Installation and Configuration

English

HD Dome Camera

DDF4820HDV-DN

Rev. 1.0.2 / 2013-09-09

Dallmeier

Information about Copyright, Trademarks, Design Patents

We reserve the right to make technical modifications.

The manufacturer accepts no liability for damage to property or pecuniary damages arising due to minor defects of the product or documentation, e.g. print or spelling errors, and for those not caused by intention or gross negligence of the manufacturer.

Dallmeier electronic GmbH & Co.KG
Cranachweg 1
93051 Regensburg, Germany

www.dallmeier.com
info@dallmeier.com

Table of Contents

1 Introduction

1.1 Validity

This document applies to the following HD network cameras:

- **DDF4820HDV-DN-IM**
  (in-ceiling mount variant)
- **DDF4820HDV-DN-SM**
  (surface mount variant)

The descriptions in this document are based on the software version **6.3.2.5** and apply to all above-mentioned devices.

If text passages require distinctions to be made between the devices, the complete product names will be mentioned.

Pictures in this document may differ from the actual product.

1.2 Documents

Commissioning

The document entitled “Commissioning” contains the most important steps for the connection and commissioning of the respective device.

Installation and Configuration (this document)

This document contains detailed descriptions of the installation, connection, commissioning and configuration of the above-mentioned devices.

In addition, safety instructions, general notes and technical data/drawings are provided.

The target audience is trained and authorized professionals (installers).

1.3 Typographical Conventions

This document may contain various warning words and symbols that indicate potential sources of danger.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE indicates practices for preventing property damage, incorrect configurations or faulty operations.

For reasons of clarity and readability, various text formatting elements and types of emphasis are used in this documentation:

Instructions are indicated by arrows (➢).

➢ Always carry out instructions one after the other in the sequence described.

Expressions in ***bold/italics*** generally indicate a control element on the device (switches or labels) or on its user interface (buttons, menu entries).

Paragraphs in italics provide information on basic principles, special features and efficient procedures as well as general recommendations.

2 Safety Instructions

Only use the units described in this document if they are technically in proper working condition and for the intended purpose while keeping safety and potential dangers in mind.

Qualified Personnel

The installation, mounting, connection, commissioning and configuration of the units may only be carried out by qualified personnel.

This also applies to the maintenance, testing and repair, whereat the regulations of the DIN VDE 0701 series of standards (repair, modification and inspection of electrical appliances) must be followed.

Regulations

The use of video and audio surveillance systems is, in general, strictly regulated.

Inform yourself about the currently valid laws and regulations regarding data, worker and environmental protection before using the units and ensure compliance with them.

System Components

Only use internal components that have been tested and approved by Dallmeier.

Inappropriate internal components may cause malfunctions, damages and data loss and may result in the loss of warranty.

Modifications

Do not make any modifications to the hardware or software that have not been tested and approved by Dallmeier.

Inappropriate modifications may cause malfunctions, damages and data loss and may result in the loss of warranty.

Documentation

Read the documents included in the delivery carefully and thoroughly.

Always observe the contained instructions, notes and warnings.

Condensation Water

If the units are brought from a cold to a warm environment, resulting condensation water may cause malfunctions and damages.

In this case, wait (up to 8 hours) until the units have reached room temperature before commissioning.

Earthing & Equipotential Bonding

For the safety of persons (protection against dangerous contact voltages) and devices (protection against overvoltages) and the immunity of information and communication technology equipment to electromagnetic interferences (EMI), all protective measures, which are specified by the currently valid DIN, VDE and ISO standards and which provide for a standard-compliant earthing and a correct equipotential bonding of electrical and electronic devices, are mandatory and must be fulfilled by all means.

Lightning Storms

To avoid damage to the units by electrical surge during lightning storms, unplug the units from the mains power supply (pull out the power plug).

This is also recommended, when the units have been unused for a long period of time.

Operating Conditions

Unfavourable operating conditions may shorten the life of the units and may cause malfunctions, damages and data loss and may result in the loss of warranty.

Observe the specifications given in the technical data, the operating condition requirements and the maintenance instructions.

Shocks

Shocks may cause malfunctions and damages.

The units may not be moved while in operation.

Foreign Bodies

If objects or liquids get into the units, immediately disconnect them from the power supply (pull out the power plug).

Contact the sales partner responsible for your area.

Burnt Smell

If you notice burnt smell or a formation of smoke coming from the units, immediately disconnect them from the power supply (pull out the power plug).

Contact the sales partner responsible for your area.

Opening

The housings of the units may only be opened by qualified personnel for commissioning, inspection, maintenance and repair.

Disposal

Do not dispose waste electrical and electronic equipment into the household trash.

Disconnect the units from the power supply.

Remove all connected devices.

Return the units to your respective sales partner.

3 General Notes

3.1 Scope of Delivery

Included in the standard scope of delivery is:

1× HD network camera (depending on the product ordered)
1× Documentation “Installation and Configuration” (published on CD-ROM)
1× Documentation “Commissioning” (published in print and on CD-ROM)

In addition, all screws and dowels that are necessary for a proper installation of the ordered HD network camera are included.

The scope of delivery may differ depending on the ordered equipment, the device variant or the country of destination.
The functional range of the devices depends on the ordered equipment or device variant and may differ from this document’s content.
Certain functions and features may require the purchase of an additional license.

3.2 Transportation and Packaging

Store the original packaging for transportation at a later date.
Dallmeier is not responsible for any damage resulting from unprofessional/improper transportation.
The goods should only be shipped in their original packaging.
If the original packaging is no longer available, ensure that the packaging used sufficiently protects the units against damage, moisture, heat and cold.

3.3 Warranty

The terms and conditions valid at time the contract was signed shall apply.

3.4 Approvals/Certifications

The following approvals/certifications were valid for all devices described in this document at the time of this document’s compilation:

- CE
- FCC
- ACA
- UVV “Kassen” (DGUV Test)
- UL
- DIN 50130-4 compliant

Visit www.dallmeier.com for possible updates.

3.5 Appropriate Use

DDF4820HDV-DN-IM

The DDF4820HDV-DN-IM (in-ceiling mount variant) is a 3-megapixel HD network camera built into a vandal-resistant (IK10) dome enclosure.

It is exclusively designed for indoor installations in suspended ceilings and can be powered via PoE (Power over Ethernet Class 0, IEEE 802.3af) or supplied with 12 V DC (separate power supply unit required).

DDF4820HDV-DN-SM

The DDF4820HDV-DN-SM (surface mount variant) is a 3-megapixel HD network camera built into a vandal-resistant (IK10) dome enclosure.

It is designed for indoor installations on ceilings and walls and can be powered via PoE (Power over Ethernet Class 0, IEEE 802.3af) or supplied with 12 V DC (separate power supply unit required).

3.6 Performance Features

The following list of features is valid for all devices described in this document:

- 1/2.5" 5-megapixel CMOS image sensor
- Pure Digital Signal Processing
- Real-time Full HD video (1080p/30)
- Automatic Day/Night switching using ambient light sensing and ICR[1)] function (switching threshold level adjustable)
- High light sensitivity of 0.45 lux (at F0.95, 50 IRE, ICR[1)] On)
- Motor-driven megapixel varifocal lens
- Zoom, focus and iris control conveniently adjustable via web browser
- One-Push AF (Autofocus) with manual fine adjustment
- P-Iris control
- Resolution: SD (up to D1), HD (720p, 1080p, 2 MP, 3 MP)
- Video compression: H.264, MJPEG
- Frame rate up to 30 fps
- Simultaneous Dual- or Tri-Streaming
- Automatic White Balance (ATW, One-Push AWB)
- Manual White Balance (MWB)
- Automatic Gain Control (AGC)
- Automatic Electronic Shutter (AES)
- Comprehensive set of image optimization functions, such as brightness, contrast, saturation and sharpness
- 3D Digital Noise Reduction (3D DNR)
- Three different exposure metering modes:
  average metering (light information from entire scene),
  centre-weighted average metering and spot metering
- Privacy Zone Masking (hiding/masking of protected areas)
- Flip function (horizontal, vertical or both)
- Digital Image Shift[2)]
- Alarm notification via e-mail and FTP image upload
- Analogue video preview output (CVBS)
- Audio OUT[3)] / Microphone IN[3)]
- Voltage supply with 12 V DC or via PoE (Class 0, IEEE 802.3af)
- Low power consumption (max. 4.5 W)
- Compact vandal-resistant (IK10) housing
- ONVIF compliant
- DIN EN 50130-4 compliant

For device-specific features, see the relevant product data sheet.

1) ICR = IR Cut Filter Removable
2) Digital Image Shift = Provides digital fine alignment of the image section
3) Audio IN/OUT Y-Cable Connector FGA-30 required (optionally available).

4 Requirements

4.1 General

Unfavourable local conditions may shorten the life of the products and may cause malfunctions or damages.

➢ Do not install/operate the devices in places

- with a large amount of dust and dirt,
- with steam or oil vapours (e.g. kitchen),
- with direct sunlight,
- with strong heat emissions (e.g. radiator),
- with improper ambient temperatures,
- near sources with strong radiation (e.g. radio transmitters, magnetic fields),
- with corrosive surroundings (e.g. gases, salt water),
- with insufficient air ventilation (e.g. closed cabinet).

4.2 Power Supply

The devices can be powered via PoE (Power over Ethernet, Class 0) or supplied with 12 V DC (separate power supply unit required).

➢ Ensure that the existing network supports the PoE standard IEEE 802.3af if you want to supply the devices with power over Ethernet.

4.3 Earthing & Equipotential Bonding

For the safety of persons (protection against dangerous contact voltages) and devices (protection against overvoltages) and the immunity of information and communication technology equipment to electromagnetic interferences (EMI), all protective measures, which are specified by the currently valid DIN, VDE and ISO standards and which provide for a standard-compliant earthing and a correct equipotential bonding of electrical and electronic devices, are mandatory and must be fulfilled by all means.

4.4 Operation

➢ Observe the following notes for the operation of the devices:

- If the devices or the cables connected to the devices are located near sources with strong radiation, the video image may be distorted.
- The devices are equipped with an automatic gain control (AGC). In low light conditions the image may be altered (e.g. noise). However, this is not a malfunction.
- The quality of the video image depends on the lens, the lighting conditions and the used monitor.
- The accuracy of the automatic white balance (AWB) algorithm depends on the lighting used. Mixed light (consisting of artificial light and daylight) may cause colour distortions (inaccurate colour reproduction).
- Poor lighting can lead to a faulty white balance.

4.5 Outdoor Use

4.5.1 DDF4820HDV-DN-IM

The DDF4820HDV-DN-IM (in-ceiling mount variant) is exclusively designed for indoor installations.

An outdoor installation is prohibited and may result in malfunction, damage, data loss and loss of warranty.

4.5.2 DDF4820HDV-DN-SM

The DDF4820HDV-DN-SM (surface mount variant) is designed for indoor installations.

However, an outdoor installation may be permitted, but only in compliance with the following instructions/recommendations:

- Use only IP67 (Ingress Protection 67) approved components and assemblies.
- Always use the delivered O-rings.
- Adhere the delivered adhesive-backed gasket to the bottom of the housing base.
- Always use the delivered cable gland (or equivalent) for the cable feedthrough.
- Protect the device from direct influence of weather conditions (rainfall, direct sunlight, etc.).
- Always use a protected installation site (e.g. under a canopy).
- For wall mount installations, align the camera housing with the cable gland pointing down whenever possible.

5 Views and Connection Assignment

5.1 In-ceiling Mount Variant (IM)

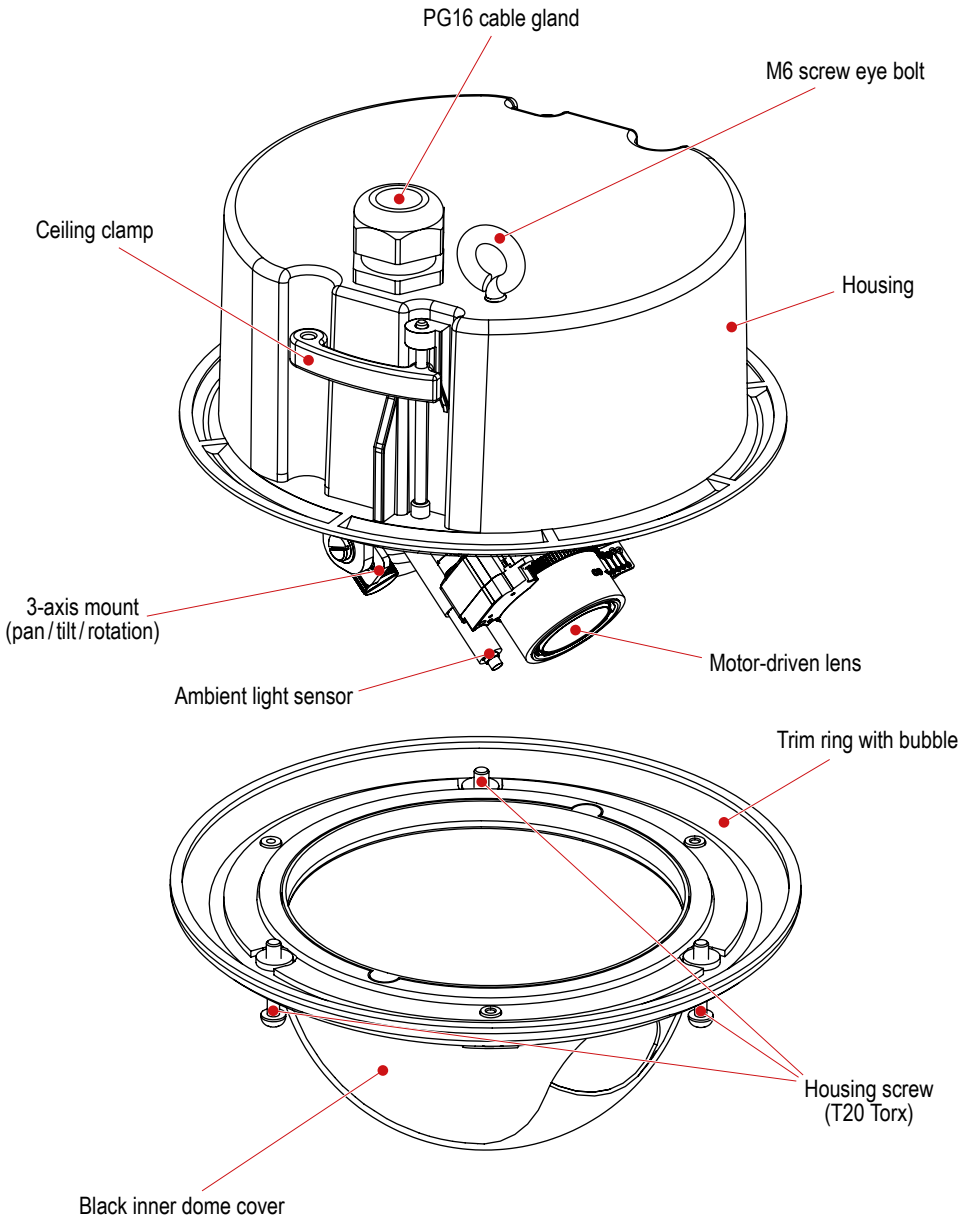


Fig. 5-1

NOTICE

Always ensure that the lens and the ambient light sensor are not covered by the black inner dome cover when assembling the camera enclosure.

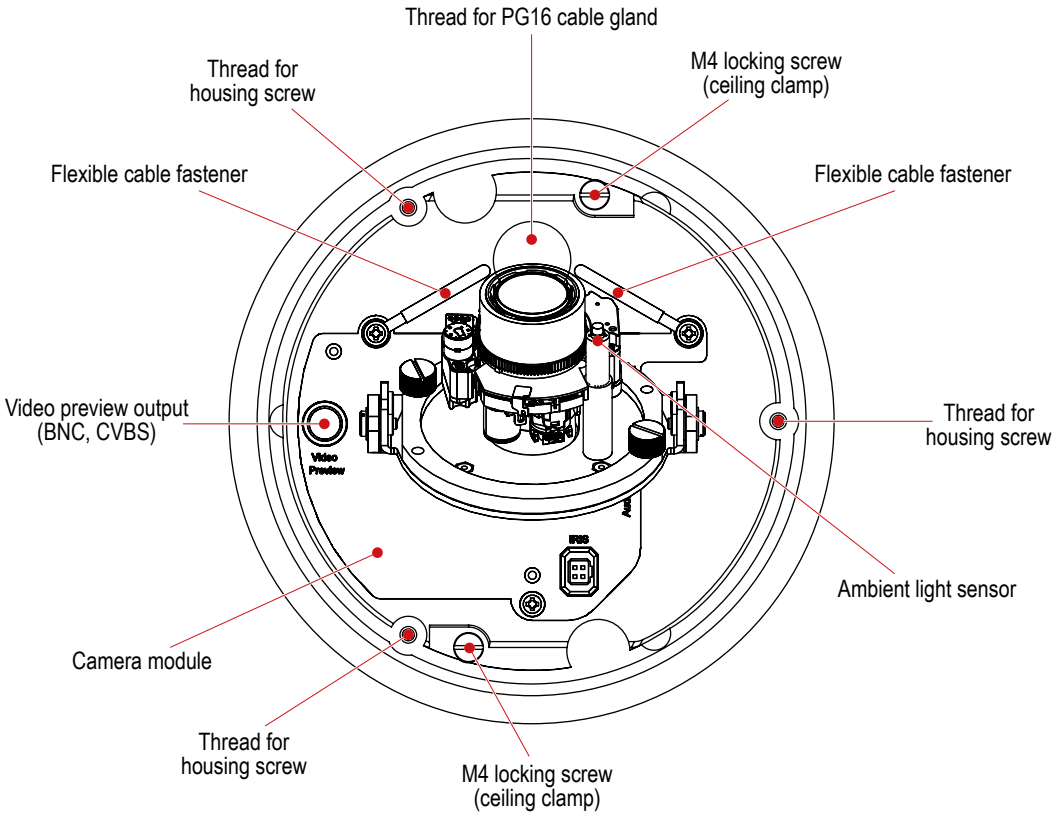


Fig. 5-2 Housing of in-ceiling mount variant (top view)

5.2 Surface Mount Variant (SM)

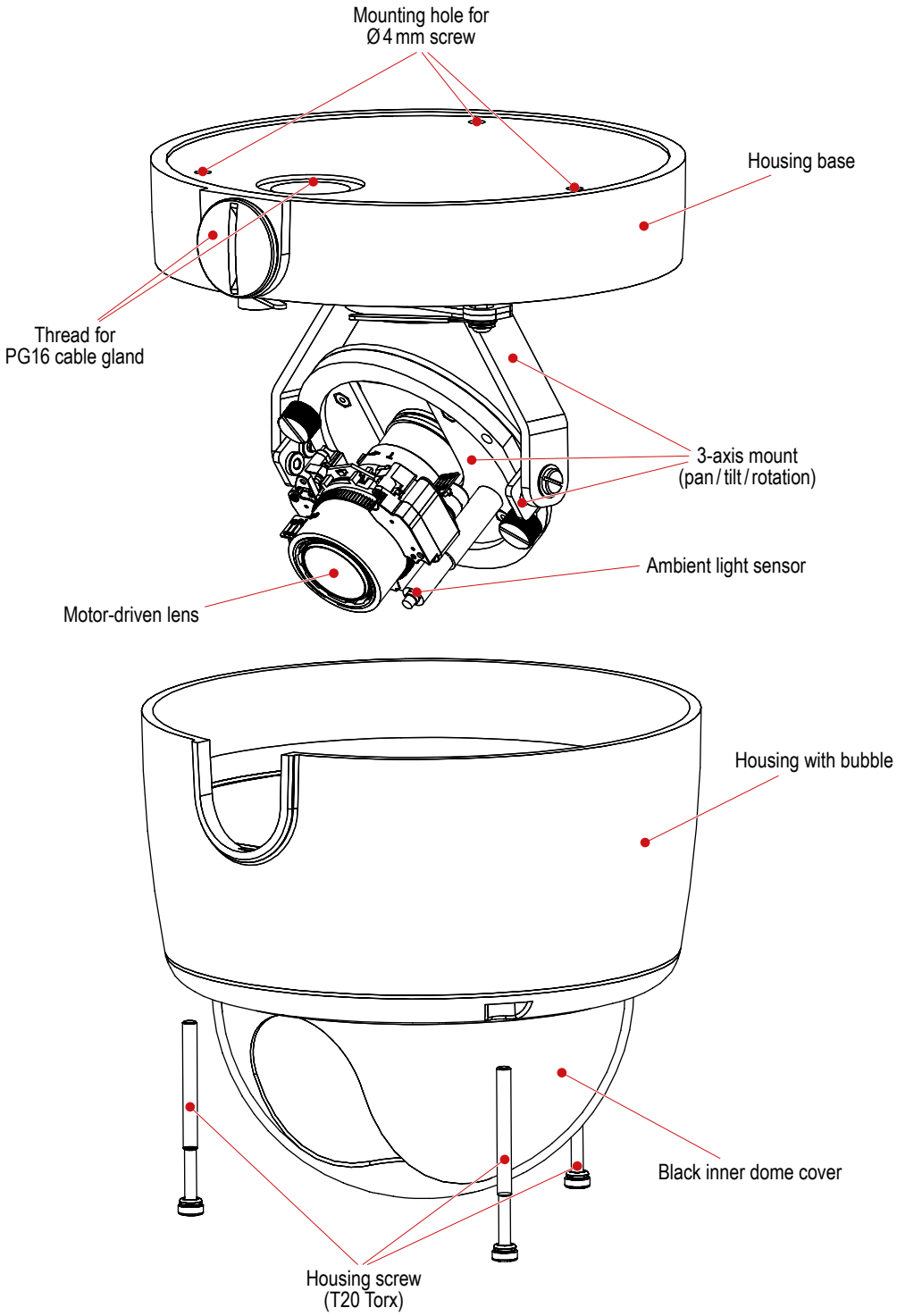


Fig. 5-3

NOTICE

Always ensure that the lens and the ambient light sensor are not covered by the black inner dome cover when assembling the camera enclosure.

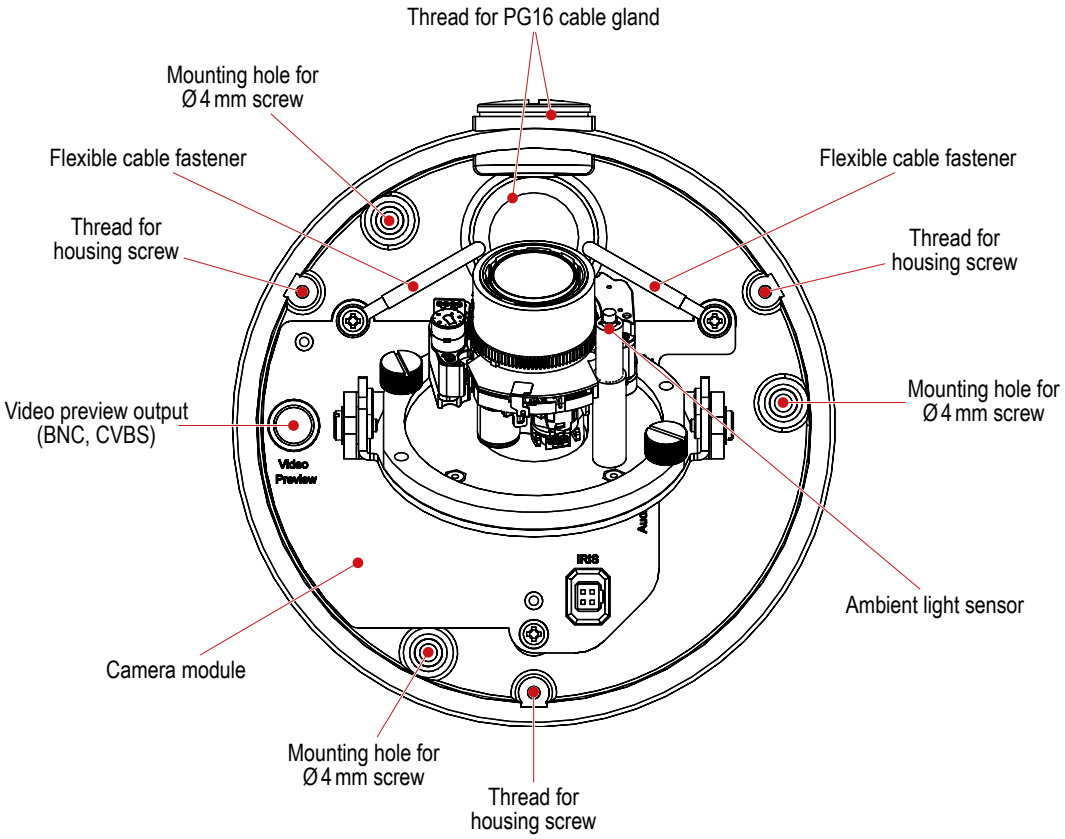


Fig. 5-4 Housing base of surface mount variant (top view)

5.3 Camera Module

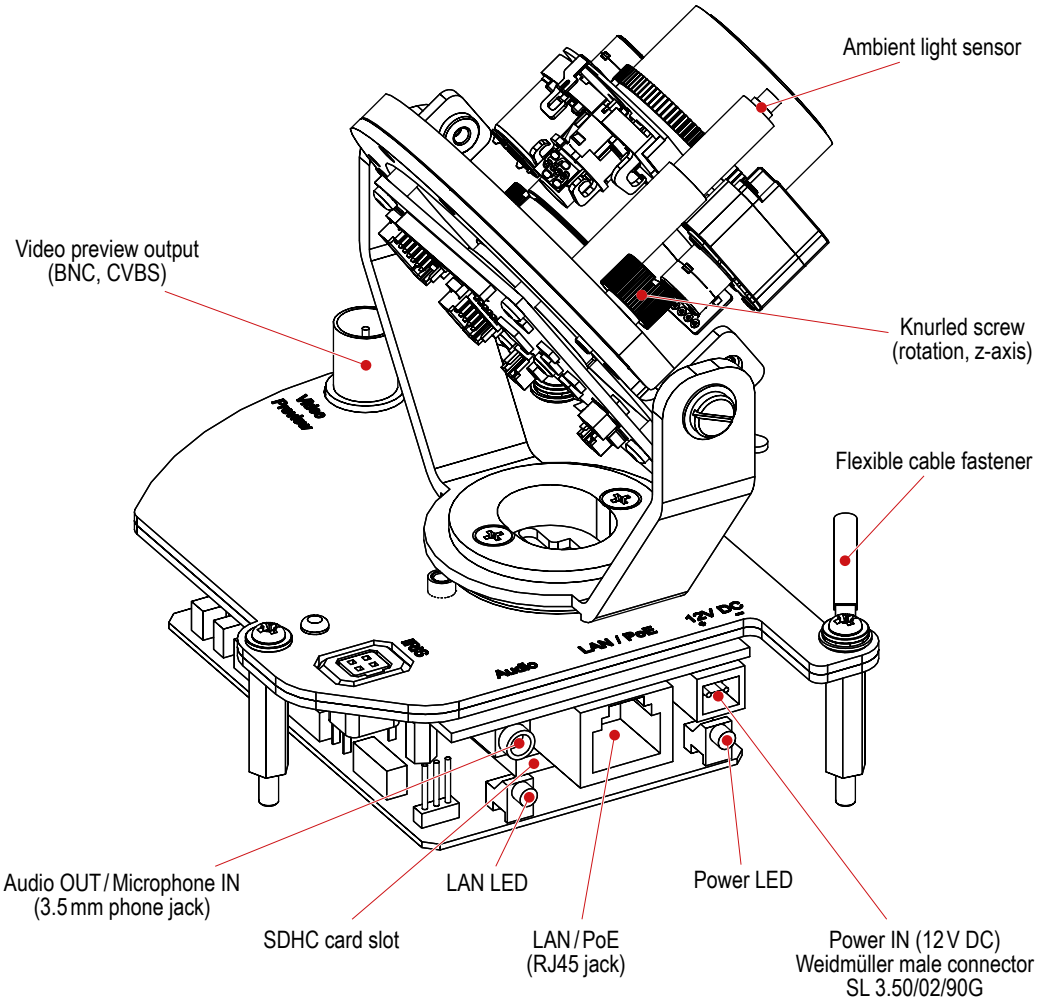


Fig. 5-5 Camera module with 3-axis mout (Pan ±90°, Tilt ±90°, Rotation 360°)

NOTICE

For a clean (interference-free) audio signal transmission, the Audio IN/OUT Y-Cable Connector FGA-30 is required (optionally available).

Always ensure that the lens and the ambient light sensor are not covered by the black inner dome cover when assembling the camera enclosure.

LAN LED Status

Red LED (constant): Critical error during update (*see below*)

Green LED (constant): Encoding active (Red LED off)

Green LED (blinking): Streaming of encoded data active

You can disable the LAN LED signal in the "WebConfig" user interface (see section "User Interface" on page 33).

The following LED states will occur during a successful update process:

Start of update process: All LEDs off
While update is running and during the critical phase: Red LED (blinking)
After successful update process until restart of system (5 – 10 sec.): Green LED
System restart: All LEDs off

Important:
If the update process has failed or the update was only partially executed, the Green LED phase will NOT occur.
Instead, the Red LED is illuminated until the restart of the system (5 – 10 sec.).

6 Installation and Commissioning

The installation and commissioning of the units may only be carried out by qualified personnel.

⚠ WARNING

Falling devices/objects or collapsing ceiling

Danger of death or serious injury to the head

- ➢ Observe the manufacturer's instructions about the maximum adequate carrying capacity of the supporting structure and the suspended ceiling or ceiling tiles.
- ➢ Use screws suitable for the ceiling/wall material.
- ➢ Use the correct type of anchor for your ceiling/wall type:
  - Plastic screw anchors for solid wall material (concrete/brick)
  - Toggle bolt style anchors for drywall / hollow wall type (plaster)

Electric shock hazard

Danger of death or serious injury

- ➢ Always disconnect the PoE switch or the separate power supply unit from the mains socket (pull out the power plug) before connecting or disconnecting the devices.

NOTICE

Damage to the units resulting from improper power supply

The devices can be powered via PoE (Power over Ethernet, Class 0) or supplied with a separate 12 V DC power supply unit.

However, always beware not to use both power sources simultaneously.

Damage to the lens units

Do not attempt to manually adjust the focal length (zoom) and the focus on the lens units.
The devices are equipped with a motor-driven varifocal lens.
The focal length (zoom) and the focus are adjusted over the network in the "WebConfig" user interface (see chapter "Lens Control" on page 87).

In order to comply with UL's requirements, always use a UL-certified, Limited Power Source (LPS) Class 2 power supply unit when operating the devices with a separate power supply unit.

6.1 In-ceiling Mount Variant (IM)

You need:

- Drywall utility saw or jigsaw
- M6 screw eye bolt
- T20 torx wrench
- Ceiling hook, safety wire and carabiner
- Phillips screwdriver (M4)

Step 1

➢ Cut a circular recess (Ø 143 mm) into the suspended ceiling using a drywall utility saw or a jigsaw.

➢ Screw the M6 screw eye bolt onto the bottom side of the housing.

➢ Unscrew the 3 housing screws using a T20 torx wrench and remove the trim ring.

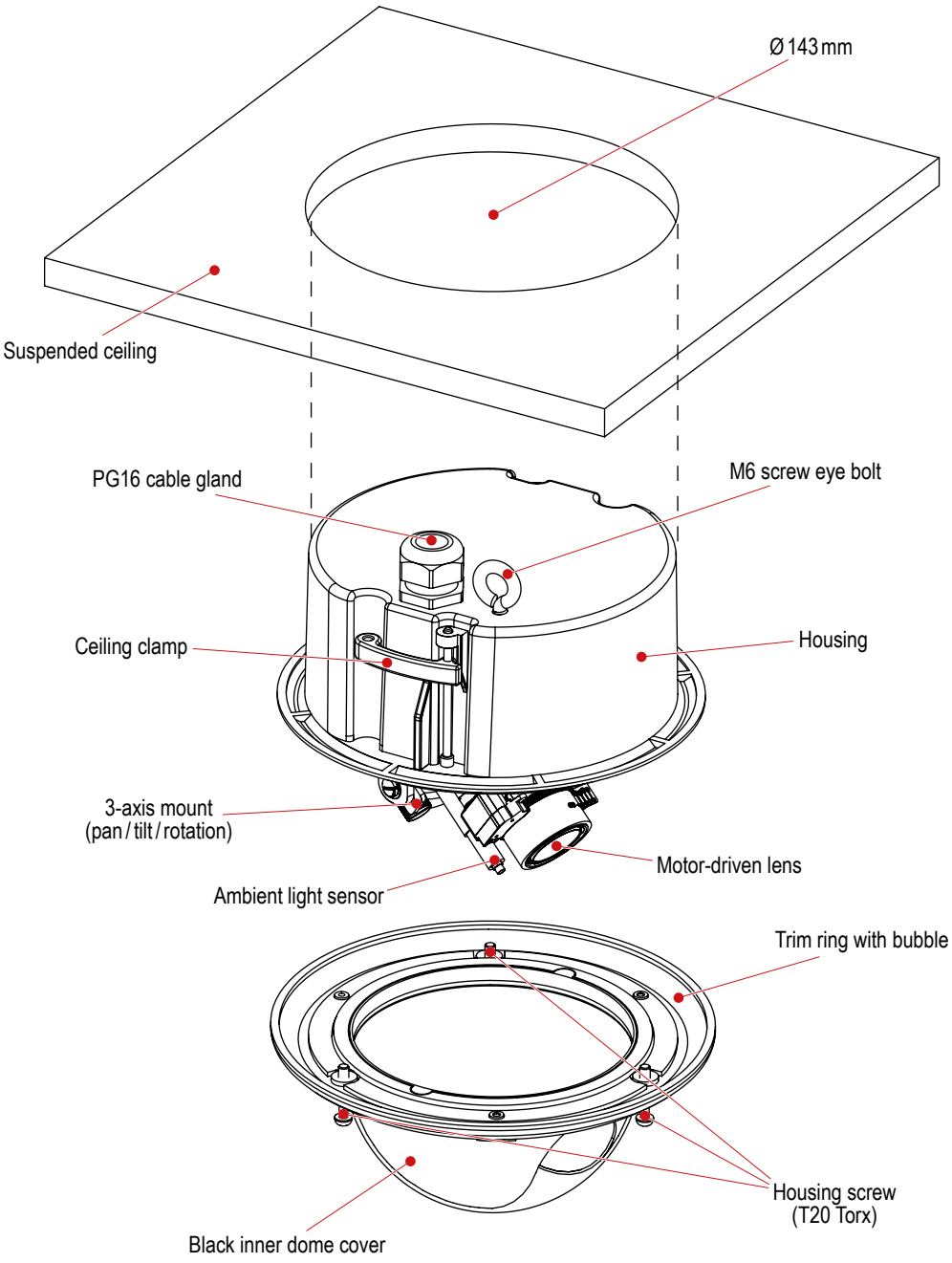


Fig. 6-1

Step 2

- Screw a ceiling hook on the supporting structure.
- Attach the safety wire to the M6 screw eye bolt (use a carabiner) and the ceiling hook.
- Run the required cables suspended from the ceiling through a PG16 cable gland.
- Screw the PG16 cable gland in the appropriate thread of the housing.
- Insert the housing into the circular recess.

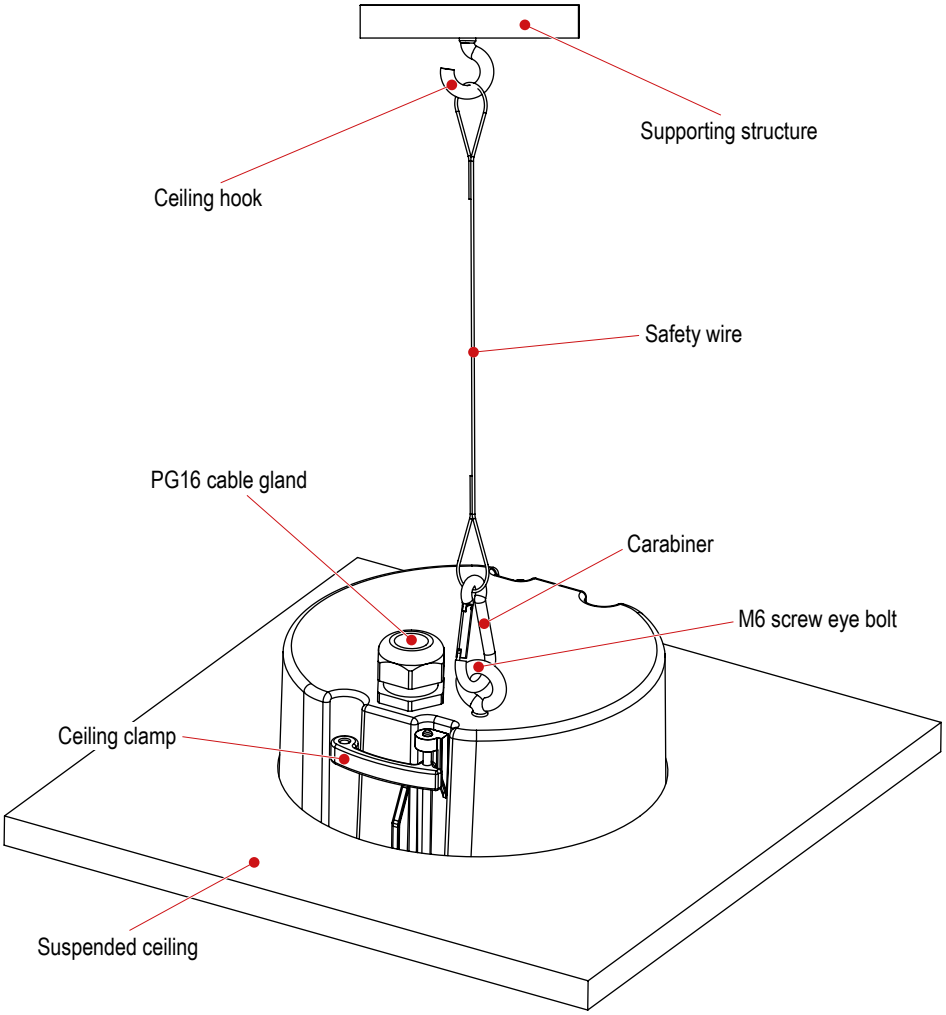


Fig. 6-2

Step 3

➢ Tighten the M4 locking screw (Fig. 5-2) of both ceiling clamps with a Phillips screwdriver until the housing is fixed (Fig. 6-4).

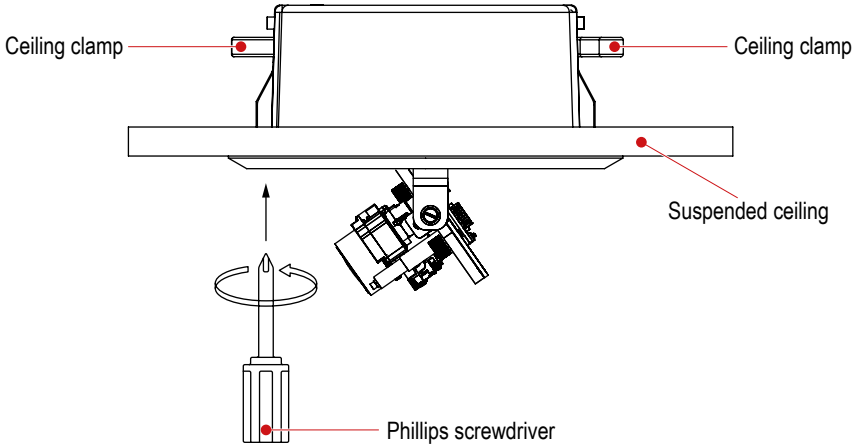


Fig. 6-3

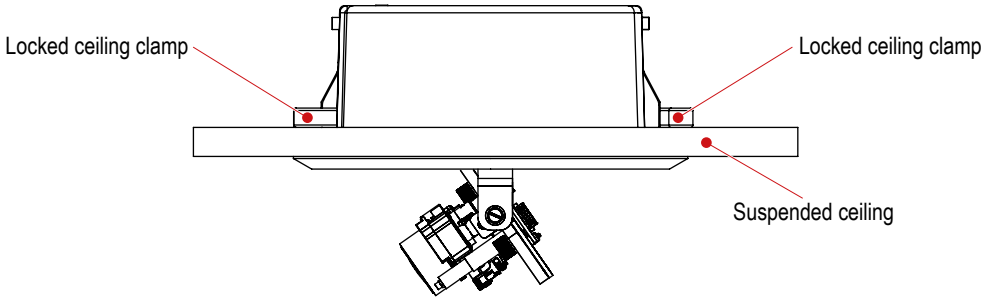


Fig. 6-4

Step 4

- Connect the required cables to the connectors of the camera module (see Fig. 5-5 and chapter “Pin Assignment” on page 98).
- If necessary, connect a CVBS monitor to the video preview output (Fig. 5-2).
- If PoE (Power over Ethernet) is not available, first connect the camera to a suitable power supply unit and then connect the power supply unit to the mains socket.
- Align the camera with your scene using the 3-axis mount.
- Login to the “WebConfig” user interface of the camera (see chapter “Connection and Login” on page 28).
- Click ***Lens control …*** in the configuration menu of the camera.
- Adjust the focal length (zoom) and the focus in the ***Lens Control*** dialogue box (see chapter “Lens Control” on page 87).
- Disconnect the CVBS monitor from the video preview output.
- Attach the trim ring to the housing while ensuring that the ambient light sensor is not covered by the black inner dome cover.
- Tighten the 3 housing screws using a T20 torx wrench.

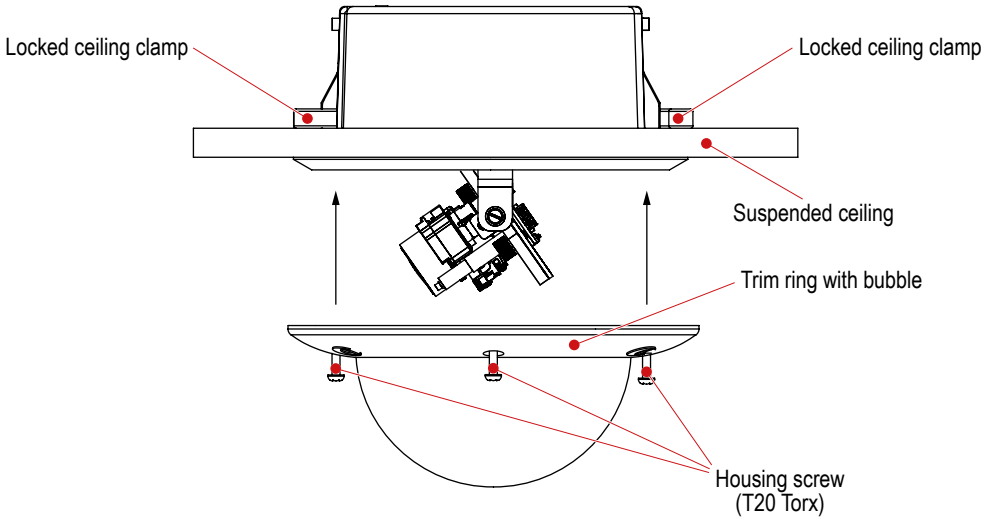


Fig. 6-5

6.2 Surface Mount Variant (SM)

The housing base is mounted with 3 screws (Ø4 mm) to the ceiling/wall.

You need:

- T20 torx wrench
- Marking tool (e.g. awl)
- 3 mounting screws (Ø4 mm)
- 3 anchors
- Electric drill
- Screwdriver

➢ Unscrew the 3 housing screws (Fig. 5-3) using a T20 torx wrench and remove the housing.
➢ Mark the drill holes on the ceiling/wall using the 3 pre-drilled mounting holes of the housing base (Fig. 5-4) as a template.
➢ At the marked locations, drill holes fitting the screws/anchors to be used.
➢ Push anchors suitable for the ceiling/wall material into the drill holes.
➢ Run the required cables suspended from the ceiling/wall through a PG16 cable gland.
➢ Screw the PG16 cable gland in the appropriate thread of the housing base.
➢ Mount the housing base with 3 screws to the ceiling/wall.

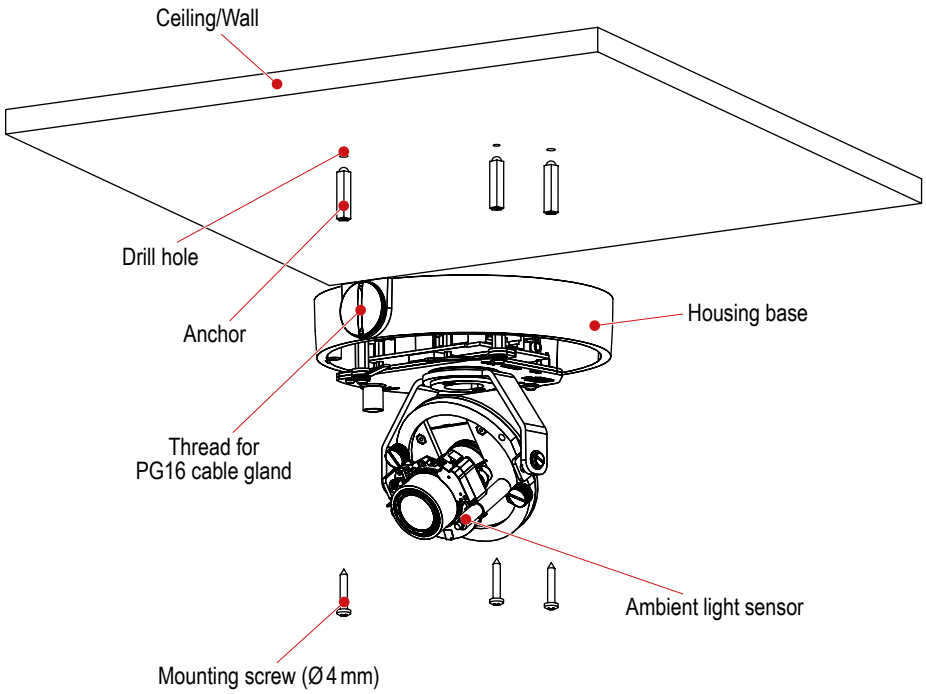


Fig. 6-6

➢ Connect the required cables to the connectors of the camera module (see Fig. 5-5 and chapter “Pin Assignment” on page 98).
➢ If necessary, connect a CVBS monitor to the video preview output (Fig. 5-4).
➢ If PoE (Power over Ethernet) is not available, first connect the camera to a suitable power supply unit and then connect the power supply unit to the mains socket.
➢ Align the camera with your scene using the 3-axis mount.

- Login to the “WebConfig” user interface of the camera (see chapter “Connection and Login” on page 28).
- Click ***Lens control …*** in the configuration menu of the camera.
- Adjust the focal length (zoom) and the focus in the ***Lens Control*** dialogue box (see chapter “Lens Control” on page 87).
- Disconnect the CVBS monitor from the video preview output.
- Attach the housing to the housing base while ensuring that the ambient light sensor is not covered by the black inner dome cover.
- Tighten the 3 housing screws (Fig. 5-3) using a T20 torx wrench.

7 Connection and Login

The configuration of the device is carried out with a PC/web browser via the local area network (LAN).

Alternatively, the PC can be directly connected to the device via an Ethernet crossover cable.

7.1 System Requirements

To configure the device with live video display and live audio output, the PC must meet the following minimum system requirements:

Computer	IBM*)-PC compatible
Operating system (OS)	Microsoft*) Windows*) XP Windows Vista*) Windows 7 (each with latest service pack)
Processor (CPU)	3 GHz Intel*) Pentium*) 4 AMD*) Athlon*) 64 3400+ or faster (or equivalent)
Random access memory (RAM)	1 GB (Windows XP) 2 GB (Windows Vista, Windows 7)
Graphics card	DirectX*) 9.0 or 10.0 compatible 64 MB of graphics memory (128 MB or higher recommended)
Sound	Sound card or on-board sound chip (min. 16 bit)
Ethernet	100 Mbps
Web browser	Microsoft Internet Explorer*) (latest version)
Software	Adobe*) Flash*) Player (latest version) JavaScript*) enabled Microsoft ActiveX*) enabled ActiveX-based Dallmeier control (latest version)

Note that

- a more powerful PC is required if several devices are configured with live video display (and/or live audio output) simultaneously.
- a DirectX compatible graphics card and the ActiveX-based Dallmeier control are not required for the configuration without live video display or live audio output.
- the ActiveX-based Dallmeier control can be directly downloaded from the device.
- the ActiveX-based Dallmeier control can be downloaded from the Dallmeier Partner Forum.
- the ActiveX-based Dallmeier control can be automatically downloaded via Internet after the connection to the device is established (only with Microsoft Internet Explorer and if it is not already installed).
- the configuration without live video display and without live audio output can be theoretically carried out with any operating system and web browser.
  However, the Adobe Flash Player is always required for the configuration.

7.2 Connection

The factory default IP address of the device is **192.168.2.28**.

- ➢ Ensure that the PC/web browser can establish a connection to the device via Ethernet.
- ➢ Start the web browser.
- ➢ Enter the IP address of the device into the address bar of the web browser.
- ➢ Confirm the input.

The connection to the device is established.
The graphical user interface (GUI) of the live mode is displayed.

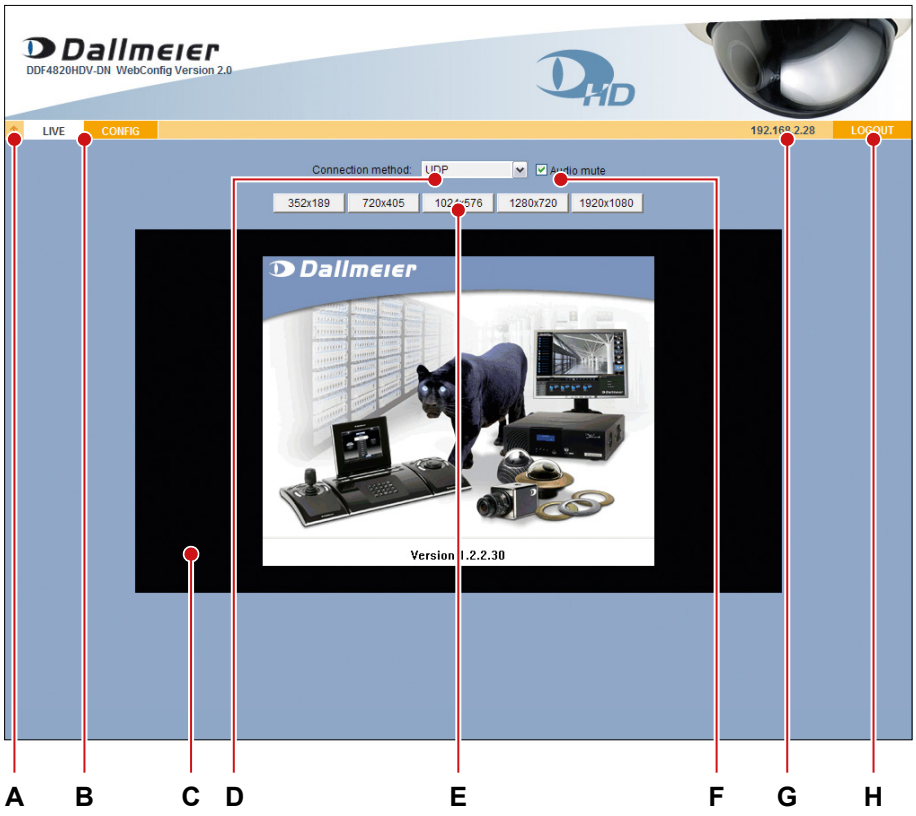


Fig. 7-1 Live mode with adjustable video resolution

A Hide/show title bar
B Switch between live and configuration mode
C Live video
D Connection method (UDP or TCP)
E Adjust video resolution
F Audio On/Off (live audio)
G IP address of the device
H Log out of configuration mode

- Note the explanations below.
- Hide the title bar (**A**) if required.
- Change the ***Connection method*** (**D**) if required.
- Adjust the live video resolution (**E**) if required.
- Enable the live audio output (**F**) if required.

The video resolution setting mentioned above only affects the live video display in the web browser and is not related to the encoder settings.

Live audio is only available for logged in users or user groups. Furthermore, audio encoding has to be enabled (see section "Audio In" on page 67).

Connection Method

If the network connection to the device is established via a router/gateway with NAT (Network Address Translation) function, the live video may not be shown in the web browser. In this case, two solutions are available:

The router/gateway has to be configured for a correct address translation of data packets sent by the User Datagram Protocol (UDP).

UDP is by default used by the streaming function of the device.

An easier solution is to select ***TCP*** from the drop-down list ***Connection method***.

In this case, the device switches the protocol of the streaming function to the Transmission Control Protocol (TCP).

To receive the data packets, the port 30000 for the DaVid Protocol[4)] and port 80 for the Hypertext Transfer Protocol (HTTP) must be open.

Note that during the data transmission via TCP

- normally no packet loss (lack of images) occurs.
- short-term peaks in network traffic may occur.
- low delays may occur.

The "Connection method" described above does not affect the streaming function (see section "Streaming" on page 47).

4) Dallmeier Video Protocol

7.3 Login

The graphical user interface of the configuration mode is displayed after the successful identification as authorized user.

The factory default admin password is “**3**”.

NOTICE

Risk of misuse by unauthorized users!

➢ Change the factory default admin password as soon as possible.

➢ Click ***CONFIG*** in the user interface of the live mode.

The login dialogue is displayed.

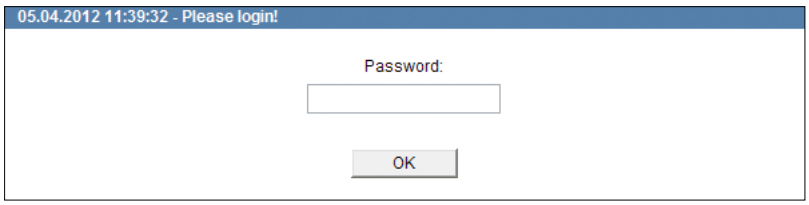


Fig. 7-2

➢ Enter the ***Username*** (Default: “**admin**”) if required.
➢ Enter the ***Password***.
➢ Confirm with ***OK***.

The graphical user interface of the configuration mode is displayed.

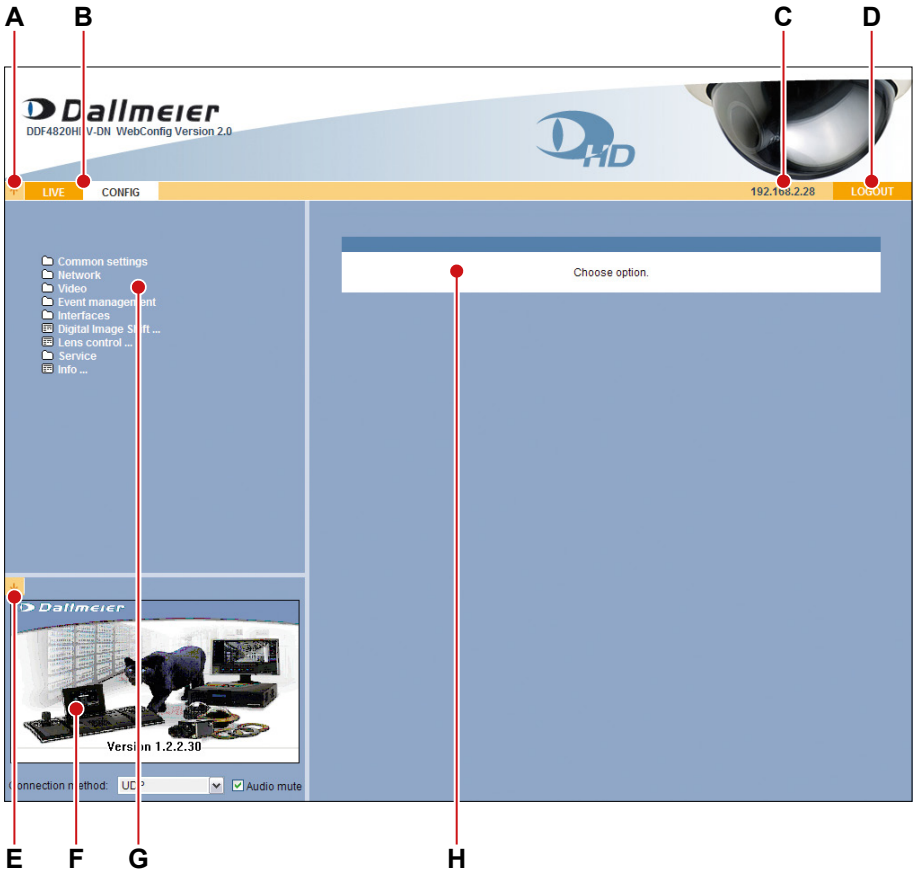


Fig. 7-3 Configuration mode

A Hide/show title bar
B Switch between live and configuration mode
C IP address of the device
D Log out of configuration mode
E Disable/enable live video display
F Live video
G Configuration menu
H Configuration dialogues

Note that

- the live video display and live audio output in the configuration mode can be disabled if merely a low bandwidth is available.
- a new login is required after 5 minutes without user action.

8 Basic Settings

The basic settings and the user management are integrated in the ***Common settings*** menu.

8.1 User Interface

The graphical user interface can be displayed in various languages.

➢ Open the ***User interface*** dialogue via ***Common settings*** > ***User interface ...***.

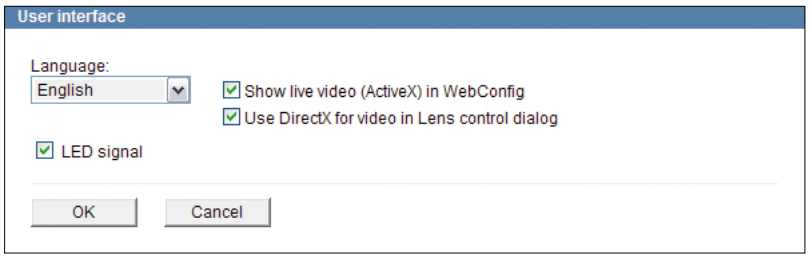


Fig. 8-1

➢ Select the required ***Language***.
➢ Deactivate the ***Show live video (ActiveX) in WebConfig*** checkbox if network bottlenecks occur or your system is overloaded.
➢ Disable the DirectX option if the live video in the lens control dialogue (see chapter “Lens Control” on page 87) turns black at the scale rate of 8× (or rather is not displayed).
➢ Set the relevant option for the LAN LED signal
(checked = LAN LED enabled, unchecked = LAN LED disabled).
➢ Confirm with ***OK***.

8.2 System Time

The system time can be set manually or synchronized with a UTC time server. However, the time zone must be set in both cases.

- Open the ***Time settings*** dialogue via ***Common Settings*** > ***Time ...***.
- Select the ***Time zone*** tab.

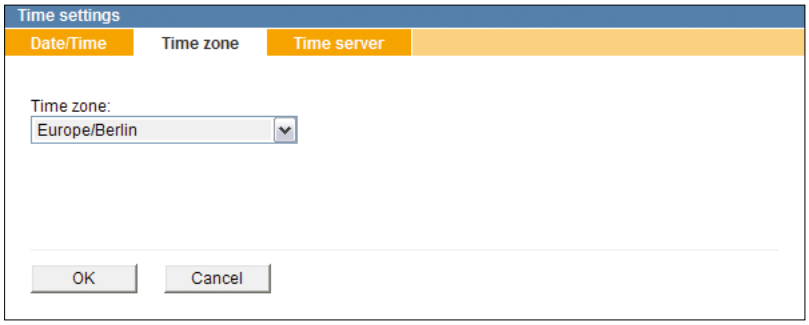


Fig. 8-2

- Set the ***Time zone***.
- Confirm with ***OK***.

8.2.1 Manual Configuration

Note that no manual configuration is possible if the UTC time server synchronization is enabled.

- Select the ***Date/Time*** tab.

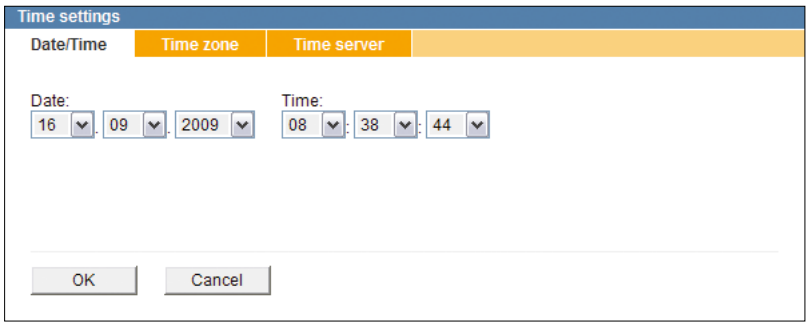


Fig. 8-3

- Set the ***Date***.
- Set the ***Time***.
- Confirm with ***OK***.

8.2.2 Time Server

Note that the time server must always be accessible via the network.

➢ Select the ***Time server*** tab.

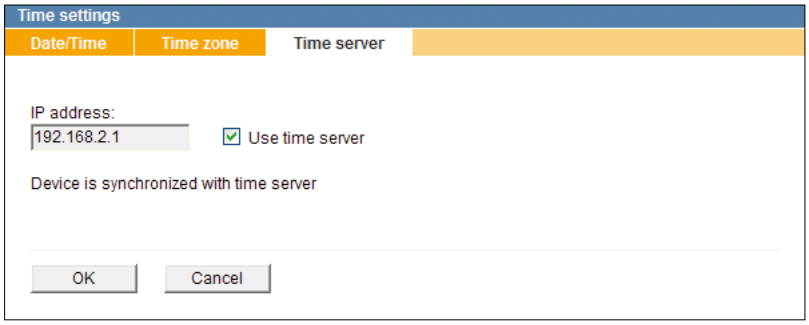


Fig. 8-4

➢ Enter the ***IP address*** (or the host name) of the time server.
➢ Activate the ***Use time server*** checkbox to enable the UTC time server synchronization.
➢ Confirm with ***OK***.

If using the host name instead of the IP address, ensure that the Domain Name System (DNS) settings are correctly configured (see section "Domain Name System (DNS)" on page 45). Contact your network administrator for more information and assistance.

8.3 Camera Name

The camera can be assigned a unique name which then is displayed in an external application (e.g. SMAVIA Viewing Client[5)]) and can be inserted directly in the video.

➢ Open the ***Camera name*** dialogue via ***Common settings*** > ***Camera name ...***.

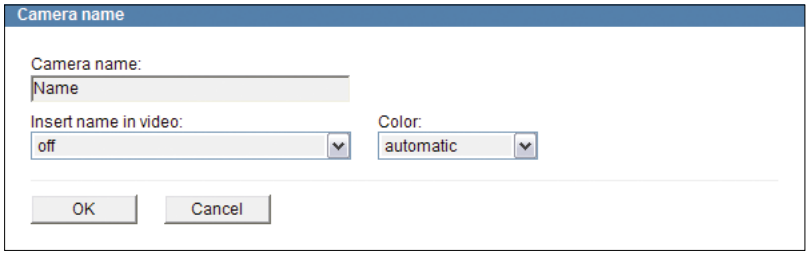


Fig. 8-5

➢ Enter a unique name for the camera.
➢ If required, select the position where the camera name is supposed to be displayed in the video from the drop-down list ***Insert name in video***.
➢ Select the option for the colour representation of the camera name in the video from the drop-down list ***Color***.

Depending on the image information, the colour option "automatic" displays the characters of the camera name either in white or in black to provide a better readability.

➢ Confirm with ***OK***.

8.4 User Management

The configuration of the device must be preceded by a successful authentication as an authorized user or user group.

The user management allows for the definition of various access and configuration rights for three different local user groups. In addition, individual local users can be assigned to the local user groups if necessary.

Furthermore, the centralized user management with LDAP (Lightweight Directory Access Protocol) is supported by an Active Directory (AD) service (such as Microsoft Windows Server*) or Linux*) server with Samba).

8.4.1 Login Mode

The login mode defines the authentication type.

Login mode	**Type**
Group login	Group password
User login	User name + user password *or* Group password
LDAP login	LDAP user name + LDAP user password

The authentication with the group password is also possible in the "User login" mode.

5) Dallmeier Video Management Software

➢ Open the ***Login options*** dialogue via
Common settings > ***User management*** > ***Login options ...***.

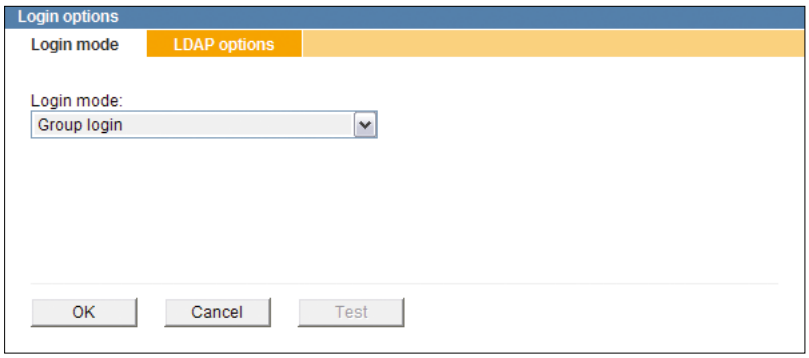


Fig. 8-6

➢ Set the ***Login mode***.
Note the following sections about the different login modes.

➢ Finally, confirm with ***OK***.

8.4.1.1 Group Login

The group names of the three local user groups can be changed.

Note that

- the factory default password of the local user group ***Group 1: admin*** is "**3**".
- the factory default password of the local user group ***Group 1: admin*** must be changed for security reasons.
- the local user groups ***Group 2: user*** and ***Group 3: guest*** are defined without a factory default password.
- a login of the local user groups ***Group 2: user*** and ***Group 3: guest*** is only possible after a password has been defined.

➢ Open the ***User groups*** dialogue via
Common settings > ***User management*** > ***User groups ...***.

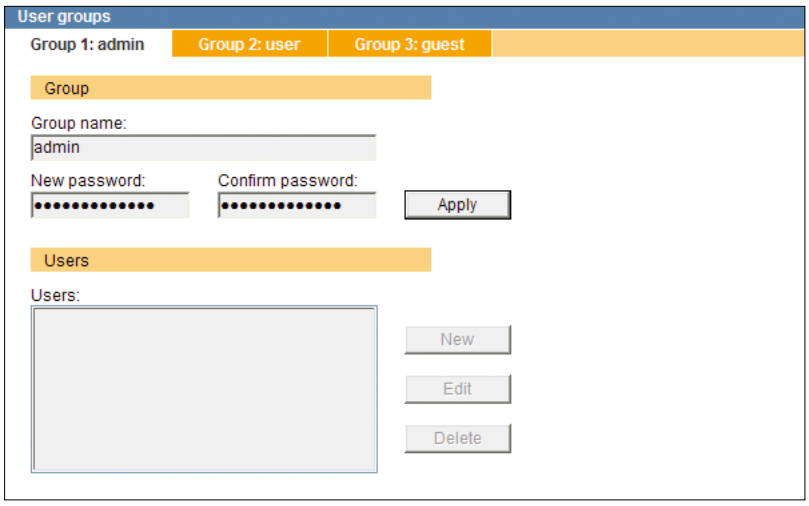


Fig. 8-7

- Select the tab of the relevant group.
- Enter a new ***Group name*** if required.
- Enter a ***New password***.
- Repeat the new password in the ***Confirm password*** field.
- Finally, confirm with ***Apply***.

8.4.1.2 User Login

In the “User login” mode, individual local users can be assigned to the three local user groups.

Define New User

- Ensure that the ***Login mode*** is set to ***User login***.
- Open the ***User groups*** dialogue via ***Common settings*** > ***User management*** > ***User groups ...***.

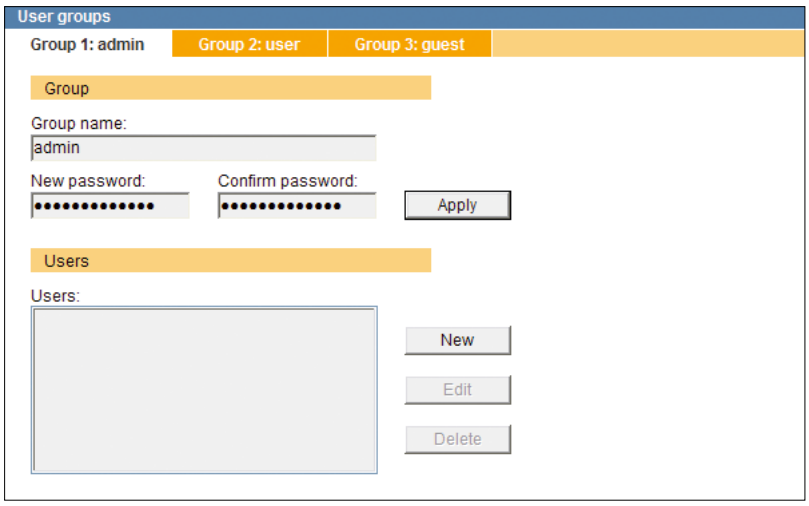


Fig. 8-8

- Select the tab of the relevant group.
- Click ***New***.

The ***New user*** dialogue is displayed.

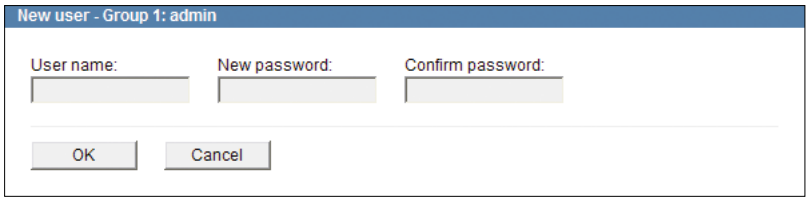


Fig. 8-9

- Enter a new ***User name***.
- Enter a ***New password***.
- Repeat the new password in the ***Confirm password*** field.
- Finally, confirm with ***OK***.

Edit/Delete User

- Ensure that the ***Login mode*** is set to ***User login***.
- Open the ***User groups*** dialogue via ***Common settings*** > ***User management*** > ***User groups ...***.
- Select the tab of the relevant group.
- Select the relevant user from the users list.
- ***Edit*** or ***Delete*** the user by clicking the related button.

8.4.1.3 LDAP Login

This setting allows for the centralized user management with LDAP (Lightweight Directory Access Protocol) using an Active Directory (AD) service (such as Microsoft Windows Server or Linux server with Samba).

The individual user rights/permissions are granted by three different group policies defined on the LDAP client (this device).

NOTICE

In the ***LDAP login*** mode, a login as a local user group or a local user is no longer possible.

The following LDAP settings should only be performed by an administrator with advanced skills in LDAP technology.

In order to be able to set the respective group policies/rights on the LDAP client (this device), each LDAP user intended to obtain access to the device must first be assigned to a specific LDAP group on the LDAP server. Then, the defined LDAP group (user-group-relation) can be read out by the LDAP client (this device).

A valid LDAP group name for each directory entry on the LDAP server must be structured as follows:

[Group prefix][Group suffix]

The group prefix is a user-definable expression (for example, `myhostname`), however, it is required.

This allows administrators to assign different user groups and, thus, variable user rights to multiple simultaneously installed LDAP clients of the same system design (e.g. Dallmeier cameras described here).

The available group suffixes are fixed expressions:

Group 1 (Administrator):	`_G4`
Group 2 (User):	`_G2`
Group 3 (Guest):	`_G1`

On the LDAP server, the LDAP group names with the group prefix `myhostname` would in this case be as follows:

Group 1 (Administrator): `myhostname_G4`
Group 2 (User): `myhostname_G2`
Group 3 (Guest): `myhostname_G1`

However, it is absolutely necessary to also enter the used group prefix on the LDAP client (this device). For further information regarding this requirement, see below.

Note that for the following settings at least one LDAP user must be a member of group 1 (administrator).

After the LDAP settings have been made on the LDAP server, the LDAP client (this device) must be configured accordingly.

In this respect, note the following steps and descriptions:

- Ensure that the ***Login mode*** is set to ***LDAP login***.
- Select the ***LDAP options*** tab.

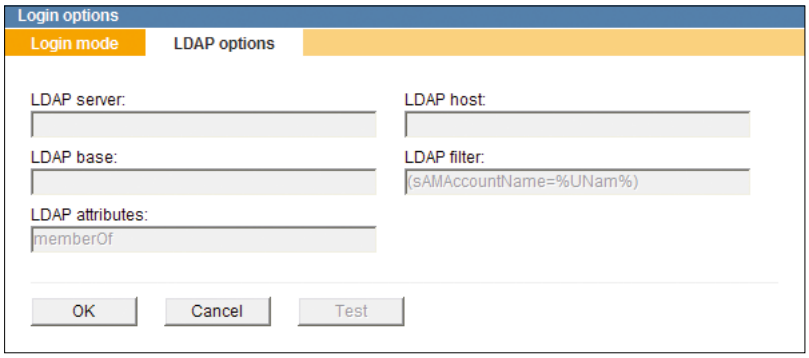


Fig. 8-10

For the correct access to the directory entries on the LDAP server, the following information must be entered:

LDAP server:	Name or IP address of the LDAP server to which the connection is to be established Example: `ldap://servername` `ldap://192.168.57.3`
LDAP host:	Group prefix of LDAP group name Example: `myhostname`
LDAP base:	Base DN (Distinguished Name, search base on the LDAP server); Object location in the LDAP directory hierarchy Example: `ou=department,dc=example,dc=com`
LDAP filter:	Default entry: `(sAMAccountName=%UNam%)`
LDAP attributes:	Default entry: `memberOf`

- Enter the relevant data to access the LDAP server.

Before saving the settings, the entries have to be verified.

The validation is performed by querying the LDAP directory for an existing authorized LDAP user with administration rights (member of group 1).

The settings on the LDAP client can only be saved if the query has been successful (returns an internal result).

➢ Click ***Test***.

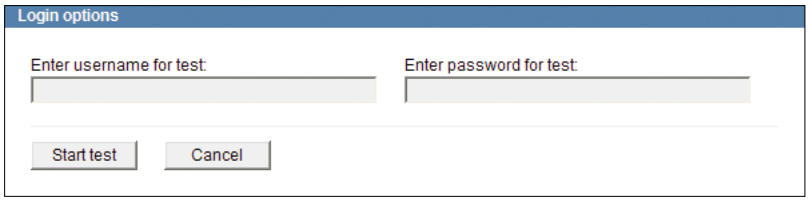


Fig. 8-11

➢ Enter the LDAP user name and the corresponding LDAP user password of an authorized administrator (member of group 1).

➢ Click ***Start test***.

➢ After a successful test, confirm with ***OK*** in order to save the settings.
From this point in time, only authorized LDAP users are able to log into the device (now the LDAP client).

8.4.2 Rights

The three user groups, and thus the assigned users, can be granted individual rights.

In addition, the general public (user group ***anonymous***) can be granted or denied access to certain types of live images (and/or live audio).

Note that

- the rights of group 1 (administrator) can not be restricted.
- certain permission levels can not be set for all rights.
- certain rights are partially or fully relevant for external applications only (e.g. for the DaVid Protocol).

➢ Open the ***Rights configuration*** dialogue via ***Common settings*** > ***User management*** > ***Rights ...***.

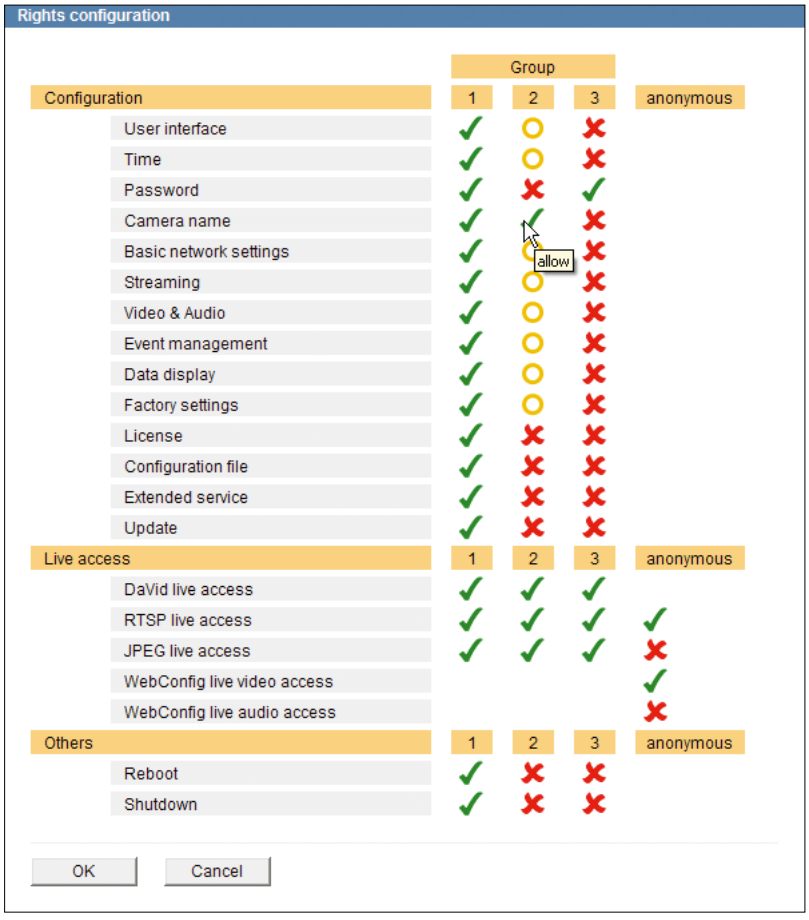


Fig. 8-12

The various rights are each displayed in one row.

The permission level of each user group is displayed with a symbol in the corresponding column (see below).

Symbol	Tooltip	Permission
✓	allow	The dialogue will be displayed. The settings can be changed. The function can be used.
○	allow read only	The dialogue will be displayed. The settings can **not** be changed.
✘	deny	The dialogue will **not** be displayed. The settings can **not** be changed. The function can **not** be used.

- Find the relevant right (row).
- Change the permission level with a click on the symbol in the column of the relevant group.
- Proceed as described above for all rights and groups.
- Finally, confirm with ***OK***.

9 Network

9.1 Basic Settings

The network settings of the device can be configured manually or automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server.

In order to avoid network conflicts, you should clarify if intended network settings are permitted. In particular, the allocation of an already used IP address may result in malfunctions.

➢ Open the ***Network settings*** dialogue via ***Network*** > ***Basic settings ...***.

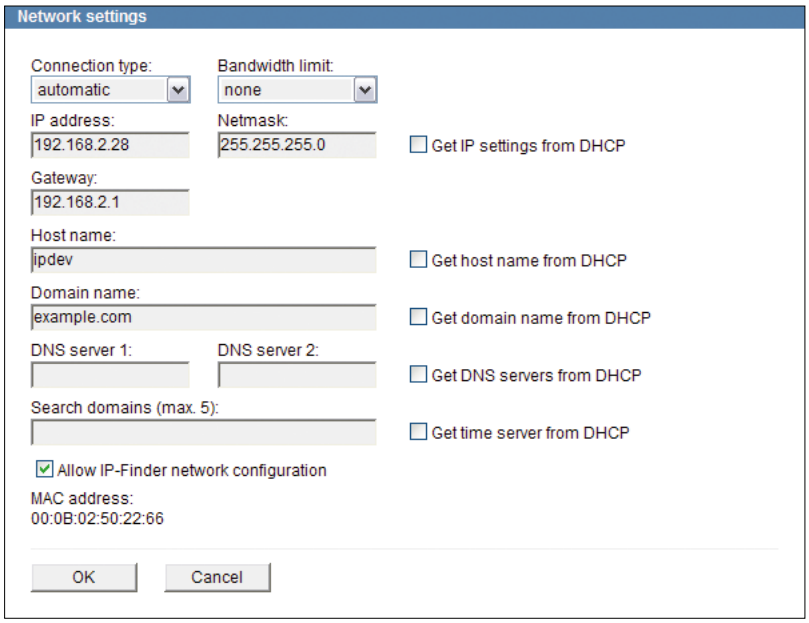


Fig. 9-1 Network settings and MAC address

Default Factory Settings

Connection type:	automatic
Bandwidth limit:	none
Get IP settings from DHCP:	deactivated
IP address:	192.168.2.28
Netmask:	255.255.255.0
Gateway:	192.168.2.1
Allow IP-Finder network configuration:	activated

NOTICE

Incorrect settings may result in the device being no longer available via the network.

➢ Contact your network administrator for more information and assistance.

➢ For troubleshooting purposes, write down the ***MAC address*** and all new settings before changing the configuration.

➢ Note the explanations below.

Connection Type

This setting defines the transfer rate and the duplex mode.

The “Connection type > automatic” (Autonegotiation) is sufficient for most applications.

Bandwidth Limit

Limiting the bandwidth (maximum allowed peak bit rate) can be useful to prevent video artifacts or frame drops due to packet loss with low bandwidth connections.

Domain Name System (DNS)

Since IP addresses are rather difficult to remember, you can also refer to devices by their host names which allows you to locate the devices or hosts more easily on the LAN (Local Area Network).

The mapping of host names to their corresponding IP addresses is handled by the so-called Domain Name Service (DNS server required). In addition, IP address mapping can also be stored directly in the hosts file on your local computer.

The ***Host name*** (or more appropriately the short host name) specifies the name of the machine itself (e.g. `myhostname`).

The ***Domain name*** is usually the network domain within your LAN associated with your company and department (e.g. `example.com` or `intranet.example.com`).

Host names are resolved by special DNS servers (known as “name servers”).

Resolving host names into IP addresses requires the assignment of a primary name server (***DNS server 1***, e.g. `ns1.example.com`) and, for reasons of reliability and availability, a secondary name server (***DNS server 2***, e.g. `ns2.example.com`).

For example, to refer to the device by its long host name or fully qualified domain name (FQDN), you can simply use `myhostname.example.com`. Depending on the DNS server or hosts file settings, you can also refer to the device by simply using its short host name (`myhostname`).

Search domains (max. 5 allowed, separated by spaces) are useful if a defined alarm host or UTC time server is not located in your specified domain name.

9.1.1 Manual Configuration

If no DHCP server is available in your LAN or if you want to assign the network settings manually, proceed as follows:

- Pay attention to the designated and valid IP address ranges in your network.
- Ensure that the ***Get IP settings from DHCP*** checkbox is deactivated.
- Enter the ***IP address*** you want to assign to the device.
- Enter the ***Netmask***.
- Enter the ***Gateway*** address.
- If required, configure the available DNS settings (as described above).
- Deactivate the ***Allow IP-Finder network configuration***[6)] checkbox if not required.
- Finally, confirm with ***OK***.

The connection to the device is terminated and the new network settings are assigned.

9.1.2 DHCP

To have a DHCP server assign the network settings automatically, proceed as follows:

- Ensure that an active DHCP server is available in your local area network (LAN).
- Activate the ***Get IP settings from DHCP*** checkbox.
- If required, configure the available DNS settings (as described above).
  To send the ***Host name*** to the DHCP server, deactivate the ***Get host name from DHCP*** checkbox and enter a specific host name.
- Deactivate the ***Allow IP-Finder network configuration*** checkbox if not required.
- Finally, confirm with ***OK***.

The connection to the device is terminated and the new network settings are assigned by the DHCP server (pay attention to the lease duration).

The newly assigned network settings can be determined by the MAC address of the device using the IP-Finder or on the DHCP server.

The IP-Finder must be executed in the same LAN in which the device is located.

6) IP-Finder: Dallmeier software for the determination and configuration of network-compatible Dallmeier devices

9.2 Streaming

9.2.1 Video Server

The (static) video server provides for a continuous transmission (streaming) of the produced video data into the network, even without an application's active data request.

Note that the format of the RTP payload to be transported must correspond with the encoding standard.

For information about encoder settings, see section "Encoder Settings" on page 63.

➢ Open the ***Streaming*** dialogue via ***Network*** > ***Streaming ...***.

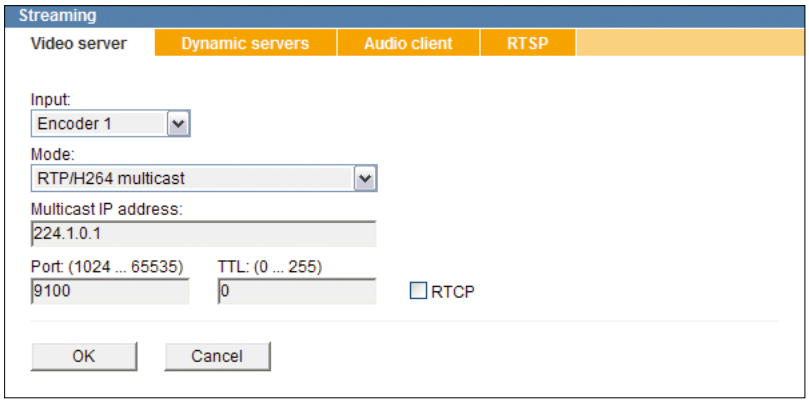


Fig. 9-2

➢ Note the explanations below.
➢ Select the encoder from the drop-down list ***Input***.
➢ Select the transfer protocol, format and method from the drop-down list ***Mode***.
➢ Depending on the selected transfer method, enter the ***Multicast IP address*** or the ***Destination IP address***.
➢ Enter the port number of the service which is supposed to receive the data packets into the ***Port (1024 … 65535)*** field.
➢ Enter the TTL value for IP packets into the ***TTL (0 …255)*** field.
➢ Confirm with ***OK***.

9.2.1.1 Transfer Protocol and Format

The transfer protocol defines the communication rules for the data exchange via the network.
The (static) video server exclusively transports the IP packets via **UDP** (User Datagram Protocol)

Note that

- UDP allows for a smooth and fast data transmission with relatively low delays.
- packet losses (lack of images) may occur during the transmission.

The transfer format defines the RTP payload to be transported.

RTP/H264

The video data is packetized by the Real-Time Transport Protocol (**RTP**) for a **H.264** Video Elementary Stream.

Audio data is **not** transferred.

The data must be encoded to H.264 format.

The packaging is based on the following standards:

RFC3550 - RTP: A Transport Protocol for Real-Time Applications

RFC3551 - RTP Profile for Audio and Video Conferences with Minimal Control

RFC3984 - RTP Payload Format for H.264 Video

RTP/MJPEG

The video data is packetized by the Real-Time Transport Protocol (**RTP**) for a **MJPEG** Video Stream.

Audio data is **not** transferred.

The data must be encoded in MJPEG format.

The packaging is based on the following standards:

RFC3550 - RTP: A Transport Protocol for Real-Time Applications

RFC3551 - RTP Profile for Audio and Video Conferences with Minimal Control

RFC2435 - RTP Payload Format for JPEG-compressed Video

9.2.1.2 Transfer Method

The transfer method defines the distribution of the data throughout the network.

Multicast

The data packets are provided with the specified IP multicast address and port number and transferred to a group of receivers (clients) via a point-to-multipoint connection.

The packets have to be transferred only once; the distribution is done by especially configured routers (capable of IP multicasting).

A receiver will only receive data packets if it has (already) joined the IP multicast group and if the appropriate application service is available at the specified port number.

IP multicast uses the address range between **224.0.0.0** and **239.255.255.255** (Class D).

Note that certain IP multicast address ranges are reserved for special purposes.

For intranet applications, the use of addresses ranging from 239.0.0.0 to 239.255.255.255 is recommended.

Unicast

The data packets are provided with the specified destination IP address and port number and transferred to exactly one receiver (client) in the network via a point-to-point connection.

The receiver will only receive the data packets if the appropriate application service is available at the specified port number.

9.2.1.3 TTL

The TTL value (Time To Live) defines the lifetime of an IP packet.

Each router an IP packet passes through reduces the time-to-live value by one (1). As soon as the value has reached zero (0), the IP packet is discarded.

While preventing IP packets from endlessly circulating in the network due to routing errors, this method stops IP packets from breaking through the limits of the LAN and being sent to the WAN (TTL = 1).

Depending on the requirements, a TTL value ranging from 1 – 255 can be entered. When entering 0 (zero), the default values are used (TTL = 1 for multicast, TTL = 64 for unicast).

9.2.1.4 RTCP

The Real-time Transport Control Protocol (RTCP) is an extension to the Real-time Transport Protocol (RTP) and is used for i.a. the transmission of periodic status information such as timestamps of the transmitted video streams.

9.2.2 Dynamic Servers

A dynamic server is created whenever a UDP or TCP data transmission is actively requested, for example, via the ActiveX-based Dallmeier control, the DaVid Protocol, the Real Time Streaming Protocol (RTSP) or via SMAVIA Viewing Client.

The **Dynamic servers** tab provides information on the currently created dynamic servers.

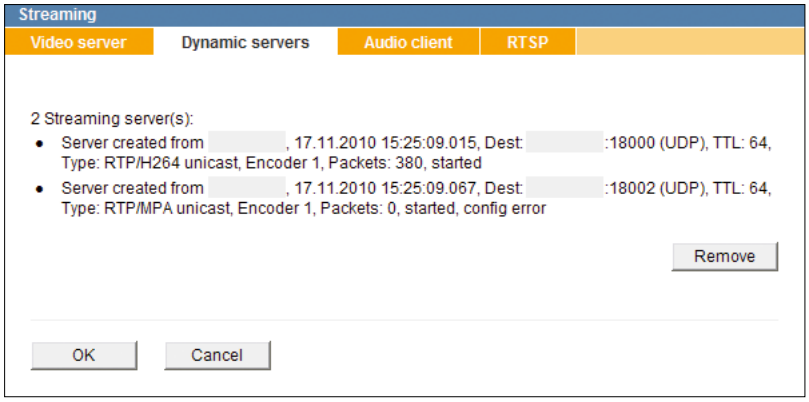


Fig. 9-3

The removal of dynamically generated servers is useful whenever servers, which are no longer used and have not been automatically quit by a request, are to be deleted manually.

9.2.3 Audio Client

The ***Audio client*** tab allows for the configuration of the processing of audio data being sent to the device by external applications via UDP (User Datagram Protocol), or rather the activation of the output of the received audio signal via the installed analogue Audio OUT interface.

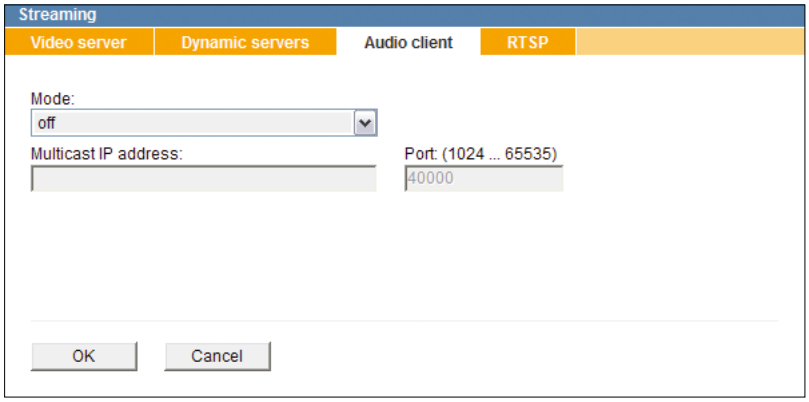


Fig. 9-4

Note the following requirements for the output of audio data via the analogue Audio OUT interface:

- The audio format of the audio source and the audio format defined in the audio client of the camera (drop-down list ***Mode***) must be compatible.
- The defined destination port in the audio source and the port registered in the audio client of the camera (input field ***Port (1024 … 65535)***) must be identical.
- With unicast, the audio source must transmit to the IP address of the camera and the IP address of the audio source (***Source IP address***) must be registered in the audio client of the camera.
- With multicast, the IP multicast address used by the audio source must be identical with the ***Multicast IP address*** registered in the audio client of the camera.

For descriptions about the different transfer methods unicast and multicast, see section "Transfer Method" on page 48.

If UDP is used to transmit the audio data, the settings in the audio client of the camera must be configured manually.

If the DaVid Protocol is used to control the audio output, the necessary information is sent to the camera's audio client automatically.

Note that the settings in the ***Audio client*** tab are disabled if the audio output is controlled via the DaVid Protocol (e.g. via SMAVIA Viewing Client).

In order to control the audio output via SMAVIA Viewing Client, right-click into the SMAVIA Viewing Client split of the displayed camera and select the required audio format and audio bit rate via "Recorder" > "Transmit Audio".

SMAVIA Viewing Client will then transmit incoming audio data (e.g. via the microphone input of the PC) to the audio client in the camera using the DaVid Protocol.

The camera decodes the incoming audio data and outputs the generated analogue audio signals via the analogue Audio OUT interface of the camera (e.g. via a connected speaker).

9.2.4 RTSP

The Real Time Streaming Protocol (RTSP) is used to control the continuous transmission of multimedia content via IP based networks (media streams).

Thereby, RTSP uses a direct (bidirectional) communication with the RTSP streaming server of the camera; on the one hand in order to determine the applicable transmission protocol for the RTP data transfer (UDP or TCP), on the other hand to transmit control actions of IP based RTSP-capable applications (players) such as the starting and stopping of video transmission.

The encoding, packet assembly and transport of the data streams from server to client is thereby carried out directly (unidirectionally) via the Real-Time Transport Protocol (RTP).

Usually, the RTP transmissions of the streaming content are realised via UDP (User Datagram Protocol), whereas the RTSP transmissions are realised via a TCP connection (TCP = Transmission Control Protocol).

The following points need to be considered for RTP transmissions via UDP:

- UDP is a so-called “unreliable” and connectionless protocol.
  No connection is established to the receiver/client prior to the data transmission.
  The receiver/client does not send a confirmation of the receipt of the data.
  During the transmission via UDP packet losses (e.g. lack of individual images) can occur.
  Lost packets will not be sent again.
- Usually, UDP packets that come from outside (internet) into the local area network are blocked by internet routers/firewalls in general.
- UDP allows for smooth and fast data transmission with relatively low delays, i.e. without a time offset of the IP packets (jitter).
- Each RTSP/RTP transmission via UDP requires three ports to be open: a static port for the RTSP control commands (standard port number 554) and two dynamic ports for the RTP data stream.

The following points need to be considered for RTP/RTSP transmissions via TCP:

- TCP is a so-called “reliable” and connection-oriented protocol.
  A connection to the receiver/client is established prior to the data transmission.
  The receiver/client sends a confirmation of the receipt of each IP packet.
  During the data transmission via TCP there are usually no packet losses (unless in the case of a buffer overload in the camera due to permanent network overload). However, the transmission may be slower than with UDP.
- Usually, only the RTSP port at the internet router/firewall needs to be open in order to allow for data transmissions of RTP/RTSP/TCP packets from the internet to the local area network.
- With RTSP the transmission of RTP streams can be embedded in the existing RTSP/TCP connection; a separate UDP transmission or an additional port for the RTP data stream is not necessary.

The ***RTSP*** tab is used to configure the RTSP server in the camera.

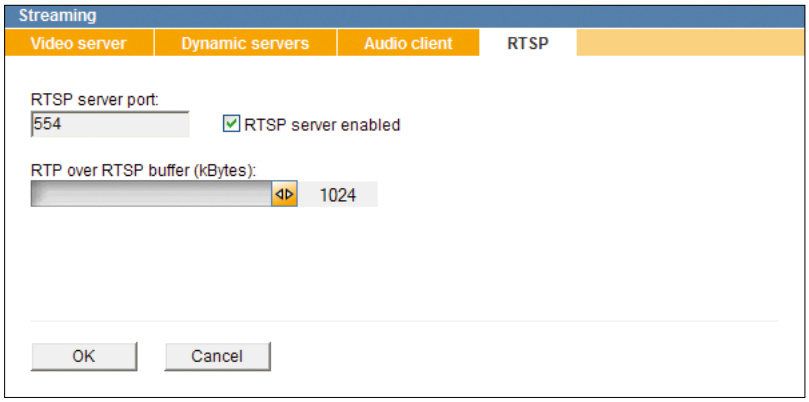


Fig. 9-5

The standard port number for RTSP is 554.

In the ***RTSP server port*** input field the port number can be changed as needed.

In order to generally prevent access to the RTSP server in the camera, which means not to allow any RTSP transmission, the relevant checkbox can be deactivated.

RTP over RTSP buffer

Note that the following paragraph only applies to RTP via RTSP/TCP.

If the network is busy or if a switch within the network, respectively the receiver/client, no longer accepts additional data, the camera can no longer send further image data. The result is a so-called data backlog in the camera.

In order to prevent a loss of images, the yet-unsent image data can – at least for a short time – be saved in an internal RTSP buffer (default capacity 1024 kBytes).

Only in case of a buffer overload are all saved images lost.

Permanent network overload results in a delay in displaying the images at the client. The delay is proportional to the set size of the buffer (amount of images saved).

A large RTSP buffer is only recommended in case of short-term network overloads.

In case of a permanent network overload a smaller buffer as well as lower bit rates are recommended for the individual encoder settings.

10 Video

10.1 Video Standard

Countries and territories use different broadcasting television systems.

To ensure a correct video signal transmission, the device must be set to the appropriate video standard for your country:

- ***HD 25/50 fps*** for “PAL countries”
- ***HD 30/60 fps*** for “NTSC countries”

➢ Open the ***Video standard*** dialogue via ***Video*** > ***Video standard ...***.

Fig. 10-1

This dialogue may be locked by external devices/applications.

➢ Select a ***Standard***.
➢ Confirm with ***OK***.

10.2 Sensor

In the sensor settings, the image sensor can be configured and the image processing parameters can be adjusted to the local lighting conditions.

In addition, you can configure the built-in P-Iris lens behaviour.

➢ Open the ***Sensor settings*** dialogue via ***Video*** > ***Sensor ...***.
➢ Note the explanations about the sensor settings below.
➢ Set the relevant options.
➢ Finally, confirm with ***OK***.

You can restore the factory sensor settings at any time by clicking “Default”.

10.2.1 Global

In the ***Global*** tab, the following settings can be configured:

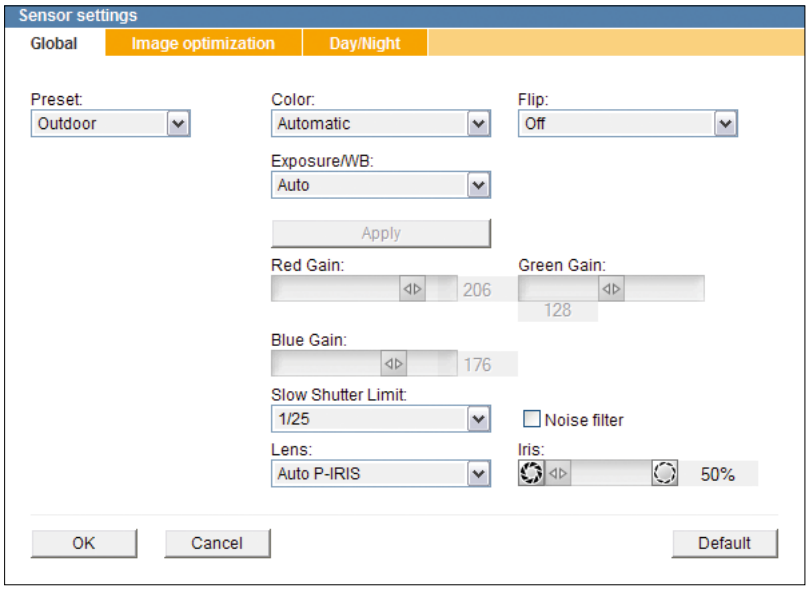


Fig. 10-2

Preset

Presets can be used to easily adjust the sensor configuration for an optimal image quality in most lighting conditions.

In addition, presets can be very useful starting points for the manual fine adjustment of different camera parameters.

The following presets are available:

- **Outdoor**
  Optimized for outdoor scenes.
- **Indoor**
  Optimized for indoor scenes with medium contrast.
- **Low light**
  Optimized for low light scenes.

Color

- **Automatic**
  This setting provides for the automatic switching between colour and black-and-white mode as lighting conditions change.
  The switching depends on the ambient light level, i.e. at low light levels the camera automatically switches to black-and-white mode and removes the colour burst.
  Without colour information, or rather in black-and-white mode, the image quality in low light conditions will be much clearer (e.g. less colour noise).
  Depending on the ambient light (when a certain brightness level is reached again), the camera automatically switches back to colour mode.
- **On**
  The video is always displayed in colour, even at low light levels.
- **Off**
  The video is always displayed in black-and-white.

Flip

By using the flip function, the image in the camera can be mirrored (flipped) horizontally, vertically or on both axes simultaneously.

This provides flexible installation options for desktop, wall or ceiling applications.

Exposure/WB

To reproduce accurate colours, regardless of the prevailing light sources and colour temperatures (measured in Kelvin), a correct white balance is required.

For this purpose, the camera provides the following white balance modes:

- **Auto**
  ATW (Auto Tracking White Balance):
  This white balance setting automatically determines and permanently readjusts the white balance value output using colour information from the entire scene in order to continually compensate for colour temperature changes in varying light conditions.
  For best results, at least one white object (as reference white) should be within the scene that is to be captured.
  The use of ATW is especially recommended for scenes with permanently varying lighting situations/colour temperatures, such as indoor scenes with artificial light sources and incident daylight.
- **One Push**
  AWB (Automatic White Balance):
  The “One Push” white balance value is a fixed measured value which is only readjusted at user request (***Apply*** button), assuming that a white or neutral grey object (as reference value), in correct lighting conditions, is located in more than a half of the entire image.
- **Manual**
  MWB (Manual White Balance) for manual adjustment of red, green and blue gain (see below).

Red Gain

Manual adjustment of red gain with white balance mode **Manual**, 256 steps (0 – 255).

Green Gain

Manual adjustment of green gain with white balance mode **Manual**, 256 steps (0 – 255).

Blue Gain

Manual adjustment of blue gain with white balance mode **Manual**, 256 steps (0 – 255).

Slow Shutter Limit

For a proper exposure, the camera automatically determines the best combination of shutter speed, aperture and signal gain.

The slow shutter limit thereby defines the maximum allowable automatic exposure time (electronic shutter speed).

As soon as the set shutter limit has been reached, the automatic exposure (AE) is exclusively controlled by the automatic iris (aperture) control and/or the automatic gain control (AGC).

Noise filter

This setting can improve the image quality by reducing noise in signal processing.

In scenes with lots of complex objects, enabling this function, however, may lead to a loss of detail in the image.

The noise filter described here can be enabled at all resolutions.

Lens

The camera is equipped with a P-Iris lens.
The P-Iris technology is designed for the precise and automatic adjustment of the ideal aperture (“optimum aperture”).

Compared with conventional DC auto iris lenses, P-Iris (Precise Iris) attains a significantly improved image quality with excellent contrast, brilliant clarity and increased detail resolution with, at the same time, a larger depth of field under almost all lighting conditions.

Especially when monitoring objects in different distances to the camera, such as in extended hallways, waiting areas or parking lots, maximizing the depth of field is crucial to the quality of the results of a later image analysis.

In cases of extremely bright lighting conditions, the P-Iris technology prevents the effect of a so-called diffraction blur (reduction of the overall image sharpness). This effect would typically occur with conventional DC-controlled auto iris lenses (especially with high-resolution megapixel cameras, due to a smaller sensor pixel pitch) when automatically stopping down too far (high f-stop number).

- **Auto P-IRIS**
  Together with the P-Iris lens, the camera software, first of all, automatically determines the most ideal compromise (also called “optimum aperture”) between depth of field, lens resolution and diffraction and, then, continually adjusts the diaphragm opening (aperture) accordingly with a stepping motor.
  For best focusing results during the camera installation, P-Iris automatically selects the widest aperture and, with it, the smallest depth of field. Hence, it is able to achieve perfect image sharpness regardless of the lighting conditions.
- **Manual P-IRIS**
  Manual adjustment of diaphragm opening (aperture).

Iris

This option is only available when the ***Lens*** option is set to **Manual P-IRIS**.

- **Normal (50%, slider on left position)**
  Fixed diaphragm opening (aperture) for largest possible depth of field.
- **Open (100%, slider on right position)**
  Maximum aperture (diaphragm opening);
  useful, for example, under very dark lighting conditions.

10.2.2 Image Optimization

In the ***Image optimization*** tab, the following camera parameters can be configured:

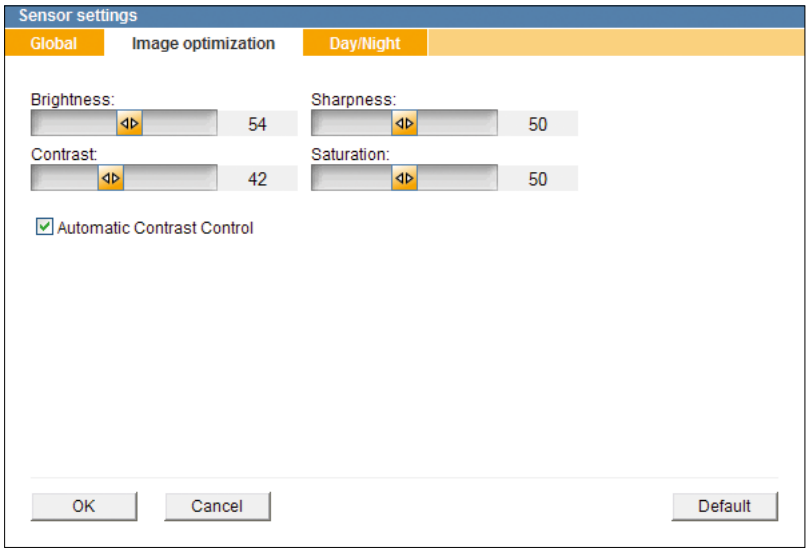


Fig. 10-3

Brightness

Defines the overall image brightness by linear adjustment of the tonal values.

Contrast

Adjusts the difference in brightness between light and dark areas.

The "Automatic Contrast Control" provides an automatic and continuous contrast adjustment to the prevailing light conditions.

Sharpness

Influences the perceived sharpness by edge enhancement.

Saturation

Defines the colourfulness and luminance of colours and therefore their perceived intensity.

10.2.3 Day/Night

The camera is designed to produce high-quality images in daylight as well as under low light conditions or at night.

In the ***Day/Night*** tab, the following settings can be configured:

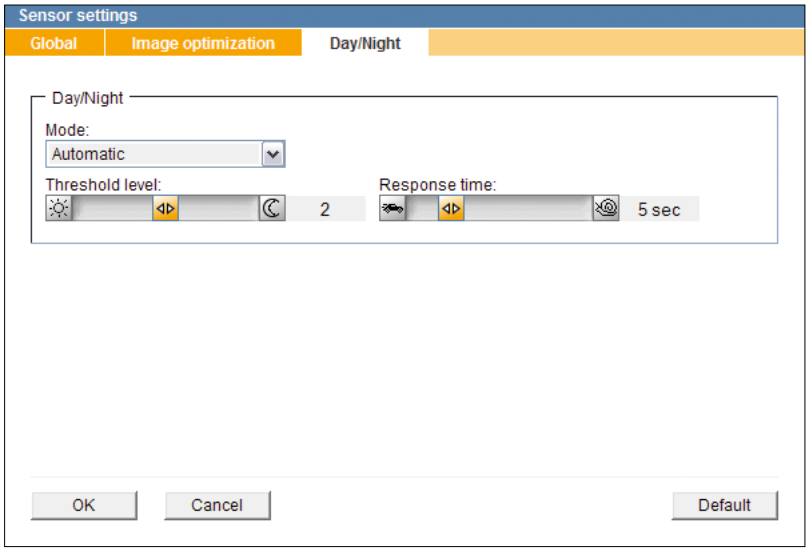


Fig. 10-4

Mode

- **Automatic** (Day/Night switching):
  The automatic Day/Night switching depends on the amount of visible light detected by the integrated ambient light sensor and internal defined parameters. In low light conditions, the infrared (IR) cut filter is automatically removed (ICR ON, night mode), which significantly enhances the sensor's sensitivity for near infrared light.
  In night mode the video image is displayed in black and white.
  Depending on the amount of visible light, the IR cut filter is automatically engaged (ICR OFF) and the camera switches back to day (and colour) mode again.
  The switching threshold level and response time can be manually adjusted (see below).
- **Day** (day mode permanently active):
  The built-in infrared (IR) cut filter is always engaged (ICR OFF).
- **Night** (night mode permanently active):
  The built-in infrared (IR) cut filter is always removed (ICR ON).

Threshold Level

This setting provides the manual adjustment of the Day/Night switching threshold levels (threshold values of brightness and darkness).

Possible values: 0 – 4 (Default: 2)

Higher level:

The camera switches earlier to night mode (ICR ON) and later to day mode (ICR OFF).

Lower level:

The camera switches later to night mode (ICR ON) and earlier to day mode (ICR OFF).

Response Time

This function provides further fine adjustments of the automatic Day/Night switching.

The response time defines the Day/Night switching delay time once the particular threshold levels are reached.

Possible values: 1 sec. – 20 min. (Default: 5 sec.)

Example:

If during the day the camera is operated inside a room with windows that face a public road, the entire room could become very dark for a short time when a big truck passes.

Depending on the set threshold levels for the automatic Day/Night switching, the camera would normally switch to night mode immediately and, moments later, back in to day mode.

In the reverse example there would be an unwanted permanent switching to day mode and back as soon as the headlights of passing vehicles would light up the room.

Using the reaction time setting it is thus possible to delay the automatic Day/Night switching.

10.3 Exposure Control

Using the exposure control allows you to adjust the automatic exposure metering of the camera.

➢ Open the ***Exposure Control*** dialogue via ***Video*** > ***Exposure Control …***.

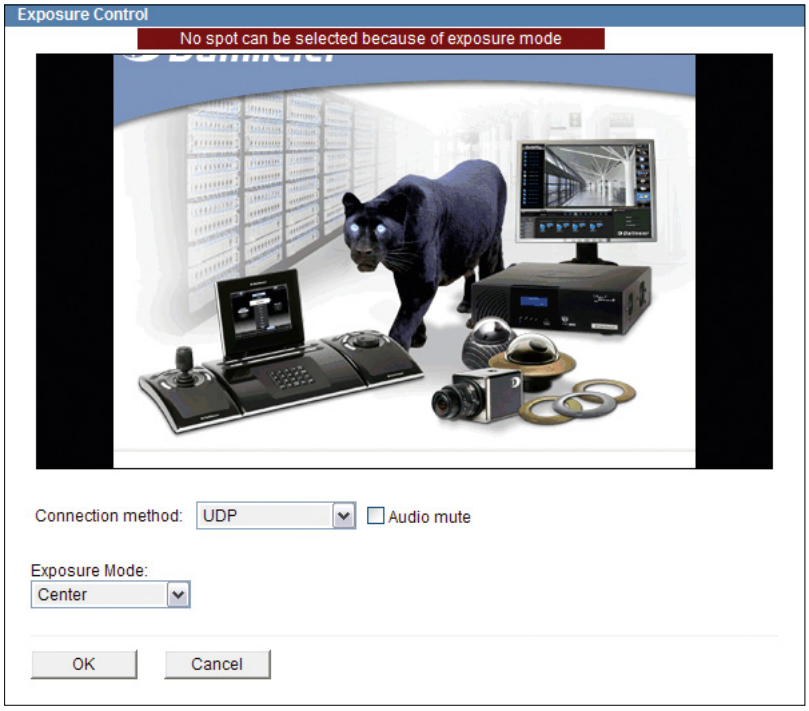


Fig. 10-5

➢ Note the explanations below.

➢ Set the relevant options.

➢ Finally, confirm with ***OK***.

Exposure Mode

- **Automatic**
  The entire image is used for exposure metering.
  This setting is only recommended if the entire image section is illuminated homogeneously.
- **Center** (centre-weighted metering, default setting):
  With this exposure metering option, the centre image section is prioritised over the outer image areas.
  This setting is recommended in case the relevant image details are primarily at the centre of the image rather than the outside margins of the image.

- **Spot Light** (spot metering):
  The exposure metering is only carried out for the image section as defined by the user. That area is then optimally exposed. However, the other image areas can be heavily overexposed or underexposed.
  This setting is recommended for scenes with extreme variations in brightness when a specific image section is to be exposed absolutely correctly.

  In order to define an area for spot metering, proceed as follows:

  ➢ Select ***Spot Light*** from the drop-down list ***Exposure Mode***.
  ➢ Click and hold the left mouse button and draw a rectangle (red) over the relevant image area you want to define for spot metering.
  ➢ Release the mouse button.
  Another click within the image removes the defined metering area.
  ➢ Once the area defined for spot metering meets your requirements, click ***OK***.

10.4 Privacy Zones

This function allows you to hide (mask) up to 4 user-definable areas in the camera to ensure privacy protection and compliance with laws and regulations that prohibit certain locations from being monitored and/or recorded. The defined Privacy Zones are then directly blackened in the camera.

Note that the combined area of all active Privacy Zones can maximally amount to up to 20% of the entire image.

Open the ***Privacy Zones*** dialogue via ***Video*** > ***Privacy Zones …***.

Fig. 10-6

- Select a zone (1 – 4) you would like to define by using the appropriate radio button (option button).
- Click and hold the left mouse button and draw a rectangle (going from upper left to lower right) over the relevant image area you would like to hide (mask) in the camera. The selected image area is indicated in red.

  If the selected image area does not meet your requirements, use the mouse and click on an unmasked area.
  The red masking is then removed and a new image area can be selected.

- If the selected image area meets your requirements, activate the defined zone by selecting the appropriate checkbox.
- Click ***OK*** to apply the settings.
- If you want to define another image area as a Privacy Zone, select the appropriate radio button and proceed as described above.
  However, if the combined area of all already activated zones amounts to more than 20% of the entire image, you cannot mask any more zones.
  In that case, reduce the size of the already defined zones and save the settings again by clicking ***OK***. Then, define the new zone.
- Finally, click ***OK*** in order to save all settings.

You should always activate and save each defined zone first ("OK") before defining another zone.

In order to display masked image areas again, deactivate the appropriate checkbox and click "OK". The defined image area remains saved in the camera as long as you do not click into an unmasked image area within the corresponding zone. Thus, you can always activate or deactivate the masking for an already defined image area.

10.5 Encoder Settings

The audio and video encoding is configured in the ***Encoder settings*** dialogue.

This dialogue may be locked by external devices/applications.

Note that the produced camera images can be recorded in the “Motion” recording mode (image comparison) by Dallmeier recorders of the DMS and VNB series (as of version 7.1.1).

For this, the Encoder 1, which has to be set to H.264 encoding, is used.

Encoder 2 and 3 are then automatically disabled.

In addition to the recording, a second stream from Encoder 1 can be used for the live display if Encoder 1 is set to a bit rate not higher than 6 MBit.

10.5.1 Encoder 1

➢ Open the ***Encoder settings*** dialogue via ***Video*** > ***Encoder settings ...***.

The ***Encoder 1*** tab is displayed.

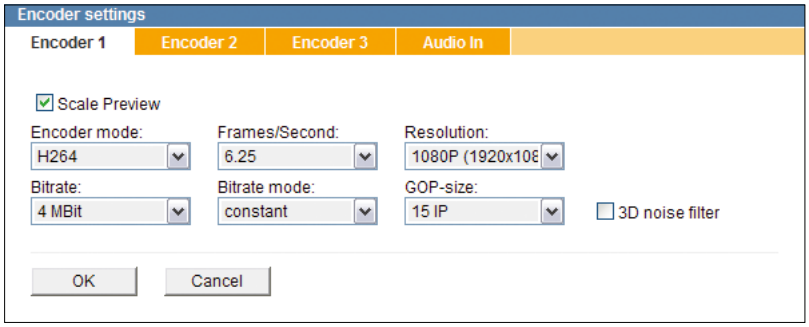


Fig. 10-7

➢ Note the explanations below.
➢ Activate the ***3D noise filter*** if required.
➢ Select the encoding standard from the drop-down list ***Encoder mode***.
➢ Select the frame rate from the drop-down list ***Frames/Second***.
➢ Select the ***Resolution*** (width × height in pixels).
➢ Select the ***Bitrate***.
➢ Select the ***Bitrate mode***.
➢ Select the ***GOP-size*** (only with H.264).
➢ Finally, confirm with ***OK***.

3D noise filter (spatial + temporal)

This function can improve the image quality by noise reduction and therefore enhance the compression performance.

Note that this function is not effective with resolutions higher than 720p.

- Compares pixels both within and between frames
- Very effective noise suppression
- May cause high CPU load and therefore may slow down the encoding speed and lead to a loss of frames
- May blur moving objects
- May cause a loss of detail

Frames/Second

The frame rate (value in fps) defines the number of consecutive frames produced per second.

The higher the frame rate, the smoother the video playback.

However, a higher frame rate also requires a higher bandwidth usage (transmission capacity) and more hard disk storage space for the recording of video material.

25 (“PAL countries”) or 30 fps (“NTSC countries”) meet the requirements for real-time applications.

Bitrate

The bit rate refers to the number of bits per second used to encode the video.

The more bits are used to represent the video data per second, the higher the quality is.

However, a higher bit rate also requires a higher bandwidth usage (transmission capacity) and more hard disk storage space for the recording of video material.

Low bit rate	⇨	High image compression Small data volume Poor image quality Low bandwidth and hard disk space usage
High bit rate	⇨	Low image compression Large data volume High image quality High bandwidth and hard disk space usage

Usually, most requirements in surveillance applications are met with a bit rate between 4 and 6 Mbps.

Bitrate mode

The bit rate mode allows you to configure a constant (CBR) or a variable bit rate (VBR) for the video encoding.

The VBR correlates with the changes in the image dynamically.

In scenes with many changes in the image the bit rate is temporarily increased.

The admissible deviations from the defined bit rate are indicated in percentages.

The higher the percentage value, the higher the maximum admissible peak rate and the longer the regulation time to return to the nominal bit rate.

Example:

In case of a defined (nominal) bit rate of 4 Mbps and a bit rate mode of “variable 100 %” the peak rate may temporarily increase to up to 8 Mbps.

Variable bit rates allow for a higher image quality while simultaneously enabling a better use of both available hard disk storage space and transmission capacities.

A constant bit rate on the other hand allows for a more precise calculation of required storage capacity.

GOP-size

The H.264 coding is carried out by dividing the video stream into so-called GOPs (Group of Pictures) of a defined length (defined GOP-size).

A GOP sequence always starts with an Intra-Frame (I-Frame), which contains all image data and serves as a reference for the subsequent images within a GOP.

The I-Frame is compressed with a low compression rate, similar to the JPEG compression method.

Depending on the defined GOP-size, an I-Frame is followed by one or more Predicted Frames (P-Frames), which only contain the motion predictions and difference information about the preceding images (I-Frame or P-Frames) (Long-term prediction).

The compression rate with P-Frames is much higher than with I-Frames since changes in relation to reference images need to be coded as motion vectors only. The required bit rate thus decreases so that, with a given total encoding bit rate, more bits are available for the I-Frame. This means that the quality of the I-Frame can be increased, for example, the detail resolution in case of a larger GOP-size.

However, if there are scenes with many motion changes, a high number of P-Frames can have a negative effect on the image quality, because the motion predictions become increasingly inaccurate.

Additionally, a larger GOP-size always leads to an increase in delays regarding processing or accessing a stream.

The GOP sequence ends before the next I-Frame.

At a later stage, the visible single frames are generated at the decoder, using the individual GOPs.

The GOP-size 1 (I-Frames only) indicates a low compression factor and should only be used with specific applications, because the bandwidth requirements increase significantly.

Generally, a GOP-size of between 6 and 15 will provide a good image quality with sufficient compression.

If large GOP-sizes are defined, reverse playback can result in frame drops with some decoders.

10.5.2 Encoder 2

Encoder 2 is disabled by default.

Note that the availability of the ***Encoder 2*** option depends on the settings made in the ***Encoder 1*** tab.

➢ Select the ***Encoder 2*** tab.

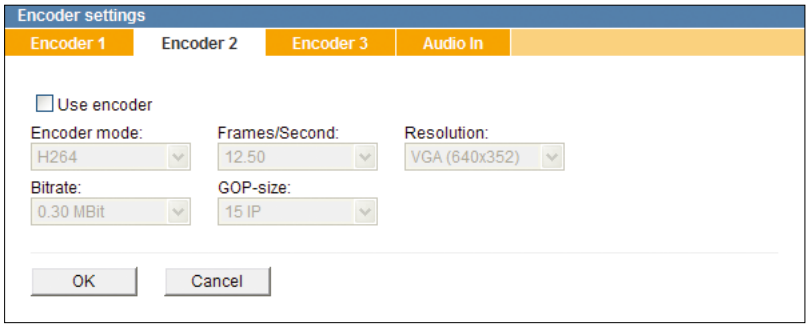


Fig. 10-8

➢ If required, activate the ***Use encoder*** checkbox to enable Encoder 2.
➢ Select the required settings (see section “Encoder 1” on page 63).
➢ Confirm with ***OK***.

10.5.3 Encoder 3

Encoder 3 is disabled by default.
Encoder 3 only supports the encoding standard H.264.

Note that the availability of the ***Encoder 3*** option depends on the settings made in the ***Encoder 1*** tab and ***Encoder 2*** tab.

➢ Select the ***Encoder 3*** tab.

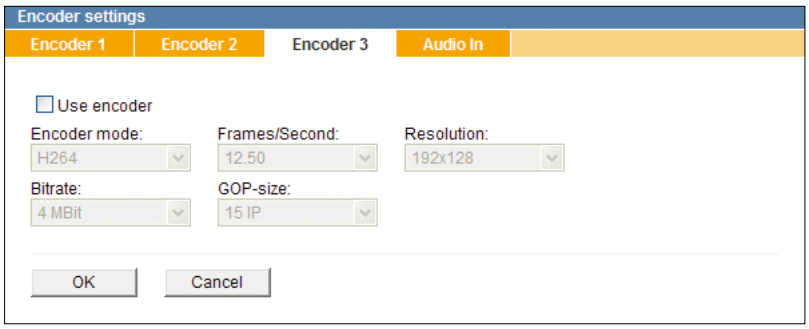


Fig. 10-9

➢ If required, activate the ***Use encoder*** checkbox to enable Encoder 3.
➢ Select the required settings (see section “Encoder 1” on page 63).
➢ Confirm with ***OK***.

10.5.4 Audio In

In the ***Audio In*** tab, you can configure the processing (encoding) options of the analogue audio signal coming from the built-in Audio IN port.

➢ Select the ***Audio In*** tab.

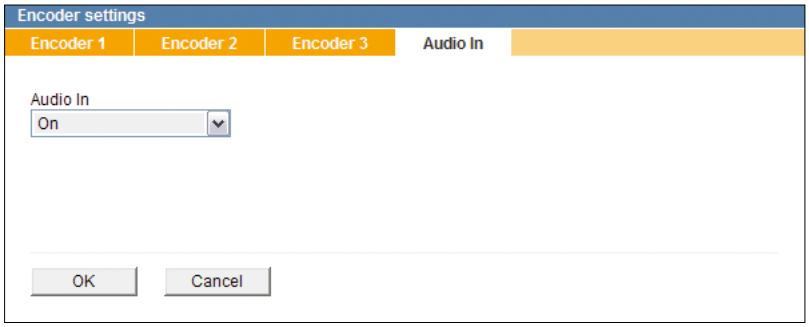


Fig. 10-10

➢ Select the relevant audio processing option from the drop-down list ***Audio In***.
➢ Confirm with ***OK***.

11 Event Management

The event management provides event-triggered e-mail notifications (including image attachments) to several alarm hosts via SMTP and supports the automatic FTP upload of still images based on events and/or a definable time interval.

➢ Click ***Event management*** in the configuration menu.

If no event handler has been set yet, only the ***New ...*** item is displayed.

➢ Click ***Event management*** > ***New ...***.

The configuration menu is expanded with the ***Event 1*** item and the related dialogue is displayed.

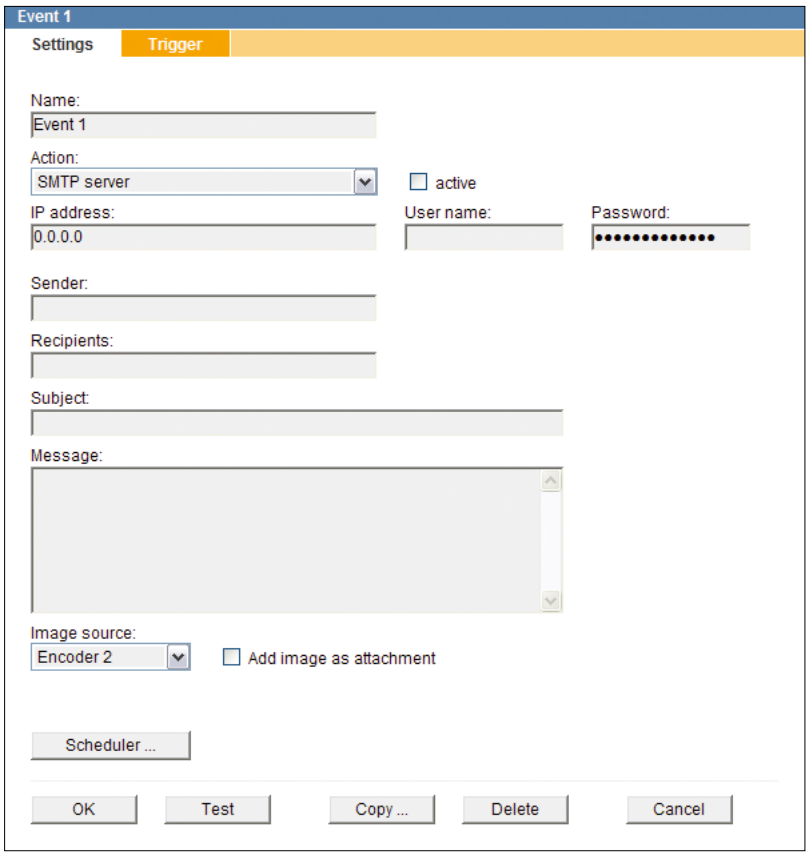


Fig. 11-1

➢ Enter a unique name for the new event handler into the ***Name*** field.
➢ Select the action type which is supposed to be executed when a defined event occurs (is triggered) from the drop-down list ***Action***.
➢ Set the required settings for the selected action type (see below).
➢ Activate the ***active*** checkbox to enable the event handling.
➢ Finally, confirm with ***OK***.

The item name in the configuration menu and the dialogue title is automatically updated with the entered event handler name after the settings have been saved.

To edit an already set event handler, click the related item in the configuration menu.

11.1 SMTP Server

When using this action type, the alarm/event messages are sent as e-mails via SMTP (Simple Mail Transfer Protocol) to the specified alarm host (SMTP server) which may then forward them to several e-mail recipients.

Depending on the used SMTP server and its configuration, any name can be used for the sender or a SMTP authentication is required.

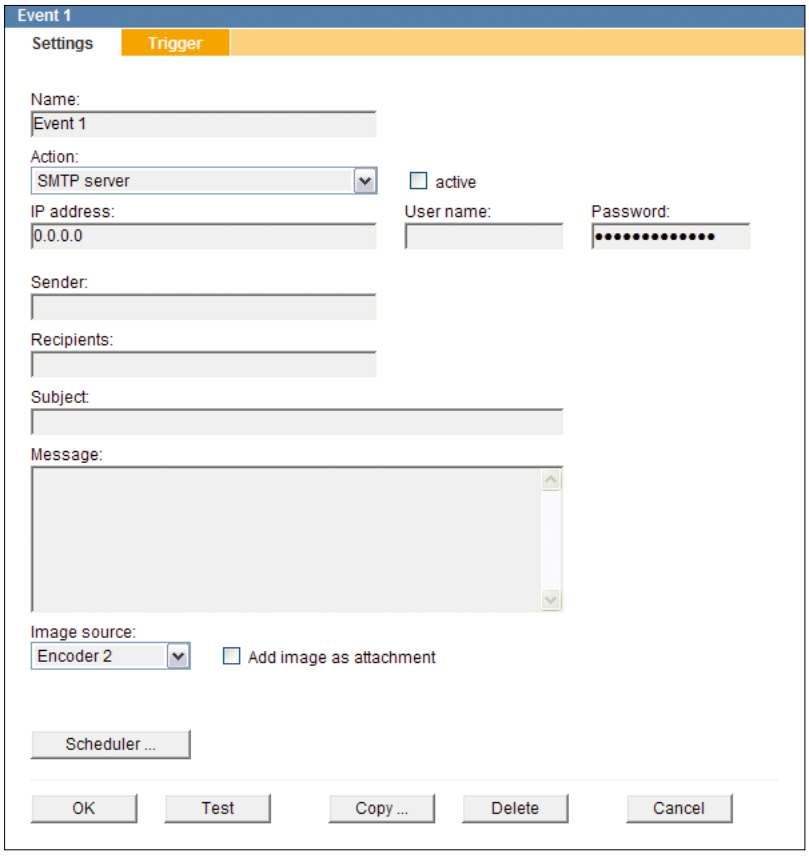


Fig. 11-2

- If necessary, enter the ***User name*** and the ***Password*** for the SMTP authentication.
- Enter the ***Sender***.
- Enter the e-mail addresses of the ***Recipients*** (separated by semicolons) to which the SMTP server is supposed to forward the event-triggered e-mails.
- Enter the ***Subject*** and the ***Message*** of the e-mail.

The following variables can be used for the ***Subject*** and the ***Message*** of the e-mail:

%ALARMTYPE%	Alarm/event type (trigger)
%ALARMHOSTNAME%	Name of the event handler (or alarm host)
%CAMERANAME%	Name of this device
%ALARMTIME%	Date and time the alarm/event is triggered
%DEVICEIP%	IP address of this device

- Activate the ***Add image as attachment*** checkbox to attach the current JPEG image (captured exactly at the moment the event is triggered) to the e-mail.
- Select an encoder from the drop-down list ***Image source*** to define the source of the JPEG image.

The used encoder must be enabled ("Encoder 2" is disabled by default) and configured for MJPEG encoding (see section "Encoder Settings" on page 63).

- Click ***Test*** to check your configuration by sending a test e-mail.
  The test was successful if a new e-mail from the device is in your specified e-mail account.

- Select the ***Trigger*** tab.

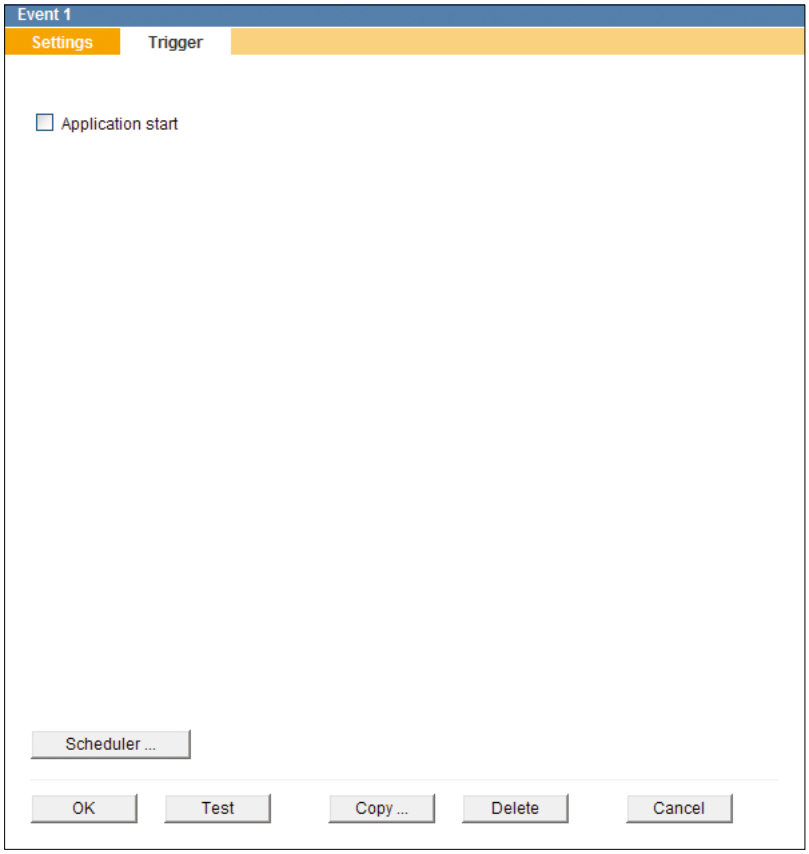


Fig. 11-3

- Select all relevant triggers which are supposed to be sent out as event messages by activating the related checkboxes.
- Finally, confirm with ***OK***.

11.2 FTP Server

This action type allows you to configure the automatic FTP (File Transfer Protocol) upload of JPEG images based on events and/or a definable time interval.

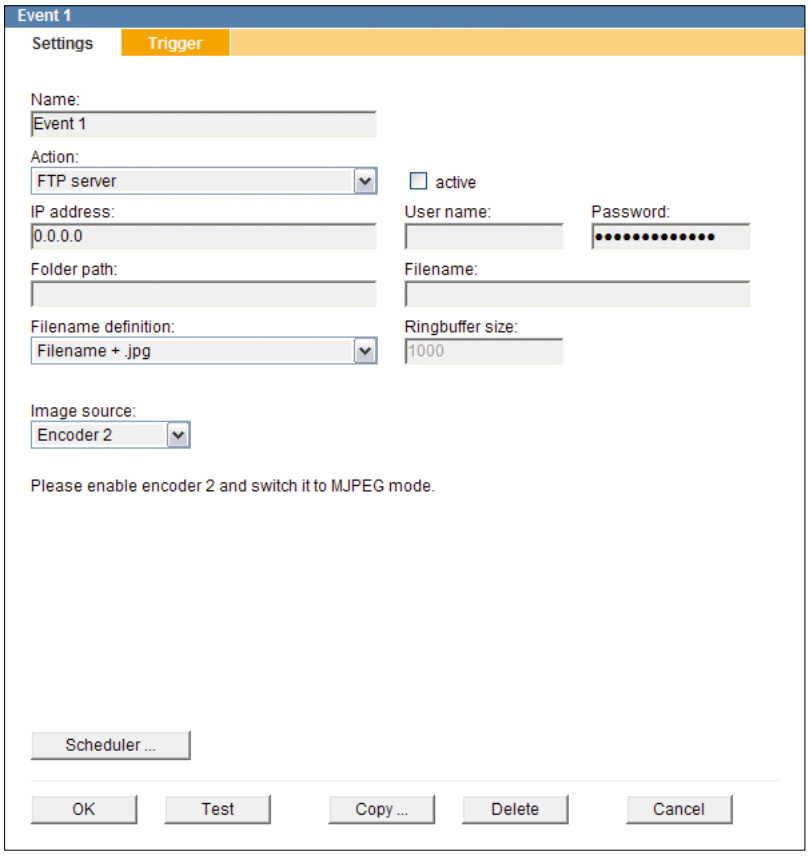


Fig. 11-4

- Enter the ***User name*** and the ***Password*** for the FTP authentication.
- Enter the full path to the directory to which the JPEG images are to be saved to into the ***Folder path*** field.

Ensure that read and write permissions are set for the specified directory and enough free disk space is available.

- Enter the name under which the JPEG images are to be saved into the ***Filename*** field.
- Select the ***Filename definition***:

  - ***Filename + .jpg***
    An already existing image in the directory will be overwritten.
  - ***Filename + number (ring) + .jpg***
    The oldest image in the directory will be overwritten after a certain number of uploaded images (***Ringbuffer size***).
  - ***Filename + number + .jpg***
    Existing images in the directory will not be overwritten.
  - ***Filename + date + .jpg***
    Existing images in the directory will not be overwritten.

- If necessary, enter the ***Ringbuffer size***.
- Select an encoder from the drop-down list ***Image source*** to define the source of the JPEG images.

The used encoder must be enabled ("Encoder 2" is disabled by default) and configured for MJPEG encoding (see section "Encoder Settings" on page 63).

- Click ***Test*** to check your configuration.
  The test was successful if a new JPEG image is uploaded to the FTP directory you specified.

- Select the ***Trigger*** tab.

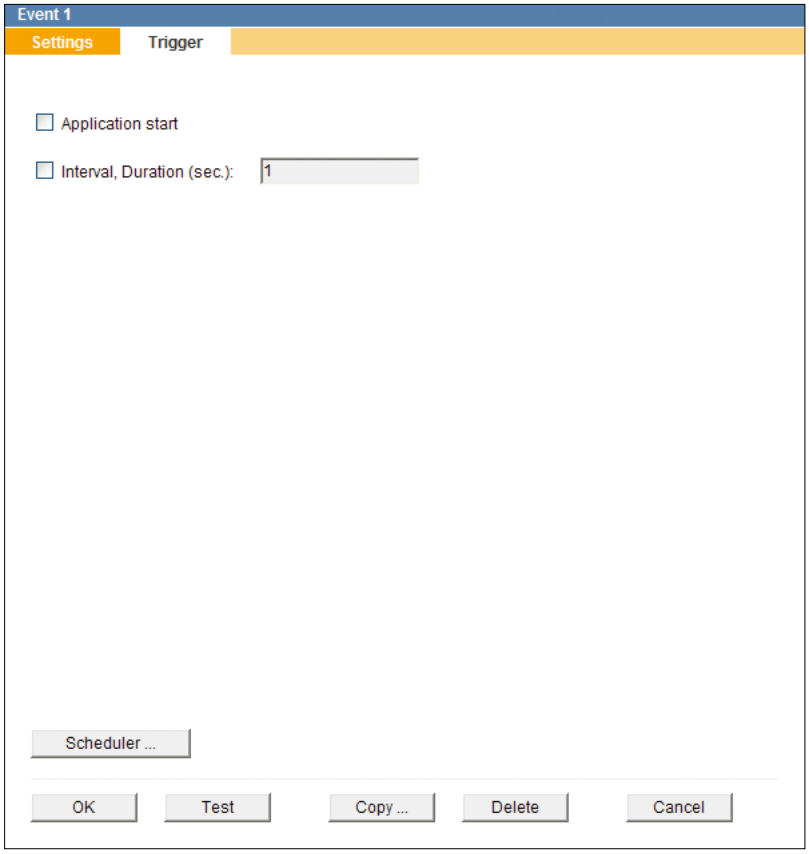


Fig. 11-5

- Select all relevant triggers which are supposed to initiate an FTP image upload by activating the related checkboxes.
- Finally, confirm with ***OK***.

Interval, Duration (sec.)

This trigger option allows you to configure the automatic FTP upload of still images based on a time interval.

The minimum time interval for FTP image uploads is 1 second.

The less the duration between two FTP image uploads is set, the more the network utilization rate (traffic level, bandwidth consumption) may increase.

11.3 Scheduler

The scheduler function allows you to define specific time periods during which event messages are sent out or event-triggered actions are executed.

Note that

- scheduler settings only apply to the currently selected event handler.
- the minimum selectable period is 15 minutes.
- the week timer applies to the entire year if no exceptions are set.

11.3.1 Week Timer

➢ Click ***Scheduler ...***.

The ***Week timer*** tab is displayed.

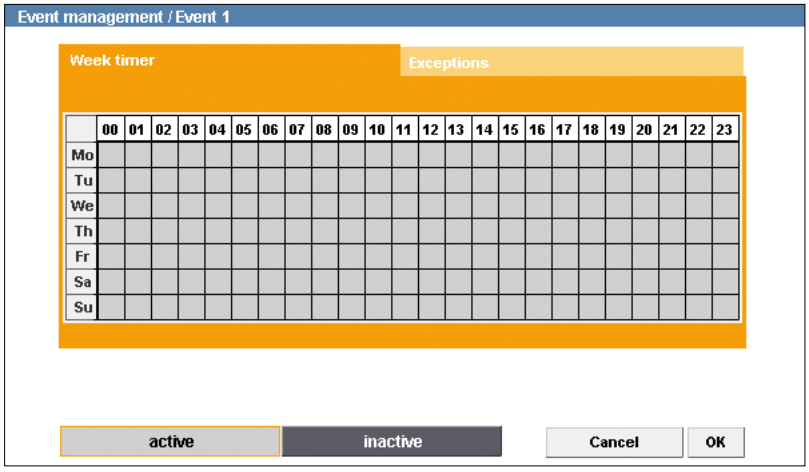


Fig. 11-6

Light grey areas in the week timer represent **active** periods.
During active periods the **messaging function** is **enabled** and **event actions are executed**.
By default, the entire period in the week timer is active.

Select Inactive Periods

➢ Click ***inactive***.
➢ In the week timer, click and hold the left mouse button and draw a rectangle over a relevant period.
➢ Release the mouse button.
➢ Repeat the last two steps until all relevant inactive periods are selected.

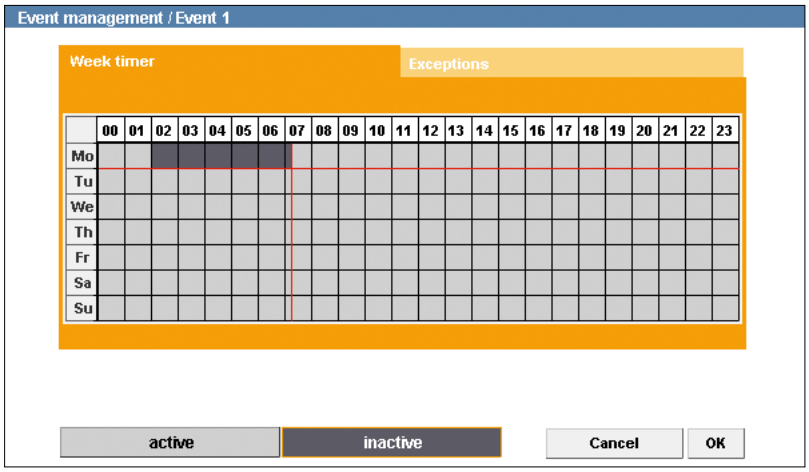


Fig. 11-7

Dark grey areas in the week timer represent **inactive** periods.

During inactive periods the **messaging function** is **disabled** and **no event actions are executed**.

In the example shown (Fig. 11-7) the period **on Monday from 02:00 to 07:15 am** is inactive. During this period no messages are sent out and no event actions are executed.

➢ Confirm with ***OK*** if you do not want to make any additional settings.

Delete Inactive Periods

➢ Click ***active***.

➢ In the week timer, click and hold the left mouse button and draw a rectangle over an inactive period.

➢ Release the mouse button.

➢ Repeat the last two steps until all relevant inactive periods are deleted.

It is also possible to delete sections (at least 15 minutes) between inactive periods.

➢ Confirm with ***OK*** if you do not want to make any additional settings.

11.3.2 Exceptions

For days with deviations, exceptions can be defined.

Note that exceptions will overwrite the settings of the entire relevant day in the week timer.

➢ Select the ***Exceptions*** tab.

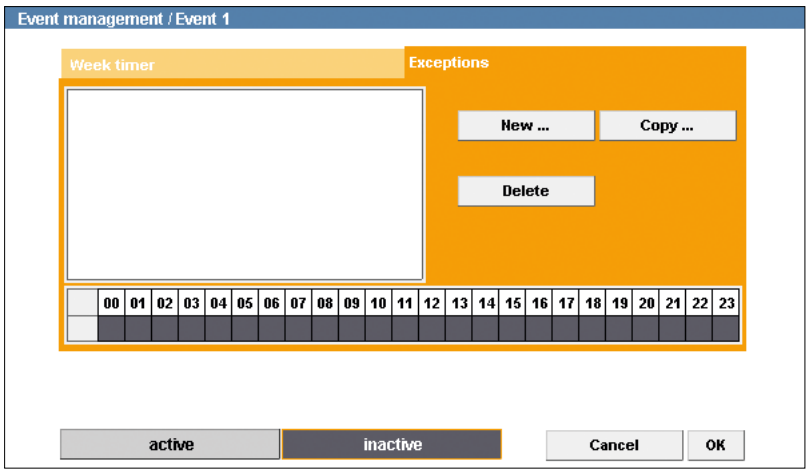


Fig. 11-8

➢ Click ***New ...***.

The ***Calendar*** is displayed.

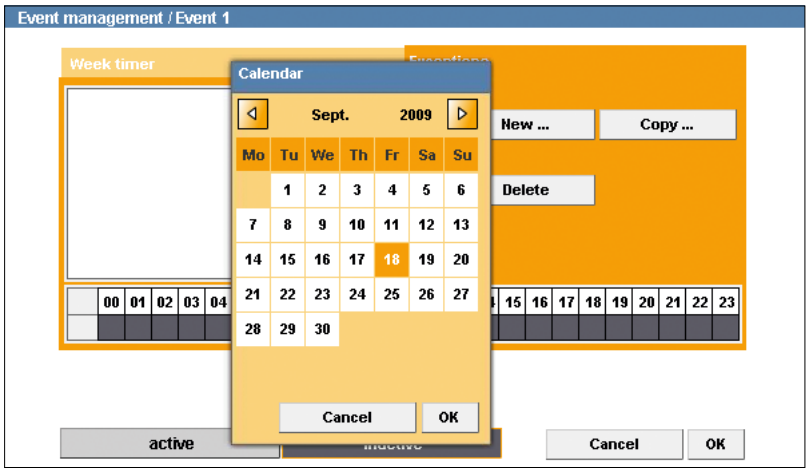


Fig. 11-9

➢ Select a date.

➢ Confirm with ***OK***.

The selected date is added to the exceptions list.

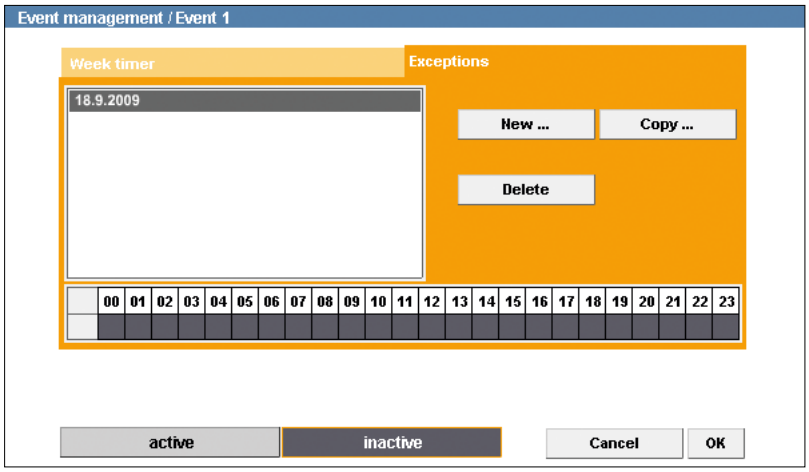


Fig. 11-10

Dark grey areas in the timetable represent **inactive** periods.

During inactive periods the **messaging function** is **disabled** and **no event actions are executed**.

By default, the entire period (24 hours) in the timetable is inactive.

Select Active Periods

- Click ***active***.
- In the timetable, click and hold the left mouse button and draw a rectangle over a relevant period.
- Release the mouse button.
- Repeat the last two steps until all relevant active periods are selected.

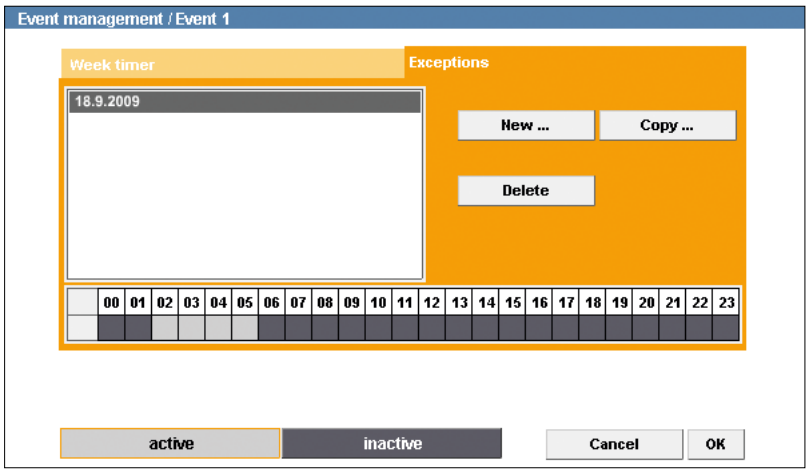


Fig. 11-11

Light grey areas in the timetable represent **active** periods.

During active periods the **messaging function** is **enabled** and **event actions are executed**.

In the example shown (Fig. 11-11) the period **from 02:00 to 06:00 am** is active. During this period messages are sent out and event actions are executed.

- Confirm with ***OK*** if you do not want to make any additional settings.

Delete Active Periods

- Click ***inactive***.
- In the timetable, click and hold the left mouse button and draw a rectangle over an active period.
- Release the mouse button.
- Repeat the last two steps until all relevant active periods are deleted.

It is also possible to delete sections (at least 15 minutes) between active periods.

If the exception settings are to apply to other days, as well, they can be can copied to another date (see below).

- Confirm with ***OK*** if you do not want to make any additional settings.

11.3.3 Copy Exceptions

- Select a date from the exceptions list.
- Click ***Copy ...***.

The ***Calendar*** is displayed.

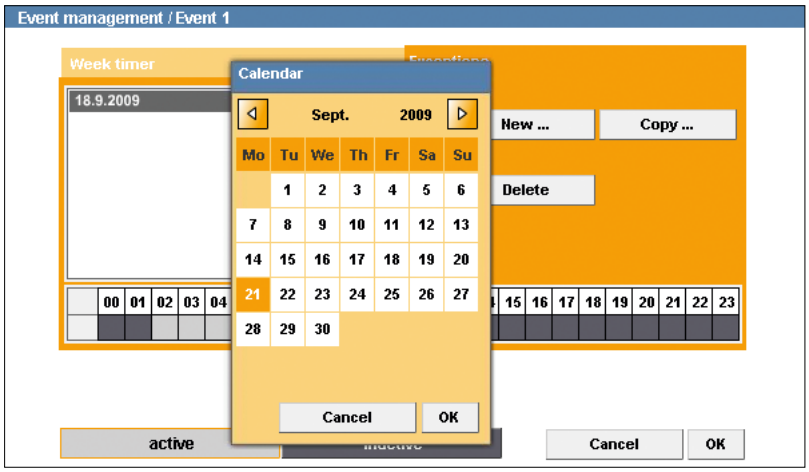


Fig. 11-12

- Select the new date to which you want to copy the exception settings.
- Confirm with ***OK***.

The new date with the copied exception settings is added to the exceptions list.

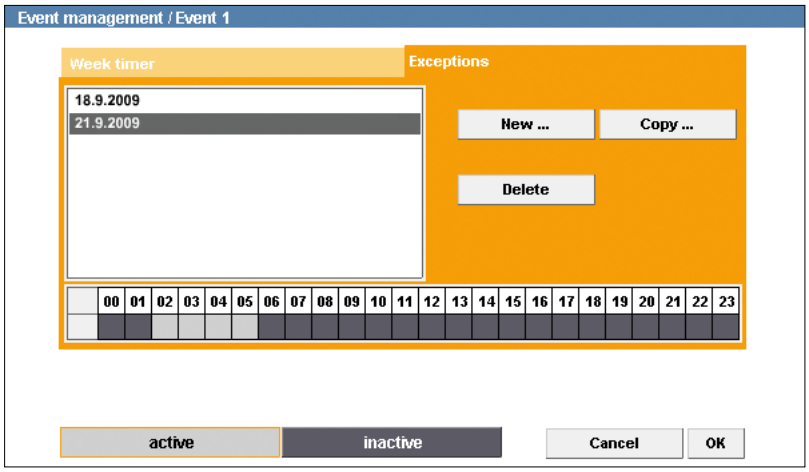


Fig. 11-13

To delete exceptions, select the relevant date in the exceptions list and click “Delete”.

➢ Confirm with ***OK*** if you do not want to make any additional settings.

11.4 Copy Event Settings

The copy function allows you to copy saved event settings to other event handlers.

- Click ***Event management*** in the configuration menu.
- Click on a saved event handler item in the configuration menu.

The related dialogue is displayed.

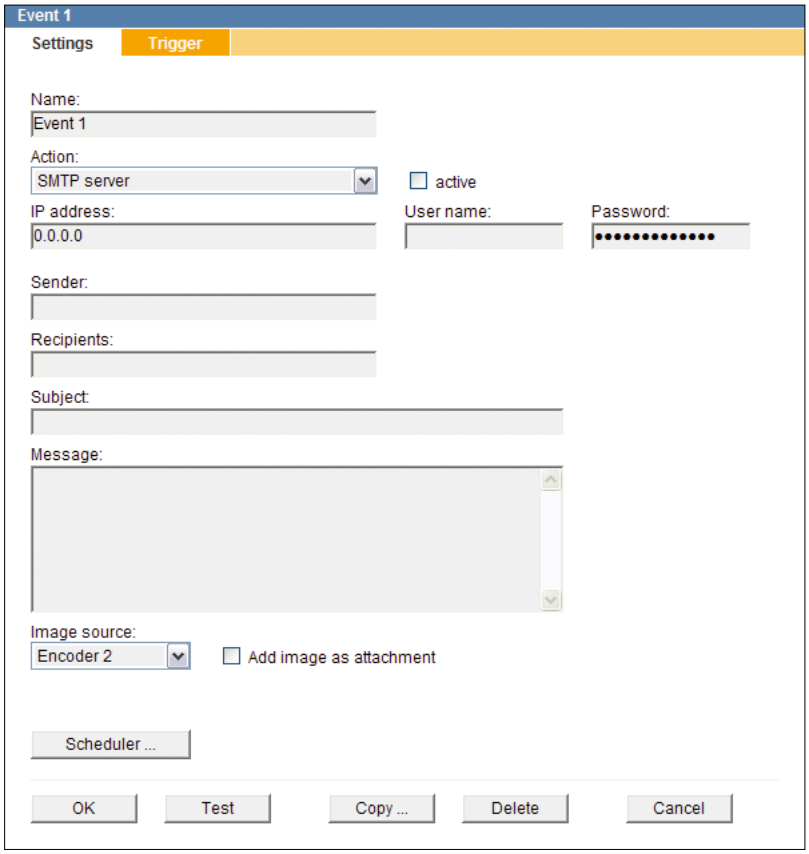


Fig. 11-14

- Click ***Copy ...***.

The configuration menu is expanded with the name of the copied event handler with the addition ***(1)*** (represents copy 1) and the related dialogue of the copy is displayed.

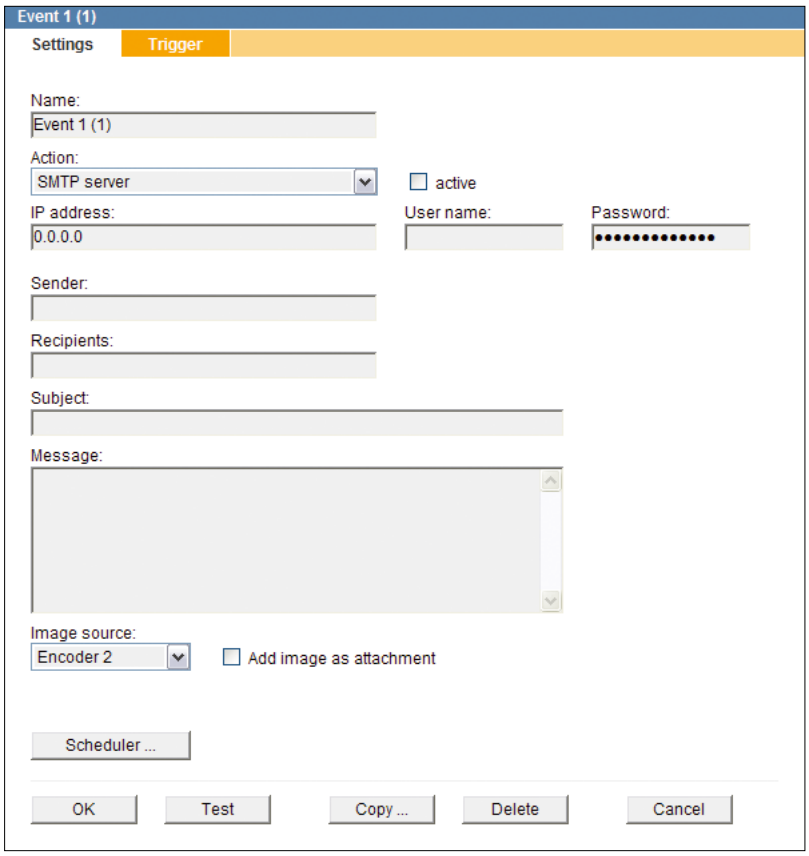


Fig. 11-15

- Customize the relevant settings.
- Finally, confirm with ***OK***.

11.5 Delete Event Handler

To delete an event handler, proceed as follows:

- ➢ Click ***Event management*** in the configuration menu.
- ➢ In the configuration menu, click on an event handler you want to delete.

The related dialogue is displayed.

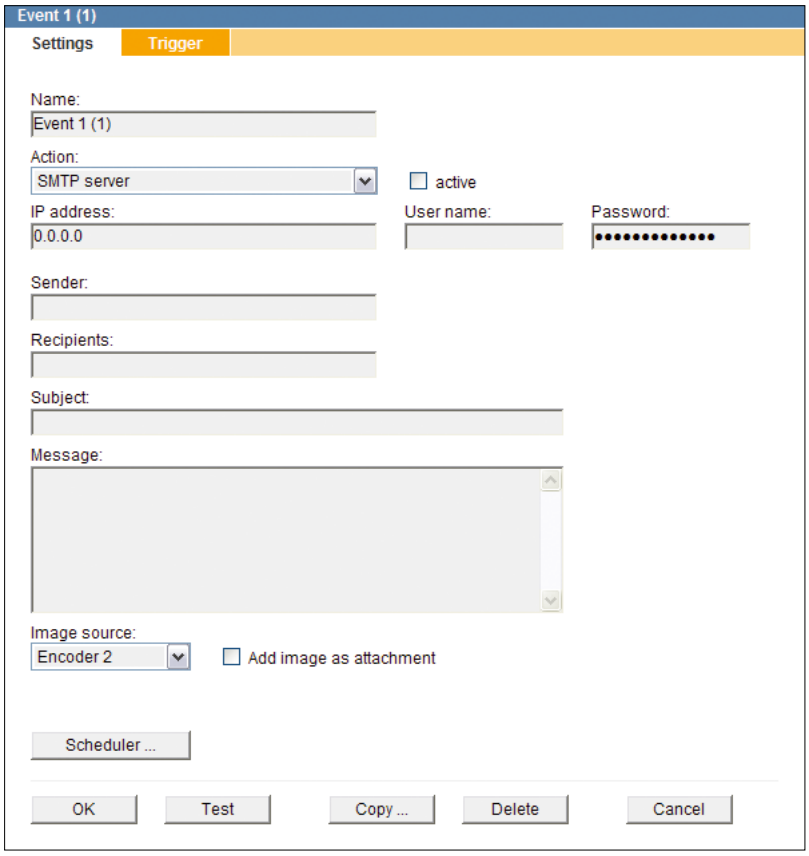


Fig. 11-16

- ➢ Click ***Delete***.

The event handler is deleted and its menu item removed from the configuration menu.

12 Interfaces

12.1 Data Display

The data display function provides the embedding of data transferred from external devices/applications (via the DaVid Protocol).

The embedded data is displayed in the live mode of DaVid Protocol capable devices/applications. A recording of the embedded data has to be configured separately.

For detailed information, refer to the separate documentations of the respective devices.

12.1.1 Filter

The externally transferred data can be filtered before embedding.

The filtering (selection) only takes effect on externally sent data.

➢ Open the ***Data display - Filter*** dialogue via ***Interfaces*** > ***Data display*** > ***Filter ...***.

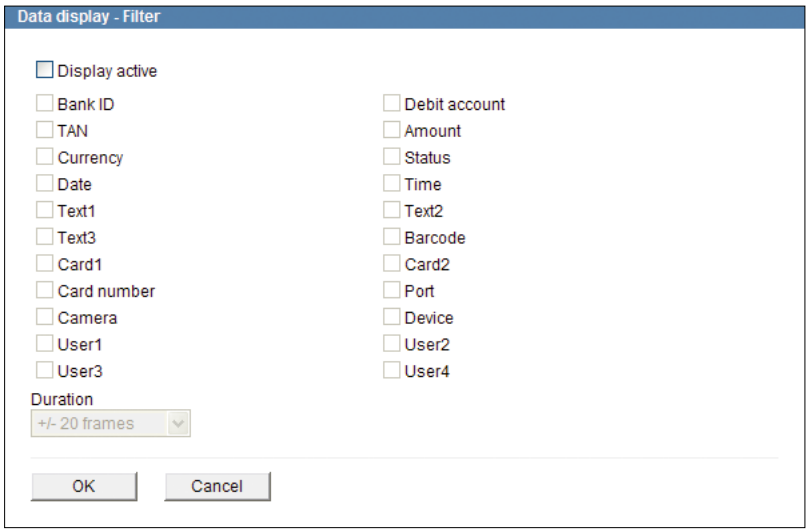


Fig. 12-1

By default, no externally transferred data is embedded.

To embed externally transferred data, proceed as follows:

➢ Activate the ***Display active*** checkbox.
➢ Select the relevant data by activating the related checkbox.
➢ Select the ***Duration***.
➢ Confirm with ***OK***.

The externally transferred data is embedded in the current image (frame) that is captured exactly at the moment when the data is received and stays embedded for the selected ***Duration*** (frames).

12.1.2 Position

The embedded data can be positioned for the live mode display with DaVid Protocol capable devices/applications.

➢ Open the ***Data display - Position*** dialogue via ***Interfaces*** > ***Data display*** > ***Position ...***.

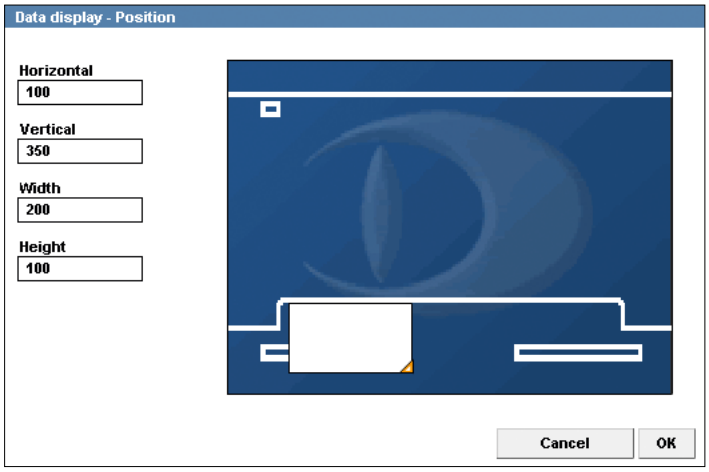


Fig. 12-2

The right-hand side of the dialogue (blue rectangle with Dallmeier logo) represents a exemplary screen for displaying live videos with full “PAL” or “NTSC” resolution.

Note that the aspect ratio and size (resolution) of the actual screen depend on the used client. Specified coordinates are automatically converted (rescaled) for the screen resolution of the used client (e.g. Full HD) and matched to its aspect ratio (e.g. 16:9).

The white lines illustrate the stylized graphical user interface (GUI) of a typical application for displaying live videos.

The white rectangle with the yellow corner (in the bottom right) shows the display area of the embedded data.

On the left-hand side of the dialogue the coordinates and dimensions of the display area are displayed (values in pixels).

The coordinates refer to the top left corner of the display area.

The display area can be positioned by drag & drop.

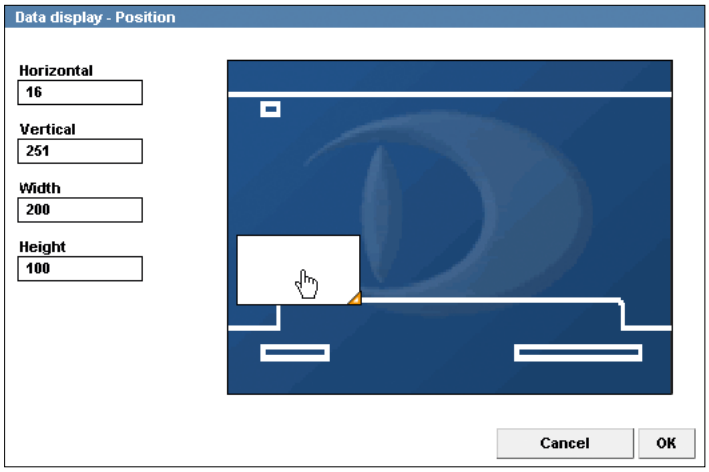


Fig. 12-3

The display area can be resized by dragging its yellow corner (in the bottom right).

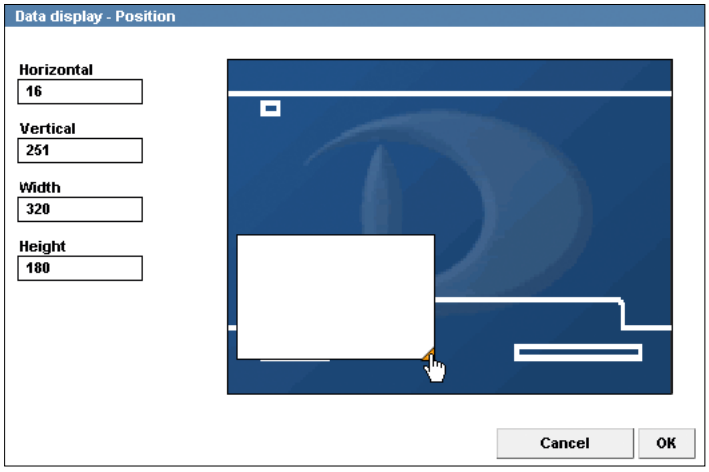


Fig. 12-4

An exact positioning and resizing is possible by using the corresponding input fields.

- ➢ Adjust all relevant settings.
- ➢ Confirm with ***OK***.

13 Digital Image Shift

The “Digital Image Shift” function allows for a subsequent fine alignment of the selected image section.

Depending on the set resolution, a certain area of the sensor is in each case used to capture the image, yet never the entire sensor area.

By using Digital Image Shift, the used sensor area can be digitally shifted and thus the monitored image section can be fine-tuned.

That function is particularly useful if, once the camera has been installed, it turns out that the selected image section does not exactly meet your requirements.

➢ Click ***Digital Image Shift ...*** in the configuration menu.

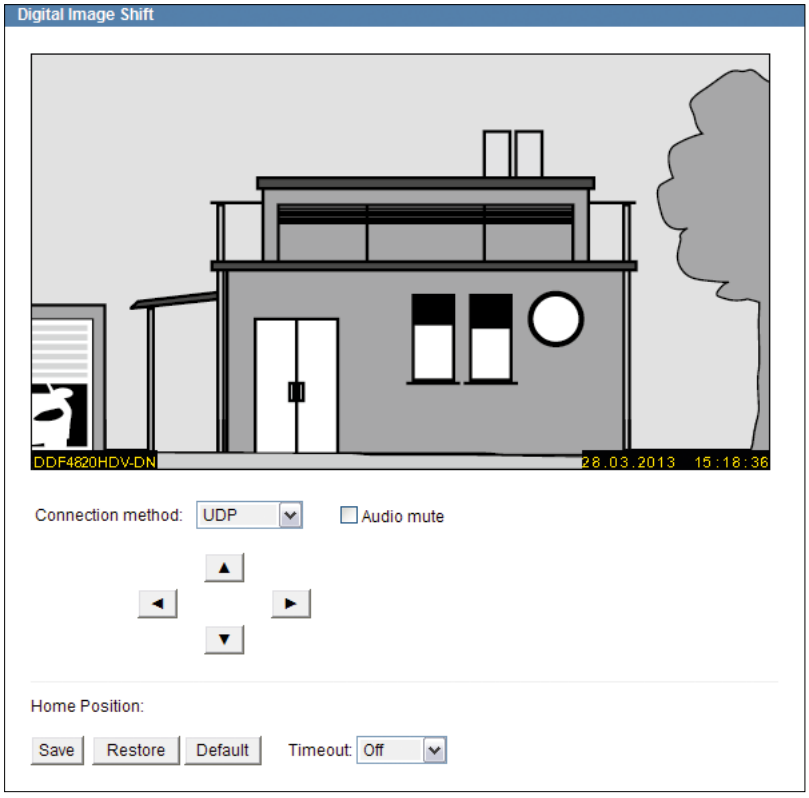


FIg. 13-1

In the example above, the defined image section does not exactly meet the requirements following the installation of the camera.

The garage (on the left of the image) is only half captured by the image capturing sensor.

However, using the arrow buttons the image section can be easily shifted via the web browser afterwards.

➢ Left-click on an ***arrow button*** in order to shift the image section accordingly.

Left-click and hold an arrow button longer in order to shift the image section faster.

In the example below, the image section was shifted until the garage (on the left of the image) is completely covered by the image capturing sensor.

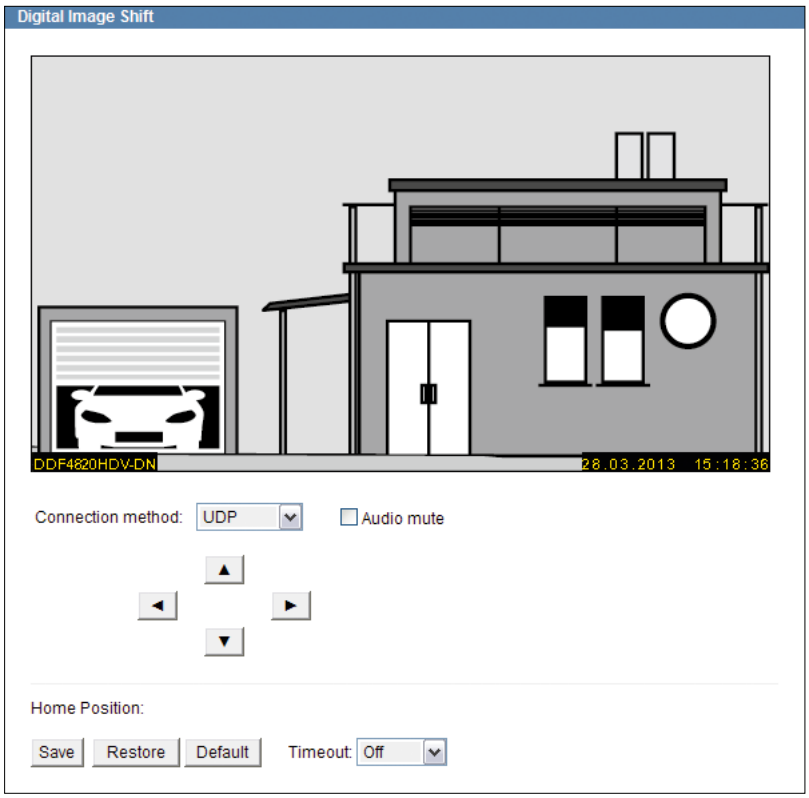


FIg. 13-2

- In order to apply the new image section, click ***Save***.
- If you want to restore the previously saved new image section, click ***Restore***.
- To restore the standard image section, click on ***Default***.

Using the time-out function, allows you to activate the automatic recovery of the last saved image section.

14 Lens Control

The camera is equipped with a motor-driven varifocal P-Iris lens.

The focal length (zoom) and the focus are adjusted in the ***Lens Control*** dialogue.

Note that the Microsoft Internet Explorer is required and the ActiveX-based Dallmeier control must be installed in order to display the live video.

➢ Click ***Lens control …*** in the configuration menu to open the ***Lens Control*** dialogue.

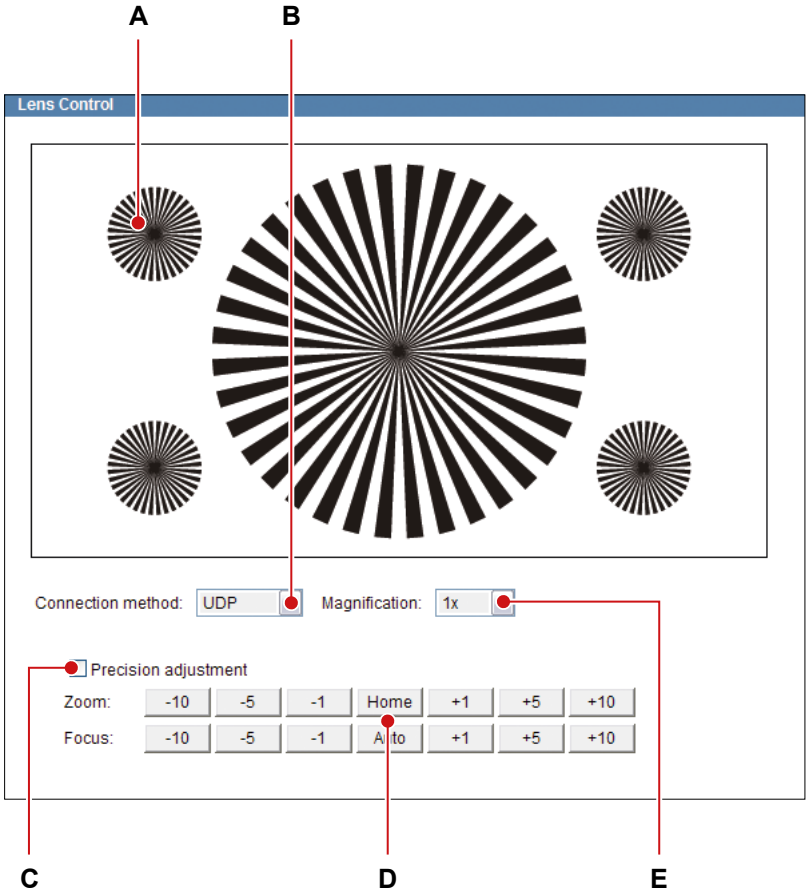


Fig. 14-1

A Live video (image is illustrative only)

B UDP or TCP connection (see section “Connection Method” on page 30)

C Precision adjustment of zoom and focus

D Zoom In (+) / Zoom Out (−)
incl. Auto Home Position

Far Focus (+) / Near Focus (−)
incl. One-Push Autofocus

E Scale live video for more details
(if >1×, click and drag the mouse to move image section)

➢ Observe the notes and recommendations mentioned below.

➢ Adjust the relevant settings.

For best focusing results during the camera installation, P-Iris automatically selects the widest aperture and, with it, the smallest depth of field. Hence, it is able to achieve perfect image sharpness regardless of the lighting conditions.

After 20 – 25 seconds without user action the diaphragm opening (aperture) of the P-Iris lens is automatically set to its previous f-stop position.

NOTICE

Damage to the lens unit

Do not attempt to manually adjust the focal length (zoom) and the focus on the lens unit.

Reduce the encoding data/bit rate to minimize long delays (response times) during zoom and focus control with low bandwidth connections.

Disable the DirectX option in the "User interface" dialogue (see section "User Interface" on page 33) if the live video turns black at the scale rate of 8× (or rather is not displayed).

15 Service and Info

15.1 Downloads

This dialogue allows you to download the following files directly from the device:

- Dallmeier Live Video ActiveX
- MIB file of the device for SNMP applications

The Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network elements (cameras, recorders, routers, switches, printers, etc.) with a Network Management System (NMS).

MIB files allow for the unambiguous assignment of network elements within the Management Information Base (MIB) of the network management system.

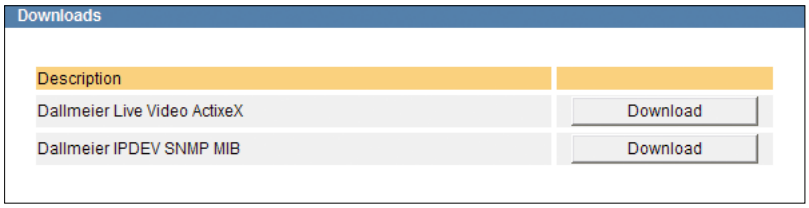


Fig. 15-1

15.2 Factory Settings

The device can be reset to its default settings at any time.

Open the ***Factory settings*** dialogue via ***Service*** > ***Factory settings …***.

The ***Factory settings*** dialogue is displayed.

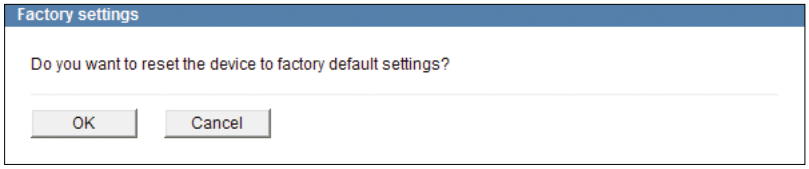


Fig. 15-2

➢ Confirm with ***OK*** to reset the device to its factory default settings.

15.3 Licenses

The ***License*** dialogue allows you to activate possible extra features.
For information about available extra features, contact the Dallmeier Support.
For purchasing license codes, contact the Dallmeier Sales Department.

➢ Open the ***License*** dialogue via ***Service*** > ***License ...***.

Fig. 15-3

➢ Enter the ***License code***.
➢ Confirm with ***OK***.

15.4 Event Log

The device logs IP addresses of applications that temporarily blocked certain resources of the device in a log file. The list of IP addresses is displayed in the ***Event log*** dialogue.

➢ Open the ***Event log*** dialogue via ***Service*** > ***Event log ...***.

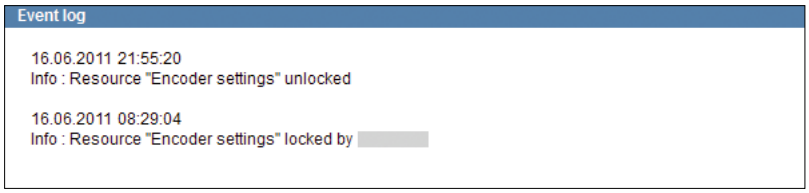


Fig. 15-4

15.5 Configuration File

The configuration of the device can be exported to a file and thus be saved.

In addition to the configuration recovery of the device that is currently connected, the saved configuration can also be transferred to several devices simultaneously.

15.5.1 Download

NOTICE

If the configuration file is to be transferred to several devices, the ***Network settings*** must not be exported.

➢ Open the ***Configuration file management*** dialogue via ***Service*** > ***Configuration file*** > ***Download ...***.

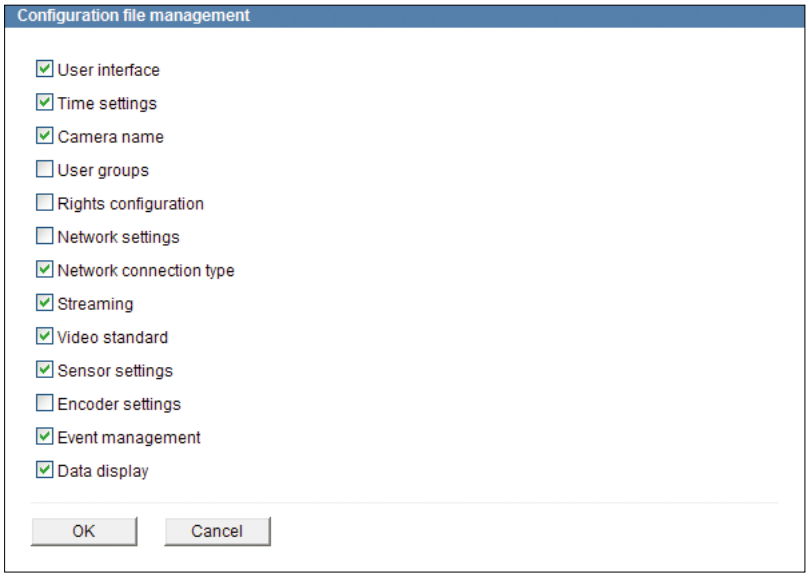


Fig. 15-5

➢ Select all relevant settings which are to be exported to the configuration file by activating the related checkboxes.

➢ Confirm with ***OK***.

➢ Follow the instructions of the download dialogue and save the configuration file to a data storage device.

The configuration file name contains the IP address of the related device.

15.5.2 Upload

The saved configuration file can be transferred to an individual device. This allows for the recovery of the configuration of the device that is currently connected.

In addition, the configuration file can also be transferred to several devices simultaneously. This is a very effective method to identically configure several devices in terms of certain configuration groups.

15.5.2.1 Configuration Recovery

To recover the configuration of an individual device, the connection to the device must be established first (see section “Connection” on page 29).

➢ Open the ***Configuration file management*** dialogue via ***Service*** > ***Configuration file*** > ***Upload ...***.

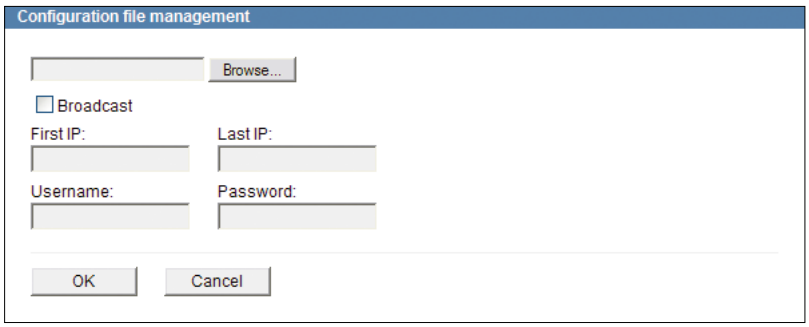


Fig. 15-6

➢ Click ***Browse...***.
➢ Select the relevant configuration file on your data storage device.
➢ Confirm with ***OK***.

At the end of the transfer a list of the transferred (or skipped) configuration settings is displayed.

15.5.2.2 Configuration Transfer to Several Devices

As a precondition all relevant devices must be located in the same LAN (with suitable cabling and a separate IP address for each device). In addition, the access rights to all devices must be identical (same user name and password).

Before the configuration file can be transferred, it must be saved as described above.

However, the configuration of the ***Network settings*** must not be included in the configuration file. If these settings were included, the same IP address would be transferred to all devices. Since, however, every IP address in a LAN must be unique, this would cause massive problems in the network.

NOTICE

Ensure that the configuration of the ***Network settings*** is not transferred to several devices.

To be able to send the configuration file to several devices, a connection to one of the devices must be established first (see section “Connection” on page 29).

➢ Open the ***Configuration file management*** dialogue via ***Service*** > ***Configuration file*** > ***Upload ...***.

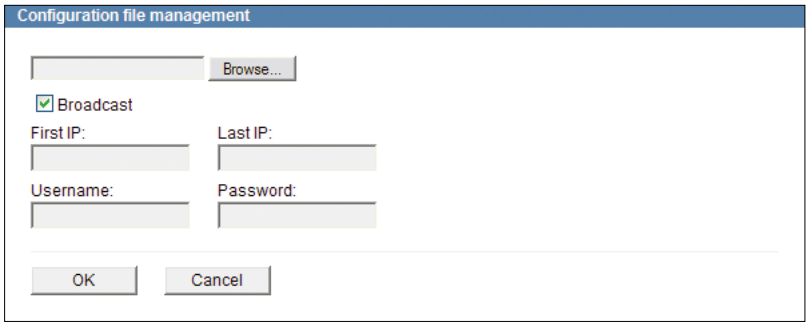


Fig. 15-7

➢ Click ***Browse…***.
➢ Select the relevant configuration file on your data storage device.
➢ Activate the ***Broadcast*** checkbox.
➢ Enter the ***First IP*** address and the ***Last IP*** address of the relevant device group.
➢ Enter the ***Username***.
➢ Enter the ***Password***.
➢ Confirm with ***OK***.

At the end of the transfer a list of the transferred (or skipped) configuration settings is displayed.

15.6 Info

General information about the device is displayed in the ***Info*** dialogue.

➢ Click ***Info …*** in the configuration menu.

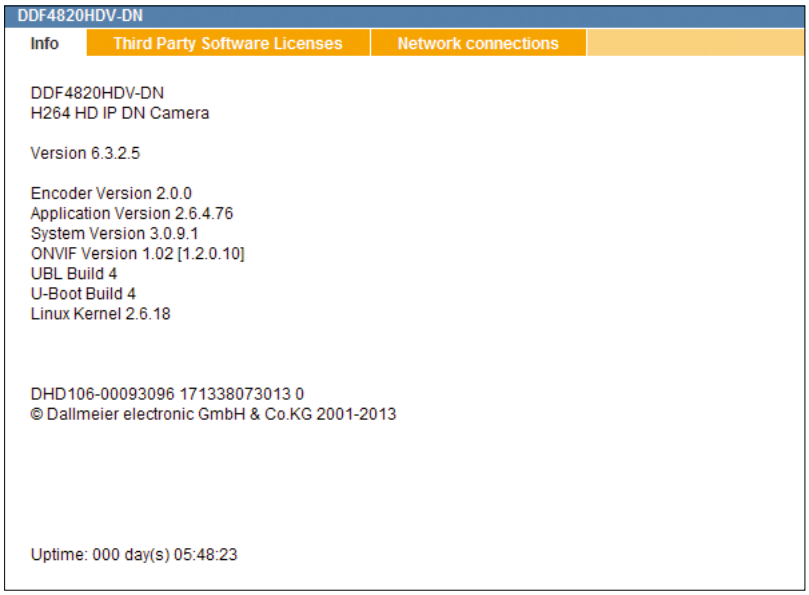


Fig. 15-8

Among other things, the following information is displayed:

- Device type
- Software version
- Version number of the encoder
- ONVIF version
- Version number of the Linux Kernel
- Serial number of the device
- Uptime

Information about the network connections is displayed in the ***Network connections*** tab.

16 Image Transmission

The device can be configured as an active network element for the continuous transmission (streaming) of the produced video data (see section “Video Server” on page 47).

In addition, the device, as a passive network element, can be triggered for transmission of video data via various transport and data protocols by external devices and applications.

16.1 Web Browser

Current video data can be requested as a single image (JPEG) by any web browser.

Transmission protocol	HTTP
Transport protocol	TCP
Port	80

Note that

- the used encoder must be configured for ***MJPEG*** encoding.
- the used encoder must be enabled.
- the ***JPEG live access*** right/permission must be enabled.

Use the following URL request for the various encoders:

Encoder 1	`http://IP address of the device/live/image0.jpg`
Encoder 2	`http://IP address of the device/live/image1.jpg`

The displayed image can be refreshed at any time. The URL request can be integrated in an HTML (JavaScript) page that refreshes the image automatically.

16.2 RTSP Application

The live video can be actively requested and controlled (start and stop) by external RTSP capable applications. For more information, refer to section “RTSP” on page 51.

Communication protocol	RTSP
Transmission protocol	RTP
Transport protocol	UDP/TCP
Port	554

Note that

- the used encoder must be enabled.
- the RTSP server in the camera must be enabled.
- the ***RTSP live access*** right/permission must be enabled.

Use the following URL request for the various encoders:

Encoder 1 `rtsp://IP address of the device/encoder1`
Encoder 2 `rtsp://IP address of the device/encoder2`
Encoder 3 `rtsp://IP address of the device/encoder3`

Encoder 1, 2 and 3 can be requested by three applications simultaneously. This allows you to realize a “Tri-Streaming” functionality (three streams with different quality).

The required bandwidth proportionally increases to the number of applications requesting for the data of an encoder. In this case, a multicast configuration should be preferred, because it only requires bandwidth for one stream.

17 Maintenance

The housings of the units may only be opened by qualified personnel for commissioning, inspection, maintenance and repair.

Cleaning

If it is necessary to clean the devices, observe the following notes:

NOTICE

Damage to the surface of the devices

- Clean the housings (outside) with a soft, dry and antistatic cloth.
  Do not use detergents.
- Clean the plastic bubbles with water and some dishwashing agent using a soft, non-linting cloth or sponge.
  Do not wipe the bubbles dry.
  Do not use common glass cleaners.
  Avoid excessive rubbing.
  Dry gently with a clean dry cloth to avoid scratching the surface.

18 Pin Assignment

The installation and commissioning of the units may only be carried out by qualified personnel.

⚠ WARNING

Electric shock hazard

Danger of death or serious injury

- Always disconnect the PoE switch or the separate power supply unit from the mains socket (pull out the power plug) before connecting or disconnecting the devices.

NOTICE

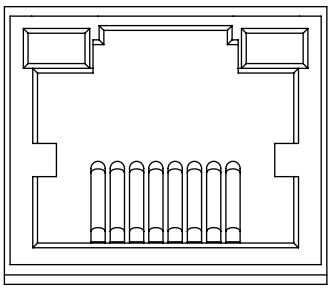
Damage to the units resulting from improper power supply

The devices can be powered via PoE (Power over Ethernet, Class 0) or supplied with a separate 12 V DC power supply unit.

However, always beware not to use both power sources simultaneously.

In order to comply with UL's requirements, always use a UL-certified, Limited Power Source (LPS) Class 2 power supply unit when operating the devices with a separate power supply unit.

18.1 LAN/PoE

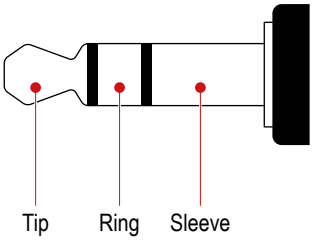


RJ45 jack

10BASE-T-/100BASE-TX-PoE
PoE conformity IEEE 802.3af

Fig. 18-1

18.2 Audio OUT / Microphone IN



Audio OUT / Microphone IN (3.5 mm phone jack, for stereo plug)

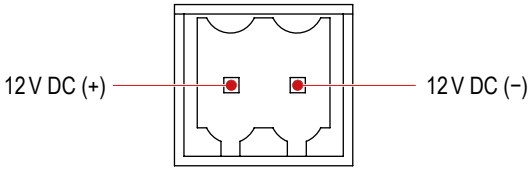
Fig. 18-2

	Audio OUT (mono)	**Microphone IN (mono)**
Tip	Signal	*Not used*
Ring	*Not used*	Signal
Sleeve	Ground	Ground

NOTICE

For a clean (interference-free) audio signal transmission, the Audio IN/OUT Y-Cable Connector FGA-30 is required (optionally available).

18.3 Power IN



Weidmüller male connector SL 3.50/02/90G

Fig. 18-3

19 Technical Data

The following basic technical data was valid at the time of this document's compilation.

Detailed specifications and possible updates for each device can be found in the corresponding current product data sheet on www.dallmeier.com.

The following specifications are valid for all devices described in this document, unless otherwise indicated.

Specifications

Sensor	1/2.5" 5-megapixel CMOS image sensor
Video output	1× BNC: CVBS, analogue SD video preview output, for local installation only
Audio OUT / Microphone IN (each mono signal)	1× 3.5 mm phone jack (for stereo plug)[7] Microphone IN: max. 63 mV (RMS), input resistance 10 kOhm, internal gain 20 dB
Ethernet	1× RJ45 jack, 10BASE-T/100BASE-TX PoE
Voltage supply	12 V DC ±10% or via PoE (Class 0)
PoE standard	IEEE 802.3af
Power consumption	Max. 4.5 W
Dimensions	In-ceiling mount variant: approx. Ø 170 × H 135 mm (Ø 6.7 × H 5.3 inches) Surface mount variant: approx. Ø 153 × H 135 mm (Ø 6.0 × H 5.3 inches)
Weight	In-ceiling mount variant: approx. 1200 g (2.6 lb) Surface mount variant: approx. 1100 g (2.4 lb)
Mechanical adjustment	3-axis mount: Pan ±90°, Tilt ±90°, Rotation 360°
Operating temperature	In-ceiling mount variant (indoor): 0 °C to +35 °C (32 °F to 95 °F) Surface mount variant (indoor and outdoor): −10 °C to +40 °C (14 °F to 104 °F)
Relative humidity	0 % – 90 % RH, non-condensing
IP rating	IP67 (surface mount variant only)
IK code[8]	IK10 (EN 62262, IEC 62262:2002)
Approvals/certifications	CE, FCC, ACA, UVV "Kassen" (DGUV Test), UL DIN EN 50130-4 compliant

7) Audio IN/OUT Y-Cable Connector FGA-30 required (optionally available)
8) Protection against external mechanical impacts

20 Technical Drawings

The following technical drawings were valid at the time of this document's compilation. Visit www.dallmeier.com for possible updates.

20.1 In-ceiling Mount Variant (IM)

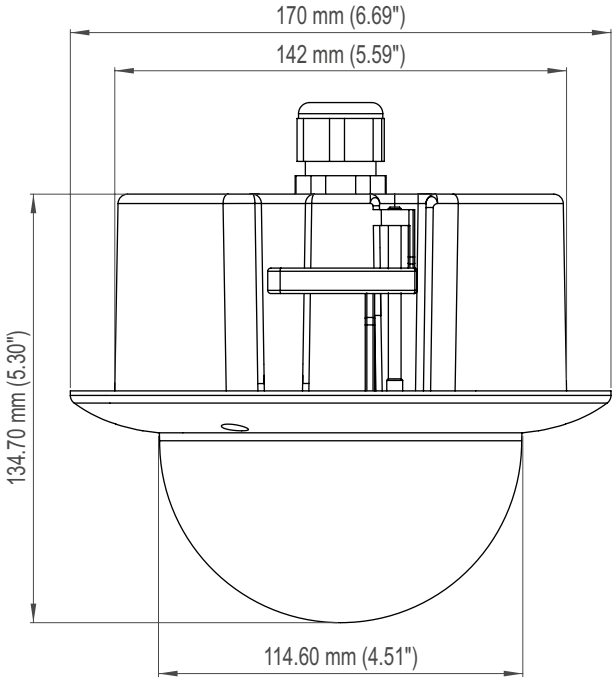


Fig. 20-1

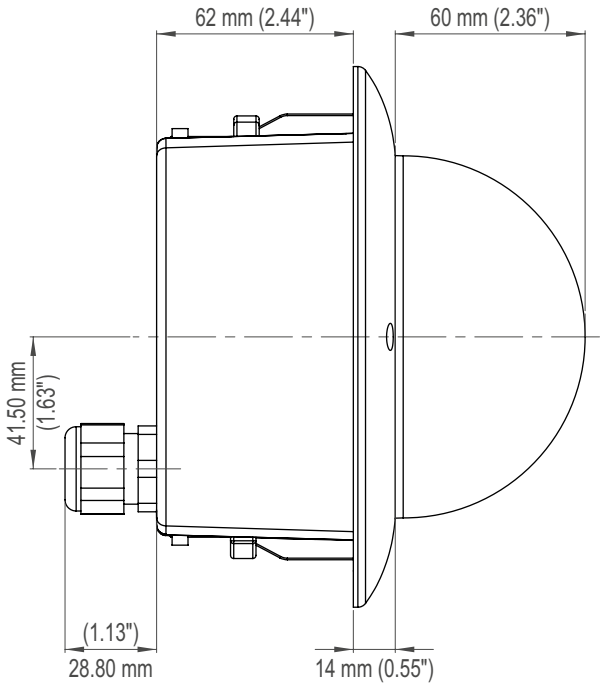


Fig. 20-2

20.2 Surface Mount Variant (SM)

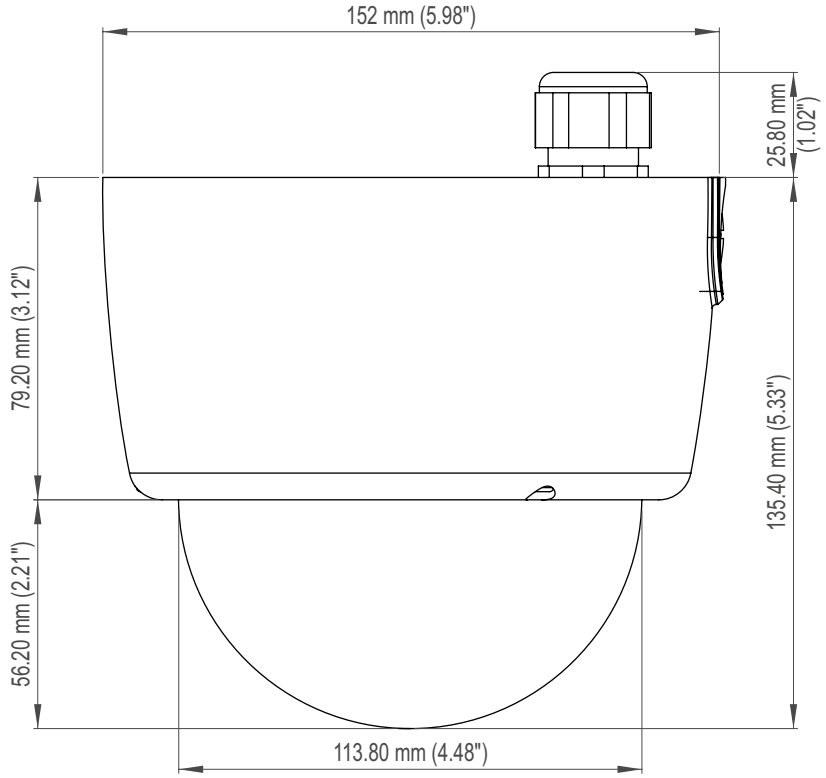


Fig. 20-3

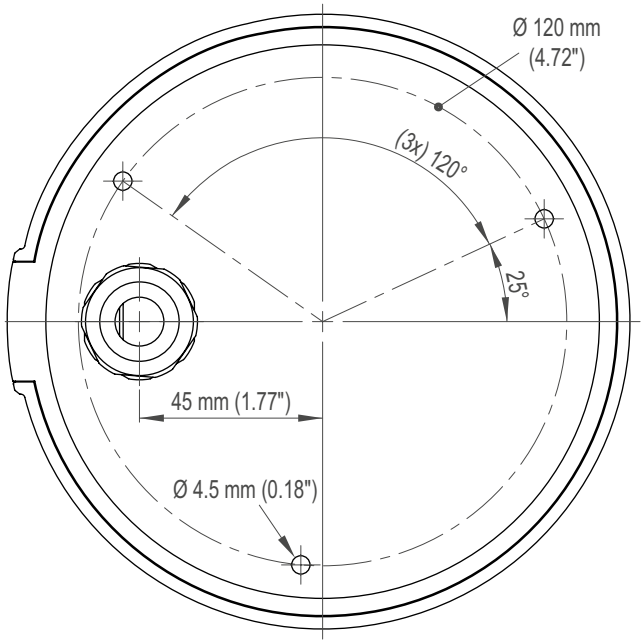


Fig. 20-4

CE

Declaration of Conformity

This declaration is valid for following product:

Equipment: HD Network Dome Camera
Type: DDF4820HDV-DN

Hereby the equipment is confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (2004/108/EC).
The object of the declaration described above is in conformity with Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of certain hazardous substances in electrical and electronic equipment.

The following company is responsible for this declaration:

Dallmeier electronic GmbH & Co.KG
Cranachweg 1
93051 Regensburg
Germany

The measurements were carried out in accredited laboratories.

For the evaluation of above mentioned Council Directives for Electromagnetic Compatibility following standards were consulted:

DIN EN 55022:2006 + A1:2007 Class A
DIN EN 61000-3-2:2006 + A1:2009 + A2:2009
DIN EN 61000-3-3:2008
DIN EN 50130-4:1995 + A1:1998 + A2:2003

Regensburg, 2013-02-11

Dieter Dallmeier
-CEO-