

# Configuration

## Firmware Version

# 8.3.2.22

### Dome Cameras

DDF5400HDV-DN  
DDF5300HDV-DN  
DDF5200HDV-DN

### Module Camera

MDF5200HD-DN

### Box Cameras

DF5300HD-DN  
DF5200HD-DN

### IR Cameras

DF5400HD-DN/IR  
DF5200HD-DN/IR

*Products for Solutions*



Rev. 1.0.0 / 2017-06-27



 **Dallmeier**



## Information about Copyright, Trademarks, Design Patents

© 2017 Dallmeier electronic

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.

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  
Bahnhofstr. 16  
93047 Regensburg  
Germany

Phone: +49 941 8700-0  
Fax: +49 941 8700-180

[www.dallmeier.com](http://www.dallmeier.com)  
[info@dallmeier.com](mailto:info@dallmeier.com)

All trademarks identified by \* are registered trademarks of Dallmeier electronic.

All trademarks identified by \*) are trademarks or registered trademarks of the following owners:

Apple and Safari of Apple Inc. headquartered in Cupertino, California, USA;  
Google and Google Chrome of Google Inc. headquartered in Mountain View, California, USA;  
JavaScript of Oracle Corporation (and/or its affiliates) headquartered in Redwood Shores, California, USA;  
Linux of Linus Torvalds (in the USA and/or other countries);  
Microsoft, Internet Explorer, Windows, and Windows Vista of Microsoft Corporation headquartered in Redmond, Washington, USA;  
Mozilla and Firefox of Mozilla Foundation headquartered in Mountain View, California, USA.

Third-party trademarks are named for information purposes only.

Dallmeier electronic respects the intellectual property of third parties and always attempts to ensure the complete identification of third-party trademarks and indication of the respective holder of rights. In case that protected rights are not indicated separately, this circumstance is no reason to assume that the respective trademark is unprotected.

# Contents

|  |           |
|--|-----------|
| <b>Chapter 1: Introduction</b> .....         | <b>6</b>  |
| 1.1 Validity .....                           | 6         |
| 1.2 Disclaimer .....                         | 6         |
| 1.3 Documents .....                          | 7         |
| 1.3.1 This Document .....                    | 7         |
| 1.3.2 Other Applicable Documents .....       | 7         |
| 1.4 Typographical Conventions .....          | 8         |
| <b>Chapter 2: Connection and Login</b> ..... | <b>9</b>  |
| 2.1 System Requirements .....                | 9         |
| 2.2 Connection .....                         | 10        |
| 2.3 Login .....                              | 11        |
| <b>Chapter 3: Language</b> .....             | <b>12</b> |
| <b>Chapter 4: Image</b> .....                | <b>13</b> |
| 4.1 Presets .....                            | 13        |
| 4.2 Image Optimization .....                 | 16        |
| 4.2.1 White Balance .....                    | 17        |
| 4.2.2 Color Temperature .....                | 18        |
| 4.2.3 Local Tone Mapping .....               | 19        |
| 4.2.4 Auto Contrast .....                    | 20        |
| 4.2.5 Noise Filter .....                     | 21        |
| 4.3 Exposure Settings .....                  | 22        |
| 4.3.1 Exposure Mode .....                    | 22        |
| 4.3.2 Slow Shutter Limit .....               | 22        |
| 4.3.3 Gain Limit .....                       | 22        |
| 4.3.4 Flicker-Control .....                  | 22        |
| 4.3.5 Exposure Priority .....                | 23        |
| 4.3.6 Aperture Mode .....                    | 23        |
| 4.4 Day/Night .....                          | 24        |
| 4.4.1 Day/Night Mode .....                   | 24        |
| 4.4.2 Threshold Level .....                  | 25        |
| 4.4.3 Response Time .....                    | 25        |
| 4.4.4 Color .....                            | 25        |
| 4.4.5 Lighting Mode DF5200HD-DN/IR .....     | 26        |
| 4.4.6 Lighting Mode DF5400HD-DN/IR .....     | 27        |
| 4.5 Lens Control .....                       | 28        |
| 4.6 Privacy Zones .....                      | 29        |
| 4.7 Text-Overlay .....                       | 30        |
| <b>Chapter 5: Video</b> .....                | <b>31</b> |
| 5.1 Sensor Settings .....                    | 32        |
| 5.2 Audio Out .....                          | 33        |
| 5.3 Encoder Settings .....                   | 34        |
| <b>Chapter 6: Time</b> .....                 | <b>37</b> |
| 6.1 Manual Configuration .....               | 37        |
| 6.2 Time Server .....                        | 38        |

|  |           |
|--|-----------|
| <b>Chapter 7: Network</b> .....                            | <b>39</b> |
| 7.1 Basic Settings .....                                   | 39        |
| 7.1.1 Automatic Network Setup via DHCP .....               | 42        |
| 7.1.2 Manual Network Setup .....                           | 43        |
| 7.2 Bandwidth Limit .....                                  | 44        |
| 7.3 Streaming .....  | 44        |
| 7.4 Time Server .....                                      | 47        |
| 7.5 Network Services .....                                 | 48        |
| 7.6 Security .....   | 51        |
| <b>Chapter 8: EdgeStorage</b> .....                        | <b>52</b> |
| <b>Chapter 9: Event Management</b> .....                   | <b>53</b> |
| <b>Chapter 10: Data Display</b> .....                      | <b>55</b> |
| 10.1 Duration .....  | 56        |
| 10.2 Position .....  | 56        |
| 10.3 Filter .....  | 57        |
| 10.4 RTCP .....  | 57        |
| <b>Chapter 11: Video Content Analysis (VCA)</b> .....      | <b>58</b> |
| 11.1 Requirements .....                                    | 59        |
| 11.2 Analysis .....  | 59        |
| 11.2.1 General Settings .....                              | 60        |
| 11.2.2 Expert Settings .....                               | 62        |
| 11.2.3 Object Sizes .....                                  | 64        |
| 11.2.4 Ignore Mask .....                                   | 66        |
| 11.3 Intrusion Detection .....                             | 69        |
| 11.4 Tamper Detection .....                                | 71        |
| 11.4.1 Camera Tamper Detection .....                       | 71        |
| 11.4.2 Lights On/Off Detection .....                       | 72        |
| 11.5 Object Classification .....                           | 73        |
| 11.5.1 Object Classification by Persons and Vehicles ..... | 73        |
| 11.5.2 Face Detection .....                                | 74        |
| 11.6 Line Crossing Detection .....                         | 75        |
| 11.7 Objects & Events .....                                | 76        |
| <b>Chapter 12: Users and Rights</b> .....                  | <b>78</b> |
| 12.1 User Names and Passwords .....                        | 78        |
| 12.2 Users .....   | 79        |
| 12.3 Groups .....  | 80        |
| 12.4 Rights .....  | 81        |
| 12.5 Anonymous Access .....                                | 81        |
| <b>Chapter 13: Service</b> .....                           | <b>83</b> |
| 13.1 Configuration File .....                              | 83        |
| 13.2 Factory Settings .....                                | 84        |
| 13.3 Service .....   | 84        |
| <b>Chapter 14: Information</b> .....                       | <b>85</b> |
| 14.1 General Information .....                             | 85        |
| 14.2 Network connections .....                             | 85        |

|   |           |
|---|-----------|
| <b>Chapter 15: Image Transmission</b> ..... | <b>86</b> |
| 15.1 Single Image (JPEG) .....              | 86        |
| 15.2 RTSP Application .....                 | 87        |

# Chapter 1:

## Introduction

### 1.1 Validity

This document applies to the following Dallmeier HD cameras:

|   |  |   |
|---|--|---|
| <b>Dome Cameras</b> <ul style="list-style-type: none"><li>• DDF5400HDV-DN</li><li>• DDF5300HDV-DN</li><li>• DDF5200HDV-DN</li></ul> | <b>Box Cameras</b> <ul style="list-style-type: none"><li>• DF5300HD-DN</li><li>• DF5200HD-DN</li></ul> | <b>IR Cameras</b> <ul style="list-style-type: none"><li>• DF5400HD-DN/IR</li><li>• DF5200HD-DN/IR</li></ul> |
| <b>Module Camera</b> <ul style="list-style-type: none"><li>• MDF5200HD-DN</li></ul>   |  |   |

The descriptions in this document are based on the firmware version **8.3.2.22** and apply to all above-mentioned Dallmeier HD cameras.

For reasons of simplicity, the term “device” or “camera” is used in the following. However, if passages in the text require distinctions between the individual devices, the complete product names will be mentioned instead.

Figures (screenshots) in this document may differ from the actual product.

### 1.2 Disclaimer

This documentation includes the full functionality of the above-mentioned firmware version.

However, note that

- certain functions and features are only available if supported by the hardware.
- the functional range of the devices depends on the ordered equipment or device variant and may differ from the contents of this documentation.
- certain functions and features may require purchasing a license.

## 1.3 Documents

The product documentation for the device contains several documents which are included in the scope of delivery in a printed form and/or on a digital medium. Additional information, if available, is provided exclusively on the website [www.dallmeier.com](http://www.dallmeier.com).

Read all documents included in the delivery carefully and thoroughly before using the respective device. Always follow the instructions, notes and warnings and observe the technical specifications in the relevant product data sheet.

Keep all documents in legible condition and in a suitable location for future reference.

Regularly check the website [www.dallmeier.com](http://www.dallmeier.com) for the latest updates on product documentation (and product firmware).

### 1.3.1 This Document

The document “Configuration” (this document) contains detailed descriptions of the configuration of the respective device.

The target audience of this document is trained system integrators.

### 1.3.2 Other Applicable Documents

#### **Data sheet**

The product data sheet contains detailed technical specifications, features and characteristics of the respective device.

The target audience of the document is trained system integrators.

#### **Commissioning**

The document “Commissioning” contains detailed descriptions of the installation, connection and commissioning of the respective device as well as information on the appropriate use, safety instructions and general notes.

The target audience of the document is trained system integrators.

## 1.4 Typographical Conventions

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

### NOTICE



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

---

Instructions are indicated by arrows ( $\Rightarrow$ ).

$\Rightarrow$  Always carry out instructions one after the other in the sequence described.

“Expressions” in quotation marks generally indicate a control element on the device (switches or labels) or on its user interface (buttons, menu items).




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



# Chapter 2:

## Connection and Login


The configuration of the device is carried out with a PC and web browser over the Local Area Network (LAN).

 *Alternatively, the PC can be connected directly to the device via an Ethernet crossover cable (for devices which are powered with Power-over-Ethernet, a PoE injector is additionally required).*

### 2.1 System Requirements

The configuration of the device has no special requirements on the client PC. It can be performed with any PC or laptop that corresponds to the current state of the art.

With respect to the configuration, the user interface and the integrated functions are independent of the operating system or web browser. The download and installation of plug-ins is not required.

 *The live preview in the configuration dialogs is displayed with a frame rate of 1 fps.*

| System Requirements   |  |
|-----------------------|--|
| Operating system (OS) | Any, with the current state of the art (e.g. Microsoft® Windows® 7/8/10, Mac® OS X, Linux®)                                |
| Graphics card         | Any, with the current state of the art   |
| Ethernet              | 100 Mbps   |
| Web browser           | Microsoft Internet Explorer®<br>Apple® Safari®<br>Mozilla® Firefox®<br>Google® Chrome®<br>(always the most recent version) |
| Browser settings      | JavaScript® enabled  |
| Software              | Not required   |


## 2.2 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) is displayed:

 *The language of the user interface can be switched in the top-left corner of the screen without prior login.*

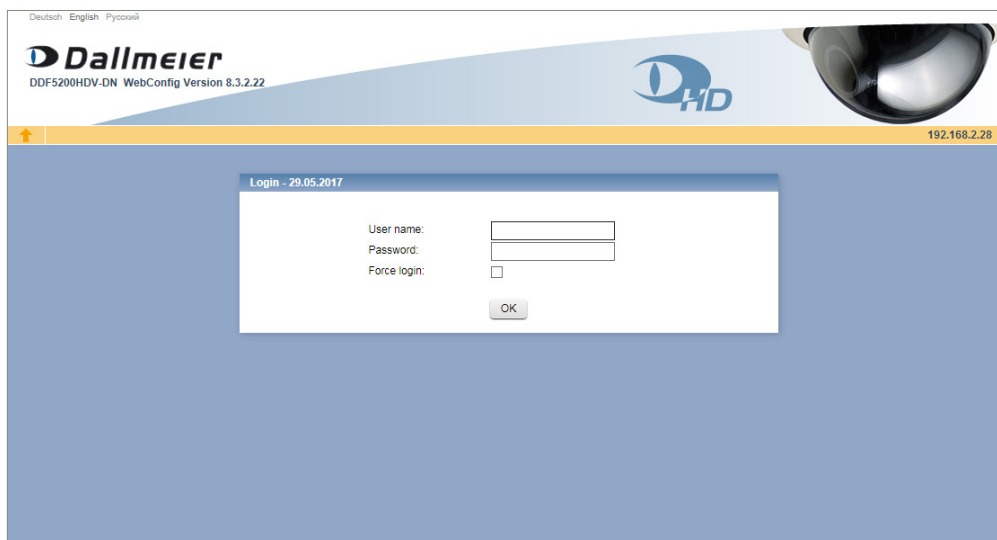

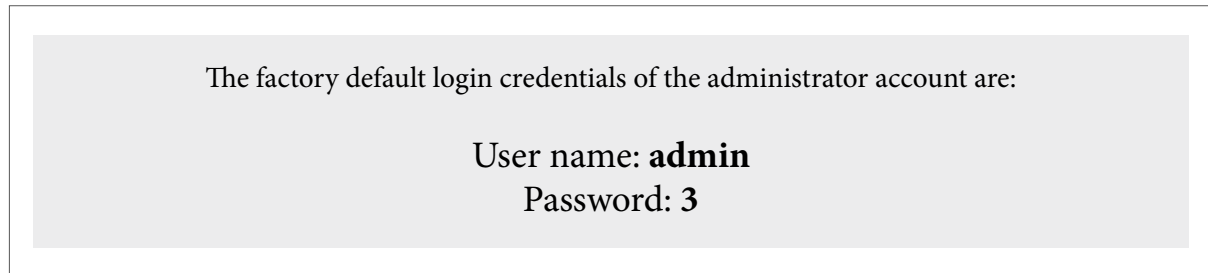


Fig. 2-1: Login

 *The “Force login” option allows you to login even when another user with minor rights is already logged in.*

## 2.3 Login

The graphical user interface of the configuration and live mode is displayed for authenticated and authorized users only.



### NOTICE



#### Risk of access and misuse by unauthorized users

Change the factory default login credentials of the administrator account as soon as possible.

- ⇒ Enter the “User name”.
- ⇒ Enter the “Password”.
- ⇒ Confirm with “OK”.

After the successful login, the graphical user interface of the configuration mode is displayed:

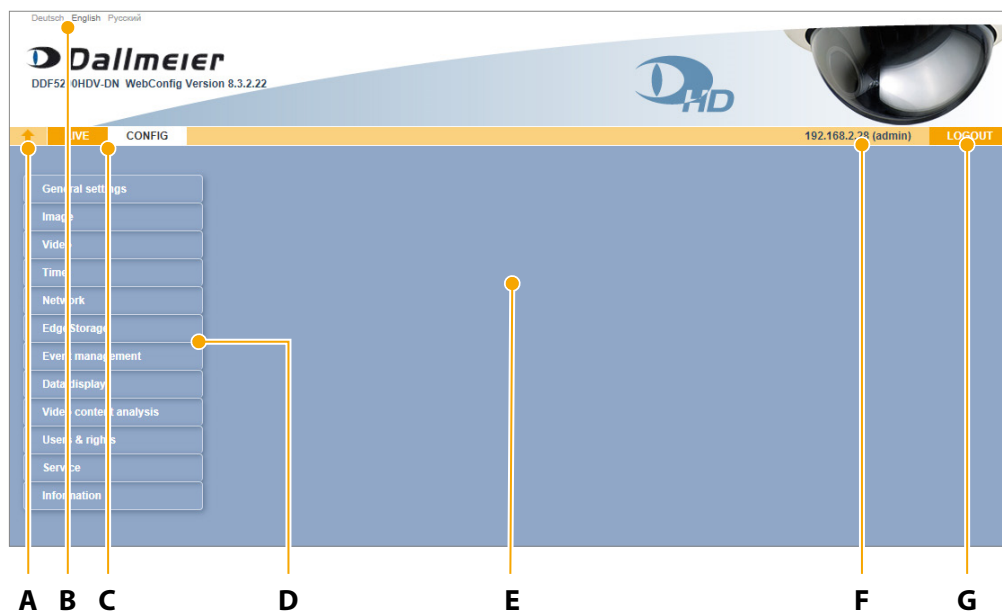


Fig. 2-2: Configuration mode

- |   |   |
|---|---|
| <p><b>A</b> Hide/show title bar</p> <p><b>B</b> Switch language</p> <p><b>C</b> Switch between live and configuration mode</p> <p><b>D</b> Configuration menu</p> | <p><b>E</b> Area for configuration dialogs</p> <p><b>F</b> IP address of the device and currently logged on user name</p> <p><b>G</b> Log out of the device</p> |
|---|---|

# Chapter 3:

## Language

The graphical user interface can be displayed in various languages.

⇒ Click “General settings”.

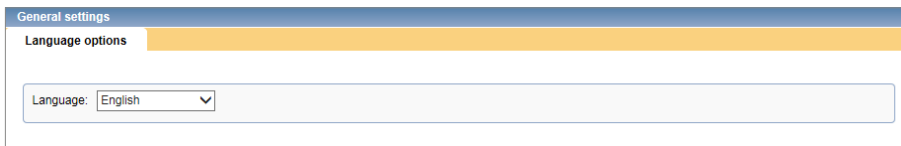


Fig. 3-1 Language

⇒ Select the desired “Language”.


The graphical user interface is switched to the new language automatically.

# Chapter 4:

## Image

In the “Image” dialog, the image sensor can be configured and the image processing algorithms can be adjusted to the local lighting conditions. In addition, the automatic day/night operation can be configured for an optimum day and night image exposure.

- ⇒ Open the “Image” dialog with a click on “Image”.
- ⇒ Note the following explanations on the various settings.

 *You can restore the factory settings at any time in the “Service” > “System state” dialog.*

### 4.1 Presets

The “Presets” tab allows the setting of various AE (Automatic Exposure) presets for the image capture and for the live preview on the following tabs.

#### Pre-defined presets

Using factory-predefined exposure settings and image processing algorithms that are stored into so-called presets, the camera can be very easily adapted to the most lighting conditions in order to always obtain the best image quality.

In addition, presets serve as useful starting points for the manual adjustment of various camera parameters, such as exposure time, aperture, white balance, local tone mapping etc.

The firmware has seven predefined presets for the best possible image capture in various areas of application.

- Casino - for indoor scenes with high contrast
- Indoor - for indoor scenes with medium contrast
- Low-light - for scenes with poor illumination
- Outdoor - for outdoor scenes with high contrast
- Universal - suitable for most scenes
- SEDOR Day - special preset for the SEDOR® video analysis software during the day
- SEDOR Night - special preset for the SEDOR® video analysis software during the night

#### Creating user-defined presets

Changes to presets are initially only temporary (in the preview image). If you want to apply the changes permanently, they have to be saved explicitly.

User-defined presets then can then be selected, for example, for the “Preset automatic” feature or used as starting points for further manual adjustments of the camera parameters (re-saving or overwriting required).

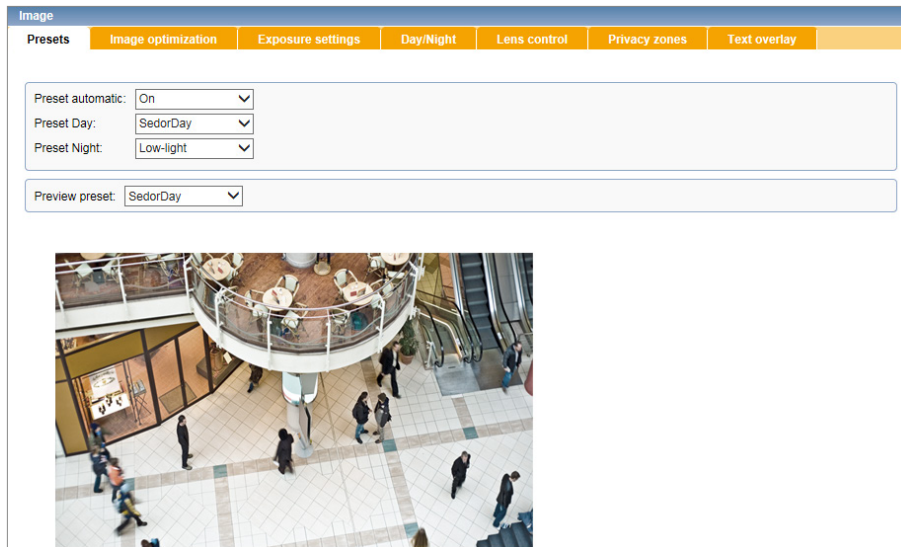


Fig. 4-1

The “Save preset” option is automatically available after a parameter has been changed.



Fig. 4-2

⇒ Click “Save Preset” after all necessary parameters have been changed to create a new user-defined preset.

The “Save preset” dialog is displayed.

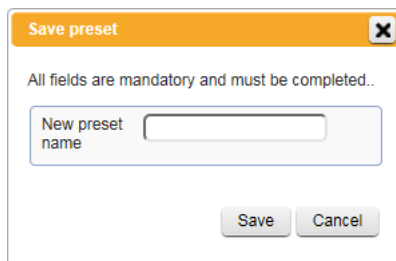



Fig. 4-3

⇒ Enter a name for the preset.

⇒ Confirm with “Save”.

 *The settings of the 7 predefined presets cannot be changed or overwritten.*

The preset is now available for further use, for example in the “Preset automatic” function (see below). To make the necessary changes effective, the preset has to be activated, for example as “Preset Day” or “Preset Night”.

The number of user-defined presets is not limited. They can be selected for the preview, optimized and saved again.

## Deleting user-defined presets

### NOTICE



#### Immediate execution

The selected action is executed without prior confirmation prompt.

To delete presets, proceed as follows:

Fig. 4-4

- ⇒ Click the pen-button next to “Delete preset”.
- ⇒ Select the required preset and click the corresponding “X”-button (red).

The preset is now deleted.

### Preset automatic

The “Preset automatic” function switches the active preset to image capture when the camera switches between day and night modes.



*By linking a preset each to the day/night modes, especially generated for the changing light conditions, the image is always captured with the optimal (chosen) settings.*

### Preview preset

A preset can be set for live preview on the following tabs. The parameters of the preset can be used as starting points for manual fine adjustment and then saved as a user-defined preset.

## 4.2 Image Optimization

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

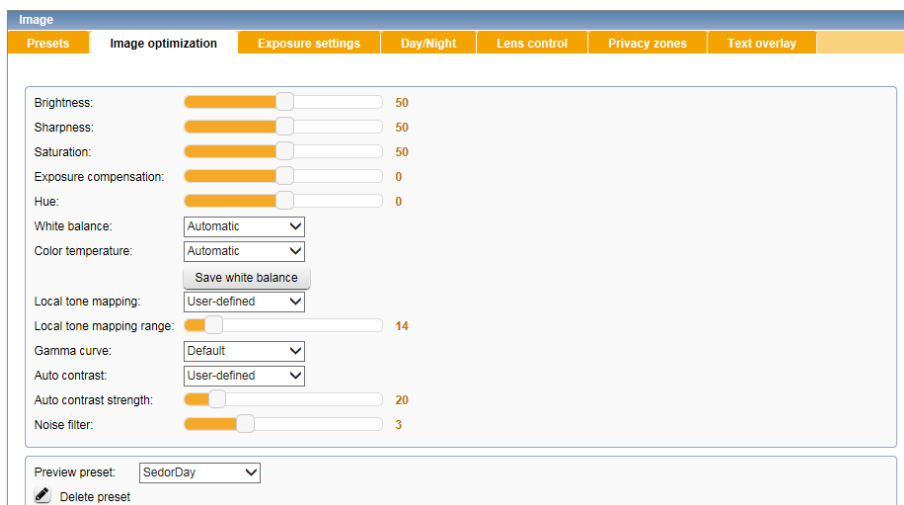


Fig. 4-5

### Brightness

This setting defines the overall image brightness by linear adjustment of the tonal values.

***i** Brightness is a global setting that does not respond to changing image contents.*

### Sharpness

This setting influences the subjective impression of sharpness by emphasizing the edge transitions.

***i** A very strong emphasis on the edges (high sharpness) appears unnatural. It can lead to image artefacts (double edges) and increased image noise in poor lighting conditions.*

### Saturation

This setting defines the determines the color intensity and brilliance of colors and thus their perceived intensity.

***i** The saturation is reduced automatically when the image noise is too strong in low light conditions.*

### Exposure compensation


This setting affects the camera raw image. It can be used to enhance details in overexposed or underexposed areas of the image.

***i** The brightness affects the processed image. Details in overexposed or underexposed areas are then already lost in the processed image.*



## Hue

This setting allows to shift the hue towards red ( $\leq$ ) or green ( $\geq$ ) and thus a correction of the white balance.

 *This function is useful if a color cast to the image is still recognizable after the white balance has been executed.*

## 4.2.1 White Balance

In order to always achieve accurate color reproduction, regardless of the prevailing light sources and color temperatures (measured in Kelvin), a correct white balance is required.

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

### Automatic

ATW (Auto Tracking White Balance):

The white balance value is automatically calculated using the color information of the entire scene and continually adjusted to the changes of color temperatures.

For the best possible result, at least one white object as a reference (value) should be in the scene to be captured.

The use of ATW is especially recommended for scenes with constantly varying lighting conditions/ color temperatures, such as indoor scenes with artificial light sources and incident daylight.

### Manual

MWB (Manual White Balance):

This setting is used to manually adjust the red, green and red, green and blue parts in the image.

The respective color components can be adjusted independently using the corresponding sliders for red and blue amplification.

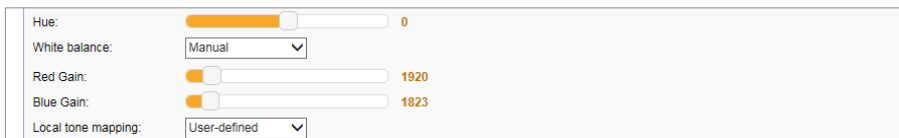


Fig. 4-6 Manual WB

### Gray World

“Gray World” is a special preset, optimizing the white balance for the special lighting conditions found in casinos.

### One Push

One Push AWB (Automatic White Balance):

The “One Push” white balance returns a fixed measurement value which is only recalculated when triggered by user request (“Save WB” button).

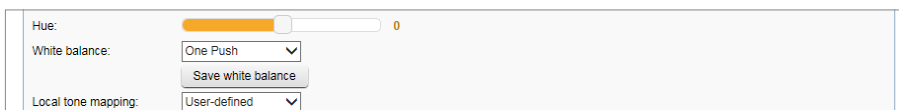



Fig. 4-7 One Push AWB

The calculations are based on the assumption that, in correct lighting conditions, a white or neutral grey object (as reference value) takes up more than half of the entire scene.

## 4.2.2 Color Temperature

 *This function is only available in the white balance mode “Automatic”.*

### **Automatic**

The recommended setting for automatically calculating the white balance indoors.

### **Automatic Outdoor**

The recommended setting for automatically calculating the white balance outdoors.

### **2800 K, 4000 K, 5000 K, 6500 K, 7500 K**

Manual setting for the calculation of the white balance is particularly useful in environments with very low white levels, for example, when green casino tables are to be observed.

The respective data in Kelvin refers to the lighting conditions (prevailing color temperature) at the installation site of the camera and each comprise a range of  $\pm 500$  Kelvin around the stated value.

2800 K roughly match the light of a regular light bulb, 4000 K neon light, 5000 K bright daylight.  
6500 – 7500 K roughly match daylight when the sky is overcast.

## 4.2.3 Local Tone Mapping

The “Local Tone Mapping” function adjusts the local tone value and thus the local contrast of dark image areas. Thereby more details can be visualized in these areas, they are perceived as “lightened”.

**i** *The image sensor captures much more details in dark areas than the human eye can normally perceive.*

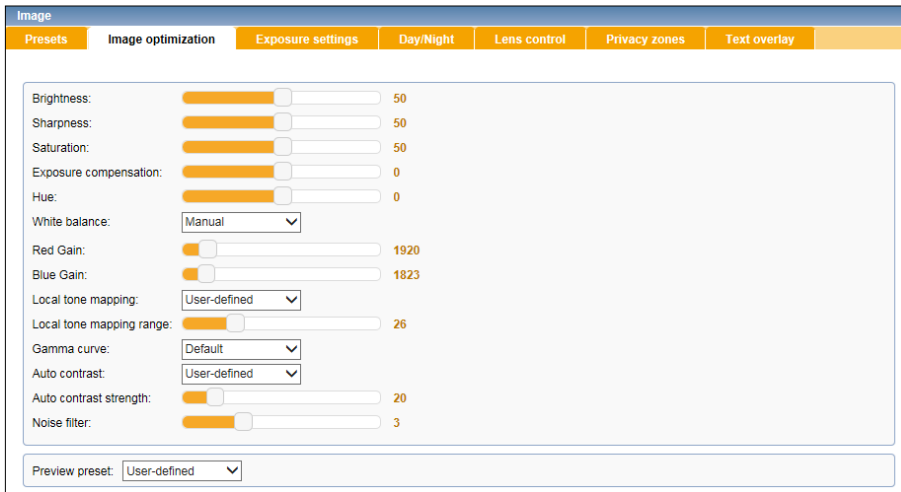


Fig. 4-8 Local tone mapping

This function is especially suitable for high-contrast scenes with constant lighting. In day mode with changing illumination, the function should be set to “Automatic”. In this case, a controlling loop adjusts the strength of the tone value permanently.

**i** *In changing lighting conditions a fixed tone value can be too much. By overemphasis of contrasts unsightly comic and halo effects may occur.*

In night mode, artificial light sources create a uniform illumination. In this case, the user-defined fine-tuning of the tone values can be very beneficial.



Fig. 4-9 Local tone mapping not active




Local tone mapping active

**i** *Use the function for automatic day/night switching of presets in order to switch the local tone mapping from automatic to user-defined.*

## 4.2.4 Auto Contrast

The “Auto contrast” function is a special algorithm for image correction. It can improve the clarity of the image, even in foggy environments or in heavy smog.

 *Due to the eye-catching image enhancement in fog, this function is often referred to as Defog function.*

The “Auto contrast” function replaces the static contrast control of previous versions. It now includes an active and automatic control, which analyzes each image and takes changing contents into account. By adjusting the greyscales a much clearer picture is achieved in cloudy scenes.

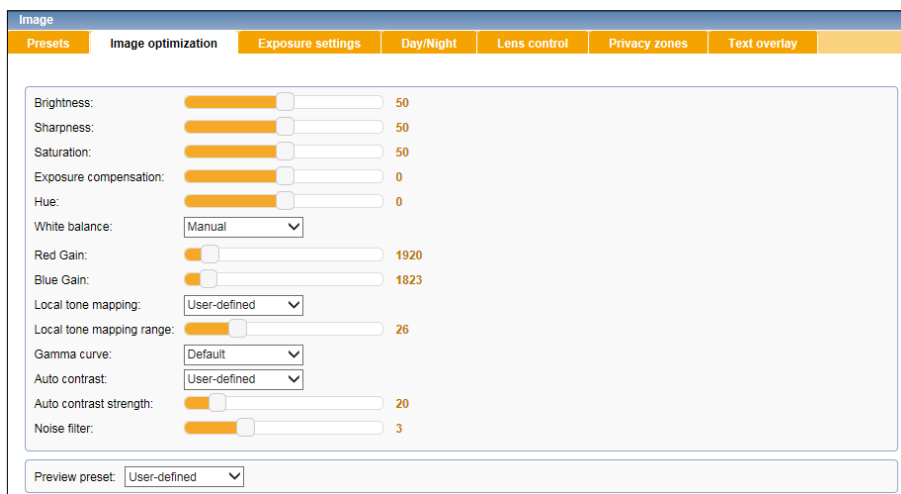




Fig. 4-10 Auto contrast

The “Auto contrast” function is particularly suitable for well illuminated but cloudy scenes during the day. In night mode it amplifies the noise of darker images considerably and thus should be disabled.

 *Use the function for automatic day/night switching of presets in order to activate or deactivate the auto contrast function.*

## 4.2.5 Noise Filter

The “Noise filter” function is a temporal filter that detects and tracks motion in the image during the reduction of the image noise. Thus, the blurred display of moving objects (ghosting effect) is effectively minimized.

 *This noise filter type is also called “MCTF - motion compensated temporal filter” or “3D-DNR - 3D digital noise reduction”.*

The filter control automatically takes changing lighting conditions into account. Thus the filter is barely active in good lighting conditions and is only applied with increasing intensity when brightness decreases.

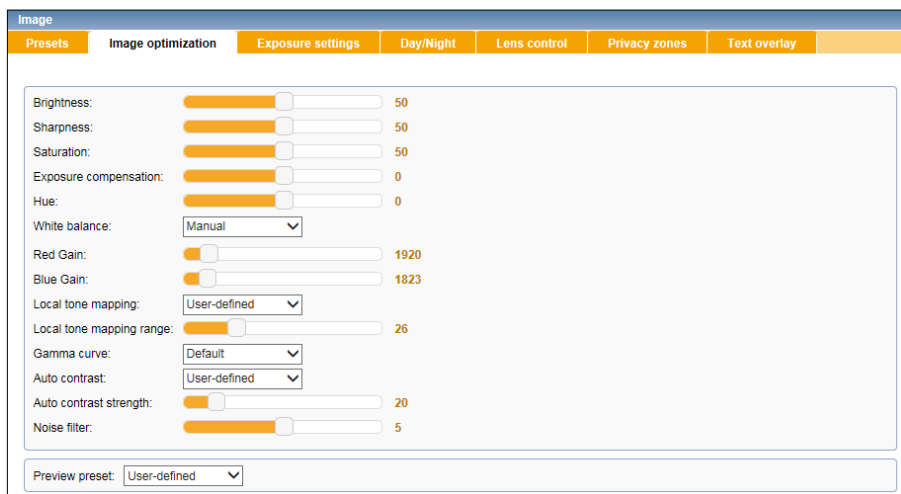



Fig. 4-11 Noise filter

The level of noise reduction can be adjusted, but increased ghosting effects have to be considered in an aggressive setting. The default value of 5 is a good compromise between noise reduction and ghosting.

The filter can be switched off by setting the value to 0. This should be avoided if possible, as it also filters out barely perceptible micro noise (high-frequency, small-scale noise). This reduces the encoder load and the required bandwidth remarkably.

 *In order to filter out micro noise, the noise filter should not be deactivated even in good lighting conditions.*

## 4.3 Exposure Settings

Using the exposure control, the automatic exposure metering of the camera can be adjusted.

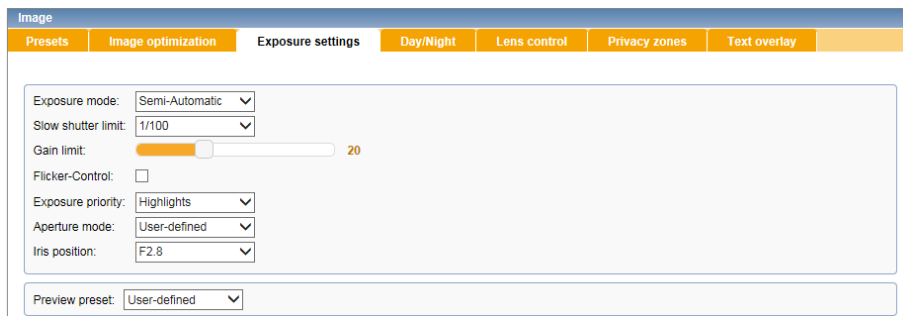


Fig. 4-12

- ⇒ Note the following explanations.
- ⇒ Set the relevant options.

### 4.3.1 Exposure Mode

#### Semi-Automatic

The entire image is used for exposure metering. For a proper exposure, the camera automatically determines the best combination of shutter speed, aperture (iris opening) and signal gain. But it remains within the set maximum values.

#### User-defined

The entire image is used for exposure metering. For a proper exposure, the camera uses the set values.

### 4.3.2 Slow Shutter Limit

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

The “Slow shutter limit” defines the maximum allowable automatic exposure time (electronic shutter speed).

As soon as the set shutter limit is reached, the Automatic Exposure (AE) is exclusively controlled by the automatic iris (aperture) control and/or the Automatic Gain Control (AGC).

### 4.3.3 Gain Limit

The “Gain” option allows to regulate the value in dB, with which the automatic exposure control is allowed to amplify the signal at the sensor, with a slider. Higher values produce greater noise than lower values.

### 4.3.4 Flicker-Control

The option “Flicker-Control” prevents possible interferences through frequency overlay, when the camera is used in conjunction with neon lamps.

### 4.3.5 Exposure Priority

Exposure priority regulates if parts of the image with higher, middle or lower tonal value shall be depicted preferably. “Highlights” emphasizes parts with higher tonal value, “Midtones” the parts in the middle, and “Shadow” the low parts.

### 4.3.6 Aperture Mode

The P-Iris technology is designed for the precise and automatic adjustment of the ideal iris opening (“*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).

#### **Automatic**

Together with the P-Iris lens, the camera firmware, first of all, automatically determines the most ideal compromise (also known as “*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 later able to achieve perfect image sharpness regardless of the prevailing lighting conditions.

#### **User-defined**

This option allows the manual adjustment of the P-Iris aperture.

## 4.4 Day/Night

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

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

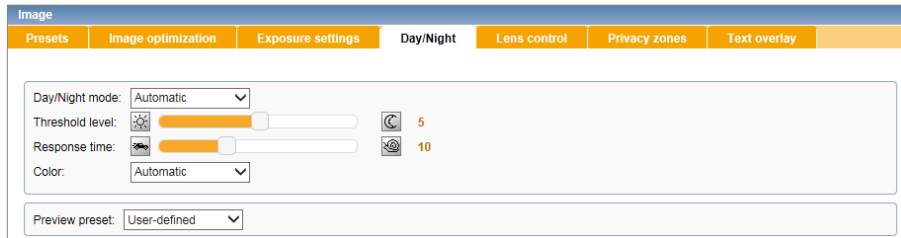


Fig. 4-13

### 4.4.1 Day/Night Mode

#### Automatic

This setting enables the automatic day/night operation depending on the amount of visible light and internal defined parameters.

In low-light conditions, the camera switches to night mode and the infrared (IR) cut filter is automatically removed (ICR OFF) which significantly enhances the sensor’s sensitivity for near infrared light.

Depending on the amount of visible light, the camera automatically switches back to day mode and the IR cut filter is automatically moved back into place again (ICR ON).

The day/night switching threshold levels can be manually adjusted (described in the following sections).

#### Day - ICR on

The camera is always in color mode.

The built-in infrared (IR) cut filter is always removed (ICR ON).

#### Night - ICR off

The camera is always in black/white mode.

The built-in infrared (IR) cut filter is always placed in front of the sensor (ICR OFF).



## 4.4.2 Threshold Level

This setting allows the manual adjustment of the day/night switching threshold levels (threshold values of brightness and darkness).

### Higher level

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

### Lower level

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

## 4.4.3 Response Time

This setting is useful for 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.

Example:

If during the day the camera is operated inside a room with a window that faces 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 to day mode.

In the reverse example, there would be a constant unwanted switching from night to day mode and back as soon as the headlights of passing vehicles light up the room.

Using the “Response time” setting, it is, thus, possible to delay the automatic day/night switching.

## 4.4.4 Color

The following color options are available:

### Automatic

This setting enables the automatic switching between black-and-white and color mode as lighting conditions change. The automatic switching depends on the ambient light level:

At low light levels the camera automatically switches to black-and-white mode and removes the color burst. Without color information, or rather in black-and-white mode, the image quality in low-light conditions is much clearer (e.g. less color noise).

Depending on the ambient light (when a certain brightness level is reached again), the camera automatically switches back to color mode.

### On

The video is always displayed in color, even at low light levels.

### Off

The video is always displayed in black-and-white.

## 4.4.5 Lighting Mode DF5200HD-DN/IR

This setting allows to configure the intensity and beam angle of the integrated IR (infrared) illumination. The IR illumination is provided by semi-covert 850 nm high-performance LEDs. There are three lighting modes available:

- **Automatic:** If the camera switches from day mode to night mode, the IR illumination is automatically activated. In doing so, the chosen “Lighting configuration” is used.
- **Always on:** The IR illumination is always active, using the chosen “Lighting configuration”.
- **Always off:** The IR illumination is always deactivated.

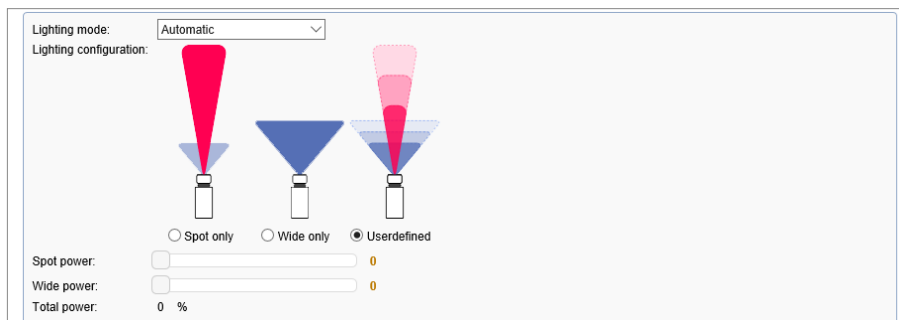


Fig. 4-14


### Lighting configuration

The following options are displayed, if the lighting modes “Automatic” or “Always on” have been selected. They can be selected using the appropriate radio buttons:

#### Spot only

This option enables a narrow IR radiation cone (directional beam angle) for a small but targeted illumination solid angle.

This option is recommended for covering a small area (e.g. a long, narrow hallway inside a building) with distant objects while preventing wall reflections.

 *Note that white or brightly-colored walls and reflecting objects increase the perceived intensity of the IR illumination.*

#### Wide only

This option enables a wide IR radiation cone (non-directional beam angle) for a large illumination solid angle.

This option is recommended for covering a large area with homogenous (uniform) IR illumination.

#### User-defined

This option allows you to manually adjust the IR illumination intensity according to the requirements using the horizontal sliders “Spot power” and “Wide power”.

The slider “Total power” can not be operated, it merely informs about the total usage of power available with the camera.

The orange numbers right of the according sliders indicate the percentage of power used.

## 4.4.6 Lighting Mode DF5400HD-DN/IR

This setting allows to configure the intensity of the integrated IR (infrared) illumination. The IR illumination is provided by semi-covert 850 nm high-performance LEDs.

There are three lighting modes available:

- **Automatic:** If the camera switches from day mode to night mode, the IR illumination is automatically activated. In doing so, the chosen “Total power” is used.
- **Always on:** The IR illumination is always active in the chosen “Total power”.
- **Always off:** The IR illumination is always deactivated.

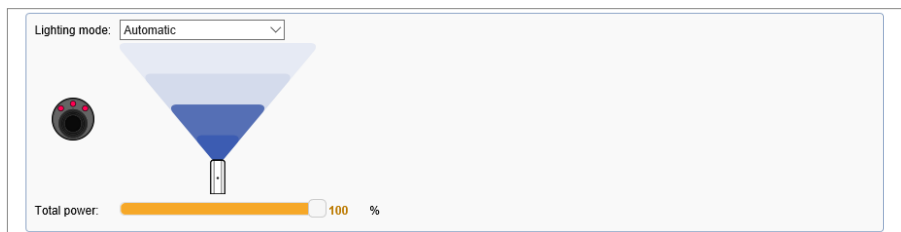


Fig. 4-15

### Total power

The option is only available, if the lighting modes “Automatic” or “Always on” have been selected.

Using the “Total power” horizontal slider one determines the total power (range and intensity) of the IR illumination. It is scalable in 5 levels: 0 %, 25 %, 50 %, 75 % and 100 %.

**i** *The determined total power of the IR illumination is represented graphically by the according icons.*

## 4.5 Lens Control

The zoom (focal length) and focus adjustments can only be carried out in the “Lens Control” dialog over the network.

### NOTICE



#### Damage to the lens unit

The motor-driven P-Iris varifocal lens is equipped with high-precision stepper motors. Therefore, do not try to manually adjust the focal length (zoom) and focus on the lens.

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

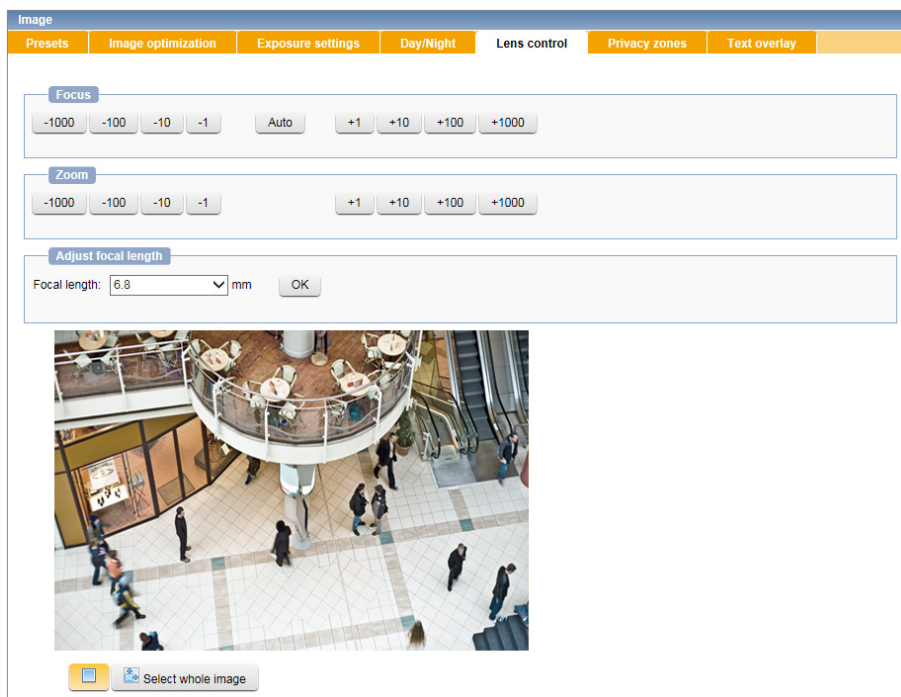


Fig. 4-16

#### Focus

Manual focusing from far (+) to near (–), with one-push autofocus (“Auto”)

#### Zoom

Zoom in (+) / zoom out (–)

## Focal length

This is the option for adjusting the focal length manually.

- ⇒ Select the necessary focal length from the corresponding drop-down list.
- ⇒ Confirm with “OK”.

**i** *Reduce the encoding bit rate to minimize long delays (response times) during lens control with low-bandwidth connections .*

## 4.6 Privacy Zones

This function allows you to hide (mask) 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 directly blackened in the camera.

**i** *The number of privacy zones is unlimited. The combined area of all privacy zones can amount to up to 100% of the entire image.*

- ⇒ Click “Image” > “Privacy zones”.

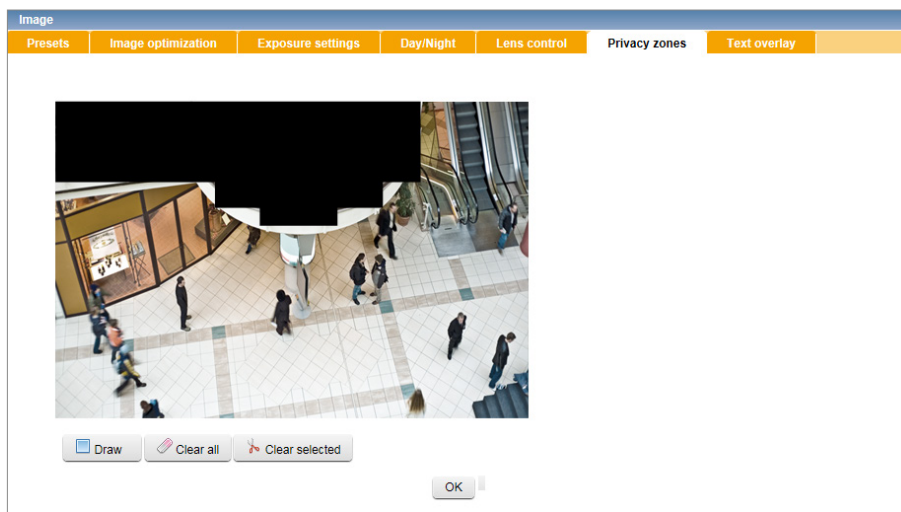


Fig. 4-17


- ⇒ Click the “Rectangle” button (left).
- ⇒ Click and hold the left mouse button and draw a rectangle over the relevant image area.
- ⇒ Confirm with “OK”.

The selected image area is masked as privacy zone.

**i** *Moving a defined privacy zone is supported by drag&drop. Every single action has to be confirmed with “OK” in this tab.*

## 4.7 Text-Overlay

The camera allows the insertion of any text in the image, such as a camera name, on the “Text overlay” tab. Text position and color are specified with the right top and orange.

 *The text will be inserted into the image. It cannot be hidden later.*

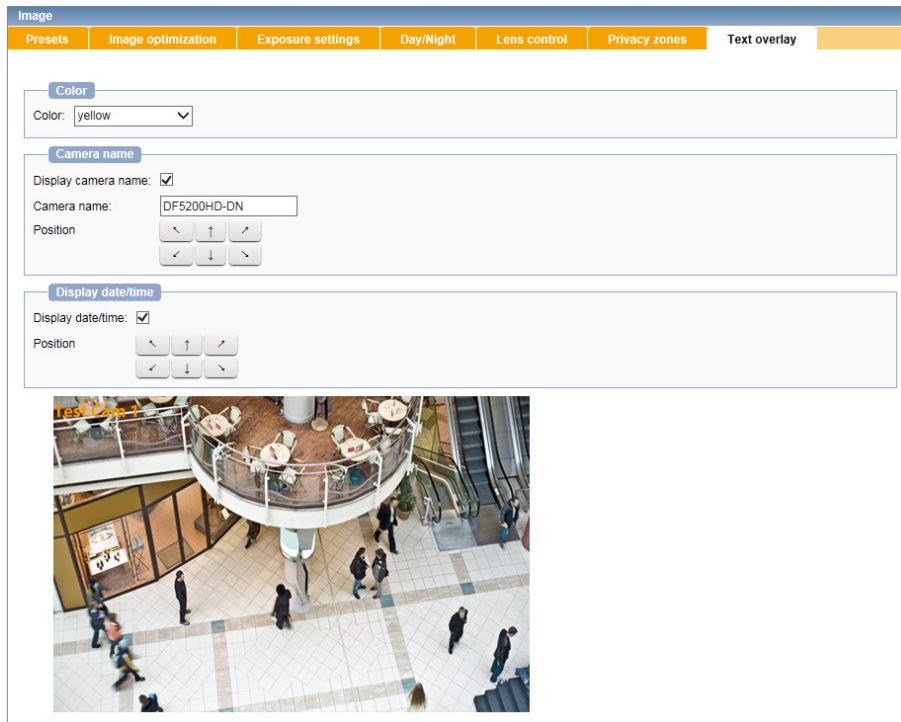


Fig. 4-18

- ⇒ Enter the text in the „Camera name“ field.
- ⇒ Activate the overlay with the „Display camera name“ check box.

### Color

- ⇒ Select the necessary color for the displayed information from the corresponding drop-down list.

### Camera name

- ⇒ Enter the text in the „Camera name“ field.
- ⇒ Activate the overlay with the „Display camera name“ check box.
- ⇒ Determine the necessary position of the camera name with the arrow buttons.

### Display date/time

- ⇒ Activate the overlay with the „Display date/time“ check box.
- ⇒ Determine the necessary position of date and time with the arrow buttons.

# Chapter 5:

## Video

The “Video” dialog allows the configuration of the sensor and encoder settings.

- ⇒ Open the “Video” dialog with a click on “Video”.
- ⇒ Note the following explanations on the various settings.

Fig. 5-1

**i** Note that certain functions and features are only available if supported by the hardware.

## 5.1 Sensor Settings

The section “Sensor settings” offers basic options that are valid for all four streams (encoders).

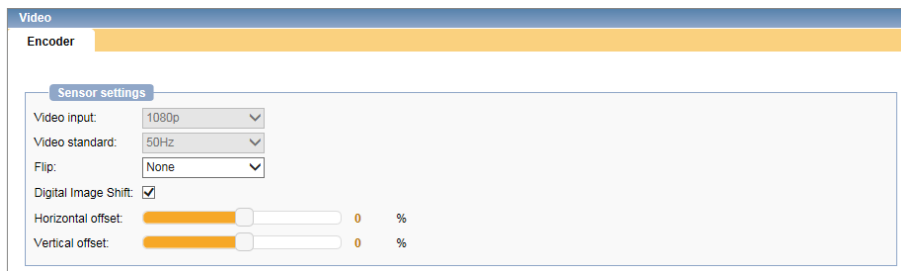


Fig. 5-2

### Video input

This option specifies the resolution and aspect ratio of the image that is retrieved from the image sensor and sends it to the encoder.

**i** *The ratio of the resolution should match the ratio (4:3 or 16:9) of the monitor in use.*

Depending on the setting of the “Video input” different resolutions for the output image are available for the encoders. Some video input modes support the function “Digital Image Shift” (Sensor shift).

**i** *Note that this option is currently available for the cameras of the 5300 series only.*

### Video standard

Countries and territories use different broadcasting television systems.

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

- 50 Hz for PAL countries
- 60 Hz for NTSC countries

### Flip



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

**i** *The flip function allows for flexible installation options for wall or ceiling applications.*

### Digital Image Shift (Sensor Shift)

The “Digital Image Shift” function allows for a subsequent digital fine alignment of the set image section by horizontal and vertical displacement of the retrieved sensor area.



-  *The degree of the displacement depends of the camera model and the selected video input mode. Some video input modes only support a horizontal displacement.*
-  *This option is currently available for the cameras of the 5300 series and the camera DF5200HD-DN/IR only.*

## 5.2 Audio Out

Received audio data (G.711  $\mu$ -law or G.711 A-law) can be decoded by the camera in real-time and output as analog audio signals on the built-in (analog) audio output interface (e.g. on a connected speaker).

SeMSy® III and SMAVIA Viewing Client transmit audio signals (for example, incoming from the microphone input port of the client PC) in a digitized form to the corresponding camera using the DaVid protocol. No manual settings are required in the audio client (decoder) of the camera

For this, the following prerequisites have to be met:

- The audio encoding format (audio codec) of the audio source and the selected audio codec in the audio client (decoder) of the camera have to be compatible.
- The specified destination port in the audio source and the assigned receiving port for inbound audio connections in the audio client (decoder) of the camera have to be identical (default port number: 40000).
- For unicast applications, the audio source has to transmit the audio data to the IP address of the camera and the IP address of the audio source has to be entered in the audio client (decoder) of the camera.
- For multicast applications, the multicast IP address used by the audio source has to be identical with the multicast IP address entered in the audio client (decoder) of the camera.

⇒ Click “Video” > “Decoder”.

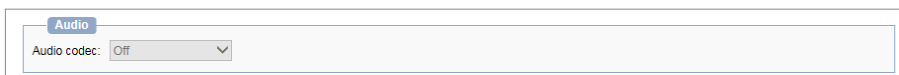


Fig. 5-3

⇒ Select the required “Audio codec” from the corresponding drop-down list.

-  *Note that only one client can transfer audio data to the camera at a time.*

## 5.3 Encoder Settings

The settings for all four encoders are made in one common dialog. The procedure is identical, but the adjustable values may differ.

**i** Depending on the camera model, the encoder 3 can be set for streaming or for output of the analog video preview signal (BNC interface).

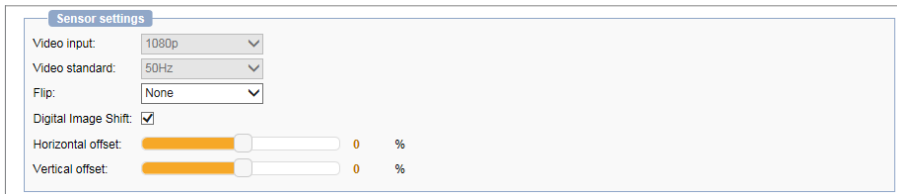


Fig. 5-4

**i** When the encoding standard “MJPEG” is selected, the settings “Bitrate”, “Bitrate mode” and “GOP size” are not required.

### Frames/Second

The frame rate (value in fps) defines the number of consecutive frames generated per second. The higher the frame rate, the smoother the video playback. However, higher a frame rate also requires a higher bandwidth (transmission capacity) and more hard disk storage space for the recording of video material.

**i** A frame rate of 25 (PAL/50 Hz) or 30 fps (NTSC/60 Hz) meets 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 is the quality. However, a higher bit rate also requires a higher bandwidth (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 small hard disk storage space required

High bit rate = Low image compression  
 = Large data volume  
 = High image quality  
 = High bandwidth and large hard disk storage space required

**i** A bit rate between 4 and 6 Mbps meets the requirements in most applications.

**Bitrate mode**

The bitrate mode allows for the setting of a constant bitrate or a variable bitrate for video encoding, each with a priority setting for the image quality.

**Constant**

At a constant bitrate the video encoding is always performed with the set bitrate, even if it is not required for scenes with few changes in the image.

If the set bitrate is not sufficient for scenes with much changes in the image, the image quality is adjusted.

Constant bitrates allow for a more accurate calculation of the required bandwidth (transmission) and storage capacity (recording).

**Variable**

A variable bitrate is dynamically adjusted to the changes in the image. For scenes with few changes in the image it is lowered, for scenes with much changes in the image increased.



*The slider “Bitrate” is extended in this case and allows for the setting of a lower limit. It is not exceeded even for scenes with no changes in the image.*

For scenes with very much changes in the image, the bitrate can be briefly raised above the set value. If the total available bit rate for all encoders is insufficient, the image quality is adjusted.

Variable bit rates allow for a high image quality and at the same time a better utilization of the available bandwidth (transmission) and storage capacity (recording).

**Priority Setting for the image quality**

The modes „Constant QK“ and „Variable QK“ (QK = Quality Keep) are a variation of the bitrate modes described above.

If the set bitrate (Constant QK) or the total available bit rate for all encoders (Variable QK) are not sufficient for scenes with very much changes in the image, the frame rate is adjusted in stead of the image quality.

**GOP size**

The H.264 encoding (compression) is carried out by dividing the video stream into so-called GOPs (Group Of Pictures) of a defined length (“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 of the preceding images (I-Frame or P-Frames) – also called “*Long-term prediction*”.


The compression rate of P-Frames is much higher than that of I-Frames since changes in relation to reference images only need to be coded as motion vectors.

Thus, the required bit rate decreases so that, with a given total encoding bit rate, more bits are available for the I-Frame. Consequently, the quality (e.g. the detail resolution) of the I-Frame can be increased by the use 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.

A GOP sequence ends before the next I-Frame.

Later on, the individual GOP sequences are used to generate the visible single frames (reconstruct the original compressed image data) at the decoder.


 *In general, a GOP size between 6 and 15 provides a good image quality with a sufficiently high compression level.*

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

Note that reverse playback at high GOP sizes can lead to frame drops with some decoders.

### **Resolution**

The different camera of this series offer different resolutions for the encoding of the video stream. Depending on the built-in image sensor (and the set frame rate) they can range from SD (320 × 240) to 8 MP (3840 × 2160). The HD resolutions 720p (1280 × 720) and 1080p (1920 × 1080) are supported by all cameras in this series.


 *Detailed information about the available resolutions can be found in the data sheet of the respective camera.*

# Chapter 6:

## Time

The system time can be set manually or synchronized with an NTP time server.

### 6.1 Manual Configuration

 Note that manual configuration is not possible if the NTP time server synchronization is activated.

- ⇒ Click “Time”.
- ⇒ Click into the “System time” field.

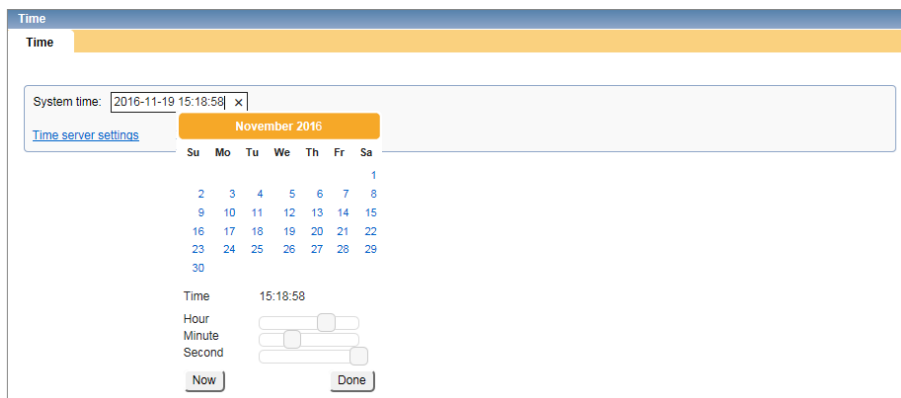



Fig. 6-1 Time

- ⇒ Make the required settings.
- ⇒ Confirm with “Done”.

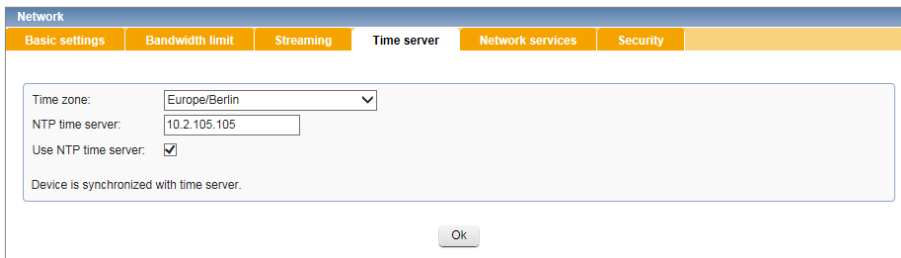
The set time is applied as system time.

## 6.2 Time Server

 Note that the specified NTP time server has to be constantly accessible over the network.

⇒ Click „Time server settings“ in the „Time“ dialog.

The “Time server” tab is displayed.



The screenshot shows a web-based configuration interface for a camera. At the top, there is a blue header bar with the word "Network" in white. Below the header is a navigation bar with several tabs: "Basic settings", "Bandwidth limit", "Streaming", "Time server" (which is currently selected and highlighted in orange), "Network services", and "Security". The main content area is a light gray box containing the following settings:

- "Time zone:" with a dropdown menu showing "Europe/Berlin".
- "NTP time server:" with a text input field containing "10.2.105.105".
- "Use NTP time server:" with a checked checkbox.
- A status message: "Device is synchronized with time server."
- An "Ok" button at the bottom right.

Fig. 6-2 Time server

- ⇒ Select the “Time zone”.
- ⇒ Enter the IP address of the “NTP time server”.
- ⇒ Select the “Use NTP time server” check box.
- ⇒ Confirm with “OK”.

The synchronization with the specified NTP time server is activated.

# Chapter 7:

## Network

### 7.1 Basic Settings

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

#### NOTICE



#### Network conflicts due to invalid or incorrect IP address

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

⇒ Click “Network” > “Basic settings”.

The screenshot shows the 'Network' settings page with the following sections and values:

- Basic settings** (selected):
  - IP-Settings:**
    - Enable DHCP:
    - IP address: 192.168.2.28
    - Subnet mask: 255.255.0.0
    - Gateway: 10.2.2.1
  - DNS-Settings:**
    - Primary DNS server: . . . .
    - Secondary DNS server: . . . .
    - DNS search domains: . . . .
  - Domainname-Settings:**
    - Domain name: dallmeier.de
  - Hostname-Settings:**
    - Host name: ipc
  - Link-Settings:**
    - MTU: 1500
    - Connection type: Automatic
    - Monitor network availability:
    - Link speed: 1Gbps
    - Duplex mode: Full duplex
    - MAC address: 00:0b:02:40:27:92
- Other tabs:** Bandwidth limit, Streaming, Time server, Network services, Security.
- Buttons:** An 'Ok' button is located at the bottom center.

Fig. 7-1: Network settings

### Default factory settings

|              |               |
|--------------|---------------|
| Enable DHCP: | disabled      |
| IP address:  | 192.168.2.28  |
| Subnet mask: | 255.255.255.0 |
| Gateway:     | 192.168.2.1   |

#### NOTICE



#### Network connection failures due to incorrect configuration settings

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

- Contact your network administrator for more information and assistance.
- For troubleshooting purposes, write down the “MAC address” of the device and all new settings before changing the configuration.

- 
- ⇒ Note the following explanations.
  - ⇒ Configure the required network settings.
  - ⇒ Click “OK” to save the settings.

### IP-Settings

- **Enable DHCP**  
Refer to “[Automatic Network Setup via DHCP](#)” on page 42.
- **IP address**  
Manual entry of the new (static) IP address that you want to assign to the camera.
- **Subnet mask**  
Manual entry of the subnet mask in which the device is located. Using the IP address and subnet mask, you can determine whether network devices are located in the same subnet (single network segment) and can communicate directly with each other, or whether they are located in different networks and a default gateway (router) has to regulate the traffic between those network devices.
- **Gateway**  
Manual entry of the default gateway (router address). This information is necessary for accessing the camera from different subnets.



## DNS-Settings, Domainname-Settings and Hostname-Settings

Since IP addresses are relatively hard to remember, you can also refer to devices using host names which makes it much easier to find the devices or hosts in 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, the IP address mapping can also be stored directly in the hosts file on your local computer.

The “Host name” (or more accurately, the short host name) specifies the actual computer or device name (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, also known as name servers.

Resolving host names into IP addresses requires the assignment of a primary name server (“Primary DNS Server”, e.g. `ns1.example.com`) and, for reasons of reliability and availability, a secondary name server (“Secondary DNS Server”, 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 settings of the DNS server or entries in your local hosts file, you can also refer to the device by simply using its short host name (here: `myhostname`).

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

## Link-Settings


“Link-Settings” lets you adjust several settings concerning the network protocol, and read the current values for link speed, duplex mode and MAC address.

- **MTU**  
The Maximum Transmission Unit (MTU) defines the maximum packet size of TCP/IP packets sent by the camera. The default MTU size is 1500 bytes (maximum size for Ethernet standard). A large MTU usually provides the best data throughput, a smaller MTU, however, can be useful to avoid packet fragmentation. Highly fragmented packets may not be forwarded by routers or firewalls.
- **Connection type**  
This setting determines the transmission rate and the duplex mode between the Network Interface Controller (NIC) of the camera and the connected Ethernet port of a router, hub or switch. For most applications, the “Auto” (auto-negotiation) setting is recommended.  
The auto-negotiation method allows network components or end devices to self-determine and configure the maximum transmission speed and duplex mode.
- **MAC address**  
The “Mac address” field displays the hardware address (physical address) of the camera.  
The MAC address uniquely identifies your device in the network and cannot be changed.

### 7.1.1 Automatic Network Setup via 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 network (LAN).

 *Contact your network administrator for additional information and support.*

⇒ Select the “Enable DHCP” check box.


The IP address, subnet mask and gateway address can then no longer be set manually but are automatically assigned by the central DHCP server after saving the network settings.

 *To send manual data to the DHCP server, clear the corresponding check boxes “DNS-Settings“, “Domainname-Settings“ or “Hostname-Settings and enter the specific data.*

⇒ If necessary, configure the available DNS-Settings under “[DNS-Settings, Domainname-Settings and Hostname-Settings](#)” on page 41.

⇒ Confirm with “OK”.


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

 *After changing the network settings, you have to re-establish a connection to the device (with the newly assigned IP address):*

- *The newly assigned IP address can be determined in the “IP Finder” (PService) or on the DHCP server by searching for the MAC address of the device.*
- *The “IP Finder” (PService) must be run on the same LAN where this device is located.*


## 7.1.2 Manual Network Setup

⇒ First, observe the designated and valid IP address ranges in your network.

 *Contact your network administrator for more information and assistance.*

- ⇒ Make sure the “Enable DHCP” check box is unchecked.
- ⇒ Enter the “IP address” that you want to assign to the device.
- ⇒ Enter the “Subnet mask”.
- ⇒ Enter the “Gateway” address.
- ⇒ If necessary, configure the available DNS-Settings under “[DNS-Settings, Domainname-Settings and Hostname-Settings](#)” on page 41.
- ⇒ Confirm with “OK”.

The connection to the device is then terminated and the new network settings will be applied.

 *After changing the network settings, you have to reestablish the connection to the device (with the newly assigned IP address).*

## 7.2 Bandwidth Limit

Bandwidth limit sets an upper limit in Mbps for the data transfer rate of the individual streams of the camera.

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.

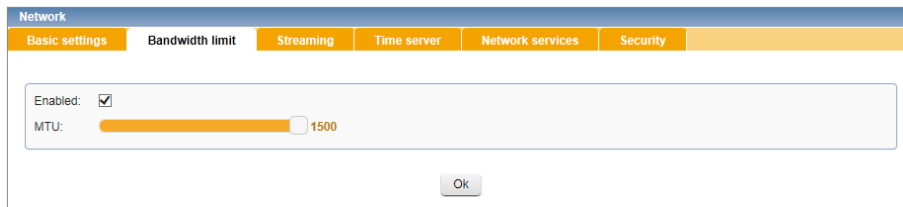


Fig. 7-2

- ⇒ Select the “Enabled” check box.
- ⇒ Set the peak bandwidth limit with the corresponding slider.

## 7.3 Streaming

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

- ⇒ Click “Network” > “Streaming”.

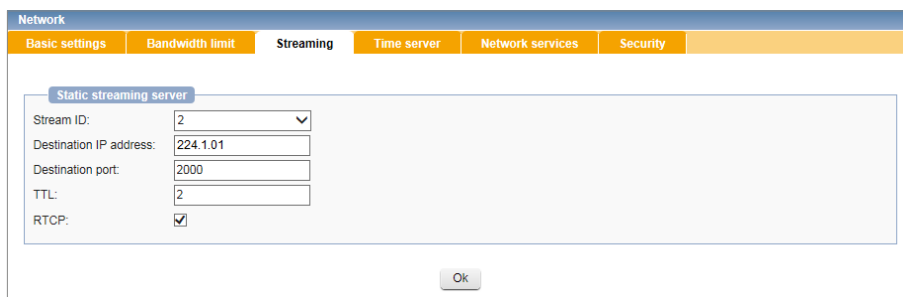


Fig. 7-3 Streaming

- ⇒ Note the following explanations.
- ⇒ Select an encoder from the “Stream ID” drop-down list.
- ⇒ Enter the “Destination IP address”.
- ⇒ In the “Destination port” field, enter the port number of the service that is supposed to receive the IP data packets.
- ⇒ Enter the TTL value for IP packets into the “TTL” field.
- ⇒ Select the “RTCP” check box if required.
- ⇒ Confirm with “OK”.

Depending on the IP address used, the transfer method and the data distribution over the network changes (see below):

### **Destination IP address (multicast)**

Using the multicast technology, a single stream can be replicated in the network for multiple target hosts or receivers without the need for the source host to create multiple copies of the same stream. Thus, the network traffic can be significantly optimized and the processor load of the sending host can be considerably reduced.



*Before you can use IP multicasting, you have to make sure that the receiving host and the local routers/switches in your network support IP multicasting and are correctly configured.*

*Contact your network administrator for more information and assistance.*

In a multicast-enabled network, each datagram is provided with a special IP multicast group address and then transmitted to a group of receivers (multicast group). This is also known as one-to-many distribution (from one source to multiple destinations).

Compared to unicast data transmission, the source host sends only a single copy of the data packet to the network; the replication of the multicast data packet and its distribution to each individual member of the multicast group (one copy for each target host) is performed by specially configured (multicast-capable) routers/switches.

To periodically determine whether registered members of a multicast group are still active, multicast switches should be used that support IGMP snooping (in IPv4) or MLD snooping (in IPv6).

Hence, the network utilization can further be reduced as multicast datagrams are only forwarded to those recipients that really want to receive the multicast packets (i.e. only to those recipients that periodically announce their current multicast group membership).

A group of endpoints (multicast group) is identified by a single IP multicast group address: Multicast uses addresses of Class D in the range of 224.0.0.0 to 239.255.255.255 (summarized as 224.0.0.0/4 in network prefix or CIDR notation – Classless Inter-Domain Routing).



*Note that certain ranges of IPv4 multicast addresses are reserved for special purposes. For local networks, the use of addresses in the range of 239.0.0.0 to 239.255.255.255 is recommended. Since this address range is reserved for private (non-public) use within an organization, multicast datagrams sent to addresses in this range are not forwarded (“routed”) to the Internet.*

*The address details are nonbinding. Therefore, adhere to the current specifications and guidelines concerning the individual address ranges.*

*Contact your network administrator for more information and assistance.*

*For more information on IP multicasting and on recommended switches for Dallmeier systems, read the “Switch Basics” and “Switch Whitelist” white papers that are available on [www.dallmeier.com](http://www.dallmeier.com).*

### **Destination IP address (unicast)**

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

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

### **TTL**

The TTL (Time To Live) value 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 (Local Area Network) and being sent to the WAN (Wide Area Network) (TTL = 1).

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

### **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.

## 7.4 Time Server

 Note that the specified NTP time server has to be constantly accessible over the network.

⇒ Click “Network” > “Time server”.

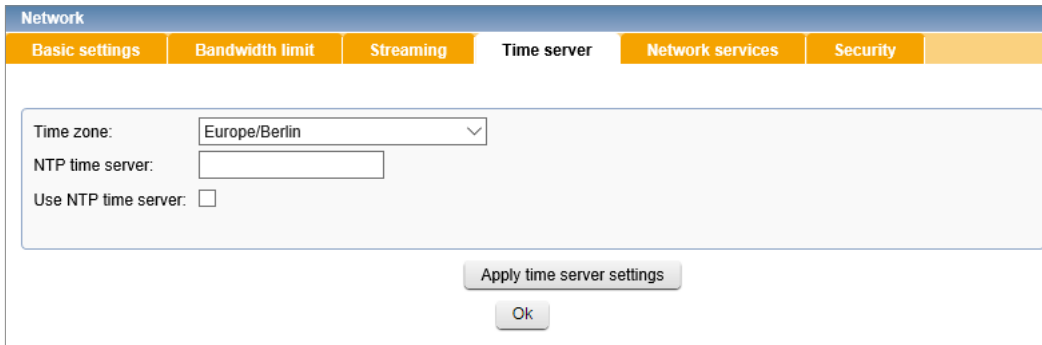


Fig. 7-4

- ⇒ Select the “Time zone”.
- ⇒ Enter the IP address of the “NTP time server”.
- ⇒ Select the “Use NTP time server” check box.
- ⇒ Confirm with “OK”.

The synchronization with the specified NTP time server is activated.

## 7.5 Network Services

### Default factory settings

ONVIF:       deactivated  
RTSP:       deactivated

⇒ Click “Network” > “Network services”.

Fig. 7-5

- ⇒ Note the following instructions.
- ⇒ Select the relevant check box.
- ⇒ Enter the required port if necessary.

### ONVIF

ONVIF (Open Network Video Interface Forum) is a standardized interface for network-based video devices. The ONVIF protocol allows the configuration of the device and the request of the video stream by any client, regardless of proprietary protocols of the manufacturer.

The “Enabled” check box under “Network services” > “ONVIF” enables the corresponding interfaces for access by external clients.



**RTSP**

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

RTSP uses a direct (bidirectional) communication with the RTSP streaming server of the camera. On the one hand to determine the appropriate transmission protocol for the RTP data transfer (UDP or TCP). On the other hand to transmit control actions of IP-based RTSP applications (players) such as the starting and stopping of video transmissions.

The encoding, packaging and transport of the data streams from server to client is carried out unidirectionally using the Real-Time Transport Protocol (RTP).

Usually, RTP transmissions of streaming contents are realized by using UDP (User Datagram Protocol). However, RTSP transmissions are realized over a TCP connection (TCP = Transmission Control Protocol).

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

- UDP is a so-called “unreliable” and connectionless communication protocol.  
No connection is established to the receiver/client prior to the data transmission.  
The receiver/client does not acknowledge the receipt of data. During data transmissions over UDP, packet loss (lack of images) may occur.  
Lost packets will not be sent again.
- Usually, UDP packets sent from the Internet to your Local Area Network (LAN) are blocked by Internet routers/firewalls in general.
- UDP allows for smooth and fast data transmissions with relatively low delays, i.e. with low packet delay variation (low “jitter”).
- Each RTSP/RTP transmission over 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 over TCP:

- TCP is a so-called “reliable” and connection-oriented communication protocol.  
A connection to the receiver/client is established prior to the data transmission.  
The receiver/client confirms the receipt of each IP data packet by sending an acknowledge packet.  
During data transmissions over TCP, usually, no packet loss occurs (unless in the case of a buffer overload in the camera due to a permanent network overload).  
However, data transmissions over TCP may be slower than data transmissions over UDP.
- Usually, only the RTSP port has to be open at the Internet router or the firewall to receive data transmissions of RTP/RTSP/TCP packets sent from the Internet to your Local Area Network (LAN).  
RTSP allows you to embed the transmission of RTP streams into the existing RTSP/TCP connection; a separate UDP transmission or an additional port for the RTP data stream is not necessary.

The default port number for RTSP streaming data (live audio and live video) is 554.

You can change the default port number to any valid number within the range of 1024 – 65535.

If multiple cameras are located on the same subnet (behind the same NAT router), you have to assign each camera a unique internal RTSP port number in order to be able to access the RTSP server of each camera from the WAN (may not be required if your NAT router supports port redirection).

Information regarding URL requests for the corresponding stream types can be found under “[RTSP Application](#)” on page 87.

## HTTP/HTTPS

The HTTPS (HyperText Transfer Protocol Secure) communication protocol is supported in addition to HTTP in order to transfer data securely and protected against unauthorized access over the network. HTTPS is used, on the one hand, to authenticate the identity of two connection partners using certificates when establishing the communication, and on the other to encrypt the transmitted payload (video and audio data packets that are transported between the two communication partners).

The following TLS protocol versions for the encryption of data packets are supported with the current version:

- TLS 1.0
- TLS 1.1
- TLS 1.2

In case of an HTTPS configuration, a valid HTTPS certificate has to be previously created under “Network” > “Security”.

The default port for HTTPS connections is 443.



*For more information and assistance with the creation and integration of a valid TLS certificate, contact your network administrator.*

## 7.6 Security

⇒ Click “Network” > “Security”.

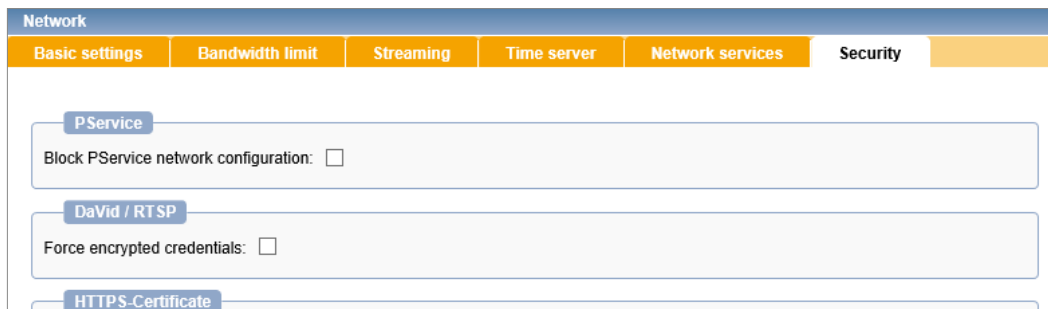


Fig. 7-6

- ⇒ Note the following instructions.
- ⇒ Select the relevant check box.


### Block PService network configuration

PService is a tool for the remote configuration of Dallmeier network devices. PService scans the network, detects the network devices and provides among other things a function for changing the network settings.

The setting “Block PService network configuration” prevents the modification of the network settings with PService.

### Force encrypted credentials

This setting enforces the encryption of credentials that are sent via the DaVid protocol (Dallmeier Video Protocol).

 *Note that this setting does not encrypt the login credentials when you log on to the WebConfig user interface of the device via a web browser.*

If the security option is activated, the device will only accept encrypted credentials in the authentication data of external applications via the DaVid protocol.

The device will, then, no longer accept authentication credentials in plain text but only send and accept DaVid commands that contain encrypted user names or passwords.

### NOTICE



#### Access failure due to incorrect configuration settings

Note that older applications that do not support an encrypted authentication may no longer be able to access the device when the security option is activated.

# Chapter 8:

## EdgeStorage

The function EdgeStorage allows for the loss-free recording of a Dallmeier VideoIP system in case of a temporary failure of the IT infrastructure or the recording system.

Dallmeier IP cameras are equipped with a RAM. EdgeStorage uses this internal storage in order to save the recordings and compensate for a network failure without losing data.

If long network failures are to be expected, the internal storage of Dallmeier IP cameras can be expanded.

⇒ Click “EdgeStorage”.

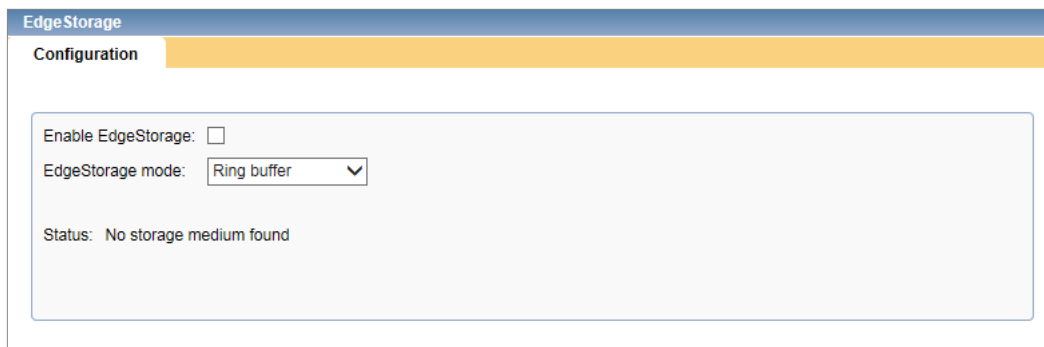


Fig. 8-1

⇒ Select the “Enable EdgeStorage” check box.

⇒ Select the “EdgeStorage mode” (see below).

### Ring buffer

When the RAM of the camera is full, older images are overwritten.

### Linear buffer

Recording stops when the RAM is full.

# Chapter 9:

## Event Management

The event management provides the option to send event triggered notifications to an alarm host via the DaVid protocol.

A software capable of handling the DaVid protocol must be running on the corresponding alarm host (e.g. PGuard advance) in order to be able to interpret the event notification.

- ⇒ Ensure that the device and the alarm host are in the same LAN or can communicate via a gateway.
- ⇒ Click “Event management in the configuration menu.



Fig. 9-1

If no event routine has been set up, only the “Add event handler” button is shown.

- ⇒ Click “Event management” > “Add event handler”.

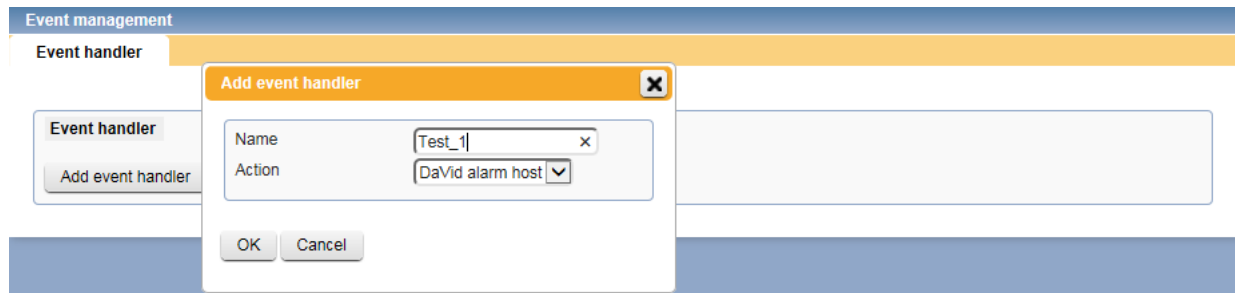


Fig. 9-2

- ⇒ Enter an informative name for the new event handler.
- ⇒ Confirm with “OK”.

A new menu item with the event handler name is added to the configuration menu and the new event handler is listed in the dialog.

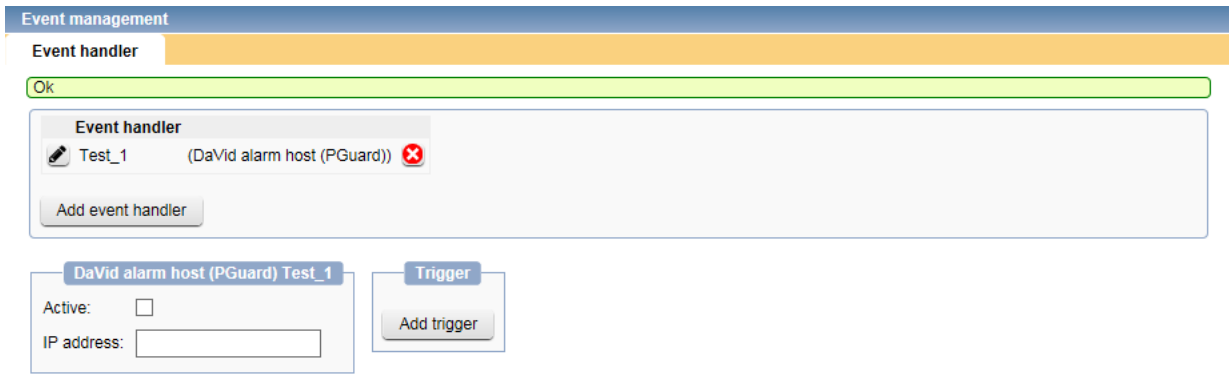


Fig. 9-3

- ⇒ Enter the IP address of the alarm host to which the DaVid event notification shall be sent to in case an event happens.
- ⇒ Click the “Add trigger” button.

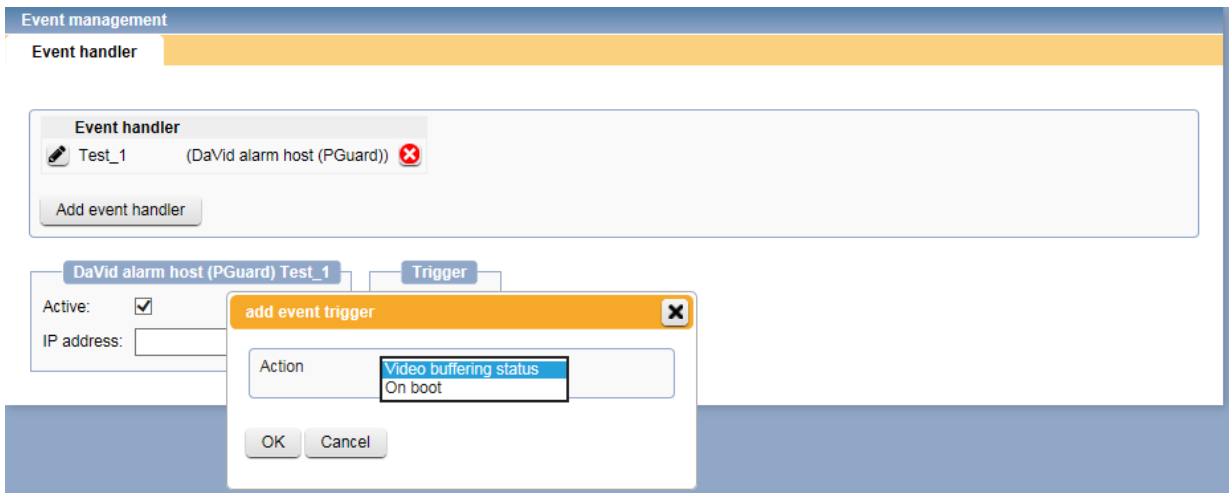


Fig. 9-4

- ⇒ Select the necessary trigger from the drop-down list.
- ⇒ Confirm with “OK”.

# Chapter 10:

## Data Display

The “Data display” function allows you to embed external transaction data or other monitoring information into the video stream.

External data can be transmitted directly to the camera by cash registers, automated teller machines (ATMs), access control systems, casino systems (e.g. slot machines) or other monitoring applications using the DaVid Protocol.

Depending on the client application or device, the embedded data is then displayed directly in the video image (video text overlay) or in the info area of the corresponding camera split (e.g. during video analysis with SMAVIA Viewing Client).

Before embedding external data into the video stream, the received data can be filtered. In addition, you can specify the position of the text overlay directly in the video.

### NOTICE



#### **Video text overlay failure due to incompatible hardware**

Note that the video text overlay is only displayed in conjunction with the following Dallmeier devices:

- DIS-2/M DecoderPro HD
- DIS-2/M Multi-D HD
- WSD-2 HD

In conjunction with the above-mentioned devices, the embedded data is displayed directly in the live video on a connected (via BNC or HDMI interface) monitor as video text overlay.

However, a recording of the embedded data must always be configured separately. For this purpose, activate the “SW contact” or “Field contact” option in the recording settings (event recording) of the corresponding track.

Detailed information on recording embedded data can be found, for example, in the product documentation of the following Dallmeier recording systems:

- DIS-2/M Multi-D HD
- DIS-2/M NSU
- WSD-2 HD

## 10.1 Duration

⇒ Click “Data display” > “Display”.



Fig. 10-1 Display

- ⇒ Activate the data display by selecting the “Show data” check box.
- ⇒ Set the “Duration” for later data display.

The received data is embedded into the current image (frame) that is captured exactly at the moment when the external data is received and stays embedded (is displayed) for the selected “Duration” (frames).

## 10.2 Position

To prevent covering any important image details, the video text overlay can be positioned in the video image.

⇒ Click “Data display” > “Position”.

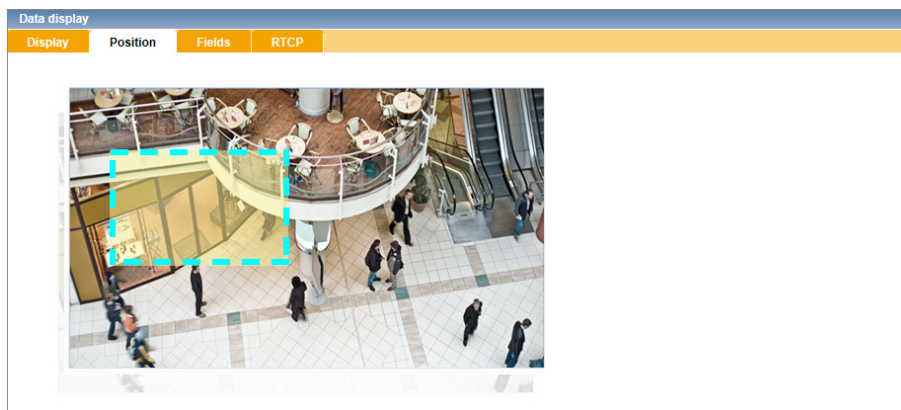


Fig. 10-2 Position

⇒ Define the display area by drawing a rectangle with your mouse.

**i** Note that the aspect ratio and resolution of the actual screen depend on the used client.



## 10.3 Filter

Before embedding external data into the video stream, the received data can be filtered.

**i** *The filtering (selection) affects only to received data, i.e. data that was actually sent from external devices to the camera.*

⇒ Click “Data display” > “Fields”.

| Field          | Use                      | Overwrite label      |
|----------------|--------------------------|----------------------|
| Bank ID:       | <input type="checkbox"/> | <input type="text"/> |
| Debit account: | <input type="checkbox"/> | <input type="text"/> |
| TAN:           | <input type="checkbox"/> | <input type="text"/> |
| Amount:        | <input type="checkbox"/> | <input type="text"/> |
| Currency:      | <input type="checkbox"/> | <input type="text"/> |
| Status:        | <input type="checkbox"/> | <input type="text"/> |
| Date:          | <input type="checkbox"/> | <input type="text"/> |
| Time:          | <input type="checkbox"/> | <input type="text"/> |
| Text1:         | <input type="checkbox"/> | <input type="text"/> |

Fig. 10-3 Fields

⇒ Activate the relevant data by selecting the corresponding check boxes.

**i** *The data is displayed with a preset text (“Field” column). This can be replaced with a new text in the “Overwrite label” column.*

## 10.4 RTCP

**i** *If streaming over RTCP is activated in the network settings (see section “Streaming” on page 44) the transmission of data over RTCP has to be activated as well for a successful data display.*

⇒ Click “Data display” > “RTCP”.

Send data over RTCP:

Fig. 10-4

⇒ Select the “Send data over RTCP” check box.

# Chapter 11:

## Video Content Analysis (VCA)

*This chapter applies to the following Dallmeier HD cameras that are equipped ex factory with firmware version 8.3.2.19 or higher and the “Video Content Analysis (VCA)” function (only available as factory pre-installed function).*

### Box Camera

- DF5200HD-DN

### Dome Camera

- DDF5200HDV-DN

### IR Camera

- DF5200HD-DN/IR

### Module Camera

- MDF5200HD-DN

The “Video Content Analysis (VCA)” function – also called Intelligent Video Analysis (IVA) – allows the above-mentioned cameras to autonomously detect moving objects and suspicious or unusual events in the captured scene while analyzing them with highly sophisticated algorithms in real-time (Real-time Video Analysis).

Depending on the requirements, detected objects can additionally be classified according to their specific characteristics and automatically assigned to a defined object type.

Detected objects and camera analysis events are sent in real-time to the respective **SMAVIA appliance** in the form of metadata (additional information on video data, such as date, time and position of detected events as well as object type or event duration) for storage and further processing.

Using **SMAVIA Viewing Client** and its **SmartFinder** function, image sequences with motion events and classified objects can be specifically searched for and evaluated in the recorded video material.

Besides the general motion detection of objects (video motion detection, VMD) with virtual motion tracking, the following advanced video analysis applications can be individually enabled and configured on the camera in the corresponding tabs:

- **Intrusion detection**  
Automatic generation of event metadata as soon as detected objects (persons, vehicles, etc.) enter or leave user-defined sensitive areas in the image
- **Line crossing detection**  
Automatic generation of event metadata as soon as detected objects touch or cross a user-defined virtual line in the image (virtual tripwire); suitable, for example, for perimeter protection (fence monitoring, protection against climbing)
- **Tamper detection**  
Automatic generation of metadata in the case of camera tampering (camera sabotage protection) or when a sudden change of the illumination level is detected in the captured scene
- **Object classification**  
Automatic classification of detected objects based on their specific characteristics (detection of persons and vehicles)
- **Face detection** (function is available in the “Classification” tab)  
Automatic face detection for a simplified subsequent manual forensic analysis of the recorded video material (only for event filtering by faces; there is no automatic recognition/identification of faces or data matching with face recognition databases)

## 11.1 Requirements


At the time of this document's compilation, the following points have to be observed for the use of the camera-based intelligent video (content) analysis described here:

### Storage and further processing of camera analysis events

- The storage and further processing of camera analysis events is supported by **SMAVIA appliances of generation 5 as of firmware version 8.x.11**.
- On the respective **SMAVIA appliance**, the “Image processing on recorder” option must be disabled in the recording settings for the respective camera and the option for storing camera analysis events (analysis metadata) in the database must be enabled.
- On the respective **SMAVIA appliance**, the “Movement coordinates” and “Sedor data” search items must be enabled in the recording settings for the respective camera in order to be able to evaluate the stored analysis data with **SMAVIA Viewing Client**.

### Evaluation of camera analysis events

The evaluation of camera analysis events is supported by **SMAVIA Viewing Client as of software version 2.4.18**.

 *In this context, also note the explanations in the document “System Description – Video Content Analysis” and in the current documentations of your SMAVIA appliance and SMAVIA Viewing Client.*

## 11.2 Analysis

⇒ In the configuration menu, click the “Video Content Analysis” menu item to open the “Video Content Analysis” dialog.

The “Analysis” tab is displayed.

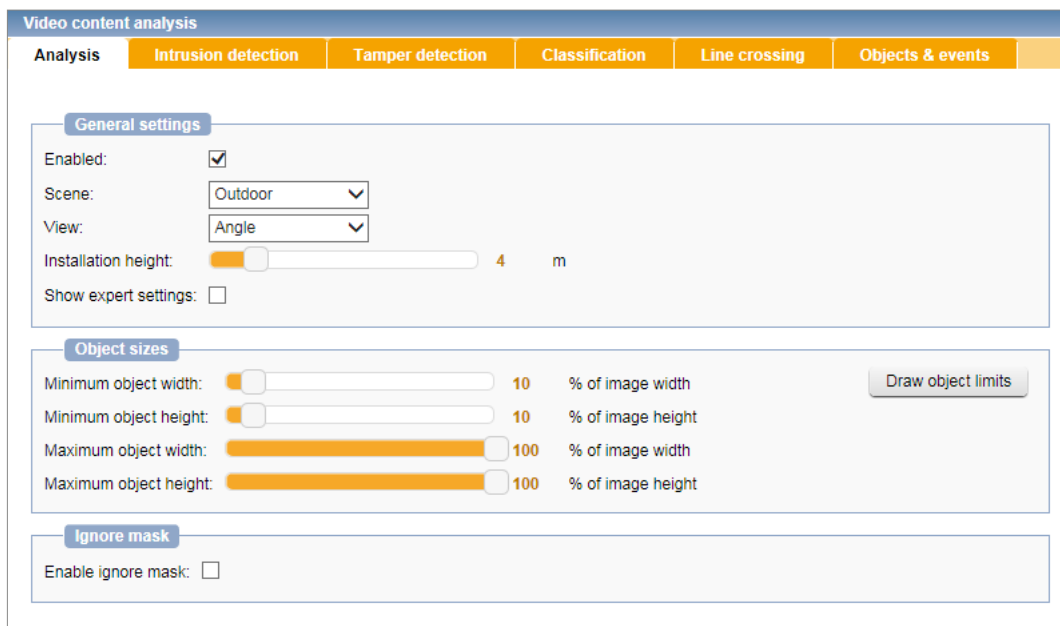


Fig. 11-1


In the screenshot above (Fig. 11-1), the video content analysis on the camera has already been enabled.

In the “Analysis” tab, the video content analysis on the camera can be globally enabled or disabled. In addition, various general preconditions can be set regarding the lighting conditions in different environments (indoor or outdoor), the camera viewing direction (horizontal view, top-down view or angled view), the camera installation height as well as the minimum and maximum size limits for the objects of interest.

Using the advanced (expert) settings, the internal analysis algorithms can be further customized for best analysis performance and results.

Finally, image areas can be generally excluded from the video content analysis to minimize the number of non-relevant detected objects and events on the one hand (e.g. passing persons or vehicles of no interest detected at the edge of the image; movement of clouds, vegetation or water) and to reduce the processor utilization of the camera on the other.

As long as no advanced video analysis applications (“Intrusion detection”, “Line crossing detection”, “Tamper detection”, “Object classification” or “Face detection”) are enabled on the camera, only the tracking coordinates of detected objects (current object position in the image) along with their associated time stamps are continuously transmitted in the form of metadata to the respective SMAVIA appliance until the detected objects are no longer valid.

 For the best possible analysis results during live operation, all changed settings should always be tested in the “Objects & Events” tab for number, plausibility and relevance of detected objects and events (see section “Objects & Events” on page 76).

## 11.2.1 General Settings

⇒ Select the “Enabled” check box to globally enable the video content analysis on the camera.

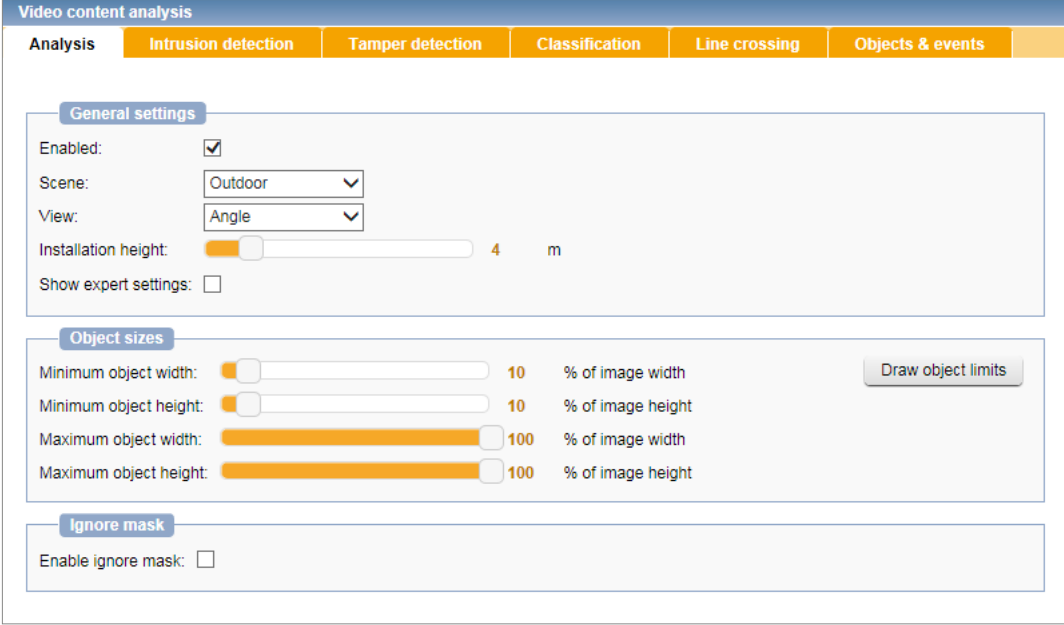


Fig. 11-2

⇒ Configure all required settings (note the following explanations).

## Scene

The “Scene” option allows you to optimize the video analysis algorithms with respect to the prevailing general lighting situation in your scene.

⇒ Select the relevant setting for your scene from the corresponding drop-down list:

- **Outdoor:** Optimized setting for outdoor scenes
- **Indoor:** Optimized setting for indoor scenes

## View

The „View“ option allows you to optimize the video analysis algorithms with respect to the current viewing direction (orientation) of the camera.

⇒ Select the relevant setting for your scene from the corresponding drop-down list:

- **Horizontal:** Optimized setting for horizontal side view (wall mount at lower height); only recommended for “Face detection”
- **Head:** Optimized setting for top-down view (vertical ceiling mount); generally well suited for detecting the direction of movement
- **Angle:** Optimized setting for perspective or angled view looking down (wall or corner mount, tilt angle approx. 30°, installation height approx. 2.5 – 3.0 m); recommended e.g. for “Intrusion detection”

## Installation height

This setting allows you to optimize the video analysis algorithms with respect to the camera installation height.

⇒ Use the corresponding slider to adjust the value of the camera installation height in meters (m).

## Show expert settings

This check box can be selected to display the “Expert settings” (see below).

## 11.2.2 Expert Settings

The “Expert settings” provide special functions for the fine adjustment of the video content analysis. They are only displayed if the corresponding check box has been selected under “General settings” (see above).

⇒ Select the “Show expert settings” check box to display the following options:

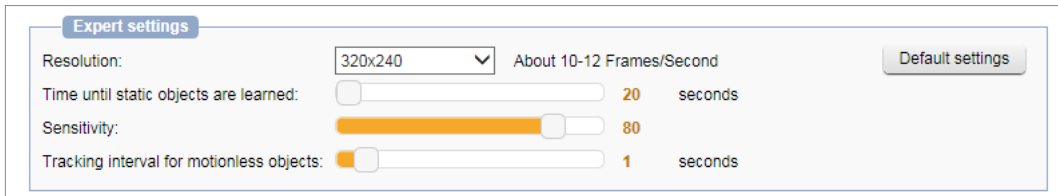


Fig. 11-3

### Resolution

This setting determines the input resolution of the video analysis. The suitable setting depends on the type, distance and motion speed of monitored objects as well as on the scene condition.

Using a higher analysis resolution, smaller objects can be detected in a better way, but with fewer frames per second. The higher the analysis frame rate (frames/second), however, the more accurate the virtual object tracking.

The following table provides an overview of the recommended analysis input resolutions for different scene conditions:

| Scene Condition                | Recommended Analysis Input Resolution (Pixels) |
|--------------------------------|--|
| Indoor – medium/large objects  | 80 × 60  |
| Indoor – small objects         | 160 × 120                                      |
| Outdoor – medium/large objects | 160 × 120                                      |
| Outdoor – small objects        | 320 × 240                                      |

The following table provides an overview of the recommended analysis frame rates for various video analysis applications:

| Video Analysis Application   | Recommended Analysis Frame Rate (Frames/Second) |
|--|---|
| General motion detection of objects (video motion detection, VMD) with virtual motion tracking | 10 – 20 (min. 8)                                |
| Intrusion detection  | 5 – 15 (min. 5)                                 |
| Tamper detection   | 5 – 15 (min. 5)                                 |

⇒ Select the required analysis resolution from the corresponding drop-down list.

**Time until static objects are learned**

This setting determines the elapse time in seconds until detected objects that are no longer moving in the captured scene are viewed as part of the background and not as objects anymore (e.g. a vehicle after parking). Once the set time has elapsed, the corresponding object-related metadata (current tracking coordinates along with their time stamps) are no longer generated.

⇒ Set the required elapse time in seconds with the corresponding slider.

**Sensitivity**

This setting defines the sensitivity of the motion detection.

The higher the set value, the higher the sensitivity and the more motions are detected (i.e. minor changes in the video image are sufficient to detect a motion event).

Recommended sensitivity values for different situations:

**60:** For situations with flickering light sources (e.g. light bulbs).

**70:** For situations with a large amount of pixel noise in the video image due to high signal gain or with continuously small changes in the image (e.g. due to rainfall, snowfall or moving tree branches and leaves in the wind).

**80:** This is the default setting and is suitable for most situations.

**90:** For situations with low video contrast (for example, due to low signal gain) or with gray or dark objects at night.

**95:** For situations with very low video contrast (for example, in foggy environments) or with hardly visible objects at night.

⇒ Set the required sensitivity value with the corresponding slider.

**Tracking interval for motionless objects**

This setting determines the time interval in seconds between repeatedly sending (static) tracking coordinates of no longer moving objects until they are finally viewed as part of the background (see section “[Time until static objects are learned](#)” on page 63). This setting is useful to reduce the number of redundant metadata that is not necessary for later evaluation.

Example:

After a car has been parked, it is still perceived as an object by the camera. However, the no longer changing tracking coordinates of the parked car are still periodically transmitted in the form of metadata to the respective SMAVIA appliance in the set tracking interval until the parked car is viewed as part of the background.

⇒ Set the required tracking interval in seconds with the corresponding slider.

**Default settings**

⇒ Click the “Default settings” button if you want to restore the default expert settings.

### 11.2.3 Object Sizes

This setting allows you to specify the size limits for objects of interest by setting the minimum required and maximum valid object dimensions (width and height values as a percentage in relation to the total image).

The “Draw object limits” function facilitates the estimation of object dimensions in the captured scene.

For a reliable object detection and tracking, the size of objects should be at least 5 – 10 % of the total image.

To detect the presence of average-sized persons in the captured scene, the size of objects (persons) should be approx. 10 – 20 % of the total image.

The size of an object should generally not exceed 40 % of the total image.

Objects (persons) should not get much closer than 3 meters to the camera.

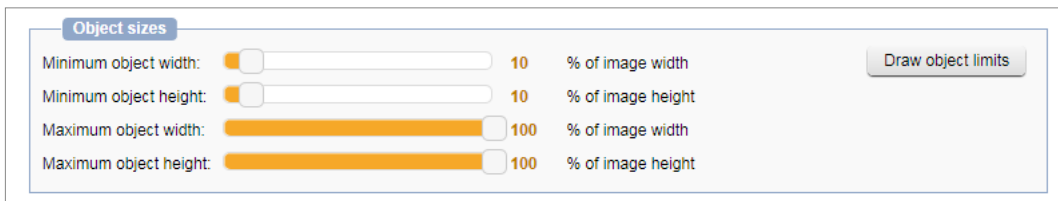


Fig. 11-4

#### Minimum object width/height

⇒ Set the minimum object size (width and height in percentage) with the corresponding sliders.

#### Maximum object width/height

⇒ Set the maximum object size (width and height in percentage) with the corresponding sliders.

#### Draw object limits

⇒ Click the “Draw object limits” button (Fig. 11-4) to define the minimum required and the maximum valid object dimensions with your mouse.

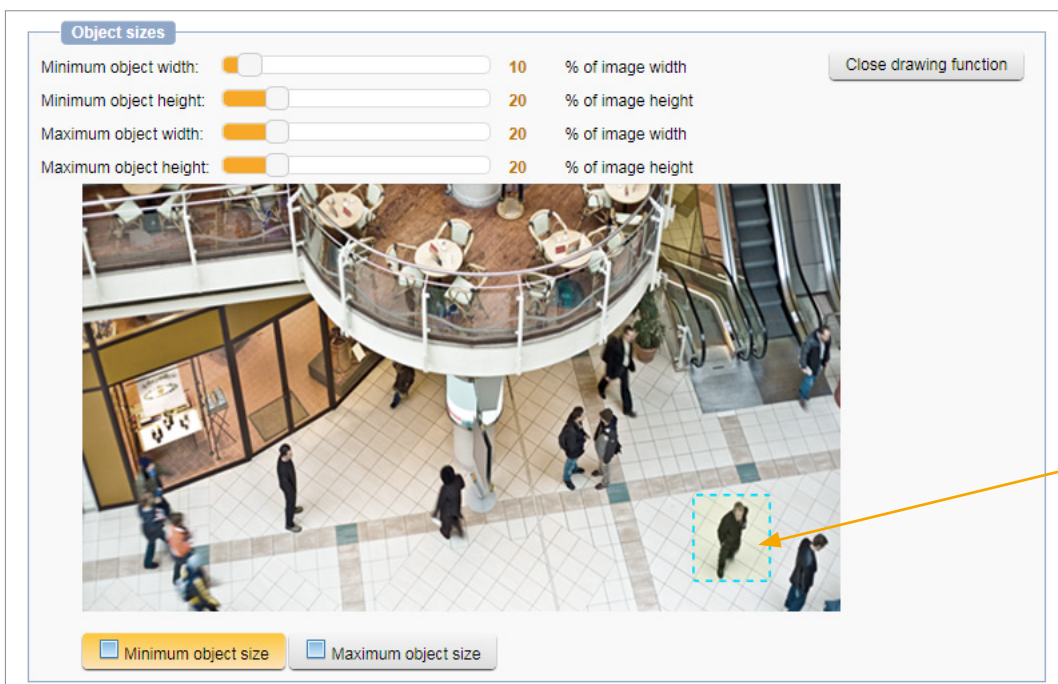



Fig. 11-5



- ⇒ Click the “Minimum object size” button.
- ⇒ Position the mouse pointer over the preview image where you want to start drawing.
- ⇒ Click and hold the left mouse button down, then draw a rectangle for the minimum required object size by dragging the mouse pointer around a reference object of interest (see the arrow in [Fig. 11-5](#)).
- ⇒ Release the mouse button to finish drawing the rectangle.
- ⇒ Click the “Maximum object size” button.
- ⇒ Position the mouse pointer over the preview image where you want to start drawing.
- ⇒ Click and hold the left mouse button down, then draw a rectangle for the maximum valid object size by dragging the mouse pointer around a reference object of interest.
- ⇒ Release the mouse button to finish drawing the rectangle.

The values of the respective dimension sliders are automatically adjusted according to the drawn rectangles (object sizes).

- ⇒ Click the “Close drawing function” button to apply the settings and quit the drawing function.

 *Use real-world objects as a reference when drawing the size limits for objects of interest.*

## 11.2.4 Ignore Mask

The “Ignore mask” function allows you to generally exclude one or multiple user-definable areas in the captured scene from the camera-based video content analysis (inactive areas). This function is useful to minimize the number of non-relevant detected objects and events on the one hand (e.g. passing persons or vehicles of no interest detected at the edge of the image; movement of clouds, vegetation or water) and to reduce the processor utilization of the camera on the other.

After selecting the “Enable ignore mask” check box, a live preview (with a frame rate of 1 fps) as well as various tools are displayed for creating and editing masks that specify inactive areas.

Inactive area masks are highlighted in red in the live preview. Any changes are always applied without further user action.

To create inactive areas, proceed as follows:

- ⇒ Select the “Enable ignore mask” check box.
- ⇒ Click the required tool (button) to draw, edit or delete inactive areas (see below).

### Draw rectangle

- ⇒ Click the “Draw rectangle” button.
- ⇒ Click and hold the left mouse button down while drawing a rectangle over the relevant part of the image.

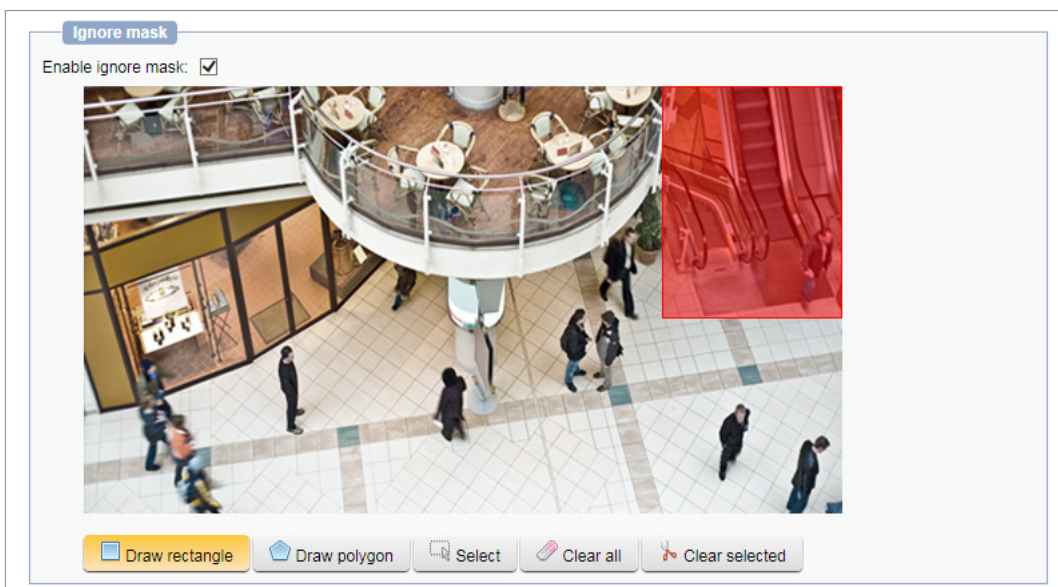


Fig. 11-6

**i** You can define multiple rectangular inactive areas. The corners of a drawn rectangle can also be edited later on (see section “[Select/edit](#)” on page 68).

## Draw polygon

- ⇒ Click the “Draw polygon” button.
- ⇒ Left-click and release the mouse button to set the vertices (corners) of the polygon except for the last vertex.
- ⇒ Right-click and release the mouse button to set the final vertex of the polygon.

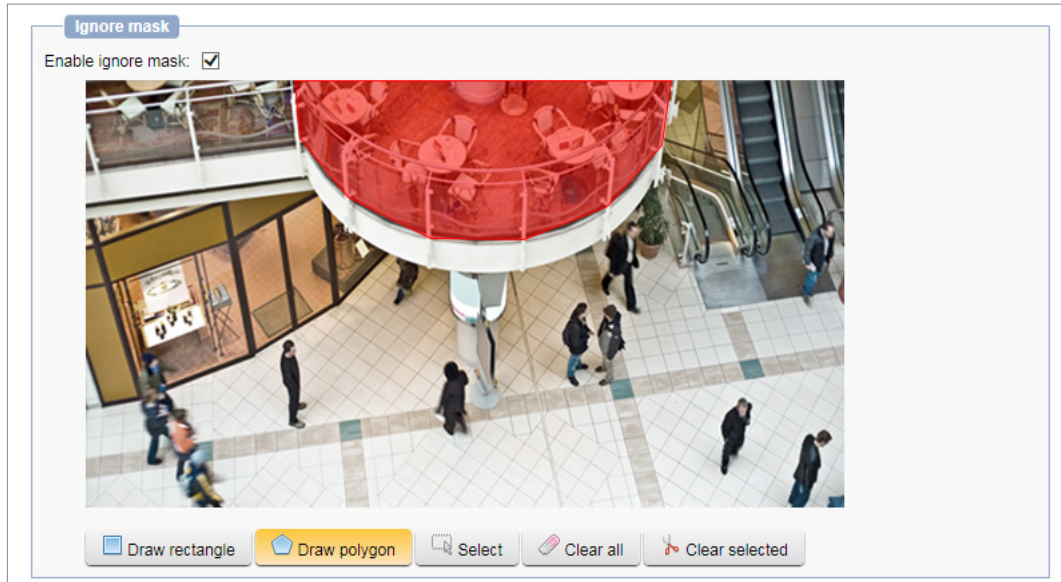


Fig. 11-7

- i** You can define multiple polygonal inactive areas.  
The vertices (corners) of a drawn polygon can also be edited later on (see section “[Select/edit](#)” on page 68).

**Select/edit**

- ⇒ Click the “Select” button.
- ⇒ Left-click an inactive area.

The selected inactive area is marked with small white circles at its vertices.

To edit an inactive area, proceed as follows:

- ⇒ Left-click a white circle and move it to the required position while holding the mouse button down.
- ⇒ Release the mouse button when finished.
- ⇒ Repeat the last two steps for all vertices you want to edit.

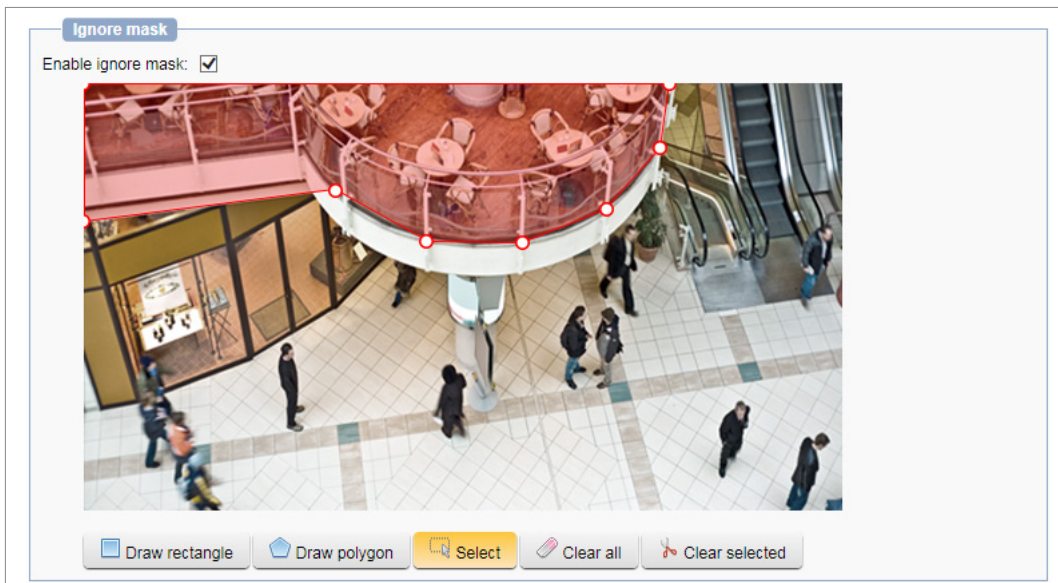


Fig. 11-8: Polygon selected for editing; the vertices (corners) are indicated by white circles with red borders

**i** *New vertices cannot be added to an existing mask and existing vertices cannot be deleted.*

For deleting inactive areas, see descriptions below.

**Clear all**

- ⇒ Click the “Clear all” button to delete all defined inactive areas.

**Clear selected**

- ⇒ Click the “Clear selected” button to delete a previously selected inactive area (see section “[Select/edit](#)” on page 68).

## 11.3 Intrusion Detection

Besides the general motion detection of objects (video motion detection, VMD) with virtual motion tracking, the advanced video analysis application “Intrusion detection” allows for the automatic generation of event metadata as soon as detected objects (persons, vehicles, etc.) enter or leave user-defined sensitive areas in the image.

After selecting the “Enable intrusion detection” check box, a live preview (with a frame rate of 1 fps) as well as various tools are displayed for creating and editing masks that specify active sensitive areas in the image.

Active sensitive areas are highlighted in red in the live preview.  
Any changes are always applied without further user action.

To create active sensitive areas, proceed as follows:

⇒ Select the “Enable intrusion detection” check box.

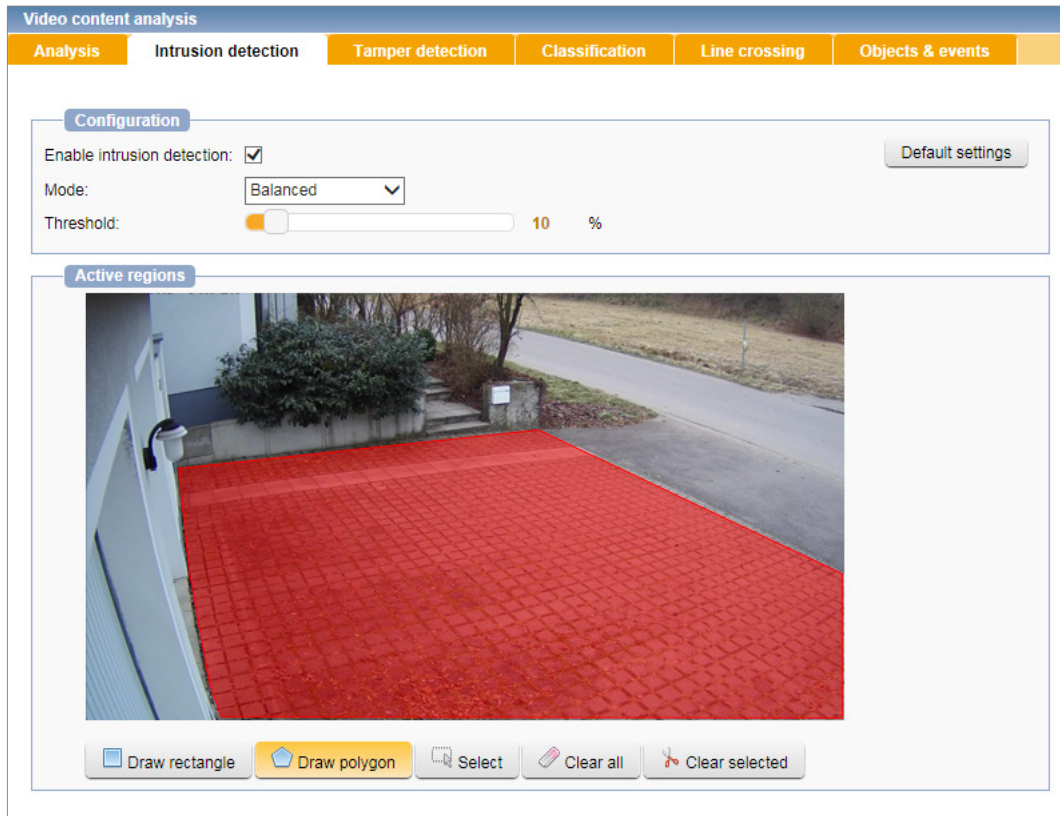


Fig. 11-9

The procedure for creating and editing active sensitive areas in the image corresponds to the procedure for creating and editing globally inactive areas of the video content analysis (see section “Ignore Mask” on page 66).

⇒ Define the required active sensitive areas in the image where the video analysis application “Intrusion detection” is to be applied.

In the example shown above (Fig. 11-9), the driveway to the garage was defined as an active sensitive area using the “Polygon” tool. As soon as an object enters (or leaves) this area, an event is automatically generated and sent to the respective SMAVIA appliance in the form of metadata in real-time for storage and further processing.

Using the “Mode” and “Threshold” settings, the detection results can be further optimized (see below).

### **Mode**

This setting specifies the detection sensitivity:

- **Balanced**  
This setting is the default setting being suitable for most situations as a balance between insensitive and sensitive (see below).
- **Insensitive**  
With this setting, the priority is on avoiding events that are falsely considered as relevant. However, there is an increased risk that an actually relevant event may not be detected.
- **Sensitive**  
With this setting, the priority is on detecting as many relevant events as possible. However, events falsely considered as relevant are tolerated.

⇒ Select the required sensitivity setting from the “Mode” drop-down list.

### **Threshold**

The “Threshold” value determines the percentage of a detected object generating an event when entering (or leaving) the active sensitive area.

⇒ Set the required threshold value with the corresponding slider.

### **Default settings**

⇒ Click the “Default settings” button if you want to restore the default settings.

## 11.4 Tamper Detection

The advanced video analysis application “Tamper detection” allows for an automatic detection of camera tampering (camera sabotage protection). As soon as any manipulation on the camera is detected, e.g. spraying, covering or blinding the lens or in case of a fast scene change (e.g. caused by changing the current camera orientation), an event is automatically generated and sent to the respective SMAVIA appliance in the form of metadata in real-time for storage and further processing.

In addition, the camera can be configured to automatically generate an event when detecting a sudden change of the illumination level in the captured scene (“Lights on/off detection”).

### 11.4.1 Camera Tamper Detection

To use the camera tamper detection, proceed as follows:

⇒ Select the “Enable tamper detection” check box.

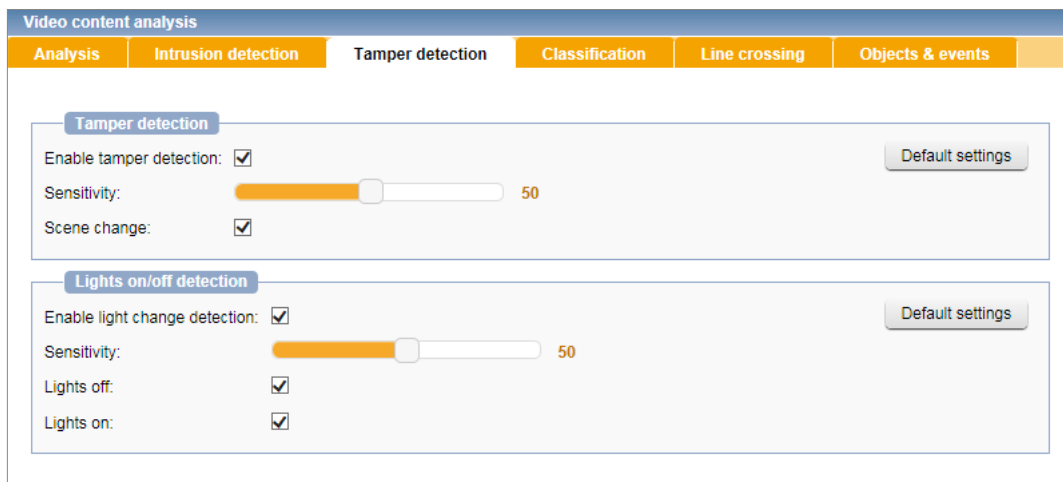


Fig. 11-10

⇒ Set the relevant options (see below).

#### Sensitivity

The sensitivity of the camera tamper detection determines how quickly a manipulation on the camera is detected as such. For example, the higher the set sensitivity, the less the camera lens has to be covered to generate an event.

⇒ Set the sensitivity of the camera tamper detection with the corresponding slider.

#### Scene change

⇒ Select the “Scene change” check box to configure the camera to automatically generate an event in case of a fast scene change (e.g. caused by changing the current camera orientation).

Note, however, that a high sensitivity setting of the camera tamper detection (see above) may also lead to a lot of non-relevant events, e.g. due to weather-related camera movements. In this case, set a lower sensitivity value.



**Default settings**

⇒ Click the “Default settings” button if you want to restore the default settings.

**11.4.2 Lights On/Off Detection**

Using the “Lights on/off detection” function, the camera can be configured to automatically generate an event as soon as a sudden change of the illumination level is detected in the captured scene (“Lights on/off detection”), e.g. when a light source in a room is switched on or off.

To use the “Lights on/off detection” function, proceed as follows:

⇒ Select the “Enable light change detection” check box.

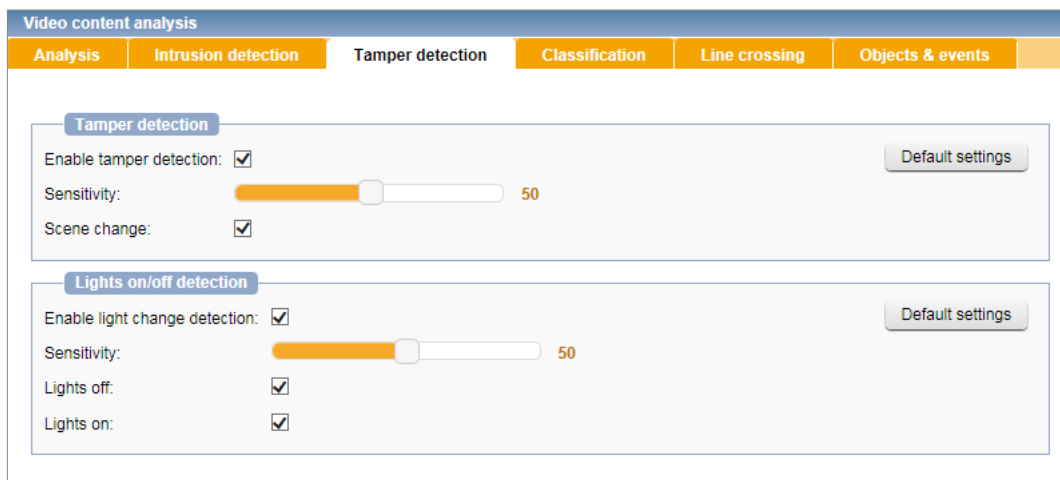


Fig. 11-11

⇒ Set the relevant options (see below).

**Sensitivity**

This setting determines how large the change in light intensity has to be to generate an event. The higher the set sensitivity value, the less the light intensity has to change within a given (internal) time to generate an event.

⇒ Set the required sensitivity value with the corresponding slider.

**Lights off/on**

The “Lights off” and “Lights on” check boxes can be selected to further specify the light change generating an event: in case of a sudden drop in the illumination level (e.g. by switching off a light source in the captured scene), in case of a sudden increase (e.g. by switching on a light source) or in both cases.

⇒ Select the required check boxes.

**Default settings**

⇒ Click the “Default settings” button if you want to restore the default settings.



## 11.5 Object Classification

By enabling the “Object classification” function in the “Classification” tab, detected objects can be classified according to their specific characteristics and automatically assigned to a defined object type (persons or vehicles).

Furthermore, the camera can be configured to analyze detected objects for the presence of faces.

The additional object type information is sent in real-time to the respective SMAVIA appliance in the form of metadata for storage and further processing.

During the subsequent evaluation of events with SMAVIA Viewing Client and its SmartFinder function the search results can be filtered specifically according to matching object types and, if present, existing faces.

### 11.5.1 Object Classification by Persons and Vehicles

The object classification by persons and vehicles attempts to interpret whether a detected object in the captured scene is a person or a vehicle and assigns it to the corresponding object type.

To use the automatic object classification by persons and/or vehicles, proceed as follows:

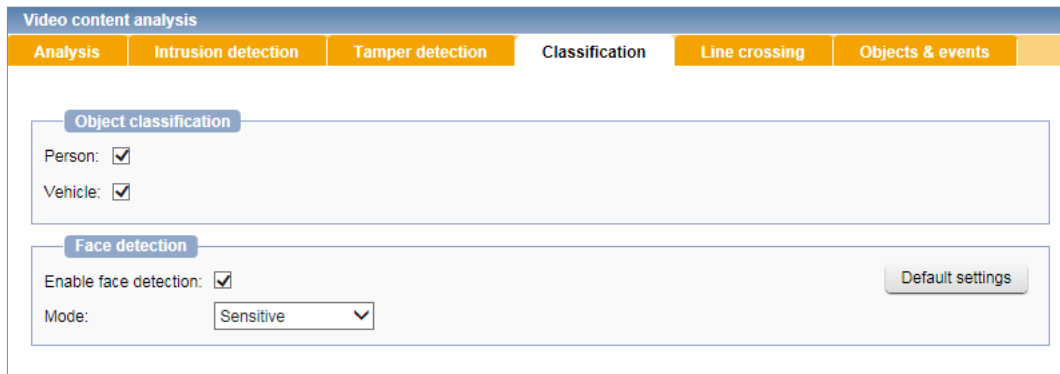


Fig. 11-12

⇒ Select the required check box(es):

#### Person

Using this option, detected objects having typical characteristics of a person can be assigned to the object type “Person”.

#### Vehicle

Using this option, detected objects having typical characteristics of a vehicle can be assigned to the object type “Vehicle”.


Generally, a detected object is initially considered as an *unknown object*.

The longer an object is analyzed, the more accurate is the assignment of a detected object to a particular object type.

If, for example, a delivery van moves slowly into the captured scene, the detected object may initially be interpreted as a *person*. However, with progressing analysis (the van continues to move into the scene), the appropriate *vehicle* type is detected/selected.

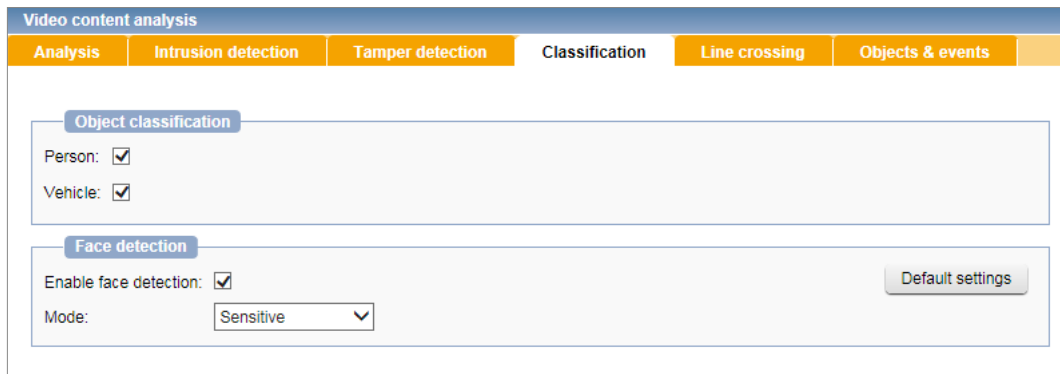
## 11.5.2 Face Detection

The “Face detection” function analyzes detected objects in the captured scene for the presence of faces and serves for a simplified subsequent manual forensic analysis of the recorded video material. As soon as the camera interprets characteristics of a detected object as a face, a corresponding event is generated.

 *The “Face detection” function only analyzes whether a face is present in the captured scene; there is no automatic recognition/identification of faces or data matching with face recognition databases.*

To use the “Face detection” function, proceed as follows:

⇒ Select the “Enable face detection” check box.



The screenshot shows the 'Video content analysis' interface with several tabs: Analysis, Intrusion detection, Tamper detection, Classification, Line crossing, and Objects & events. The 'Objects & events' tab is active. Under 'Object classification', 'Person' and 'Vehicle' are checked. Under 'Face detection', 'Enable face detection' is checked, and the 'Mode' is set to 'Sensitive'. A 'Default settings' button is visible.

Fig. 11-13

⇒ Select the required sensitivity setting from the “Mode” drop-down list (see below).

### Mode

This setting determines the sensitivity of the face detection:

- **Insensitive**  
With this setting, the priority is to avoid misinterpreting object features as faces. However, there is an increased risk that the actual presence of a face in the captured scene may not be detected.
- **Sensitive**  
With this setting, the priority is on detecting as many potential faces as possible. However, object features that are misinterpreted as faces are tolerated.

### Default settings

⇒ Click the “Default settings” button if you want to restore the default settings.

## 11.6 Line Crossing Detection

Besides the general motion detection of objects (video motion detection, VMD) with virtual motion tracking, the advanced video analysis application “Line crossing detection” allows for the automatic generation of event metadata as soon as detected objects touch or cross a user-defined virtual line in the image (virtual tripwire). This function is suitable, for example, for perimeter protection (fence monitoring, protection against climbing).

To create a virtual line in the image, proceed as follows:

⇒ Select the “Enable line crossing detection” check box.

A live preview of the captured scene (with a frame rate of 1 fps) is displayed.

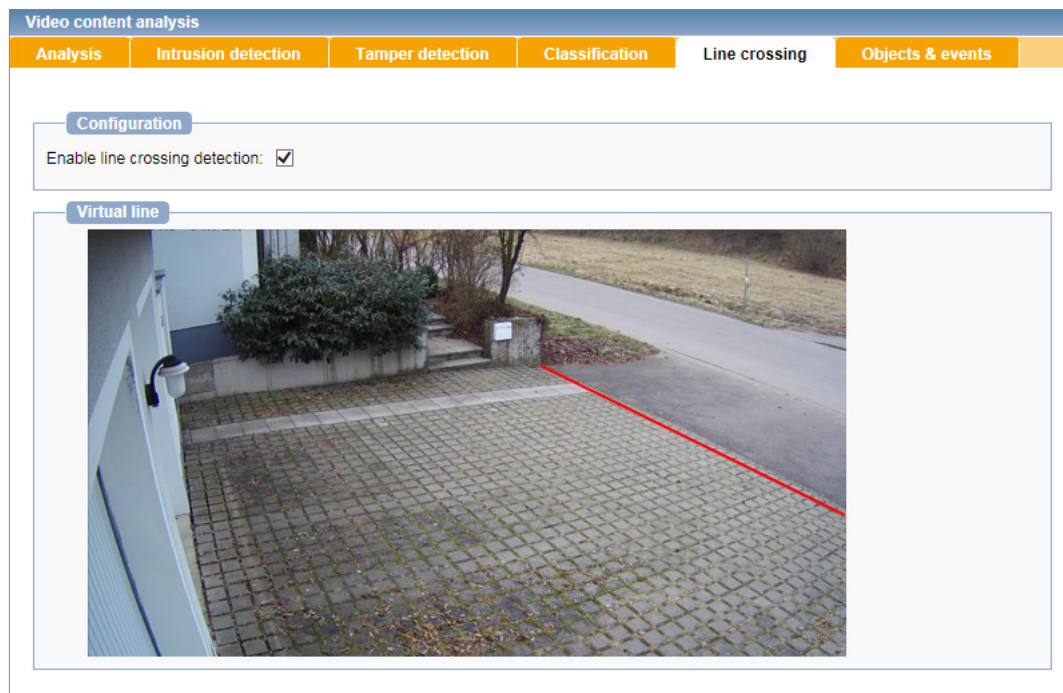


Fig. 11-14

⇒ Click and hold the left mouse button down while drawing a virtual line across the relevant part of the image.

The virtual line is displayed in red.

### Edit virtual line

Only one virtual line can be drawn in the image.


An existing virtual line is automatically replaced by drawing a new one.

### Delete virtual line

To remove a drawn virtual line, click into the image.

## 11.7 Objects & Events


In the “Objects & Events” tab, the video analysis settings can be tested in detail before live operation of the camera.

 For the best possible analysis results during live operation, all changed settings should always be tested in the “Objects & Events” tab for number, plausibility and relevance of detected objects and events.

Video content analysis

Analysis
Intrusion detection
Tamper detection
Classification
Line crossing
Objects & events

Objects



Events

| Date/time           | Event no. | Event description | Related object |
|---------------------|-----------|-------------------|----------------|
| 16.05.2017 15:14:50 | Event 6   | Lights off        |                |
| 16.05.2017 13:39:06 | Event 5   | Camera tampered   |                |
| 16.05.2017 13:38:34 | Event 4   | Camera tampered   |                |
| 16.05.2017 11:45:30 | Event 3   | Lights off        |                |
| 16.05.2017 11:45:29 | Event 2   | Lights on         |                |
| 16.05.2017 10:33:40 | Event 1   | Camera tampered   |                |
| 16.05.2017 10:33:38 | Event 0   | Lights off        |                |

Statistics

| Name            | Value |
|-----------------|-------|
| CPU utilization | 36.3% |
| Frames/Second   | 12.53 |

Fig. 11-15

### Objects

In the “Objects” section, detected objects are highlighted with colored bounding boxes in a live preview of the captured scene (frame rate 1 fps) and virtually tracked until they are no longer perceived as objects. Depending on the detected object type, different colors are used (e.g. red bounding box around unclassified objects, green bounding box around persons, yellow bounding box around faces).


## Events

In the “Events” section, the last 20 events generated by the video analysis applications “Intrusion detection”, “Line crossing detection” and “Tamper detection” are listed.

Each list item provides the exact time stamp of the event as well as a short event description.

## Statistics

In the “Statistics” section, the current CPU load (in percentage) generated exclusively by the video content analysis algorithms is displayed as well as the current analysis frame rate (frames/second).

 *In this context, also note the descriptions about the analysis input resolution and analysis frame rate in section “[Resolution](#)” on page 62.*

# Chapter 12:

## Users and Rights

The configuration of the device is accessible for authenticated and authorized users only.

The user management allows you to grant multiple access and configuration rights for different user groups. The individual users can be assigned to a certain user group.

### 12.1 User Names and Passwords

For security reasons, passwords should consist of at least 8 characters. Do not use any personal information, conventional expressions (real words) or names.

A secure password needs to be complex, random and long.

A combination of upper-case letters (e.g. ABC), lower-case letters (e.g. abc), numerals (e.g. 123) and non-alphanumeric keyboard symbols (e.g. \_ / ^) is usually secure.

#### Character sets supported by the camera

The following character sets are supported by the camera:

- ISO-8859-1 (all languages except Russian)
- Windows-1251 (Russian language only)

#### Characters supported by Dallmeier recording systems

#### NOTICE



#### Invalid user name or password due to unsupported characters

Dallmeier recording systems currently only support a combination of the following characters:


- Upper-case letters (A – Z)
- Lower-case letters (a – z)
- Digits (0 – 9)
- Non-alphanumeric keyboard symbols ( \_ - . )

In addition, user names must always start with a letter.

---

## 12.2 Users

The login on the device always requires the entry of a user name and the corresponding password.

 *During the definition of a user, the entry of an e-mail address is required.*

⇒ Click “Users & Rights” > “User management”.

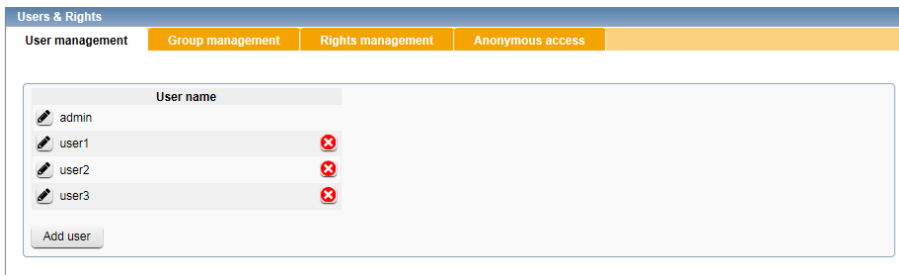



Fig. 12-1 User management

### Define user

- ⇒ Click “Add user”.
- ⇒ Enter a user name.
- ⇒ Enter an e-mail address.
- ⇒ Enter a password.
- ⇒ Finally, confirm with “Create new user account”.

### Edit user


- ⇒ Click the “X” button (right) to delete the user account.

 *The user account “admin” cannot be deleted.*

- ⇒ Click the “Pencil” button (left) to edit the password.

## 12.3 Groups

All users can be assigned to a user group. They receive the rights that have been set for this group.

 *Each user can be assigned to one group only.*

⇒ Click “Users & Rights” > “Group management”.

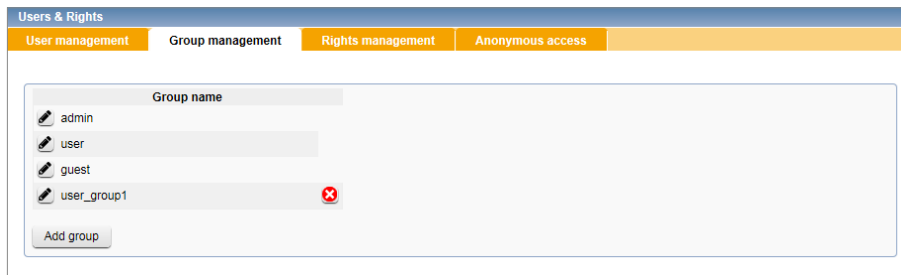



Fig. 12-2 Group management

### Define group

- ⇒ Click “Add group”.
- ⇒ Enter a group name.
- ⇒ Finally, confirm with “Create new group”.

### Edit group

- ⇒ Click the “X” button (right) to delete the group.

 *The groups “admin”, “user” and “guest” cannot be deleted.*

⇒ Click the “Pencil” button (left) to edit the members of the group.

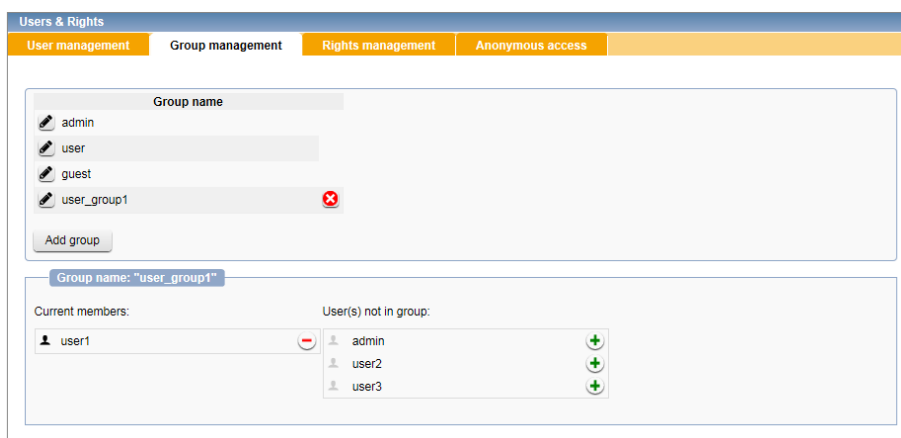



Fig. 12-3 Members

- ⇒ Click the “+” button (right column) to assign the user to the group.
- ⇒ Click the “-” button (left column) to remove the user from the group.



## 12.4 Rights

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

 *The rights of the user group “admin” cannot be restricted.*

⇒ Click “Users & Rights” > “Rights management”.

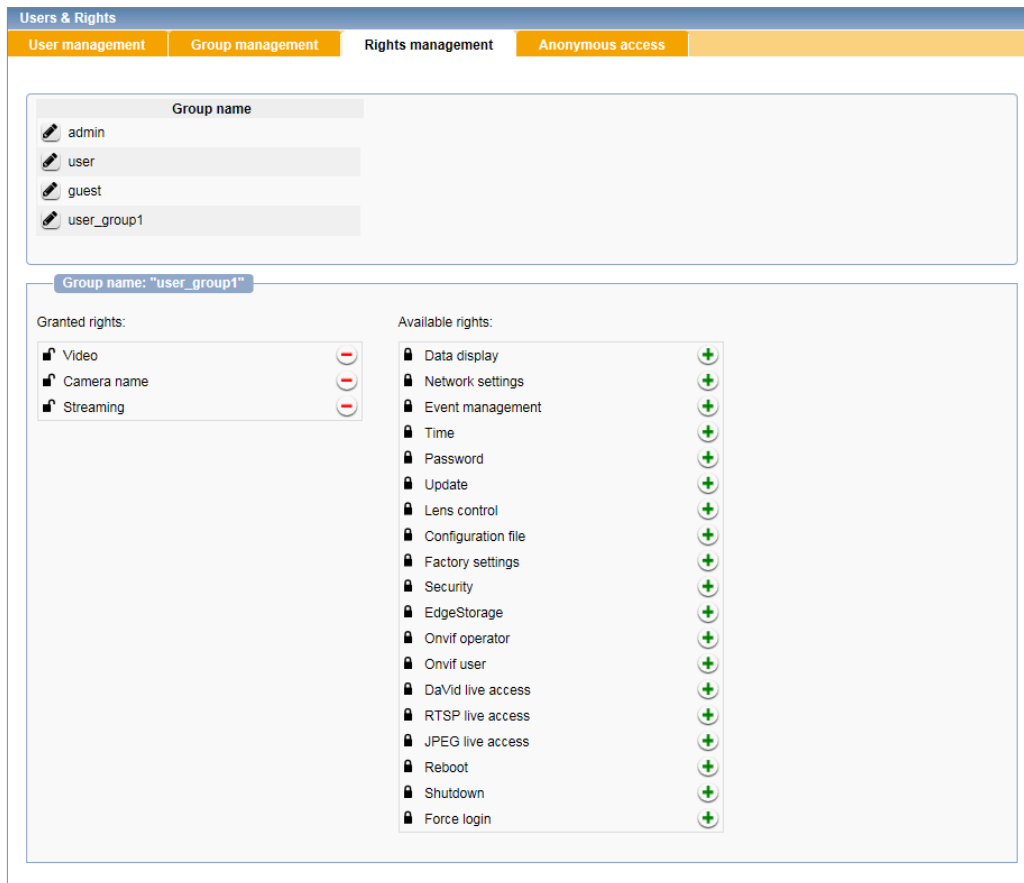


Fig. 12-4

- ⇒ Click the “Pencil” button (left) to edit the rights of a group.
- ⇒ Click the “Check” button (green) to grant the right for the group.

## 12.5 Anonymous Access

“Anonymous access” regulates how image transmission without prior authentication by the user is handled (see “[Image Transmission](#)” on page 86).

⇒ Click “Anonymous access”.

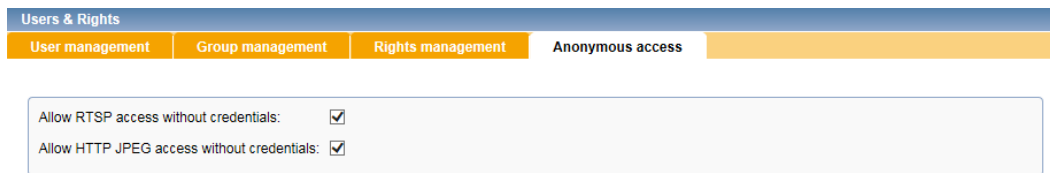


Fig. 12-5

⇒ Select the necessary check box.

# Chapter 13:

## Service

### 13.1 Configuration File

The configuration of the device can be exported and saved.

⇒ Click “Service” > “Configuration file”.

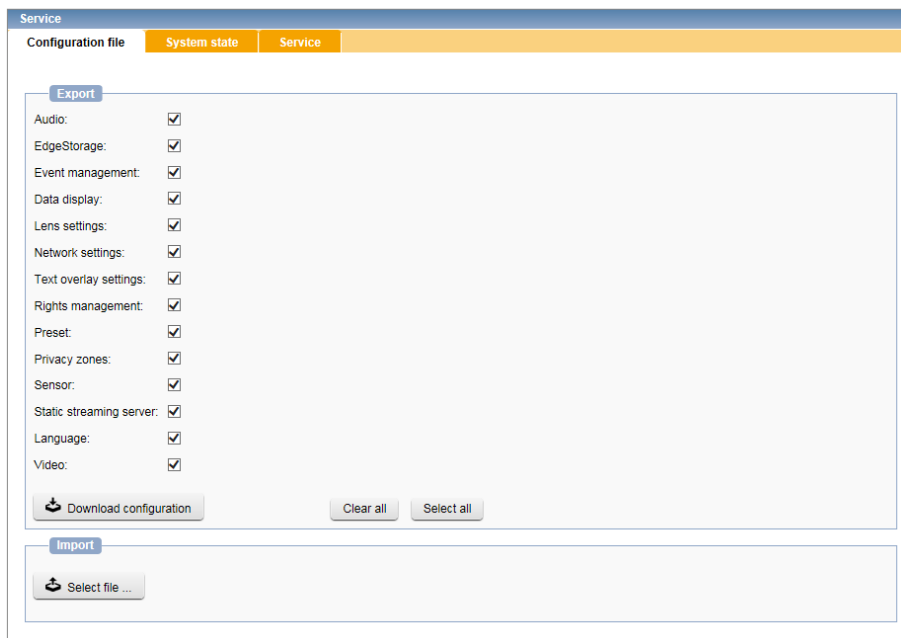


Fig. 13-1 Configuration file

- ⇒ Select all relevant settings that you want to export to the configuration file by selecting the corresponding check boxes.
- ⇒ Confirm with “Download configuration”.

The configuration file is displayed as text in the browser.

- ⇒ Save the configuration file on your workstation.

## 13.2 Factory Settings

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

⇒ Click “Service” > “System state”.

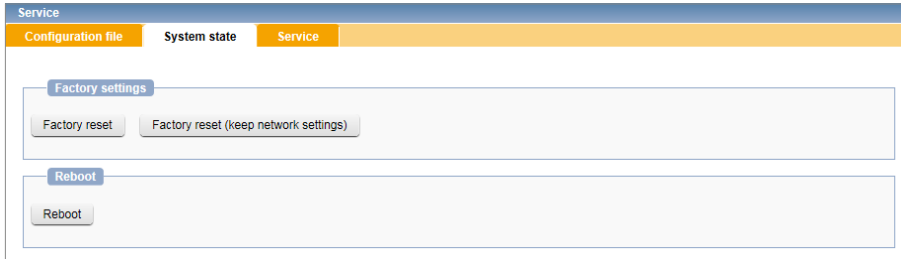


Fig. 13-2 System state

⇒ Click the necessary button.

### NOTICE



#### Immediate execution

The selected action is executed without prior confirmation prompt.  
The device is reset to factory settings or restarted immediately.

## 13.3 Service

The “Service” option allows you to download support information as a .dat file for further use.

⇒ Click the “Download support information” button.

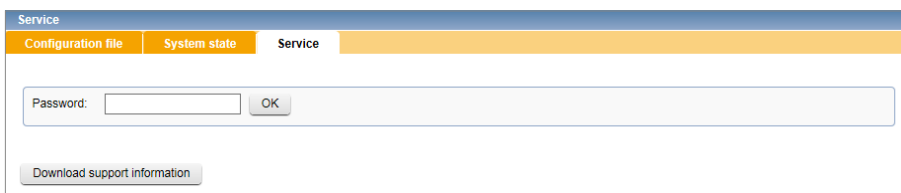


Fig. 13-3

⇒ Save the .dat file at an appropriate location.



*The keyword detection serves as a special option to access additional data for the development team of Dallmeier. It is not necessary for downloading the support information.*

# Chapter 14:

## Information

### 14.1 General Information

General information on the device is displayed in the “Information” dialog.

⇒ Click “Information” > “General information”.

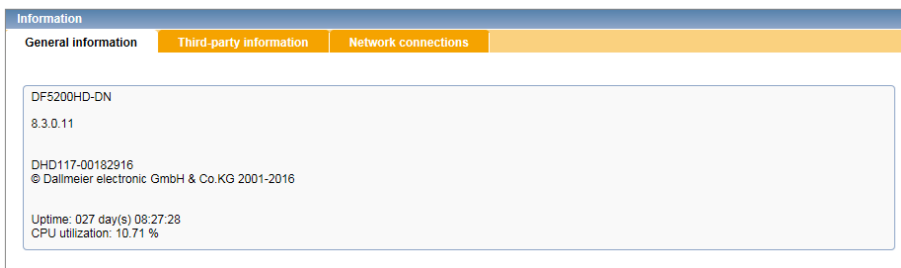


Fig. 14-1 Information

The following information is displayed:

- Device type
- Firmware version
- Serial number of the device
- Uptime (elapsed time since last system boot)

### 14.2 Network connections

Information on the current connections is displayed in the “Network connections” tab.

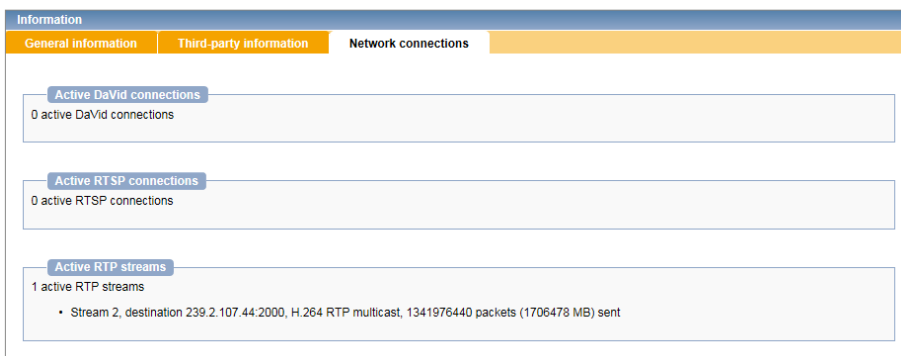


Fig. 14-2 Network connections

Also note the information in the “Third-party information” tab.

# Chapter 15:

## Image Transmission

### 15.1 Single Image (JPEG)

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

|                       |      |
|-----------------------|------|
| Transport protocol    | TCP  |
| Transmission protocol | HTTP |
| Port                  | 80   |

Note that

- the requested encoder must be configured for “MJPEG” encoding.
- the requested encoder must be activated.
- the “JPEG live access” right/permission must be activated (see section “[Rights](#)” on page 81).

or

- the “Allow JPEG access without credentials” check box has to be selected (see section “[Anonymous Access](#)” on page 81)

Use the following URL requests for the various encoders:

|           |  |
|-----------|--|
| Encoder 1 | <code>http://IP address of the device/live/image0.jpg</code> |
| Encoder 2 | <code>http://IP address of the device/live/image1.jpg</code> |
| Encoder 3 | <code>http://IP address of the device/live/image2.jpg</code> |
| Encoder 4 | <code>http://IP address of the device/live/image3.jpg</code> |

The displayed single image (JPEG) can be refreshed at any time (e.g. by using the F5 key on your keyboard).

The query expression (URL request) can also be integrated into an HTML (JavaScript) page that refreshes the image automatically.

## 15.2 RTSP Application

The live video can be requested by RTSP clients (e.g. players) and the transmission of the streaming content can be controlled (start and stop) using RTSP.

For more information, refer to the section “[Network Services](#)” on page 48.

|                       |                       |
|-----------------------|-----------------------|
| Transport protocol    | TCP/UDP               |
| Transmission protocol | RTP                   |
| Control protocol      | RTSP                  |
| Port                  | 554 (default setting) |

### RTSP and RTP over HTTP tunneling

|                       |      |
|-----------------------|------|
| Transmission protocol | HTTP |
| Port                  | 80   |

Note that

- the requested encoder must be activated.
- the RTSP server in the camera must be activated (see section “[Network Services](#)” on page 48).
- the “RTSP live access” right/permission must be activated (see section “[Rights](#)” on page 81).

or

- the “Allow RTSP access without credentials” check box has to be selected (see “[Anonymous Access](#)” on page 81).

Use the following URL requests for the various encoders:

|           |   |
|-----------|---|
| Encoder 1 | <code>rtsp://IP address of the device/encoder1</code> |
| Encoder 2 | <code>rtsp://IP address of the device/encoder2</code> |
| Encoder 3 | <code>rtsp://IP address of the device/encoder3</code> |
| Encoder 4 | <code>rtsp://IP address of the device/encoder4</code> |

The encoders 1 – 4 can be requested by two applications simultaneously. This allows you to realize a “Dual-, Tri or Quad-Streaming” functionality (up to four streams with different quality).

If multiple applications are requesting the data of one encoder, the network load and, thus, the required bandwidth increases proportionally. I

In this case, a multicast configuration should be preferred since this only requires bandwidth for one stream.



*Note that if there is a deviation from the standard port (554) it has to be added explicitly to the URL.*

*After the IP address add a “:” (colon) followed by the number of the new port.*

*Example for Encoder 1 with new RTSP-port-number 1024:*

`rtsp://IP address of the device:1024/encoder1`

