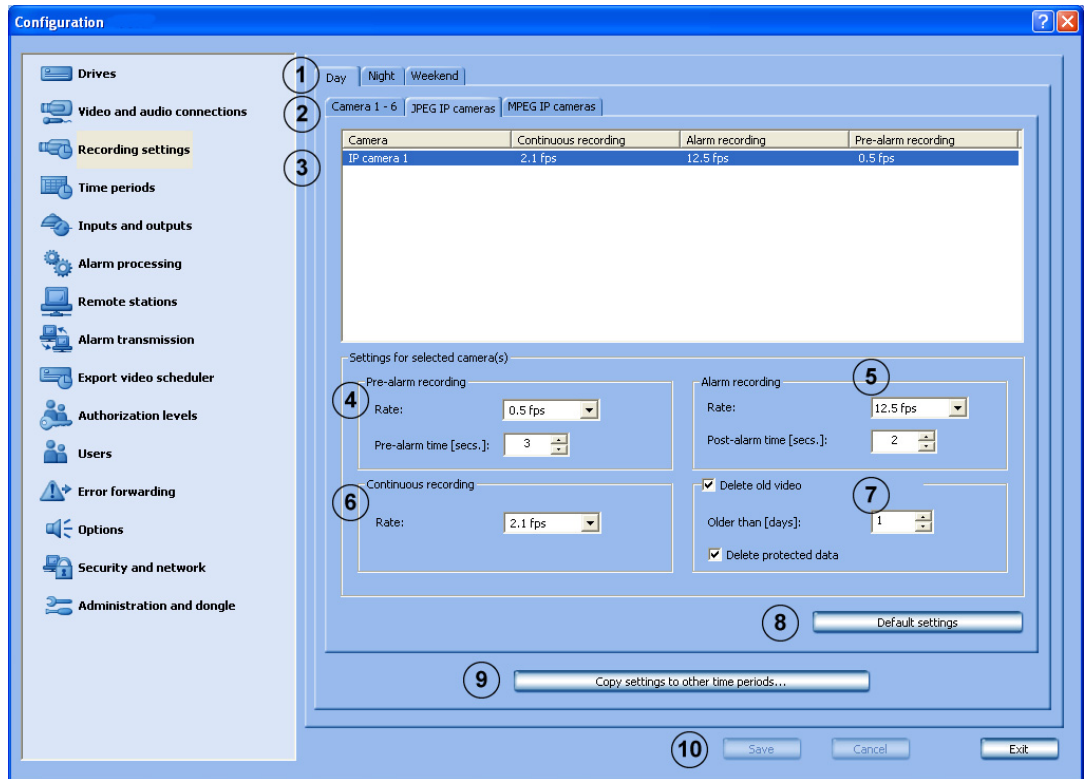
1		List of existing recording qualities.
2	Add	Adds a new recording quality.
3	Remove	Removes an existing recording quality. To do so, select the name.
4	Rename	Changes the name of a recording quality. To do so, select the name.
5	Image format	Select the image format.
6	Bit rate [KBit/s]	If necessary, activate this check box and enter a maximum value for the bit rate. <b>Note:</b> If a function is not activated, the bit rate is variable.
7	Quality level:	Activate the check box and select the quality level (2 = highest quality level, 30 = lowest quality level). <b>Note:</b> If a function is not activated, the standard values are adopted.
8	OK	The entries are saved.

Pre-defined standard values of the quality levels:

Recording quality	Image format	Quality level
Excellent 4CIF	4CIF	4
Very good 4CIF	4CIF	6
Excellent 2CIF	2CIF	4
Very good 2CIF	2CIF	6
Good CIF	CIF	10
Normal CIF	CIF	15

### 6.3.2 Configuring Recording Settings of JPEG IP Cameras

Recording settings menu > IP cameras tab



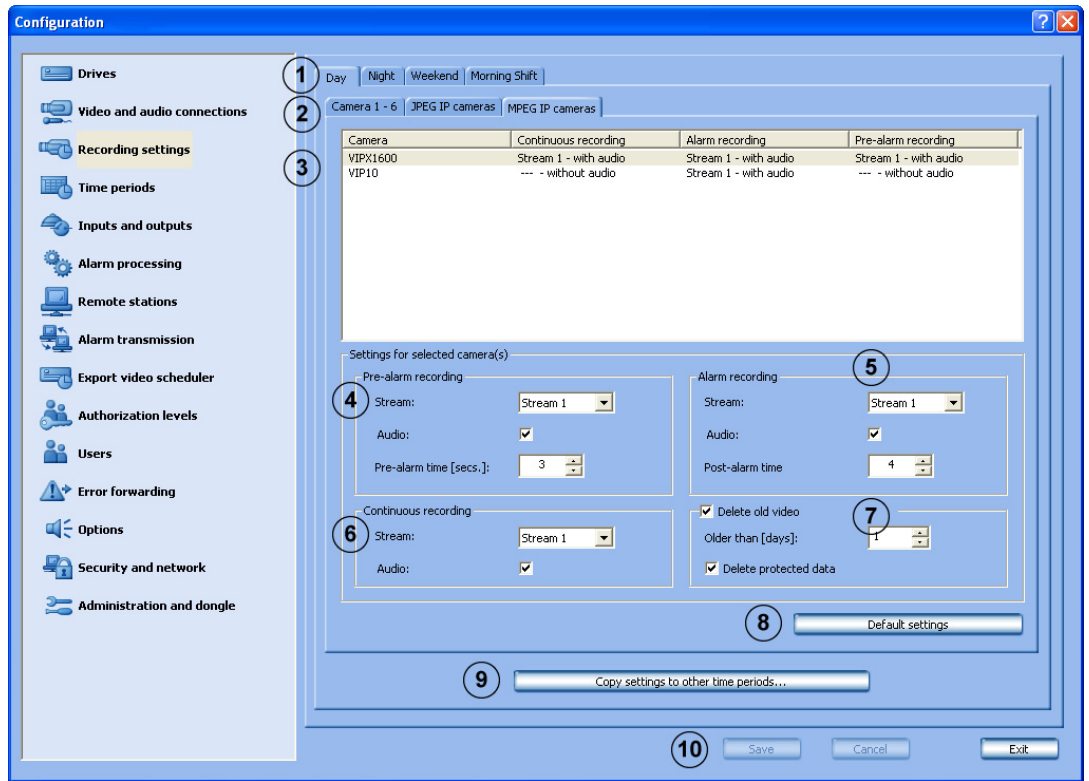
You can configure the recording settings for the JPEG IP camera in this dialog box.

1	Day   Night   Weekend ...	All configured time profiles are displayed as tabs. Select the time profile to which the settings should apply. <b>Note:</b> Only the time profiles configured under <b>Time periods</b> are displayed.
2	IP cameras	Select the tab. All JPEG IP cameras are displayed in the list field underneath.
3	In the camera list field	Select the camera for which you want to edit the settings.
4	Pre-alarm recording	Make the settings for pre-alarm recording.
	Rate:	Select the recording rate. <b>Note:</b> The actual recording rate depends on the camera type and the parameters set for the camera (e.g.: resolution, compression setting). The average setting is 4 - 6 images per second.

	Pre-alarm time [sec.]:	Select the pre-alarm time for the alarm and motion recording. <b>Note:</b> The maximum pre-alarm time is 1800 seconds. The pre-alarm time depends on the recording rate of the pre-alarm recording. A maximum of 3600 images can be recorded for each pre-alarm and by each camera. <b>Example:</b> 1 image/second = 1800 seconds, 2 images/second = 1800 seconds, 4 images/second = 900 seconds, 5 images/second = 720 seconds etc.
5	Alarm recording	Make the settings for alarm recording.
	Rate:	Select the recording rate. <b>Note:</b> The actual recording rate depends on the camera type and the parameters set for the camera (e.g.: resolution, compression setting).
	Post-alarm time [secs.]:	Enter the post-alarm time. <b>Note:</b> The maximum post-alarm time is 999 seconds. The default setting is 0 seconds.
6	Continuous recording	Make the settings for continuous recording.
	Rate:	Select the recording rate. <b>Note:</b> The actual recording rate depends on the camera type and the parameters set for the camera (e.g.: resolution, compression setting).
7	Delete old video	Activate this check box to automatically delete data after a specified number of days.
	Older than [days]:	Enter the number of days after which data should be deleted. <b>Example:</b> 3 means that all data older than 3 days is automatically deleted.
	Delete protected data:	Check box is activated: Protected data is automatically deleted after a specified number of days. Check box is not activated: protected data is not automatically deleted.
8	Default settings	Click the button to see the default settings.
9	Copy settings to other time periods...	Copies all tabs from the selected time period with all the settings they contain into other time periods. Click the button. A dialog box opens where you can select the time periods.
10	Save	The entries are saved.

### 6.3.3 Configuring Recording Settings of MPEG4 IP Cameras

Recording settings menu > MPEG IP cameras tab



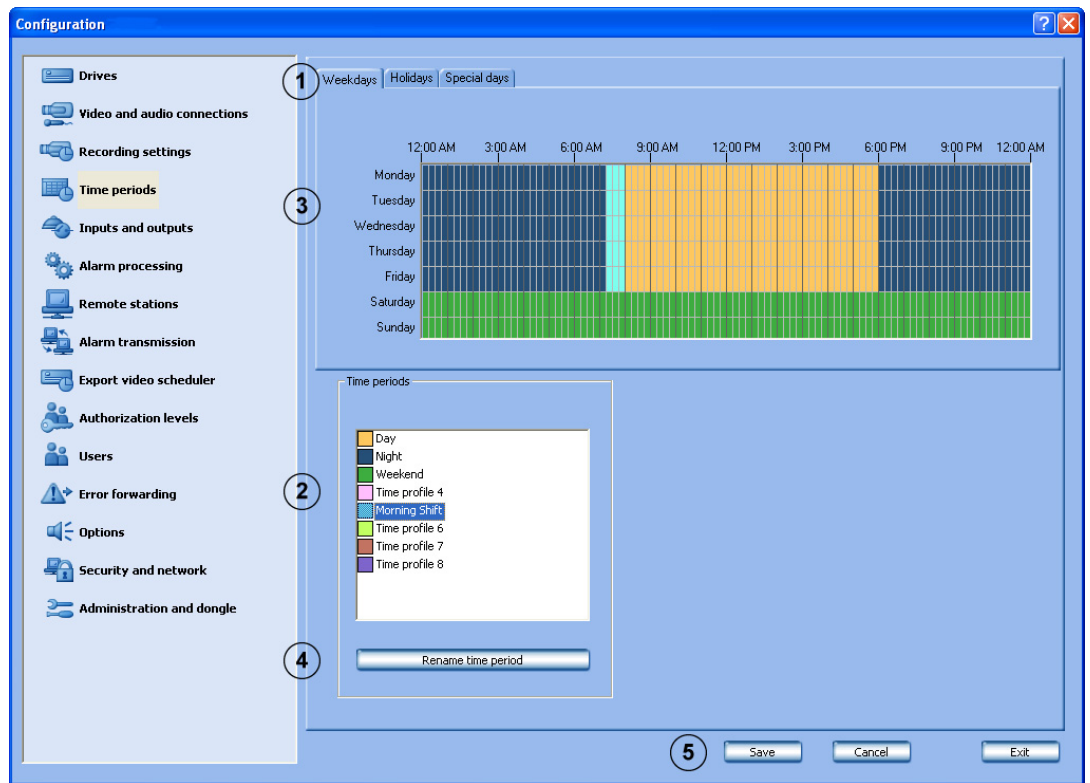
You can configure the recording settings for the MPEG4 IP camera in this dialog box.

1	Day   Night   Weekend ...	All configured time profiles are displayed as tabs. Select the time profile to which the settings should apply. <b>Note:</b> Only the time profiles configured under <b>Time periods</b> are displayed.
2	MPEG IP cameras	Select the tab. All MPEG IP cameras are displayed in the list field underneath.
3	In the camera list field	Select the camera for which you want to edit the settings.
4	Pre-alarm recording	Make the settings for pre-alarm recording.
	Stream	Select the stream for the MPEG4 device (Stream 1 or Stream 2).
	Audio	Activate this check box if audio is also to be recorded. <b>Note:</b> Audio can only be selected if the <b>Activate audio input</b> check box is selected under <b>Video and audio connections</b> ➔ <b>MPEG4 IP cameras - Modify</b> ➔ <b>General settings</b> .

	Pre-alarm time [sec.]:	Select the pre-alarm time for the alarm and motion recording. <b>Note:</b> The maximum pre-alarm time is 1800 seconds. The pre-alarm time depends on the recording rate of the MPEG4 device's pre-alarm recording. A maximum of 3600 images can be recorded for each pre-alarm and by each camera.
5	Alarm recording	Make the settings for alarm recording.
	Stream	Select the stream for the MPEG4 device (Stream 1 or Stream 2).
	Audio	Activate this check box if audio is also to be recorded.
	Post-alarm time [secs.]:	Enter the post-alarm time. <b>Note:</b> The maximum post-alarm time is 999 seconds. The default setting is 0 seconds.
6	Continuous recording	Make the settings for continuous recording.
	Stream	Select the stream for the MPEG4 device (Stream 1 or Stream 2).
	Audio	Activate this check box if audio is also to be recorded.
7	Delete old video	Activate this check box to automatically delete data after a specified number of days.
	Older than [days]:	Enter the number of days after which data should be deleted. <b>Example:</b> 3 means that all data older than 3 days is automatically deleted.
	Delete protected data:	Check box is activated: Protected data is automatically deleted after a specified number of days. Check box is not activated: protected data is not automatically deleted.
8	Default settings	Click the button to see the default settings.
9	Copy settings to other time periods...	Copies all tabs from the selected time period with all the settings they contain into other time periods. Click the button. A dialog box opens where you can select the time periods.
10	Save	The entries are saved.

## 6.4 Configuring Time Periods

### Time periods menu



Time periods are assigned with the mouse cursor in a graphical time planner. There are 8 time periods available. These time periods can be assigned to any day of the week, individual holidays and special days. The time periods are displayed in different colors.

1	Weekdays	Select the corresponding tab.
	Holidays	<b>Note:</b> You can add holidays or special days if you have selected the <b>Holidays</b> or <b>Special days</b> tab.
	Special days	
2	Time periods	Select the time period to which you want to assign a day. A time span can be assigned to only one time period.
3	Graphical time planner	<p>Move the mouse cursor into the graphical time planner. Clicking with the left mouse button marks a cell. Dragging up a square while pressing the left mouse button marks a time period. All selected cells take the color of the selected time period.</p> <p><b>Note:</b> The 24 hours of the day are displayed on the horizontal axis of the graphical time planner. Each hour is subdivided into four cells. A cell is the smallest selectable time unit and represents 15 minutes.</p> <p>The days are shown on the vertical axis.</p> <p>To edit selected cells in the graphical time planner, select another time period and overwrite the cell already selected.</p>

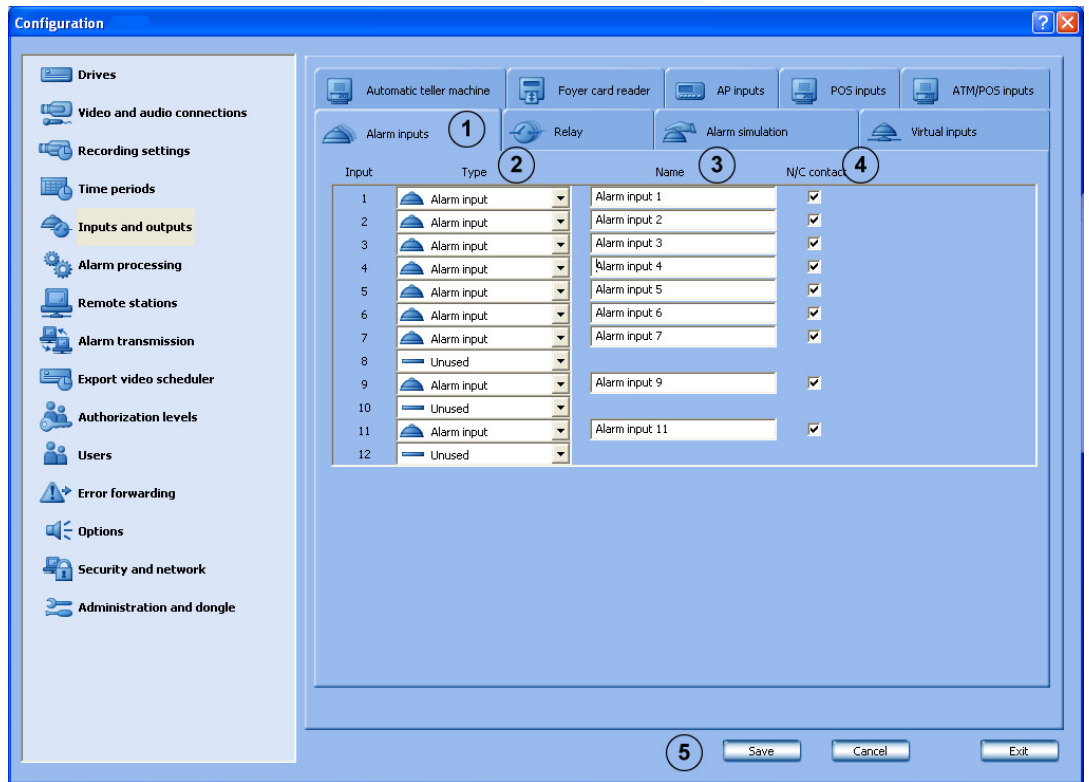
4	Rename time period	To change the name. Select a time period and click the button. Enter a new name and confirm the entry by pressing <b>Enter</b> .
5	Save	The entries are saved.



## 6.5 Configuring Inputs and Outputs

### 6.5.1 Configuring Alarm Inputs

Inputs and outputs menu > Alarm inputs tab

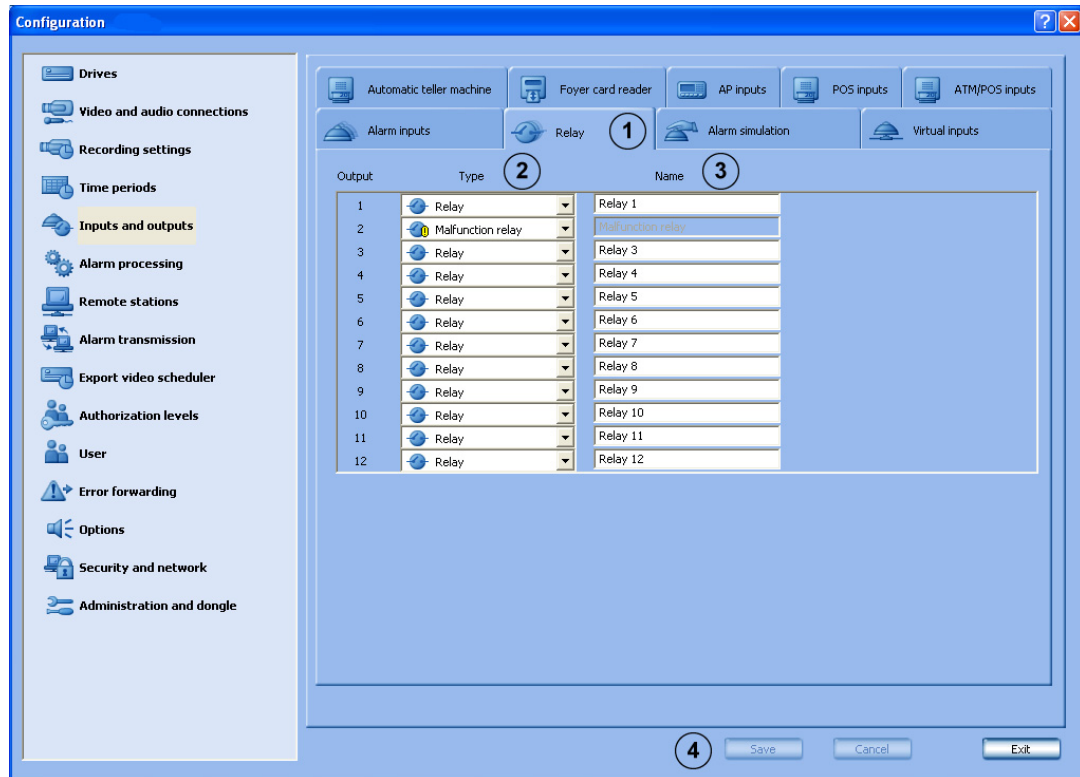


This dialog box allows the user to activate or deactivate the alarm inputs on the grabber card and select the standby condition. There are 32 alarm inputs available in DiBos and 12 alarm inputs in DiBos micro.




1	Alarm inputs	Click the tab.
2	Type	Click the down arrow in the column and select whether an input is to be configured or not.
		The input is assessed as an alarm input.
		The input is not assessed as an alarm input.
3	Name	Place the cursor in the column and enter the name of the alarm input.
4	N/C contact	Specify whether an N/C or N/O contact is connected to the alarm input.
	<input checked="" type="checkbox"/>	N/C contact connected.
	<input type="checkbox"/>	N/O contact connected.
5	Save	The entries are saved.

## 6.5.2 Configuring Relay Outputs

### Inputs and outputs menu > Relay tab

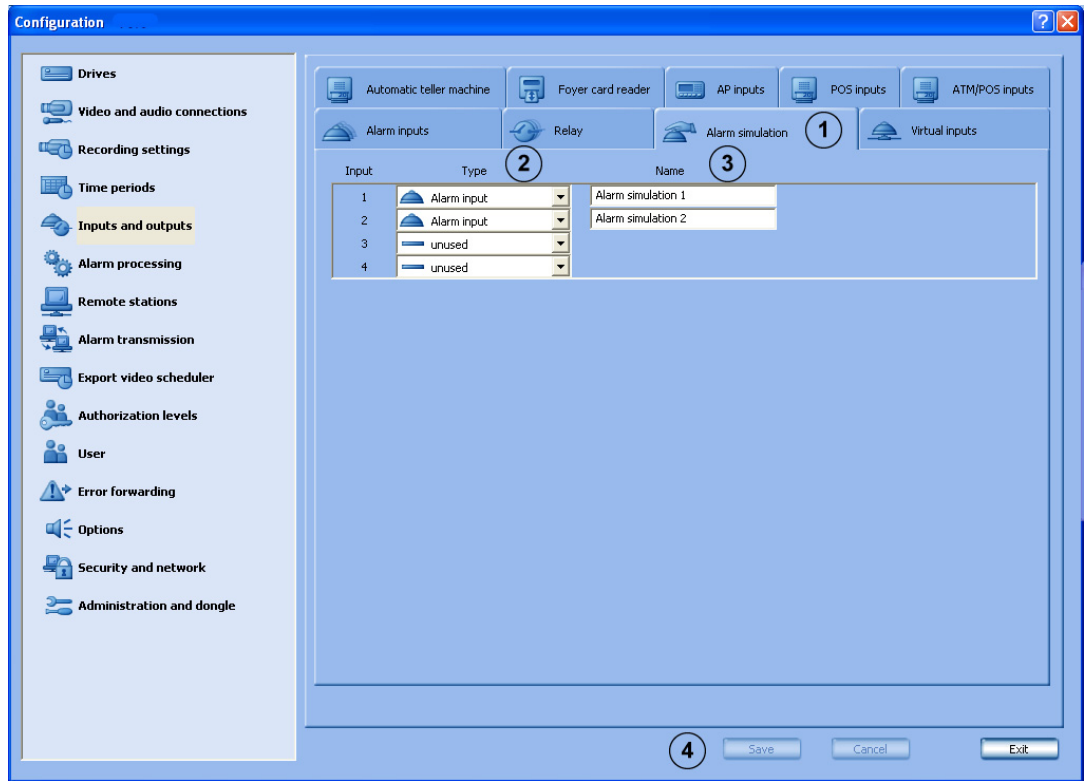


The number of relay outputs depends on the model. In DiBos there are a maximum of 16 relay outputs available and in DiBos micro, 12 relay outputs. The relays can be activated locally, from a remote station, via a job or via a browser.



1	Relay	Click the tab.
2	Type	Click the down arrow in the column and select whether an output is to be activated or not.
		The relay output is activated.
		A malfunction relay can be connected to the relay output. <b>Note:</b> Only one malfunction relay can be connected. The events that trigger the malfunction relay can be found in the <b>Connecting a Malfunction Relay</b> chapter in the installation handbook
		The relay output is not activated.
3	Name	Place the cursor in the column and enter the name.
4	Save	The entries are saved.

### 6.5.3 Configuring Alarm Simulation

Inputs and outputs menu > Alarm simulation tab

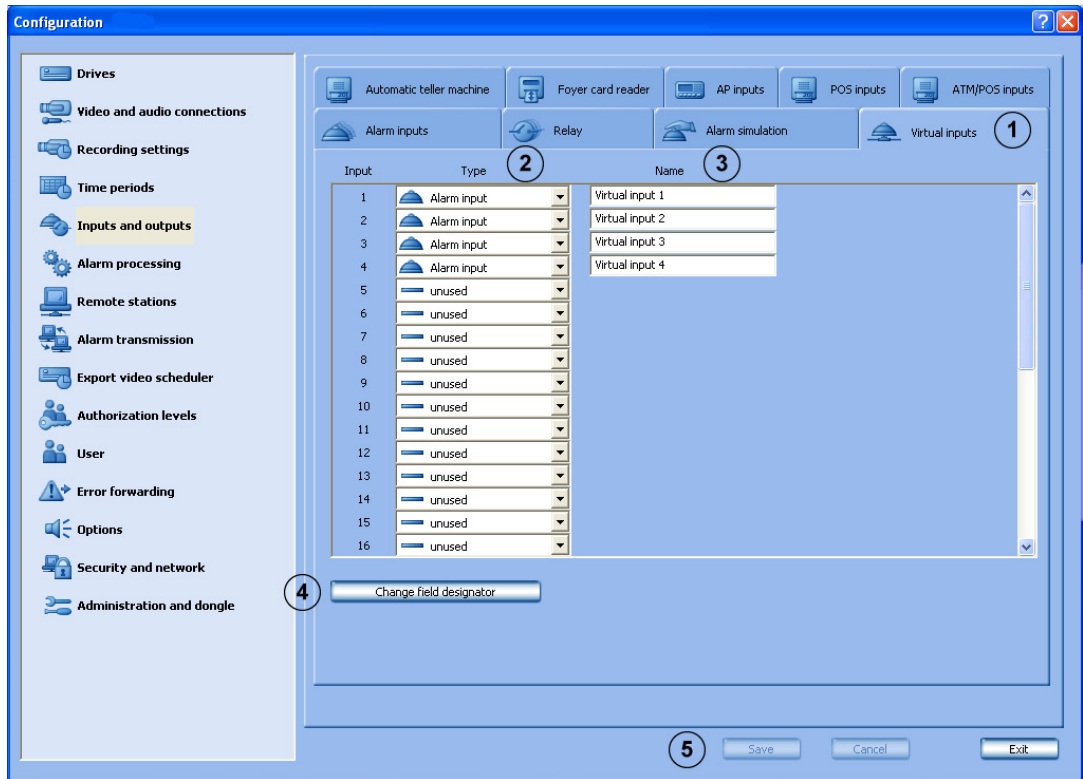


The video system supports 4 inputs for the triggering of user alarms in the user interface.

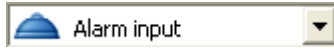
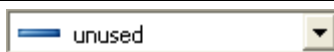
1	Alarm simulation	Click the tab.
2	Type	Click the down arrow in the column and select whether an input is to be activated or not.
		Input is to be used for alarm simulation.
		Input is not to be used for alarm simulation.
3	Name	Place the cursor in the column and enter the name.
4	Save	The entries are saved.

## 6.5.4 Configuring Virtual Inputs

Inputs and outputs menu > Virtual inputs tab



Virtual inputs are inputs that are controlled via the browser interface or by a piece of software. They offer the same functionality as the other inputs in the system. The virtual inputs can be used to execute jobs in the video system, for example for alarm transmission or export video. There are 32 virtual inputs available.

1	Virtual inputs	Click the tab.
2	Type	Click the down arrow in the column and select whether a virtual input is to be configured or not.
		Input is to be used as virtual input.
		Input is not to be used as virtual input.
3	Name	Place the cursor in the column and enter the name.
4	Change field designator	Click the button. A dialog box opens. Edit the designation of the additional data as necessary.
5	Save	The entries are saved.

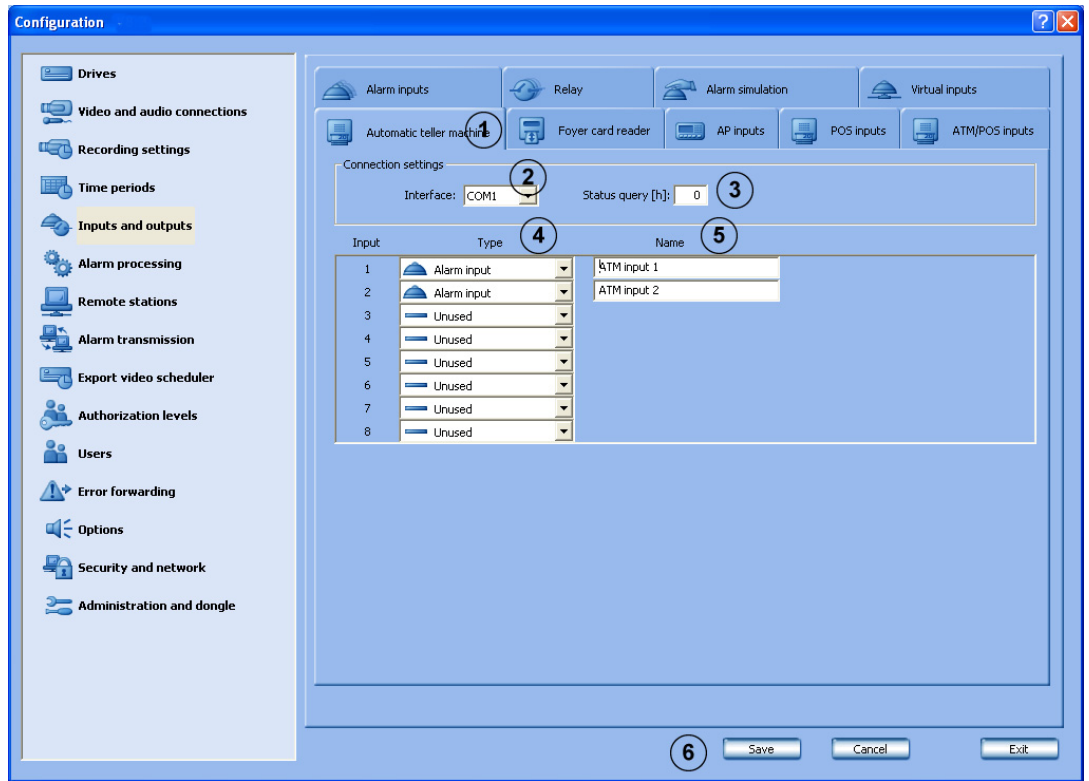


### NOTICE!



It is not necessary to log on to gain access to the virtual inputs interface.

### 6.5.5 Configuring Automatic Teller Machines

Inputs and outputs menu > Automatic teller machine tab



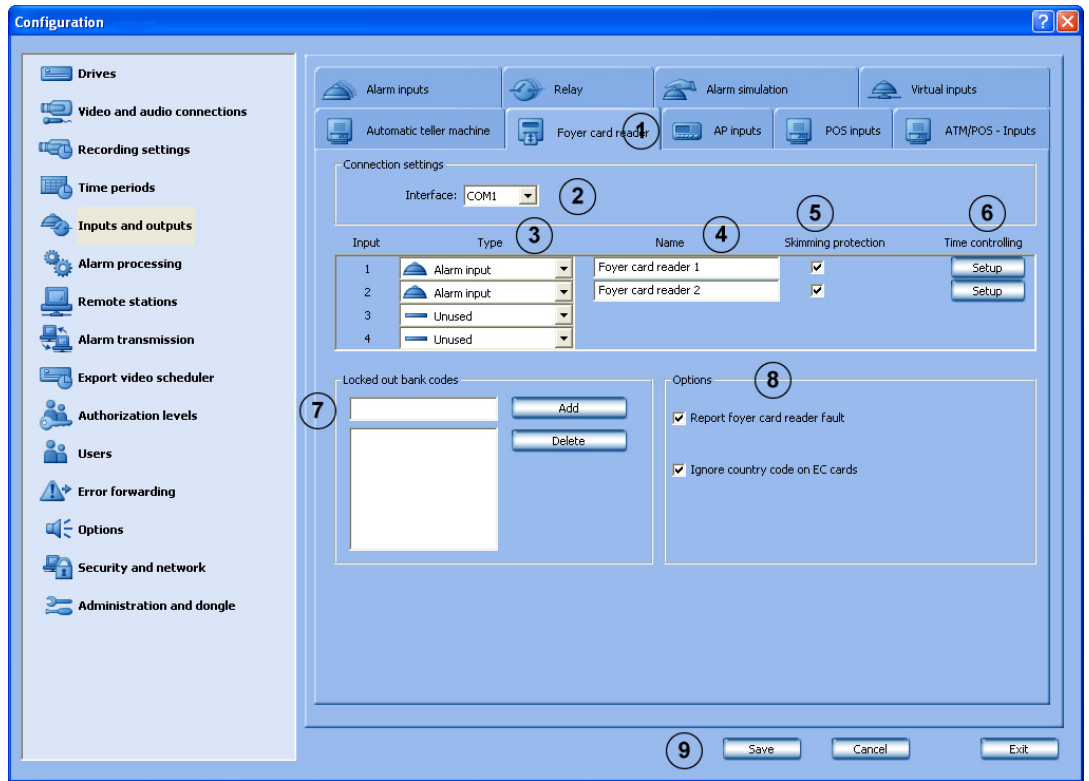
A maximum of 4 automatic teller machines, each with 2 inputs, can be connected to one video system.

1	Automatic teller machine	Click the tab.
2	Interface:	Select the interface.
3	Status query [h]:	After this time interval, the system checks repeatedly whether the connected automatic teller machines have completed a transaction. Enter the time in hours. Example: Entering 2 would mean that a check is run every 2 hours. Entering 0 would mean that no check is run. <b>Note:</b> If the system does not display a transaction, an error message is sent. If the connection between DiBos and the automatic teller machine is faulty, another error message is sent.
4	Type	Click the down arrow in the column and select whether an input is to be configured or not.
		The input is assessed.
		The input is not assessed.

		Assignment of inputs: Input 1 + 2 = Automatic teller machine 1 Input 3 + 4 = Automatic teller machine 2 Input 5 + 6 = Automatic teller machine 3 Input 7 + 8 = Automatic teller machine 4 Inputs 1, 3, 5, 7 normally activate the portrait camera and inputs 2, 4, 6, 8 the cash dispenser camera.
5	Name	Place the cursor in the column and enter the name. The name can be freely selected.
6	Save	The entries are saved.

## 6.5.6 Configuring Foyer Card Readers

Inputs and outputs menu > Foyer card reader tab



A maximum of 4 foyer card readers can be connected to one video system. Each foyer card reader uses one input. Anti-skimming is possible on the foyer card reader.



**NOTICE!**

You may not configure more foyer card readers than the number connected.

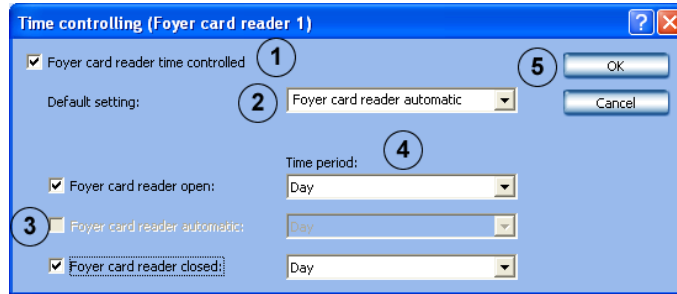
1	Foyer card reader	Click the tab.
2	Interface:	Select the interface.
3	Type	Click the down arrow in the column and select whether an input is to be configured or not.
		A foyer card reader is connected to the input.
		No foyer card reader is connected to the input.
4	Name	Place the cursor in the column and enter the name. The name can be freely selected.

5	Skimming protection	<p>This function recognizes whether there are any alien objects on the foyer card reader that may be able to read the data from an EC card without authorization.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>– If this function is activated, the skimming input is available as a trigger.</li> <li>– If anything triggers this, the event is recorded in the logbook.</li> <li>– If the <b>Report foyer card reader fault</b> function is also activated, a message appears in the user interface when a trigger is activated.</li> </ul>
6	Time management - Setup	<p>Click the button if you want to enter a time control. A dialog box opens, allowing you to select the default setting for the foyer card reader (open, automatic, closed) and the time period (see also <i>Section Configuring foyer card reader time control</i>).</p>
7	Locked out bank codes	<p>You have the possibility of locking out specific bank sort codes, i.e. the EC cards with the lock characteristics entered here do not have access authorization. Access is denied by the foyer card reader. The default setting of the foyer card reader must be set to <b>Foyer card reader automatic</b>.</p>
	Add	<p>Enter the bank sort code to be locked into the text field and click the button. After the entry, the bank sort code is held in the list field.</p> <p><b>Note:</b></p> <p>When making an entry, the use of wild cards (? or *) in any combination is allowed.</p> <p>?: The exact position of the question mark may indicate any or no character.</p> <p>*: The exact position of the asterisk may indicate a sequence (one or more characters) of any or no characters (exception:</p> <p>* on its own means that all bank sort codes are locked out).</p>
	Delete	<p>Select the entry in the list field and click the button. The bank sort code is deleted from the list field.</p>
8	Report foyer card reader fault	<p>A message is displayed in the user interface if there is a fault in the foyer card reader. If the <b>Skimming protection</b> function is activated, a message also appears in the event of a skimming alarm.</p> <p><b>Note:</b></p> <p>If anything triggers this, the event is recorded in the logbook.</p>
	Ignore country code on EC cards	<p>Does not analyze credit card data used to identify which country a card is from. Access is possible for cards with a different country code.</p>
9	Save	<p>The entries are saved.</p>



### Configuring foyer card reader time control

**Inputs and outputs** menu > **Foyer card reader** tab > **Setup** button  
(see also *Section 6.5.6 Configuring Foyer Card Readers*)

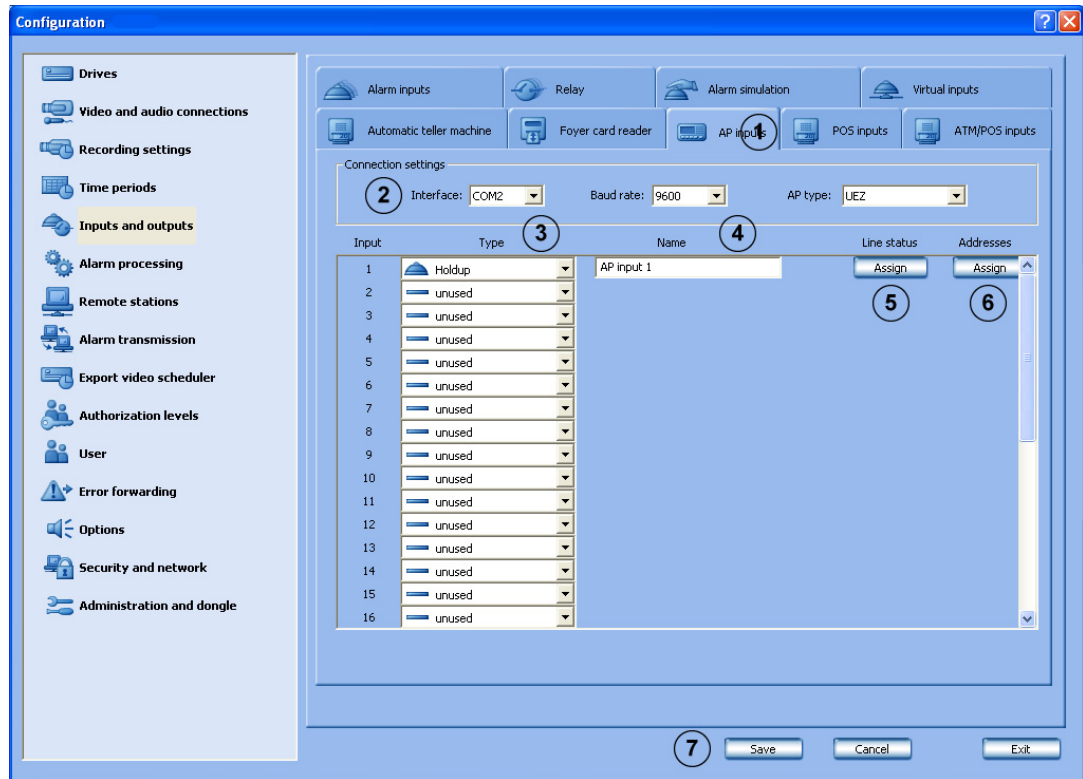


Make the settings for time control.

1	Foyer card reader time controlled	Activate the check box.
2	Default setting:	Click the down arrow in the list field and select which default setting the foyer card reader should have.
3		In the previous point, you specified the default setting for the foyer card reader. If the default setting is to be limited in time, activate one or more of the following characteristics, as required.
	Foyer card reader open:	Foyer always open.
	Foyer card reader automatic:	Access is only possible with an EC card or a credit card. EC cards from specific banks can be locked out.
	Foyer card reader closed	Foyer always closed.
4	Time period:	Select the time period within which the time limitation should apply (see also <i>Section 6.4 Configuring Time Periods</i> ).
5	OK	The entries are saved.



## 6.5.7 Configuring AP Inputs

Inputs and outputs menu > AP inputs tab



If an AP is connected serially, a maximum of 32 inputs that can cause triggering of an alarm in the system can be specified.

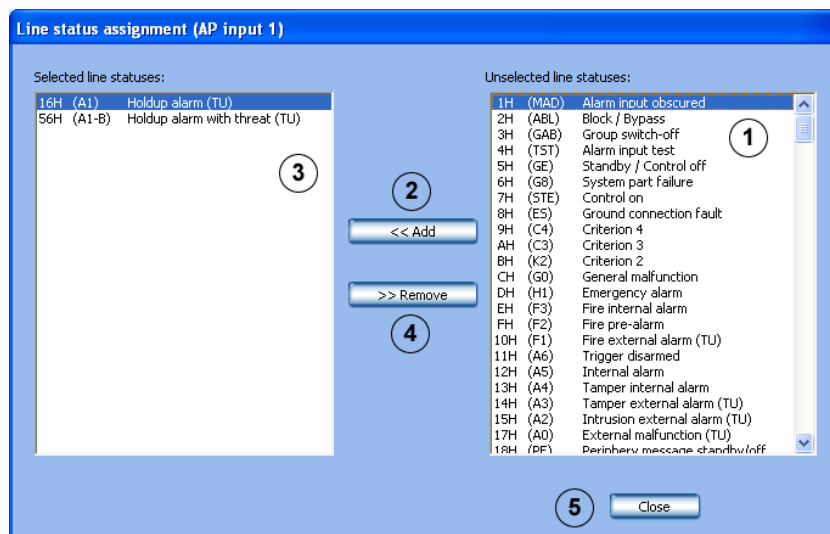
As standard, every input has line statuses assigned that can be modified in LSN alarm panels for the specific project. In addition, AP addresses can be assigned to each input.

1	AP inputs	Click the tab.
2	Connection settings	
	Interface:	Select the interface.
	Baud rate:	Select the Baud rate.
	AP type:	Select the AP type.
3	Type	Click the down arrow in the column and select the type of input.
		The input type, e.g. holdup, is activated.
		The input type is not activated.
		<b>Note:</b> Each input has specific types of line statuses assigned as standard. This assignment can be changed for LSN alarm panels.
4	Name	Place the cursor in the column and enter the name.

5	Line status - Assign	Click the button. A dialog box opens, allowing you to view and edit the default assignment of the line statuses (see also <i>Section Assigning AP line statuses to inputs (not for Bosch G Series)</i> ). <b>Note:</b> Only possible for LSN alarm panels.
6	Addresses - Assign	Click the button. A dialog box opens, allowing you to assign specific AP addresses to the input (see also <i>Section Assigning AP addresses to inputs (not for Bosch G Series)</i> and <i>Section Assigning AP addresses (Bosch G Series) to inputs</i> ).
7	Save	The entries are saved.

**Assigning AP line statuses to inputs (not for Bosch G Series)**

**Inputs and outputs** menu > **AP inputs** tab > **Line status** section > **Assign** button  
(see also *Section 6.5.7 Configuring AP Inputs*)



Assign AP line statuses to the inputs.

**Adding line statuses**

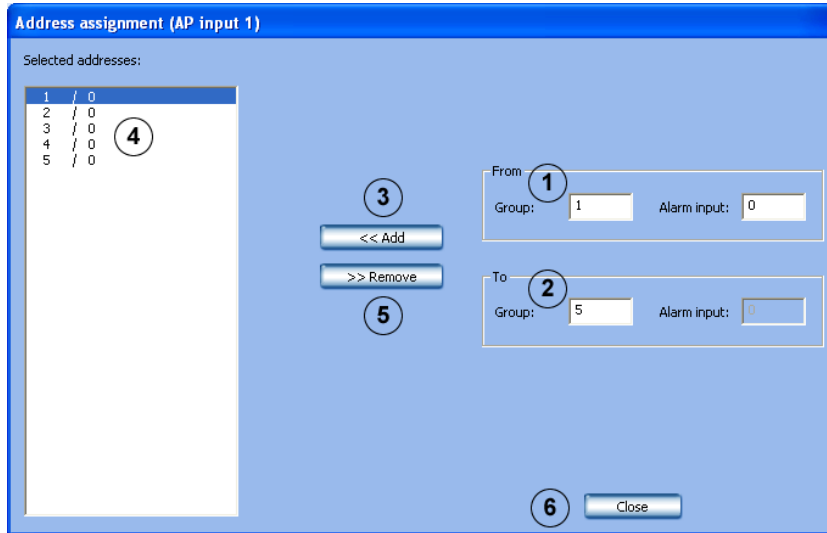
1	Unselected line statuses:	Select the line status.
2	Add	Click the button. The line status is added to the <b>Selected line statuses:</b> list field.
5	Close	Finishes the procedure. Saves the entries.

**Removing line statuses**

3	Selected line statuses:	Select the line status.
4	Remove	Click the button. The line status is removed from the <b>Selected line statuses:</b> list field.
5	Close	Finishes the procedure. Saves the entries.

### Assigning AP addresses to inputs (not for Bosch G Series)

**Inputs and outputs** menu > **AP inputs** tab > **Addresses** section > **Assign** button  
(see also *Section 6.5.7 Configuring AP Inputs*)



Assign AP addresses (not Bosch G series) to the inputs.

#### Adding addresses

1	From	
	Group: Alarm input:	Enter the starting address in the input fields.
2	To	
	Group: Alarm input:	Enter the final address in the input fields.
3	Add	Click the button. The addresses are added to the <b>Selected addresses:</b> list field.
6	Close	Finishes the procedure. Saves the entries.

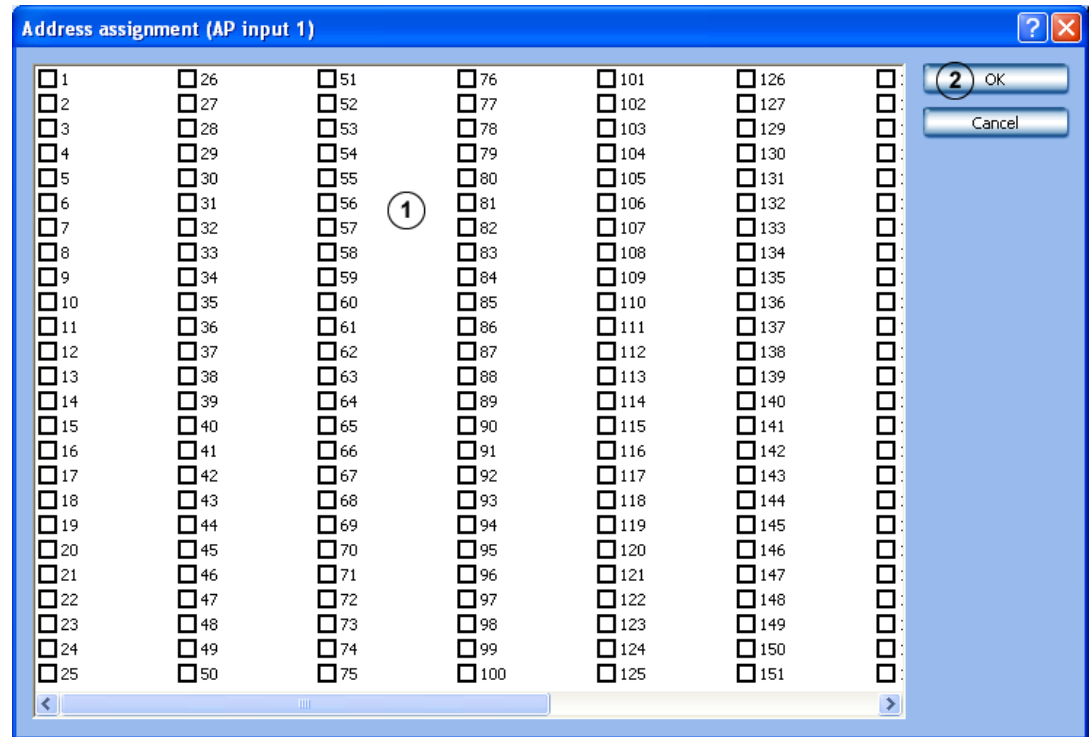
#### Removing addresses

4	Selected addresses:	Select the addresses you wish to remove.
5	Remove	Click the button. The addresses are removed from the <b>Selected addresses:</b> list field.
6	Close	Finishes the procedure. Saves the entries.

### Assigning AP addresses (Bosch G Series) to inputs

**Inputs and outputs** menu > **AP inputs** tab > **Addresses** section > **Assign** button

(see also *Section 6.5.7 Configuring AP Inputs*)

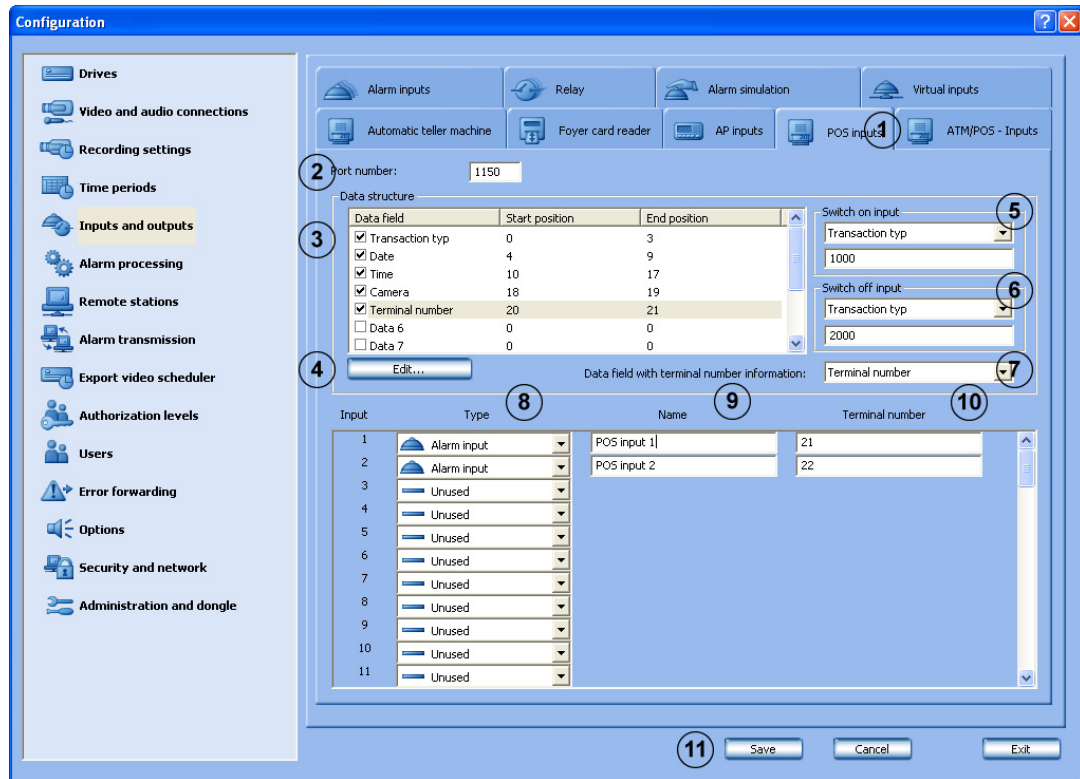


Assign AP addresses for Bosch G series to the inputs.

1	AP addresses	Activate the check boxes of the AP addresses you wish to assign to the input.
2	OK	The entries are saved.

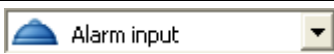

## 6.5.8 Configuring POS Inputs

### Inputs and outputs menu > POS inputs tab



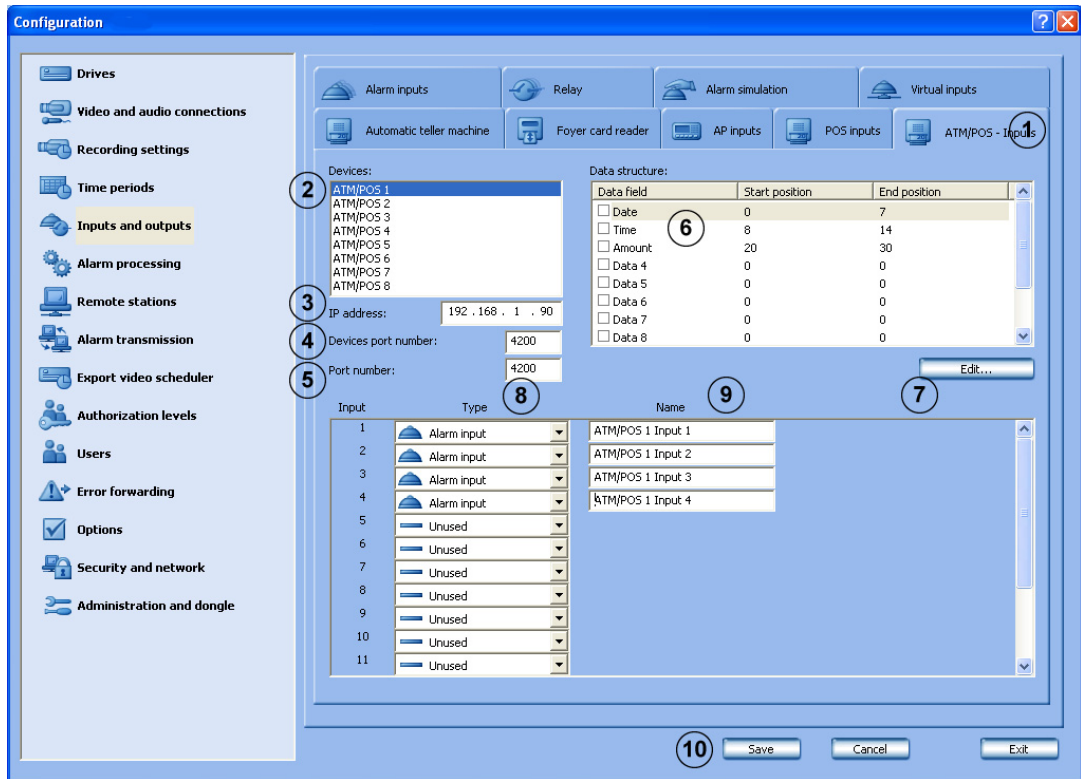
A POSserver (POS= point of sale) is connected via the IP network (LAN). To do this, the DiBos IP address must be configured in the POS server. A maximum of 64 virtual inputs are available in DiBos. When activating defined transactions at the POS points, an image is automatically recorded.

1	POS inputs	Click the tab.
2	Port number:	Enter the DiBos port number to which the IP server sends the data. <b>Note:</b> The port number in the DiBos configuration must match the port number that has been entered in the POS server.
3	Data structure:	Shows the structure of the data stream that is sent to DiBos by the POS server. It is possible to have a maximum of 10 data fields as distinguishing factors. A maximum of 100 characters are possible per data field.
4	Edit	Click the button. A dialog box opens in which you can configure the type of data field and the corresponding start and end position in the data stream. <b>Note:</b> Mark in advance the rows to be processed under <b>Data structure</b> .

5	Switch on input	Click the arrow. The list of available data fields will be displayed. The list contains all data fields that are displayed under <b>Data structure</b> . Select the name of the data field and, in the text field underneath, enter the value that triggers an image recording in the data stream of the POS server. Where there are several values, these must be separated by semi-colons.
6	Switch off input	Click the arrow. The list of available data fields will be displayed. Select the name of the data field and, in the text field underneath, enter the value that ends an image recording in the data stream of the POS server. Where there are several values, these must be separated by semi-colons.
7	Data field with terminal number information:	Click the arrow. The list of available data fields will be displayed. Select the name of the data field which describes the terminal number (e.g. cashpoint number).
8	Type	Click the down arrow in the column and select whether an input is to be activated or not.
		Input should be used to trigger image recording.
		Input should not be used to trigger image recording.
9	Name	Place the cursor in the column and enter the name of the input.
10	Terminal number	Enter the terminal number to which the POS input is allocated on DiBos.
11	Save	The entries are saved.

## 6.5.9 Configuring ATM/POS Inputs



Inputs and outputs menu > ATM/POS- Inputs tab



The ATM/POS-Bridge is used to connect cashpoint systems and ATMs. The video system can be connected to a maximum of 8 ATM/POS-Bridges, each with 4 ATMs. The video is connected via the IP network (LAN).

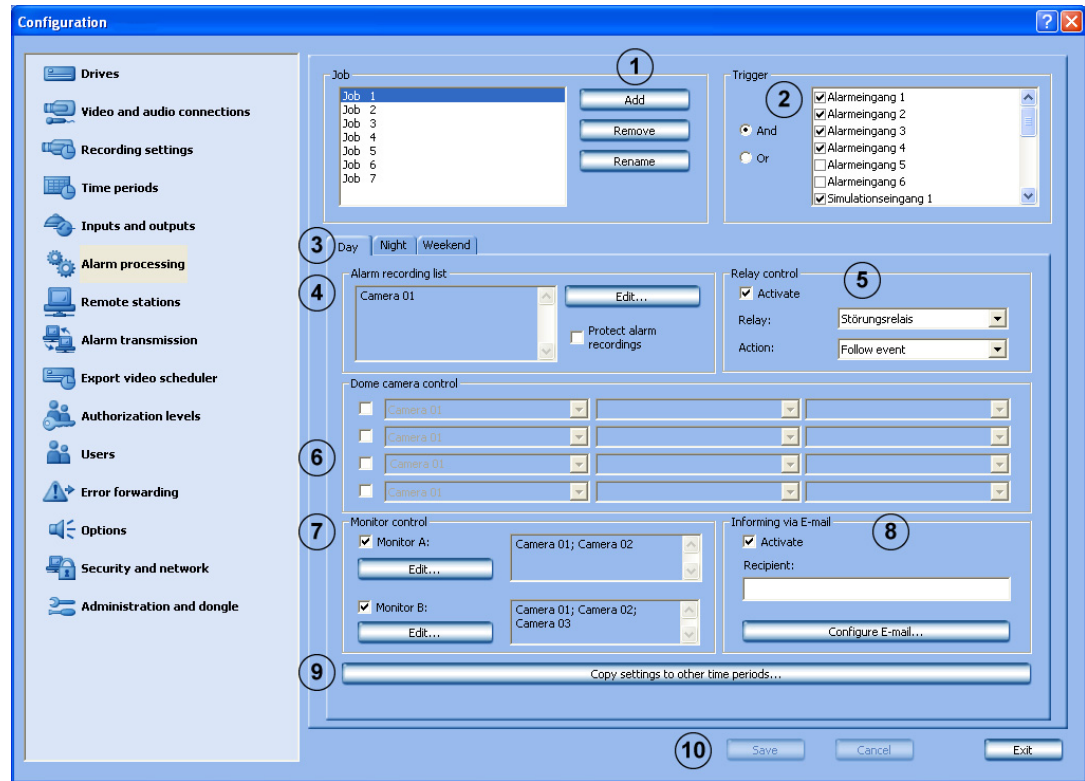
1	ATM/POS inputs	Click the tab.
2	Devices:	Select the device.
3	IP address:	Enter the IP address of the ATM/POS-Bridge.
4	Devices port number:	Enter the port number of the ATM/POS-Bridge.
5	Port number:	Enter the DiBos port number.
6	Data structure:	Shows the structure of the data stream that is sent to DiBos by the ATM/POS-Bridge. It is possible to have a maximum of 10 data fields as distinguishing factors. The size of the data stream is limited to 7 kilobytes. <b>Note:</b> Each of the individual data fields can be activated by selecting the relevant check box. If none of the check boxes are selected, the entire data stream is written in the first data field.
7	Edit	Click the button. A dialog box opens in which you can configure the type of data field and the corresponding start and end position in the data stream. <b>Note:</b> Mark in advance the rows to be processed under <b>Data structure</b> .



8	Type	<p>Click the down arrow in the column and select whether an input is to be activated or not.</p> <p><b>Note:</b>          Input 1 = ATM/Pos device 1          Input 2 = ATM/Pos device 2          Input 3 = ATM/Pos device 3          Input 4 = ATM/Pos device 4</p>
		Input should be used to trigger image recording.
		Input should not be used to trigger image recording.
9	Name	<p>Place the cursor in the column and enter the name of the input.</p> <p>Note:</p>
10	Save	The entries are saved.

## 6.6 Configuring Alarm Processing

### Alarm processing menu



In this dialog box you can specify jobs for every time profile. Jobs are activities that are started by inputs and cameras with motion detection.

The following actions are possible:

- Starting an alarm recording
- Controlling a relay output
- Controlling a maximum of four dome cameras and pan/tilt cameras
- Controlling camera sequences for a maximum of two video monitors
- Informing via E-mail

1	Job	
	Add	Adds a new job. The name of the new job is sequentially numbered and can be renamed.
	Remove	Removes a job. To do so, select the job.
	Rename	The name of the job can be changed. To do so, select the job.
2	Trigger	In the list field, select the inputs or cameras with motion detection whose triggering starts the job. The following are displayed as triggers: <ul style="list-style-type: none"> <li>– All types of inputs</li> <li>– Cameras with activated motion detection or activated tamper detection</li> <li>– JPEG IP cameras and MPEG4 IP cameras with motion detection</li> <li>– Skimming protection of foyer card reader</li> </ul>

	And	All selected inputs and cameras with motion detection must trigger in order to start the job.
	Or	Only one input or one camera with motion detection must trigger in order to start the job.
3	Day   Night   Weekend ...	Select the time profile. The job is assigned to this time profile. <b>Note:</b> Only the time profiles configured under <b>Time periods</b> are displayed. <b>Note:</b> With the <b>Copy settings to other time periods...</b> button, it is possible to quickly copy jobs to other time periods.
4	Alarm recording list	The inputs or cameras selected under <b>Trigger</b> trigger an alarm recording for locally connected cameras.
	Edit...	Click the button. A dialog box opens. Select the cameras for which alarm recording should take place.
	Protect alarm recordings	Activate the check box. The alarm recordings are protected against overwriting (including pre-alarm images). <b>Note:</b> Protected data will only be automatically deleted after a specified number of days if the <b>Delete old video</b> and <b>Delete protected data</b> options are activated under <b>Recording settings</b> . It is also possible to manually delete data via the user interface.
5	Relay control	Specify the relay that is to be controlled.
	Activate	Activates the relay to be controlled.
	Relay:	Select the relay to be controlled.
	Action:	Select the relay behavior. Relay behavior: <ul style="list-style-type: none"> <li>- <b>Start of event:</b> At the start of an event the relay switches for one second.</li> <li>- <b>End of event:</b> At the end of an event the relay switches for one second.</li> <li>- <b>Follow event:</b> The relay switches at the beginning of the event, maintains this status during the event and returns to its original status at the end of the event.</li> <li>- <b>Follow recording:</b> The relay switches at the start of the event and only returns to its original status after the end of alarm recording (including the post-alarm time).</li> </ul>

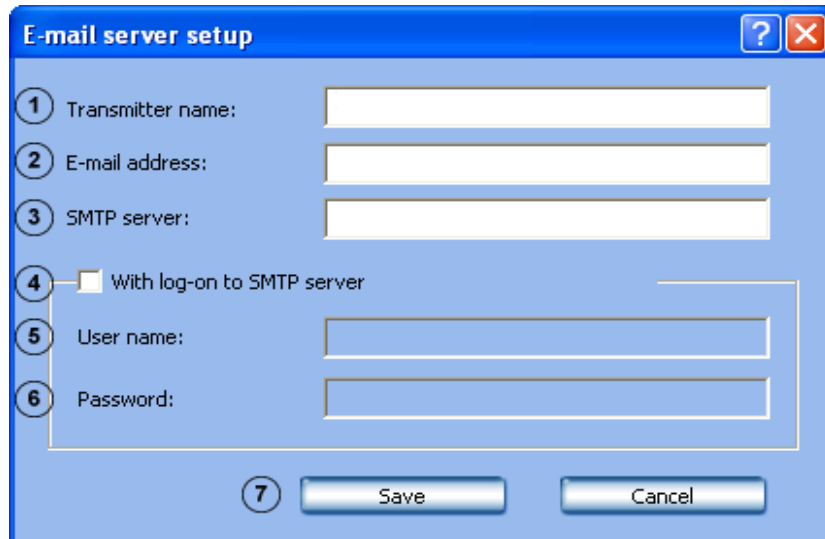
6	Dome camera control	<p>A job can control a maximum of 4 dome cameras and pan/tilt cameras.</p> <p>Activate the check box of the line concerned. Then select the camera to be controlled in the list field and a preposition or a command.</p> <p><b>Note:</b> Only different dome cameras and pan/tilt cameras can be controlled. The saved positions and commands must be configured under <b>Video and audio connections</b> → <b>Add/Modify camera</b> → <b>Dome settings</b>.</p>
7	Monitor control	Once a job has been triggered, an alarm sequence can be displayed on monitor A/monitor B.
	Monitor A / Monitor B	Activate the check box. The cameras are displayed on the monitor.
	Edit	Click the button. A dialog box opens. Select the cameras and the display duration.
8	Informing via E-mail	Once a job has been triggered, a notification e-mail can be sent.
	Activate	Activates the e-mail notification.
	Recipient:	<p>Enter the e-mail address of the recipient.</p> <p><b>Note:</b> Where there are several e-mail addresses, these must be separated by semi-colons.</p>
	Configure E-mail	The e-mail server setup opens after the button is clicked. During setup, enter data on the transmitter name, e-mail address, user name etc.
9	Copy settings to other time periods...	<p>Copies the selected job with all the settings it contains to other time periods.</p> <p>Select a job and click the button. A dialog box opens where you can select the time periods.</p>
10	Save	The entries are saved.

**Configuring the e-mail server setup**

**Alarm processing** menu > **Configure E-mail...** button

or

**Error forwarding** menu > **E-mail server** button



E-mails can be sent regardless of whether or not you log on to the SMTP server.

1	Transmitter name:	Enter the name of the sender. The name appears as the sender name for the e-mail recipient.
2	E-mail address:	Enter the e-mail address of the sender.
3	SMTP server:	Enter the name or the IP address of the SMTP servers (e-mail server).
4	With log-on to SMTP server	E-mails can only be sent when the sender is authorized to do so. The SMTP server checks the sender's authorization in this case.
5	User name:	Enter the user name for logging on to the SMTP server.
6	Password:	Enter the password for logging on to the SMTP server. Password transmission is encrypted.
7	Save	The entries are saved.

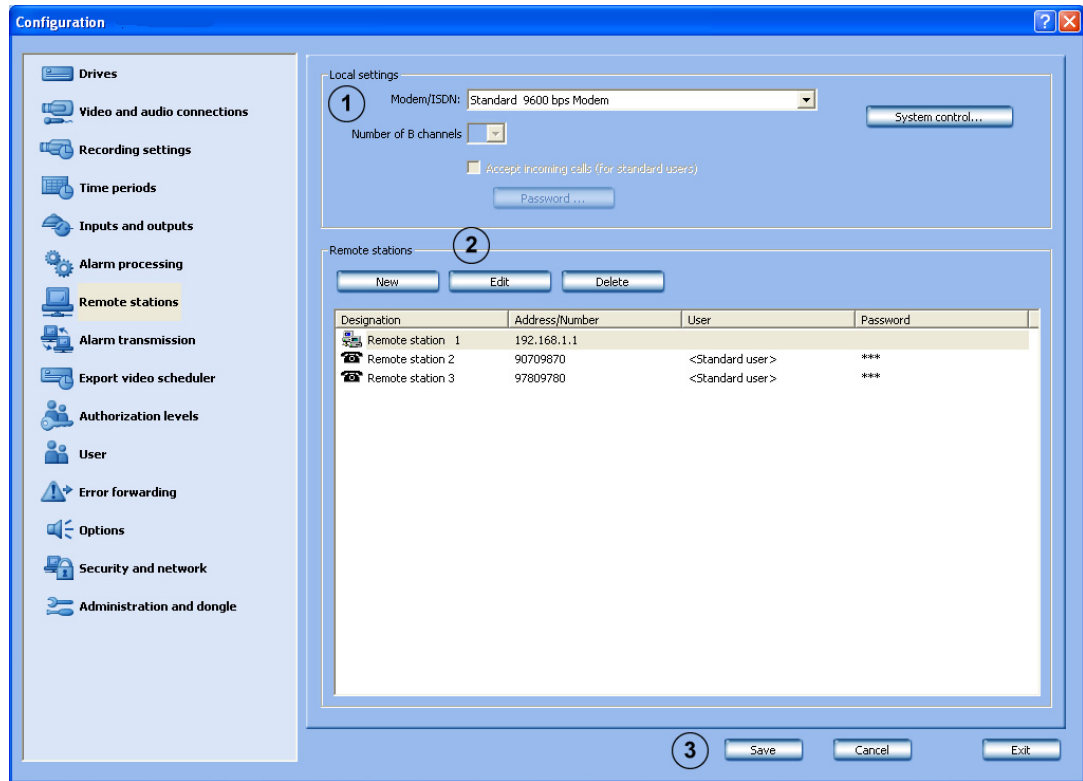
**NOTICE!**



- For information on how to add an e-mail recipient for alarm processing, see *Section 6.6 Configuring Alarm Processing*
- For information on how to add an e-mail recipient for error forwarding, see *Section Adding a recipient/editing recipient data, page 110*

## 6.7 Configuring Remote Stations

### Remote stations menu



In this dialog box, you determine the remote stations for your own workstation (local computer) so that you can connect to these remote stations later in the configuration procedure.

1	Local settings	Edit the following settings for your own workstation.
	Modem/ISDN:	Select the modem or ISDN card. <b>Note:</b> To configure a modem connection, an RAS-capable modem must be connected and an RAS service installed.
	Number of B channels	Enter the number of B channels.
	Accept incoming calls (for standard users)	Incoming calls may be accepted by standard users.
	Password...	Enter the password that allows remote stations to be dialed into.
	System control...	Under Windows XP, opens Network Connections in the Control Panel. <b>Note:</b> Here you can configure your own IP address or make firewall settings, for example.
	Info	If no RAS-capable modem is connected or no RAS service is installed, a notes icon and a button with additional information appears.

2	Remote stations	New remote stations can be added here. Existing remote stations are displayed in the list field. <b>Note:</b> If the remote stations are configured to do so, the <b>Low bandwidth</b> column is also displayed in the list field.
	New	Creates a new remote station. Input your entries in the dialog box that opens.
	Edit	Data on existing remote stations can be edited. Select the remote station from the overview in the lower part of the dialog box and click the button.
	Delete	Deletes the connection to a remote station. Select the remote stations in the overview in the lower part of the dialog box that you want to delete and click the button.
3	Save	The entries are saved.

## Adding/processing remote stations

**Remote stations** menu > **New** button

In this dialog box, you determine remote station settings that enable connections to this remote station to be established. Connection is possible via modem/ISDN and network.

1	Designation	Enter a name for the remote station.
	Number/Address	<b>For a modem/ISDN:</b> Enter the complete telephone number of the remote station. If your own workstation is connected to a PBX, you must enter a prefix (in most cases 0) before entering the remote station number. <b>For a network:</b> Enter the remote station IP address or the computer name.
	Modem/ISDN	Connect the remote station via a modem or ISDN.
	Low bandwidth (live mode)	In live mode, only every 30th image is displayed.
2	Windows user account	Make the Windows user account settings for modem/ISDN transmission.
	User:	If required, enter the user here. In the default settings, a user has already been created.
	Change password	The password can be changed as necessary. The password must match that of the remote station.
	Reset user account	Resets the user account.
	OK	The entries are saved.



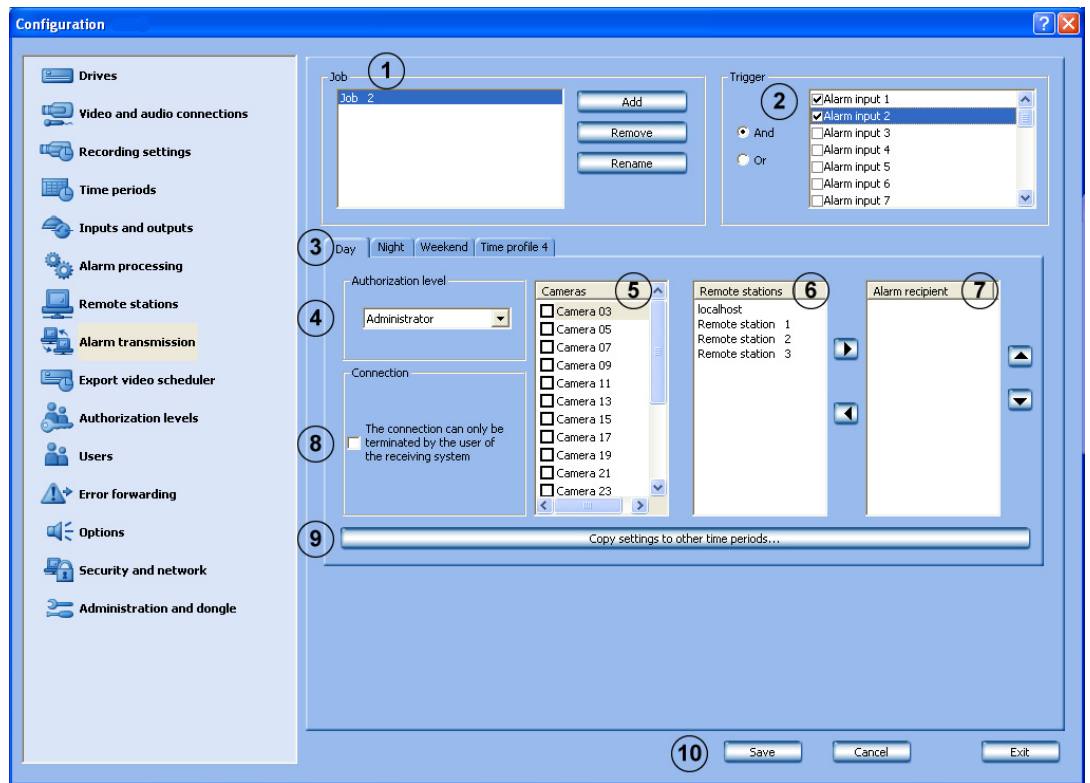
### NOTICE!

To configure a modem connection, an RAS-capable modem must be connected and an RAS service installed. If no RAS-capable modem is connected or no RAS service is installed, a notes icon and a button with additional information appears.



## 6.8 Configuring Alarm Transmission


### Alarm transmission menu




In this dialog box you can specify jobs for alarm transmissions. Jobs are activities that are started by inputs and cameras with motion detection.



In the event of an alarm, a connection is established from the station generating the alarm to the configured remote station.



In the remote station live image, the  tab blinks red. The remote station generating the alarm is displayed by clicking the tab. Clicking the remote station shows the cameras that have been triggered.

1	Job	
	Add	Adds a new job. The name of the new job is sequentially numbered and can be renamed.
	Remove	Removes a job. To do so, select the job.
	Rename	The name of the job can be changed. To do so, select the job.

2	Trigger	<p>In the list field, select the inputs or cameras with motion detection whose triggering starts the job.</p> <p>The following are displayed as triggers:</p> <ul style="list-style-type: none"> <li>– All types of inputs</li> <li>– Cameras with activated motion detection or activated tamper detection</li> <li>– JPEG IP cameras and MPEG4 IP cameras with motion detection</li> <li>– Skimming protection of foyer card reader</li> </ul> <p><b>Note:</b></p> <p>The triggers for cameras with motion detection are only displayed after the camera has been configured (see <i>Section 6.2.3 Specifying Monitoring Zone for Motion Cameras</i>, <i>Section 6.2.8 Configuring JPEG IP Cameras</i> and <i>Section 6.2.9 Configuring MPEG4 IP Cameras</i>)</p>
	And	All selected inputs and cameras with motion detection must trigger in order to start the job.
	Or	Only one input or one camera with motion detection must trigger in order to start the job.
3	Day   Night   Weekend ...	<p>Select the time profile. The job is assigned to this time profile.</p> <p><b>Note:</b></p> <p>Only the time profiles configured under <b>Time periods</b> are displayed.</p>
4	Authorization level	<p>Select the authorization level.</p> <p><b>Note:</b></p> <p>The name of the authorization level and its connection password must match in the local station and in the remote station to which the alarm is transmitted. However, the individual enabling of authorization levels, for example enabled cameras, relays etc., may be different. Enabling of the authorization level in the remote station takes place when dialing into that remote station.</p> <p>Authorization for alarm transmission must be activated in the <b>Authorization levels</b> menu.</p>
5	Cameras	Select the cameras whose images you want to transmit to the remote station.
6	Remote stations	<p>The list field contains all remote stations known in the system.</p> <p>Select the remote station and, if necessary, one or more replacement remote stations to which the alarm is to be transmitted and click . The remote station is added to the <b>Alarm recipient</b> list field.</p>

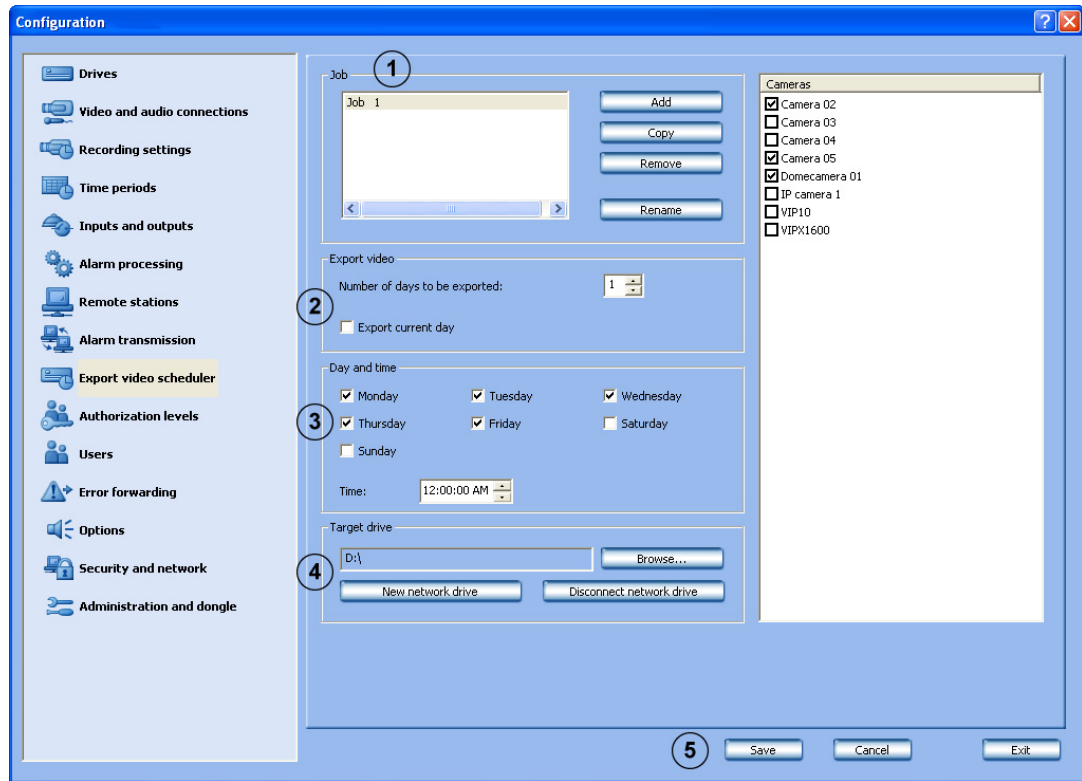
7	Alarm recipient	<p>The list field contains the remote stations to which an alarm transmission is to be made.</p> <p><b>Note:</b></p> <p>The remote stations to be called are worked through by the system from top to bottom. This means that the remote station to be dialed first must be at the top of the list. The alternative remote stations to be dialed when no connection can be established to the first remote station are listed underneath. The sequence is specified with the  and  buttons.</p>
8	The connection can only be terminated by the user of the receiving system.	<p>Activate this check box when only the user of the receiving system is allowed to end the connection. Otherwise, the connection will last as long as the event does.</p>
9	Copy settings to other time periods...	<p>Copies the selected job with all the settings it contains to other time periods.</p> <p>Select a job and click the button. A dialog box opens where you can select the time periods.</p>
10	Save	The entries are saved.

**NOTICE!**

Multiple remote stations can be called up for one event. To do so, multiple jobs must be created.

## 6.9 Configuring the Export Video Scheduler

### Export video scheduler menu



In this dialog box you can specify jobs for the export video scheduler.

1	Job	
	Add	Adds a new job. The name of the new job is sequentially numbered and can be renamed.
	Copy	An existing job is copied. To do so, select the job.
	Remove	Removes a job. To do so, select the job.
	Rename	The name of the job can be changed. To do so, select the job. The name must not contain any special characters.
2	Export video	A maximum of 160 GB per day can be exported via a 1-gigabit network. This corresponds to the maximum recording capacity of 30 analog cameras. The following requirements must be adhered to during the export process: <ul style="list-style-type: none"> <li>– In live mode, no more than 16 cameras are displayed.</li> <li>– No search available in the database.</li> <li>– No playback of recorded images.</li> </ul>
	Number of days to be exported	Enter the number of past days to be exported.

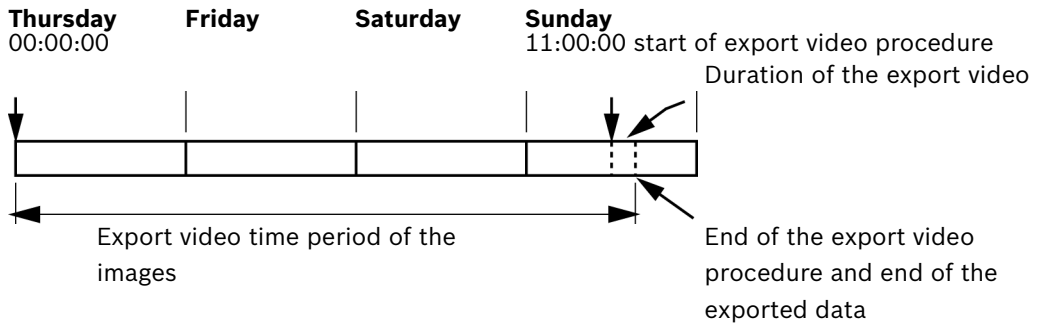
	Export current day	Activate this check box if the current day is to be exported. <b>Note:</b> Images from the current day are only exported up to the point in time at which the job is executed. Images from the current day that have not yet been saved are not exported.
3	Day and time	
	Monday.....Sunday	Select the days on which export video should be carried out.
	Time:	Enter the time for export video.
4	Hard disk	Select the target drive.
	Browse	Opens a dialog box for selecting the target drive.
	New network drive	Adds a new network drive.
	Disconnect network drive	Removes a network drive.
5	Save	The entries are saved.

**Examples of an export video scheduler**

The examples show the export video time period of the images.

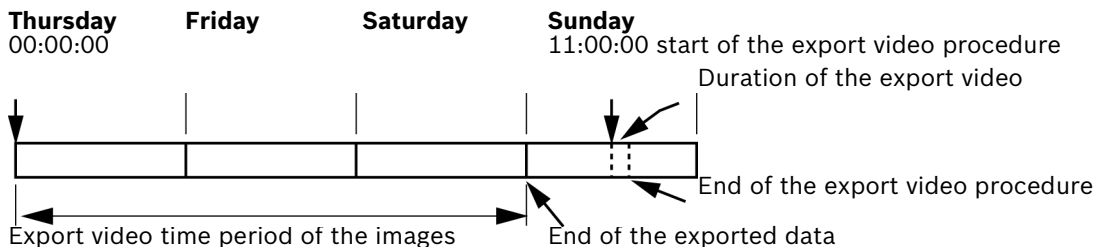
**Example 1:**

Number of days to be exported: 3  
 Export current day  
 Sunday  
 Time: 11:00:00 (= start of export video)  
 Corresponding export video time period:



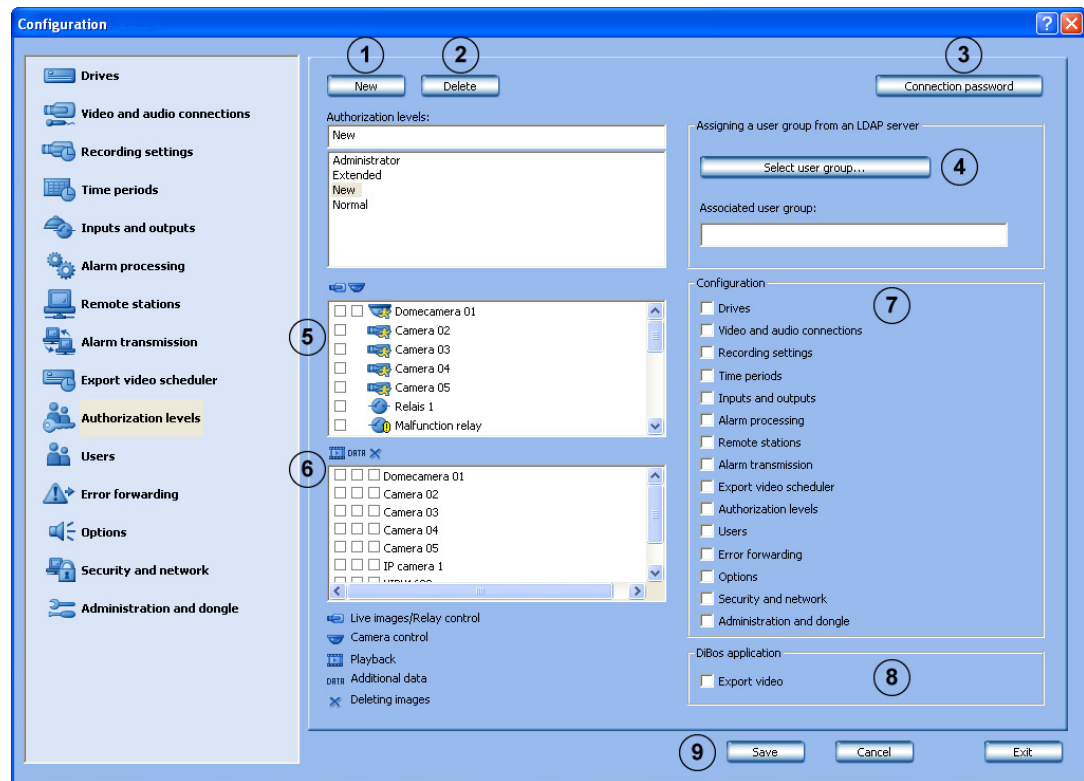
**Example 2:**

Number of days to be exported: 3  
 Export current day  
 Sunday  
 Time: 11:00:00 (= start of export video)  
 Corresponding export video time period:










## 6.10 Creating Authorization Levels

### Authorization levels menu



You can create different groups of authorizations in this menu if you have administrator rights. In these "authorization levels", you specify what the user can do in the system. The **Administrator** authorization level possesses all rights and is configured ex-factory. An **Extended user** may create a **Normal user**.

1	New	Creates a new authorization level. Click <b>New</b> and enter the name into the input field. <b>Note:</b> A user with the authorization level <b>Extended</b> may only create users who have the same or lower authorization than a user with the authorization level <b>Normal</b> .
2	Delete	Deletes an existing authorization level. Select an authorization level in the list field and click <b>Delete</b> . The authorization level is deleted.
3	Connection password	A dialog box opens after the button is clicked. The connection password is entered into this dialog box. <b>Note:</b> To establish a connection, the connection password must match that of the remote station.
4	Select user group	A dialog box opens after the button is clicked. An LDAP server user group must be selected. After this selection is confirmed, the user group (in the LDAP server) is assigned to the authorization level in DiBos. See also <i>Section Selecting LDAP server user group</i> .

5		<p>Activate the check boxes of elements (cameras, relays) that should be available to users with this authorization level. For dome cameras and pan/tilt cameras, a second column with check boxes is displayed.</p> <p>The check boxes in front of the elements mean:</p>  <p>In live mode, only those cameras and relays are shown to the user that have the check box activated.</p>  <p>In live mode, the user can only control those dome cameras and pan/tilt cameras with activated check boxes.</p> <p><b>Note:</b> Only video hardware that is already configured is offered by the video system. If new components are created, access to these by all access-authorized users must be configured afterwards.</p>
6		<p>Select the access rights for the authorization level by activating the check box.</p> <p>Here, the activated check boxes in front of the elements mean:</p>  <p>In playback mode, only those cameras are shown to the user that have the check box activated.</p>  <p>The saved images with additional data (e.g. date, time, ATM data) can be searched for, viewed, assessed, copied and printed out.</p>  <p>The saved images from the corresponding camera can be deleted.</p>
7	Configuration	Specifies which function in the DiBos configuration can be carried out by users with this authorization level. Activate the check box next to the function in question.
	Export video	<p>Allows users with this authorization level to export video images.</p> <p><b>Note:</b> For the three pre-defined authorization levels, the exportation of video images cannot be deactivated.</p>
8	DiBos application	Specifies which function in DiBos operation can be carried out by users with this authorization level. Activate the check box next to the function in question.
9	Save	The entries are saved.

### Selecting LDAP server user group

**Authorization levels** menu > **Select user group...** button

In networked DiBos systems, the use of LDAP (LDAP = Lightweight Directory Access Protocol) allows central information, such as user groups, passwords etc., to be called up from a server to be used in the DiBos system.

The advantage of this is as follows:

- Users available in the DiBos network only need to be configured once on the LDAP server, rather than on every DiBos.
- A user's authorization level can easily be changed by modifying the group association of the user. Group association is only changed on the LDAP server.
- It is only on the LDAP server that new users are added and previous users deleted.
- Local users are also available. They can continue to be created on each system.

Before you can make the settings below, the individual groups and their members have to be put on the LDAP server. These groups will then be assigned to the authorization levels in DiBos. The configuration of the LDAP server is normally undertaken by the IT administrator, not the DiBos administrator.

You will require the assistance of your IT administrator to make the following entries.



#### NOTICE!

All paths should be specified as accurately as possible. This makes it quicker to search the LDAP server. The length of the search depends on the size of the database and can take several minutes.

The screenshot shows the 'Select user group' dialog box with the following fields and controls:

- 1: LDAP server\* (text input)
- 2: Port\* (text input, value: 389)
- 3:  Activate encryption
- 4: LDAP basis for users\* (text input)
- 5: Filter for users\* (dropdown menu)
- 6: LDAP basis for groups\* (text input)
- 7: Filter for group members\* (dropdown menu)
- 8: User name (DN\*) (text input)
- 9: Password\* (text input)
- 10: Testing button
- 11: User name (text input)
- 12: Password (text input)
- 13: Testing button
- 14: Group (DN) (text input)
- 15: Testing button
- 16: Filter for groups (dropdown menu)
- 17: Search user groups button
- 18: existing user group (list box)
- 19: OK button

\*) Mandatory entries

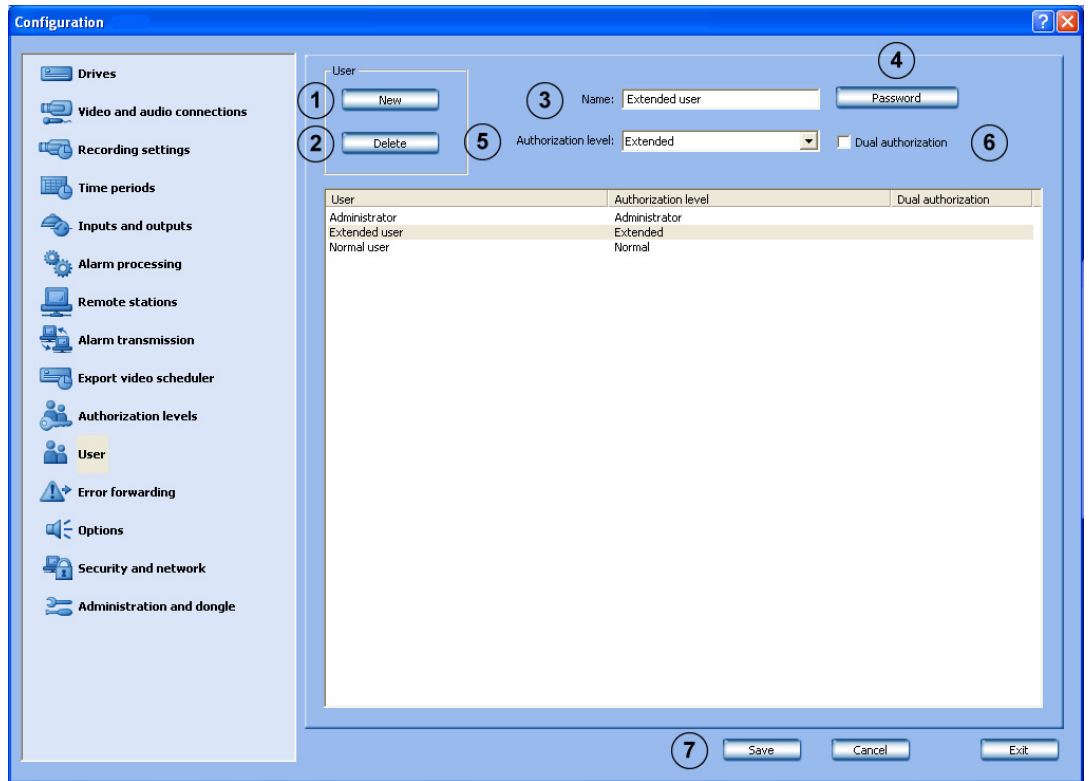


<b>LDAP server settings</b>		
1	LDAP server:	Name or IP address of the LDAP server.
2	Port	Port number of LDAP server (Default: unencrypted = 389; encrypted = 636)
3	Activate encryption	For encrypted data transmission.
4	LDAP basis for users:	Unique name (DN = distinguished name) of LDAP path in which the search for the user should be performed. <b>Example:</b> Ask your IT administrator for the unique name (DN) of the LDAP basis. For example, you receive the following DN: CN=Users,DC=Security,DC=MyCompany,DC=com
5	Filter for users:	Filter for searching for unique user name. <b>Example:</b> Ask your IT administrator for the filter to find a user with the user ID xy in the LDAP server. For example, for user xy, you receive the following filter: (!(sAMAccountName=xy)(userPrincipleName=xy) Replace xy with %username% and enter the filter.
6	LDAP basis for groups:	Unique name of LDAP path in which the search for groups should take place.
7	Filter for group members:	Filter used to search for group members of a group. <b>Example:</b> Ask your IT administrator for the filter to find user xy with his DN (e.g. CN=xy,CN=Users,DC=Security,DC=MyCompany,DC=com) in the LDAP server. For example, you receive the following path: (!(objectclass=group)(member=DN) Replace DN with %usernameDN% and enter the path.
<b>Proxy user</b>		
8	User name (DN):	Unique name of proxy user.
9	Password:	Proxy user password.
10	Testing	Tests whether the proxy user has access to the LDAP server.
<b>Test user authentication and group association</b>		
11	User name:	User login ID, e.g. userB. The DN should not be entered here.
12	Password:	User password.
13	Testing	Tests whether the user ID and password are correct.
14	Group (DN):	Unique group name. Used to check with which group the user is associated.
15	Testing	Tests the group association of the user.

	<b>Selection of user group</b>	
16	Filter for groups:	Filter for finding user groups. Ask your IT administrator for the filter to find the user group in the LDAP server. For example, you receive the following filter: (!(objectclass=group)(objectclass=groupofuniquenames)) Enter the filter.
17	Search user groups	After you have clicked it, all the user groups in the LDAP server that have the user as a member are searched.
18	existing user group:	The user groups are displayed in the list field. Select the user group you require.
19	OK	The user group will be saved in the <b>Authorization levels</b> dialog box.

## 6.11 Configuring Users

### User menu



To protect access to system components and data, operations can only be carried out by users who are logged on. Every user is assigned an authorization level for work that he has to carry out (see also *Section 6.10 Creating Authorization Levels*).



**NOTICE!**

The user with the "Administrator" authorization level must be protected with a password. Ensure that this password is only known to those persons who are responsible for this video system.

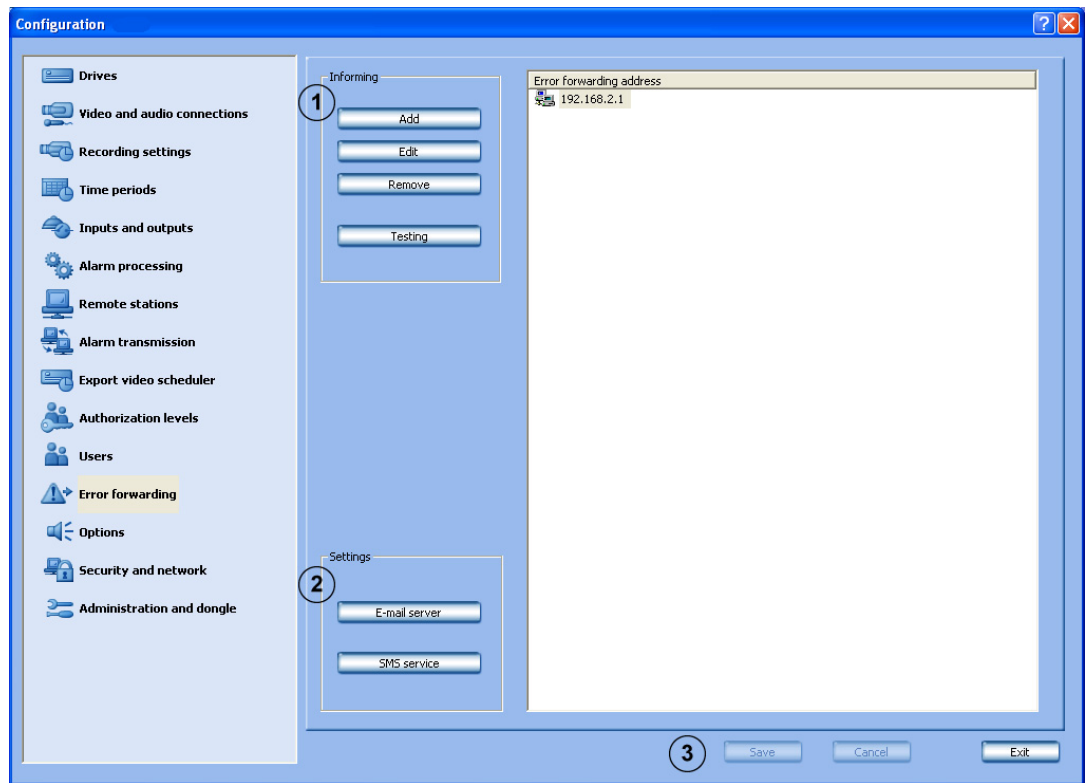
1	New	Creates a new user. Click <b>New</b> and enter a user name in the <b>Name</b> input field.
2	Delete	Deletes an existing user name. In the overview in the lower part of the dialog box, select the user name that you want to delete and click <b>Delete</b> .
3	Name:	Name of the user. You can either enter a new user name here or change an existing one.
4	Password	Click the button and enter a password for the user. Confirm your entries.
5	Authorization level:	Click the down arrow in the list field and select an authorization level for the user.
6	Dual authorization	Activate this function when the user may only log on to the system together with another user.
7	Save	The entries are saved.

**NOTICE!**

- An unlimited number of users can be created.
  - The user password only applies to the log-on procedure of a local user.
  - The administrator authorization can only be issued by administrators.
-

## 6.12 Configuring Error Forwarding

### Error forwarding menu



In case of malfunction, for example, external locations can be informed via network (= net send), SMS, e-mail or batch file. Error forwarding also applies to the malfunction relay.

1	Informing	Specify the locations to be informed here.
	Add	Opens a dialog box. You can add a new recipient who will be informed in case of malfunction. <b>Note:</b> The computer name must not contain any special characters. The recipient's messenger service must be started up.
	Edit	Opens a dialog box. Data on existing recipients can be edited. Select the recipient in the overview and click the button.
	Remove	An existing recipient can be removed from the list of those to be informed. Select the recipient in the right-hand part of the dialog box in the overview and click the button.
	Testing	Test the connection to the recipient. Select the recipient in the right-hand part of the dialog box in the overview and click the button.
2	Settings	Make the settings here for the e-mail server and the SMS service.
	E-mail server	The e-mail server setup opens after the button is clicked. During setup, enter data on the transmitter name, e-mail address, user name etc.

	SMS service	The SMS service configuration opens after the button is clicked. In the SMS configuration, enter data on the dialing parameters and modems, transmit options etc.
3	Save	The entries are saved.

The following events lead to error forwarding:

- The camera does not deliver a video signal
- The logbook cannot be created or written
- The images could not be recorded by the database server
- Database server could not be started
- Hard disk failure: Drive X deactivated, all drive X deactivated
- The hard disk is full (protected data)
- Internal database error
- Device could not be started
- Grabber card not working
- Export video scheduler error
- Reference image check failed

#### Adding a recipient/editing recipient data

**Error forwarding** menu > **Add** button or **Edit** button

Here you enter the recipient who is to be informed if problems arise.

#### Notification via the Network:

Transmission type	Click the down arrow and select the transmission type <b>Network</b> (= net send).
Computer name/IP address	Enter the computer name or IP address of the recipient. <b>Note:</b> The computer name must not contain any special characters. The recipient's messenger service must be started up.
OK	The entries are saved.

#### Notification via E-Mail:

Transmission type	Click the down arrow and select the transmission type <b>E-mail</b> .
E-mail address	Enter the e-mail address of the recipient.
OK	The entries are saved.

#### Notification via SMS:

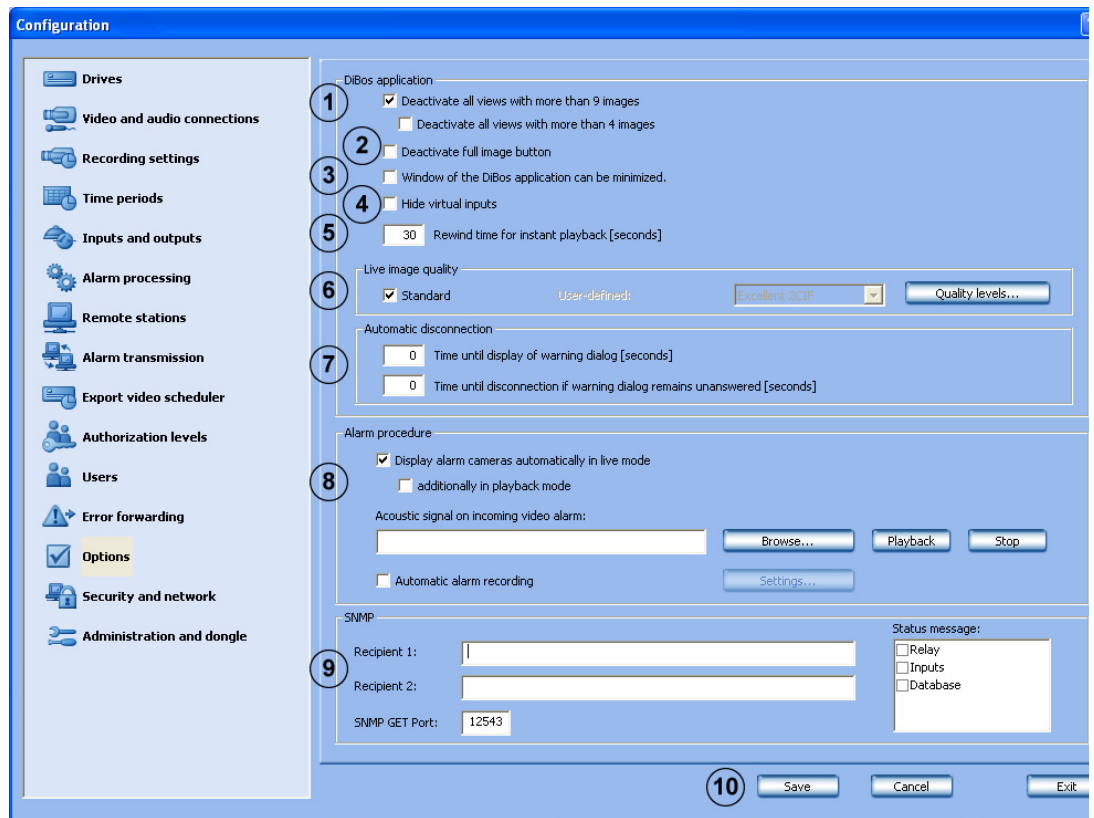
Transmission type	Click the down arrow and select the transmission type <b>SMS</b> .
Telephone number	Enter the telephone number of the recipient.
OK	The entries are saved.

#### Notification via Batch File:

Transmission type	Click the down arrow and select the transmission type <b>Batch file</b> .
Batch file	Enter the file name or click the adjacent button and select the file.
OK	The entries are saved.

# 6.13 Configuring Options

## Options menu



In this dialog box you can edit optional settings, for example automatic disconnection, instant playback and audible signals.

1	Deactivate all views with more than 9 images	Deactivates all buttons in DiBos Explorer that display more than 9 image windows.
	Deactivate all views with more than 4 images	Deactivates all buttons in DiBos Explorer that display more than 4 image windows.
2	Deactivate full image button	Deactivates the full image button in DiBos Explorer. This setting is useful if there is a touch screen, as depending on the model it may not be possible to return to full image mode.
3	Window of the DiBos application can be minimized.	Here you can select whether the user interface can be shrunk or not. Changes are first saved after a reboot of DiBos.
4	Hide virtual detectors	No longer displays virtual detectors in the user interface.
5	Rewind time for instant playback	Enter the time here. A time between 2 seconds and 300 seconds can be selected.  In Instant Playback, the images that have been saved in the selected camera are played back with a time delay to the live images. This means you will see the live image of the camera and the image of this camera from about 30 seconds ago. Playback is in real time.

6	Live image quality	Specifies the quality of the live image.
	Standard	Resets the live image quality to the default settings. <b>Note:</b> Live image default settings – CIF resolution – Quality level 4
	User-defined:	A live image quality can be selected.
	Quality levels	Opens a dialog box in which recording qualities can be displayed and edited or new recording qualities added.
7	Automatic disconnection	This function is used to disconnect the local live image and all ISDN and network connections (previously independently connected by the video system) automatically after a specific period of time.
	Time until display of warning dialog	Enter the time after which a warning dialog is to be displayed. <b>Note:</b> The warning dialog allows you to either maintain the connection or break it immediately.
	Time until disconnection if warning dialog remains unanswered	Enter the time after which disconnection is to take place if the warning dialog remains unanswered (a value of 0 means that no disconnection will take place).
8	Alarm procedure	Specifies how incoming alarms are displayed in live or playback mode.
	Display alarm cameras automatically in live mode	When incoming alarms are received in live mode, the cameras or remote stations in alarm status are listed in the device list. The images are displayed automatically.
	additionally in playback mode	When in playback mode, if there is an alarm input, the system switches to live mode. Cameras or remote stations in alarm status are listed in the device list. The images are displayed automatically.
	Acoustic signal on incoming video alarm:	Here you can assign an audio signal (wav file) to incoming video alarms. Enter the path and the file name or click <b>Browse</b> .
	Search	Click <b>Browse</b> and, in the window that opens, select the wav file you want to assign to the incoming video alarms. Click Open to save the file.
	Playback	If you want to listen to the audio signal, click <b>Playback</b> .
	Stop	Ends playback of the audio signal.
	Automatic alarm recording	Automatically displays all incoming alarms on the DiBos receiver. <b>Note:</b> The automatic alarm recording is displayed on the user interface.



	Settings	Click <b>Settings</b> and configure more precise details on automatic alarm recording. See also <i>Section 6.13.3 Configuring Automatic Alarm Recording</i>
9	SNMP	DiBos sends camera, relay, input and database status messages to an SNMP recipient via SNMP (Simple Network Management Protocol). See also <i>Section 6.13.1 MIB List for SNMP</i> and <i>Section 6.13.2 Notification via SNMP</i> <b>Note:</b> The option to send messages via relay, inputs and databases can be activated and deactivated. Camera messages cannot be deactivated.
	Recipient 1:	IP address or computer name of the 1st recipient.
	Recipient 2:	IP address or computer name of the 2nd recipient.
	SNMP GET Port:	Number of the port via which input, relay and camera statuses can be called up.
	Status message:	Displays the statuses that trigger an SNMP message. Select the corresponding check box to activate.
10	Save	The entries are saved.

### 6.13.1

### MIB List for SNMP

The MIB list (MIB = Management Information Base) shows the hierarchical structure of the object identifiers (OID) that are used to clearly identify individual objects.

<b>MIB DiBos 8.6</b>			
<b>Prefix = 1.3.6.1.4.1.5318.2501.1.1.8</b>			
<b>Text</b>	<b>Numeric</b>	<b>[Min - Max]</b>	<b>Values Cameras</b>
<b>Cameras</b>	.1		Camera_Ok = 0 Camera_Video_Loss = 1 Camera_Image_Check = 2 Camera_Too_Noisy = 4 Camera_Too_Dark = 8 Camera_Too_Bright = 16 Camera_Not_Present = 32
Grabber	.1 .x	[.1 - .30]	
IP	.2 .x	[.1 - 32]	
<b>InOutModules</b>	.2		
Alarm inputs (AI)	.1		<b>Values InOutModules</b>
Analog	.1 .x	[.1 - .16]	
IP	.2		Input_Off = 0
Camera	.x	[.1 - .32]	Input_On = 1
AI	.y	[.1 - .10]	Input_Error = 2
Virtual inputs	.2 .x	[.1 - .32]	Input_Not_Present = 3
Atm	.3 .x	[.1 - .8]	
Alarm panel	.4 .x	[.1 - .32]	
Foyer card reader	.5 .x	[.1 - .8]	
Relays	.6		<b>Values Database</b>
Analog	.1 .x	[.1 - .16]	DB_Ok = 0
IP	.2		DB_Drive_Disabled = 1
Camera	.x	[.1 - .32]	DB_Drive_Compressed = 2
Relay	.y	[.1 - .5]	DB_No_data_Drives = 3
Simulation input	.7 .x	[.1 - .4]	DB_Database_Error = 4
POS input	.8 .x	[.1 - .64]	DB_No_Diary = 5
ATM/POS input	.9 .x	[.1 - .128]	DB_Server_Overloaded = 6
			DB_Server_Recovered = 7
			DB_Write_Queue_Full = 8
			DB_Protected = 9
			DB_Disk_Full = 10
			DB_Undefined = 11
<b>Database</b>	.3		<b>Foyer card reader</b>
			1: Input of device 1
			2: Input of device 2
			3: Input of device 3
			4: Input of device 4
			5: Skimming-Input of device 1
			6: Skimming-Input of device 2
			7: Skimming-Input of device 3
			8: Skimming-Input of device 4

### 6.13.2

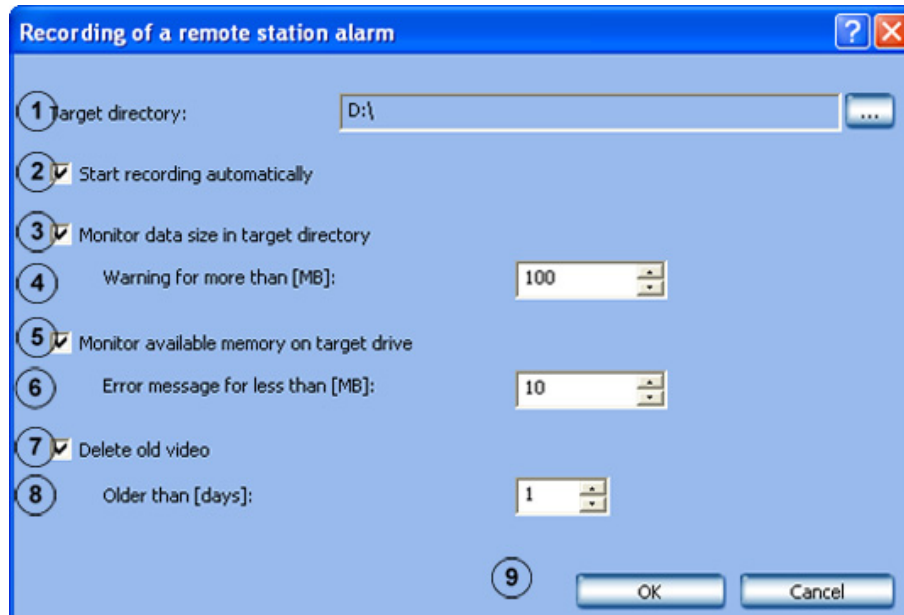
#### Notification via SNMP

The following events lead to notification:


- The camera does not deliver a video signal
- The logbook cannot be created or written
- Database server could not be started
- Hard disk failure: Drive X deactivated, drive X not deactivated
- The hard disk is full (protected data)
- Internal database error
- Live image and reference image differ
- Scene is noisy
- Scene too dark
- Scene too bright
- Relay activated
- Relay not activated
- Internal malfunction or malfunction of external hard disks (e.g. malfunction relay has triggered, hard disk is full)
- Inputs activated (all DiBos inputs)
- Inputs deactivated (all inputs)

### 6.13.3 Configuring Automatic Alarm Recording

**Options** menu > **Settings** button



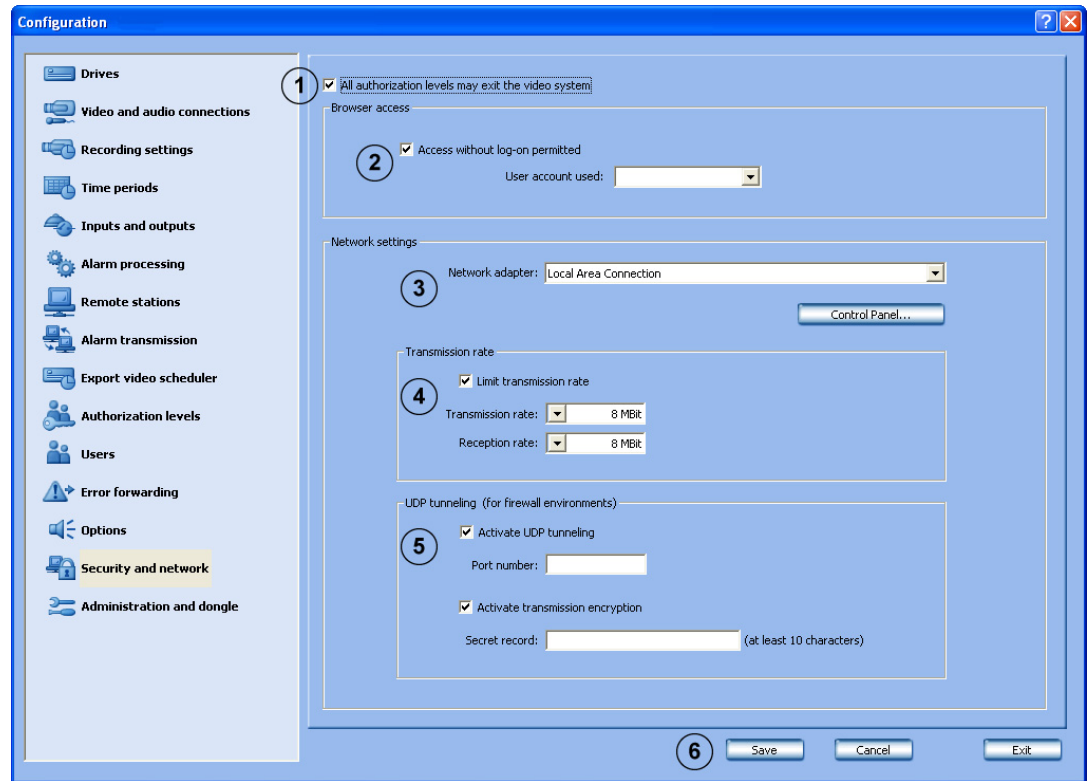
In this dialog box you can configure automatic alarm recording of a remote station alarm.

1	Target directory:	Click  and select the directory where the data will be saved.
2	Start recording automatically	Activate the check box to automatically save the data for alarm input.
3	Monitor data size in target directory	Activate the check box to monitor the size of the saved data.
4	Warning for more than [MB]	Enter the value for the data size in the target directory. A warning is displayed if the value is exceeded.
5	Monitor available memory on target drive	Activate the check box to monitor available memory on the target drive.
6	Error message for less than [MB]	Enter the value for the available memory that the actual value must fall below for an error message to be displayed.
7	Delete old video	Activate this check box when you want to delete data.
8	Older than [days]:	Enter the number of days after which data should be deleted. <b>Example:</b> 3 means that all data older than 3 days is automatically deleted.
9	OK	The entries are saved.

## 6.14

# Configuring Browser Access and Network Settings

### Security and network menu



In this dialog box you can specify security settings, such as browser access and network connection encryption.

1	All authorization levels may exit the video system	Activate this check box if all users are to receive authorization to exit the video system. <b>Note:</b> In the default setting, only the administrator can exit the video system.
2	Browser access	For browser access via the network.
	Access without log-on permitted	Activate this check box when access to the system via a browser (without logging on) is to be permitted. <b>Note:</b> This function is only available for self-generated http log-ons, not for standard log-ons.
	User account used:	Select the user in the list field whose authorization is to be used for the access.
3	Network settings	
	Network adapter:	Click the down arrow and select the network adapter.
	Control Panel	Under Windows XP, opens Network Connections in the Control Panel. <b>Note:</b> Here you can configure your own IP address or make firewall settings, for example.

4	Transmission rate	
	Limit transmission rate	Activate this check box if you want to limit the transmission rate.
	Transmission rate:	Select the transmission rate for DiBos-DiBos connections and browser.
	Reception rate:	Select the reception rate.
5	UDP tunneling (for firewall environments)	Allows a network connection between DiBos computers via a single port.
	Activate UDP tunneling	Activate this check box when you want to permit a network connection between DiBos computers via a fixed port.
	Port number:	Enter a port number that is not already used in the network. The port number must be the same for the DiBos recorder and the DiBos receiver. <b>Note:</b> This port must be enabled in the network. The video system's Windows firewall must be deactivated.
	Activate transmission encryption	Activate this check box if data transmission is to be encrypted.
	Secret record:	Enter a secret record of at least 10 digits. The secret record must be the same on both computers.
6	Save	The entries are saved.

The DiBos recorder already contains the preinstalled Web application for access via the browser. The Web application is activated by default. If access via http is to be prevented, the World Wide Web Publishing Service must be deactivated.

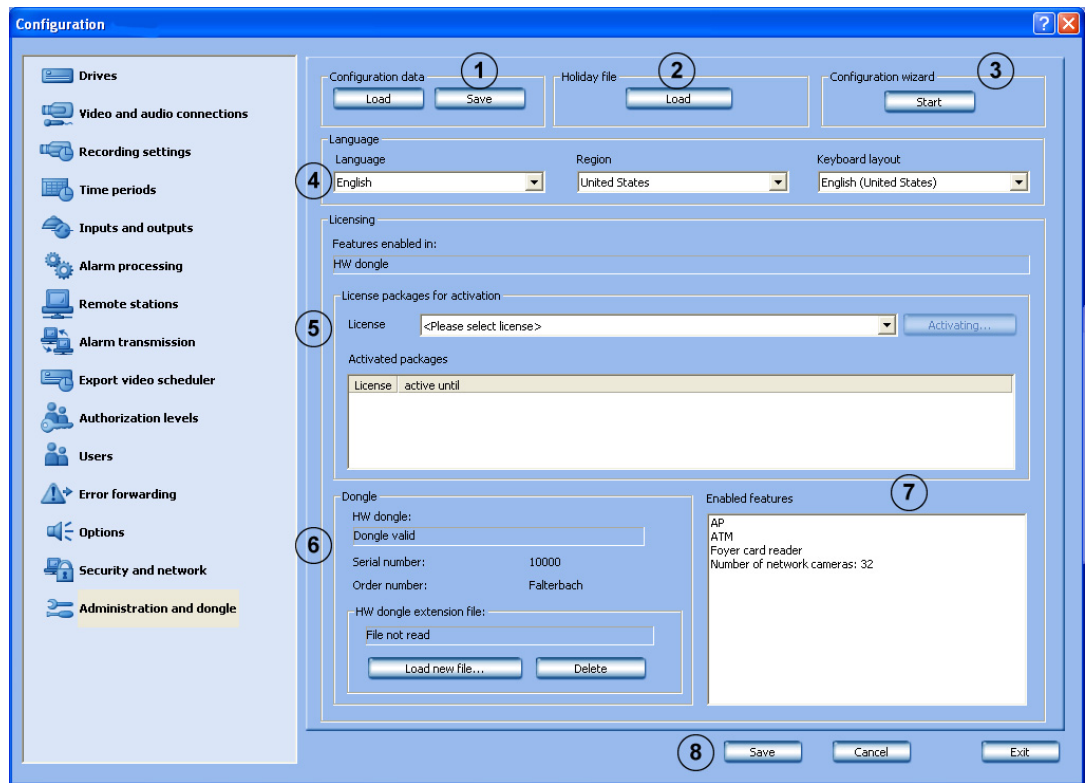
**Activating/deactivating the web application:**

Administrator rights are necessary for the following steps.

1. Log on to the operating system as Administrator.
2. Select **Start > Control Panel**.
3. Double-click the **Administrative Tools** icon.
4. Double-click the **Internet Information Services** icon.
5. Open the tree structure under **Internet Information Services** until you see the entry **Default Web Site**.
6. Select the entry **Default Web Site**.
7. Start or stop the service. To do so, click the corresponding buttons.

## 6.15 Administration and Dongle

### Administration and dongle menu



In this dialog box you have the following options:

- Load and save the configuration data
- Load the holiday file
- Start the Configuration wizard
- Set the language
- Activate the license packages
- Load and delete the HW dongle extension file
- Overview of enabled features
- HW dongle serial and order number
- Enable status of the HW dongle and the HW dongle extension file

1	Configuration data	
	Load	A new configuration can be loaded. The new configuration overwrites the previous one.
	Save	The configuration can be saved on a network drive or a data carrier. <b>Note:</b> For security reasons, it is advisable to always save the configuration on an external data carrier.
2	Holiday file	Here you have the possibility of modifying the holidays for the time program according to the country. The modification must be made in the Holidays.xml file.

	Load	Click the button and answer the warning note with <b>OK</b> if the previous file is to be overwritten or with <b>Cancel</b> if you want to modify the file.
3	Configuration wizard	
	Start	Click the button to start the Configuration wizard. <b>Caution:</b> The default configuration is overwritten with the last settings saved in the Configuration wizard. Overwriting settings may lead to the loss of previously configured settings (e.g. recording settings, IP cameras). We recommend only using the Configuration wizard for a newly installed system.
4	Language	Click the arrow and select the language for the operating system and the DiBos software. <b>Note:</b> If the language is changed, the system must be rebooted.
	Region	Click the arrow and make your selection.
	Keyboard layout	Click the arrow and select the layout of the keyboard connected.
5	Licensing	The software is activated using a license activation key. Devices that have been supplied with a HW dongle also require the activation of the HW dongle. <b>Note:</b> <ul style="list-style-type: none"> <li>– Factory-supplied DiBos recorders are already activated. The license activation key is affixed to the front flap for 19-inch devices. The license activation key for DiBos micro can be found on the left-hand side of the unit.</li> <li>– DiBos receivers, DiBos IP recorders and DiBos expansions are supplied with an authorization letter, which includes an authorization number. After the software is installed, they must be activated with a license activation key. See <i>Section 6.15.1 Activating a License</i> to find out how you obtain these license activation keys.</li> <li>– For devices with an existing dongle, the dongle is further required. This also applies for the dongle extension file. However, additionally ordered features must still be activated with a license activation key.</li> </ul>
	License packages for activation	The license packages that can be activated using a license activation key are displayed.
	License	Click the arrow and select a license package you would like to activate.
	Activate	Click the button to activate the selected license package. A dialog box will open for you to enter the license activation key.
	Activated packages	The activated license package is displayed.



6	Dongle	This field is only activated for devices that are enabled using a dongle. In this field, the serial and order number of the HW dongle and any existing dongle extension file is displayed.
	HW dongle extension file	The hardware dongle extension file contains features purchased retrospectively. The file must be loaded to activate these features. The hardware dongle extension file refers to a specific dongle.
	Load new file...	Click the button to load a dongle extension file. The existing file will be overwritten. <b>Note:</b> Keep a copy of the dongle extension file so that you can re-load it, should this be necessary following a recovery process (with recovery DVD).
	Delete	Click the button to delete the existing dongle extension file.
7	Enabled features	This field displays the features that are activated with a dongle, dongle extension file or a license activation key.
8	Save	The entries are saved.

## 6.15.1

### Activating a License

**Administration and dongle** menu > Select License > **Activate...** button

You can enter the license activation key in this dialog field in order to activate the license package.

There are two different application scenarios for activation:

#### **You already have a license activation key and have to re-install a license package:**

1. Enter the license activation key in the **License activation key** field. The license activation key is affixed to the front flap for 19-inch devices. The license activation key for DiBos micro can be found on the left-hand side of the unit.
2. Click **Activate**. The license package is activated.

#### **You have an authorization number and need a license activation key:**

1. Make a note of the computer signature or copy and paste it into a text file.
2. On a computer with Internet access, enter the following URL in the browser:  
`https://activation.boschsecurity.com`

You are now in Bosch License Manager.

Follow the instructions to call up a license activation key. Make a note of the license activation key or copy and paste it into a text file. There is a field for the license activation key in the authorization letter, under the sticker with the authorization number. This also applies to the computer signature of the affected computer. Enter the license activation key and the computer signature in the authorization letter.

3. In the **Activate license** dialog field in the DiBos configuration, enter the license activation key called up from Bosch License Manager and then click **Activate**. The license package is activated.

## 7 Remote configuration

A remote station can be configured remotely via the DiBos application if this remote station is located in the device list of the local DiBos.

In contrast to the standard configuration, with remote configuration the following limitations apply:

- It is not possible to configure analog cameras and audio inputs.
- It is not possible to configure the menus **Drives, Security and network** and **Administration and dongle**.
- The option of creating network drives via the **Export video scheduler** menu is not available. A target path can be selected.
- The option of configuring the alarm procedure via **Options** is not available.
- It is not possible to display a live image in the configuration page of a BVIP device.

---

### **CAUTION!**

Ensure that a DiBos device is not configured remotely if the local configuration is already open at the time. This procedure may lead to loss of data.

---

## 8 XP Administration

### 8.1 Logging On as a Windows® XP User

Proceed as follows to log on to Windows® XP as a video system user:

1. In Windows® XP, select **Start** -> **Log off**. The Windows log-off dialog appears.
2. The system automatically logs itself on as a DiBos standard user and starts the DiBos software.



#### NOTICE!

An automatic start, e.g. after a power failure, can only be carried out on DiBos recorder as a DiBos standard user.

### 8.2 Logging On as a Windows® XP Administrator

#### To be carried out by authorized personnel only!

Proceed as follows to log on as a Windows® XP Administrator or to change from the video system to the Windows® XP Administrator level.

1. Exit the video system. This is done by selecting **System** -> **Exit** from the menu bar.
2. In Windows® XP, select **Start** -> **Log off**. The Windows log-off dialog appears.
3. Press the left shift key and click the **Log off** button. Hold the left shift key down until the Windows log-on screen appears.
4. Log on with the user name **Administrator**.  
The default password on delivery is 1357. Change the password for security reasons once installation is complete.



#### NOTICE!

The default password on delivery is 1357. Change the password for security reasons once installation is complete (see *Section 8.3 Changing the Administrator Password*).

### 8.3 Changing the Administrator Password

#### To be carried out by authorized personnel only!

Proceed as follows to change the password:

1. Log on as a Windows® XP Administrator (see *Section 8.2 Logging On as a Windows® XP Administrator*).
2. Press CTRL+ALT+DELETE. The **Windows Security** dialog box appears.
3. Click **Change Password**. The **Change Password** dialog box appears.
4. In the corresponding fields, enter the old and new password and the new password again to confirm.
5. Click **OK**.

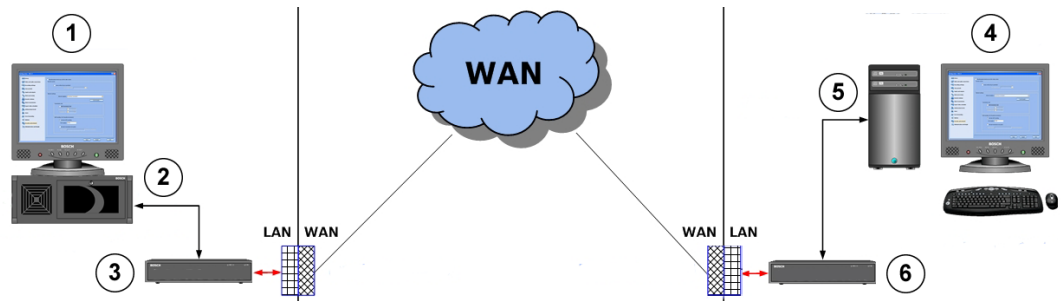
## 9 Connections

### 9.1 Network Connection via DSL

**To be carried out by authorized personnel only!**

The following example explains how the connection is set up:

#### DiBos recorder network connection to DiBos receiver via DSL



1	<b>DiBos recorder</b>		4	<b>DiBos receiver</b>	
	Computer name:	DiBos1		Computer name:	Receiver1
	DiBos recorder IP address:	192.168.1.10		DiBos receiver IP address:	192.168.0.2
	Subnet mask:	255.255.255.0		Subnet mask:	255.255.255.0
2	UDP port:	1750	5	UDP port:	1750
3	<b>DSL router</b>		6	<b>DSL router</b>	
	Gateway: (Intranet address of router in the LAN)	192.168.1.1		Gateway: (Intranet address of router in the LAN)	192.168.0.254
	Public address (Internet address) of router:	193.251.9.31		Public address (Internet address) of router:	193.252.10.5

#### For the DiBos Recorder

In the configuration of the DiBos recorder:

1. Select the **Remote stations** menu.
2. Click **New** and enter the name of the remote station (DiBos receiver).
3. Enter the public address (Internet address) of the remote station router (DiBos receiver), e.g. 193.252.10.5.
4. Select **Low bandwidth (live mode)** as necessary.
5. Click **OK**.
6. Select the **Security and network** menu in the configuration.
7. Select **Activate UDP tunneling**.
8. Enter a free number under **Port number** (e.g. 1750).

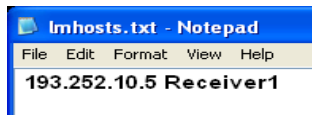
#### Note:

Check that the port is unused using the `netstat -a` command.

9. Click **OK**.

Mapping IP addresses and computer names:

1. Open the Notepad program.
2. Enter the public address (Internet address) of the remote station router and the computer name of the remote station (DiBos receiver). The address and the computer name must be separated by at least one space or tab character.



3. Save the file under the file name lmhosts in the directory  
C:\WINDOWS\system32\drivers\.
4. Remove the file extension .txt in Windows Explorer. The file must not have an extension.
5. Reboot the computer.

In the router configuration:

1. Use the standard configuration of the network provider.
2. Activate the router's firewall.
3. Activate port forwarding and forward the UDP port configured in DiBos (e.g. 1750) to the DiBos recorder IP address (e.g. 192.168.1.10). To do this, use the manufacturer's router documentation.



#### NOTICE!

The DSL router and DiBos recorder must be located in the same network.

#### For the DiBos Receiver

In the configuration of the DiBos receiver:

1. Select the **Remote stations** menu.
2. Click **New** and enter the name of the remote station (DiBos recorder).
3. Enter the public address (Internet address) of the remote station router (DiBos recorder), e.g. 193.251.9.31.
4. Select **Low bandwidth (live mode)** as necessary.
5. Click **OK**.
6. Select the **Security and network** menu in the configuration.
7. Select **Activate UDP tunneling**.
8. Enter the port number that you have already used in the DiBos recorder (e.g. 1750) under **Port number**.

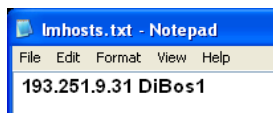
#### Note:

Check that the port is unused using the `netstat -a` command.

9. Click **OK**.

Mapping IP addresses and computer names:

1. Open the Notepad program.
2. Enter the public address (Internet address) of the remote station router and the computer name of the remote station (DiBos recorder). The address and the computer name must be separated by at least one space or tab character.



3. Save the file under the file name `1mhosts` in the directory  
`C:\WINDOWS\system32\drivers\`.
4. Remove the file extension `.txt` in Windows Explorer. The file must not have an extension.
5. Reboot the computer.

In the router configuration:

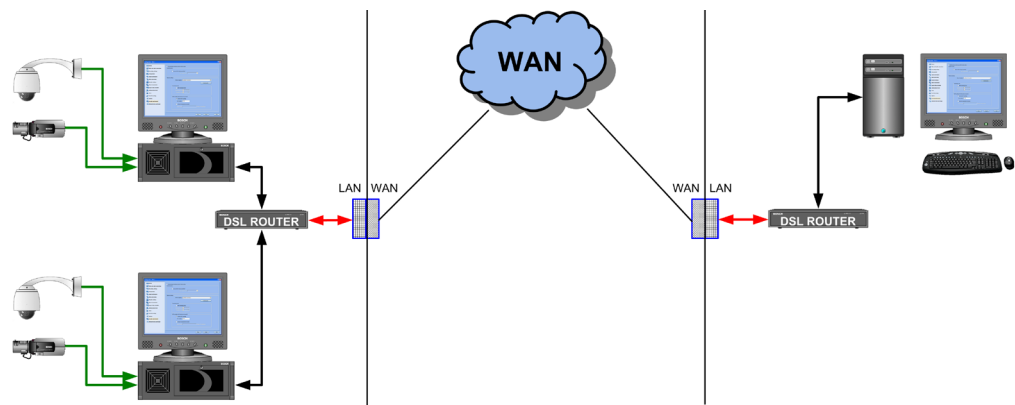
1. Use the standard configuration of the network provider.
2. Activate the router's firewall.
3. Activate port forwarding and forward the UDP port configured in DiBos (e.g. 1750) to the DiBos recorder IP address (e.g. 192.168.0.2). To do this, use the manufacturer's router documentation.



**NOTICE!**

The DSL router and DiBos receiver must be located in the same network.

**With several DiBos recorders behind the DSL router**



**NOTICE!**

If there are several DiBos recorders behind the DSL router, it is recommended that you use a VPN (Virtual Private Network). You can obtain more detailed information regarding VPN settings from Bosch Security Systems.

## 9.2 Connecting the ISDN Controller

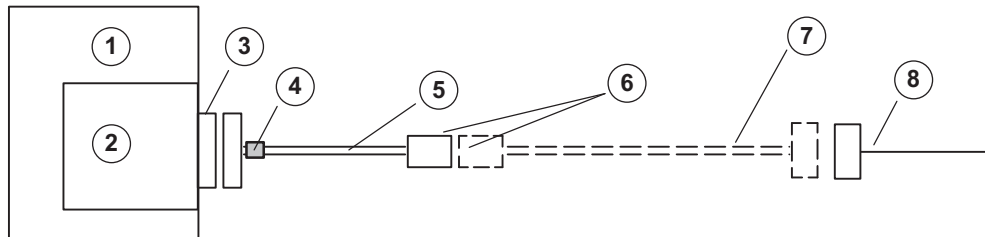
**To be carried out by authorized personnel only!**

The ISDN connection is established via the supplied adapter cable (with Western plug) on the computer's S<sub>0</sub> interface.



### NOTICE!

Only the card type Fritz! Card PCI V2.0 may be used.



1	Video system	5	Supplied adapter cable
2	ISDN controller (transmitter or receiver)	6	Western plug
3	ISDN adapter card socket	7	Only necessary for TAE sockets (not included in delivery)
4	Ferrite core	8	ISDN connection

To install the ISDN card, the computer must be next to the ISDN connection and the card must be integrated in the computer.

For data to be transmitted, the connection must support the EURO ISDN (DSS1) protocol. S<sub>0</sub> connections in PBXs may first have to be enabled in the PBX. The data service must also be enabled in the incoming and outgoing direction. The video system is delivered for EURO ISDN ex-works.

**ISDN socket TAE 8** on the S<sub>0</sub> interface of the video system (9-pin Sub-D socket)

Sub-D socket	TAE 8 plug	Function
1-		
2 - SR1-	- 4 (b1)	Transmit wire
3 - SR2+	- 3 (a1)	Transmit wire
4 - SX1-	- 6 (a2)	Receive wire
5 - SX2-	- 5 (b2)	Receive wire

**ISDN socket IAE (RJ 45)** on the S<sub>0</sub> interface of video system (9-pin Sub-D socket)

Sub-D socket	IAE 8 plug	Function
1-		
2 - SR1-	- 5 (b1)	Transmit wire
3 - SR2+	- 4 (a1)	Transmit wire
4 - SX1-	- 3 (a2)	Receive wire
5 - SX2-	- 6 (b2)	Receive wire



## 9.3 Connecting VSCom 200 H (Interface Expansion)

**To be carried out by authorized personnel only!**



### NOTICE!

Only the card type VSCom 200 H PCI may be used.

When retrofitting the interface expansion card, the following installation must be carried out.

1. Switch off the computer and insert the interface expansion card in the appropriate computer slot.
2. Reboot the computer.
3. Log on as Administrator.
4. The system automatically recognizes the interface expansion card.

## 9.4 Connecting External Hard Disks

An SCSI controller must be installed in order to connect the external hard disk housing. The type and number of hard disks that can be connected can be found in the price list.

External hard disks must be switched on before booting the PC.



### NOTICE!

Only the following card type may be used as an SCSI controller: LSI Logic 320 MB Ultra Wide 68 PIN HD SYM 21320.

### CAUTION!

Do not position the SCSI cable near to a power cable. This influences the transmission rate and may cause the connection to be interrupted.

## 9.5 Connecting a Malfunction Relay

The malfunction relay is connected to a relay output. It must be activated in the configuration (see *Section 6.5.2 Configuring Relay Outputs*).

The following events are signaled by the malfunction relay.

- The camera does not deliver a video signal
- The logbook cannot be created or written
- The images could not be recorded by the database server
- Database server could not be started
- Hard disk failure: Drive X deactivated, drive X not deactivated
- The hard disk is full (protected image data)
- Internal database error
- Device could not be started
- Grabber card not working
- Export video scheduler error
- Reference image check failed

## 9.6 Connecting an ATM (Serial)

A maximum of four customer-operated ATMs or three customer-operated ATMs and one access control system can be connected to the video system via an interface processor. The following ATM connection variants are possible:

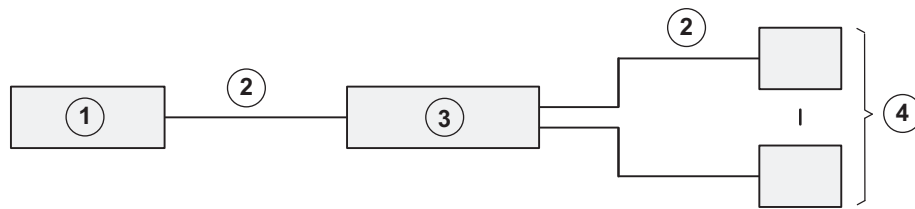
### Variante 1:

The customer-operated ATMs are not far from the video system. The video system and interface processor, as well as the interface processor and the ATMs, can be connected together in such a way that the distance between each of them is less than 15 m.

Possible solution:

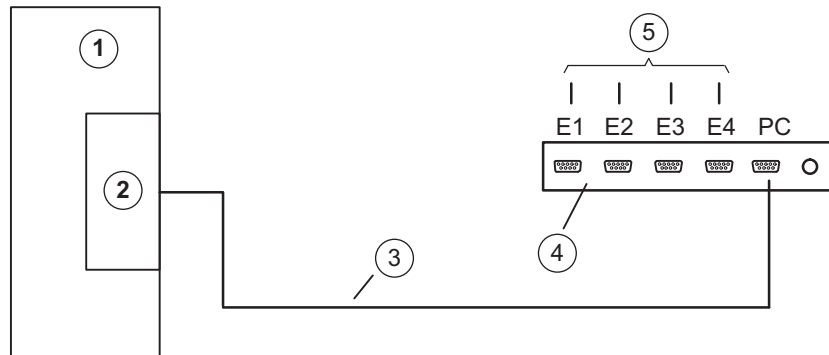
Connection of each ATM is made directly at the interface processor and is ATM-specific. The distance between the video system and the interface processor, as well as the distance between the interface processor and the ATMs, is a maximum of 15 m.

Connection principle:



1	Video system	3	Interface processor
2	Max. 15 m	4	ATM1 - ATM4

Connection details:



1	Video system	4	Interface processor
2	COM x	5	ATM1 - ATM4
3	Connection cable, 9-pin		

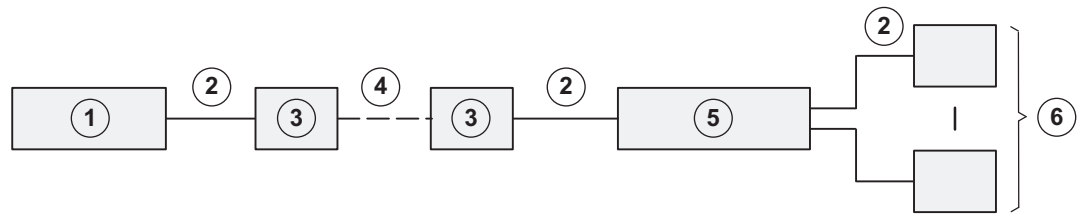
**Variante 2:**

The customer-operated ATMs are further away from the video system. The video system and interface processor, as well as the interface processor and the ATMs, cannot be connected together in such a way that the distance between each of them is less than 15 m. The ATMs are, however, close enough together to allow them all to be connected to the interface processor in such a way that the distance between the interface processor and each ATM is less than 15 m.

Possible solution:

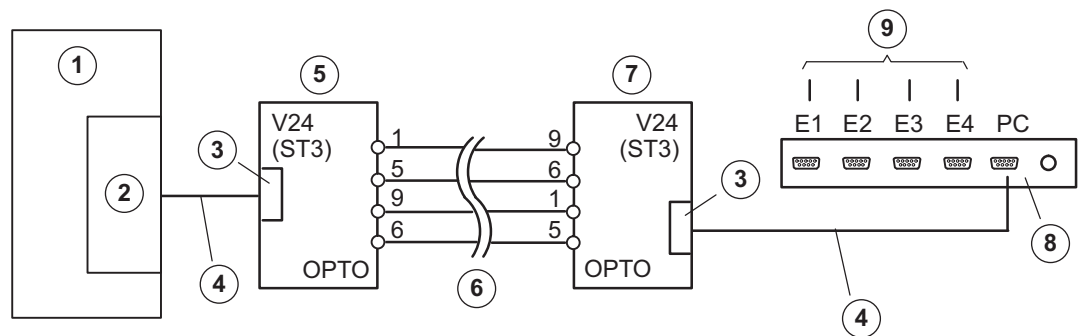
Connection of each ATM is made directly at the interface processor and is ATM-specific. To increase the range, two OVS are required between the video system and the interface processor.

Connection principle:



1	Video system	4	Max. 1000 m
2	Max. 15 m	5	Interface processor
3	OVS	6	ATM1 - ATM4

Connection details:



1	Video system	6	Max. 1000 m
2	COM x	7	OVS 2 BR1 and BR2: Position 2/3 ST3: Pin 2 = receive line, Pin 3 = transmit line
3	9-pin	8	Interface processor
4	Connection cable, 9-pin, part no. 4.998.079.686 (1:1 connection)	9	To ATM1 - ATM4
5	OVS 1 BR1 and BR2: Position 1/2 ST3: Pin 2 = transmit line, Pin 3 = receive line		



**NOTICE!**

By re-plugging the bridges BR1 and BR2 in the OVS, it is possible to swap over the transmit and receive lines.

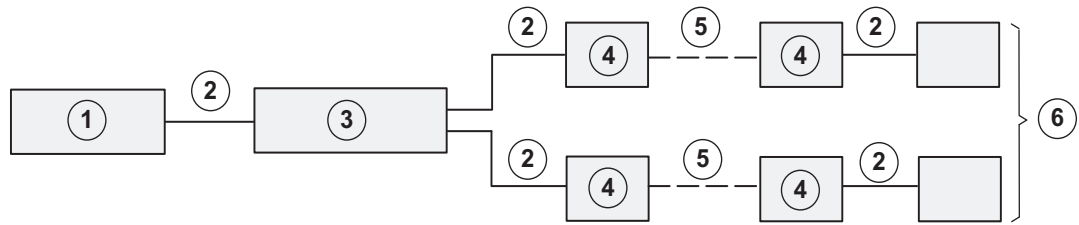
**Variante 3:**

The customer-operated ATMs are further away from the video system. The video system and interface processor, as well as the interface processor and the ATMs, cannot be connected together in such a way that the distance between each of them is less than 15 m. The individual ATMs are not close enough together to allow them all to be connected to the interface processor in such a way that the distance between the interface processor and each ATM is less than 15 m.

Possible solution:

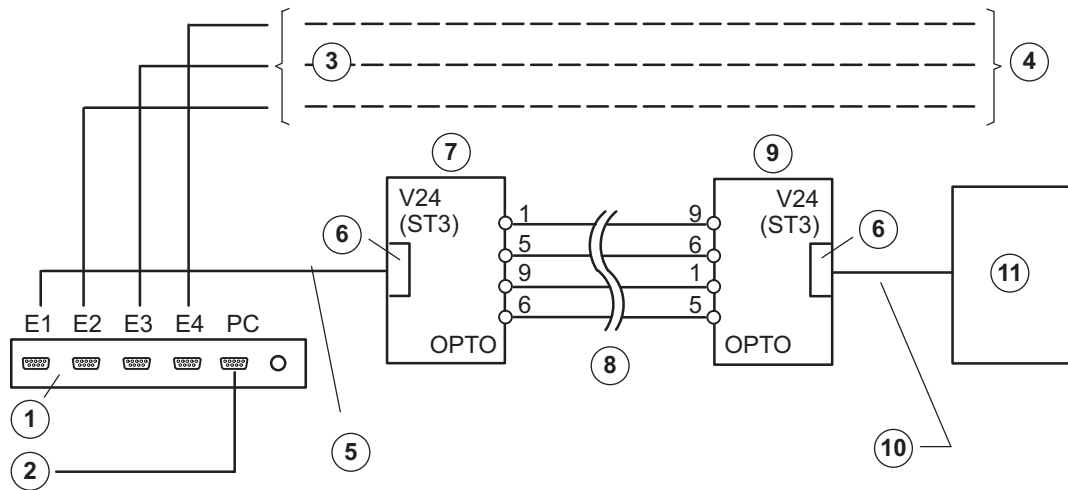
The interface processor is connected directly to the video system. To increase the range, two OVS are required between the interface processor and the ATM.

Connection principle:



1	Video system	4	OVS
2	Max. 15 m	5	Max. 1000 m
3	Interface processor	6	ATM1 - ATM4

Connection details:



1	Interface processor	7	OVS 1 BR1: Position 1/2 BR2: Position 1/2 ST3: Pin 2 = transmit line, Pin 3 = receive line
2	Connection cable to video system (COM x)	8	Range max. 1000 m
3	As ATM1	9	OVS 2 (bridge setting depending on ATM)
4	To ATM2 - ATM4	10	ATM-specific cable connection or adapter

---

5	Connection cable, 9-pin, part no. 4.998.079.686 (1:1 connection)	11	ATM1
6	9-pin		

---

**NOTICE!**

By re-plugging the bridges BR1 and BR2 in the OVS, it is possible to swap over the transmit and receive lines.

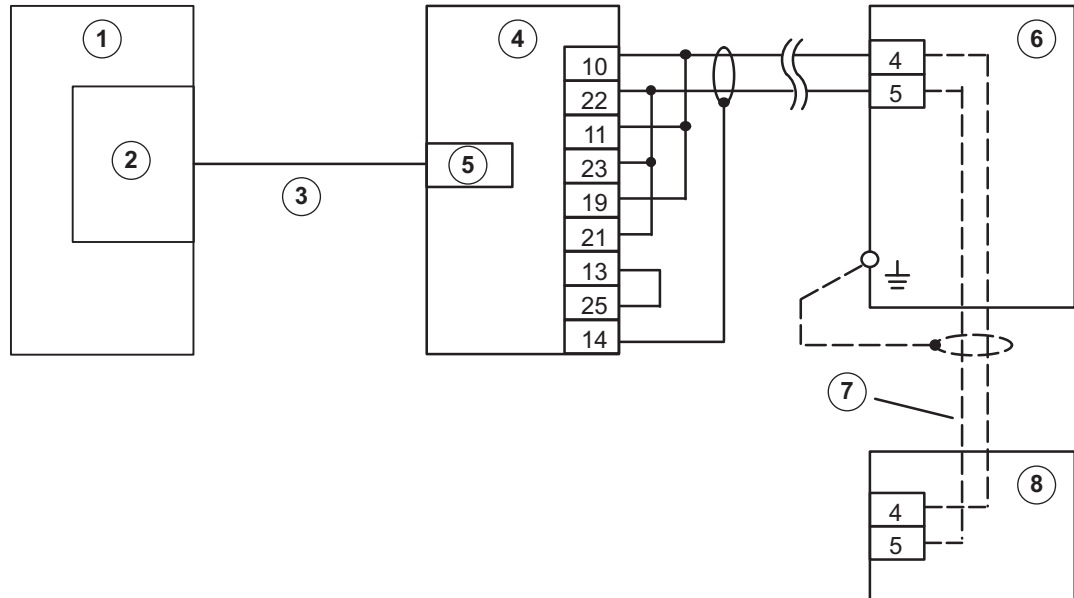
---

## 9.7

## Connecting the MINITER RS 485 Foyer Card Reader

The MINITER RS 485 foyer card reader is connected via a serial interface. A maximum of four foyer card readers can be connected in series.

It is possible to operate the LS23M and the MINITER RS 485 foyer card readers on the same serial bus. Note that the LS23M foyer card reader should preferably be installed as the last bus element.



1	Video system	5	RS232
2	COM x	6	Foyer card reader 1 (MINITER RS 485) (4.998.098.769 / 4.998.098.767)
3	Connection cable, 9-pin - 25-pin	7	Per wire 2 x 0.6 mm
4	Interface converter W&T 86000 (4.998.053.926)	8	Foyer card reader 4 (LS23M), J2 connected

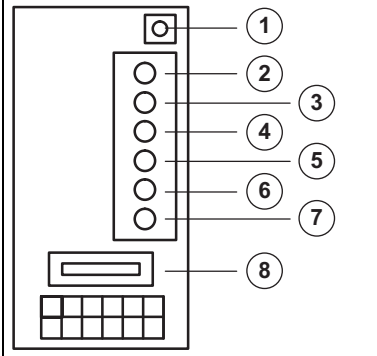
### NOTICE!

- The distance between the interface converter and the last foyer card reader can be a maximum of 1000 m (installation cable J-Y(St) Y 2 x 2 x 0.6 mm).
- The foyer card reader must be correctly grounded!
- Shielding may only be applied on one side.
- The connection between the foyer card readers may only be made via the connector strip of the reader.
- If the last foyer card reader on the RS 485 bus is a MINITER, the RS 485 bus must always be terminated with a 250 Ohm termination resistor (resistor is included in delivery).
- For flush mounting: At the rear of the housing, the angle bracket that the credit card hits must be cut off. Only then is the credit card data read correctly.



**For further information on how the interface converter works, see the description W&T Interface Model 86000.**

**MINITER RS 485 contact assignment**

	1	Tamper switch
	2	0 V DC input, GND (PIN 1)
	3	Door opener output ground (PIN 2)
	4	Standby contact/working contact door opener output (PIN 3)
	5	Signal RS 485- (PIN 4)
	6	Signal RS 485+ (PIN 5)
	7	+ 12 V DC input (PIN 6)
	8	Fuse

**Configuring MINITER RS 485 foyer card readers**

Configuration is carried out with the MINITER RS 485 software. This can be installed on a service laptop or on the video system. Proceed as follows to configure the card readers:

1. Start the configuration software and select RS485 operation.
2. Select the COM port to which the foyer card readers are connected via the **Interface** menu item. Even if several MINITER RS 485 foyer card readers are to be programmed for the first time, only one foyer card reader should be connected during programming. This is because the foyer card reader will assign all the card readers with the same bus address by default.
3. Select the **MINITER > Miniter auslesen/identifizieren (Read/Identify Miniter)** menu and click **Identifikation aller Adressen (Identification of all addresses)**. **Adresse: 48 (Address: 48)** and **Protokoll: Bosch (Protocol: Bosch)** is displayed.
4. Select foyer card reader number 48 and confirm your selection with **OK**.
5. Click **Miniter auslesen (Read Miniter)** and enter **Passwort: 991357 (Password: 991357)**. Confirm with **OK**.
6. The foyer card reader addresses must be assigned as follows.
  - Foyer card reader no. 1 = address 48
  - Foyer card reader no. 2 = address 49
  - Foyer card reader no. 3 = address 50
  - Foyer card reader no. 4 = address 51

The other parameters must be set as follows for operation:

- Door opening time: optional
- Door opener with buzzer: optional
- Door opener interval tone: optional
- Monitoring module: no
- Password: 991357
- Signal chip card: no
- Send start character: no
- Data on display: no
- Evaluate track 2: yes
- Evaluate track 3 or 1: yes
- Open door on fault: no
- Protocol: Bosch
- Block list: optional
- Data length track 2: 18 (for credit cards)
- Data length track 3/1: 26 (for EC cards)

7. Set separate authorizations for credit cards (track 2) and for EC cards (track 3) to permit access to the foyer if the connection between the video system and the Miniter is interrupted (see Miniter RS 485 operating manual). Otherwise, the video system manages access authorizations during operation.
8. Save the file via **File via FTP > Save as** under the name DiBos\_foyer\_card\_reader\_x (x = 1 .. 4).
9. Select **File via FTP > Exit**.
10. Select the **MINITER > Miniter beschreiben (Write Miniter)** menu and select and open the DiBos\_foyer\_card\_reader\_x file. The new and current address of the foyer card reader is displayed.
11. Confirm the address with **OK**.
12. Click **Datei in Miniter schreiben (Write file in Miniter)** and confirm this by entering the old password.  
System confirmation is given when programming has been completed successfully.



## 9.8 Connecting the DCF 77 Radio Clock

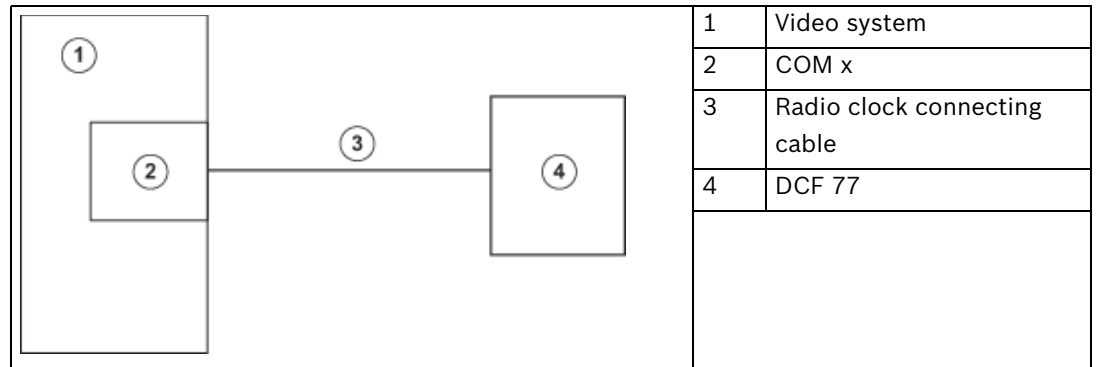
**To be carried out by authorized personnel only!**

The radio clock is connected via a serial interface.



### NOTICE!

Only the NeoClock DCF 77 radio clock may be used.



When retrofitting, the following installation must be carried out. Use the supplied installation CD.

1. Connect the radio clock to the serial interface.
2. Log on as Administrator.
3. Select the interface.
  - Select **Start > Control Panel > System**.
  - Select the **Hardware** tab and click **Device Manager**.
  - In the tree structure, open the entry **Ports** with a double click and select the interface, e.g. **Communications Port (COM1)** with a double click.
  - Select the **Connection settings** tab.
  - Enter the settings for the interface:  
 Baud rate:2400  
 Data bits:8  
 Parity:None  
 Stop bits:2  
 Protocol:None  
 Confirm with **OK**.
4. Radio clock installation
  - Insert the installation CD.
  - Call up `Setup.exe` in Windows® XP Explorer.
  - Select **Install server** and click **Next**.
  - Select the target directory for the program. Click **Next**, if you want to use the default path or click **Browse** to select another one.
  - Follow the on-screen instructions.
5. Once installed, configure the **Time Synchronization** program.
  - Select **Start > Control Panel > NeoClock Time Synchronization**.
  - Make the following settings in the configuration menu:  
 Language: **German**  
 Port: **COM x** (interface used)  
 Synchronization: Select **Automatic**

Time lag: Select 0 (hours) and **Daylight saving time**

License: Enter serial number and activation code (please note these entries are case sensitive) and confirm with **OK**.

- Click **Save**.
- Click **Yes** in the information window to start the **Time Synchronization** service.

**Note:**

A timer appears in the Windows XP task bar (at the bottom edge of the screen). This confirms that the **Time Synchronization** program has started. The color of the clock depends on the receiver status.

Yellow: Program starting (takes up to three minutes!)

Red: No synchronization or installation error

Green: Synchronization of system clock with receiver is OK.

6. Exit the **NeoClock Time Server** service as follows:
  - Select **Start -> Control Panel -> Administrative Tools -> Services**.
  - Double-click **NeoClock Time Server** and click **Exit** under **Service Status (General tab)** to exit it.
  - Deactivate the service by selecting **Deactivated** as the **Start type**.
  - Confirm with **OK** and close the **Services** dialog box and the Control Panel.
7. Reboot the PC.
8. The **NeoClock Time Server** program must not be configured; instead, TARDIS should be used. (Program used to synchronize video systems in a network; can be requested from the video system manufacturer's video product service).
9. To position the clock, use the NeoClock XP operating manual (available on the CD as a PDF file).

## 9.9 Connecting a Modem/ISDN Card (for Incoming Connections)

**To be carried out by authorized personnel only!**

Administrator rights are necessary for the following steps.

### Modem selection:

- Both internal PCI modems and modems connected via serial port (exception: DSL modems) or USB can be used if supported by Windows XP.
- The V.90 and V.34 protocols must be supported.
- The country-specific approval regulations must be observed (particularly regarding operation in a telephone network, radio interference suppression, electrical safety and fire protection).
- Compatible with the properties of the national telephone network.
- The characteristics of company telephone systems must be taken into account (e.g. call-connected recognition disabling if necessary, tone/pulse dialing).

### Modem installation

Install the modem according to the manufacturer's instructions provided. Many modem types are recognized automatically under Windows® XP. However, take into account any special features of the installation (example: If the modem does not recognize the call connected signal of a telephone system, the option **Wait for call connect before dialing** must be deactivated).

### For modem: Reducing timeout values for outgoing connections

1. From the Windows® XP desktop, select **Start > Control Panel**.
2. From the **Control Panel** folder, select the **Phone and Modem Options** icon.
3. In the **Phone and Modem Options** dialog box, click the **Modems** tab.
4. Select the installed modem in the list field and click the **Properties** button.
5. In the dialog box, click **Properties of ..** on the **Extended** tab and then click the **Edit standard settings...** button.
6. On the **General** page, under **Cancel dialing procedure after .. seconds**, change the value from 60 to 15.
7. Confirm the open dialog boxes with **OK**.

### For Modem and ISDN: Enabling dial-in (if incoming calls are to be accepted)

1. From the Windows® XP desktop, select **Start > Control Panel**.
2. From the **Control Panel** folder, select the **Network Connections** icon.
3. In the **Network Connections** folder, under **Network Tasks**, click the **Create new connection** icon.
4. In the **New Connection Wizard** dialog box, click the **Next** button.
5. On the **Network Connection Type** wizard page, select the option **Set up an advanced connection** and click the **Next** button.
6. On the **Advanced Connection Options** wizard page, select the **Accept incoming connections** option and click **Next**.
7. On the **Devices for Incoming Connections** wizard page, select the previously installed modem or ISDN card under **Connection Devices**. Place a checkmark next to this entry and click **Next**.
8. On the **Incoming VPN Connection** wizard page, activate the **Do not allow virtual private connections** option and click the **Next** button.
9. On the **User Authorizations** wizard page, click **Next**.

10. Make the settings for the network protocol as follows: On the **Networking Software** wizard page, select the **Internet protocol (TCP/IP)** entry from the list box and make sure that there is a checkmark next to this entry.
  - Click **Properties** and make sure that in the **Incoming TCP/IP properties** dialog box, the following settings are made: **Allow callers to access my local area network** must not be selected. **Specify TCP/IP addresses** must be selected and the address range from 169.254.x.1 to 169.254.x.254 must be entered. Number x must be a unique system number in the customer's RAS network and may be assigned from 2 to 254.

Example: A customer owns 10 DiBos systems and 1 alarm receiver system. In this case, number x varies from 2 to 12. The same number must not be used for two different systems.

The option **Allow calling computer to specify its own IP address** must be selected. Confirm with **OK**.
  - Click the **Next** button on the wizard page.
11. On the **Completing the Wizard** wizard page, click **Finish**.
12. Make the necessary settings in the DiBos configuration.

**Required configuration settings on the computer on which dialing in is to take place.**

1. Select the **Remote stations** menu.
2. Activate the **Accept incoming calls** check box to allow dialing in via modem/ISDN.

**Note:**

When the check box is activated, you are requested to enter a password. Enter the password to dial in to the computer.

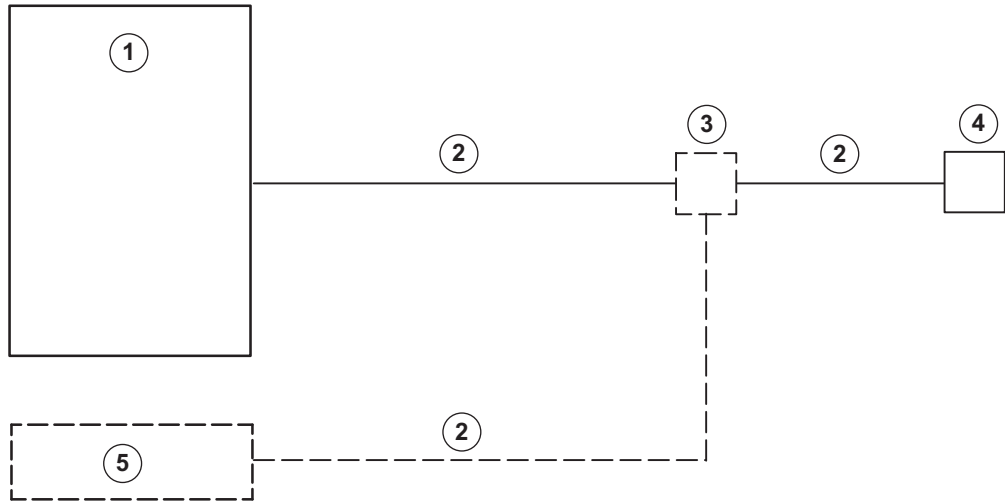
3. Confirm the entries with **OK**.

**Required configuration settings on the computer from which dialing in is to take place.**

1. Select the **Remote stations** menu.
2. Click **New** and enter a name.
3. Activate the **Modem/ISDN** check box.
4. Under **Number**, enter the telephone number.
5. Leave the **User** field unchanged.
6. Click **Enter password**.
7. Enter the password for the computer on which dialing in is to take place.
8. Confirm the entries with **OK**.

## 9.10 Connecting to AutoDome/SAE Dome

### 9.10.1 Connecting to Bosch Dome Cameras (Directly)



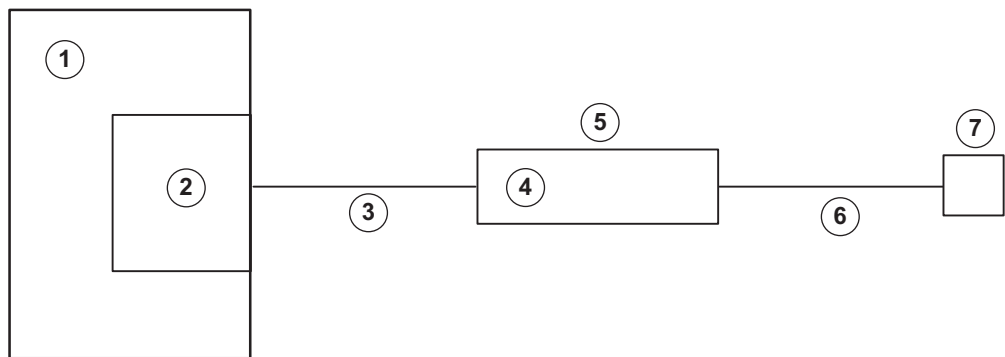
1	Video system	4	AutoDome
2	Biphase	5	LTC matrix switch
3	Code multiplexer LTC 8569 or LTC 8570		



**NOTICE!**

An LTC 8569 or LTC 8570 is needed if a Bosch LTC matrix switch is connected to the video system at the same time as an AutoDome.

### 9.10.2 Connecting to Bosch Dome Cameras via Matrix Switch



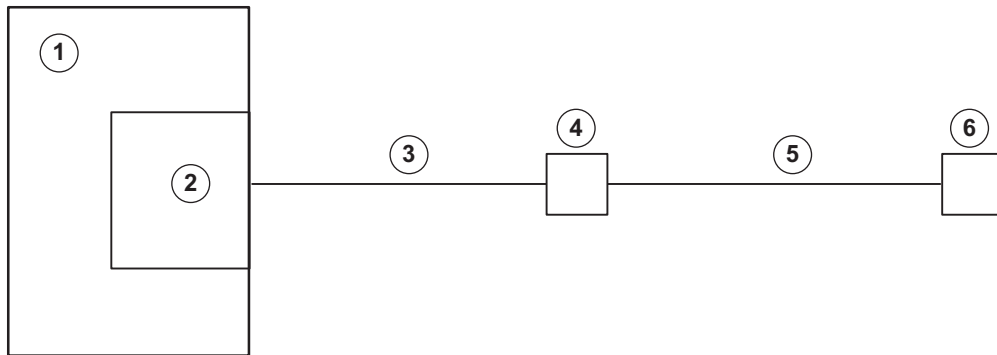
1	Video system	5	LTC 8x00
2	COM x	6	Biphase
3	Allegiant console cable LTC8506/00	7	AutoDome
4	Console port		



**NOTICE!**

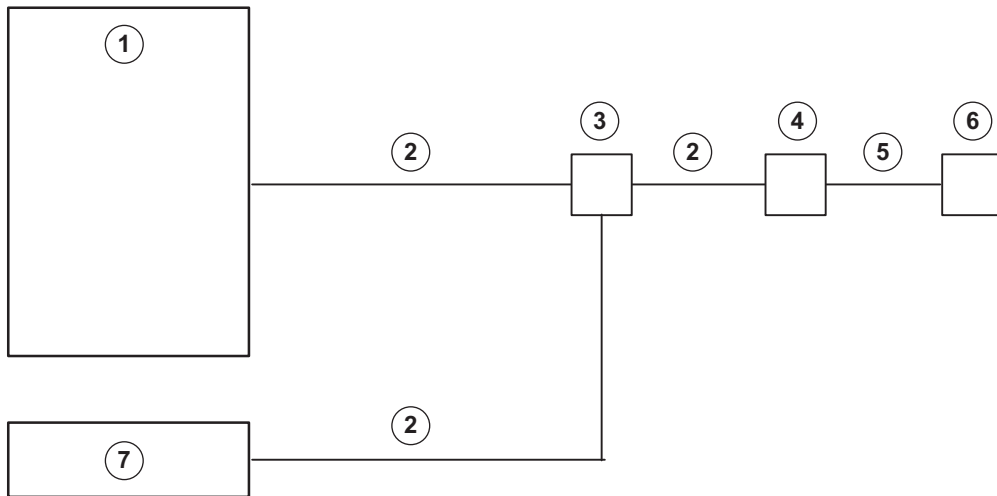
Valid CCL commands can be configured in DiBos. These pre-configured commands can then be sent to the Allegiant matrix switch manually or automatically.

### 9.10.3 Connecting to SAE Dome Cameras (Directly)



1	Video system	4	RS 232/RS 485 converter e.g. LNL-108 A
2	COM x	5	RS 485
3	RS 232	6	SAE Dome

### 9.10.4 Connecting to SAE Dome Cameras with V3032 Biphas Interface



1	Video system	5	RS 485
2	Biphase	6	SAE dome camera
3	Code multiplexer LTC 8569 or LTC 8570	7	LTC matrix switch
4	Protocol converter SAE (V3032)		



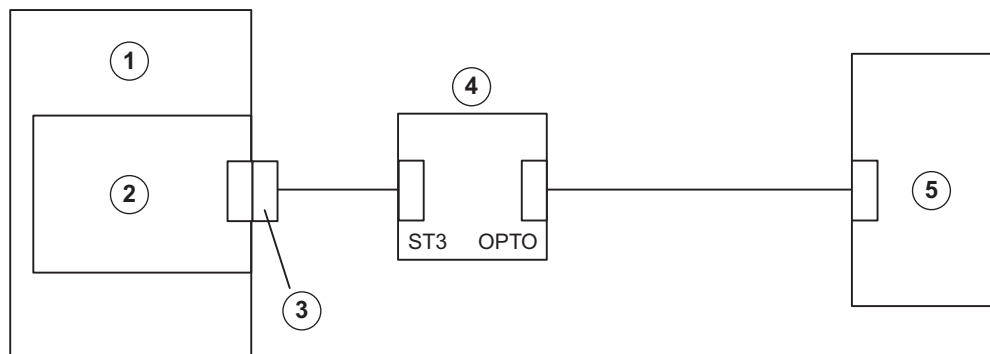
**NOTICE!**

An LTC 8569 or LTC 8570 is needed if a Bosch LTC matrix switch is connected to the video system at the same time as an SAE Dome.

## 9.11 Connecting an AP

### 9.11.1 General

The video system is connected to an AP via an RS232 interface on COM x, for example using an intermediate OVS interface converter.



1	Video system
2	COM x
3	RS 232 interface
4	OVS interface converter
5	Bosch AP

When connecting the video system, no alarm-specific modifications are necessary on the respective APs (the required interface module must be present). All settings are made via the video system user interface.

The AP must have data transmission enabled and be fitted with an appropriate interface module (see relevant connection).

Using the OVS assembly, any differing transmit and receive assignments on the devices for V.24 connection can be balanced out. Bridges BR1 and BR2 must be re-plugged.

**OVS interface converter bridge assignment**

<p>The diagram shows the internal wiring of the OVS interface converter. It includes several bridge relays (BR1, BR2, BR4, BR5, BR6) and switches (ST11, ST3). The OPTO and V.24 terminals are also shown. Pin connections are indicated by numbers 1, 2, and 3. A circled '1' is in the top left, and a circled '2' is next to the ST11 switch.</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%; text-align: center;">1</td> <td>OVS</td> </tr> <tr> <td style="text-align: center;">2</td> <td>12 V/24 V connection</td> </tr> </table> <p>Warning: Disconnect the mains plug before opening the OVS!</p> <p><b>For 12 V/24 V supply</b>  BR4: Position 1/2  BR5: Position 1/2  BR6: Position 1/2</p> <p>For 230 V supply  BR4: Position 2/3  BR5: Position 2/3  BR6: Open</p>	1	OVS	2	12 V/24 V connection
1	OVS				
2	12 V/24 V connection				

**Exchanging transmit and receive lines**

- Variant 1:  
BR1, BR2: Position 1/2  
ST3: Pin 2 = transmit line, Pin 3 = receive line
- Variant 2:  
BR1, BR2: Position 2/3  
ST3: Pin 2 = receive line, Pin 3 = transmit line

OPTO pin assignment		V.24 (ST3) pin assignment	
Direction	Connection	Direction	Connection
Input -	1	Transmit/Receive *	2
Input +	6	Receive/Transmit *	3
Output +	5	0 V	5
Output -	9		

\* depending on BR1/BR2

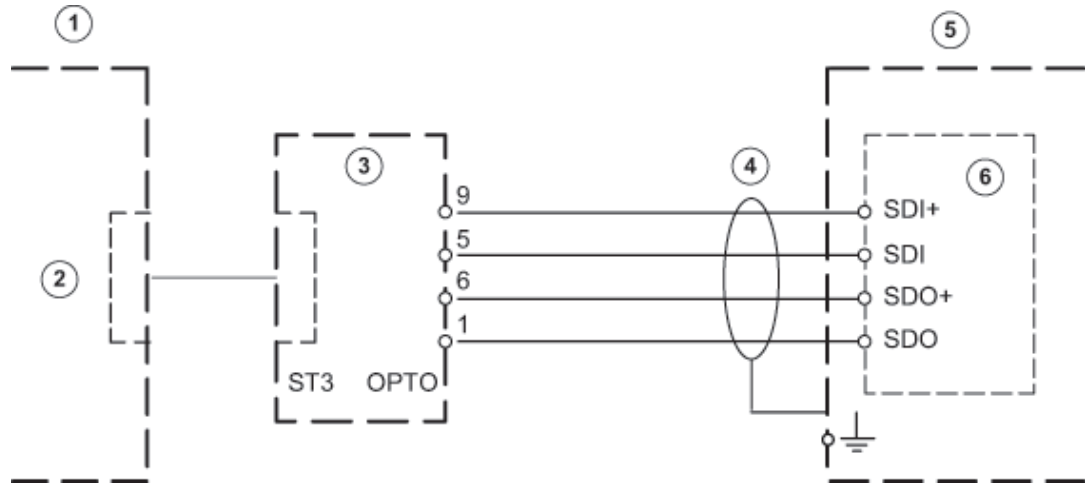


**NOTICE!**

For cabling, telephone cables of type J-Y(St)Y 2x2x0.6 are recommended. The cable shielding must be grounded at the alarm panel side to avoid earth currents.



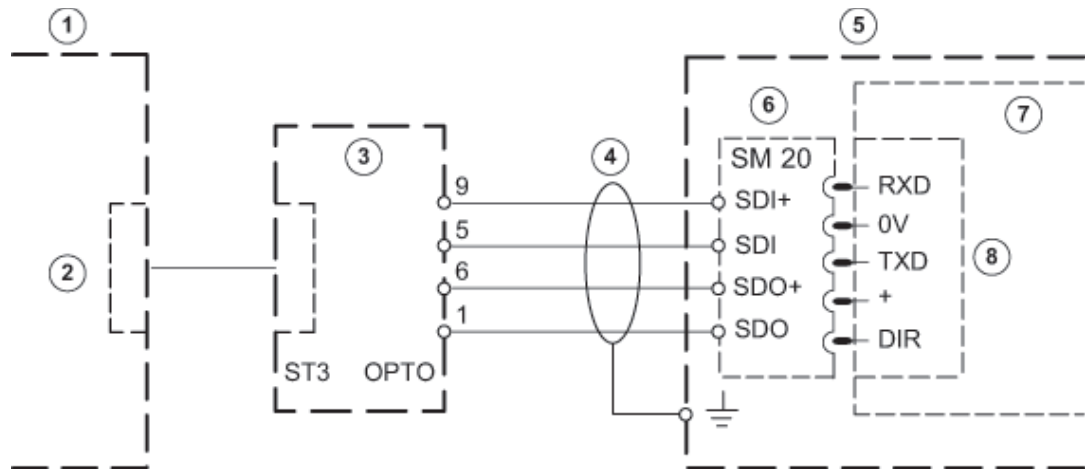
### 9.11.2 Connecting to NZ 500 (20 mA) Video System NZ 500



Connect shielding wire to NZ 500 only Installation cable J-Y (St) Y 2x2x0.6	SU 500: BR1 connected (1200 bit/s)
--	---------------------------------------

1	Video system	4	Range max. 1000 m
2	COM x	5	NZ 500
3	OVS	6	SU 500

### 9.11.3 Connecting to BZ 500 (20 mA)

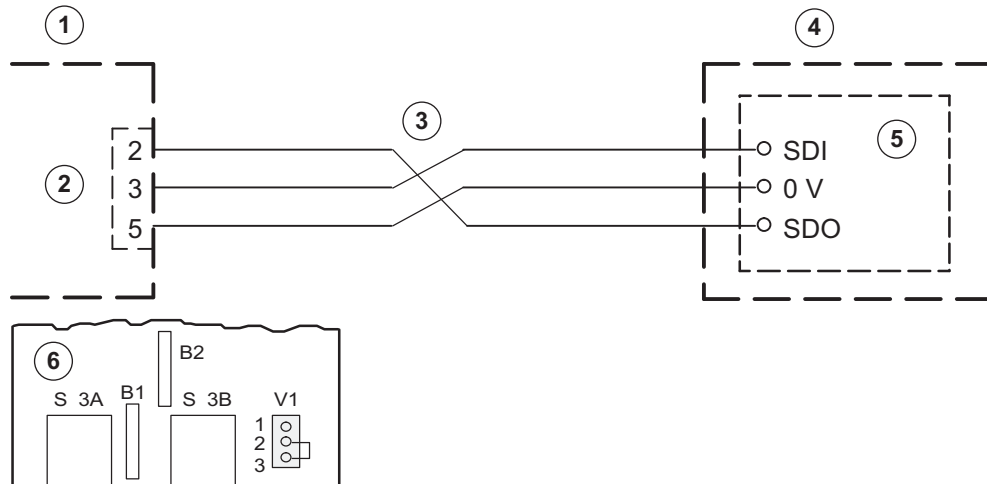


Connect shielding wire to NZ 500 only Installation cable J-Y (St) Y 2x2x0.6	COM 2 and COM 3 only with interface assembly ERSE 10
--	---

1	Video system	5	BZ 500 LSN
2	COM x	6	SM 20
3	OVS	7	ANNE 10
4	Range max. 1000 m	8	COM 1 to COM 3

### 9.11.4 Connecting to AZ 1010/NZ 1008

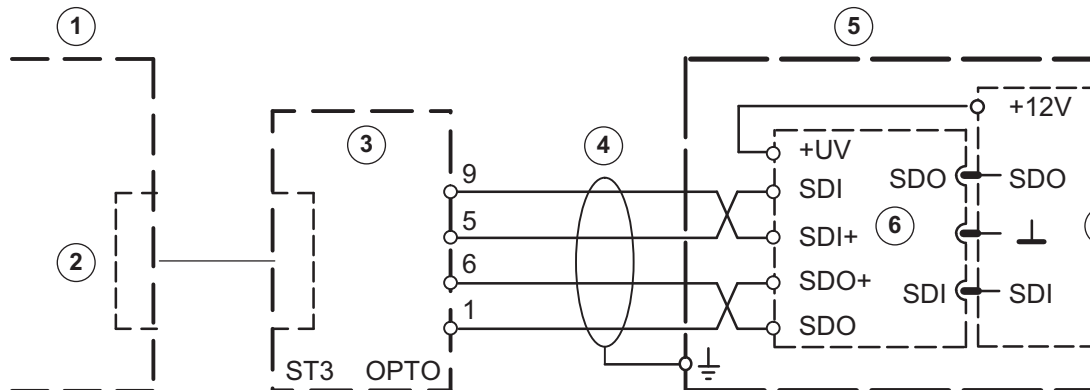
#### V.24 connection to AZ 1010/NZ 1008



<b>Bridge assignment (V) on the SMA</b> Plug-in bridge V1 in pos. 2/3 Level for V.24 interface	Connection of the AZ 1010/NZ 1008 must be programmed on the alarm panel side.
--	---

1	Video system	4	AZ 1010/NZ 1008 (connection must be programmed on the alarm panel side)
2	COM x	5	SMA
3	Max. 25 m	6	SMA (plug-in bridge V1 in pos. 2/3, level for V.24 interface)

#### 20 mA connection to AZ 1010/NZ 1008

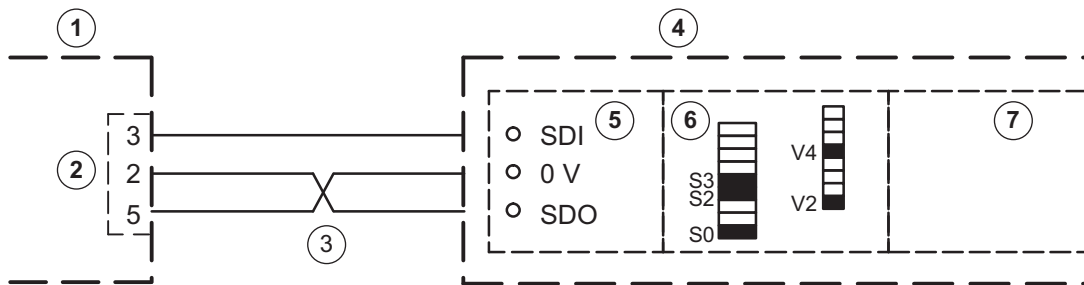


<b>Bridge assignment (V) on the SMA</b> Plug-in bridge V1 in pos. 1/2 Level for V.24 interface	Connect shielding wire to AZ 1010/NZ 1008 only. Cable J-Y (St) Y 2x2x0.6
--	---

1	Video system	4	Range max. 1000 m
2	COM x	6	GOM
3	OVS	7	LNA
5	AZ 1010/NZ 1008		

### 9.11.5 Connecting to NZ 1012

#### V.24 connection to NZ 1012



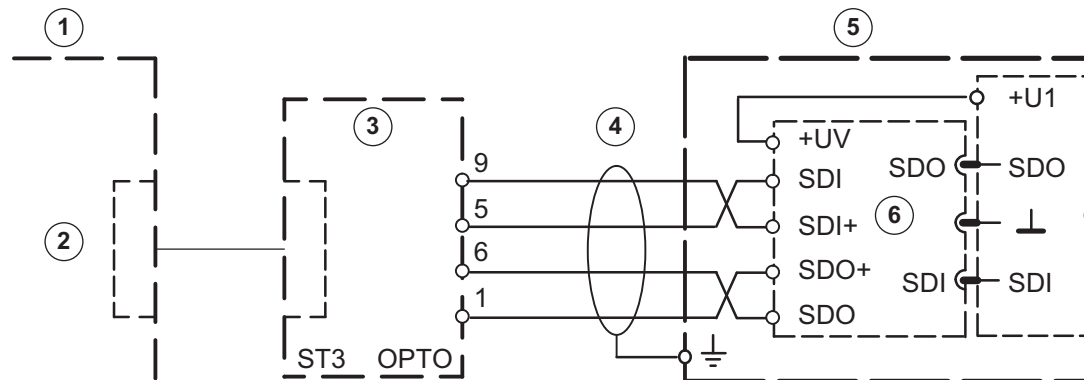
1	Video system	5	EAN
2	COM x	6	SSM
3	Max. 25 m	7	ZSN SW issues: 18508.0 A8.1, 18508.1 A8.1
4	NZ 1012		

Dip-Fix assignment (S) and bridges (V) on the SSM			
Interface 1:		Interface 2:	
S0	On: 1200 baud	S4	On: 1200 baud
S1	Off: Video system	S5	Off: Video system
S2	On: Transmission priority for NZ 1012	S6	On: Device is connected
S3	On: Device is connected	S7	On: Transmission priority for NZ 1012
V2, V4	Connected V.24 interface	V12, V14	Connected V.24 interface
:		:	



**NOTICE!**  
It is possible to connect to interface 2.

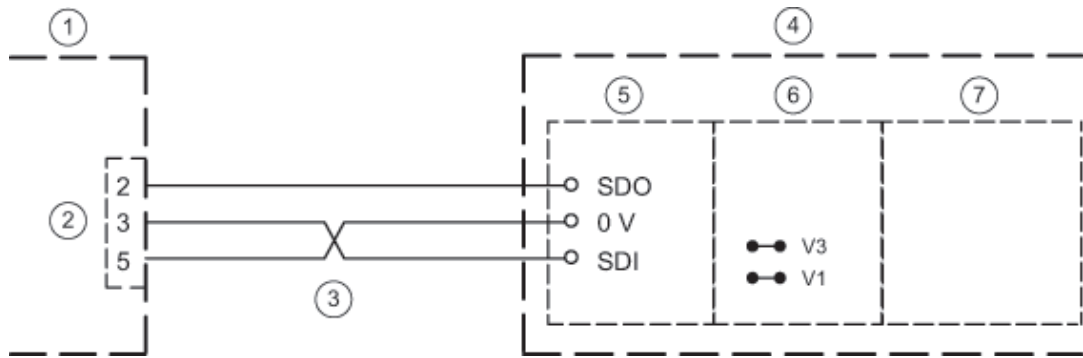
#### 20 mA connection to NZ 1012



1	Video system	5	NZ 1012 (insert SSM bridges at 20 mA)
2	COM x	6	GOM
3	OVS	7	EAN
4	Range max. 1000 m		

### 9.11.6 Connecting to NZ 1060

#### V.24 connection to NZ 1060

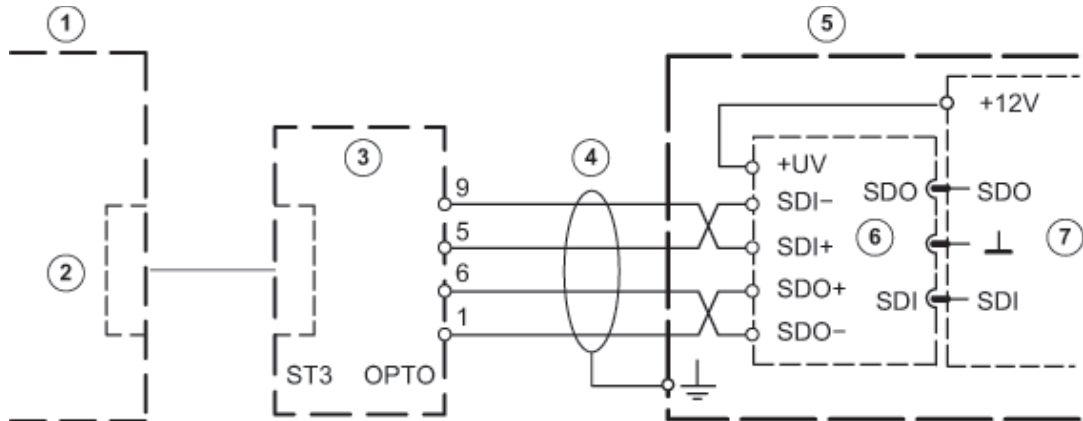


1	Video system	5	ZAN
2	COM x	6	SIE
3	Max. 25 m	7	ZVE (SW issues: 18033.0 A6.2, 18033.2 A6.2, 18033.3 A6.2)
4	NZ 1060		

Ideally, interfaces 6 to 9 should be used; connection to interfaces 2 to 5 is also possible on a project-specific basis.

Program the appropriate interface to AUX (1200 baud), insert bridges at SIE (V1, V3) for V.24 interface.

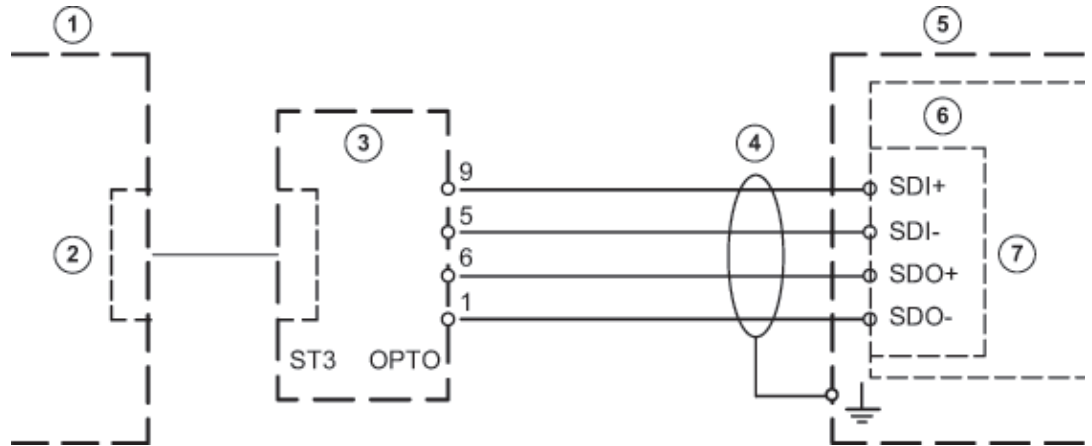
#### 20 mA connection to NZ 1060



1	Video system	5	NZ 1060
2	COM x	6	GOM
3	OVS	7	ZAN
4	Range max. 1000 m		

Ideally, interfaces 6 to 9 should be used; connection to interfaces 2 to 5 is also possible on a project-specific basis. Program the appropriate interface to AUX (1200 baud), insert bridges at SIE (V2, V4) for 20 mA interface.

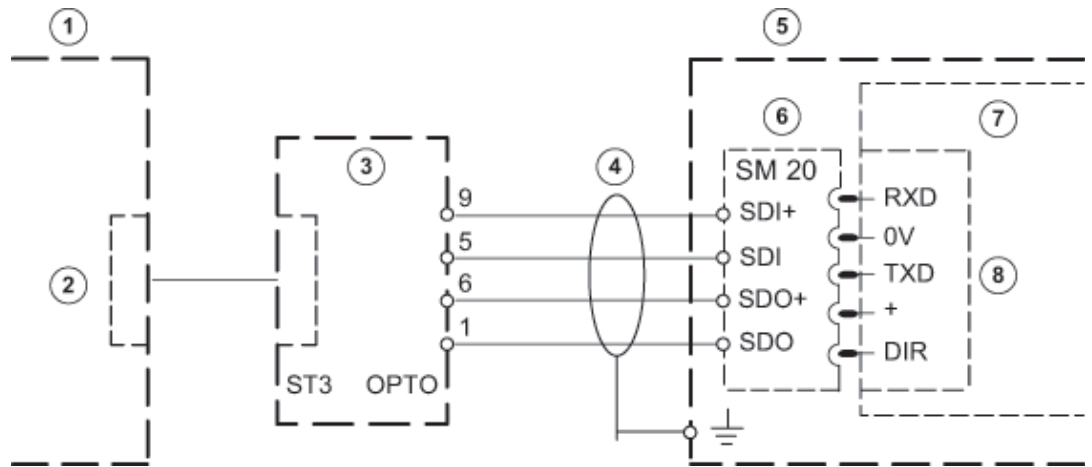
### 9.11.7 Connecting to UEZ 1000 (20 mA)



1	Video system	5	UEZ 1000
2	COM x	6	AVK
3	OVS	7	20 mA-1 to 20 mA-3
4	Range max. 1000 m		

Connect shielding wire to UEZ 1000 only.  
 Installation cable J-Y (St) Y 2x2x0.6

### 9.11.8 Connecting to UEZ 2000 (20 mA)



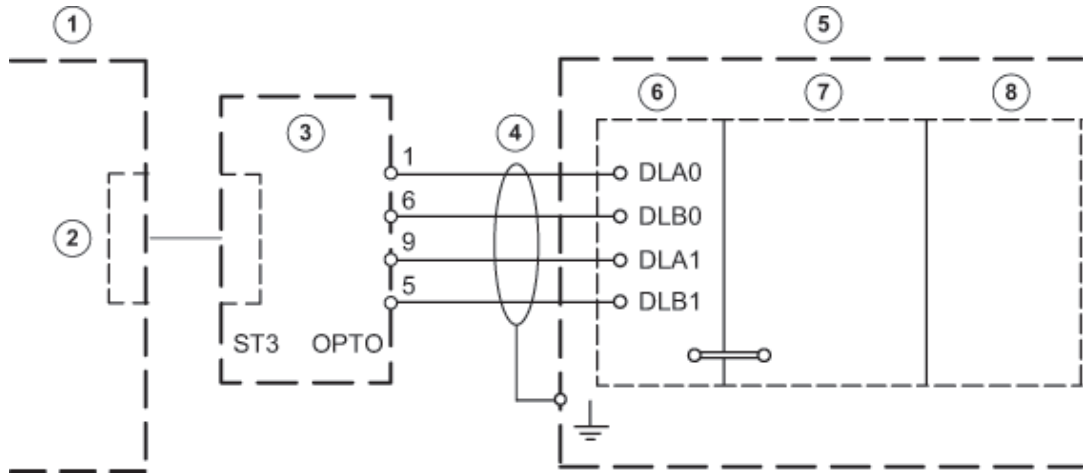
1	Video system	5	UEZ 2000 LSN
2	COM x	6	SM 20
3	OVS	7	AVM 100
4	Range max. 1000 m	8	COM 1 to COM 5

Connect shielding wire to UEZ 2000 only.  
 Installation cable J-Y (St) Y 2x2x0.6

COM 4 and COM 5 only with interface assembly SEMO1

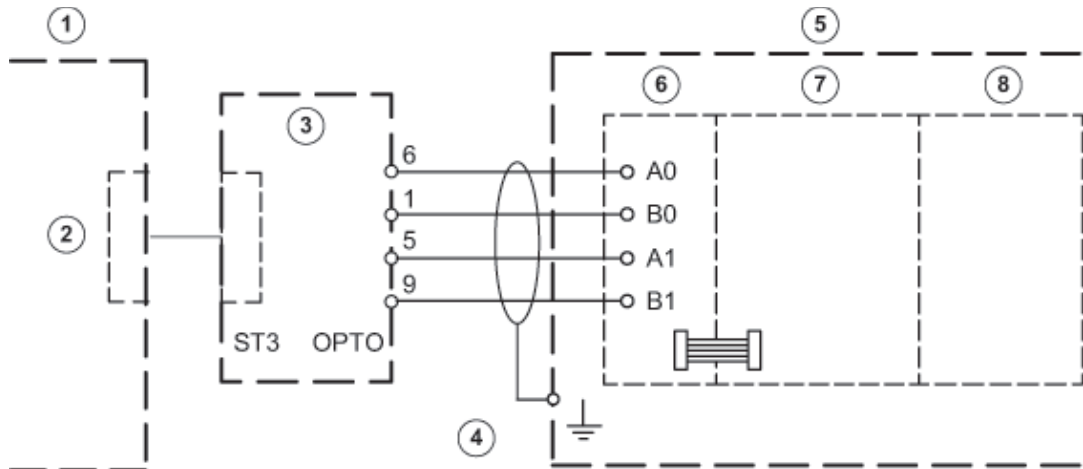
### 9.11.9 Connecting to UGM 2020

#### 20 mA connection to UGM 2020 via TESP (for Telephony)



1	Video system	5	UGM 2020
2	COM x	6	TESP (Br. 1-4 open)
3	OVS	7	SGK (SW issues: SGKUGM)
4	Range max. 1000 m	8	EPC/EPC2 (from EAPS-4, EAPS-5)

#### 20 mA connection to UGM 2020 via UESS



1	Video system	5	UGM 2020
2	COM x	6	UESS (power surge protection)
3	OVS	7	SGK (SW issues: SGKUGM)
4	Range max. 1000 m	8	EPC/EPC2 (from EAPS-4, EAPS-5)

## 10 Troubleshooting and Checks

This chapter outlines the causes of malfunctions that you may encounter when installing or operating the system. If you are unable to remedy the malfunction, please consult the video system manufacturer's product service video.

### 10.1 Troubleshooting

Malfunction	Possible cause	Solution
Device stops during the computer's boot phase.		Restore system. To do this, use the recovery CD.
The DiBos software application stops.		<b>Note:</b> Only send back the system if the recovery procedure was unsuccessful.
There is a message stating that there are files on the drive that cannot be accessed.	There are corrupt sectors or corrupt files on the drives.	Check the affected drives using the <b>Chkdsk</b> program. Delete the affected files. Also delete the directories in which the corrupt files are located.  If this is not successful, the system must be restored using the recovery CD. <b>Note:</b> A list of the corrupt files is created in the DB server log file each time DiBos is started up.
All cameras are crossed out.	No video signal available.	Replace grabber card.
	The grabber card is faulty.	Check video signal.
Network connection cannot be established and cameras are crossed out.	Computer name is assigned more than once.	Do not assign the computer name more than once.
	IP address is incorrect.	Enter correct IP address.
	Firewall is activated.	Deactivate the firewall or, if this is not possible, use UDP tunneling.
All AP inputs have been sounding for more than 10 seconds.	Interface error to AP.	Remedy interface error.
<b>Hardlock not found</b> message	Hardlock (dongle) missing or feature not enabled.	Plug in dongle or add feature.
Camera video signal missing.	No video signal available.	Check video signal.
Images cannot be written.	Images have been written in too many archives.	Modify recording.
Software feature not working.	Check dongle is enabled.	Dongle enabling can be seen in the configuration.

Malfunction	Possible cause	Solution
External hard disks are not recognized by the system.	Terminator missing.	Plug in terminator.
	Hard disk ID used twice.	Set hard disk IDs in ascending order.
	Disks are not formatted.	Format disks for NTFS in Disk Manager.
No ISDN connection available.	Transmitter and receiver connection passwords do not match.	Check connection passwords.
	Wrong protocol is set.	Select appropriate protocol (EURO-ISDN) via an ISDN-PCI setup.

## 10.2 Checking the Optional Network Connection

### Information on networking

To install and test the network, you will require the following information from the network provider:

- IP address
- Subnet mask
- (Gateway)

### Notes on testing the network

To install and test the network, use the following test program:

1. Select **Start -> Programs -> Accessories -> Command Prompt.**
2. The commands available include:

#### **ping**

This command is only available if the TCP/IP protocol is installed.

#### **ping localhost**

This program checks the communication to the computer it is running on.

#### **ping <remote station name> or**

#### **ping <remote station TCP/IP address>**

The program checks the communication to the remote station.

#### **arp -a**

The program displays other computers after making contact with them.

#### **ipconfig**

Shows all current TCP/IP network configuration values (IP address, subnet mask, default gateway)

#### **tracert <remote station name>**

This program determines the path taken to a destination.

#### **net view**

Displays all available remote stations.



### **NOTICE!**

Ping does not work if UDP tunneling is activated in the configuration.



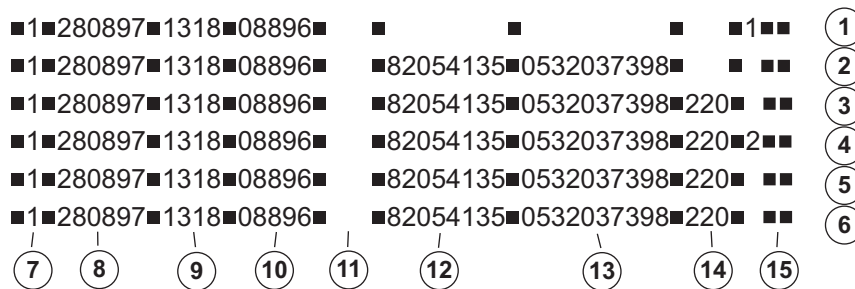
### 10.3 Checking the Optional ATM Connection

The data telegram between the video system and ATM can be checked using the **HyperTerminal** program in Windows® XP.

- Start the program using the menu **Start > Programs > Accessories > Communications > HyperTerminal**.
- When the program has started, enter a name (test name) in the dialog box and confirm the entry.
- In the following dialog box, select the interface to which the interface processor is connected (**Connect using** input field). Confirm with **OK**.
- Enter the following parameters:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
 Confirm the entries with **OK**.
- In the **File -> Properties -> Settings -> ASCII-Setup** menu, activate the **Append line feeds to incoming line ends** check box. Confirm with **OK**.

The HyperTerminal configuration is finished. The data can now be evaluated.

**Data telegram between video system and interface processor:**



1	Card in ATM	8	Date
2	Card recognized by ATM	9	Time
3	Enter amount	10	Transaction number
4	Hand to cash	11	Machine number
5	Removal of cash	12	Bank sort code
6	End of transaction	13	Account number
7	Interface number (0 - 3 for ATM1 - ATM4)	14	Amount
		15	Camera number/Action

**NOTICE!**



Action 1 = **Card in ATM** message

Action 2 = **Hand to cash** message

For some ATMs, a message is generated as soon as the card is inserted, but does not display BRC or account number. For other ATMs, the message is not generated until the BRC and account number have been read and the PIN number has been entered correctly.

## 10.4 Checking the Optional Web Connection

After activating the web application, check that you actually have access.

Proceed as follows:

1. Start the web browser (Internet Explorer 5.x and above).
2. In the browser, enter `http://<hostname>` under address. As `<hostname>`, specify either the IP address or the name of the computer on which the web server is installed.  
The video system web application log-on mask is displayed when the connection has been made. It is now possible to log on.

# 11 Notes on Service and Maintenance

## 11.1 Maintenance Work to be Carried Out

Perform the following maintenance work:

- On the video system itself:
  - check that all cables are connected firmly
  - check the fans and clean if necessary
  - clean the screen if dirty
  - check the system time and set if necessary
- Check the quality of the last five saved images per camera (e.g. sharpness, brightness, contrast).
- The images stored in the archives must be randomly checked (with regard to image quality and additional data)
- At least one trigger by a connected AP or a directly connected contact must be undertaken. The images placed in the archives as a result of this action must be checked and then deleted.
- The hard disk load must be checked. In agreement with the customer, it may be necessary to delete images.
- All freely accessible cameras and lenses as well as dome cameras and front screens of external cameras should be cleaned. While doing so, the connecting cables and plugs must be checked.
- The reference images printed or saved during installation of the system must be compared with the live images of the corresponding cameras with regard to their alignment. The customer is answerable to the administrative association (BGV) with regard to setting the image frame size.
- A functional test in accordance with UVV Kassen must be carried out at least once per month. The SP 9.7/7 **Requirements for testing of optical room monitoring systems** must be taken into account.
- Checking of the customer-owned printer (1 printout).
- A test connection is to be set up for the ISDN connection.
- For ATM connection:
  - check the connecting cables on the interface processor and on the OVS
  - check the transmission of the transaction data
  - access control data display (check the access control connection cable)
- All work carried out is to be documented in the operating handbook.



### NOTICE!

All work on the system that affects recording may only be carried out with the prior agreement of the customer. For UVV-relevant devices, it is preferable that this work is carried out outside of counter opening times.

If defective, the system (without dongle) is to be exchanged. A loan device will be made available by the video system manufacturer during this time.

### Maintenance work to be carried out by the operator

The operator must:

- replace the toner cartridge for laser printers,
- replenish printer paper or the video printer paper cartridge, and
- replace the color cartridge for ink jet printers.

## 11.2 Software Update

Installation of the software is carried out principally as Windows® XP Administrator.

## 11.3 Troubleshooting

The following malfunctions are to be fixed if applicable:

- Backlighting:  
If backlighting effects are identified during recording, the light source must be covered up, for example using curtains over windows or lampshades on lighting; alternatively, the location of the camera should be changed.
- Reflections:  
If the optical room monitoring system is enclosed in bulletproof or toughened glass, the lighting conditions may cause reflections. These become stronger as the degree of light within the glass enclosure increases. Such reflections can be reduced by increasing the illumination of the area outside the glass enclosure and positioning the cameras closer to the glass. Reflections can also often be avoided by covering light sources behind or next to the camera. If these measures do not help, a polarization filter can be fitted in front of the lens.
- Sharpness:  
When checking recordings, care should be taken that persons and objects are sharply delineated within the defined recording zone. To improve the image sharpness, "gray" or ND filters can be placed in front of the lens.
- Contamination:  
The quality of the recordings is frequently affected by dirt on the lens or the window of the security housing.

Errors or functional problems can be fixed by

1. disconnecting and reconnecting the local or remote connection in the video system program
2. exiting the program and booting it again, or
3. warm starting or switching the system off and then on again (with a wait time of approximately twenty seconds).

If this does not restore normal operation, the configuration must be checked.

If the malfunction cannot be fixed, the system must be replaced.



**Bosch Sicherheitssysteme GmbH**

Robert-Koch-Straße 100

D-85521 Ottobrunn

Germany

Telefon +49 89 6290-0

Fax +49 89 6290-1020

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

© Bosch Sicherheitssysteme GmbH, 2009