CAMERAS
5000 SERIES
FIRMWARE VERSIONS 8.3.4.17 & 10.1.0.4
# CONTENTS

## CHAPTER 1: INTRODUCTION
- 1.1 Validity ................................................................. 6
- 1.2 Compatibility .......................................................... 6
- 1.3 Disclaimer .............................................................. 7
- 1.4 Documents ............................................................. 7
- 1.4.1 This Document .................................................... 7
- 1.4.2 Other Applicable Documents ................................. 7
- 1.5 Typographical Conventions ....................................... 8

## CHAPTER 2: CONNECTION AND LOGIN
- 2.1 System Requirements ............................................... 9
- 2.2 Connection ............................................................ 10
- 2.3 Login ................................................................. 11

## CHAPTER 3: SECURITY AND DATA PROTECTION
- 3.1 Security .............................................................. 13
- 3.2 Data protection ...................................................... 13

## CHAPTER 4: IMAGE
- 4.1 Presets ................................................................. 14
- 4.2 Image Optimization ................................................ 17
- 4.2.1 White Balance .................................................... 18
- 4.2.2 Color Temperature ............................................... 19
- 4.2.3 Local Tone Mapping ............................................. 20
- 4.2.4 Auto Contrast ..................................................... 21
- 4.2.5 Noise Filter ........................................................ 22
- 4.3 Exposure Settings .................................................. 23
- 4.3.1 Exposure Mode ................................................... 23
- 4.3.2 Slow Shutter Limit .............................................. 23
- 4.3.3 Gain limit .......................................................... 23
- 4.3.4 Flicker-Control .................................................... 23
- 4.3.5 Exposure Priority ................................................ 24
- 4.3.6 Aperture Mode .................................................... 24
- 4.4 Day/Night ............................................................. 25
- 4.4.1 Day/Night Mode .................................................. 25
- 4.4.2 Threshold Level .................................................. 25
- 4.4.3 Response Time .................................................... 26
- 4.4.4 Color ............................................................... 26
- 4.4.5 Lighting Mode DF5200HD-DN/IR .......................... 26
- 4.4.6 Lighting Mode DF5400HD-DN/IR & DF5210HD-DN/IR 27
- 4.5 Lens Control .......................................................... 28
- 4.6 Privacy Zones ........................................................ 30
- 4.7 Text Overlay .......................................................... 31
INTRODUCTION

1.1 VALIDITY

This document applies to the following devices:

<table>
<thead>
<tr>
<th>Box Cameras</th>
<th>IR Cameras</th>
<th>Module/Fisheye Cameras</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DF5300HD-DN</td>
<td>• DF5400HD-DN/IR</td>
<td>• SDF5410HD-DN</td>
</tr>
<tr>
<td>• DF5200HD-DN</td>
<td>• DF5210HD-DN/IR</td>
<td>• MDF5400HD-DN</td>
</tr>
<tr>
<td></td>
<td>• DF5140HD-DN/IR</td>
<td>• MDF5200HD-DN</td>
</tr>
<tr>
<td></td>
<td>• DF5120HD-DN/IR</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dome Cameras</th>
<th>Panomera®</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DDF5400HDV-DN</td>
<td>• Nightline Series</td>
</tr>
<tr>
<td>• DDF5300HDV-DN</td>
<td>• Topline Series</td>
</tr>
<tr>
<td>• DDF5200HDV-DN</td>
<td>• Ultraline Series</td>
</tr>
<tr>
<td>• DDF5140HDV-DN</td>
<td></td>
</tr>
<tr>
<td>• DDF5120HDV-DN</td>
<td></td>
</tr>
<tr>
<td>• DDF5140HD-DN (Indoor)</td>
<td></td>
</tr>
<tr>
<td>• DDF5120HD-DN (Indoor)</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-1

The contents of this document are based on the released camera firmware versions 8.3.4.17 & 10.1.0.4.

For reasons of simplicity, the term “device” or “camera” is used in the following. However, if text passages require a distinction 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 COMPATIBILITY

The camera firmware versions 8.3.4.17 & 10.1.0.4 are compatible with the following hardware/software:

- SMAVIA appliances as of firmware version 8.x.11 SP C
- SMAVIA Viewing Client as of software version 2.4.18
- SMAVIA Viewer as of software version 2.4.18
- SeMSy® III Video Management System as of version 1.7.3
- Dallmeier Live Video ActiveX® control as of version 1.3.110
1.3 DISCLAIMER

The contents of this document describe the full functional range of the above-mentioned camera firmware versions.

However, note that

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

1.4 DOCUMENTS

The product documentation contains several documents that are supplied with your device in a printed form and/or on a digital medium. Further technical documentation for your device, if available, is published exclusively on the website www.dallmeier.com.

Read the available product documentation carefully and thoroughly before using your device. Always observe and follow the contained instructions, notes and warnings as well as the technical data in the currently valid product specification of your device.

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

Regularly check the website www.dallmeier.com for the latest product documentation updates (and camera firmware versions).

1.4.1 This Document

This document contains detailed information on how to configure the web-based graphical user interface of the devices listed above. The target audience of this document is trained video security system integrators.

1.4.2 Other Applicable Documents

- **Product Specification**
  The product specification contains detailed technical data, features and characteristics of the respective device. The target audience of the document is trained video security systems integrators.

- **Commissioning**
  The “Commissioning” document contains detailed information on the installation, connection and commissioning of the respective device as well as on its intended use, safety instructions and general notes. The target audience of the document is trained video security system integrators.
1.5 TYPOGRAPHICAL CONVENTIONS

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

**NOTICE**

*NOTICE* indicates measures to prevent device and/or property damage due to improper configuration of the device or faulty operations.

Instructions are indicated by arrows (▶).

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

**Expressions** highlighted in bold and dark gray usually refer to the name of an application, product or function or indicate a user interface control element (button, check box, drop-down list, menu item, etc.).

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

The device is configured with a web browser on a desktop PC or laptop over the local area network (LAN).

Alternatively, the device can be connected directly to your desktop PC or laptop via an Ethernet crossover cable. However, if you intend to operate the device with Power over Ethernet, in this case, a single-port PoE injector is additionally required.

2.1 SYSTEM REQUIREMENTS

The configuration of the device has no special requirements to the used computer and can be carried out with any modern desktop PC or laptop regardless of the installed operating system or web browser. You do not need to download and install any plug-ins to successfully configure the camera firmware via the web-based graphical user interface.

<table>
<thead>
<tr>
<th>SYSTEM REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system (OS)</strong></td>
</tr>
<tr>
<td>• Linux*1</td>
</tr>
<tr>
<td>• Mac<em>1 OS X</em>1</td>
</tr>
<tr>
<td>• Microsoft<em>1 Windows</em>1 7/8.1/10</td>
</tr>
<tr>
<td><strong>Graphics card</strong></td>
</tr>
<tr>
<td><strong>Web browser</strong></td>
</tr>
<tr>
<td>• Apple<em>1 Safari</em>1</td>
</tr>
<tr>
<td>• Google<em>1 Chrome</em>1</td>
</tr>
<tr>
<td>• Microsoft Internet Explorer*1 11 (Windows 7/8.1)</td>
</tr>
<tr>
<td>• Microsoft Edge*1 (Windows 10)</td>
</tr>
<tr>
<td>• Mozilla<em>1 Firefox</em>1</td>
</tr>
<tr>
<td>• Opera*1</td>
</tr>
<tr>
<td><strong>Browser settings</strong></td>
</tr>
<tr>
<td><strong>Ethernet</strong></td>
</tr>
<tr>
<td><strong>Sound</strong></td>
</tr>
<tr>
<td><strong>Software/plug-ins</strong></td>
</tr>
</tbody>
</table>

Table 2-1
2.2 CONNECTION

DEFAULT IP ADDRESS

The factory default IP address of the device is:

192.168.2.28

To establish a connection to a device using a web browser, proceed as follows:

▶ Ensure that your computer and web browser can establish an Ethernet connection to the device (if necessary, contact your network administrator for more information and assistance).
▶ 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 then established.

After a successful connection to the device, the login dialog of the camera’s web-based graphical user interface is displayed.

![Login Dialog](image)

Fig. 2-1

The language of the web-based graphical user interface can be switched in the top-left corner of the screen without prior login.
2.3 LOGIN

DEFAULT LOGIN CREDENTIALS

The factory default login credentials for full administrator access to the device are:

User name: admin
Password: 3

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

Fig. 2-2

To log in to the device, proceed as follows:

▶ Enter the login credentials (User name and Password) of your user account into the login form.
▶ Confirm with OK.

You can use the Force login option to log in even if another user (with a lower privilege/permission level) is already logged in.

NOTICE

Risk of unauthorized access to the device and intentional misuse of the system
▶ Change the factory default login credentials of the administrator account as soon as possible.
After a successful login, the graphical user interface of the configuration mode is displayed.

![Diagram of the configuration mode interface]

**Fig. 2-3**

- Switch language
- Hide/show title bar
- Switch between live and configuration mode
- IP address of the current device and user name
- Logout of the device
- Configuration menu
- Current configuration dialog
3.1 SECURITY

The Security tab enables a quick check of all security-related system states. This allows potential security issues and critical vulnerabilities caused by incorrect or unwise device configuration to be easily identified and addressed.

In order to identify the required security measures with regard to cyber and IT security as early as possible, the system security overview page is usually displayed immediately after each login.

> In the event of a device status error, the corresponding error is always displayed first on the device after logging on until it has been cleared – for example, if the registered time server cannot be reached for a longer period of time.

3.2 DATA PROTECTION

The Data protection tab provides quick access to all relevant menus concerning privacy and user rights.

▶ Click the pencil button next to the corresponding option to enter the respective menu.
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.

> The factory settings can be restored under **Service > System state**.

### 4.1 PRESETS

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

**Pre-defined presets**

Using factory-predefined exposure settings and image processing algorithms stored into so called presets, the camera can be very easily adapted to 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 (Day) - for indoor scenes with high contrast
- Indoor (Day/Night) - for indoor scenes with medium contrast
- Low-light (Day/Night) - for scenes with poor illumination
- Outdoor (Day/Night) - for outdoor scenes with high contrast
- Universal (Day/Night) - suitable for most scenes
- SEDOR Day (Day/Night) - special preset for the SEDOR® video analysis software during the day
- SEDOR Night (Day/Night) - special preset for the SEDOR® video analysis software during the night
- Low-light ICR on (Day/Night) - for scenes with poor illumination, infrared cut filter always engaged

**Creating user-defined presets**

Changes to presets are initially only saved temporary in the preview image. To apply the changes permanently, they have to be saved explicitly as user-defined presets. These 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 rights required).
Select a predefined preset from the **Preview preset** drop-down list as the starting point for manually fine-tuning subsequent settings.

Make the necessary settings in the **Image optimization**, **Exposure settings**, and **Day/Night** tabs (see below).

The **Save preset** option becomes available after a parameter has been changed.

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

The **Save preset** dialog is displayed.

Enter a name for the preset.

Confirm with **Save**.

*The settings of the seven 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 preview, optimized and saved again.

**Deleting user-defined presets**

### NOTICE

**Immediate execution**

The selected action is executed without prior confirmation.

To delete presets, proceed as follows:

1. Click the pen-button next to **Delete preset**.
2. Select the required preset and click the corresponding X-button (red).

The preset is then deleted.

**Preset automatic**

The Auto Preset function switches the active preset for image capture when the camera switches between day and night mode.

*If presets tailored to the respective lighting conditions are combined with day/night switching, image capture always takes place with the optimal (selected) 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 tuning and then saved as a user-defined preset.
4.2  IMAGE OPTIMIZATION

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

![Image Optimization Tab](image)

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

> **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.

> **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 determines the color intensity and brilliance of colors and thus their perceived intensity.

> **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.

- **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 (<=) or green (=>) 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 and 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](image)

**Gray World**
This setting is a special preset, optimizing the white balance for the special lighting conditions found in casinos.

**One Push**
This option returns a fixed measurement value which is only recalculated when triggered by user request (Save WB button).
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 Automatic white balance mode.

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 ±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. In these areas more details become visible, they are perceived as "lightened".

![Image Sensor Captures Much More Detail In Dark Areas Than The Human Eye Can Normally See](image)

User-defined

This function is particularly suitable for high-contrast scenes with constant lighting in night mode. In this case the user-defined fine adjustment of the tonal values can be very advantageous.

![User-Defined Tone Mapping](image)

In changing lighting conditions a fixed tone value is usually unfit. For example, by overemphasis of contrasts unsightly comic and halo effects may occur.
Automatic
In day mode with changing lighting, the function should be set to **Automatic**. In this case, a control loop permanently adjusts the strength of the tonal value.

### 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 noticeable image enhancement in fog, this function is often called 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 grayscales, a much clearer picture is achieved in cloudy scenes.

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

> **Automatic day/night switching of presets can be used 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. In that way, 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 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.

![Image showing filter settings](image)

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

The noise filter can be switched off by setting the value to 0. This should be avoided if possible, because barely perceptible micro noise (high-frequency, small-scale noise) is filtered too, reducing 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**

Exposure control can be used to control the camera’s automatic exposure metering.

![Exposure Settings](image)

- 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 limit** option uses a slider to set the value in dB with which the automatic exposure control may amplify the signal at the sensor. 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 a setting 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, the P-Iris (Precise Iris) attains a significantly improved image quality with excellent contrast, brilliant clarity and increased detail resolution with 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**

First of all the P-Iris lens, in conjunction with the camera firmware, 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:

![Image](image.png)

**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 internally 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 (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 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.
**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. The setting 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 & DF5210HD-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 with the chosen **Total power**.
- Always off: The IR illumination is always deactivated.

![Fig. 4-15](image)

**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 %.
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**.

ℹ️ To minimize long delays (response times) during lens control, reduce the encoding bit rate.
4.6 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 supported number of private zones depends on the camera model and can be found in the corresponding specification. The total area of all private zones can be up to 100% of the total image.

▶ Click **Image > Privacy zones**.

![Image with privacy zones](image)

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 can be changed as needed.

The text will be hard coded 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.
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.

![Video dialog](image)

> Note that certain functions and features are only available if supported by the hardware.
5.1 Encoder

This tab offers basic options that are valid for all streams (encoders).

**Sensor Settings**

**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.

![Sensor settings](image)

*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 **Digital Image Shift (Sensor shift)** function.

*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.

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 DECODER

Audio out
Received audio data (G.711 μ-law or G.711 A-law) can be decoded by the camera in real-time and output as analog audio signals via 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 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
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.

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

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

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

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

> 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 many 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 many changes in the image increased.

> The Bitrate slider is extended in this case and allows for the setting of a lower limit. This 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 a lot of changes in the image, the frame rate is adjusted instead 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 to 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 to previous 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.

The smaller the GOP size (i.e. more I-Frames, less P-Frames):

- the less effective is the compression
- the higher is the image quality
- the less the CPU is utilized
- the higher is the required RAM and memory space
- the smoother is the playback during fast-forward and backward.

The larger the GOP size (i.e. less I frames, more P-Frames)

- the more effective is the compression
- the lower is the image quality
- the more the CPU is utilized
- the smaller is the required RAM and memory space
- the more choppy is the playback during fast-forward and backward.

> In general, a GOP size between 6 and 15 provides a good image quality with a sufficiently high compression level.
Later on, the individual GOP sequences are used to generate the visible single frames (reconstruct the original compressed image data) at the decoder.

> **Note**
> 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 cameras 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.

> **Note**
> Detailed information about the available resolutions can be found in the data sheet of the respective camera.
**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](image)

- 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 Network > Time server tab is displayed.

![Fig. 6-2](image)

- 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.
7.1 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**.
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 Apply basic setting to save the settings.

The button Apply basic settings is only active when all necessary data have been entered.

IP-Settings

Enable DHCP
Refer to “Automatic Network Setup using DHCP” on page 43.

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 using 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** allows you to adjust several settings concerning the network protocol and to 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, leads to more 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.

**Automatic Network Setup using 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.

ℹ️ To ignore data sent by 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 42.
▶ 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).

ℹ️ 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.

-Manual Network Setup
▶ First, observe the designated and valid IP address ranges in your network.

ℹ️ 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 42.
▶ Confirm with OK.

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

ℹ️ After changing the network settings, you have to re-establish 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.

▸ Click Network > Bandwidth limit.

![Network Settings](image)

▸ Click the **Enabled** check box to activate the bandwidth limit function.
▸ Note the following options.

**Manual setting**
▸ Set the peak bandwidth limit with the corresponding slider.
▸ Confirm with **OK**.

**Automatic setting**
With the **Automatic limit** checkbox enabled, the camera automatically selects the maximum permissible peak bit rate, taking into account the highest bit rate selected, so that a smooth live transmission is maintained.

▸ Activate the **Automatic limit** checkbox.
▸ Confirm with **OK**.
7.3 STREAMING

The (static) video server provides for a continuous transmission (streaming) of the generated video data into the network without the data being actively requested by an application.

▶ Click Network > Streaming.

Fig. 7-3

<table>
<thead>
<tr>
<th>Static streaming server</th>
</tr>
</thead>
</table>
▶ 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 hosts and the local routers/switches in your network support IP multicasting and are correctly configured.
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). This can further reduce the network load, as multicast datagrams are only forwarded to those recipients who wish to receive them.

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.

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.

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 only receives 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**.

![Network settings](image)

*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 **Apply time server settings**.

*The **Apply time server settings** button becomes active only after all necessary data have been entered.*

The synchronization with the specified NTP time server is now activated.
7.5 QUALITY OF SERVICE

The Quality of Service function flags the data packets of the video stream with a special DSCP code. During transmission over the network, the switches detect these data packets and assign the highest priority to their transmission. In the event of load peaks, a switch reduces the bandwidth for other data packets (e-mail, VoIP, FTP, etc.) and automatically increases the bandwidth for the video stream. This avoids a data jam and all data packets reach the client for smooth display of the video stream almost in real time.

Note that the preferred transmission of video streams can seriously disrupt other services (e-mail, VoIP, FTP, etc.). The use of Quality of Service should always be discussed with the network administrator.

UDP video and audio QoS DSCP setup
The DSCP code identifies the data type and forwarding behavior of the switch. A higher DSCP code therefore does not mean a higher priority but identifies a different data type with a different forwarding behavior. In conjunction with Cisco Catalyst switches, for example, DSCP code 32 must always be used for video streams.

▶ Click Network > QoS.

▶ Enter the correct UDP video and audio QoS DSCP code (see above).
7.6 **SNMP**

The Simple Network Management Protocol (SNMP) is a network protocol for monitoring and controlling network elements using a Network Management System (NMS). The protocol is currently supported in three different versions.

- Click **Network > SNMP**.

![Network settings](image)

- Make the necessary settings (see below).
- Confirm with **Save SNMP configuration**.

*The Save SNMP configuration button becomes active only after all necessary data have been entered.*

*The selected SNMP version has to match the setting of the used Network Management System (NMS)*

**SNMP v1/v2**

SNMP versions 1 and 2 are common, but do not provide sufficient security and should not be used if possible.

*Note that community strings (which serve as a kind of password) are transmitted in plain text with SNMP v1/v2c and can be “overheard” by anyone in the network.*
Activate the checkbox of the required SNMP version.
Enter the name of the Community you want to use in the appropriate field.

### SNMP v3
SNMP version 3 provides user accounts and password prompting as a security measure.

- Click the Enable SNMP v3 checkbox.
- Enter the user to be used in the appropriate field.
- Select the required authentication from the drop-down list (see below).
- Select the required encryption from the drop-down list (see below).

**Authentication**
Three different modes are available:

- OFF — No authentication is necessary
- MD5 — Message-Digest Algorithm 5
- SHA — Secure Hash Algorithm

**Encryption**
There are three options to choose from:

- OFF — The communication is not encrypted
- DES — Data Encryption Standard
- AES — Advanced Encryption Standard

### Common settings
This section contains information and settings that are valid for all three versions. The Contact and Location fields are intended for the corresponding information.

- Click Save SNMP configuration to save the settings.

> Note that the Save SNMP configuration button will be inactive unless all necessary settings have been made.

### Use INFORM instead of TRAPS
If it is necessary for the addressee of the SNMP message to send a response about its receipt, you can switch from TRAP to INFORM.

- If necessary, activate the Use INFORM instead of TRAPS checkbox.

### MIB
The MiB file can be downloaded for information on possible queries.

- Click Download to download the MiB file, if necessary.
7.7 NETWORK SERVICES

<table>
<thead>
<tr>
<th>Default factory settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONVIF: deactivated</td>
</tr>
<tr>
<td>RTSP: deactivated</td>
</tr>
</tbody>
</table>

▶ Click Network > Network services.

Fig. 7-7

▶ Note the following instructions.
▶ Select the relevant check boxes.
▶ Enter the required port if necessary.

Network services become active immediately.

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. To determine the appropriate transmission protocol for the RTP data transfer (UDP or TCP) and 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 via UDP (User Datagram Protocol). However while RTSP transmissions are realized over a TCP connection (TCP = Transmission Control Protocol).

**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.

**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 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. Normally, only the RTSP port on the Internet router or firewall must be open for data transmissions of RTP/RTSP/TCP packets from the Internet to your Local Area Network (LAN).

RTSP allows the transmission of RTP streams to be embedded into the existing RTSP/TCP connection; no separate UDP transmission or an additional port for the RTP data stream is 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 to be able to access the RTSP server of each camera from the WAN (may not be required if the NAT router supports port redirection).

Information regarding URL requests for the corresponding stream types can be found under “RTSP Application” on page 100.
HTTP/HTTPS

In addition to HTTP, the HTTPS (HyperText Transfer Protocol Secure) communication protocol is supported 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).

Only TLS 1.2 is supported with the current version for the encryption of data packets:

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

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.

DaVid/DaVidTLS

It is possible to use and encrypt the DaVid protocol. For the encryption, a certificate path must first be created in the keystore (see "Keystore" on page 56).

▶ Activate the David activated checkbox, if necessary.
▶ Select the certificate path for the encryption from the drop-down list.
▶ Activate the David-tLS checkbox, if necessary.

DaVid alarm host (PGuard)

The behaviour of the system concerning TLS encryption when sending event triggered messages to an alarm hose using the DaVid protocol can be regulated using the drop down menu.

▶ Select the necessary TLS Mode from the drop down list.

PService

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

DaVid/RTSP

▶ To enforce the encryption of credentials that are sent using the DaVid protocol (Dallmeier Video Protocol) activate the Force encrypted credentials checkbox.

Note that this setting does not encrypt the login credentials when you log on to the WebConfig user interface of the device using a web browser.
7.8 802.1X

802.1X is a standard that governs access control in networks. Authentication via 802.1X includes three elements: a supplicant (here: the camera) who wants to access the network, an authenticator who manages the access data (e.g. an Ethernet switch or a WLAN access point) and an authentication server. The authenticator provides the server with the supplicant’s credentials for verification, and prevents access to the network until the supplicant’s identity is verified and access is granted.

▶ Click Network > 802.1X.

![Image of network settings with 802.1X configuration options]

Fig. 7-8

**EAP-TLS**

▶ Click the Enable 802.1X check box.
▶ Select the necessary options using the drop-down lists (see below).
▶ Enter an Identity in the corresponding field.
▶ Confirm with Apply 802.1X settings.

*The button Apply 802.1x settings is only active when all necessary data have been entered.*

**Client Certificate**

An overview of the lists of client certificates created in the keystore is displayed here (see “Keystore” on page 56).

**CA-Certifikate**

A list of the CA certificates created in the keystore is displayed here (see “Keystore” on page 56).

**EAPOL**

The Extensive Authentication Protocol is the protocol used by the supplicant and authenticator to transmit authentication information.

*The selected EAPOL version must match that of the IEEE 802.1X-compatible router or switch (authenticator) used on your network.*
7.9 KEystore

The Keystore tab is used to display and manage network certificates.

▶ Click Network > Keystore.

Fig. 7-9

7.9.1 General Functions

The following functions behave the same for all available options:

Info
▶ Click the required entry in the list.
▶ Click the Info button to open the dialog with additional information about the selected entry.

Delete Element

Note that the action is performed immediately and no confirmation prompt appears.

▶ Click the required item in the list.
▶ Click the Delete item button to remove the corresponding entry.
Delete all elements

$i$ Note that the action will be executed immediately and there will be no confirmation prompt.

Click the **Delete all elements** button to delete all entries in the respective list.

Delete all unused items

$i$ Note that the action is performed immediately and no confirmation prompt appears.

▶ Click the **Delete all unused items** button to remove all entries in the list that are currently unused.

7.9.2 Managing Certificates and Keys

<table>
<thead>
<tr>
<th>Certification paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Activate the <strong>Show certification paths</strong> check box.</td>
</tr>
</tbody>
</table>

A list of certificate paths with additional information as well as the administration buttons are displayed.

![Certification paths](image)

Fig. 7-10

Create certification path

▶ Click **Create certificate path** to open the corresponding dialog.

![Create certification path](image)

Fig. 7-11

▶ Enter an **Alias**.
▶ Choose the start of the chain from the **Start of path** drop-down list.
▶ Generate the necessary path using the + and - buttons.
Confirm with Create.

The path has now been created and is displayed in the list.

**Client and server certificates**

- Activate the *Show client and server certificates* check box.

A list of the client and server certificates and the administration buttons are displayed.

Fig. 7-12

**Self-signed certificate**

- Click the *Self-signed certificate* button to open the corresponding dialog.

Fig. 7-13

- Activate the *Use existing key* check box, if necessary.
- Enter the necessary data under *Subject*.
- Confirm with Create.

The self-signed certificate has been created and is displayed in the list. It can now be used.
Create Certificate signing request
To create a signing request proceed as follows:

▶ Mark the relevant certificate.
▶ Click Create signing request to open the corresponding dialog.

![Certificate signing request dialog](image)

▶ Enter the necessary data.
▶ Click Create to finish the process.

Import certificate
▶ Click Import certificate to open the import dialog.

![Import certificate dialog](image)

Certificate and key can either be imported in one PKCS12 file or separately from two different files.

▶ Choose the necessary option using the radio buttons.

<i>The corresponding options are only displayed when the relevant radio button is activated.</i>

PKCS12 format:
▶ Click the Browse PKCS12 file button.
▶ Enter the file path using the explorer.
▶ Enter an Alias, if necessary.
▶ Activate the PKCS12 encrypted checkbox, if necessary.
▶ Enter the appropriate Password, if necessary.
▶ Confirm with OK.
Separate import:

➢ Click the **Browse certificate** button.

![Fig. 7-16](image)

➢ Select the correct file path using the explorer.
➢ Click the **Add CA certificate** button.

*The **Browse CA certifikate** button is displayed.*

➢ Click the **Browse CA certifikate** button.
➢ Select the correct file path using the explorer.
➢ Activate the **Add optional private key** check box, if necessary.
➢ Click the **Browse PKCS8 file** button.
➢ Select the correct file path using the explorer.
➢ Activate the **PKCS8 encrypted** check box, if necessary.
➢ Enter the appropriate password, if necessary.
➢ Confirm with **OK**.

*CA certificates*

➢ Activate the **Show CA certificates** check box.

*A list of CA certificates and the buttons for their management are displayed.*

![Fig. 7-17](image)

➢ Click the **Import certificate** button to open the corresponding dialog.

![Fig. 7-18](image)
Click Browse certificate.
Select the correct file path using the explorer.
Enter an Alias, if necessary.
Confirm with OK.

The certificate is now imported and displayed in the list.

Key pairs
Activate the Show key pairs check box.

The list of key pairs and the buttons for their management are displayed.

Create key pair
To create a key pair proceed as follows:

Click Create key pair in order to open the corresponding dialog.

Enter the required data.
Click Create to complete the creation.

The key pair is now created and displayed in the list. It can now be used.
The EdgeStorage function 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 loosing data.

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

▶ Click EdgeStorage to open the corresponding Configuration menu.

▶ Activate the Enable EdgeStorage check box.
▶ Select the relevant EdgeStorage mode (see below).

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

Linear buffer
Recording stops as soon as the RAM is full.
EVENT MANAGEMENT

The event management provides the option to send event triggered notifications to an alarm host using the DaVid protocol.
To evaluate the event messages, a DaVid protocol-capable software (e.g. PGuard advance) must run on the respective alarm host.

➤ Ensure that the device and the alarm host are in the same LAN or can communicate using a gateway.
➤ Click Event management in the configuration menu.

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

➤ Click Event management > Add event handler.

➤ 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.
▶ Enter the IP address of the alarm host to which the DaVid event notification shall be sent to when an event occurs.
▶ Click the **Add trigger** button.

▶ Select the necessary trigger from the drop-down list.
▶ Confirm with **OK**.
The Data display function allows you to embed texts or data from external interfaces 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 image.

**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 DISPLAY

▶ Click Data display > Display.

Fig. 10-1

▶ 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

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

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.

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

▶ Click Data display > Fields.

![Fig. 10-3](image)

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

> 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

If streaming over RTCP is activated in the network settings (see section “Streaming” on page 46) the transmission of data over RTCP has to be activated as well for a successful data display.

▶ Click Data display > RTCP.

Fig. 10-4

▶ Select the Send data over RTCP check box.
VIDEO CONTENT ANALYSIS (VCA)

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)

**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.

11.1 ANALYSIS

▶ Click the Video Content Analysis menu item.

The Analysis tab is displayed.

In the screenshot above, 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 86).

General Settings

► Select the Enabled check box to globally enable the video content analysis on the camera.

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).

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:

![Expert settings](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 the monitored objects as well as on the scene conditions. 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:

<table>
<thead>
<tr>
<th>Scene Condition</th>
<th>Recommended Analysis Input Resolution (Pixels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indoor – medium/large objects</td>
<td>80 × 60</td>
</tr>
<tr>
<td>Indoor – small objects</td>
<td>160 × 120</td>
</tr>
<tr>
<td>Outdoor – medium/large objects</td>
<td>160 × 120</td>
</tr>
<tr>
<td>Outdoor – small objects</td>
<td>320 × 240</td>
</tr>
</tbody>
</table>

Table 11-1

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

<table>
<thead>
<tr>
<th>Video Analysis Application</th>
<th>Recommended Analysis Frame Rate (Frames/Second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General motion detection of objects (video motion detection, VMD) with virtual motion tracking</td>
<td>10 – 20 (min. 8)</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>5 – 15 (min. 5)</td>
</tr>
<tr>
<td>Tamper detection</td>
<td>5 – 15 (min. 5)</td>
</tr>
</tbody>
</table>

Table 11-2

▶ 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 (e.g. due to low signal gain) or with gray or dark objects at night.
- **95**: For situations with very low video contrast (e.g. 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 73). 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.

**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.
**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 to define the minimum required and the maximum valid object dimensions with your mouse.

▶ 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 Abb. 11-5).
▶ 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 size reference when drawing the rectangles.*
Ignore Mask
This 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 1fps) 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.

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 78).
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.

![Draw polygon interface](image)

**Fig. 11-7**

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 78).
Select/edit

- Click the **Select** button.
- Left-click an inactive area.

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

![Image of screen capture showing a selected inactive area with white circles at vertices.](image)

Fig. 11-8

- Move the white circles with the mouse pointer to change the defined inactive area.

  *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.
11.2 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.

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>After selecting the Enable intrusion detection check box, a live preview (with a frame rate of 1fps) as well as various tools are displayed for creating and editing masks that specify active sensitive areas in the image.</td>
</tr>
</tbody>
</table>

- 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.

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 76).

- 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, 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 to restore the default settings.
11.3 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).

Tamper Detection

To use the camera tamper detection, proceed as follows:

▶ Select the Enable tamper detection check box.

![Tamper Detection](image)

▶ 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 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 tamper detection (see above) can also lead to many irrelevant events, such as weather-related camera fluctuations when the camera is mounted outside on a high pole. In this case, adjust the sensitivity setting downwards.
Default settings
Click the Default settings button if you want to restore the default settings.

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.

▶ 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 to restore the default settings.
11.4 CLASSIFICATION

By enabling the functions 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.

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:

![Classification interface](image)

- 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.
**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.

- 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 corresponding button if you want to restore the default settings.
11.5 LINE CROSSING

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:

**Configuration**
- Select the **Enable line crossing detection** check box.

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

- 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.
11.6  OBJECTS & EVENTS

In this 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.

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 73.
**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.

**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 recommended.

**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**

*DALLMEIER*

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.
12.1 USER MANAGEMENT

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]

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.
12.2 GROUP MANAGEMENT

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.

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.
▶ Click the + button (right column) to assign the user to the group.
▶ Click the - button (left column) to remove the user from the group.
12.3 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](image)

- Click the **Pencil** button (left) to edit the rights of a group.
- Click the **+** button (green) to grant a right to the group.
- Click the **-** button (red) to withdraw a right from the group.
12.4 ANONYMOUS ACCESS

Anonymous access regulates how image transmission without prior authentication by the user is handled (see “Image Transmission” on page 99).

▶ Click Anonymous access.

Fig. 12-5

▶ Select the necessary check box.
13.1 CONFIGURATION FILE

The configuration of the device can be exported and saved.

▶ Click Service > Configuration file.

![Image of configuration file settings]

**Export**

▶ 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.
Import

Configuration files can also be imported.

▶ Click the Select file button.
▶ Use the file manager to select the required configuration file.
▶ Confirm with OK.

The configuration file is now imported and the required settings are made.

13.2 SYSTEM STATE

Factory Settings

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

NOTICE

Immediate execution

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

Click Service > System state.

▶ Click the required button.

Reboot

▶ Click the Reboot button for restarting the system.
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.

▶ Save the .dat file to the required location.

ℹ️ The Password query is used to read out special information by the Dallmeier development team and is not required to download the support information.
14.1 GENERAL INFORMATION

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

Click Information > General information.

Fig. 14-1

The following information is displayed:

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

14.2 DEVICE STATUS

The Device status tab displays further information concerning the functionality of the recorder.

Fig. 14-2
14.3 NETWORK CONNECTIONS

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

Fig. 14-3

Also note the information in the Third-party information tab.
15.1 SINGLE IMAGE (JPEG)

Current video data can be displayed as a single image (JPEG) with 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 92).

or

- the Allow JPEG access without credentials check box has to be selected (see section “Anonymous Access” on page 93)

Use the following URL requests for the various encoders:

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

The displayed single image (JPEG) can be refreshed manually 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 52.

<table>
<thead>
<tr>
<th>Transport protocol</th>
<th>TCP/UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission protocol</td>
<td>RTP</td>
</tr>
<tr>
<td>Control protocol</td>
<td>RTSP</td>
</tr>
<tr>
<td>Port</td>
<td>554 (default setting)</td>
</tr>
</tbody>
</table>

RTSP and RTP over HTTP tunneling
<table>
<thead>
<tr>
<th>Transmission protocol</th>
<th>HTTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>80</td>
</tr>
</tbody>
</table>

Note that

- the requested encoder must be activated.
- the RTSP server in the camera must be activated (see section “Network Services” on page 52).
- the “RTSP live access” right/permission must be activated (see section “Rights” on page 92).

or

- the “Allow RTSP access without credentials” check box has to be selected (see “Anonymous Access” on page 93).

Use the following URL requests for the various encoders:

Encoder 1  rtsp://IP address of the device/encoder1
Encoder 2  rtsp://IP address of the device/encoder2
Encoder 3  rtsp://IP address of the device/encoder3
Encoder 4  rtsp://IP address of the device/encoder4

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

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

In this case add a ":" (colon) followed by the new port number after the IP address.

Example for Encoder 1 with new RTSP port number 1024:

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