Dallmeier

Doc. Rev.: 0.3.4 | 2023-04-26

CONFIGURATION

CAMERA WEB INTERFACE

DOMERA® OS

RELEASE VERSION: 14.0.3.9

MADE IN GERMANY

See more.

CONTENTS

INTRODUCTION

1.1 VALIDITY

This document is valid for Domera® OS in conjunction with the following Dallmeier cameras:

Dome Cameras	Fisheye Camera	Panomera® (MK2 Models)
• RDF6800DN • RDF6400DN • RDF5140DN + Version E • RDF5120DN + Version E	• SDF6800DN	• Panomera® S4/S8 (MK2) • Panomera® W4/W8 (MK2)

Table 1-1

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.

The descriptions in this document are based on Domera® OS release version 14.0.3.9.

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

1.2 COMPATIBILITY

The release version 14.0.3.9 of Domera® OS is compatible with the following Dallmeier hardware and software:

- Recording systems of generation 5 with **SMAVIA Recording Server** software as of version 8.x.12* (limitations: no support for recording of H.265 encoded media and no support for establishing a secure connection and data transmission with TLS encryption)
- Recording systems of generation 6 with **SMAVIA Recording Server** software as of version 9.x.12*
- Recording systems with **SeMSy® Recording Server** software as of version 10.x.3*
- **HEMISPHERE® SeMSy®** video and alarm management system as of version 5.4.21
- **SeMSy® Compact** video management software as of version 5.3.42 for small and medium businesses
- **SeMSy® Viewer** as of software version 5.3.42 for playback and evaluation of backups
- **Dallmeier Device Manager** as of software version 1.0.22 for network discovery and secure management of Dallmeier VideoIP systems (cameras, recording systems, etc.)
- **PGuard advance** as of software version 4.7.2 for the evaluation and management of status, event and error messages of Dallmeier devices

* each with latest service pack installed

Dallmeier cameras with Domera® OS can also be integrated into ONVIF*) compliant third-party video management systems that support the ONVIF Profile M, ONVIF Profile S and ONVIF Profile T functions as well as the Real-Time Streaming Protocol (RTSP).

*) Note the information on the trademark owner given in the copyright and trademark notice on page 2.

1.3 DOCUMENTS

The product documentation for the respective device consists of various documents that are published in printed and/or digital form, for example on the Dallmeier website at https://www.dallmeier.com/.

Read the complete product documentation for your device carefully and thoroughly before using the 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 printed documents relating to your device in a legible condition and in a suitable location for future reference. Save digital documents relating to your device (e.g. the technical product specification) on a suitable data storage device.

Regularly check the Dallmeier website at https://www.dallmeier.com/ for possible updates to the product documentation as well as for the latest release version of Domera® OS (especially with regard to security updates or patches).

1.3.1 This Document

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

1.3.2 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 proper assembly, installation, cabling and commissioning of the respective device as well as on its intended use. In addition, it provides safety instructions and hazard warnings, general technical notes, and maintenance, inspection and cleaning instructions.
The target audience of the document is trained video security systems integrators.

Technical Information
“Technical Information” documents for Domera® OS provide release-specific information on recent changes (security updates or patches, functional improvements and new features) that are implemented with the latest release version.
The target audience of these documents is trained video security systems integrators.

1.4 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, checkbox, drop-down list, menu item, etc.).

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

1.5 DISCLAIMER

This document describes the full range of functions of Domera® OS.

However, note that

- certain functions and setting options are only available if supported by the used hardware (e.g. configuring an integrated IR illumination).
- the range of functions of your device depends on the ordered equipment or device variant and may differ from the contents of this document.
- certain functions and setting options may require purchasing a license.

1.6 LEGAL NOTICES

Observe the legal notices listed below concerning the product described in this document and/or its underlying software:

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This software is based in part on the work of the Independent JPEG Group.

In this context, also read and observe the license texts provided in the information dialog of your device about any other third-party software components used on your device.

CONNECTION & LOGIN

The camera is configured using a common web browser on a stationary or mobile computer (desktop PC or notebook) via the local area network (LAN).

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

2.1 SYSTEM REQUIREMENTS

The configuration of the camera does not require any special hardware or software on the used client PC. It can be performed with any modern desktop PC or notebook.
With regard to camera configuration, the web-based graphical user interface (GUI) and the integrated functions of Domera® OS are independent of the operating system and type of web browser.
The download and installation of browser extensions or plug-ins is not required.

SYSTEM REQUIREMENTS	
Operating system (OS)	Any modern operating system in its latest version, such as: • Linux*) • macOS*) • Microsoft*) Windows*) 10 or Windows 11
Web browser	Any modern desktop browser in its latest version, such as: • Apple*) Safari*) • Google*) Chrome*) • Microsoft Edge*) • Mozilla*) Firefox*)
Browser settings	JavaScript*) enabled
Browser extensions/plug-ins	Not required
Ethernet	100 Mbps (or more)
Graphics card	Any (with modern technology)
Sound	Sound card or on-board sound chip (min. 16 bit)

Table 2-1

*) Note the information on the trademark owner given in the copyright and trademark notice on page 2.

For best and efficient usability of the web-based graphical user interface, a computer mouse is recommended that is equipped with a left mouse button (or primary mouse button), a right mouse button (or secondary mouse button) and a mouse wheel.
For better readability, the descriptions in this document regarding the use of a computer mouse refer only to right-handed individuals (primary mouse button on the left).

2.2 ESTABLISHING THE CONNECTION

DEFAULT IP ADDRESS

The factory default IP address of a Dallmeier single-sensor camera is:

192.168.2.28

*You can change the IP address, subnet mask and gateway addressing of the device using the client software **Dallmeier Device Manager**.*

To establish a connection to your 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 your Dallmeier device into the address bar of the web browser.
- Confirm the input.

The connection to the device is then established.

After the successful connection to the device and before the very first login, a system security dialog for the first-time access is displayed (see below).

2.3 FIRST-TIME ACCESS

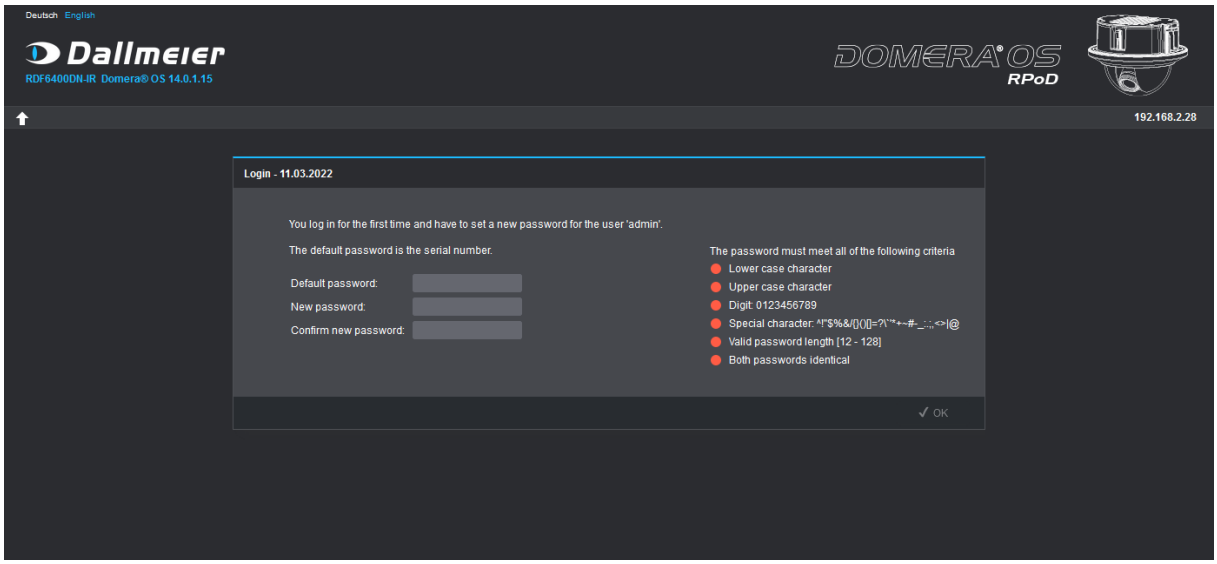

Fig. 2-1: “First-time access” dialog

> *The language of the web-based graphical user interface can be changed in the top-left corner of the screen without the need to be logged in first.*

Before you can log in to the device via a web browser for the first time, you have to enter the default password that is specifically valid for your device and then assign a new password for the factory default system administration account (user name: `admin`).

The default password is the complete serial number of the device (e.g. DHD001-23456789).
The serial number is printed on the type plate of the device and can also be determined using the client software **Dallmeier Device Manager**.

- ► Enter the **Default password** (complete serial number of the device incl. hyphen).
- ► Enter a new password for the default system administration account (observe the password criteria) and confirm your input (the strength of the selected password is displayed during input).
- ► Click **OK**.

NOTICE

Login error due to incorrect login credentials or risk of unauthorized access to the device and intentional misuse of the system

- ► Write down all relevant login credentials (user names and passwords) associated with your device and store them in a safe place.
- ► Always protect user account information from unauthorized access by others.

After the first successful access to the device, the login dialog is displayed (see below).

2.4 LOGIN

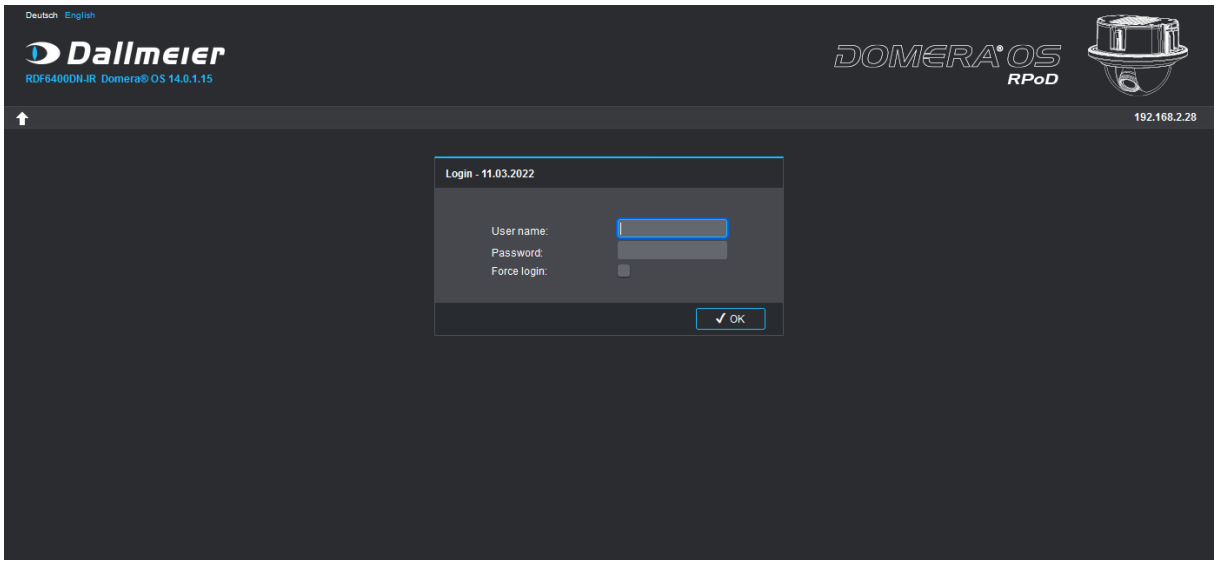

Fig. 2-2: Login dialog

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

The web-based graphical user interface (Domera® OS GUI) of the configuration and live mode is displayed for authenticated and authorized users only.

DEFAULT LOGIN CREDENTIALS
The user name of the factory default system administration account is: `admin`

To log in to the device, proceed as follows:

- Enter your login credentials into the **User name** and **Password** fields.
- Click **OK**.

After a successful login to the device, the user interface of the configuration mode is displayed (see below).

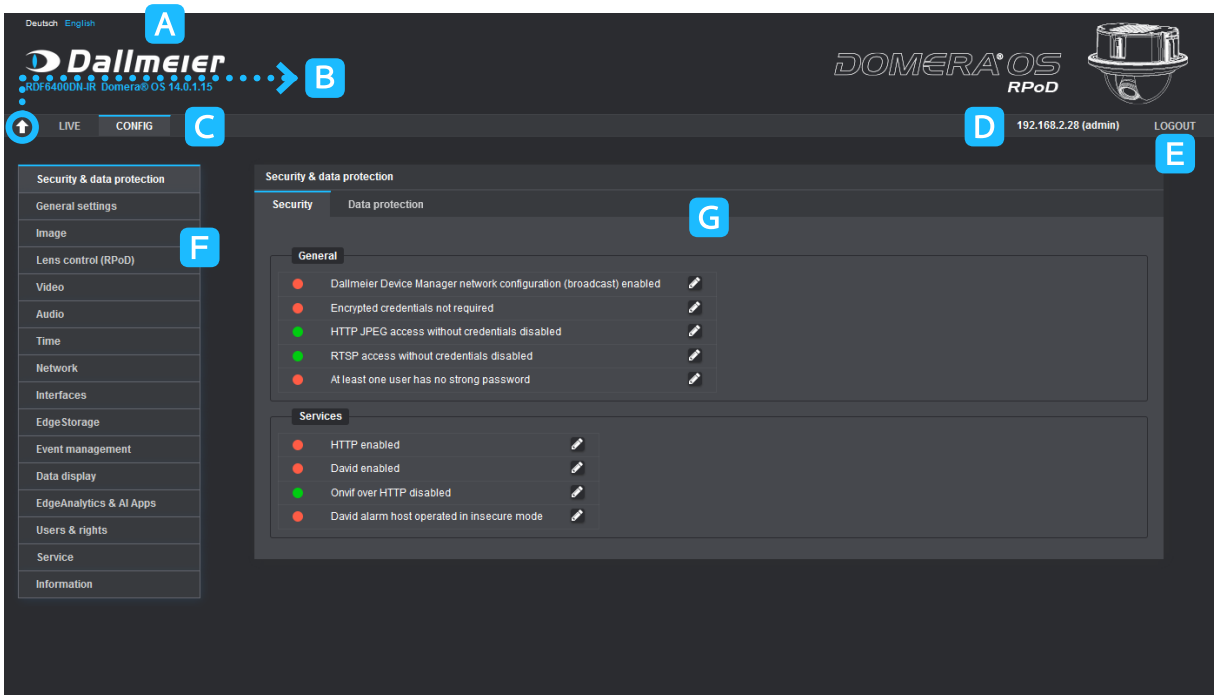

Fig. 2-3: Configuration mode

A Change language
B Hide/show title bar
C Toggle between configuration and live mode
D IP address of the device and user name of the currently logged in user
E Logout of the device
F Navigation menu
G Main content area for configuration dialogs

- ► Configure all required settings (see the following chapters).
- ► Finally, click **LOGOUT** to properly log out of the device.

For reasons of system security, you will be automatically logged out of the device after 5 minutes without user action.

SECURITY & DATA PROTECTION

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.*

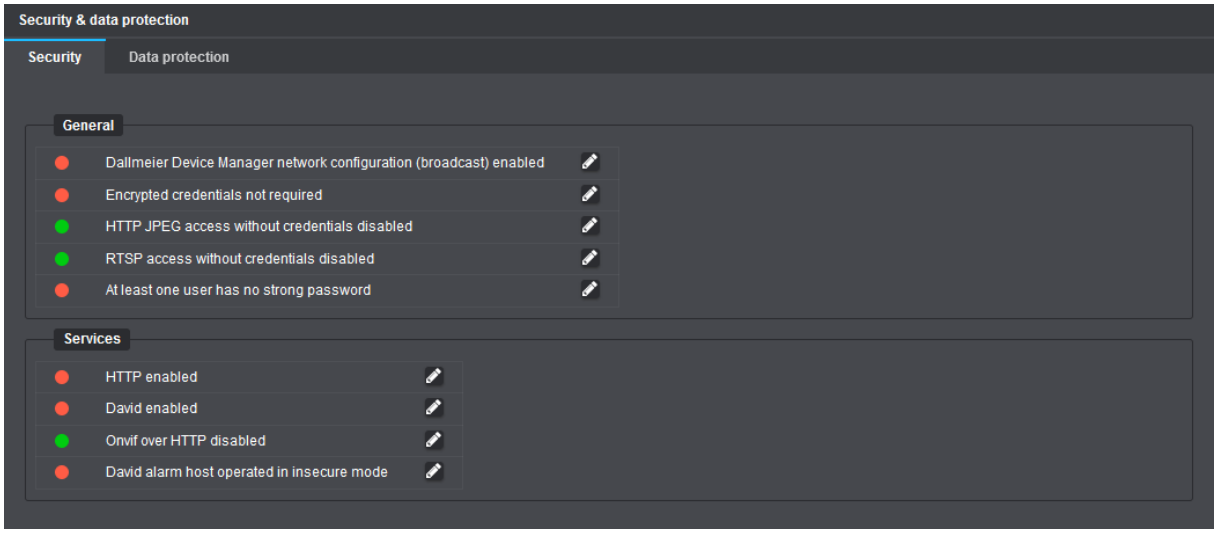

Fig. 3-1

3.2 DATA PROTECTION

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

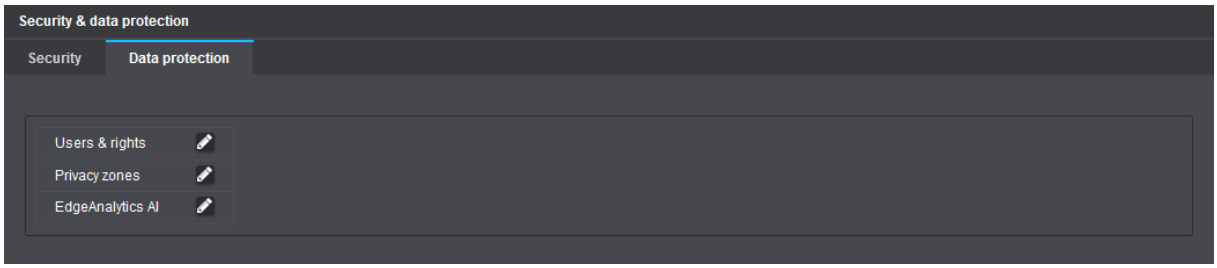

Fig. 3-2

- Click the **Pencil** icon button next to an element to open the corresponding configuration dialog.

GENERAL SETTINGS (LANGUAGE)

The web-based graphical user interface can be displayed in various languages.

To change the language, proceed as follows:

► Click the **General settings** menu item in the navigation menu.

The **User interface** tab is displayed.

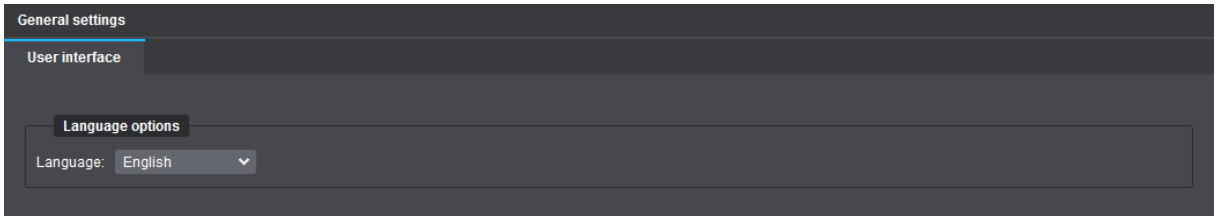

Fig. 4-1

► Select the preferred language option from the **Language** drop-down list.

The user interface is then automatically changed to the selected language.

IMAGE

In the **Image** dialog, the camera's exposure settings can be configured and the image processing algorithms can be adapted to the captured scene and the lighting conditions prevailing at the installation site. In addition, the automatic day/night mode can be customized for optimal exposure both during the day and at night.
Finally, privacy protection zones (hidden/masked image areas of the captured scene) and/or embedded text overlays in the video (e.g. current date and time or custom text elements) can be set up if required.

- ▶ Click the **Image** menu item in the navigation menu to open the corresponding dialog.
- ▶ Note the following explanations concerning the various tabs and settings.

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

5.1 PRESETS

By default, the **Presets** tab already provides a variety of automatic exposure (AE) presets that are suitable for different types of scenes and lighting conditions:

- **Casino (Day)** – special preset for indoor casino scenes with high contrast
- **Indoor (Day/Night)** – for indoor scenes with normal to medium contrast
- **Indoor HDR (Day/Night)** – for indoor scenes with high contrast
- **Low-light ICR on (Day/Night)** – for scenes with poor lighting (the built-in IR cut filter remains engaged even in night mode; only recommended for very special applications)
- **Low-light (Day/Night)** – for scenes with poor lighting
- **Outdoor (Day/Night)** – for outdoor scenes with normal to medium contrast
- **Outdoor HDR (Day/Night)** – for outdoor scenes with high contrast
- **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
- **Universal (Day/Night)** – basic preset for most scenes with normal to medium contrast
- **Universal HDR (Day/Night)** – basic preset for most scenes with high contrast

Predefined Presets
Using factory predefined exposure settings that are stored in presets, the camera can be very easily adapted to most lighting conditions to always maintain the best possible image quality.
In addition, these presets serve as useful starting points for manually adjusting various exposure settings and image optimization parameters, such as exposure time, aperture (f-stop) or white balance.

User-defined Presets
Any changes made to presets (e.g. brightness, saturation, hue or contrast) are initially only temporarily effective (applied to the preview image). If the changes made are to apply permanently, they have to be explicitly saved as a new user-defined preset.
User-defined presets can then be selected, for example, for the **Preset automatic** feature or used again as a starting point for further adjustments to the exposure settings and image optimization parameters (re-saving or overwriting required).

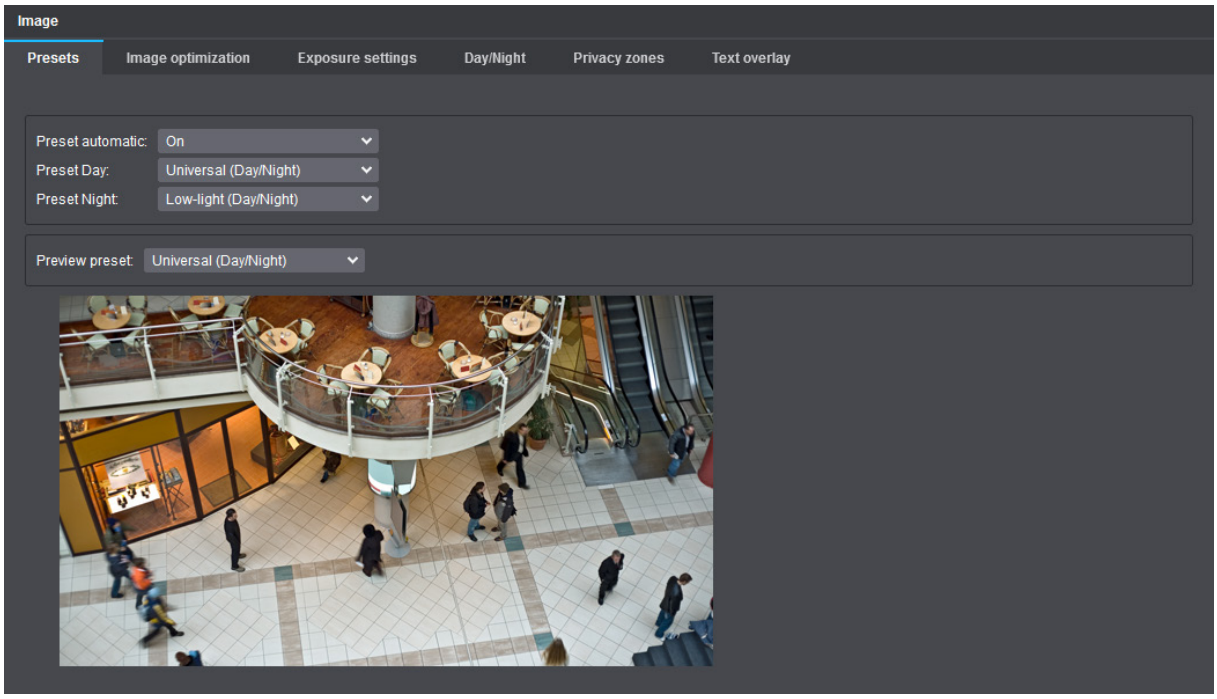

Fig. 5-1

- From the **Preview preset** drop-down list, select a factory predefined preset as a starting point for the manual adjustment of the available exposure settings and image optimization parameters.
- Adjust the required settings in the **Image optimization**, **Exposure settings** and **Day/Night** tabs (see descriptions in the following sections).

The option **Save preset** is automatically available after changing a parameter of a factory predefined preset.

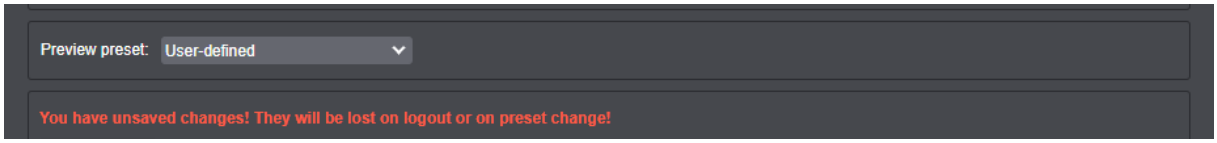

Fig. 5-2

- Click **Save Preset** after you have made all the necessary changes in order to create a new user-defined preset.

The settings of a factory predefined preset can not be overwritten.

The **Save preset** dialog is then displayed.

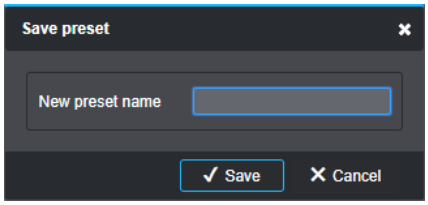

Fig. 5-3

- Enter a unique name for the new user-defined preset.

► Confirm with **Save**.

The new user-defined preset is then saved and can be used, for example, for the **Preset automatic** feature (see below).

The number of user-defined presets that can be created is not limited.

User-defined presets can be selected for the live preview on the various tabs, optimized and saved again.

Deleting User-defined Presets
To delete a user-defined preset, proceed as follows:

► Click the **Pencil** icon button to the left of the **Delete preset** label.

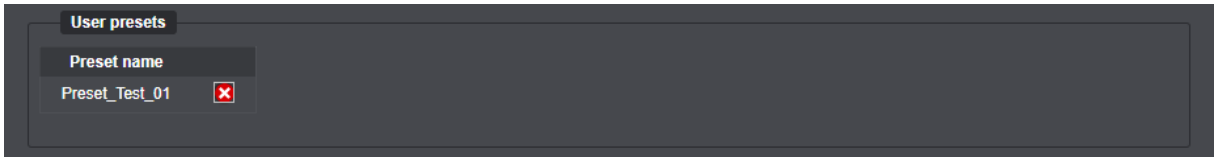

Fig. 5-4

► Click the **Delete** icon button (red circle with a white cross) to the right of a user-defined preset.

The user-defined preset is then deleted.

A factory predefined preset can not be deleted.

Preset Automatic
The **Preset automatic** feature, if enabled, automatically switches from the set day preset (**Preset Day**) to the set night preset (**Preset Night**) whenever the camera switches from day to night mode (or vice versa).

Preview Preset
This setting allows you to select a preset for the live preview on the various tabs.
The parameters of the selected preset can be used as a starting point for manual fine-tuning and then saved as a new user-defined preset.

5.2 IMAGE OPTIMIZATION

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

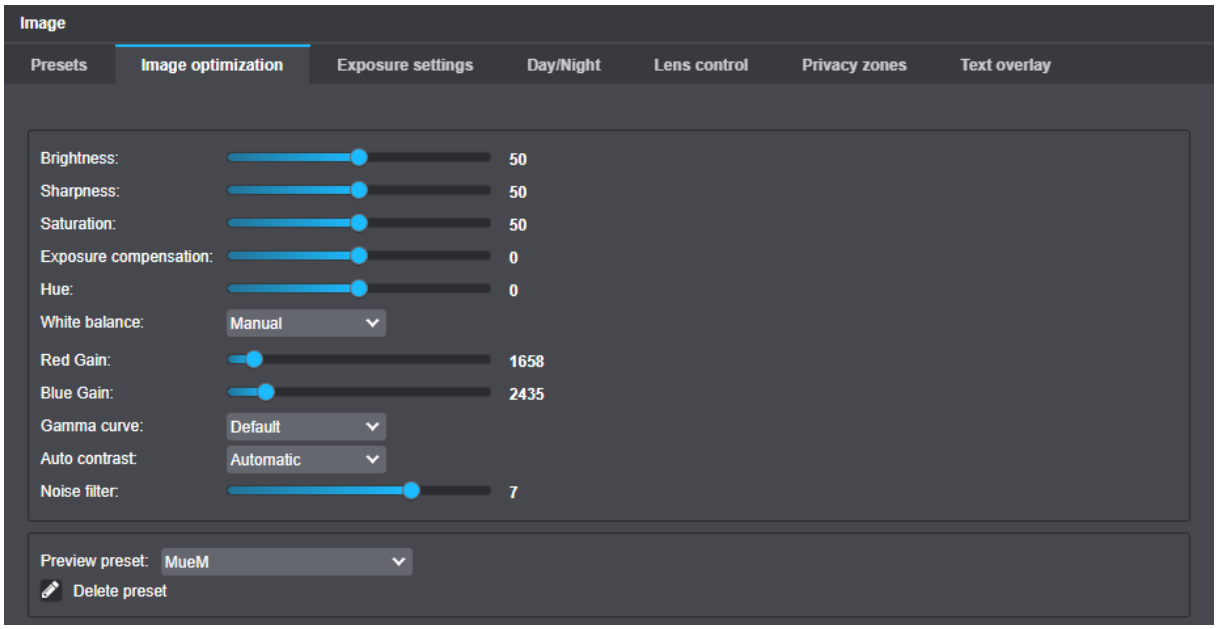

Fig. 5-5 Image optimization

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.

Contrast
This setting is useful to adjust the brightness differences between light and dark areas.

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 condition

Saturation
This setting defines 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 poor lighting conditions.

5.2.1 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

Fig. 5-6

With this setting, 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 (Auto Tracking White Balance) is especially recommended for scenes with constantly varying lighting conditions/color temperatures such as indoor scenes with artificial light sources and incident daylight.

Manual

Fig. 5-7

This setting is used to manually adjust the red, green and blue parts in the image.
With the manual white balance (MWB – Manual White Balance) the respective color components can be adjusted independently using the corresponding sliders for red and blue amplification.

5.2.2 Color Temperature

*This setting is only available in **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
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 and 5000 K bright daylight.

5.2.3 Noise Filter

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

Fig. 5-8

This noise filter type is also called "MCTF – Motion Compensated Temporal Filter" or "3D-DNR – 3D Digital Noise Reduction".

This filter automatically adapts to changing lighting conditions. In good lighting conditions, the filter is almost inactive, but becomes more intense as the brightness decreases.
The noise reduction level can be set manually, but increased ghosting effects have to be taken into account if the filter is applied in a very aggressive way. The default value of 5 is a good compromise between noise reduction and any visible ghosting effects.
The filter can be disabled by setting the value to 0. However, disabling the filter should be avoided as far as possible, since otherwise even barely perceptible micro noise (high-frequency, small-scale noise) would no longer be filtered out. This would noticeably increase the encoder load and the required bandwidth.

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

5.3 EXPOSURE SETTINGS

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

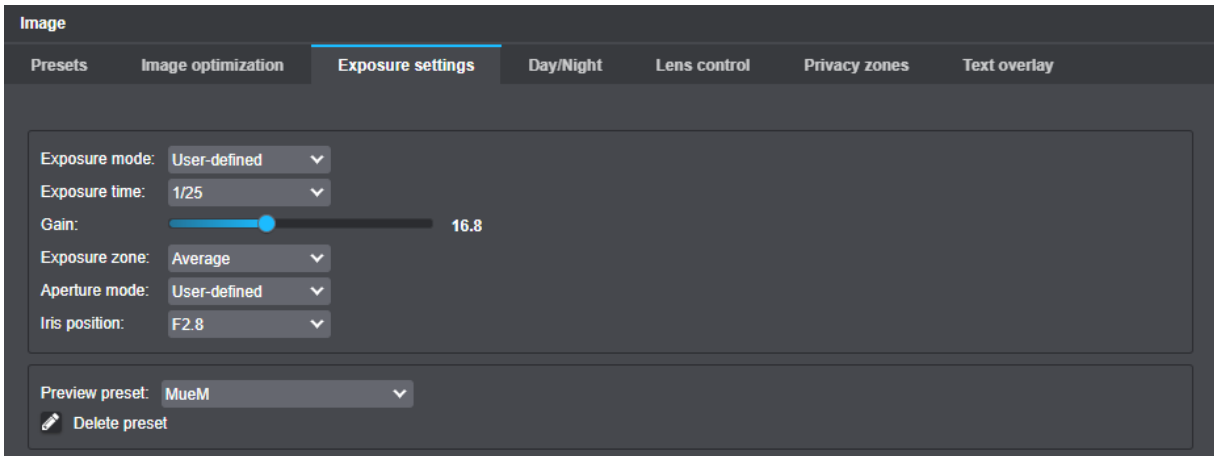

Fig. 5-9

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

5.3.1 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. While doing so, it adheres to the set maximum values.

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

5.3.2 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).

5.3.3 Gain

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

5.3.4 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.

5.3.5 Aperture Mode

Automatic
In this setting, the diaphragm opening (aperture) is automatically adjusted by the camera (depending on exposure time and gain).

User-defined
This option allows the manual adjustment of the aperture.

5.4 DAY/NIGHT

Dallmeier cameras with Domera® OS are designed for maximum image quality in daylight as well as in poor lighting conditions or even total darkness at night.

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

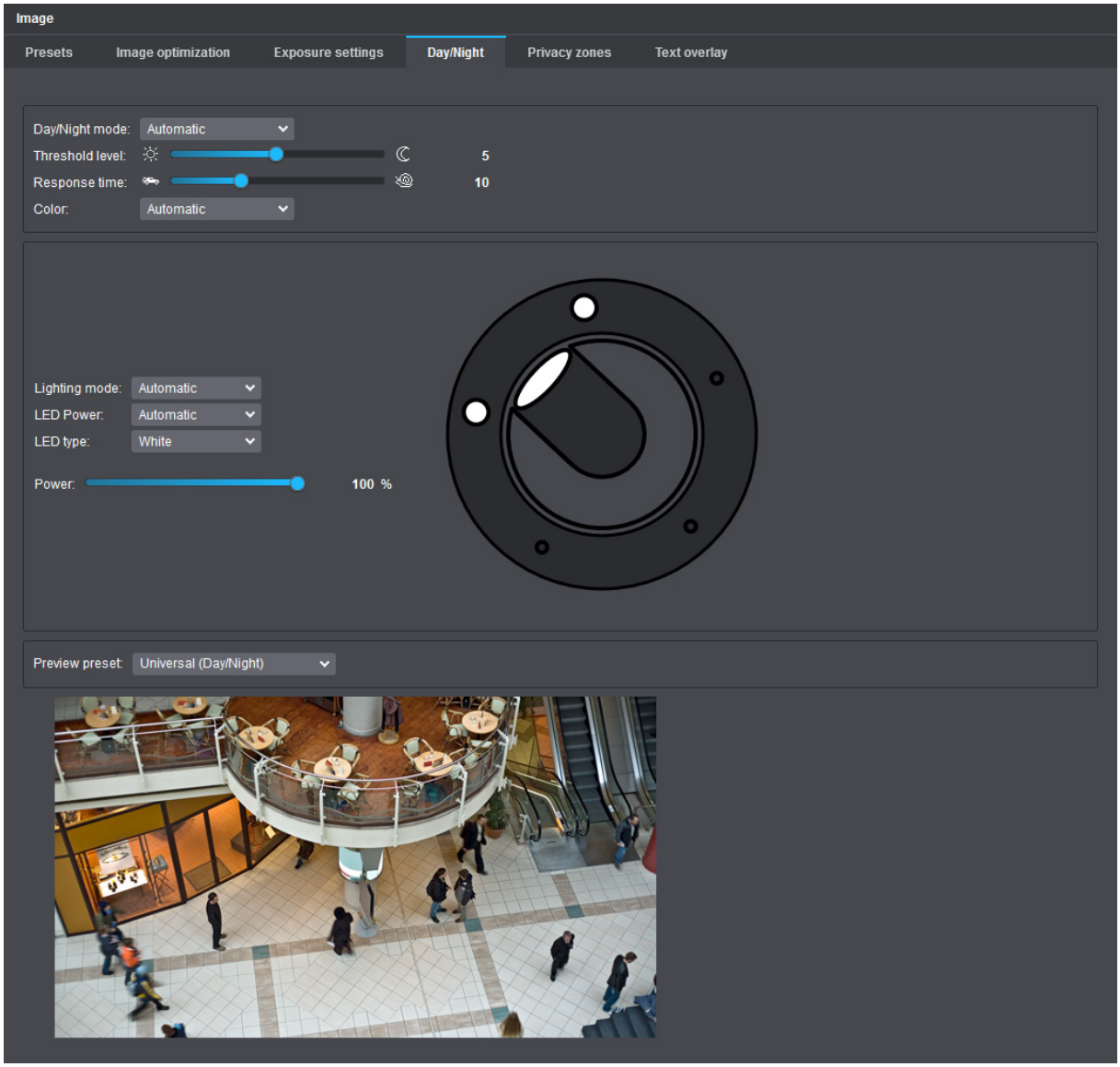

Fig. 5-10

5.4.1 Day/Night Mode

Automatic
Using this setting, the camera automatically switches between day and night mode depending on the continuously measured visible ambient light and after reaching (exceeding or falling below) an internally defined switching threshold in response to the particular values determined for exposure time, signal gain and aperture (f-stop).
In low-light conditions, the camera switches to night mode below a certain brightness level and the built-in infrared (IR) cut filter is disengaged (mechanically shifted away from the image sensor), thus taking advantage of the image sensor's spectral sensitivity to near-infrared light.
As soon as a certain brightness level of visible light is measured again by the integrated ambient light sensor, the camera switches back to day mode and the IR-cut filter is engaged again (mechanically positioned in front of the image sensor) to block the interfering near-infrared wavelengths in day mode and produce highly accurate color images.
The upper threshold hysteresis for automatically switching to day mode and the response time before the actual day/night switching process can be manually adjusted (see descriptions below).

Day – ICR On
Using this setting, the camera always operates in day mode, regardless of the measured ambient light. The built-in IR-cut filter remains permanently engaged (positioned in front of the image sensor).

Night – ICR Off
Using this setting, the camera always operates in night mode, regardless of the measured ambient light. The built-in IR-cut filter remains permanently disengaged.

Automatic – ICR On
This setting corresponds to the **Automatic** setting described above, but the IR-cut (blocking) filter remains permanently engaged even in night mode.

This setting option is intended for very special application scenarios only.

5.4.2 Threshold Level

This setting is used to adjust the upper hysteresis for switching back to day mode in order to prevent the camera from toggling too frequently between day and night operation.
The set value (default: **5**) indicates how much brighter the current visible light measured by the integrated ambient light sensor needs to be than the last known brightness level prior to switching to night mode before the camera switches back to day mode again.

Lower Level
The camera switches back to day mode comparatively early. This means that only slight differences need to exist between the last known brightness level prior to switching to night mode and the brightness level of the visible light currently measured by the integrated ambient light sensor.

Higher Level
The camera switches back to day mode relatively late.

5.4.3 Response Time

This setting is useful for further fine adjustment of the automatic day/night switching.
The response time in seconds (default: **10**) defines the amount of time (delay or waiting time) before the actual day/night switching process is initiated once the measured visible ambient light level has reached (exceeded or fallen below) the internally defined switching threshold.

Example:
If the camera is operated during the day in a room with a window facing a traffic road, the entire room may be temporarily darkened when a large truck passes. Normally, this would cause the camera to switch to night mode immediately after falling below the internally defined switching threshold and return to day mode almost instantly.
In the opposite case, however, each time the headlights of passing vehicles light up the room at night, the camera would switch from night to day mode and back again all in a very short amount of time.

The response time setting can therefore be used to delay the automatic day/night switching according to your needs.

5.4.4 Color

Automatic
Using this setting, the camera automatically switches to grayscale mode (also called black-and-white mode) during nighttime operation and back to color mode during daytime operation.

On
Using this setting, the camera always operates in color mode regardless of the current D/N operating mode (day or night mode).

> *When using infrared light during the night mode (IR-cut filter is disengaged), the presence of any visible residual light in your scene may, under certain circumstances, cause false colors in the output images, depending on the distance and surface type of the captured objects (spectral reflectance).*

Off
Using this setting, the camera always operates in black-and-white mode regardless of the current D/N operating mode (day or night mode). Any color information from the captured scene gets irretrievably lost.

> *Without the color information present in the output images, the overall image quality for scenes with only very poor lighting during day mode can possibly be improved (e.g. by avoiding disturbing color noise).*

5.4.5 Lighting Mode

This setting allows you to configure the built-in infrared (IR) or white light LED illumination of your camera. The IR illumination, for example, is provided by semi-covert 850 nm high-power IR LEDs.

There are three lighting modes available:

Automatic
The selected illumination type (IR or white light; see **LED type** drop-down list) is automatically enabled as soon as the camera switches from day to night mode, and disabled if the camera operates in day mode again.
The LED power can be adjusted manually according to your needs.

Always On
The selected illumination type always remains enabled regardless of the current D/N operating mode (day or night mode).
The LED power can be adjusted manually according to your needs.

Always Off
The integrated illumination LEDs (IR or white light) always remain disabled regardless of the current D/N operating mode (day or night mode).

5.5 PRIVACY ZONES

To protect personal privacy and comply with data protection laws and regulations that prohibit certain areas from being monitored and/or recorded, the **Privacy zones** feature allows you to hide (mask) user-definable areas of the captured scene directly in the camera using various masking tools. The critical parts of your scene can be easily masked with black rectangles or black polygons according to your needs.

The number of supported privacy zones depends on the product model used (refer to the product specification of your device).
The total area of all combined privacy zones can be up to 100% of the entire image.

Privacy zone masks are highlighted in red in the live preview.
All changes made are always immediately applied without any further user action.

To create privacy zones, proceed as follows:

- Click the **Image** menu item in the navigation menu to open the corresponding dialog.
- Select the **Privacy zones** tab.
- Click the required tool (button) to draw, edit or delete privacy zones (see below).

Draw Rectangle

- Click the **Draw rectangle** button.
- Click and hold the left mouse button down while drawing a rectangle over the relevant image area (release the mouse button to finish).

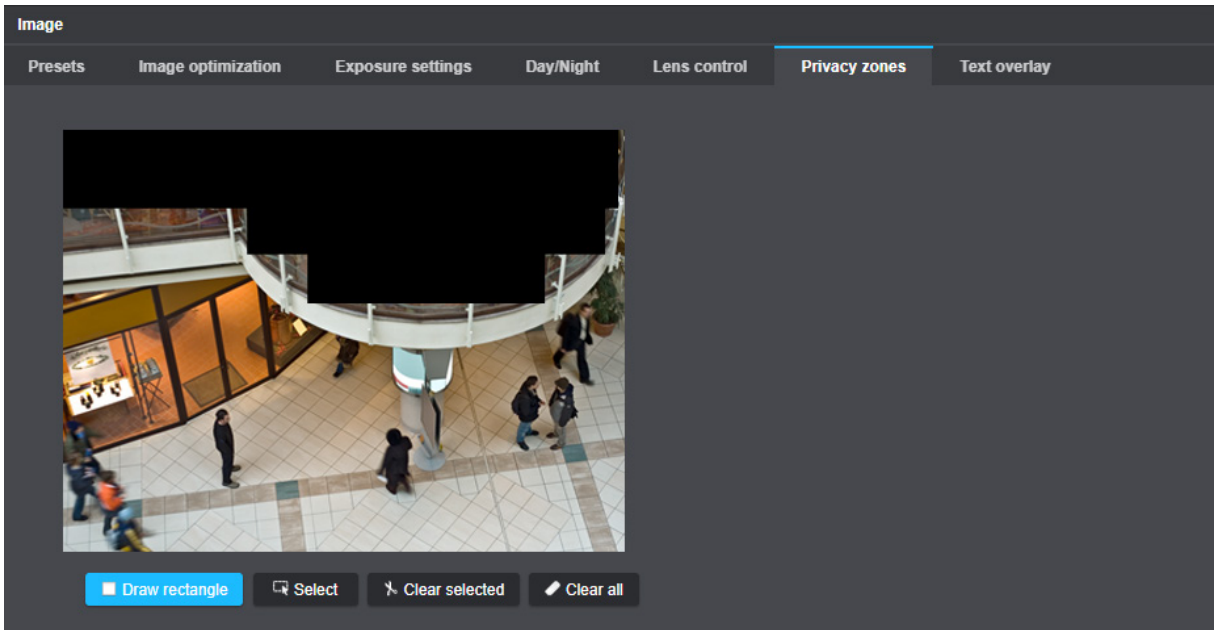

Fig. 5-11

You can define multiple rectangular privacy zones.
The anchor (corner) points of a drawn rectangle can be edited later if needed (see section "Select/Edit" on page 30).

Draw Polygon

- Click the **Draw polygon** button.
- Left-click and release the mouse button to set each of the anchor (corner) points of the new polygonal privacy zone.
- Right-click and release the mouse button or press the **Enter** key on your keyboard to finish creating the new polygon (no other anchor point will be set).

> *You can define multiple polygonal privacy zones.*
> *The anchor (corner) points of a drawn polygon can be edited later if needed (see section "Select/Edit" on page 30).*

Select/Edit

- Click the **Select** button.
- Left-click a drawn privacy zone.

The selected privacy zone is marked with small white circles at its anchor (corner) points.

- Move the white circles while holding down the left mouse button to change the defined privacy zone (new anchor points can be added by use of the left mouse button, but no existing anchor points can be deleted).

> *You can move a drawn privacy zone to a new position by drag-and-drop.*

For deleting defined privacy zones, proceed as follows:

Clear All

- Click the **Clear all** button to delete all defined privacy zones.

Clear Selected

- Click the **Select** button.
- Left-click the privacy zone you want to select (hold down the **Ctrl** key on your keyboard to select multiple privacy zones).
- Click the **Clear selected** button or press the **Delete** key on your keyboard to delete all previously selected privacy zones.

5.6 TEXT OVERLAY

On the **Text overlay** tab, various text elements can be defined and configured, which are then permanently displayed in the live video and during playback of the recorded video material.

The individual character strings of a defined text overlay are permanently inserted into the video data. They cannot be hidden or removed afterwards.

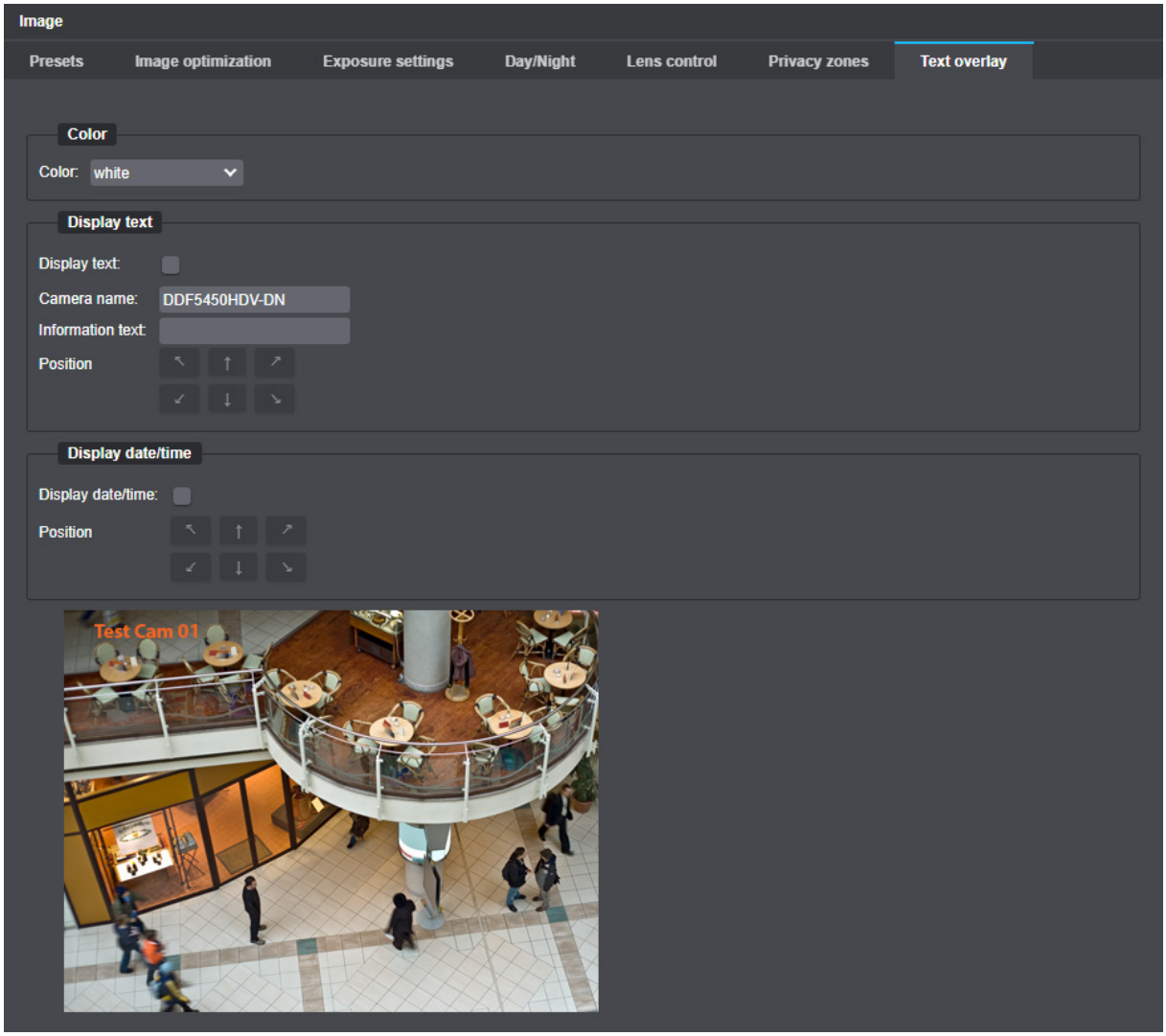

Fig. 5-12

Color

- First select a global text overlay color from the **Color** drop-down list that is best suited for the captured scene and the individual text overlay positions, so that the character strings can later be easily differentiated and read by the operator.

Display Text

- Enable the **Display text** checkbox.
- From the **Display mode** drop-down list, select one of the following text overlay options:

  - **Camera name**
  - **Information text**
  - **Type and serial number** of your camera

- If necessary, change the name of your camera in the **Camera name** field, or enter an individual and descriptive **Information text** for your camera in the corresponding input field.
- Position your text overlay according to your needs using the provided arrow buttons.

Display Date/Time

- Enable the **Display date/time** checkbox if you want to permanently display the current system time of your camera in the video data.
- Position the displayed system time according to your needs using the provided arrow buttons.

LENS CONTROL (RPOD)

Domera® OS allows the positioning (orientation) of the lens/sensor unit as well as the adjustment of the zoom (focal length) and focus to be carried out conveniently via the network in the web browser thanks to the integrated **PTRZ (Pan Tilt Roll Zoom)** function of the **Dallmeier RPoD** (Remote Positioning Dome).

NOTICE

Damage to the camera gimbal and the lens

The camera gimbal and the P-Iris varifocal lens are equipped with high-precision stepper motors. Therefore, under any circumstances, do not attempt to manually adjust the orientation of the lens/sensor unit or the zoom and focus on the camera hardware.

► Click the **Lens Control (RPoD)** menu item in the navigation menu to open the corresponding dialog.

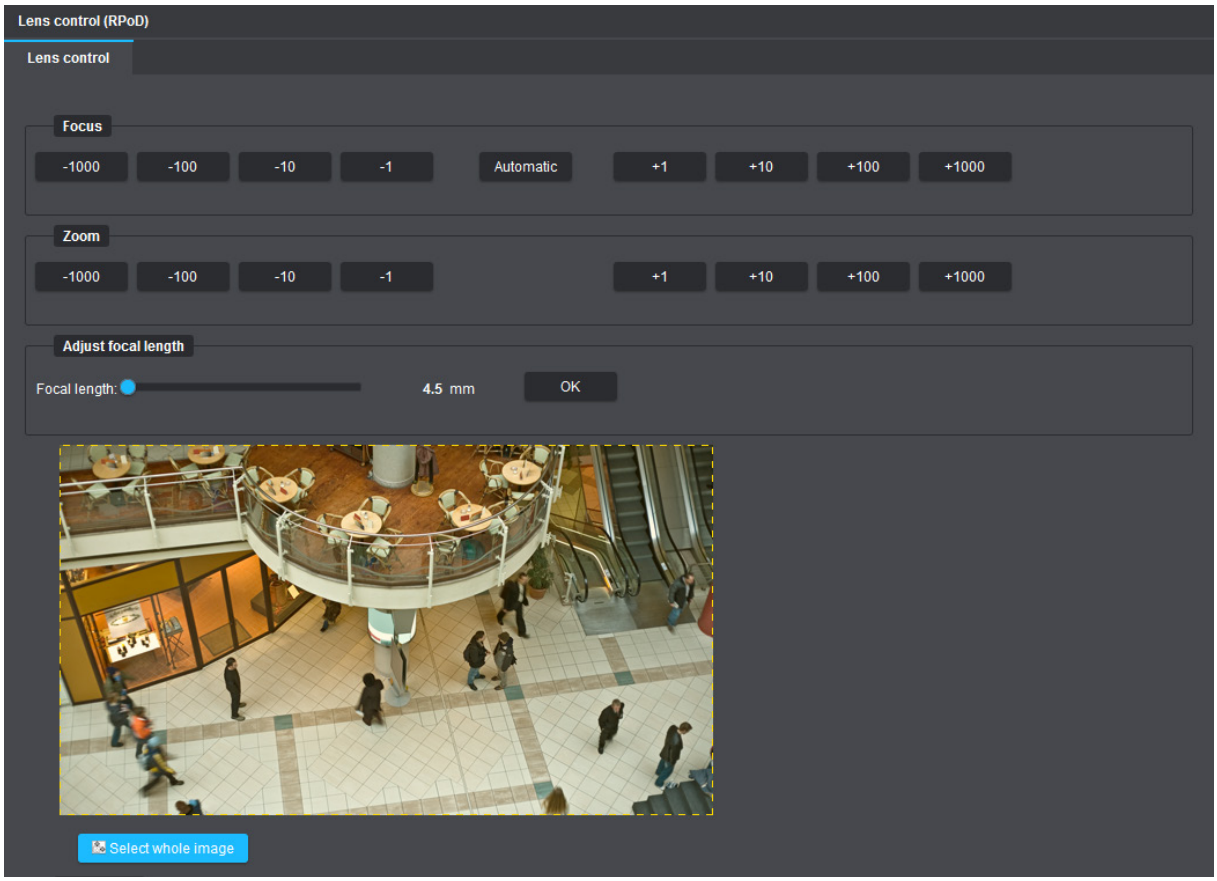

Fig. 6-1

Focus

Manual focusing from far (**+**) to near (**–**) with one-push autofocus* (**Automatic** button)

* For optimal results during one-push autofocus, P-Iris automatically selects the widest possible aperture (smallest possible f-number) and thus an initial minimum depth of field in order to later obtain excellent imaging quality and maximum extent of the focus range in the object space under all lighting conditions.
After a short period without user action, the diaphragm opening (aperture) of the P-Iris lens is reset to its previous f-stop position.

Zoom

Zoom in (**+**) / Zoom out (**–**)
Adjustment of the image section by changing the focal length in several variable steps

Adjust Focal Length

Adjustment of the image section by changing the focal length using fixed values (step zoom with several factory-set focal lengths)

- ► Select a predefined **Focal length** using the corresponding slider.
- ► Confirm with **OK**.

> *If necessary, reduce the encoding data rate (bit rate) to minimize possible delays (longer response times) in browser-based lens control.*

Positioning

This dialog area is used for electronic positioning (orientation) of the lens/sensor unit via the network.

Fig. 6-2

> *Move the mouse pointer over the available buttons to display the associated tooltip (function description).*
> *Changes to the electronic positioning (pan, tilt, roll) are graphically displayed for better clarity and usability.*

VIDEO

The **Video** dialog is used to configure the sensor and encoder settings.

- ▶ Click the **Video** menu item in the navigation menu to open the corresponding dialog.
- ▶ Note the following explanations on the various settings.

7.1 SENSOR SETTINGS

The **Sensor settings** tab provides the essential configuration settings that apply to all available streams (see section "Stream (Encoder) Settings" on page 38).

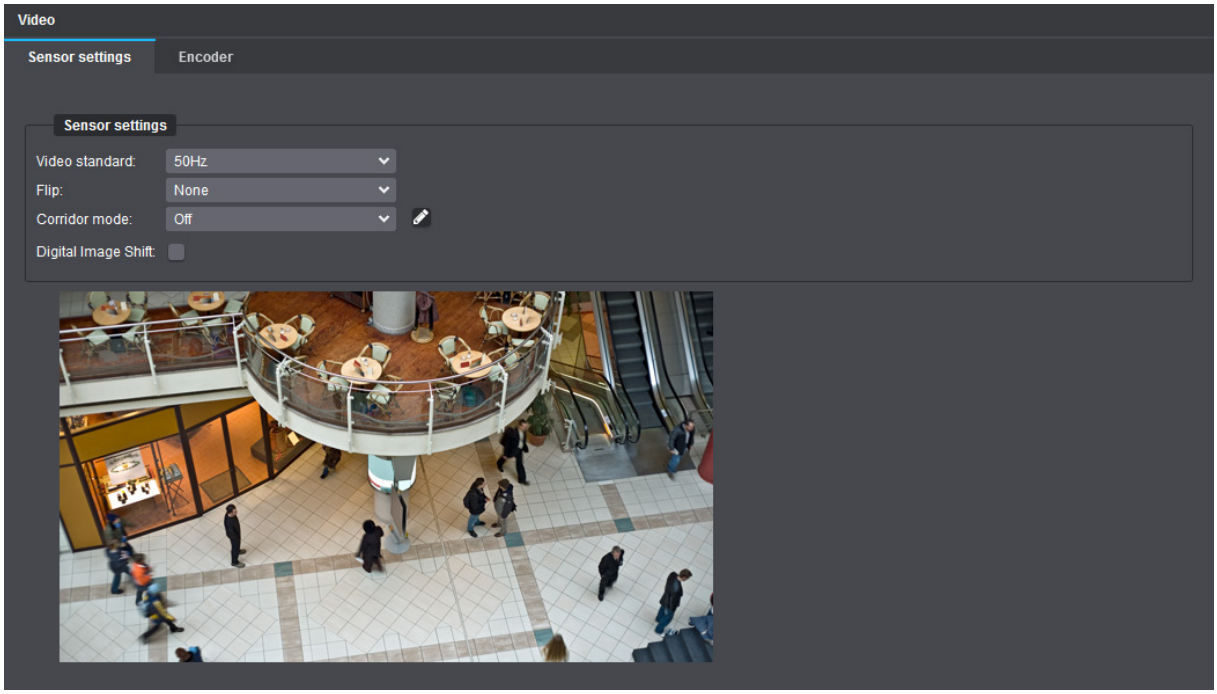

Fig. 7-1

Video Standard (Frequency Setting)
For best image capturing and signal processing results, the frequency setting on your camera must match the nominal grid frequency (also known as utility frequency or mains frequency) in your country or region:

- **50 Hz** (used in PAL countries such as Europe, Australia, and many countries in Africa and Asia)
- **60 Hz** (used in NTSC countries such as the USA and Japan)

The selected frequency setting on your camera affects, for example, the frame rates (**Frames/Second**) that can be individually set for each enabled stream on the **Encoder** tab (e.g. 25/50 fps@50 Hz or 30/60 fps@60 Hz) as well as some of the selectable **Exposure time** values (e.g. 1/50 s@50 Hz or 1/60 s@60 Hz) on the **Exposure settings** tab in the **Image** dialog.

Note that a mismatched setting of this parameter can cause typical unwanted 50/60 Hz video flickering (strobe effect), such as in environments with artificial light sources (e.g. fluorescent lamps) that are operated with alternating current (AC).

Flip

Using the **Flip** function, the image in the camera can be mirrored on the horizontal axis (**vertical** flip), on the vertical axis (**horizontal** flip), or on both axes simultaneously. This allows flexible installation options for tabletop, ceiling or wall-mounted camera use.

Corridor Mode

*The **Corridor mode** feature is not available for fisheye camera models.*

The **Corridor mode** function is particularly suitable for monitoring vertically oriented scenes such as long rooms (passages, hallways, corridors), streets and sidewalks, railway platforms or perimeter fences.
First, the camera or lens/sensor unit is physically rotated during installation so that the scene is not captured in an aspect ratio of 16:9 or 4:3 (landscape format) as usual, but in 9:16 or 3:4 (portrait format). Thus, the full available sensor resolution can be used exclusively for important areas of the scene. Encoding, network transmission, recording and later decoding of superfluous information on the sides of the image can be avoided.
During evaluation of the video material (live view or playback), the images are then automatically displayed correctly rotated for the operator applying the previously selected corridor mode setting.

Example:

Fig. 7-2:
Full HD resolution,
sensor aspect ratio 16:9,
no physical camera rotation,
Corridor mode > Off

Fig. 7-3:
Full HD resolution,
sensor aspect ratio 9:16,
physical camera rotation by 90°,
Corridor mode > Off

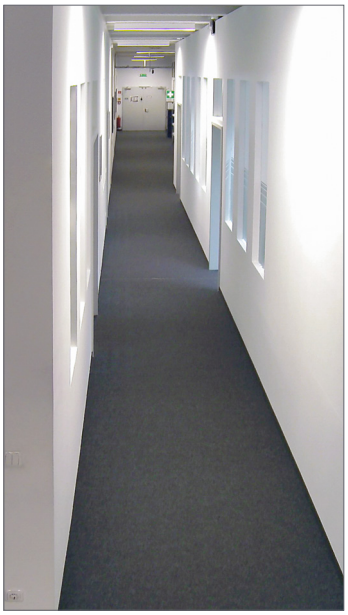

Fig. 7-4:
Full HD resolution,
sensor aspect ratio 9:16,
physical camera rotation by 90°,
Corridor mode > Rotation by 90°

Digital Image Shift

*The **Digital Image Shift** feature is not available for dome cameras with a motor-driven gimbal ("Remote Positioning Dome" – RPoD).*

Usually, only a certain area from the center of the image sensor is effectively used for capturing images, but never the entire one. Depending on the selected output resolution for **Stream 1** (see section "Stream (Encoder) Settings" on page 38), a specific number of sensor pixels at the edges of the image sensor therefore typically remain unsampled (are not read out).

The **Digital Image Shift** function allows the captured scene area to be slightly readjusted via the web browser by digitally shifting the pixel area to be read out in horizontal and/or vertical direction offset from the center of the image sensor.

Applying this function using the corresponding sliders is particularly useful if the captured scene area does not exactly meet your requirements once the camera has been installed. Hence, manual fine adjustment of the viewing direction of the lens/sensor unit directly on the camera is not necessary.

7.2 STREAM (ENCODER) SETTINGS

On the **Encoder** tab, the individual encoder settings for each of the available streams are defined.

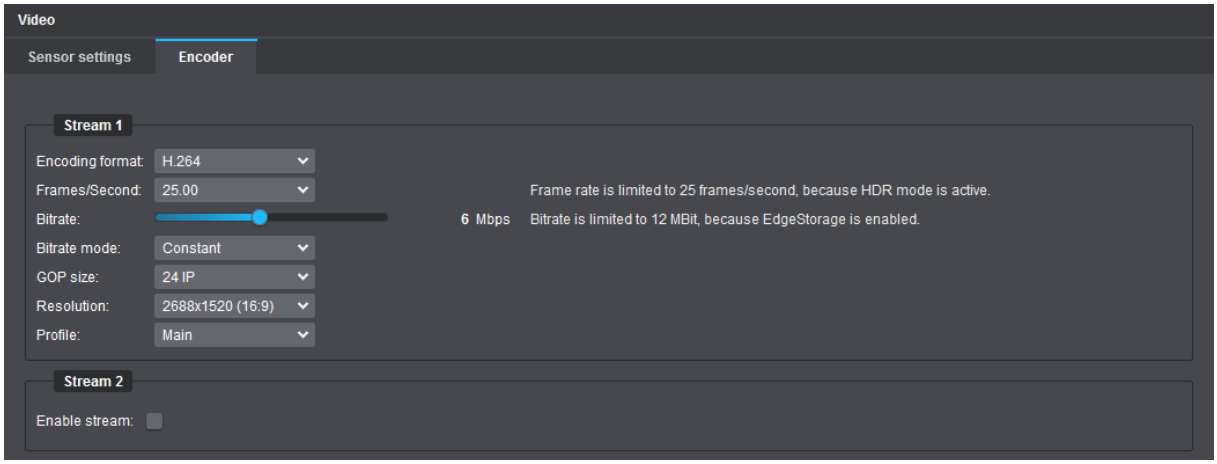

Fig. 7-5

*The **Bitrate**, **Bitrate mode** and **GOP size** settings described on the following pages are not available if the **Encoding format** > **MJPEG** is selected.*

Encoding Format

The **Encoding format** determines the video codec (**H.264**, **H.265** or **MJPEG**) used to encode the individual stream.

Frames/Second

The **Frames/Second** setting or frame rate (value in fps) defines the number of images (frames) that are consecutively produced per second.
The higher the frame rate, the smoother the video output. However, a higher frame rate always requires a higher network bandwidth (transmission capacity) and more hard disk storage space for the recording of video content.
A frame rate of 25 fps (in PAL countries or in countries with a nominal grid frequency of 50 Hz) or a frame rate of 30 fps (in NTSC countries or in countries with a nominal grid frequency of 60 Hz), for example, meets the requirements for real-time video applications.

JPEGQuality

This setting is only available if the **Encoding format** > **MJPEG** (Motion JPEG) is selected.
Using the **MJPEG** encoding format, each produced frame is compressed separately as a single JPEG image.
The **JPEGQuality** slider defines the quality of the JPEG images that are produced consecutively according to the set frame rate.
The higher the quality value set, the lower the compression rate and the higher the quality of the individual images, but the higher the bandwidth and storage requirements.

Bitrate

The video bit rate specifies the number of bits per second used to encode the generated video data.
The more bits the video encoder is allowed to utilize per second for representing the input video data in a compressed form, the better the resulting image quality usually is.
However, a higher video bit rate also requires a higher network bandwidth (transmission capacity) for the transmission of the outgoing data packets and more hard disk storage space for data recording.

Lower bit rate = Higher image compression
= Smaller data size
= Lower image quality and detail resolution
= Lower bandwidth and storage space requirements

Higher bit rate = Lower image compression
= Bigger data size
= Higher image quality and detail resolution
= Higher bandwidth and storage space requirements

Bitrate Mode

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

Constant Bitrate

In case of a constant bit rate, video encoding is always performed using the set bit rate, even if it is not necessarily required for scenes with only minor changes.
If the set bit rate is no longer sufficient for scenes with many changes (such as those with fast-moving objects), the image quality is adjusted.
Constant bit rates allow for a more accurate calculation of the required network bandwidth (transmission capacity) and storage capacity (for data recording).

Variable Bitrate

A variable bit rate is dynamically adjusted to the changes in the captured scene. For scenes with only minor changes, it is decreased; for scenes with many changes (such as those with fast-moving objects), it is increased.

*The **Bitrate** slider is extended in this case allowing a bit rate lower limit to be set.*
This limit (minimum bit rate value) is maintained even for scenes without any changes.

For scenes with many changes (such as those with fast-moving objects), the bit rate can be automatically raised above the set maximum value for a short-term period.
If the total available bit rate is no longer sufficient for all streams/encoders, the image quality is adjusted.
Variable bit rates allow for a high image quality and, at the same time, better utilization of the available network bandwidth (transmission capacity) and storage capacity (for data recording).

Priority Setting for the Image Quality

The **Constant QK** and **Variable QK** (QK = Quality Keep) modes are a variation of the bit rate modes described above. If the set bit rate (**Constant QK**) or the total available bit rate for all streams/encoders (**Variable QK**) is no longer sufficient for scenes with very many changes, the frame rate (fps) is adjusted instead of the image quality.

GOP Size

[Default setting: **24 IP**]

Video encoding with **H.264** (MPEG-4 Part 10 / AVC – Advanced Video Coding) or **H.265** (MPEG-H Part 2 / HEVC – High Efficiency Video Coding) is carried out by arranging frames within the MPEG video stream into so-called "Group of Pictures" (GOP) of a defined length (specified **GOP size**).

Each GOP starts with an Intra-Frame (I-Frame), which is also known as key frame, and ends before the next I-Frame. The I-Frame contains all of the picture information that is needed to reconstruct a complete image and serves as a reference for the subsequent pictures within a GOP.
I-Frames are coded completely independent of any other pictures of the video stream and are compressed with a low compression rate, similar to that of 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 picture(s) – this is called long-term prediction (prediction is based on previous I-Frame and/or P-Frames within the GOP).
The compression rate of P-Frames is much higher than that of I-Frames since changes in relation to reference pictures only need to be coded as motion vectors. Thus, P-Frames are typically much smaller than I-Frames and the required bit rate for P-Frames 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**.
In scenes with only a few or no moving objects, a large **GOP size** can significantly increase the compression efficiency. However, in scenes with a lot of motion changes, a high number of P-Frames can lead to a reduced image quality as the motion predictions become increasingly inaccurate.

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

- the lower the compression efficiency.
- the higher the image quality.
- the smaller the CPU utilization during encoding and decoding.
- the higher the bandwidth and storage space requirements.
- the smoother (more fluent) the video playback when fast forwarding and rewinding.

The higher the **GOP size** (i.e. the less I-Frames and the more P-Frames),

- the better the compression efficiency.
- the lower the image quality (especially in scenes with many motion changes).
- the higher the CPU utilization during encoding and decoding.
- the lower the bandwidth and storage space requirements.
- the more jerky/choppy (less fluent) the video playback when fast forwarding and rewinding.

The visible frames are generated by decoding the pictures contained in each GOP.

*The **GOP size: 1 I** (I-Frames only) indicates a very low compression level (similar to MJPEG) and should only be used in exceptional cases as it would significantly increase the bandwidth and hard disk storage space requirements.*
Reverse playback with very high GOP sizes can lead to frame drops with some decoders. Furthermore, a large GOP size (many P-Frames) always leads to an increase in delays regarding processing or accessing individual images of a stream during playback.

Resolution

This setting defines the output resolution of the generated images (number of pixels in horizontal and vertical direction).
Depending on the camera model and the built-in image sensor, different output resolutions are supported.

For detailed information on the available output resolutions, refer to the product specification of your camera model.

Wide Angle

This setting is only available if the output resolution for **Stream 1** is not set to the maximum supported sensor resolution of your camera model.

As a general rule of geometric optics, the angle of view is determined by the size (format) of the image plane and the set focal length on the lens. Changing (reducing) the output resolution for **Stream 1** and thus the read-out sensor area (used image format) therefore usually changes (reduces) the angle of view at a given focal length, which in turn also changes (reduces) the visible extent of the scene captured on the image sensor.
By default, the resolution of the generated images (selected output resolution) always corresponds to the resolution of the used sensor area (input resolution or number of sensor pixels that are read out in horizontal and vertical direction).
The **Wide angle** feature, by contrast, ensures that even at lower output resolution settings exactly the same sensor area is used for capturing images as is the case when using the maximum available output resolution; the read-out sensor pixels, however, are subsequently downscaled to the selected output resolution (see example below). Since the image format (the sensor area used) now remains the same, the angle of view does not change at a given focal length – regardless of the output resolution selected. In this way, the same extent of the scene can be reproduced with a lower output resolution than with the maximum supported sensor resolution.

Example for dome camera RDF6400DN at a given (unchanged) focal length:

Resolution at **Stream 1**: 2688×1520 (maximum supported sensor resolution)
Checkbox **Wide angle**: Not available, since the largest possible angle of view is already available for a given focal length.
Read-out sensor pixels: 2688×1520
Output resolution: 2688×1520

Resolution at **Stream 1**: 720p (1280×720)
Checkbox **Wide angle**: Available but **cleared (not selected)** -> Downscaling Off
Read-out sensor pixels: 1280×720
Output resolution: 1280×720
->The angle of view reduces in comparison to the angle of view that exists at maximum resolution.

Resolution at **Stream 1**: 720p (1280×720)
Checkbox **Wide angle**: Available and **selected** -> Downscaling On
Read-out sensor pixels: **2688×1520**
Output resolution: 1280×720
-> The angle of view corresponds to the angle of view that exists at maximum resolution.

Profile

This setting is available only for **H.264** encoding.

The **High** profile is the most widely used and also the most efficient and powerful **H.264** encoding profile. In contrast to the **Main** profile, it uses much more complex encoding techniques and thus allows slightly lower bandwidth requirements for data transmission as well as slightly lower storage space requirements for recording video content while maintaining the same high image quality.
However, the **High** profile also requires more computing power (CPU resources) for later decoding of the recorded video stream than the **Main** profile.

> *The selected **H.264** encoding profile must be supported on the decoder side.*
> *In combination with Dallmeier systems and applications, the use of the **High** profile is recommended in most cases.*

Enable Stream

Depending on your needs, you can enable additional streams – each with its own encoder settings. Using a stream with lower image quality for the live display of the camera, for example, can save bandwidth in the network.

AUDIO

LICENSE CODE REQUIRED

This feature requires the purchase of a license code and possibly additional hardware.

For further information please refer to the product specification of your camera on the Dallmeier website at https://www.dallmeier.com/.

To purchase a valid license code for this feature, contact your Dallmeier sales partner.

The use of video security systems in conjunction with audio transmission and audio recording is usually strictly regulated (especially in public areas). Before using the provided audio functions, inform yourself about the locally applicable regulations (regional and country-specific legal requirements) regarding data and privacy protection and ensure compliance with them.

The **Audio** dialog allows you to configure the audio settings of your camera according to your needs.

- ▶ Click the **Audio** menu item in the navigation menu to open the corresponding dialog.
- ▶ Note the following explanations of the various tabs and settings.

8.1 AUDIO INPUT

The audio input interface on the camera (Line-in or integrated microphone, if available) enables the following application scenarios, among others:

- Transmission of individual requests via audio to the operator of the video security system by persons who are in front of or in the vicinity of the camera, for example, to gain access to certain restricted areas or to draw attention to special incidents in the immediate vicinity that are not located directly within the camera's field of view
- Audio-visual recording during hearings of witnesses or interrogations of suspected criminals in addition to written transcripts for a more comprehensive collection of evidence at court trials
- Audio-visual documentation as part of the admission or referral of patients to forensic psychiatric outpatient clinics or for court decisions regarding an interim protective order for temporary placement in a psychiatric facility or preventive detention
- Video and audio recordings of rallies for regulatory reporting and training purposes
- Video and audio recordings of live events, conferences, lectures and more

The variety of possible applications is almost unlimited – however, be sure to clarify in advance whether and under what conditions the transmission/recording of audio content is permitted!

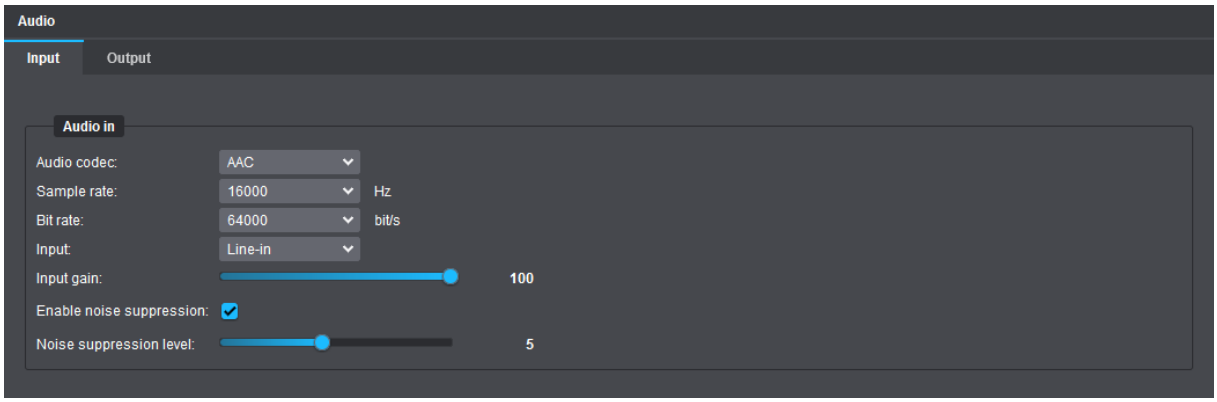

Fig. 8-1

Audio Codec

This setting specifies the codec to be used for encoding the audio data (audio data compression) after digitizing the incoming analog audio signals (analog-to-digital conversion).
The following audio codecs are available:

- **G.711**
  The **G.711** audio codec is primarily intended for **encoding and transmitting voice data** (Voice-over-IP or VoIP) **in ISDN quality** and requires relatively little CPU computing power compared to other audio codecs. For the compression and transmission of high-quality audio data such as music and sound clips, however, the **G.711 voice codec** is only suitable to a limited extent.
  Data compression with **G.711** is achieved exclusively by digitizing the analog audio signal using pulse code modulation (PCM) and companding (using the **A-LAW** or **µ-LAW** algorithm).
  The sample or sampling rate for discretization in time during the first step of the analog-to-digital conversion is **8 kHz** (8000 samples per second or one measurement every 0.125 milliseconds), and the subsequent quantization runs nonlinearly with **8 bits**, resulting in a total data rate of **64 kbit/s** (8 kHz sampling frequency × 8 bits per sample).
  The actual data transfer rate (required bandwidth) for **G.711** after encoding, including overhead, is about **80 kbit/s** to **128 kbit/s**.
  For encoding the audio data, you can choose between one of the following two companding algorithms with different quantization characteristics, depending on your country:

  - **A-LAW** (PCMA; used in Europe and most other countries)
  - **µ-LAW** (PCMU or mu-law; commonly used in North America and Japan)

  The **G.711** audio codec is generally only recommended for applications that are intended for the transmission of information exclusively by **voice in simple ISDN quality**.

- **AAC** – Advanced Audio Coding
  In addition to the **encoding and transmission of spoken content in high-level voice quality**, the **AAC** audio codec is particularly suitable for the efficient compression of sophisticated audio data such as music and sounds in high sonic accuracy, nuanced differentiation and tonal fidelity.
  The source data generated after digitization is reduced by elaborate and highly complex coding techniques in such a way that the data reduction (audio data compression) is almost imperceptible to the human ear (in terms of psychoacoustics) during later output.
  The sample or sampling rate and the audio bit rate can be set as required (see below).

Sample Rate

This setting is only available for the **AAC** audio codec.
The sample rate defines the number of times per second that the continuous voltage changes of the incoming electrical signal (analog audio signal) are measured for digitization (e.g. 48000 times per second = 48 kHz).
The higher the sampling rate is set for the discretization of the continuous-time signal, the more accurately the original analog signal can be digitally mapped and the better (more transparent) the audio quality is at the same bit rate setting (see below), but the more CPU computing power is then required for the final audio data compression.

Bit Rate

This setting is only available for the **AAC** audio codec.
The term **Bit rate** basically describes the ratio of the total amount of digital data to a certain unit of time and is usually specified in bit per second (abbreviated as bps or bit/s), while often preceded by the SI prefix kilo (1 kbit/s = 1,000 bit/s).
In this context, the audio bit rate specifies the number of bits with which the camera's audio encoder encodes the generated digital audio data per second before this data is finally transmitted in a compressed form to the network as a sequence of outgoing audio data packets.
The higher the set audio bit rate is for exactly the same source data while keeping the sample rate unchanged (see above), the better the later audio output quality usually is due to the lower compression rate, but the higher is also the bandwidth requirement for the transmission of the encoded audio data and the required storage space for recording (assuming the same title/track length and identical original audio content).
However, the output quality of digital audio material after audio data compression does not necessarily depend only on the selected encoding bit rate, but also on the overall complexity and dynamic range of the original audio signal and the frequency spectra it contains. The more complex the actual analog signal is, the more bit rate should be provided to the audio encoder for encoding. For less demanding audio content, lower bit rates may be sufficient without any perceptible degradation in quality.

*For high-quality audio transmission and recording in DVD quality, a **sample rate** of **48 kHz** and a **bit rate** of **96 kbit/s** are recommended.*

Input

This setting allows you to switch between a low-level built-in **Microphone** (if available on the hardware side) and a connected **Line-in** device with a relatively high level, such as an external microphone with preamplifier*, thus ensuring correct level processing of the incoming analog audio signals.

* A microphone preamp increases a microphone signal (the level of signal strength) to line level.

*The **Input** drop-down list is only available in the tab if your camera has a built-in microphone (either factory installed or later retrofitted).*

Input Gain

This slider allows you to control the signal gain of the incoming analog audio signal before starting the actual digitization and encoding process.

Noise Suppression

This setting may help to reduce some possible background noise in the source signal.
Note, however, that applying an excessive **Noise suppression level** can result in a loss of quality in the remaining audio signal.

Basic principle of processing incoming analog audio signals

Incoming analog audio signals (e.g. speech) at the camera via hardware audio input interface (Line-in) or integrated microphone* -> A/D conversion (sampling, quantization) -> encoding process (audio data compression) using selected audio codec -> transmission (streaming) of the compressed audio data to the network as a sequence of outgoing audio data packets.

* Air pressure fluctuations within sound waves are first converted by the microphone into varying electrical voltage levels (analog audio signals).

8.2 AUDIO OUTPUT

The analog audio output interface on the camera enables the operator of the video security system to communicate actively, quickly and in a situation-specific manner with persons who are in front of or near the camera.

Thus, the following application scenarios are conceivable, among others:

- Greeting and welcoming visitors individually and with personal touch
- Warning people in a targeted manner of potentially dangerous situations (e.g. in the case of a growing concentration of people in confined spaces on event sites)
- Addressing targeted audible warnings in the event of unconscious or intentional misconduct by persons on site in order to resolve the situation appropriately and in a pro-active manner (e.g. in the case of unauthorized entry into restricted areas or when carelessly leaving behind luggage, briefcases and other objects)
- Early warning of groups of persons or individuals of possible suspicious actions (e.g. in the case of loitering)

► Select the **Output** tab.

8.2.1 Volume and Audio Codec

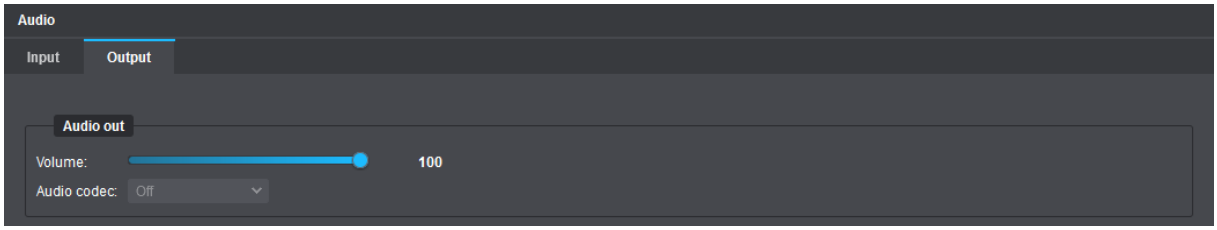

Fig. 8-2

Volume

This slider is used to control the volume when outputting decoded audio data as analog audio signals on a connected loudspeaker with integrated amplifier.

Audio Codec

Received audio data (**G.711 A-LAW**/**µ-LAW** or **AAC**) can be decoded by the camera in real-time and then output as analog audio signals via the built-in (analog) audio output interface (e.g. on a connected loudspeaker with integrated amplifier).
The **HEMISPHERE® SeMSy® Video Management System** or **SeMSy® Compact** transmit the audio signals (e.g. incoming from the microphone port of the client PC) to the camera in digitized form using the Dallmeier Video (**DaVid**) protocol. This does not require any manual settings in the audio client (audio decoder) of the camera, as the selection of the appropriate codec is carried out automatically.

Basic principle of processing received audio data (sent to the camera via LAN)
Client application (e.g. **SeMSy® Compact**) sends encoded audio data packets to the camera via LAN -> decoding of the compressed audio data streams with suitable audio codec -> D/A conversion -> output of the analog audio signals on a connected loudspeaker with integrated amplifier.

8.2.2 Audio Sequences

In addition to the targeted audio output manually initiated by the operator of the video security system via the audio output interface on the camera's hardware (e.g. for individual greeting visitors directly via the client PC in the security center using a microphone and **SeMSy® Compact**), the camera also enables the automatic, event-based playback of audio files (audio sequences) previously uploaded to the camera, for example to automatically warn intruders of entering restricted areas.

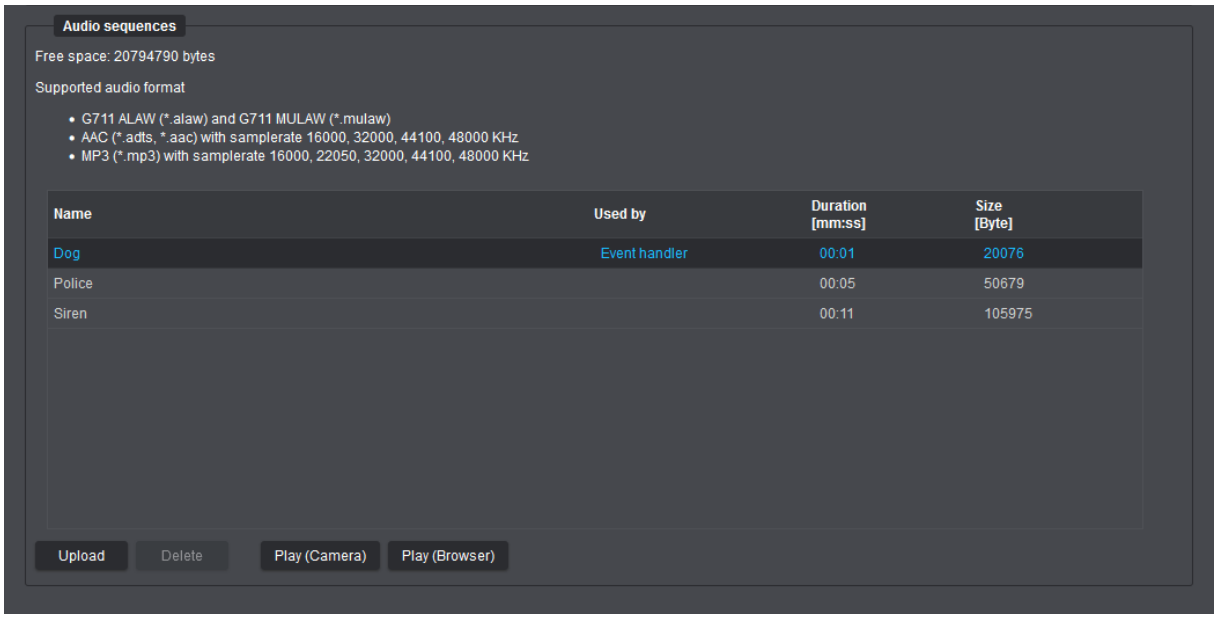

Fig. 8-3

The **Audio sequence** dialog area is used for uploading and managing audio clips, such as spoken automatic greetings and other frequently used acoustic announcements, sound signals and alarm tones, as well as any kind of voice, music and sound recordings.

Playback of audio sequences via the audio output interface on the camera can then either be started manually by clicking the **Play (Camera)** button or automatically by one or more of the following events:

- Physical change of a contact input's state on the camera
- **EdgeAnalytics** event detected:
  - Line Crossing (object has crossed a virtual line)
  - Intrusion Detection (object has entered/left a sensitive area)
  - Loitering (loitering detection started or stopped)

For testing purposes, audio sequences can also be played back directly in the web browser by clicking the **Play (Browser)** button.

> *By default, various audio sequences are already uploaded to the camera. These cannot be deleted. Before uploading audio files, also note the information in the camera dialog about the currently supported audio codecs and container or file formats, as well as the possible quality levels (sample rates).*

DATE & TIME

The camera's system time can either be set manually or synchronized with an NTP time server.

9.1 MANUAL CONFIGURATION

Note that manual configuration is not possible if synchronization with an NTP time server is enabled.

- Click the **Time** menu item in the navigation menu

The **Time** tab is displayed.

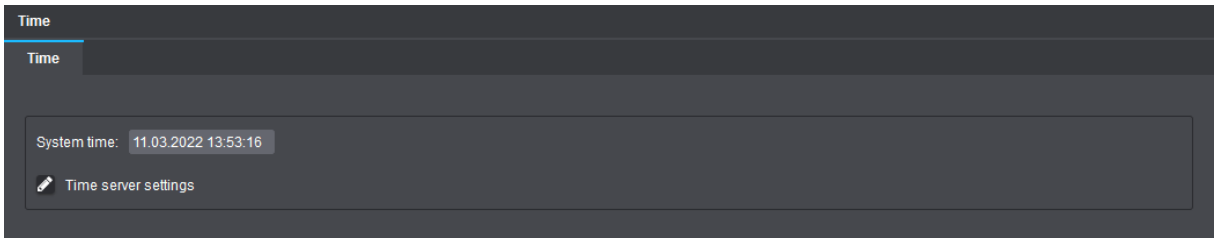

Fig. 9-1

- Click into the **System time** field.
- Change the settings as required.
- Finally, confirm with **Done**.

The set time is then applied as the new system time.

9.2 TIME SERVER SETTINGS

For descriptions regarding the **Time server settings**, see section "Time Server" on page 57.

NETWORK

10.1 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**.

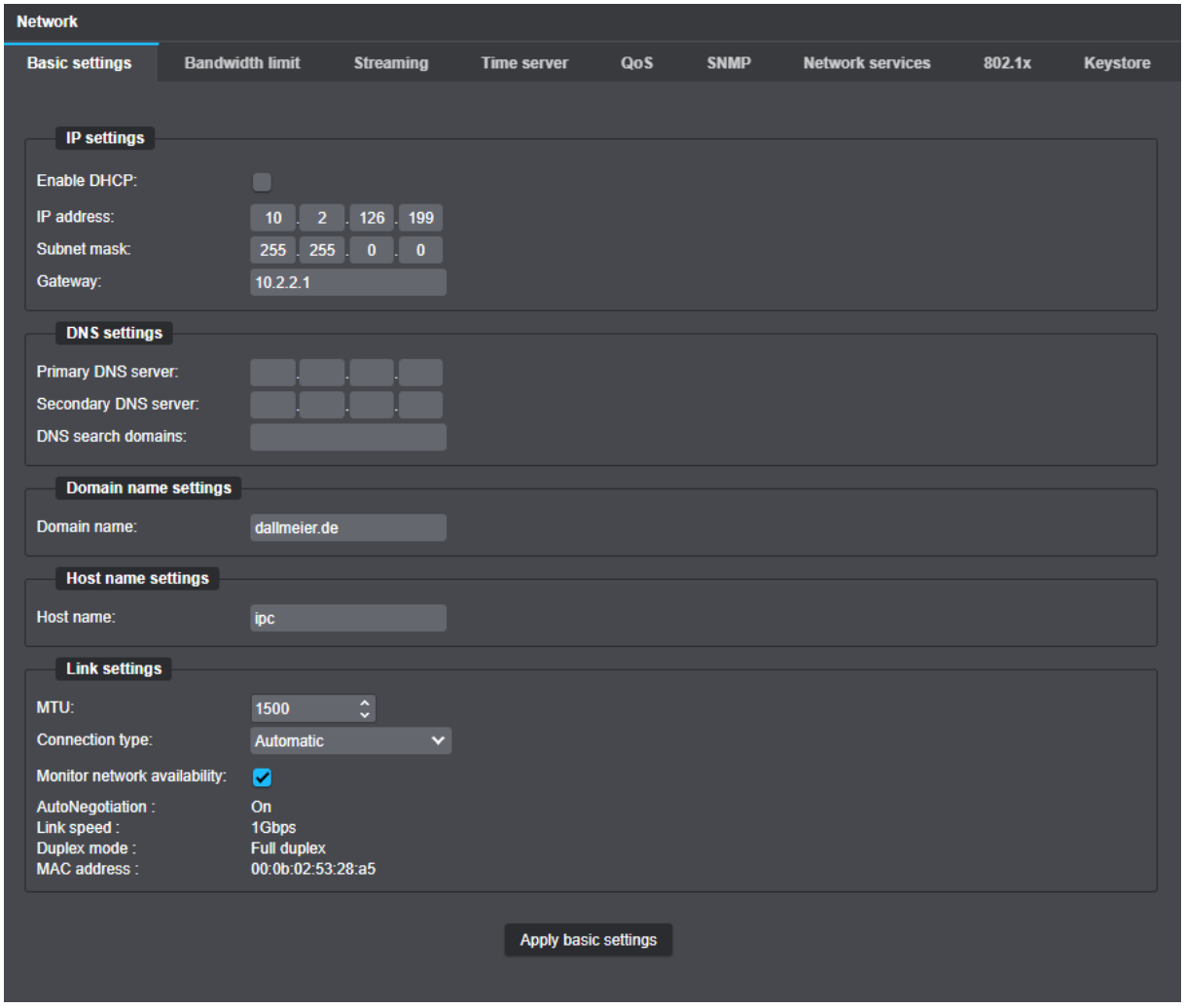

Fig. 10-1

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 has been entered.*

IP-Settings

Enable DHCP

Refer to “Automatic Network Setup using DHCP” on page 52.

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** checkbox.

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

> *To ignore data sent by the DHCP server, clear the corresponding checkboxes **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 51.
- Confirm with **OK**.

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

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

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

Manual Network Setup

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

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

- Make sure the **Enable DHCP** checkbox is cleared.
- 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 51.
- Confirm with **OK**.

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

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

10.2 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**.

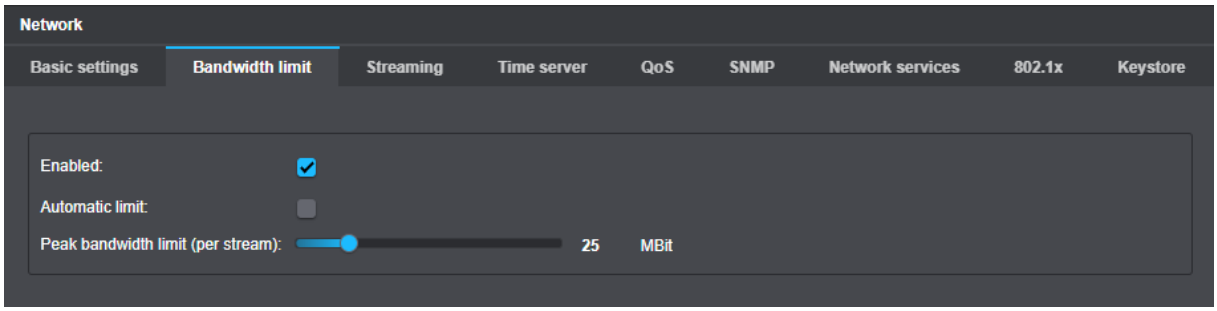

Fig. 10-2

- Select the **Enabled** checkbox 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 selected, 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.

- Select the **Automatic limit** checkbox.
- Confirm with **OK**.

10.3 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**.

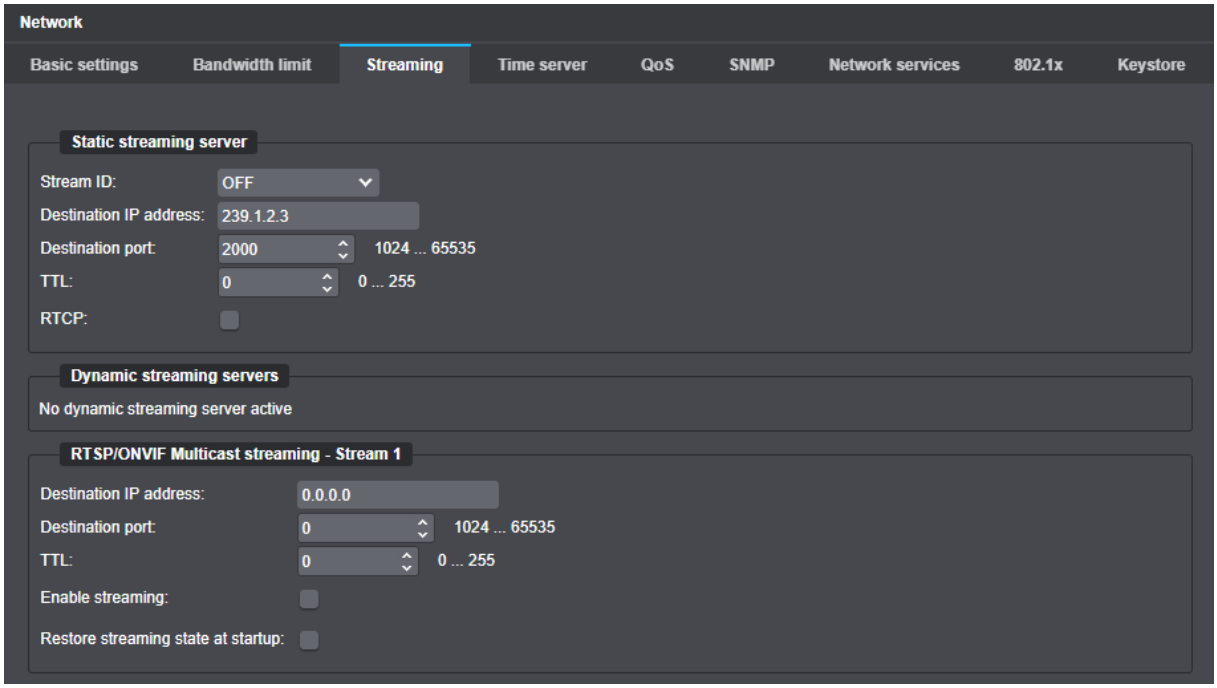

Fig. 10-3

Static streaming server

▶ 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** checkbox 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.

► Contact your network administrator for more information and assistance.

In a multicast-enabled network, each datagram is provided with a special IP multicast group address and then transmitted to a group of receivers (multicast group). This is also known as one-to-many distribution (from one source to multiple destinations).
Compared to unicast data transmission, the source host sends only a single copy of the data packet to the network; the replication of the multicast data packet and its distribution to each individual member of the multicast group (one copy for each target host) is performed by specially configured (multicast-capable) routers/switches.
To periodically determine whether registered members of a multicast group are still active, multicast switches should be used that support IGMP snooping (in IPv4) or MLD snooping (in IPv6).
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.

► Contact your network administrator for more information and assistance.

For more information on IP multicasting and on recommended switches for Dallmeier systems, read the "Switch Basics" and "Switch Whitelist" white papers that are available on www.dallmeier.com.

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.

10.4 TIME SERVER

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

- Click **Network** > **Time server**.

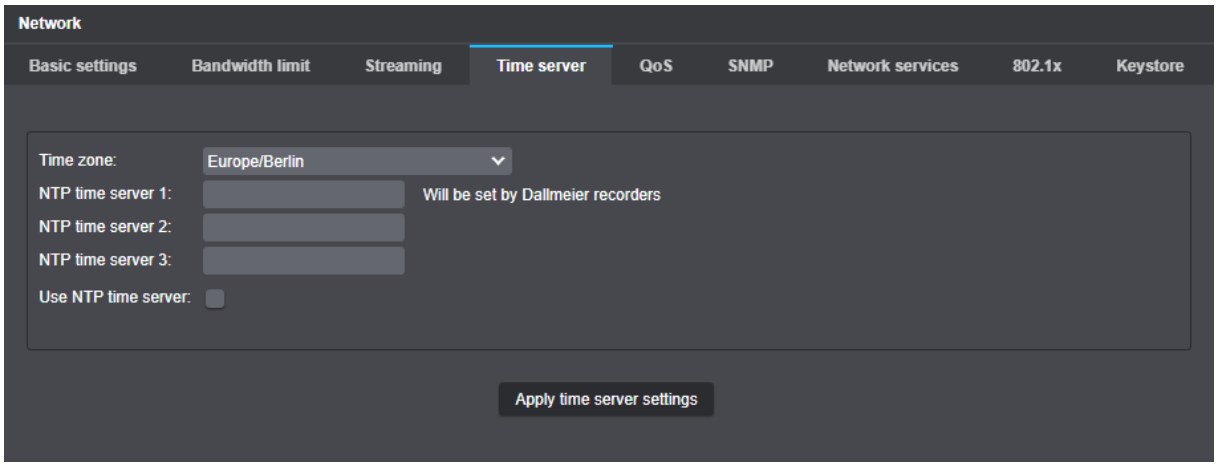

Fig. 10-4

- Select the **Time zone**.
- Enter the IP address of the **NTP time server**.
- Select the **Use NTP time server** checkbox.
- 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.

10.5 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.**

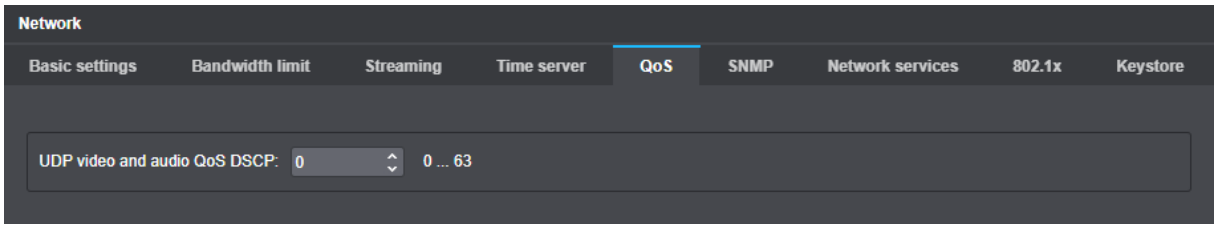

Fig. 10-5

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

10.6 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**.

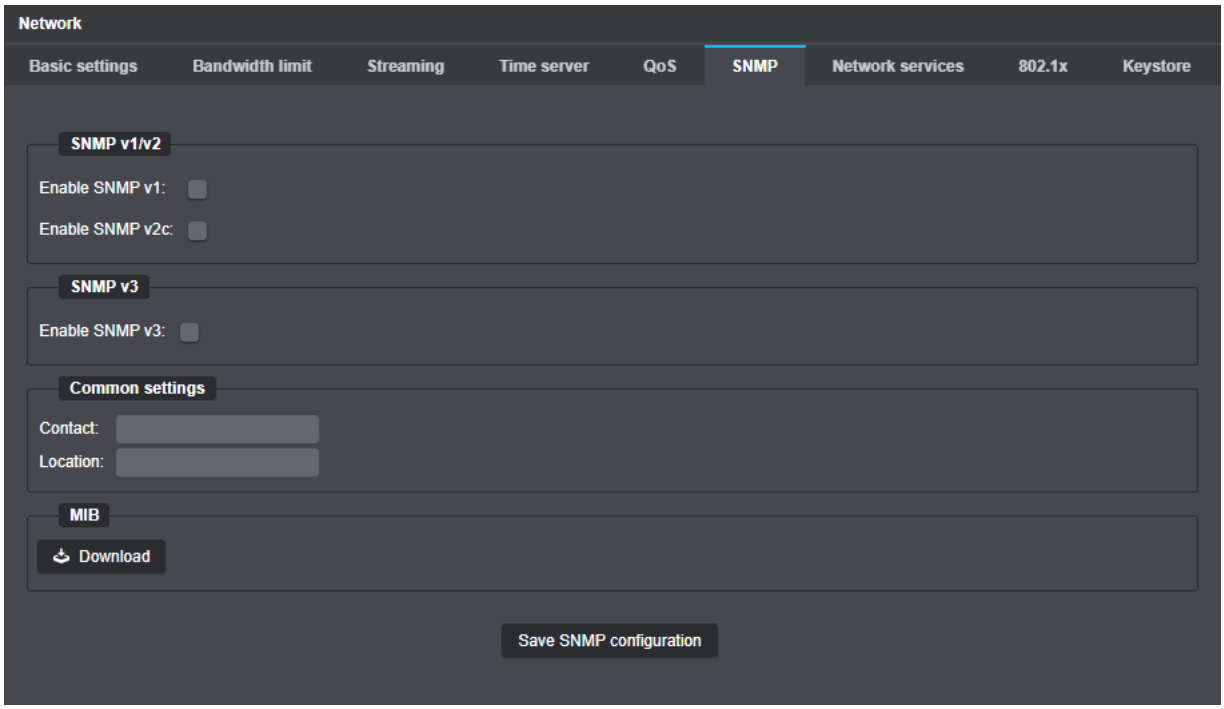

Fig. 10-6

- Configure the required settings (see below).
- Confirm with **Save SNMP configuration**.

> *The **Save SNMP configuration** button remains inactive until all required settings have been made.*

> *The selected SNMP version must match the setting of the used Network Management System (NMS).*

SNMP v1/v2c

SNMP v1/v2c are widely used, but do not provide sufficient data security, and thus 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 listened to by anyone on the network with packet sniffing.*

- Select the checkbox of the required SNMP version.
- Enter the community string you want to use (default: public) into the **Community** input field.

SNMP v3

SNMP v3 supports authentication as well as encryption of the transmitted data.

- Select the **Enable SNMP v3** checkbox.
- Enter the SNMP user name to be used into the **User** input field.
- Select the required authentication method from the **Authentication** drop-down list (see below).
- Select the required encryption method from the **Encryption** drop-down list (see below).

Authentication

The following authentication methods are available:

- **OFF**
  No message authentication (only SNMP user name required)
- **MD5**
  Message authentication with HMAC-MD5 (Hash-based Message Authentication Code based on Message-Digest Algorithm 5); required password length min. 8 characters
- **SHA**
  Message authentication with HMAC-SHA (Hash-based Message Authentication Code based on Secure Hash Algorithm); required password length min. 8 characters

Encryption

The following encryption methods are available:

- **OFF**
  Transmitted data is not encrypted
- **DES**
  Data encryption with DES (Data Encryption Standard);
  required password length for the encryption min. 8 characters
- **AES**
  Data encryption with AES (Advanced Encrpytion Standard);
  required password length for the encryption min. 8 characters

Common settings

This section allows you to specify a contact person (e-mail address) and the location (e.g. 3rd floor) of the SNMP agent to be managed (this device).

- Enter the relevant information into the **Contact** and **Location** input fields.

Use INFORM instead of TRAPs

If you want the receiver of the SNMP messages to send an acknowledgment when a Trap is received, you can switch from TRAP to INFORM (note that SNMP Inform is not supported by SNMP v1).

- If necessary, select the **Use INFORM instead of TRAPs** checkbox.

Trap Options

The following SNMP notifications (Traps) can be sent from the camera to the SNMP manager:

- **Cold start**
  Message when SNMP agent starts
- **Warm start**
  Message when SNMP agent reloads the configuration
- **Shutdown**
  Message when SNMP agent is stopped
- **Authentification failure**
  Message when access to the SNMP agent is attempted without authorization
- **Link up**
  Message when network is available again after failure
- **LLDP**
  Message on every change of the network participants detected via LLDP/CDP

In addition, the following information about the device can be queried:

- IP-MIB: Internet protocol (IP configuration)
- HOST-RESOURCES-MIB: hrSystemUptime (System uptime)
- HOST-RESOURCES-MIB: hrSystemDate (System time/date)
- UCD-SNMP-MIB: Memory Statistics (RAM utilization)
- UCD-SNMP-MIB: CPU Statistics (CPU utilization)
- UCD-SNMP-MIB: Load Average Information (average CPU utilization)

MIB

To get information about other possible queries, the MIB file of the device can be downloaded.

► Click **Download** to download the MIB file if necessary.

10.7 NETWORK SERVICES

Default factory settings

ONVIF: deactivated
RTSP: deactivated

- Click **Network** > **Network services**.

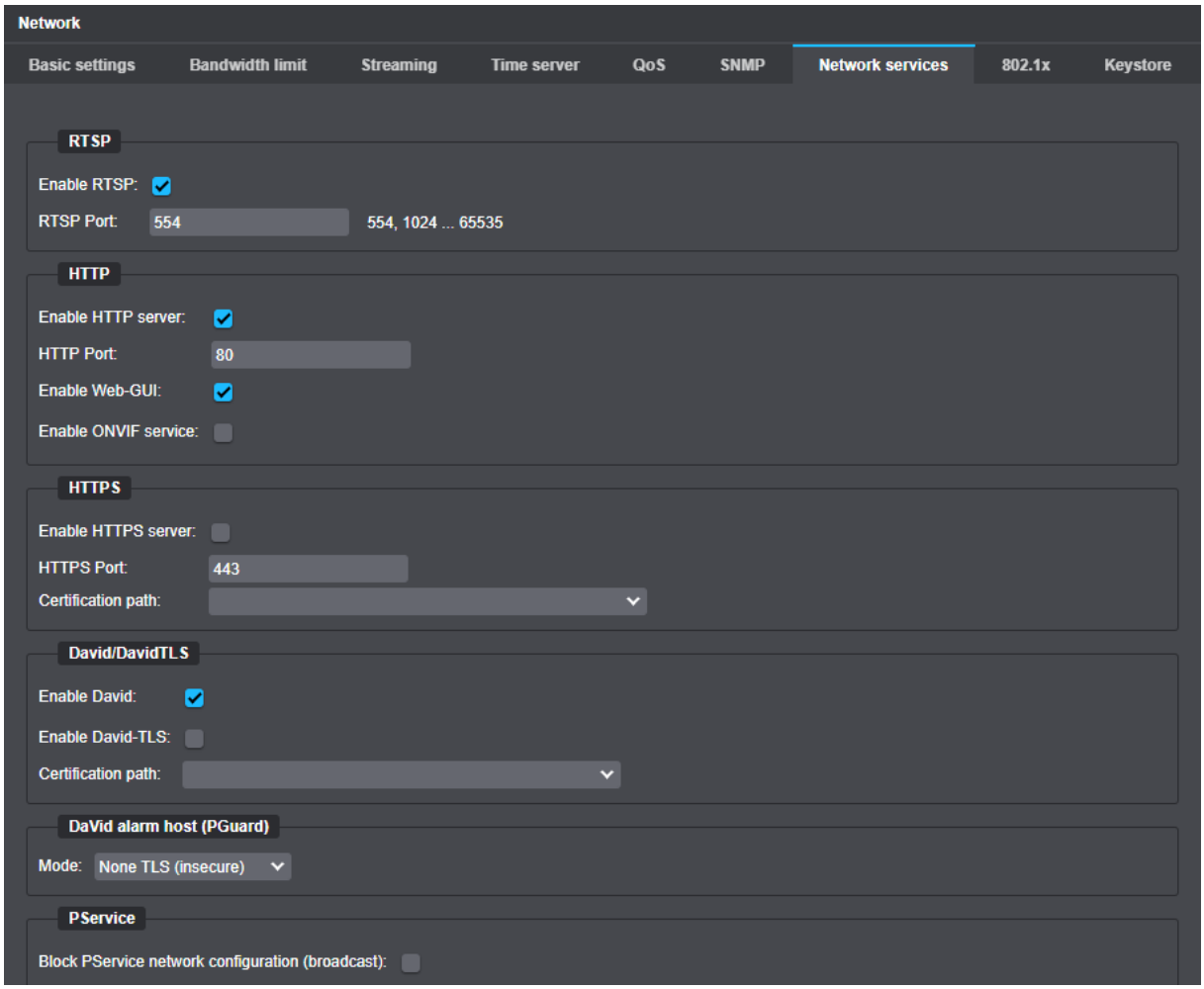

Fig. 10-7

- Note the following instructions.
- Select the relevant checkboxes.
- 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** checkbox 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 146

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 (Dallmeier Video) Protocol.
For the encryption, a certificate path must first be created in the keystore (see“Keystore” on page 66).

- ► Select the **David activated** checkbox if necessary.
- ► Select the certificate path for the encryption from the drop-down list.
- ► Select the **David-TLS** checkbox if necessary.

DaVid Alarm Host (PGuard)

The behavior of the system concerning TLS encryption when sending event triggered messages to an alarm host using the DaVid (Dallmeier Video) Protocol can be regulated using the drop down list.

- ► Select the necessary TLS mode from the **Mode** 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 (Dallmeier Video) Protocol, select the **Force encrypted credentials** checkbox.

Note that this setting does not encrypt the login credentials when you log on to the web-baed graphical user interface of the device using a web browser.

10.8 802.1X

IEEE 802.1X describes a standard for port-based network access control and ensures that newly connected network devices are only granted access to the correspondingly secured local area network (LAN) after successful authentication.
DOMERA® OS exclusively supports the secure and certificate-based authentication process via **EAP-TLS** (Extensible Authentication Protocol over a secured TLS connection).
The authentication process includes three elements: the supplicant (here: the camera) that wants to access the network, the authenticator (e.g. an IEEE 802.1X-capable managed switch) that controls access to the network via the individual network ports (e.g. physical Ethernet interfaces), and the central authentication server (RADIUS server) that checks the transmitted authentication data of a newly connected supplicant and, if valid, verifies its identity.

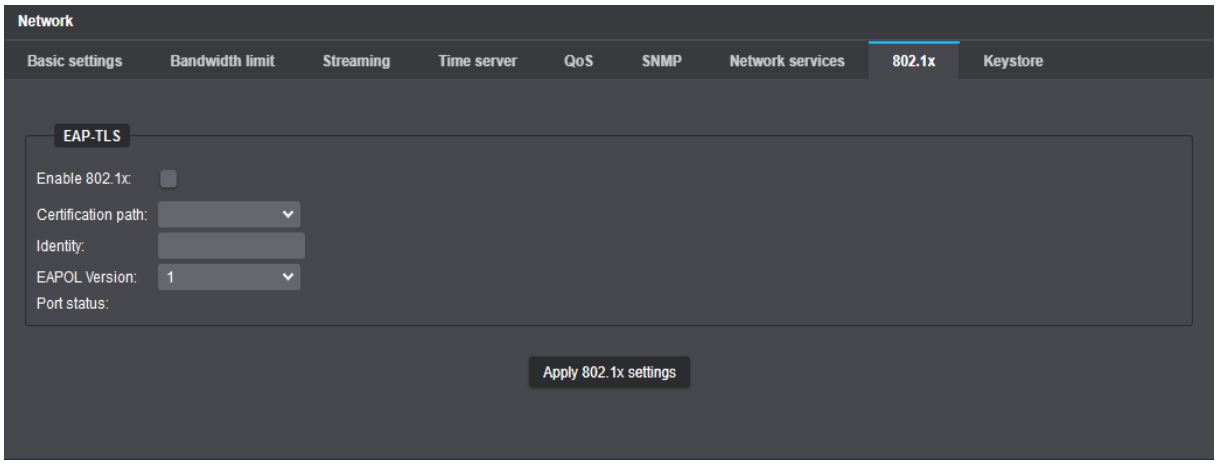

Fig. 10-8

- Select the **Enable 802.1x** checkbox.
- Select the **Certification path** that contains the signed digital client certificate for authentication with the authentication server (for descriptions of certificate management, see section “Keystore” on page 66).
- Enter the EAP identity of the camera in the **Identity** input field if this information is required for a correct authentication process at your RADIUS server.

  Whether it is necessary to specify an EAP identity and what the exact form of such an identity string may have to look like (e.g. equal to the “Common Name” in the signed client certificate) depends on the configuration of your RADIUS server.

- Select the **EAPOL Version** that is also used by your authenticator (IEEE 802.1X-capable switch) so that the authentication data is transmitted correctly later.
- Finally, confirm your entries with **Apply 802.1x settings**.

10.9 KEYSTORE

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

► Click **Network** > **Keystore**.

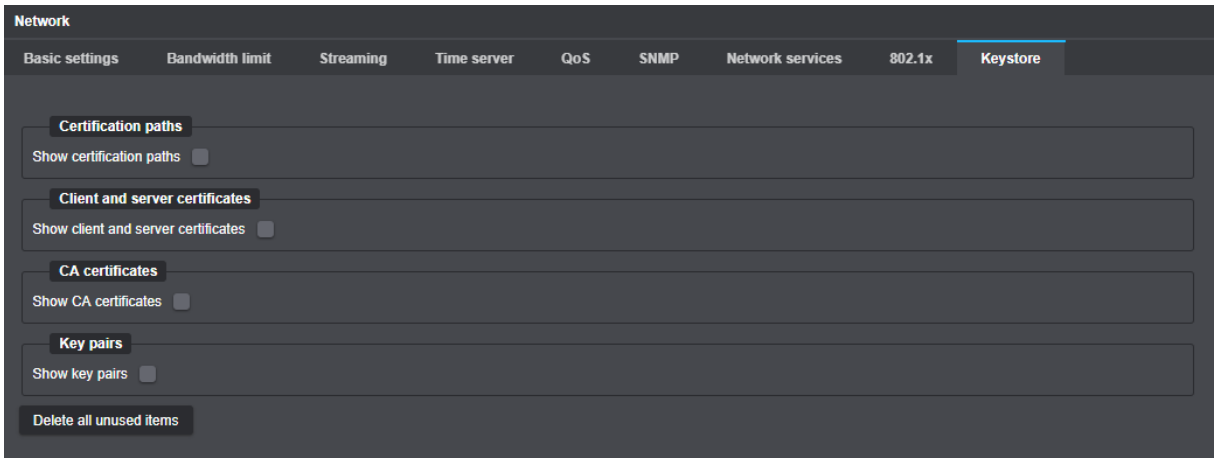

Fig. 10-9

10.9.1 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

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

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.

10.9.2 Managing Certificates and Keys

Certification paths

- Select the **Show certification paths** checkbox.

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

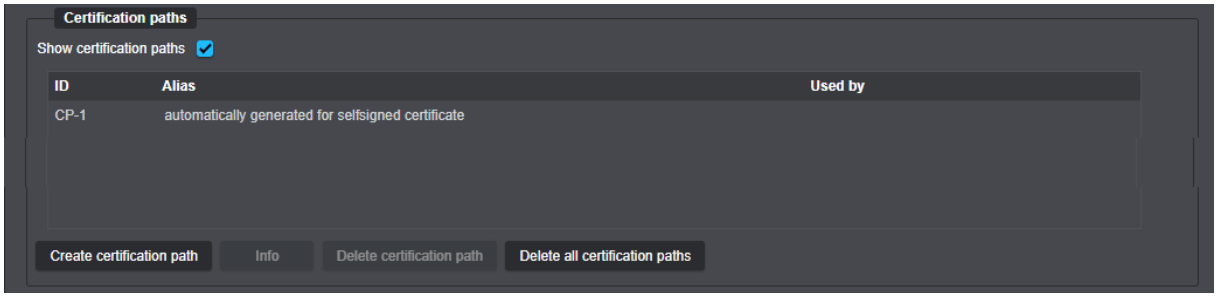

Fig. 10-10

Create certification path

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

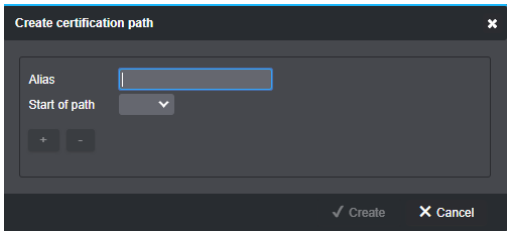

Fig. 10-11

- 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

► Select the **Show client and server certificates** checkbox.

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

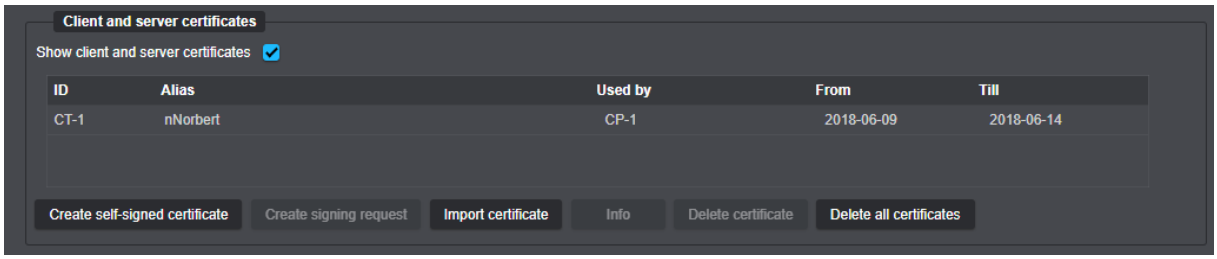

Fig. 10-12

Self-signed certificate

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

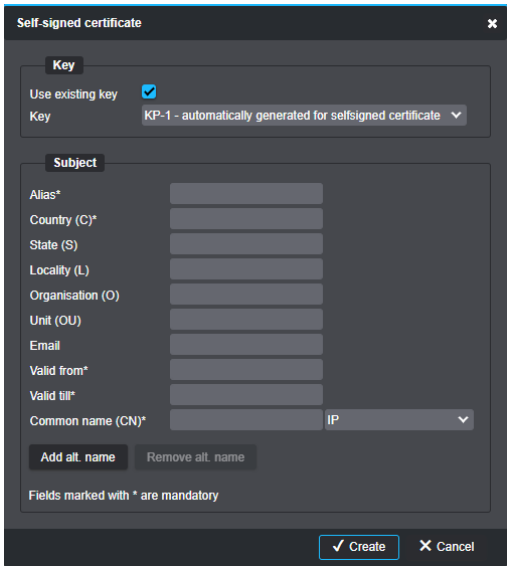

Fig. 10-13

► Select the **Use existing key** checkbox 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.

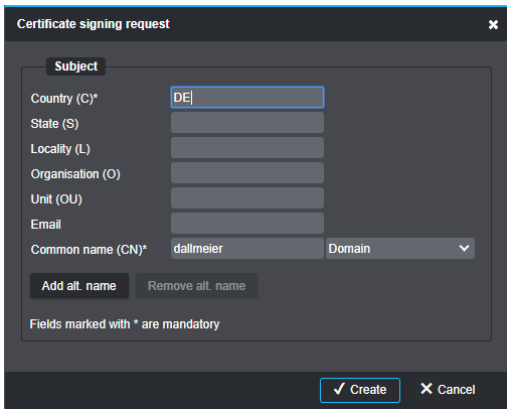

Fig. 10-14

- Enter the necessary data.
- Click **Create** to finish the process.

Import certificate

- Click **Import certificate** to open the import dialog.

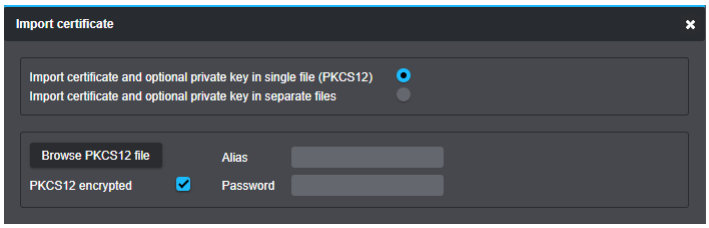

Fig. 10-15

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.

> *The corresponding options are only displayed when the relevant radio button is activated.*

PKCS12 format:

- Click the **Browse PKCS12 file** button.
- Enter the file path using the explorer.
- Enter an **Alias** if necessary.
- Select the **PKCS12 encrypted** checkbox if necessary.
- Enter the appropriate **Password** if necessary.
- Confirm with **OK**.

Separate import:

- Click the **Browse certificate** button.

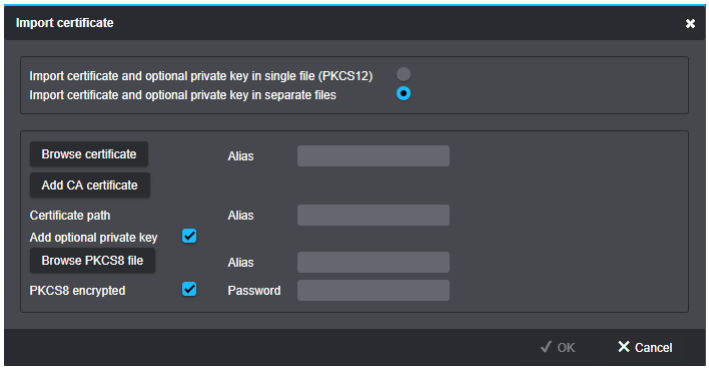

Fig. 10-16

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

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

- Click the **Browse CA certificate** button.
- Select the correct file path using the explorer.
- Select the **Add optional private key** checkbox if necessary.
- Click the **Browse PKCS8 file** button.
- Select the correct file path using the explorer.
- Select the **PKCS8 encrypted** checkbox if necessary.
- Enter the appropriate password if necessary.
- Confirm with **OK**.

CA certificates

- Select the **Show CA certificates** checkbox.

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

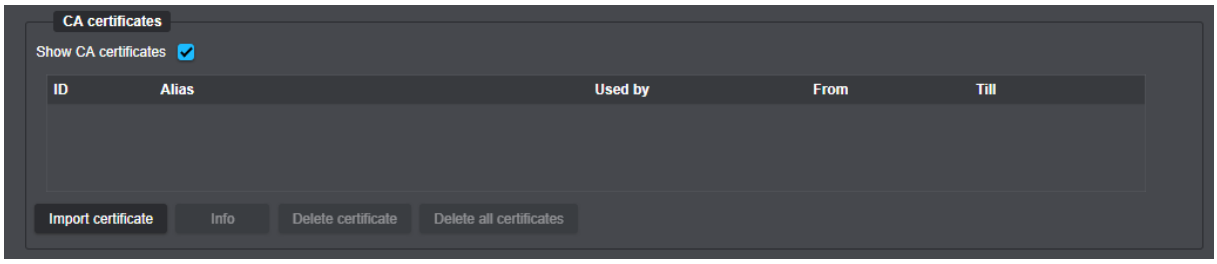

Fig. 10-17

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

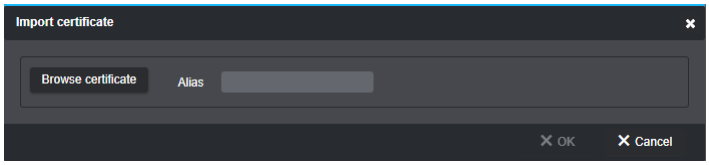

Fig. 10-18

- 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

- Select the **Show key pairs** checkbox.

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

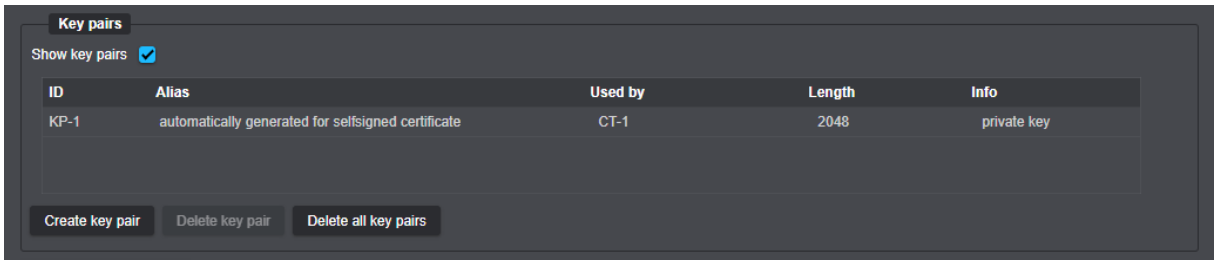

Fig. 10-19

Create key pair

To create a key pair proceed as follows:

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

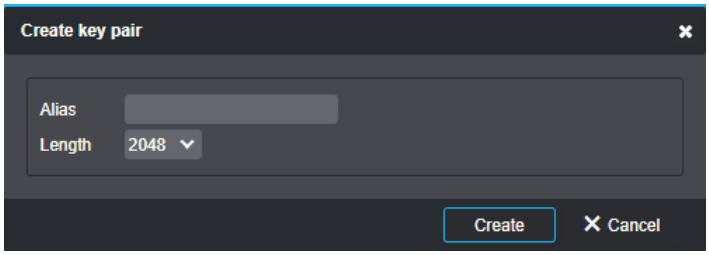

Fig. 10-20

- 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.

INTERFACES

In the **Interfaces** dialog, the built-in physical relay outputs and contact inputs of the device can be configured in the corresponding tabs.

- Click the **Interfaces** menu item in the configuration menu.

11.1 RELAY OUTPUTS

- Select the **Relay outputs** tab.

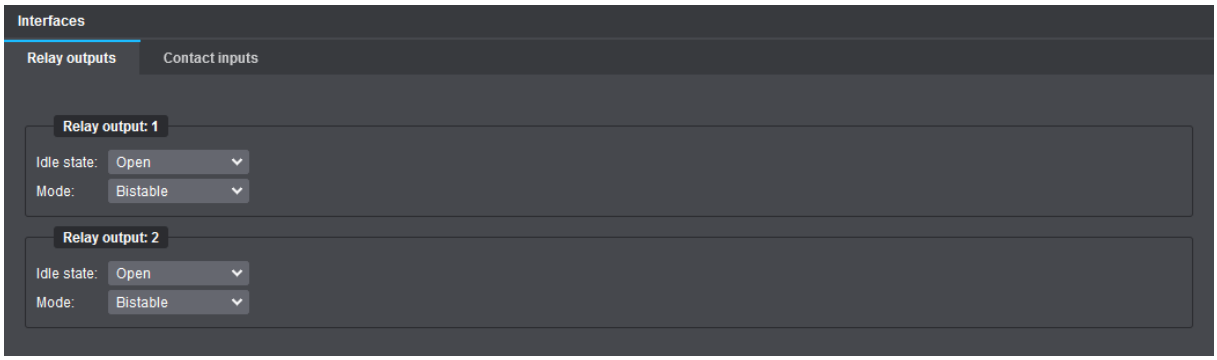

Fig. 11-1

- From the **Idle state** drop-down list, select the required physical idle state (**Open** or **Closed**) for each available relay output.
- From the **Mode** drop-down list, select the required working mode for each available relay output.

A relay output can work in two relay modes:

Bistable
In **Bistable** mode, the state of a relay output only changes when a new event handler is triggered or by a command.

> *If a relay output works in **Bistable** mode and an event handler is created that triggers the relay output to change from the idle state to the active state, a separate event handler must be configured that triggers the relay output to return to its idle state again (see chapter "Event Management" on page 76).*

Monostable

In **Monostable** mode, the state of a relay output only changes for a specified time when an event is triggered.

The **Relay output** dialog is extended by the **Duration** input field, which allows to set a timer in milliseconds (ms).

After the set time has elapsed, the relay output automatically returns to the previously defined **Idle state**.

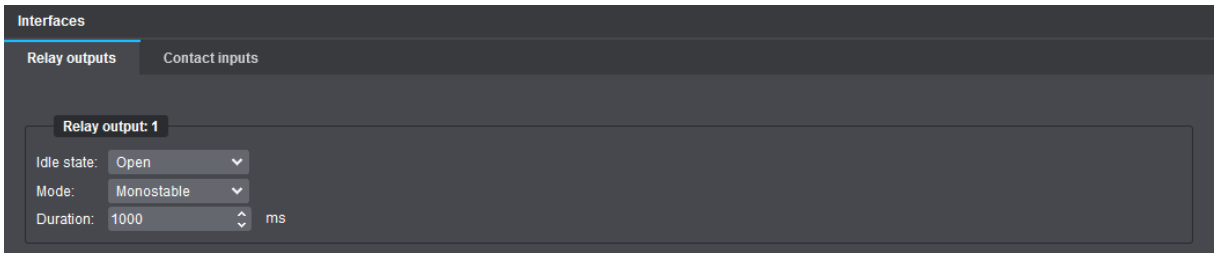

Fig. 11-2

- Enter the required **Duration** in milliseconds (ms) into the corresponding input field.

11.2 CONTACT INPUTS

- Select the **Contact inputs** tab.

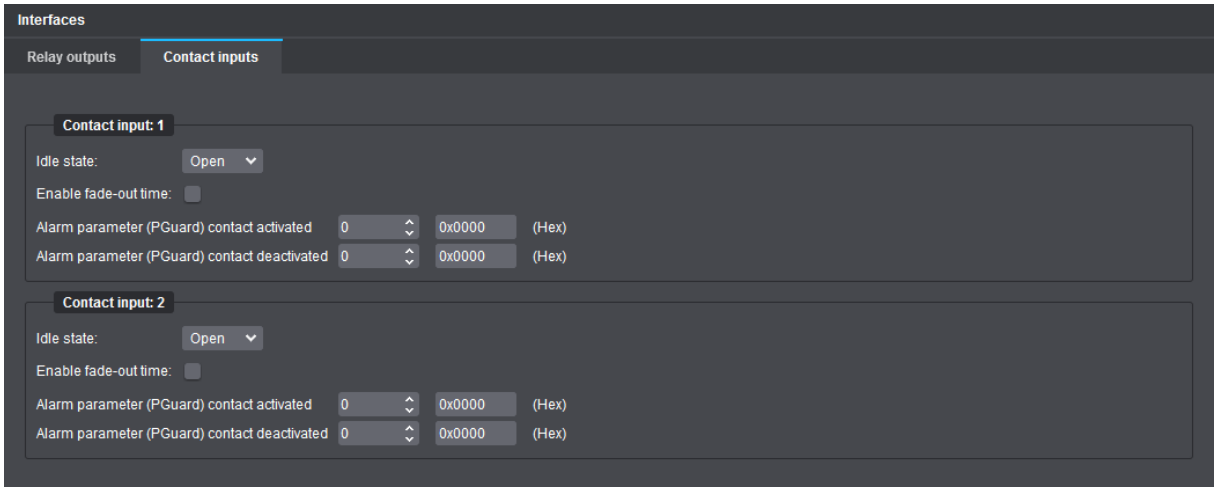

Fig. 11-3

- From the **Idle state** drop-down list, select the required physical idle state (**Open** or **Closed**) for each available contact input.

Enable Fade-out Time

The **Enable fade-out time** function allows you to specify a time delay until the physical change of a contact input's state is handled internally. This can, for example, prevent unwanted event messages from being sent if a contact input is opened and then closed again within a very short time.

► Select the **Enable fade-out time** checkbox if necessary.

The **Duration** input field is displayed.

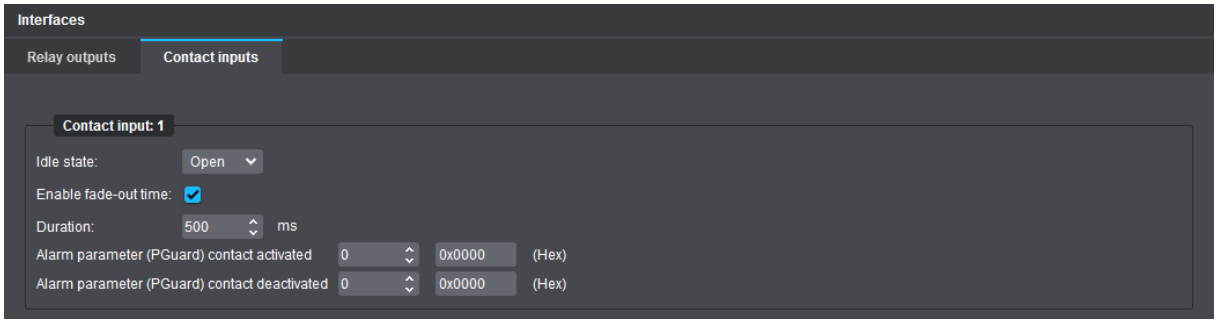

Fig. 11-4

► Enter the required delay time in milliseconds (ms) into the **Duration** input field.

Alarm Parameter (PGuard) Contact Activated/Deactivated

An alarm parameter is a parameter that is sent as additional information to a **Dallmeier Video** (**DaVid**) protocol-capable alarm host (e.g. **PGuard advance** – Dallmeier client software for the evaluation and management of event messages) each time the corresponding physical contact input [1–2] on the device hardware is activated or deactivated (set to the previously defined idle state).

Depending on requirements, a value from **1**–**65535** can be entered as alarm parameter.

For sending alarm parameters when the state of the contact inputs [1–2] changes, you have to configure an event handler of the **DaVid alarm host (PGuard)** action type with the corresponding event trigger **Contact input [1–2] activated/deactivated** (see section "PGuard Messages" on page 93).

EDGESTORAGE

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 to save the recordings and compensate for a network failure without loosing data.

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

► Click the **EdgeStorage** menu item in the configuration menu.

The **EdgeStorage** dialog is displayed.

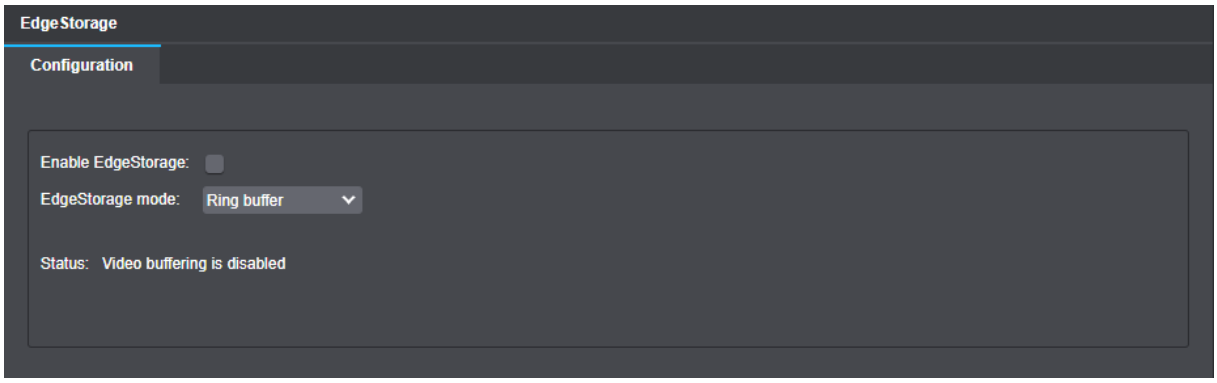

Fig. 12-1

► Select the **Enable EdgeStorage** checkbox.
► Select the **EdgeStorage mode** from the corresponding drop-down list.

The following modes are available:

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

Linear Buffer
Recording stops when the RAM is full.

*Using the **Event management** feature and **PGuard advance**, you can be notified about the **EdgeStorage** status (see chapter "Event Management" on page 76).*

EVENT MANAGEMENT

The **Event Management** of Domera® OS allows you to create various rules that automatically trigger camera actions when a stated condition is “true” (e.g. playing an audio sequence when a person has crossed a virtual line in the captured scene).

A single rule can initiate different camera actions at the same time.

For more complex tasks, multiple conditions can be combined using the logical operators AND or OR, and nested conditions can be expressed using condition groups.

When creating rules, there is no plausibility check on logically combined or nested conditions.

In addition to action rules, the configuration of multiple event handlers is supported to automatically send specific **PGuard messages** based on certain trigger criteria, such as a digital certificate approaching its expiration date.

13.1 RULES

- Click the **Event management** menu item in the main navigation menu to open the corresponding dialog.

The **Rules** tab is displayed.

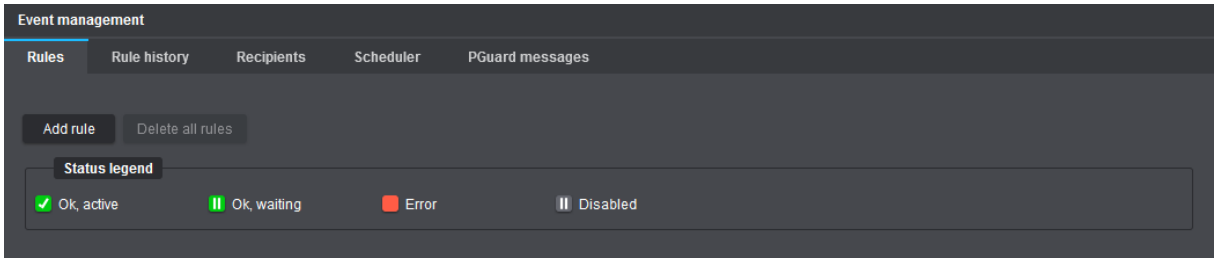

Fig. 13-1

- Click **Add rule**.

All of the user actions that are performed in the following to create rules will always take effect immediately and without any further manual confirmation steps.

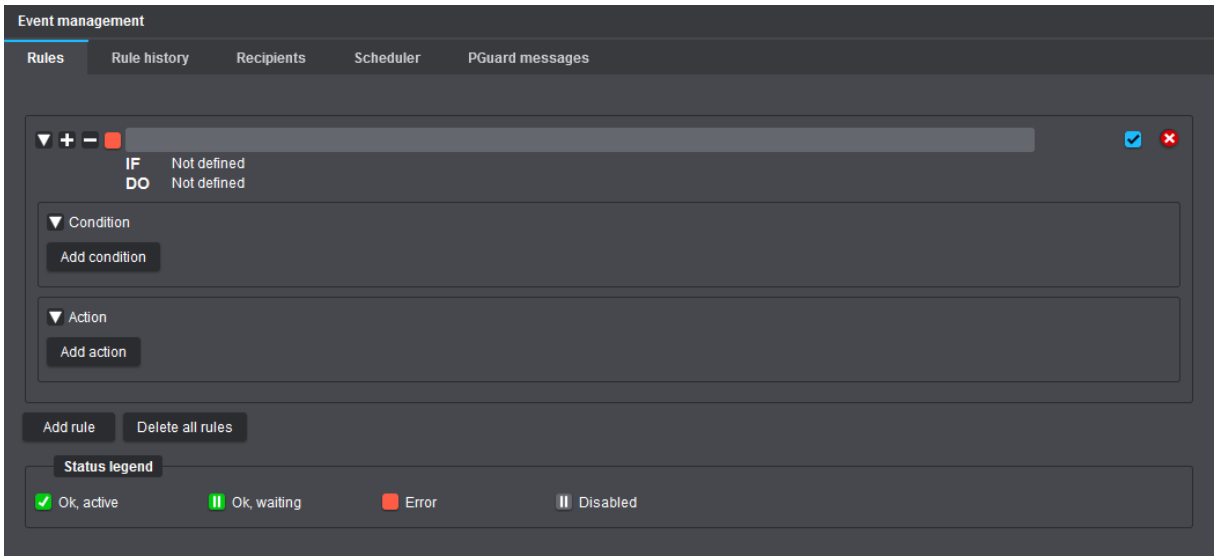

Fig. 13-2

Function Description of Icon Buttons

- Collapse the root node of an item (rule, condition or action)
- Expand the root node of an item
- Expand all tree nodes of a rule (including sub-tree nodes)
- Collapse all tree nodes of a rule
- Delete item

Description of Status Legend

- Single action is configured correctly, or single condition is currently being met (“true”), or entire rule is currently running
- Single condition or entire rule is configured correctly > camera is waiting for the condition to be met (“true”)
- Item is not configured or item is configured incorrectly
- Single condition/action or entire rule is disabled after clearing the corresponding checkbox

- ► Enter a descriptive name for the new rule in the blank input field.
- ► Click **Add condition** and configure the required parameters (see section “Conditions” on page 78).
- ► Click **Add action** and configure the required parameters (see section “Actions” on page 81).

13.1.1 Conditions

As part of a rule, you can define the following *stateless* conditions and the following *stateful* conditions:

Line crossed [“*stateless* condition”]
The condition is met (“true”) exactly once when a new object has crossed the selected virtual line in the captured scene (virtual tripwire).

> *Using the **class filter** allows you to explicitly exclude or include individual object classes as trigger entities, so that the condition is only considered to be “true” for particular object types.*

Intrusion area entered [“*stateless* condition”]
The condition is met (“true”) exactly once when a new object has entered the selected intrusion area in the captured scene either completely or in parts.

> *Using the **class filter** allows you to explicitly exclude or include individual object classes as trigger entities, so that the condition is only considered to be “true” for particular object types.*

Intrusion area exited [“*stateless* condition”]
The condition is met (“true”) exactly once when the object that previously entered the selected intrusion area has left this area again.

> *Using the **class filter** allows you to explicitly exclude or include individual object classes as trigger entities, so that the condition is only considered to be “true” for particular object types.*

Intrusion area occupied by object [“*stateful* condition”]
The condition is met (“true”) as long as there is at least one detected object in the selected intrusion area. The condition is not or no longer met (“false”) if no object is located in the selected intrusion area or if all previously detected objects in the selected intrusion area are either “lost” or become static.

> *Using the **class filter** allows you to explicitly exclude or include individual object classes as trigger entities, so that the condition is only considered to be “true” for particular object types.*

Loitering started [“*stateless* condition”]
The condition is met (“true”) exactly once when a new person remains – either completely or in parts – in the selected loitering area for an unusually long period of time (loitering start event is triggered each time the selected minimum presence dwell-time level has been exceeded).

Loitering ended [“*stateless* condition”]
The condition is met (“true”) exactly once when the person who previously triggered the loitering start event in the selected loitering area has left this area again.

Loitering [“*stateful* condition”]
The condition is met (“true”) as long as at least one person remains – either completely or in parts – in the selected loitering area for an unusually long period of time (after the selected minimum presence dwell-time level has been exceeded).
The condition is not or no longer met (“false”) if no person is present in the selected loitering area or if all previously detected persons in the selected loitering area are “lost”.

Digital input state [“*stateful* condition”]
The condition is met (“true”) as long as the selected contact input (1 – 2) on the camera hardware or the selected virtual input (1 – 4) maintains the specified input state.

Digital input transition [“*stateless* condition”]
The condition is met (“true”) exactly once when the selected contact input (1 – 2) on the camera hardware or the selected virtual input (1 – 4) changes to the specified input state.

Day/Night state [“*stateful* condition”]
The condition is met (“true”) as long as the camera operates in the specified day/night mode.

Day/Night transition [“*stateless* condition”]
The condition is met (“true”) exactly once when the camera switches to the specified day/night mode.

Tamper [“*stateless* condition”]
The condition is met (“true”) exactly once when the camera has detected the selected sabotage action or the selected camera tampering attempt.

EdgeStorage [“*stateless* condition”]
The condition is met (“true”) exactly once for each **EdgeStorage** state that occurs, if selected (see the explanations below):

- **MediumOK**
  Properly working memory card found after camera restart, or
  memory card is working properly again after a temporary card failure during operation.

- **MediumError**
  Memory card unexpectedly removed during operation, or memory card is corrupted.

- **NoMedium**
  No memory card found after camera restart.

- **BufferingStarted**
  Network connection between camera and Dallmeier recording system interrupted > storage (buffering) of audio, video and metadata on memory card started.

- **BufferingFinished**
  Network connection between camera and Dallmeier recording system re-established > storage (buffering) of audio, video and metadata on memory card finished.

- **DeliveringStarted**
  Transfer of stored data from memory card to Dallmeier recording system started (SmartBackfill).

- **DeliveringFinished**
  Transfer of stored data from memory card to Dallmeier recording system finished.

- **BufferFull** (“Linear buffer”)
  Memory card is full > storage (buffering) of any data on memory card stopped.

- **BufferOverwriting** (“Ring buffer”)
  Memory card is full > overwriting of the oldest data on memory card in ring buffer started (again).

Certificate expiry [“*stateless* condition”]
The condition is met (“true”) exactly once when the selected threshold (number of days) prior to the expiration date of a digital certificate is reached.

Service interval [“*stateless* condition”]
The condition is met (“true”) exactly once at each of the following times prior to the expiration date of the software maintenance license for the camera:

- 60 days prior to service interval end date
- 30 days prior to service interval end date
- 0 days prior to service interval end date

Scheduler [“*stateful* condition”]
The condition is met (“true”) as long as the selected scheduler (recurring 7-day weekly planner) is in the state specified here (**Inactive** or **Active**), as defined by its scheduled times and exceptions settings (see section “Scheduler” on page 92).

13.1.2 Actions

As part of a rule, the following camera actions can be initiated:

Digital output
This action changes (*or* maintains) the current physical state of the selected built-in relay output on the camera hardware

- to active state when a *stateless* condition returns “true”.
- to active state when a *stateful* condition returns “true”.
- in active state for as long as a *stateful* condition is “true”.

> *If necessary, enable the **Monostable for stateless** option for “stateless” conditions so that the relay output will automatically return to its idle state after the set time has elapsed.*

- to idle state (inactive) when a *stateful* condition changes from “true” to “false”.
- in idle state (inactive) as long as a *stateful* condition is “false”.

Lighting
This action turns (*or* keeps) the camera’s white-light LEDs

- on for the specified **Duration** (default: 30 seconds) when a *stateless* condition returns “true”.
- on when a *stateful* condition returns “true”.
- permanently turned on for as long as a *stateful* condition is “true”.
- off when a *stateful* condition changes from “true” to “false” and the specified **Duration** has elapsed.

▶ From the **Camera mode** drop-down list, select one of the following three options:

Color
When the white-light LEDs are turned on while the camera is operating in night mode as well as in black-and-white mode, the camera will automatically switch to color mode, even if the actual night-to-day switching threshold has not been reached in that process.
Under certain circumstances, this may cause the camera to frequently switch between the black-and-white mode and the color mode in response to certain conditions.

Black/White
When the white-light LEDs are turned on while the camera is operating in night mode, the camera will continue to operate in black-and-white mode regardless of the presence of visible ambient (white) light, and even if the actual night-to-day switching threshold has already been reached.

Keep current
When the white-light LEDs are turned on, the camera keeps the current mode that results from the ambient light level (amount of visible light) measured at that time and the setting selected from the **Color** drop-down list on the **Day/Night** tab in the **Image** dialog.

▶ If necessary, select the **Flash light** checkbox to use flashing white-light LEDs instead of constant white lighting.

MQTT client

This action sends specially prepared MQTT messages to a dedicated message broker (MQTT server) on your network when a condition returns “true”.

For more information on **MQTT**, see section “Recipients” on page 86.

- ► Select an MQTT recipient host (broker) previously defined on the **Recipients** tab.
- ► In the **Topic** field, enter a UTF-8 character string (e.g. LineCrossed) that the message broker will later use to filter MQTT messages for each connected MQTT client (subscriber) according to a specific topic (topics are case-sensitive).

HEMISPHERE-MQTT client

Depending on the respective condition, this action sends specially prepared MQTT messages with the selected topics (e.g. **People counting**) to the specified ActiveMQ message broker in your **Dallmeier HEMISPHERE®** environment (ASA-MQTT).

For more information on **MQTT**, see section “Recipients” on page 86.

This action can only be used in conjunction with at least one of the following “stateless” conditions:

- ***Line crossed***
- ***Intrusion area entered***
- ***Intrusion area exited***
- ***Loitering started***
- ***Loitering ended***
- ***Tamper***

- ► Select an MQTT broker (ASA) previously defined on the **Recipients** tab.
- ► Select the required MQTT topics to be sent.

HTTP client

This action sends special messages in the form of HTTP requests to the selected web server on your network, or, respectively, to a web application (web service) running on it, when a condition returns “true”. The transmitted HTTP messages can then in turn be used to trigger certain follow-up actions (application tasks) via the URI-addressed web service (e.g. for creating or updating a data record).

For more information on **HTTP**, see section “Recipients” on page 86.

- ▶ Select an HTTP recipient host previously defined on the **Recipients** tab.
- ▶ From the **Method** drop-down list, select the required HTTP request method (**GET**, **PUT**, **POST**).
- ▶ Enter the path to the running web service, followed by the appropriate query part, such as:

```
/api/CreateEvent?Ressource=CameraEvent&type=LineCrossed
```

*To find out the correct HTTP request method (**GET**, **PUT**, **POST**), as well as the exact path and query part, refer to the documentation for the web service you are using.*

Audio output

This action starts (*and* optionally repeats) playback of a selected audio sequence uploaded to the camera,

- when a *stateless* condition returns “true”.
- when a *stateful* condition returns “true”.
- for as long as a *stateful* condition is “true” (only if **Repeat audio sequence** is enabled).

A started audio sequence is always output in full length (regardless of its total playing time), even if a condition returns “false” again during audio playback.

- ▶ Note the explanations for each audio output parameter on the following page and configure the required settings.

Minimum repetition time
This parameter determines the time in seconds that must elapse after the selected audio sequence has been played back completely before other conditions within the rule that are evaluated as being met ("true") are taken into account in order to play back the same audio sequence again.

Example:
Condition = **Line crossed** OR **Intrusion area entered**; minimum repetition time = **10 seconds**

1. Person 1 crosses virtual line > Audio sequence is played back to its end >
   Minimum repetition time of **10 seconds** starts counting down after the end of the audio output.
2. Person 2 crosses virtual line at **5 seconds** after audio output >
   Audio sequence is ***not*** played back.
3. Car 1 enters intrusion area after another **3 seconds** period >
   Audio sequence is ***not*** played back.
4. Person 3 crosses virtual line at **11 seconds** after audio output >
   Audio sequence is played back again to its end >
   Minimum repetition time of **10 seconds** starts counting down again after second audio output.
5. Car 2 enters intrusion area after another **3 seconds** period >
   Audio sequence is ***not*** played back.
6. Car 3 enters intrusion area at **11 seconds** after second audio output >
   Audio sequence is played back again to its end.

Repeat audio sequence
This parameter is only effective for *stateful* conditions and determines whether the selected audio sequence should be played repeatedly ("looping audio") until the given *stateful* condition is no longer met ("true") i.e. returns "false" again.
The **Repetition time** defines the length of the pause between the end of a completed audio sequence and its restart.

Suppress short conditions
This parameter, if enabled, defines the minimum time that a condition must be met ("true") before the selected audio sequence is actually played. In this case, all *stateless* conditions are suppressed and *stateful* conditions must be met ("true") for at least the time specified by the **Suppression interval** to start playing the audio sequence.

DaVid notification
This action sends a DaVid message in the form of a selectable (and later internally used) notification ID to a system that has actively connected to the camera via the DaVid protocol (e.g. a Dallmeier recording system).
The DaVid protocol-capable system connected to the camera can then in turn be set up to initiate certain follow-up actions based on incoming DaVid notification IDs and the associated names (e.g. changing the physical state of an existing hardware relay output on the Dallmeier recording system).

// Setup example on Dallmeier recording system **IPS 10 000 MK2** //
Recorder main menu > **Interfaces** > **Relay OUT** > Select relay number from dedicated drop-down list > Select **Camera event with timer** option from **Function** drop-down list > Add Domera® OS camera > Select relevant names of **Notification events**.

Email

Subject to the specified condition, this action sends corresponding event notifications as email messages via the Simple Mail Transfer Protocol (SMTP) or Extended SMTP (ESMTP) to one or more registered email recipients using the selected email account.

For information on how to define an email account to use for sending event notifications, see section "Recipients" on page 86.
If you have set up multiple email accounts on the **Recipients** tab, you can select which account to use when sending email messages.

- Select an **Account** previously defined on the **Recipients** tab to use for sending the rule-based email notifications.
- In the **To** field, enter the recipient(s) of the email message.

> *Separate multiple email recipients with a space, a comma, a semicolon, or a line break.*

- Enter **Subject** and **Text** of the email message.

The following variables are supported in the email body, in addition to any custom plain text:

- **{rule}**
  Name of the rule that is currently running
- **{event}**
  Triggering event within the rule (the condition that was met / that has returned "true")
- **{hostname}**
  Host name of the camera (see **Network** dialog > **Basic settings** tab)
- **{ip}**
  IP address of the camera
- **{cameraName}**
  Name of the camera (see **General settings** dialog)
- **{location}**
  Location of the camera (see **General settings** dialog > **Location** tab)
- **{timestamp}**
  Time stamp of the event

- If required, select the **Attach picture** checkbox to attach the last live image captured when the event was triggered to the email message.

> *Use the **Test** button to validate all entries you have made before applying the rule in live camera operation.*

13.2 RULE HISTORY

The **Rule history** tab lists all rules by date and time that the camera has executed in response to a stated condition being met.

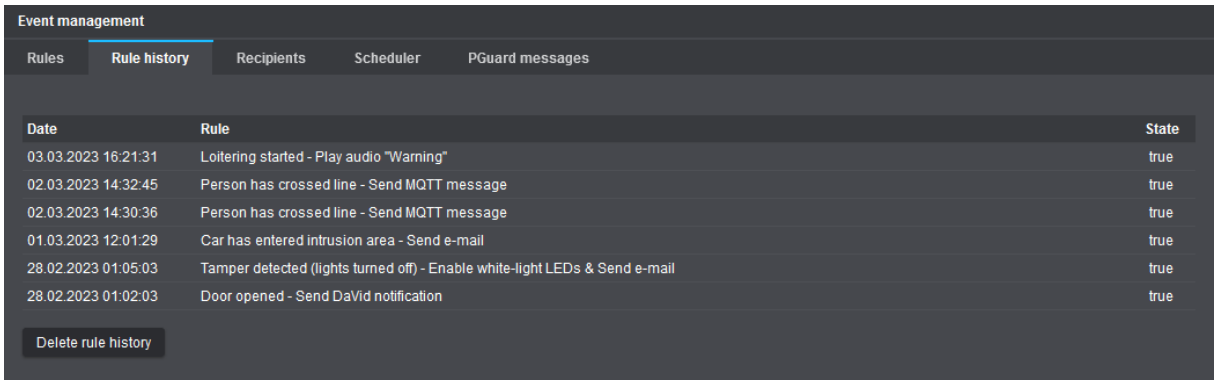

Fig. 13-3

13.3 RECIPIENTS

On the **Recipients** tab, you can define one or more **HTTP**, **MQTT**, **ONVIF-MQTT** and **Email** recipients that will handle the generated camera events according to the selected action type and its underlying communication protocol.

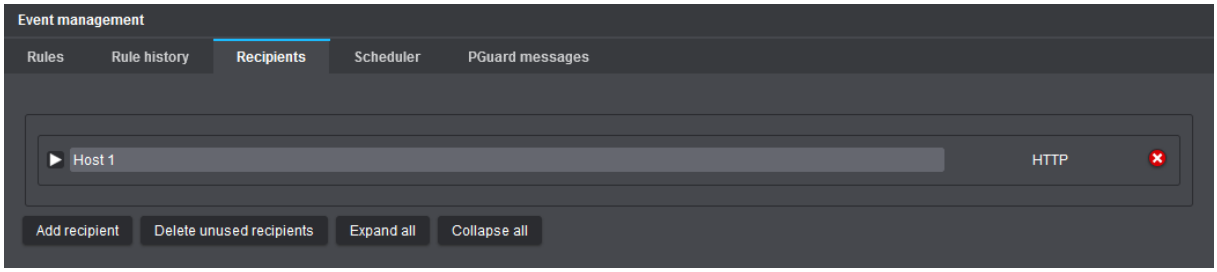

Fig. 13-4

- First, note the explanations for each recipient type on the following pages.
- Click **Add recipient**.
- Select the required recipient type from the **Recipient** drop-down list, and then click **OK** to confirm.
- Configure the required parameters for each of your recipients.

Recipients currently being used by a rule cannot be deleted.

13.3.1 HTTP

This type of recipient allows you to specify an HTTP server on your network that will receive the HTTP requests generated by the camera and deliver them to the corresponding web application (web service) via standard port 80 (in case of an unencrypted connection using HTTP) or via standard port 443 (in case of an encrypted TLS connection using HTTPS).

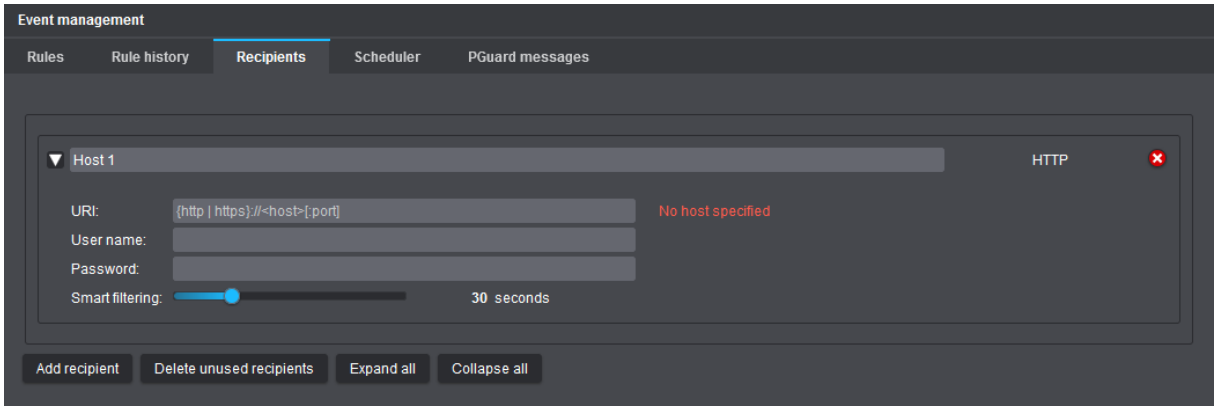

Fig. 13-5

- Enter a descriptive name for the HTTP recipient host in the designated input field (top section).
- In the **URI** field, enter the address (according to the following syntax) used to access your web service on the network:

  - Scheme/type of protocol (http or https) to be used for communication between the camera and the web server; followed by a colon (:)
  - Host of the machine/computer or web server running your web service; preceded by two slashes (//): This can be either the IP address or, if you have specified available DNS servers for resolving host names (mapping host names to IP addresses) in the camera's network settings, the Fully Qualified Domain Name (FQDN) of the web server, such as web1.example.com
  - Port number, preceded by a colon (:), on which the web service is listening for incoming HTTP requests (only optional if other than the standard HTTP port 80 or the standard HTTPS port 443)

  Example for unencrypted connection (**http**) using non-standard port **8080**:

  ```
  http://192.0.2.1:8080
  ```

  Example for encrypted TLS connection (**https**) using non-standard port **8443**:

  ```
  https://192.0.2.1:8443
  ```

  The mentioned IP address is only exemplary and must be replaced with the IP address or the FQDN of the web server running your web service.

- If client authentication is required to access your web service, enter the authentication credentials in the **User name** and **Password** fields.

Smart filtering (default: 30 seconds)
This parameter determines the time in seconds that must elapse after an HTTP request has been sent before any other conditions within rules that are evaluated as being met ("true") are taken into account in order to send a new generated HTTP request (this parameter works in the same way as outlined in the example for the **Minimum repetition time** of the **Audio output** camera action; see section "Minimum repetition time" on page 84).

13.3.2 MQTT

This type of recipient allows you to specify a so-called message broker (or MQTT server) available on your network. The MQTT server, as a central intermediary, first receives the MQTT messages from the camera (publishing client), then internally filters the messages according to the specified topic (on which the messages are to be published) and finally transmits the available data and information to all those MQTT clients (subscribers) in the network that have previously subscribed to exactly the same topic defined in the camera at the MQTT server.
MQTT (Message Queuing Telemetry Transport) is based on the publish-subscribe model. Thus, in machine-to-machine (M2M) communication, there is no direct connection between the individual IoT devices (the abbreviation “IoT” stands for “Internet of Things”).
MQTT messages are transmitted over TCP/IP using the default port 1883 for an unencrypted connection or the default port 8883 for an encrypted TLS connection (depending on the configuration of your MQTT server).

Using event-triggered MQTT messages, the following application scenarios are conceivable, for example:

- Automated creation of analytics dashboards based on MQTT topics and the underlying data (telemetry events) for the graphical visualization of **EdgeAnalytics** events generated by the camera
- Triggering actions on another IoT device (subscriber) on your network if the data in the MQTT topic sent by the camera (publisher) contains a certain value

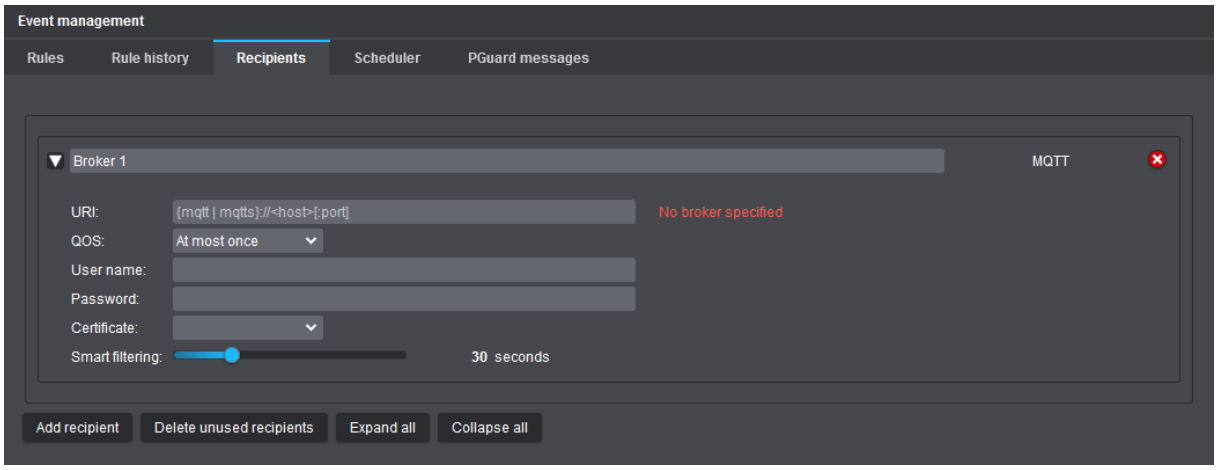

Fig. 13-6

- ▶ Enter a descriptive name for the MQTT recipient host in the designated input field (top section).
- ▶ In the **URI** field, enter the destination IP address of your MQTT server (scheme/protocol and IP address of the computer running the MQTT messaging server application) and the port number, preceded by a colon (:), on which the MQTT service is listening for incoming client connections (see examples below):

  Example for unencrypted connection (**mqtt**) using default port **1883**:

  ```
  mqtt://192.0.2.2:1883
  ```

  Example for encrypted TLS connection (**mqtts**) using default port **8883**:

  ```
  mqtts://192.0.2.2:8883
  ```

  The mentioned IP address is only exemplary and must be replaced with the IP address of the computer running your MQTT broker.

- From the **QoS** drop-down list, select one of the following QoS levels (Quality of Service level or level of reliability for message delivery to the broker):

  - **At most once** (QoS level 0 – At most once delivery; “fire and forget”; default setting):
    - Guarantees that the camera sends the MQTT message only once, but the delivery is not acknowledged by the broker
    - No guarantee that the message from the camera is delivered successfully to the broker
    - No retry of message delivery by the camera (e.g. in case the broker is temporarily unavailable), as the message is not stored on the camera after sending (“fire and forget” method)
    - No creation and delivery of duplicates of the original message
    - Fastest QoS level (best-effort delivery) with the lowest utilization of resources, but also the most unreliable MQTT messaging transfer method

  - **At least once** (QoS level 1 – At least once delivery; acknowledged delivery):
    - Guarantees that the MQTT message from the camera is delivered to the broker at least once
    - The message is first provided with a unique message number (packet identifier), then stored locally on the camera (outbound queue) and finally resent at regular intervals until the broker acknowledges the message delivery with a so-called PUBACK packet including the matching packet identifier
    - Transmission of duplicates of the original message possible (e.g. in case the acknowledgement of the MQTT server was previously lost due to network bottlenecks)
    - Best compromise between the reliability of MQTT message delivery and the utilization of resources

  - **Exactly once** (QoS level 2 – Exactly once delivery; assured delivery):
    - Guarantees that the MQTT message from the camera is delivered to the broker exactly once
    - Delivery guarantee is realized by at least four-step handshake between camera and broker
    - Most reliable method of MQTT message delivery, but also the most resource-intensive and slowest QoS level due to a relatively high overhead

  Note that the QoS level set on the camera must also be supported by your MQTT broker.

- If client authentication is required to establish a connection to the message broker, proceed as follows:

  In the **User name** and **Password** fields, enter the authentication credentials for accessing the MQTT server and/or additionally/alternatively select a valid client authentication certificate stored on your camera from the **Client certificate** drop-down list (must be provided by the broker and imported into the camera’s keystore beforehand).

  The individual procedure for authenticating to the broker depends on the configuration of your MQTT server.
  Note that MQTT authentication credentials (user name and password) are transmitted in plain text in the case of an unencrypted connection.

The **Smart filtering** feature works in the same way as the identically named parameter for the **HTTP** recipient type (see section “HTTP” on page 87).

13.3.3 ONVIF-MQTT

This type of recipient is an embedded, fully independent MQTT publishing client on the camera that, once configured, runs as a standalone background process and follows the guidelines of the ONVIF*) specification (ONVIF Profile M) for processing analytics metadata.
As soon as a connection to the specified MQTT broker has been successfully established over the network, the ONVIF MQTT publishing client on the camera starts receiving all **EdgeAnalytics** events generated by the camera (intrusion, line crossing, loitering, etc.) for outbound processing, then automatically tags the individual data elements with the appropriate topics, and finally sends them as special (ONVIF compliant) MQTT messages to the connected MQTT broker.
Note that this type of recipient cannot be explicitly selected within rules for MQTT camera actions, but instead runs as a standalone process (ONVIF MQTT publishing service) on the camera once the mandatory fields are correctly configured.

*) Note the information on the trademark owner given in the copyright and trademark notice on page 2.

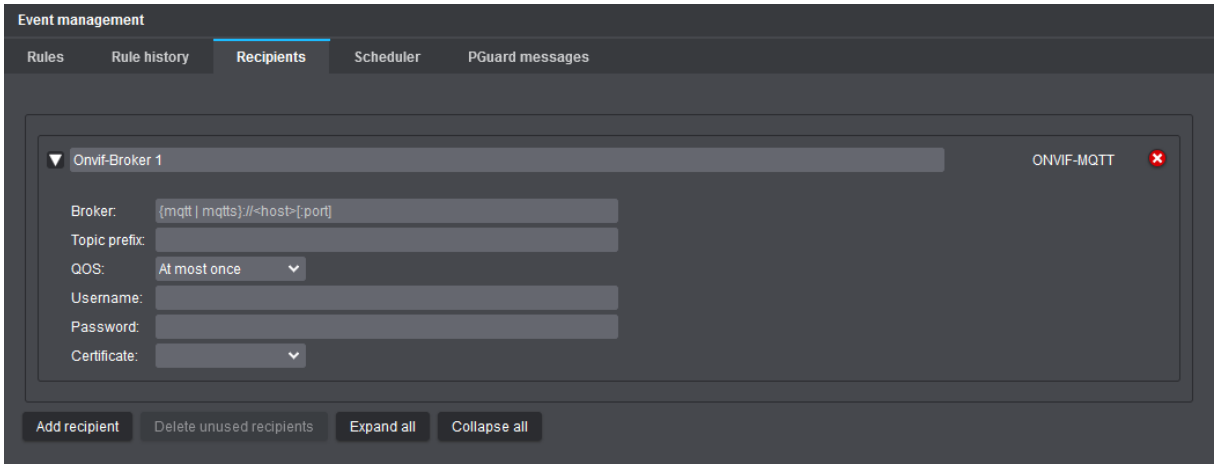

Fig. 13-7

The configuration dialog for connecting to an existing ONVIF MQTT broker in your network is very similar to the one for the **MQTT** recipient type as described in section “MQTT” on page 88.
In this context,the **Broker** field is identical to the corresponding **URI** field.

Topic prefix
The so-called **Topic prefix** is used to identify the camera within a published (**EdgeAnalytics**) topic.
Note that this identifier must be unique, otherwise MQTT clients (subscribers) will receive incorrect data or the MQTT broker may reject the connection.
For example, use either the camera name (without any blank spaces) or the camera’s IP address, making sure that the topic prefix (identifier) exists only once in your global MQTT environment.

13.3.4 EMail

This type of recipient allows you to specify an email account that will receive the email messages generated by the camera for delivery to the email recipient(s) added in your custom rule.

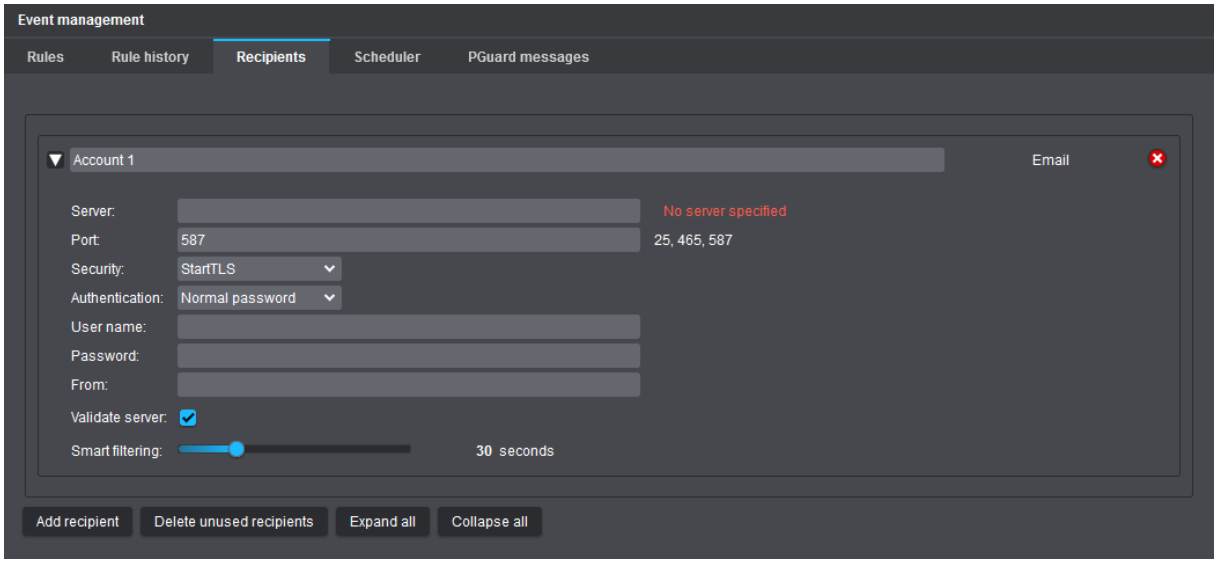

Fig. 13-8

- Enter a descriptive name for the email account in the designated input field (top section).
- In the **Server** field, enter the IP address of the computer or mail server that processes your outgoing mail (SMTP) or, if you have specified available DNS servers for resolving host names (mapping host names to IP addresses) in the camera's network settings, the Fully Qualified Domain Name (FQDN) of your mail server, such as mx1.example.com.
- In the **Port** field, enter the port number on which your outgoing (SMTP) mail server is listening for inbound SMTP connections (SMTP default port: **25**, **456**, or **587**).
- From the **Security** drop-down list, select a method to secure authentication credentials and email messages in transit, such as a certificate-based encrypted connection using **STARTTLS** (port **587**) or a certificate-based encrypted connection using **SSL/TLS** (port **465**).
- If authentication to the mail server is required, enter the authentication credentials in the **User name** and **Password** fields.
- In the **From** field, enter the email address to use as the "From" address for email messages generated by the camera.
- If validating your mail server's certificate is not applicable/required, clear the **Validate server** checkbox. During mail server validation, the client verifies that the SSL/TLS certificate provided by the server is valid before actually sending the email. A server certificate is invalid if, for example, it has expired, the certification path is invalid (the chain of trust is incomplete or contains certificates that cannot be verified), or the host name or FQDN of the mail server entered above does not match the host name specified in the certificate.

> *The correct settings depend on the configuration of your mail server. If necessary, contact your network administrator or your email provider for more information and assistance.*

The **Smart filtering** feature works in the same way as the identically named parameter for the **HTTP** recipient type (see section "HTTP" on page 87).

13.4 SCHEDULER

The **Scheduler** tab allows you to create various schedules (recurring 7-day weekly planners) that can then be used as rule conditions that must be met before a particular camera action is triggered.

> *Unless exceptions are specified for specific calendar days, the respective 7-day weekly planner will always apply throughout the year (and for future calendar years).*

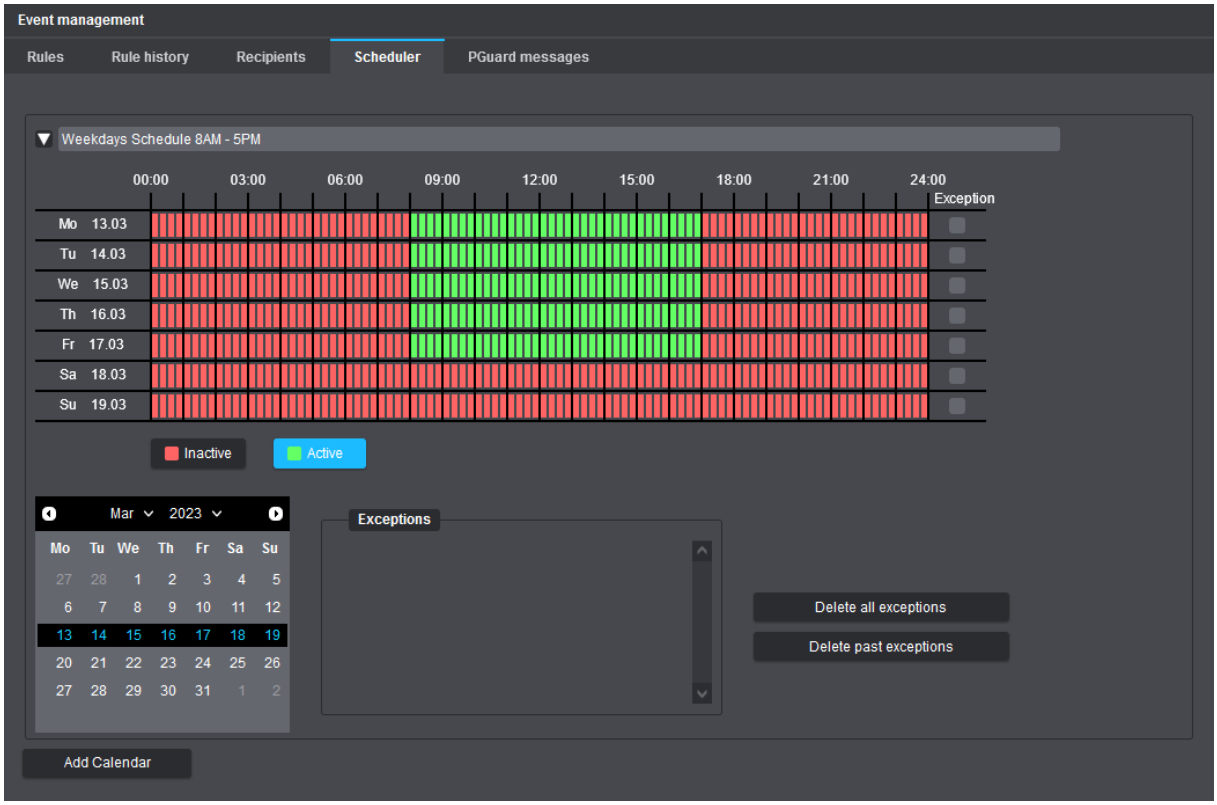

Fig. 13-9

- Enter a descriptive name for the recurring weekly schedule in the designated input field (top section).
- Click on the **Inactive** (red) or **Active** (green) button as required and select the relevant time ranges in the weekly schedule while holding down the left mouse button (the smallest selectable time range is 15 minutes).

In the example above (Fig. 13-9), a recurring weekly schedule was created that is set to be active on weekdays from 8:00 AM to 5:00 PM (written as 17:00 in 24-hour notation) throughout the year (no exceptions). Later, when you add a defined recurring weekly schedule as a condition to a rule, you can specify whether the camera initiates actions only during the active time periods or only during the inactive time periods. You can create multiple schedules, for example, one for weekdays and one for weekends, each with exceptions for certain calendar days, such as public holidays, annual vacation close-down, or times when maintenance and service tasks are scheduled.
To add exceptions, first select the intended day in the provided calendar, select the **Exception** checkbox to the right of the time block for the calendar day, and then customize the time range as needed.

13.5 PGUARD MESSAGES

13.5.1 Create Event Handler

On the **PGuard messages** tab, you can define various event handlers that automatically send predefined **PGuard messages** via the **Dallmeier Video** (**DaVid**) protocol to a registered alarm host (PGuard) when a specified event is triggered.

> *For the evaluation and management of the sent **PGuard** event messages, the Dallmeier software **PGuard advance** must be installed and running on the respective client PC (alarm host).*

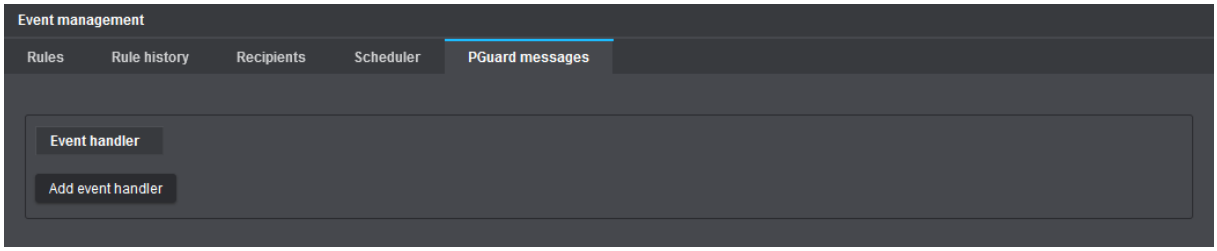

Fig. 13-10

- Click **Add event handler** to open the corresponding dialog.

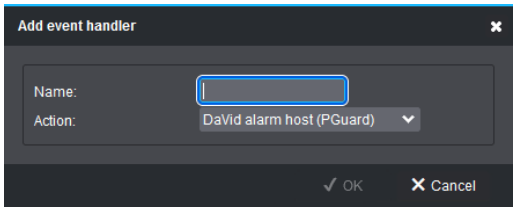

Fig. 13-11

- In the **Name** input field, enter a descriptive and unique name for the new event handler.
- Click **OK** to confirm.

The new event handler is then created and can now be configured (see below).

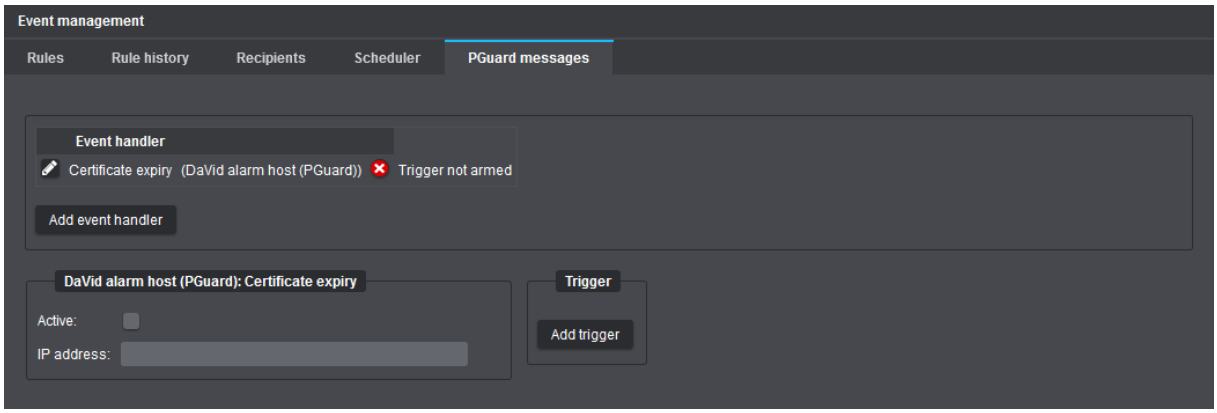

Fig. 13-12

- First, make sure that your camera and the respective alarm host are located in the same LAN or can communicate with each other via a gateway.
- Enter the **IP address** of the alarm host to which the **PGuard messages** are to be sent in case of a specified event.
- Click **Add trigger** to open the **Add event trigger** dialog.

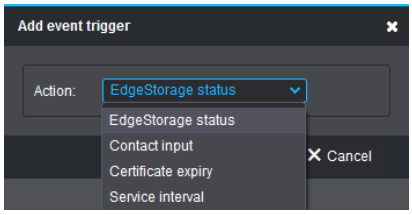

Fig. 13-13

- From the **Action** drop-down list, select an event trigger (see below).

The following event triggers are currently available (for detailed descriptions, see sections below).

- **EdgeStorage status**
- **Contact input**
- **Certificate expiry**
- **Service interval**

- Click **OK** to confirm.
- Configure the trigger parameters, if existing.
- Add additional event triggers to the event handler if required.
- Select the **Active** checkbox to enable the event handler.

EdgeStorage Status

This event trigger sends a **PGuard message** to the alarm host whenever the **EdgeStorage** status changes (see chapter "EdgeStorage" on page 75).

The following status changes are sent via the **DaVid** protocol:

- **MediaOK**
  Properly working memory card found after camera restart, or
  memory card is working properly again after a temporary card failure during operation.

- **MediaErr**
  Memory card unexpectedly removed during operation, or memory card is corrupted.

- **NoMedia**
  No memory card found after camera restart.

- **Buffering**
  Network connection between camera and Dallmeier recording system interrupted > storage (buffering) of audio, video and metadata on memory card started.

- **NoBuffering**
  Network connection between camera and Dallmeier recording system re-established > storage (buffering) of audio, video and metadata on memory card finished.

- **Delivering**
  Transfer of stored data from memory card to Dallmeier recording system started (SmartBackfill).

- **NoDelivering**
  Transfer of stored data from memory card to Dallmeier recording system finished.

- **BufferFull** ("Linear buffer")
  Memory card is full > storage (buffering) of any data on memory card stopped.

- **BufferOverwriting** ("Ring buffer")
  Memory card is full > overwriting of the oldest data on memory card in ring buffer started (again).

Contact Input

This event trigger sends a **PGuard message** to the alarm host whenever the corresponding **Contact input 1** or **Contact input 2** on the camera hardware is physically activated or deactivated (set to its idle state).

Detailed descriptions on how to configure the contact inputs of your camera can be found in the section "Contact Inputs" on page 73.

Certificate Expiry

This event trigger sends several **PGuard messages** to the alarm host before an existing TLS certificate on the camera expires. The messages are sent at intervals of 30, 10, 5, 3, 2, 1 and 0 days before expiry of a TLS certificate.

Service Interval

This event trigger sends several **PGuard messages** to the alarm host before the camera's service interval expires. The messages are sent at intervals of 60, 30 and 0 days before expiry of the service interval.

> *Details about the expiration date and time of your camera's software maintenance license currently in use (**Service interval end**) can be found in the **Information** dialog on the **General Information** tab (see section "General Information" on page 142).*

13.5.2 Edit Event Handler

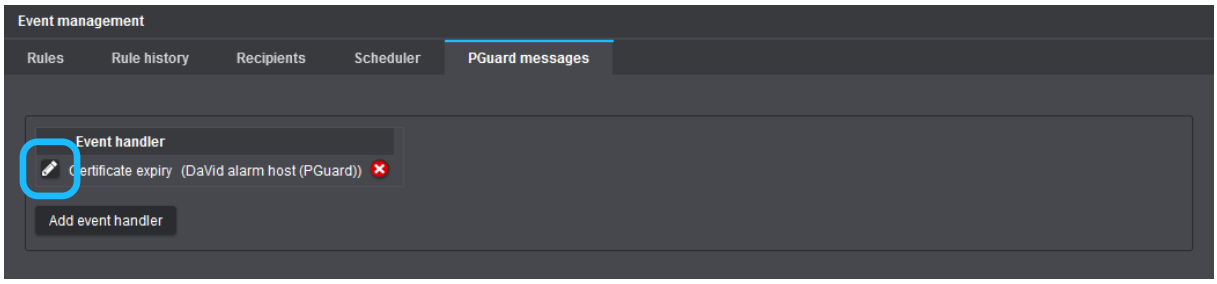

Fig. 13-14

- To edit a stored event handler, click the **Pencil** icon button to the left of the event handler name.
- Edit the required settings in the displayed configuration dialog.

13.5.3 Delete Event Handler

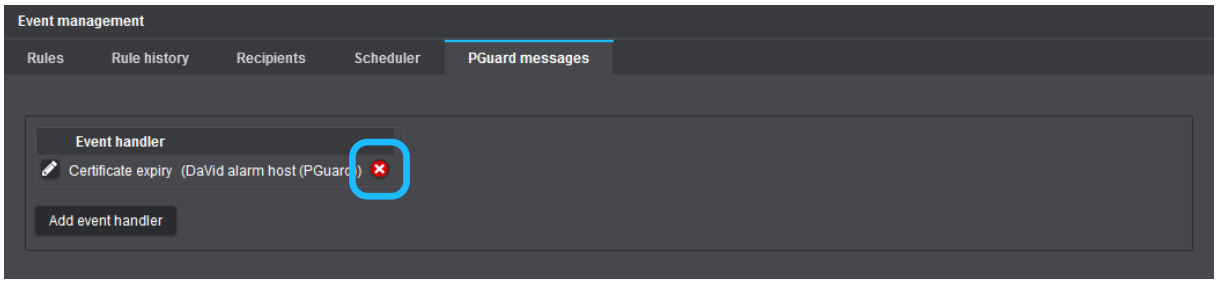

Fig. 13-15

- To delete a stored event handler, click the **Delete** icon button (red circle with a white cross) to the right of the event handler action type.
- Click **OK** to confirm.

DATA DISPLAY

The **Data display** function allows you to embed external transaction data or other monitoring information into the video stream.
External data can be transmitted directly to the camera by cash registers, automated teller machines (ATMs), access control systems, casino systems (e.g. slot machines) or other monitoring applications using the Dallmeier Video (**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 evaluation with **SeMSy® Compact**).
Before embedding external data into the video stream, the received data can be filtered. In addition, you can specify the position of the text overlay directly in the video.

NOTICE

Video text overlay failure due to incompatible hardware

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

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

In conjunction with the above-mentioned devices, the embedded data is displayed directly in the live video on a connected 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

14.1 DURATION

▶ Click **Data display** > **Display**.

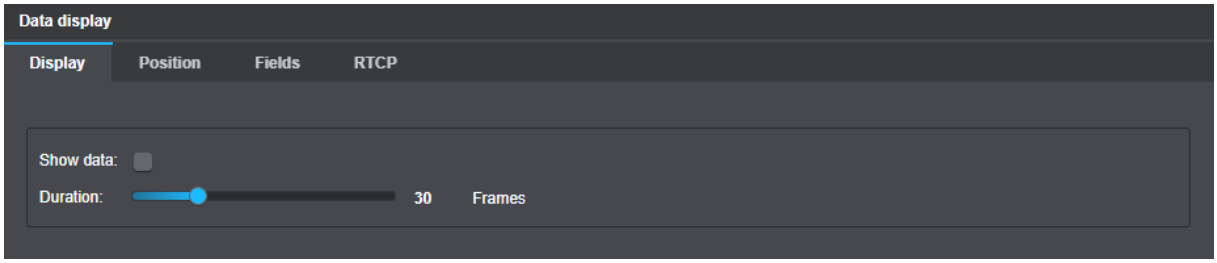

Fig. 14-1

▶ Select the **Show data** checkbox to enable the data display.
▶ Select 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).

14.2 POSITION

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

▶ Click **Data display** > **Position**.

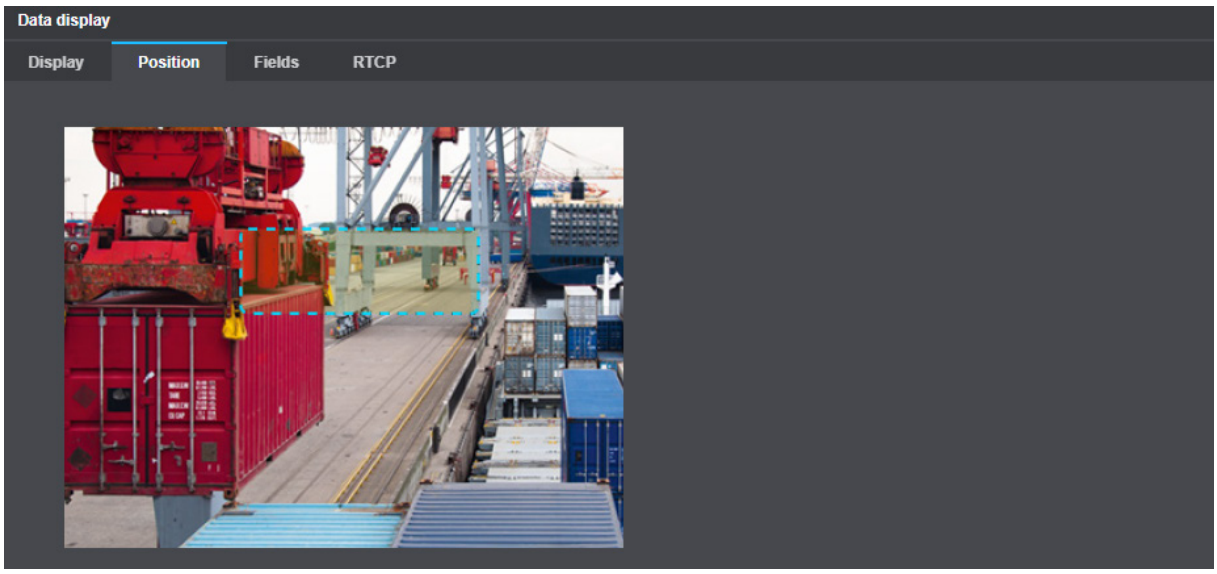

Fig. 14-2

▶ Select the display area by dragging a rectangle.

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

14.3 FIELDS

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

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

▶ Click **Data display** > **Fields**.

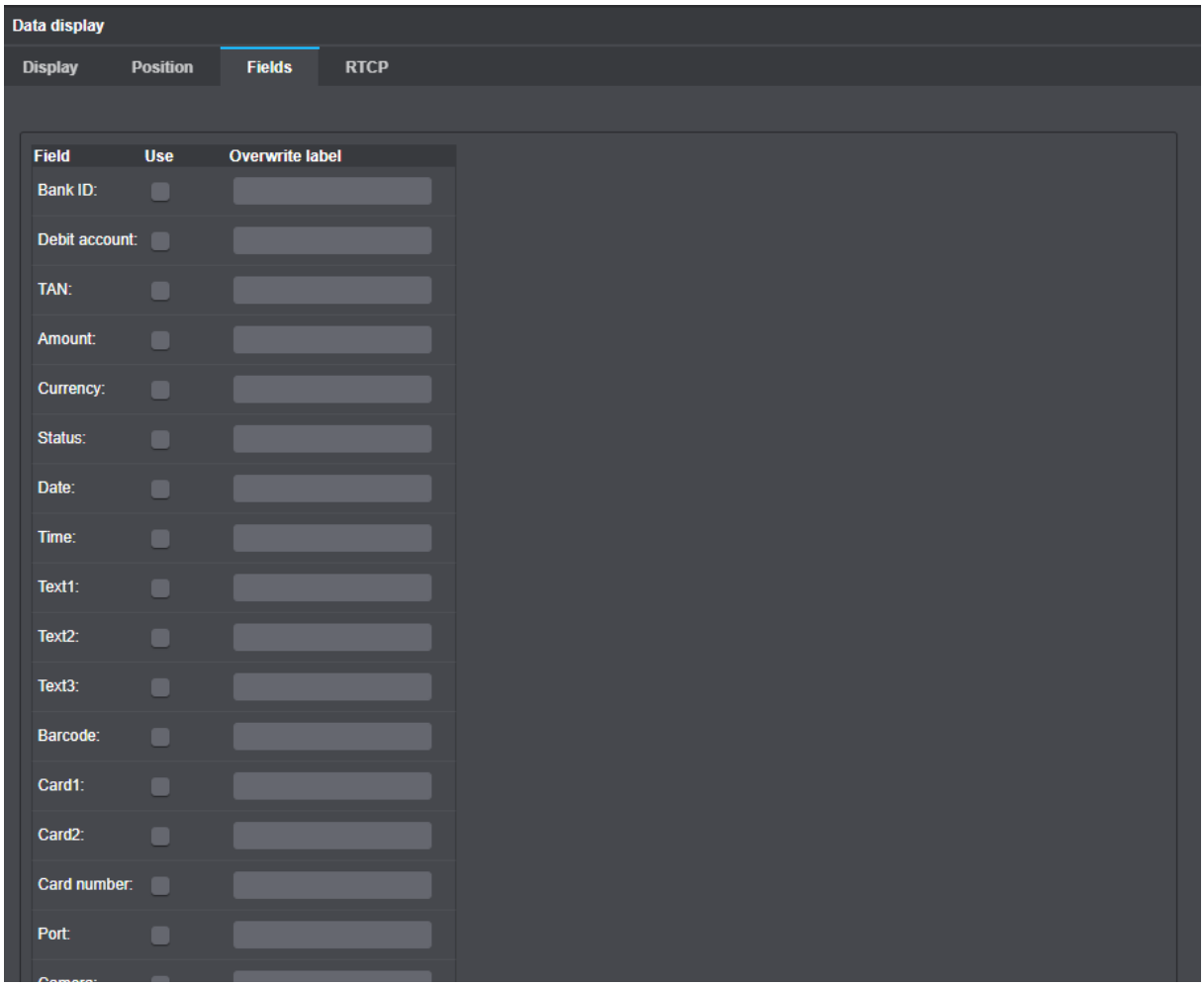

Fig. 14-3

▶ Enable the display of the relevant data by selecting the related checkboxes.

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

> *If streaming over RTCP is activated (network setting) the transmission of data over RTCP has to be activated as well (**Data display** > **RTCP**).*

EDGE ANALYTICS & AI APPS

With Domera® OS, two fundamentally different solutions and approaches for analyzing video content directly on the camera are available by default (depending on the camera model) on the basis of so-called **EdgeAnalytics** applications.

VCA Motion Detection -> see "VCA Motion Detection" on page 103
Conventional motion detection of objects with only basic object classification (this **EdgeAnalytics** technique is usually enabled by default).

EdgeAnalytics AI Object Detection App -> see "Edge Analytics AI Object Detection App" on page 116
AI-based object detection (independent of movements in the image) with advanced, high-precision object classification based on state-of-the-art deep learning techniques and a previously intensively trained artificial neural network (after a 30-day trial period, the purchase of a valid license code is required for the further use of this **EdgeAnalytics** technique)

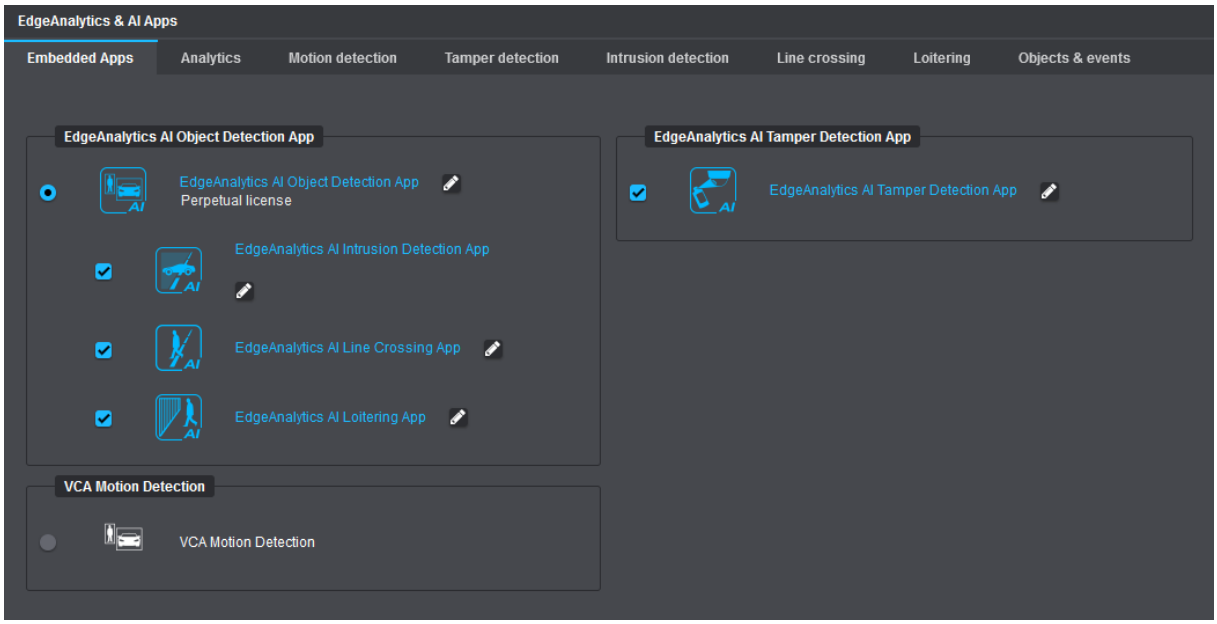

Fig. 15-1

Depending on the requirements, various additional analytics applications can be enabled on the camera, each working on the basis of the generated analytics data of the previously selected main **EdgeAnalytics** technique (see below).

*For best possible analytics results even in challenging scene conditions, the use of the **EdgeAnalytics AI Object Detection App** with AI-based object detection and advanced object classification is recommended.*

In conjunction with **VCA Motion Detection** for conventional motion detection of objects with virtual motion tracking and basic object classification, the following additional analytics applications can be enabled and then customized on the corresponding tabs:

- **VCA Intrusion Detection** -> see "Intrusion Detection" on page 121
  Automatic generation of events as soon as detected objects enter or leave user-definable sensitive areas in the image; can be used, for example, for building and site protection of critical infrastructures or for securing premises and other restricted outdoor areas

- **VCA Line Crossing** -> see "Line Crossing" on page 123
  Automatic generation of events as soon as detected objects cross user-definable virtual lines in the image (virtual tripwire); can be used, for example, for perimeter protection (fence monitoring, protection against climbing)

In conjunction with the **EdgeAnalytics AI Object Detection App** for AI-based object detection with advanced, high-precision object classification, the following additional analytics applications can be enabled by default and then customized on the corresponding tabs:

- **EdgeAnalytics AI Intrusion Detection App** -> see "Intrusion Detection" on page 121
  Automatic generation of events as soon as detected objects enter or leave user-definable sensitive areas in the image; can be used, for example, for building and site protection of critical infrastructures or for securing premises and other restricted outdoor areas

- **EdgeAnalytics AI Line Crossing App** -> see "Line Crossing" on page 123
  Automatic generation of events as soon as detected objects cross user-definable virtual lines in the image (virtual tripwire); can be used, for example, for perimeter protection (fence monitoring, protection against climbing)

- **EdgeAnalytics AI Loitering App** -> see "Loitering" on page 125
  Automatic generation of events as soon as persons remain for an unusually long (adjustable) period of time in user-definable image areas; can be used, for example, for securing buildings and access (entry and exit) points

EdgeAnalytics AI Tamper Detection App -> see "Tamper Detection" on page 127

Regardless of the main **EdgeAnalytics** technique previously selected, the additionally provided **EdgeAnalytics AI Tamper Detection App** offers special analytics and event processing features that can automatically detect the following sabotage actions or camera tampering attempts if required:

- **Lights off/on** detection as soon as the average intensity of illumination in the captured scene abruptly changes, such as in the case of:

  - a sudden change in brightness level of the ambient light (due to sabotage of a light source)
  - spraying or covering the camera or dome bubble
  - blinding of the lens or image sensor by an external very bright light source (e.g. a laser beam)

- **Image too blurry** (e.g. due to fogging of the camera or unauthorized defocusing)

- **Global scene change** (e.g. due to turning or covering the camera)

Storage, further processing and evaluation of camera analytics data

The generated camera analytics data (detected objects, identified object classes, motion events, detected sabotage actions or camera tampering attempts, etc.) is sent in the form of metadata (additional information added to the video data, such as the position and orientation of a detected object, the object type, the direction of motion as well as the timestamp of the event) in real-time to the respective Dallmeier recording system for storage and further processing.

For the correct storage, further processing and later evaluation of the generated camera analytics data, the following points must be observed at the time of this document's compilation:

On your **Dallmeier recording system**,

- select the **Use EdgeAnalytics AI (VCA)** checkbox on the **Encoder settings** tab in the recording configuration dialog for the relevant camera (or, depending on the version of your Dallmeier recording server software, clear the **Image processing on recorder** checkbox on the **Quality** tab),
- select the **Use Database** checkbox in the recording configuration dialog for the relevant camera to enable the storage of camera analytics data (metadata) in the recorder database, and
- select the **Motion coordinates** ("**Bewegungskoordinaten**") and **Sedor data** search items in the global **Recording** > **Search Criteria** configuration dialog.

For the targeted subsequent search for specific events and object classes as well as the efficient evaluation of incidents based on the camera analytics data, the Dallmeier video management software **SeMSy® Compact** with the **SmartFinder** function can then be used, for example.

*In this context, also observe the detailed information in the current documentations for your Dallmeier recording system and for **SeMSy® Compact**.*

Event-triggered camera actions on the basis of **EdgeAnalytics** events

EdgeAnalytics events (e.g. generated by the **EdgeAnalytics AI Intrusion Detection App**) can be used as triggers for a variety of intelligent camera actions if required (see chapter "Event Management" on page 76).

15.1 VCA MOTION DETECTION

The **EdgeAnalytics** technique **VCA Motion Detection** for conventional motion detection of objects with basic object classification is usually already enabled on the camera by default.
In this traditional approach of video content analytics (**VCA**) directly on the camera, objects in the captured scene are detected by motion only.
Depending on the requirements and camera configuration, moving objects detected in the image can also be automatically classified on the basis of a general, basic analytics of characteristic object attributes and thus categorized according to a specific object type (person, vehicle or, if not applicable, unclassified).
As long as no additional analytics applications (**VCA Intrusion Detection** and/or **VCA Line Crossing**) are running on the camera, only the current tracking coordinates of detected objects including the associated timestamps and, if applicable, the respective object class of identified objects are continuously sent to the respective Dallmeier recording system in the form of metadata until the respective object is no longer valid.

- Enable the **EdgeAnalytics** technique **VCA Motion Detection**, if not already running.

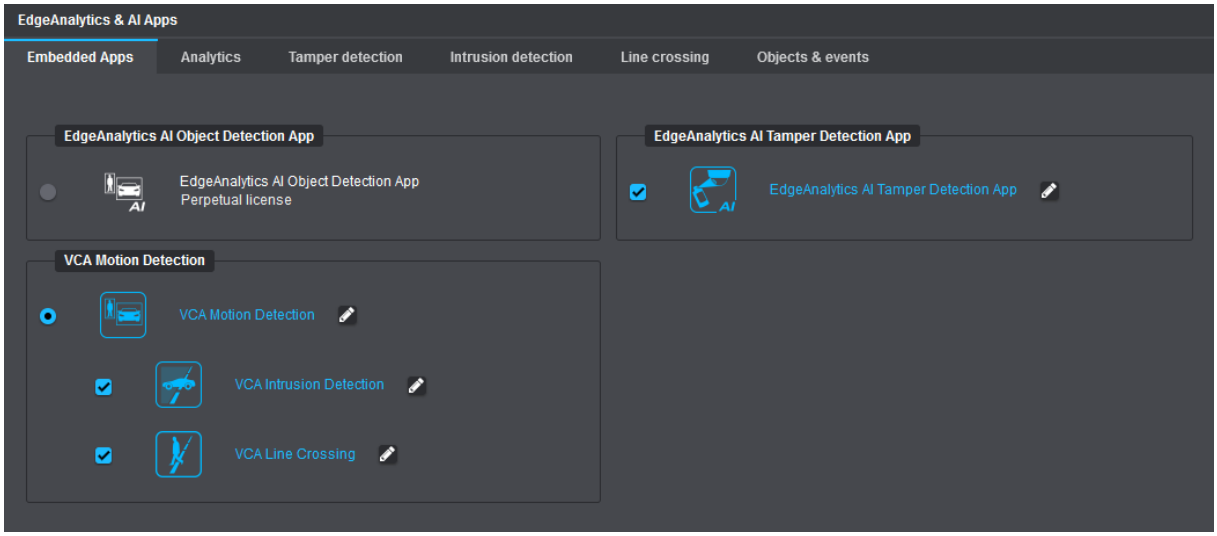

Fig. 15-2

- Click the **Pencil** icon button to the right of the **VCA Motion Detection** item or select the **Analytics** tab to edit the settings of the **EdgeAnalytics** technique (see below).

15.1.1 General Settings

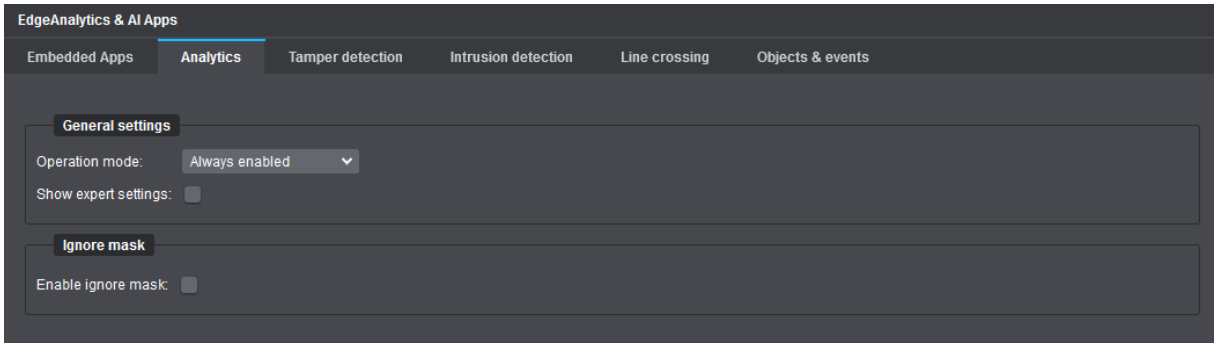

Fig. 15-3

Operation Mode

- From the **Operation mode** drop-down list, select one of the following options:

- **Always enabled**
  Default setting (recommended)

- **On recorder request**
  The video content analytics on the camera (**EdgeAnalytics**) only starts on request via **DaVid** protocol by an appropriately configured Dallmeier recording system.

Show Expert Settings

- Select the **Show expert settings** checkbox to display the available expert settings for the **VCA Motion Detection** (see section “Expert Settings” on page 105).

15.1.2 Expert Settings

The **Expert settings VCA Motion Detection** offer special setting options for detailed adjustment of the video analytics algorithms. They are only displayed if the corresponding checkbox in the **General settings** dialog area (see above) has been previously selected.
In the expert settings, among other parameters, the settings for object and motion detection can be configured with regard to the scene condition (basic lighting conditions in the captured scene), the camera orientation (viewing direction of the camera after installation) and the key object attributes (minimum required and maximum valid object size in the image).

> *For best possible analytics results during live operation, you should always test your configuration on the **Objects & events** tab after changing a setting, e.g. with regard to the number, plausibility and relevance of detected objects and events (see section "Objects & Events" on page 129).*

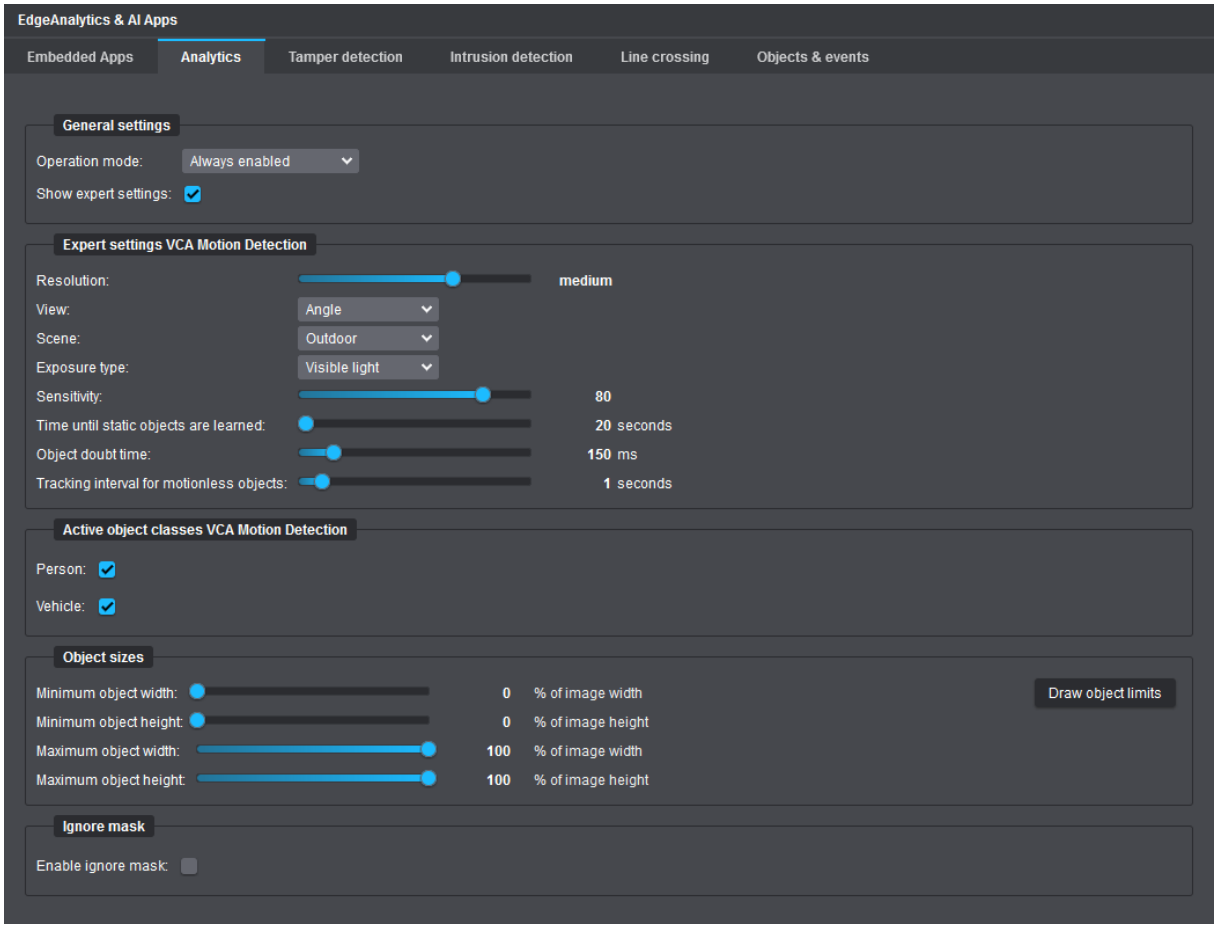

Fig. 15-4

Resolution
This setting determines the **EdgeAnalytics** input resolution. The appropriate setting depends on the type, distance and motion speed of the monitored objects as well as on the scene condition.
At higher analytics input resolutions, smaller objects are usually better detected and can be classified more accurately, but the analytics frame rate decreases, as the CPU load of the camera increases.
In contrast, the higher the analytics frame rate (images per second used for video analytics), the more accurate the virtual motion tracking of detected objects.

The following table provides a general overview of the usually recommended analytics input resolutions for different scene conditions and object sizes (however, this only applies to the **EdgeAnalytics** technique **VCA Motion Detection**):

SCENE CONDITION / OBJECT SIZE	RECOMMENDED ANALYTICS INPUT RESOLUTION
Indoor – medium/large objects	very small
Indoor – small objects	small
Outdoor – medium/large objects	small
Outdoor – small objects	medium

Table 15-1

The following table provides a general overview of the usually recommended analytics frame rates for various video analytics applications (however, this only applies in conjunction with the **EdgeAnalytics** technique **VCA Motion Detection**):

VIDEO ANALYTICS APPLICATION	RECOMMENDED ANALYTICS FRAME RATE (FRAMES/SECOND)
General motion detection of objects (video motion detection, VMD) with virtual motion tracking	10–20 (min. 8)
Intrusion detection	5–15 (min. 5)
Tamper detection	5–15 (min. 5)

Table 15-2

Information on the analytics frame rate (frames/second) currently in use and the CPU load caused by the running video content analytics on the camera is provided on the **Objects & Events** tab in the **Statistics** dialog area (see section “Objects & Events” on page 129).

► Set the required analytics input resolution with the provided **Resolution** slider.

View
This setting determines the camera orientation (viewing direction of the camera after installation) to be taken into account by the video analytics algorithms while analyzing the image data.

► Select your camera viewing direction from the **View** drop-down list:

- **Horizontal**: Horizontal viewing direction of the camera;
  recommended in case the scene is captured from the side at rather lower installation heights
- **Head**: Overhead / top-down view (the camera is looking vertically down on the scene);
  usually well suited for detecting the direction of object movements
- **Angle**: Angled view from top (the camera is looking down on the scene diagonally at a tilt angle of approx. 30° and an installation height of approx. 2.5–3.0 m);
  recommended e.g. for **VCA Intrusion Detection**

Scene
This setting determines the scene condition (basic lighting conditions in the captured scene) to be taken into account by the video analytics algorithms while analyzing the image data.

► Select your scene condition from the **Scene** drop-down list:

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

Exposure Type
This setting determines the type of exposure in the captured scene to be taken into account by the video analytics algorithms while analyzing the image data.

► Select the type of exposure that is present in your scene from the **Exposure type** drop-down list:

- **Visible light**: Recommended setting, for example, if the camera is operated in day mode only
- **Infrared light**: Recommended setting, for example, if the camera is operated in night mode only with the built-in IR LEDs switched on
- **Automatic**: The video analytics algorithms try to automatically detect what kind of lighting (exposure type) is present in the captured scene.

Sensitivity
This setting defines the sensitivity of the motion detection.

The higher the set value, the higher the detection sensitivity and the more motion is detected in the captured scene, i.e. the smaller any changes in successive frames need to be in order to define these changes as new motion objects.

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 using the corresponding slider.

Time Until Static Objects Are Learned
This setting specifies the amount of time (seconds) that must elapse before detected objects that are no longer moving in the captured scene are considered to be part of the background and not to be objects anymore (e.g. a parked vehicle). After the set time has elapsed, the associated object-related metadata (e.g. the current tracking coordinates along with the timestamps) is no longer generated and sent.

The default setting is **20 seconds**.

▶ Use the available slider to set the required amount of time that must elapse.

Object Doubt Time
This setting specifies the minimum time in milliseconds that a newly detected changing image element must exist in the captured scene before it is defined as a new valid object.

The default setting is **150 ms**.

▶ Use the available slider to set the required minimum validity period.

Tracking Interval for Motionless Objects
This setting determines the time interval in seconds between repeatedly sending (static) tracking coordinates of no longer moving objects before these objects are finally considered to be part of the background (see section “Time Until Static Objects Are Learned” on page 108).
This setting is useful to reduce the amount of redundant metadata that is not really necessary for a later evaluation.

Example:
After a vehicle has been parked, it is initially still considered to be an object. However, the tracking coordinates of the parked vehicle, which no longer change, continue to be sent periodically at the set time interval to the respective Dallmeier recording system in the form of metadata until the parked vehicle is no longer considered to be an object but part of the background.

► Use the available slider to set the required time interval.

*If the **Tracking interval for motionless objects** is set to **0 seconds** (this is the default setting), the static tracking coordinates of a detected object are sent to the respective Dallmeier recording system together with each generated frame.*

15.1.2.1 Active Object Classes VCA Motion Detection

Using the automatic object classification, moving objects can be automatically classified on the basis of a general, basic analytics of characteristic object attributes and thus categorized according to a specific object type (person, vehicle or, if not applicable, unclassified).
The detected additional object information is sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.
During the later evaluation of the generated camera analytics data (e.g. with **SeMSy® Compact**), the event search results can then be filtered specifically according to the relevant object types (classes).

- To enable the automatic object classification, select the corresponding **Person** and/or **Vehicle** check-boxes.

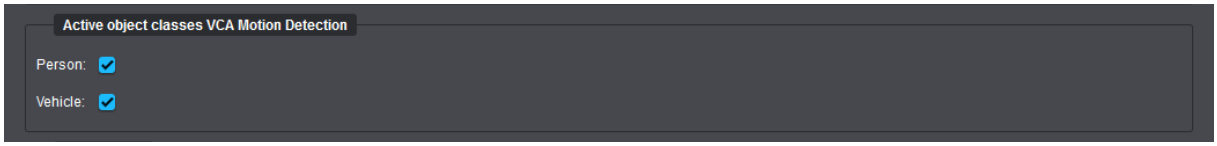

Fig. 15-5

In general, a detected object is initially considered to be unknown (unclassified).
The accuracy of classifying a detected object to its correct object type increases with the duration spent on analyzing the individual object.
For example, if a van slowly enters the scene from the edge of the image, the newly detected object may initially be misinterpreted as a “Person”.
However, as the analytics time continues, i.e. as soon as the van moves further into the scene, the new object is correctly classified as a “Vehicle”.
Therefore, please note that the class of a detected object may change in the course of being analyzed.

If automatic object classification is enabled, the CPU load of the camera increases.

15.1.2.2 Object Sizes

This dialog area allows you to specify the size limits for objects of interest by setting the minimum required and the maximum valid object dimensions (width and height values as a percentage in relation to the total image size).
Objects that are smaller or larger than the specified limits are automatically ignored by the video analytics algorithms.
The **Draw object limits** function facilitates the estimation of relevant object dimensions in the captured scene.

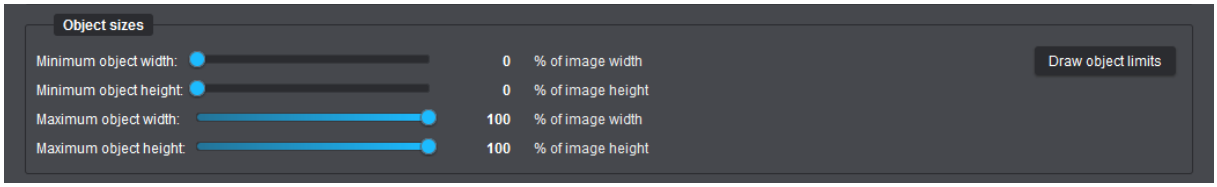

Fig. 15-6

Minimum Object Width/Height

- Set the minimum required object size (width and height in percentage) using the corresponding sliders.

Maximum Object Width/Height

- Set the maximum valid object size (width and height in percentage) using the corresponding sliders.

Recommendations:

- For reliable object detection and the most accurate virtual object 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.

*The recommendations mentioned above are only applicable to the **EdgeAnalytics** technique **VCA Motion Detection**.*

Draw Object Limits

- Click the **Draw object limits** button (Fig. 15-6) to define the minimum required and the maximum valid object dimensions with your mouse in the displayed preview image.

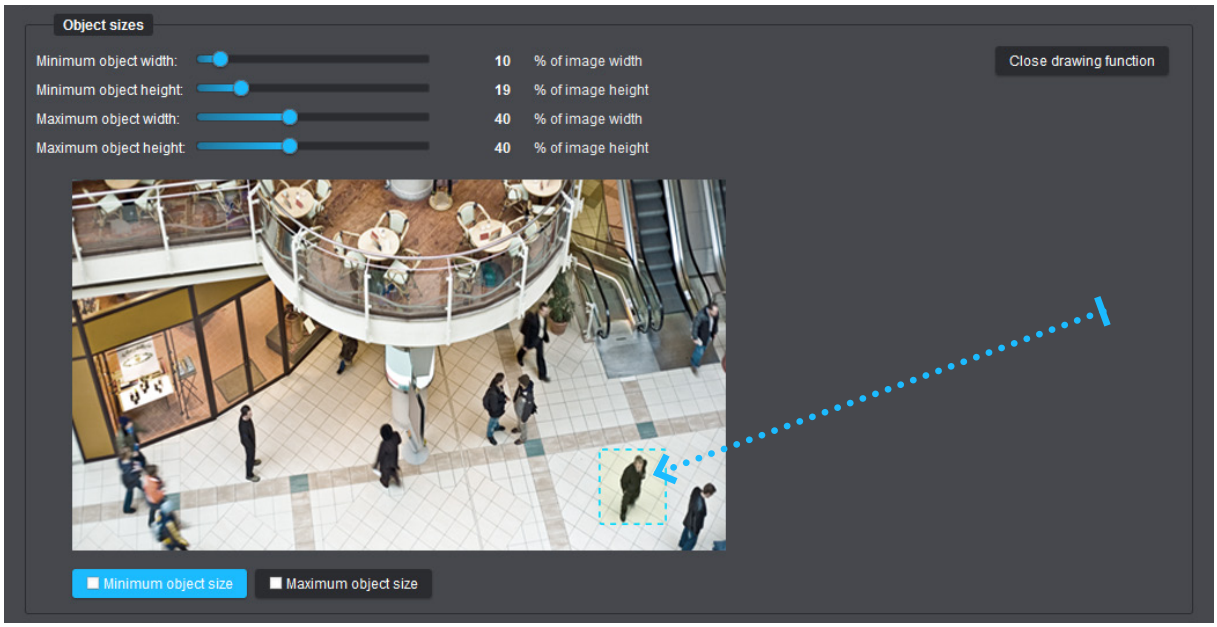

Fig. 15-7

- Click the **Minimum object size** button.
- Position the mouse pointer over the preview image where you want to start drawing.
- Click and hold the left mouse button down, then draw a rectangle for the minimum required object size by dragging the mouse pointer around a reference object of interest (see the arrow in Fig. 15-7).
- Release the mouse button to finish drawing the rectangle.
- Click the **Maximum object size** button and then repeat the previous steps.

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

- Click the **Close drawing function** button to quit the drawing function.

Use real-world objects as a size reference when drawing the rectangles.

15.1.3 Ignore Mask

The **Ignore mask** function allows you to generally exclude one or multiple user-definable areas in the captured scene from the video content analytics.
This function is useful, on the one hand, to minimize the number of non-relevant objects and events (e.g. caused by walking pedestrians or passing vehicles at the edges of the image as well as due to continuous movement of clouds, vegetation and waters) and, on the other hand, to reduce the processor utilization on the camera (CPU load caused by the running video content analytics).

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

Inactive area masks are highlighted in red in the live preview.
All changes made are always immediately applied without any further user action.

To create inactive areas in the image, proceed as follows:

- Select the **Enable ignore mask** checkbox.
- Click the required tool (button) to draw, edit or delete inactive areas (see below).

Draw Polygon

- Click the **Draw polygon** button.
- Left-click and release the mouse button to set each of the anchor (corner) points of the new polygonal inactive area.
- Right-click and release the mouse button or press the **Enter** key on your keyboard to finish creating the new polygon (no other anchor point will be set).

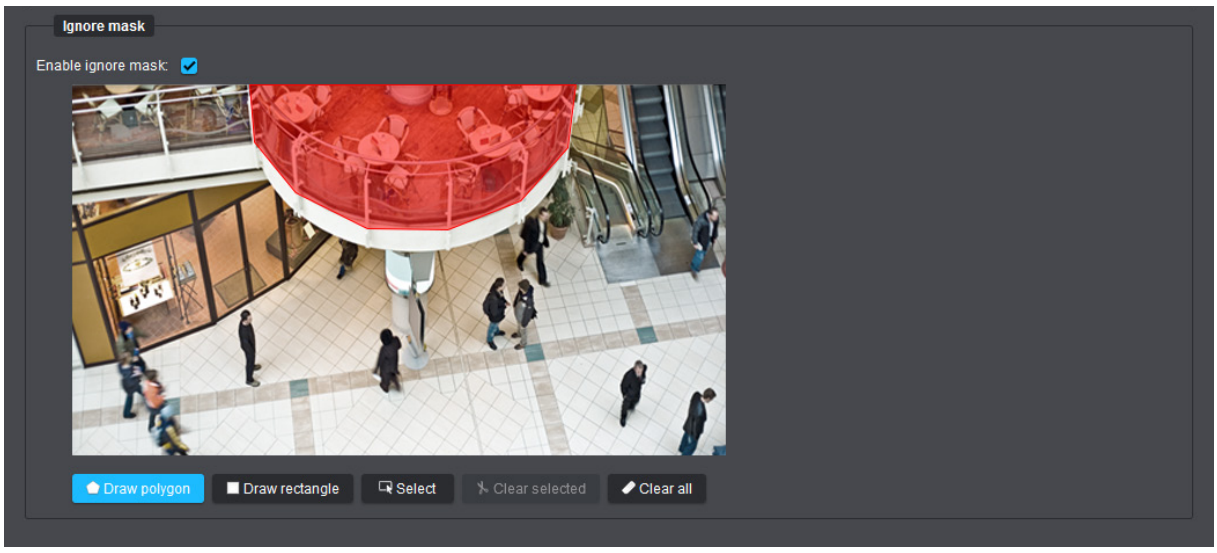

Fig. 15-8

You can define multiple polygonal inactive areas.
The anchor (corner) points of a drawn polygon can be edited later if needed (see section "Select/Edit" on page 115).

Draw Rectangle

- Click the **Draw rectangle** button.
- Click and hold the left mouse button down while drawing a rectangle over the relevant image area (release the mouse button to finish).

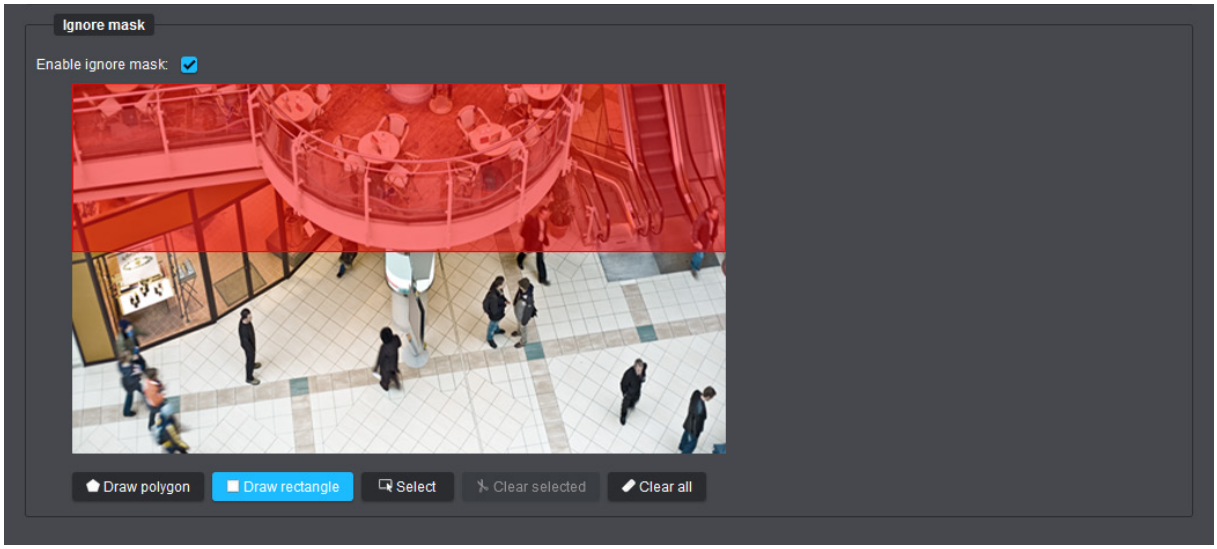

Fig. 15-9

You can define multiple rectangular inactive areas.
The anchor (corner) points of a drawn rectangle can be edited later if needed (see section "Select/Edit" on page 115).

Select/Edit

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

The selected inactive area is marked with small white circles at its anchor (corner) points.

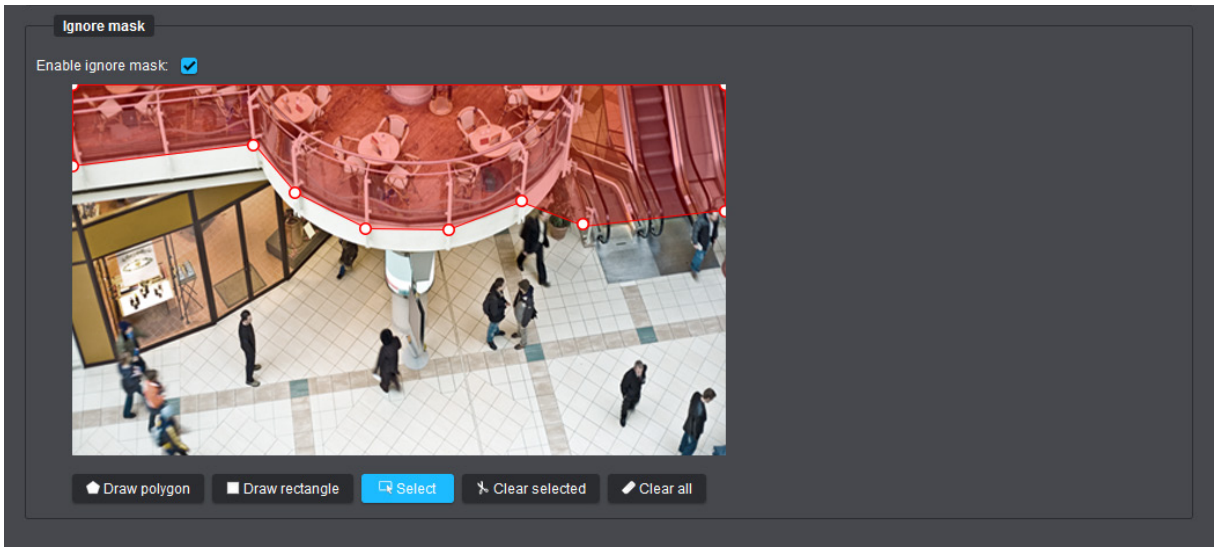

Fig. 15-10: Polygon selected for editing (indicated by white anchor points)

- Move the white circles while holding down the left mouse button to change the defined inactive area (new anchor points can be added by use of the left mouse button, but no existing anchor points can be deleted).

For deleting inactive areas, proceed as follows:

Clear All

- Click the **Clear all** button to delete all defined inactive areas.

Clear Selected

- Click the **Select** button.
- Left-click the inactive area you want to select (hold down the **Ctrl** key on your keyboard to select multiple inactive areas).
- Click the **Clear selected** button or press the **Delete** key on your keyboard to delete all previously selected inactive areas.

15.2 EDGE ANALYTICS AI OBJECT DETECTION APP

LICENSE CODE REQUIRED

After a 30-day trial period*, a valid license code must be purchased to continue using this feature.

For further information, please refer to the product specification for your camera on the Dallmeier website at https://www.dallmeier.com/.

To purchase a valid license code for this feature, contact your Dallmeier sales partner.

* The trial period does not start to expire unless the function is enabled for the first time.
As soon as the function is disabled again or the camera is disconnected from the power supply during the existing trial period, the expiry time of the 30-day trial period is paused.

The future-oriented **EdgeAnalytics AI Object Detection App** with AI-based object detection represents the next logical step beyond traditional and conventional motion detection with only basic object classification (see section "VCA Motion Detection" on page 103). The new powerful on-board analytics app uses an artificial neural network that has been intensively trained on the basis of the latest state-of-the-art deep learning techniques to help analyzing the captured scene regardless of any movements in the image while being able to classify detected objects of various types (person, two-wheeler, car and many more) with the utmost precision and reliability in real-time.

- Enable the **EdgeAnalytics AI Object Detection App**.

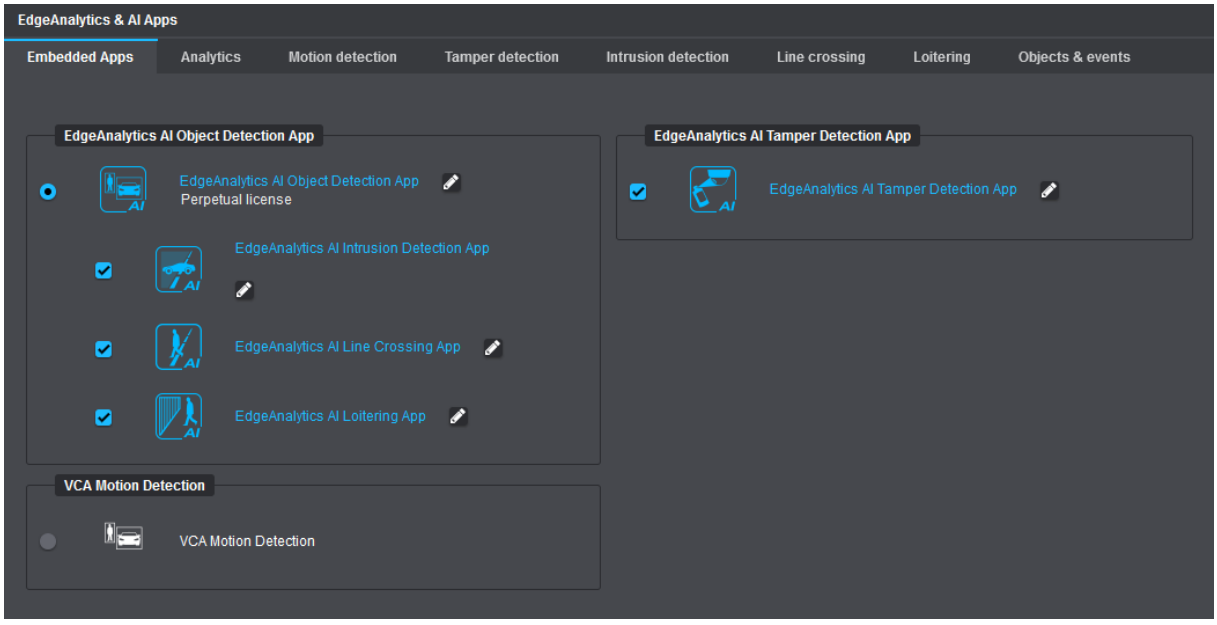

Fig. 15-11

- Click the **Pencil** icon button to the right of the **EdgeAnalytics AI Object Detection App** item or select the **Analytics** tab to edit the settings of the **EdgeAnalytics** technique (see below).

15.2.1 General Settings

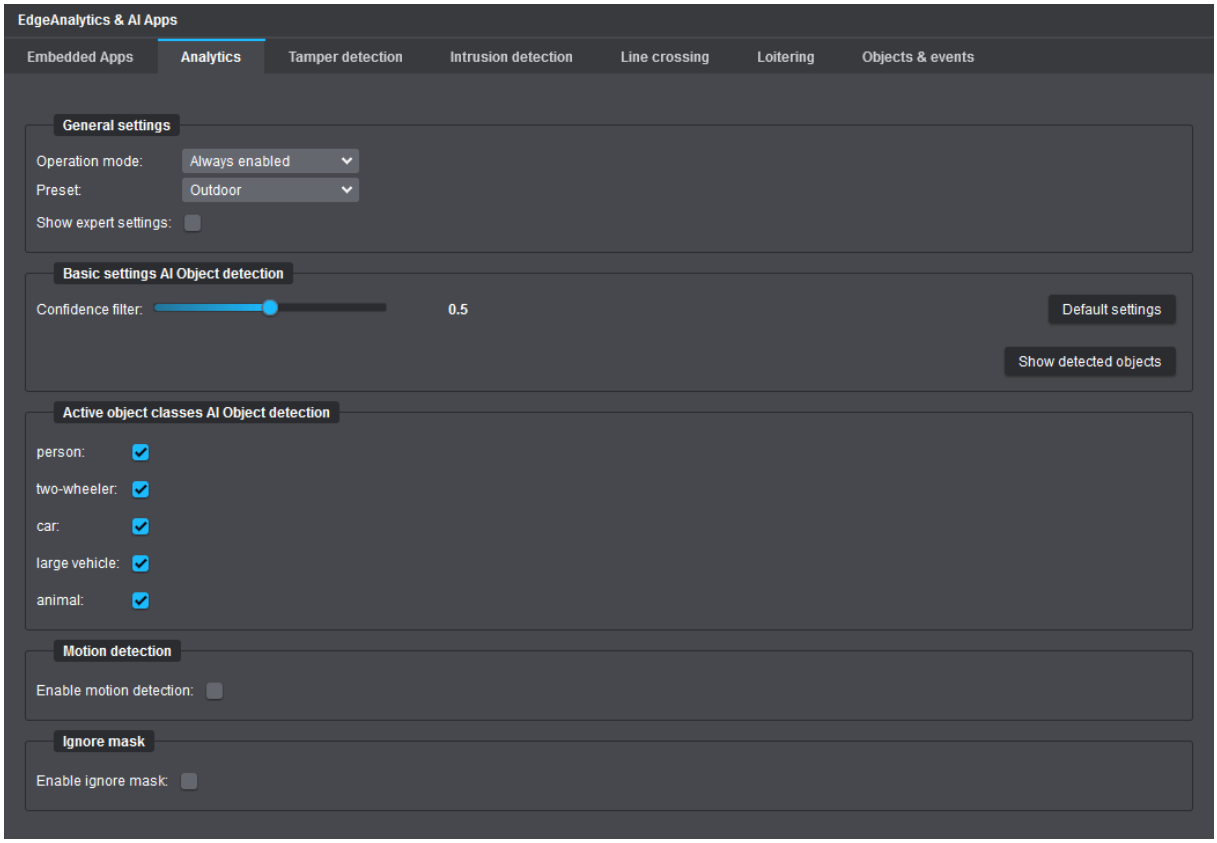

Fig. 15-12

Operation Mode

▶ From the **Operation mode** drop-down list, select one of the following options:

- **Always enabled**
  Default setting (recommended)

- **On recorder request**
  The video content analytics on the camera (**EdgeAnalytics**) only starts on request via **DaVid** protocol by an appropriately configured Dallmeier recording system.

Preset

This setting determines the scene condition (basic lighting conditions in the captured scene) to be taken into account by the video analytics algorithms while analyzing the image data.

▶ Select your scene condition from the **Preset** drop-down list:

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

Show Expert Settings

▶ Select the **Show expert settings** checkbox to display the available expert settings for the **EdgeAnalytics AI Object Detection App** (see section “Expert Settings” on page 119).

Confidence Filter
The confidence score presented for each object bounding box reflects how confident the AI-based object classifier is (how much the AI-based analytics engine trusts itself) about having correctly interpreted the object class of a detected object.
Confidence scores can range from 0 (no confidence in a particular prediction) to 1 (high confidence).
The higher the confidence score, the more likely the analytics engine is to be confident in the accuracy of its own predictions.
Using the **Confidence filter** function, analyzed objects of confidence scores below the set threshold can be automatically discarded before any further processing.

The default setting is **0.5**.

- Click the **Show detected objects** button to show the objects display viewport.
- Set the required confidence threshold with the **Confidence filter** slider.

Note that analyzed objects with a confidence score only slightly below the set threshold are not immediately discarded by the AI-based analytics engine.

Active Object Classes AI Object Detection
The automatic AI-based object classification can classify detected objects with exceptionally high precision, regardless of any movements in the image, and thus categorize each of these objects according to a specific object type (person, two-wheeler, car, etc.) with reliable accuracy, even in the most challenging scene conditions.
The detected additional object information is sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.
During the later evaluation of the generated camera analytics data (e.g. with **SeMSy® Compact**), the event search results can then be filtered specifically according to the relevant object types (classes).

- To enable the automatic object classification, select the corresponding checkbox next to the relevant object type.

If automatic object classification is enabled, the CPU load of the camera increases.

Motion Detection
This setting can be used to additionally enable conventional detection of moving objects in the image, which works largely on the same operating principle as the **EdgeAnalytics** solution **VCA Motion Detection**.
After enabling this function, a new tab called **Motion detection** is displayed, allowing you to adjust the motion detection sensitivity as needed.
The higher the detection sensitivity (default setting: **Normal**), the more motion is detected in the captured scene, i.e. the smaller any changes in successive frames need to be in order to define these changes as new, unclassified motion objects.

Ignore Mask
For descriptions of this function, see section "Ignore Mask" on page 113.

15.2.2 Expert Settings

Fig. 15-13

Resolution

This setting determines the internal image resolution the **EdgeAnalytics** technique works with (default setting: **medium**). The appropriate setting depends on the type, distance and motion speed of the monitored objects as well as on the scene condition.

At higher analytics input resolutions, smaller objects are usually better detected and can be classified more accurately, but the analytics frame rate decreases, as the CPU load of the camera increases.

In contrast, the higher the analytics frame rate (images per second used for video analytics), the more accurate the virtual motion tracking of detected objects.

Information on the analytics frame rate (frames/second) currently in use and the CPU load caused by the running video content analytics on the camera is provided on the **Objects & Events** tab in the **Statistics** dialog area (see section “Objects & Events” on page 129).

- Set the required analytics input resolution with the provided **Resolution** slider.

Scene
This setting determines which scene conditions regarding the typical maximum motion speeds of various object classes (person, vehicle, animal) as well as the potentially expected crowd density (number of people within the captured area) should be taken into account by the video analytics algorithms when processing the image data.

► From the **Scene** drop-down list, select one of the following options:

- **Automatic** (default setting)
  Using this setting, the AI-based analytics engine attempts to automatically determine as accurately as possible the prevailing scenery, the object classes commonly found in that scenery, their object-specific maximum motion speeds, and, if applicable, the expected crowd density.
- **Highway**
- **Out of town**
- **In town, many people**
- **In town**
- **User defined**
  This setting allows to manually customize the expected maximum motion speeds for the individual object classes.

Track Motion Detection Objects
This setting is only available if the **Enable motion detection** checkbox is selected (see section "Motion Detection" on page 118).
Using this setting, tracking coordinates in the form of metadata are also generated for unknown objects that cannot be categorized according to any of the possible object classes, as well as for any other moving objects in the image.

Tracking Interval for Motionless Objects
This setting determines the time interval in seconds between repeatedly sending (static) tracking coordinates of detected objects that are not moving in the image.
This setting is useful to reduce the amount of redundant metadata that is not really necessary for a later evaluation.

Example:
The tracking coordinates of a parked vehicle, which remain unchanged, are periodically sent to the respective Dallmeier recording system in the form of metadata only at the set time interval.

► Use the available slider to set the required time interval.

*If the **Tracking interval for motionless objects** is set to **0 seconds** (this is the default setting), the static tracking coordinates of a detected object are sent to the respective Dallmeier recording system together with each generated frame.*

Object Sizes
For descriptions of this function, see section "Object Sizes" on page 111.

15.3 INTRUSION DETECTION

The **Intrusion Detection** analytics application enables the automatic generation of events as soon as detected objects enter or leave user-definable sensitive areas in the image.

Typical application scenarios:
- Building and site protection of critical infrastructures
- Securing access (entry and exit) points of facilities
- Securing premises and restricted indoor/outdoor areas
- Monitoring no-stopping and no-parking zones as well as fire and emergency access routes, or similar

For creating and editing masks that specify active sensitive areas in the image, a live preview (with a frame rate of 1 fps) as well as various tools and fine adjustments are available.

Active sensitive area masks are highlighted in red in the live preview.
All changes made are always immediately applied without any further user action.

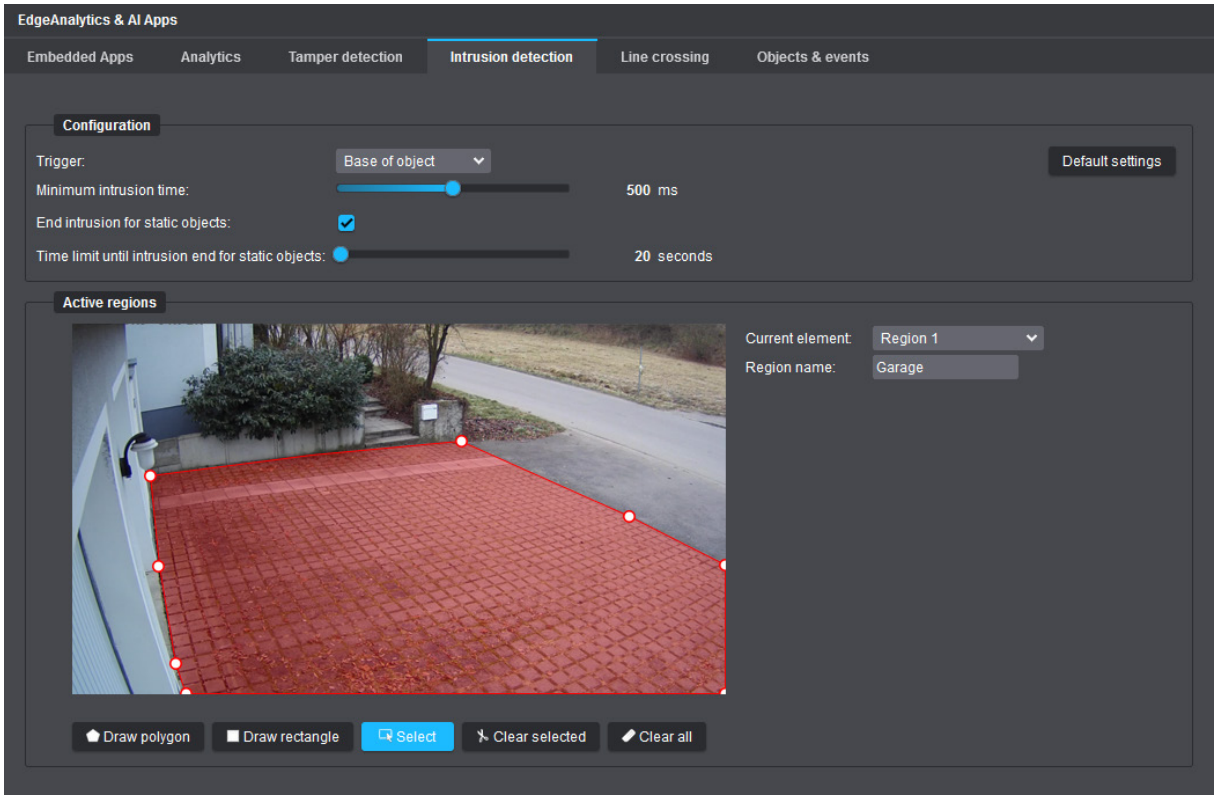

Fig. 15-14

- Define the required active sensitive areas in the image where you want the **Intrusion Detection** analytics application to run.

The procedure for creating and editing active sensitive areas in the image (max. 4 intrusion areas possible) corresponds to the procedure for defining globally inactive areas of the video content analytics (see section “Ignore Mask” on page 113).

- Assign a unique **Region name** for each drawn intrusion area (first select the relevant drawn area with the provided selection tool).

In the example shown above (Fig. 15-14), 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, a corresponding event is automatically generated and sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.
The respective intrusion events can also be used as triggers for a variety of intelligent camera actions (see chapter "Event Management" on page 76).

Trigger
This setting determines whether already the base point of an object within an active sensitive area is counted as a new event, at least the center point of an object must overlap an active sensitive area, or whether a user-defined minimum percentage overlap of an object with an active sensitive area must exist before a new event is triggered (default setting = base of object).

- Select the required **Trigger** option from the corresponding drop-down list.

Threshold
This setting is only available if the **Overlap of object** option is selected from the **Trigger** drop-down list (see above).
The threshold defines the required minimum percentage of an object (in relation to its total spatial extent) that must enter an active sensitive area (or leave the area again) to generate a new event.

- Set the required **Threshold** value with the corresponding slider.

Minimum Intrusion Time
This setting specifies the minimum amount of time (milliseconds) that a detected object must remain in an active sensitive area before an Intrusion Start event is generated (after an Intrusion Start event, an Intrusion Continued event is generated every 3 seconds until the object has left the sensitive area again, which in turn generates a final Intrusion End event).

The default setting is **500 ms**.

- Set the required **Minimum intrusion time** with the corresponding slider.

End Intrusion for Static Objects
If this setting is enabled and a moving object that has previously entered an active sensitive area becomes static after a certain period of time (e.g. after a vehicle has been parked in an active sensitive area), a final Intrusion End event is generated after a user-definable timeout (see below).

Time Limit Until Intrusion End for Static Objects
This setting is only available if the **End intrusion for static objects** setting is enabled (see above).

The default timeout value is **20 seconds**.

- Use the available slider to set the required timeout.

Default Settings
- Click the **Default settings** button if you want to restore the default settings of the **Intrusion Detection** analytics application.

15.4 LINE CROSSING

The **Line Crossing** analytics application enables the automatic generation of events as soon as detected objects cross user-definable virtual lines in the image (virtual tripwire).
The generated events are sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.
The respective line crossing events can also be used as triggers for a variety of intelligent camera actions (see chapter "Event Management" on page 76).

Typical application scenarios:

- Perimeter protection (fence monitoring, protection against climbing)

For creating and editing virtual lines in the image, a live preview (with a frame rate of 1 fps) as well as various tools and fine adjustments are available.

Virtual lines are highlighted in red in the live preview.
You can draw up to four virtual lines in the image in the form of polylines.
A polyline can consist of max. 3 joined line segments or max. 4 anchor points.
All changes made are always immediately applied without any further user action.

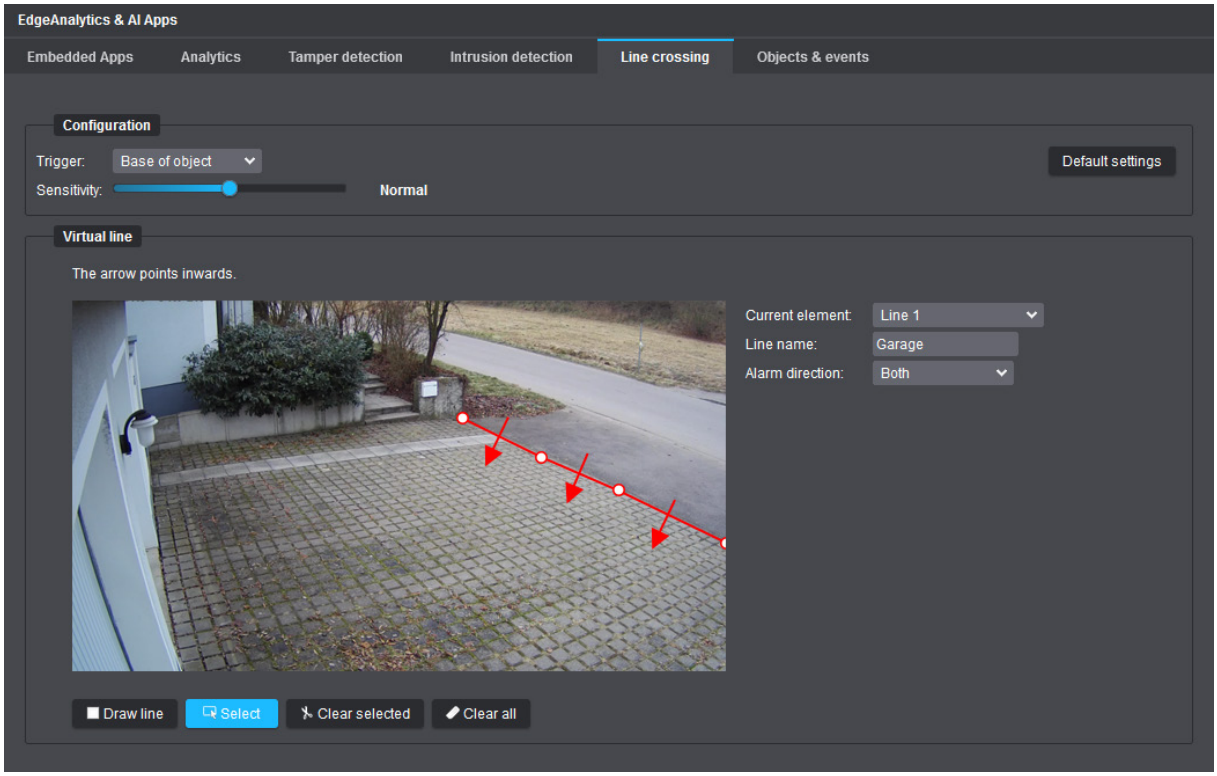

Fig. 15-15

- Position the mouse pointer over the preview image where you want to start drawing the virtual line.
- Left-click and release the mouse button to set the first anchor point of the new polyline.
- Move the mouse pointer to the next position in the preview image and click the left mouse button again to define the next anchor point of the polyline (after defining at least 2 anchor points, you can finish creating the new virtual line at any time by clicking the right mouse button).
- Repeat the last steps to add another virtual line (you can create up to four virtual lines if needed).

Edit Virtual Line

- Click the **Select** button.
- Left-click a drawn polyline.

The selected polyline is marked with small white circles at its anchor points.

- Assign a unique name for the virtual line.
- Select the alarm direction for the virtual line (the arrows of a polyline always point inwards).
- If necessary, move the anchor points to a new position using the left mouse button (you can add new anchor points to a polyline if the maximum number of 4 anchor points has not yet been reached, but you cannot delete existing anchor points).
- Repeat the last steps for each drawn polyline.

To delete polylines, proceed as follows:

Clear All

- Click the **Clear all** button to delete all defined virtual lines.

Clear Selected

- Click the **Select** button.
- Left-click the polyline you want to select (hold down the **Ctrl** key on your keyboard to select multiple polylines).
- Click the **Clear selected** button or press the **Delete** key on your keyboard to delete all previously selected polylines.

Trigger

This setting determines whether already the base point of an object on a drawn virtual line is counted as a new event or whether at least the center point of an object must cross a virtual line before a new event is triggered (default setting = base of object).

- Select the required **Trigger** option from the corresponding drop-down list.

Sensitivity

The higher the sensitivity level, the earlier a new event is triggered as soon as an object crosses a virtual line. For example, a very low sensitivity level prevents many unwanted events from being generated when objects cross the drawn virtual lines only for a very short moment up to a certain degree when passing or driving by.

The default setting is **Insensitive**.

- Set the required **Sensitivity** level with the corresponding slider.

Default Settings

- Click the **Default settings** button if you want to restore the default settings of the **Line Crossing** analytics application.

15.5 LOITERING

*The **Loitering** analytics application is only available in conjunction with the **EdgeAnalytics AI Object Detection App**.*

The **Loitering** analytics application enables the automatic generation of events as soon as detected persons remain for an unusually long (adjustable) period of time in user-definable image areas.
The generated events are sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.
The respective loitering events can also be used as triggers for a variety of intelligent camera actions (see chapter "Event Management" on page 76).

Typical application scenarios:
- Building and site protection of critical infrastructures
- Securing access (entry and exit) points of facilities
- Securing premises and restricted indoor/outdoor areas

For creating and editing masks that specify active sensitive areas in the image, a live preview (with a frame rate of 1fps) as well as various tools and fine adjustments are available.

Active sensitive area masks are highlighted in red in the live preview.
All changes made are always immediately applied without any further user action.

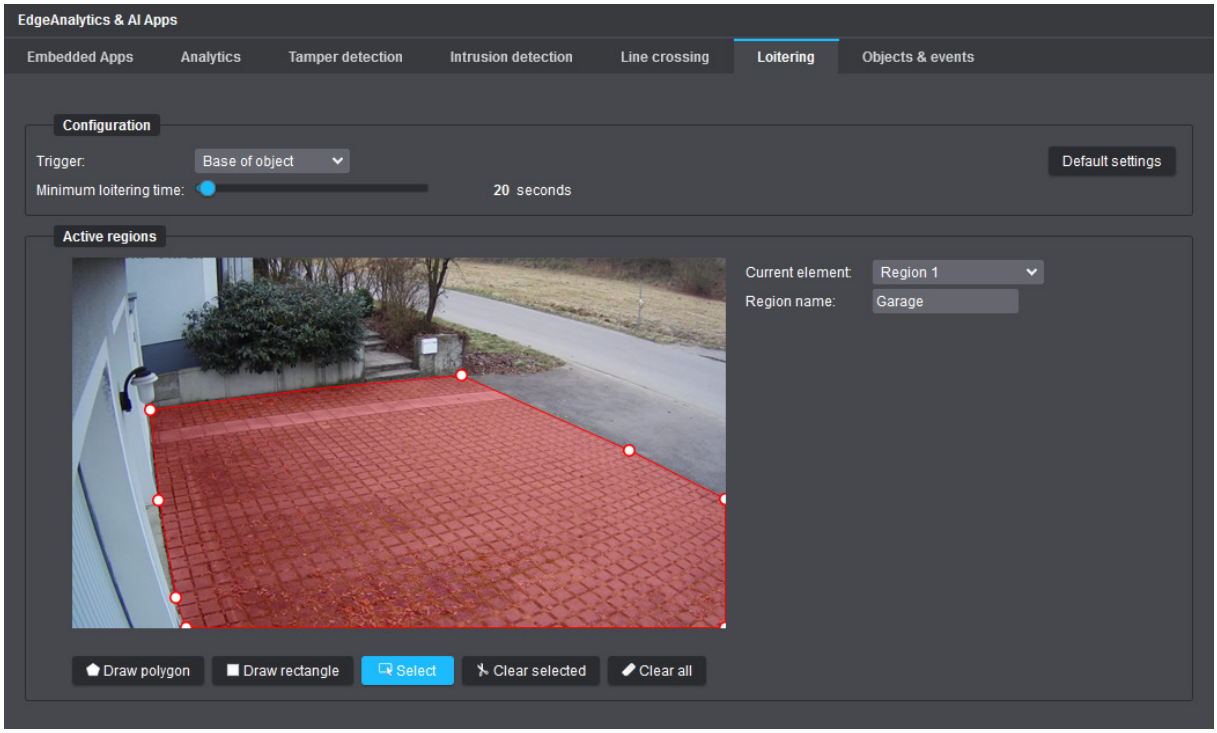

Fig. 15-16

- Define the required active sensitive areas in the image where you want the **Loitering** analytics application to run.

The procedure for creating and editing active sensitive areas in the image (max. 3 loitering areas possible) corresponds to the procedure for defining globally inactive areas of the video content analytics (see section “Ignore Mask” on page 113).

- Assign a unique **Region name** for each drawn loitering area (first select the relevant drawn area with the provided selection tool).

Trigger
This setting determines whether already the base point of a person within an active sensitive area is counted as a new event, at least the center point of a person must overlap an active sensitive area, or whether a user-defined minimum percentage overlap of a person with an active sensitive area must exist before a new event is triggered (default setting = base of object).

- Select the required **Trigger** option from the corresponding drop-down list.

Threshold
This setting is only available if the **Overlap of object** option is selected from the **Trigger** drop-down list (see above).
The threshold defines the required minimum percentage of a person (in relation to its total spatial extent) that must remain in an active sensitive area to generate a new Loitering Start event.

- Set the required **Threshold** value with the corresponding slider.

Minimum Loitering Time
This setting specifies the minimum amount of time (seconds) that a detected person must remain in an active sensitive area before a Loitering Start event is generated (after a Loitering Start event, a Loitering Continued event is generated every 3 seconds until the person has left the sensitive area again, which in turn generates a final Loitering End event).

The default setting is **20 seconds**.

- Set the required **Minimum loitering time** with the corresponding slider.

Default Settings
- Click the **Default settings** button if you want to restore the default settings of the **Loitering** analytics application.

15.6 TAMPER DETECTION

The **EdgeAnalytics AI Tamper Detection App** offers special analytics and event processing features that can automatically detect various sabotage actions or camera tampering attempts if enabled (see sections below).
As soon as a relevant event is detected, it is sent in the form of metadata in real-time to the respective Dallmeier recording system for storage and further processing.

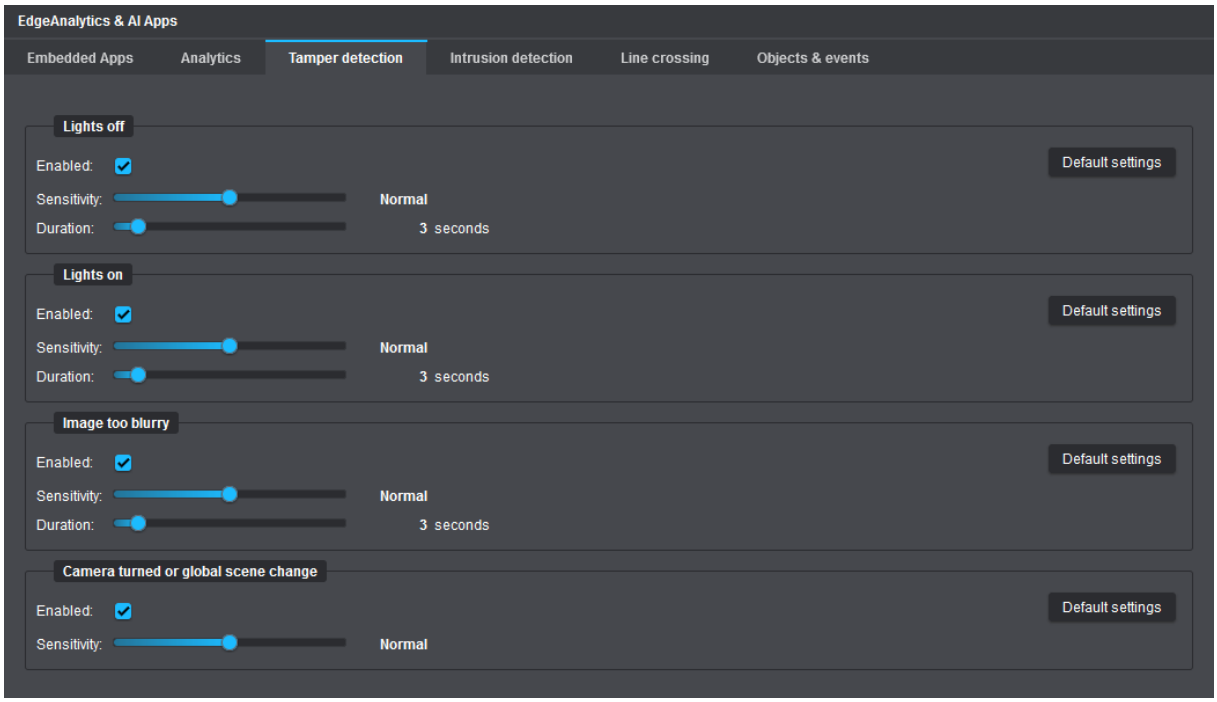

Fig. 15-17

Lights Off

Automatically generates a new event as soon as the average intensity of illumination in the captured scene decreases abruptly, such as in the case of

- a sudden change in brightness level of the ambient light due to switching off or sabotage of a light source, or
- spraying or covering the camera or dome bubble.

Sensitivity
This setting determines how strongly the intensity of illumination in the captured scene must abruptly change in order to generate a new event. The higher the sensitivity setting, the less the brightness level needs to change in an abrupt manner.

The default setting is **Normal**.

► Set the required **Sensitivity** level with the corresponding slider.

Duration
This setting specifies the minimum amount of time (seconds) that the abrupt change in illuminance must last before a corresponding new event is generated.

► Set the required **Duration** with the corresponding slider (the default setting is **3 seconds**).

Lights On

Automatically generates a new event as soon as the average intensity of illumination in the captured scene increases abruptly, such as in the case of

- a sudden change in brightness level of the ambient light due to switching on a light source, or
- blinding of the lens or image sensor by an external very bright light source (e.g. a laser beam).

Sensitivity and Duration

See descriptions in the section "Lights Off" on page 127.

Image Too Blurry

Automatically generates an event as soon as the image suddenly becomes blurry and out of focus (e.g. due to intentional fogging of the camera or unauthorized defocusing of the lens).

Sensitivity

This setting determines how considerably the image has to change in relation to the originally captured scene before a new event is generated. The higher the sensitivity setting, the less the image has to change.

The default setting is **Normal**.

► Set the required **Sensitivity** level with the corresponding slider.

Duration

This setting specifies the minimum amount of time (seconds) that the image alteration must last (in relation to the originally captured scene) before a corresponding new event is generated.

► Set the required **Duration** with the corresponding slider (the default setting is **3 seconds**).

Camera Turned or Global Scene Change

Automatically generates an event in case of an abrupt global scene change, such as when the camera is turned or covered, or when large objects suddenly become visible in the camera's immediate field of view.

Sensitivity

This setting determines how early a potential camera tampering attempt is counted as a new event. For example, the higher the sensitivity setting, the less the camera lens needs to be covered or the camera orientation changed to generate a new camera tampering event.
Note, however, that a high sensitivity setting may lead to many non-relevant events, e.g. resulting from some camera movements caused by the weather when the camera is mounted outdoors on a high camera pole. In this case, adjust the sensitivity setting to a lower level.

The default setting is **Normal**.

► Set the required **Sensitivity** level with the corresponding slider.

*Click the **Default settings** button displayed in the right dialog area of the respective tamper detection feature if you want to restore the associated factory settings.*

15.7 OBJECTS & EVENTS

On the **Objects & events** tab, the configuration settings of the video content analytics applications can be tested in detail prior to live operation of your camera.

> *For best possible analytics results during live operation, you should always test your configuration on the **Objects & events** tab after changing a setting, e.g. with regard to the number, plausibility and relevance of detected objects and events.*

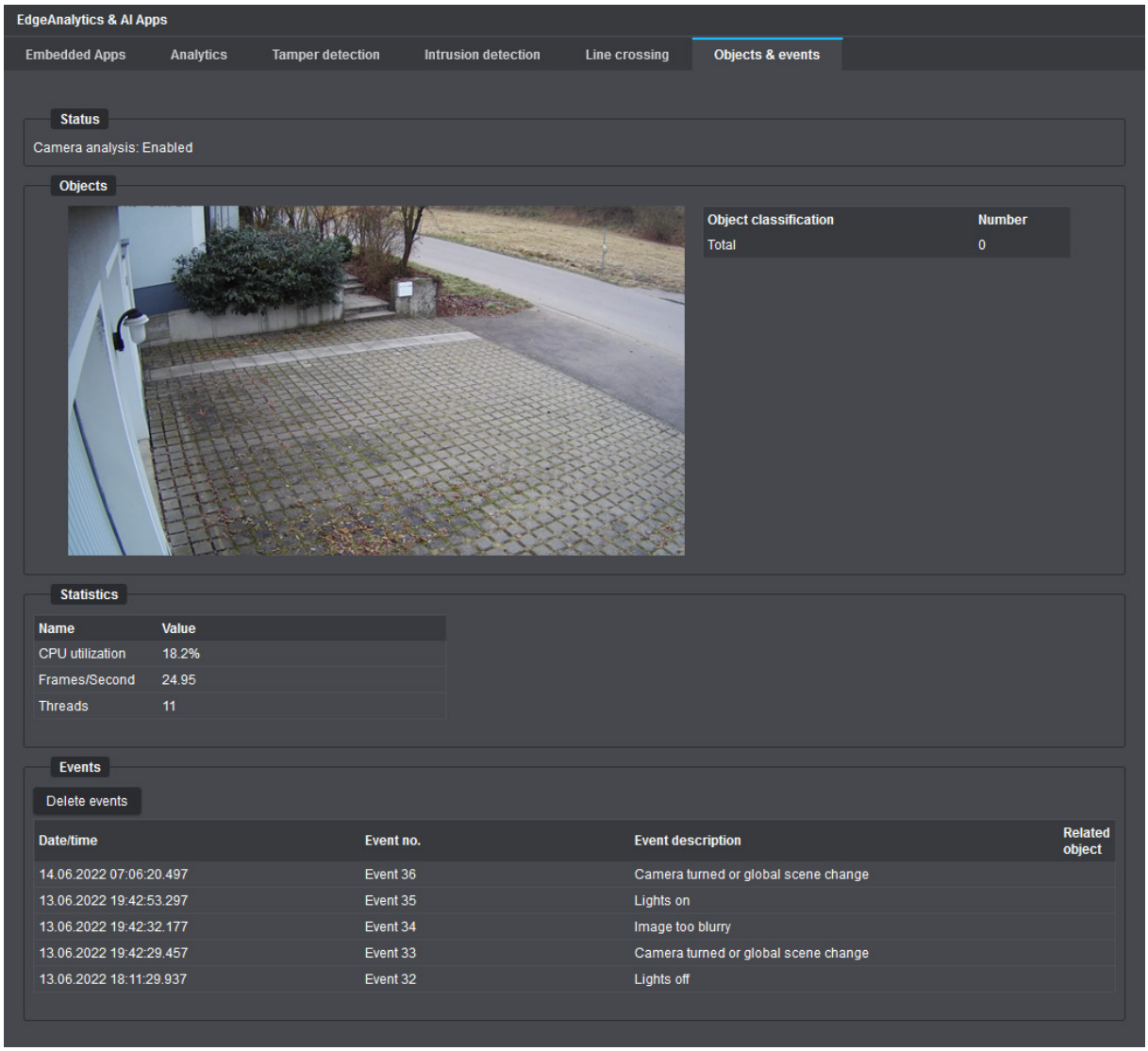

Fig. 15-18

Objects

In this dialog area, all objects detected in the image are highlighted in a live preview (with a frame rate of 1fps) by colored object bounding boxes and are virtually tracked until they are no longer considered to be objects.

Depending on the identified object type (person, vehicle, etc.), various bounding box colors are applied.

Statistics

This dialog area provides the following information:

- Current CPU load caused by the running video content analytics on the camera
- Current analytics frame rate (frames/second)

> *In this context, note the explanations on the analytics input resolution and the analytics frame rate (frames/second) in the section "Resolution" on page 106.*

Events

This dialog area lists the last 20 events generated by the analytics applications running on the camera (e.g. **Intrusion Detection**, **Line Crossing** or **Tamper Detection**).
Each event record includes, for example, the exact event timestamp (date/time of the event) and a short event description.

USERS & RIGHTS

The camera configuration is only accessible to authenticated and authorized users.
The camera's users and rights management allows you to grant different types of access and system configuration rights (privileges) to multiple user groups and to assign individual users to each of these groups.

► Click the **Users & rights** menu item in the navigation menu to open the corresponding dialog.

The **User management** tab is displayed.

16.1 USER MANAGEMENT

Logging in to the camera always requires a user name in combination with a password.
A strong and secure password is essential in this context. It should be complex, random, and long.
Do not use any personal information, common phrases (real words) or names as part of a password.
For security reasons, passwords must be at least 12 characters long (with a maximum of 128 valid characters) and must meet all of the following criteria (consist of the following characters):

- Lower-case character
- Upper-case character
- Digit: 0123456789
- Special character: ^!"$%&/{}()[]=?\`'*+~#-_:.;,<>|@

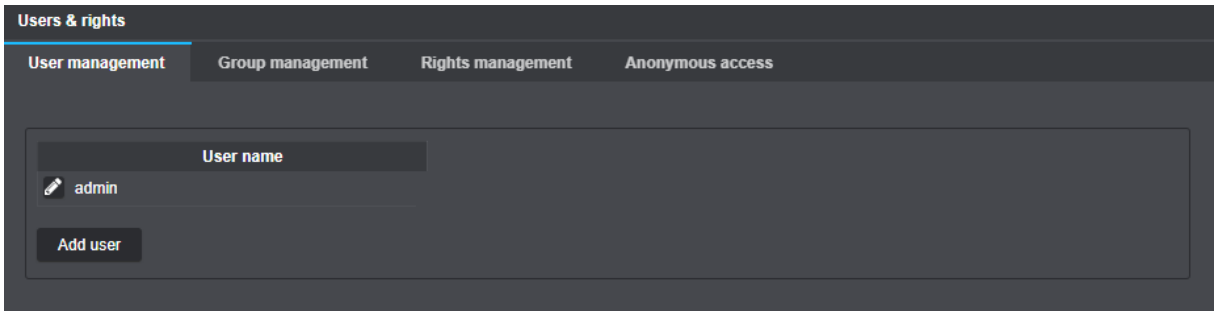

Fig. 16-1

Add User

► Click **Add user**.
► Enter a unique user name (user names cannot be changed later).
► Enter a strong and secure password (follow password policy), and then confirm your entry (both passwords must be identical).
► Finally, click **OK**.

Edit User (Password)

► Click the **Pencil** icon button (to the left of a user name) to edit the user password.

Delete User

► Click the "X" button (red icon next to a user name) to delete the user.

Note that the **admin** user (the default administrator account) cannot be deleted.

16.2 GROUP MANAGEMENT

Each user can be assigned to a user group and will then have the rights (privileges) granted to that user group.

- Open the **Group management** tab.

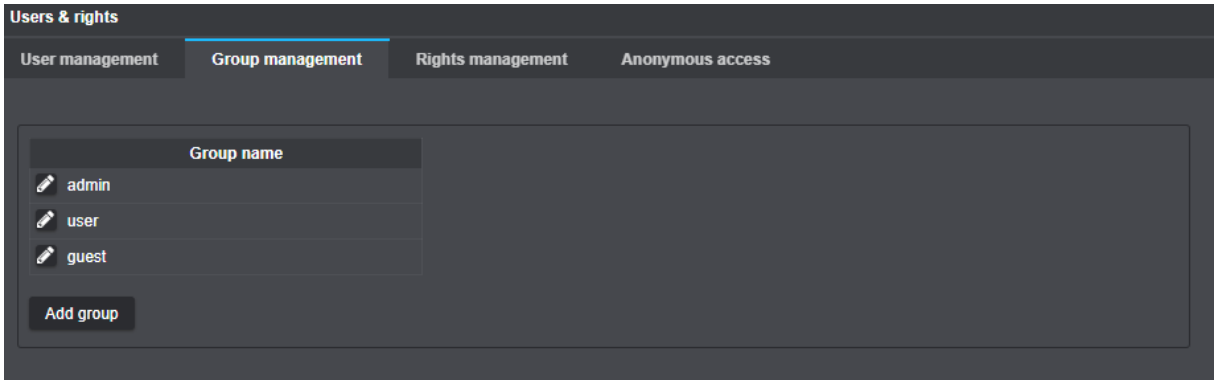

Fig. 16-2

Add Group

- Click **Add group**.
- Enter a unique group name (group names cannot be changed later).
- Finally, click **OK**.

Edit Group

- Click the **Pencil** icon button (to the left of a group name) to edit the members of the group.

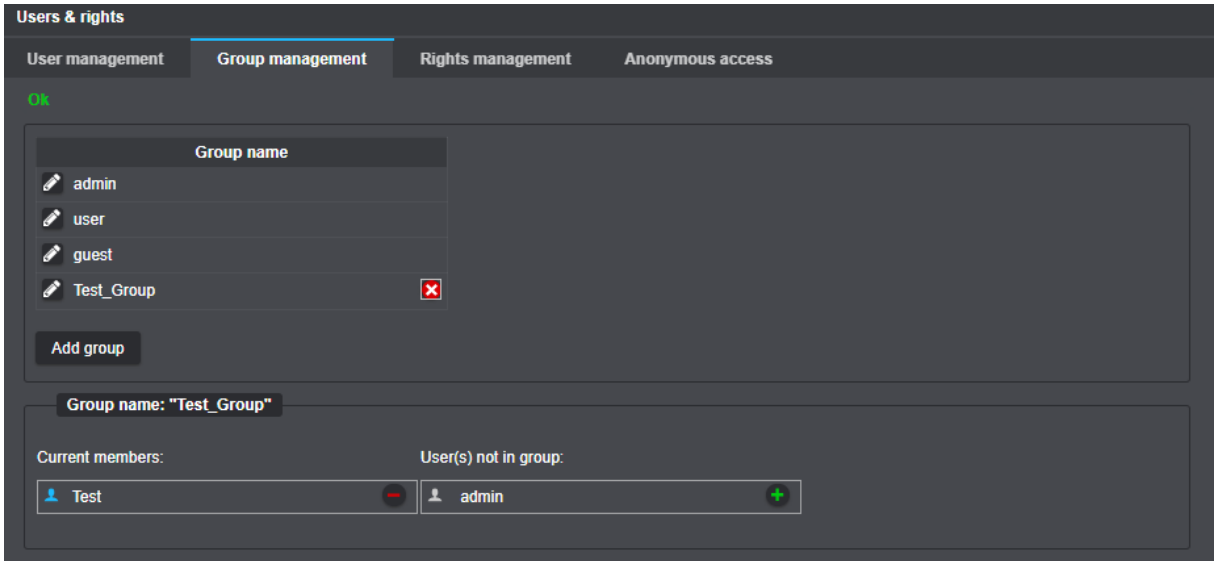

Fig. 16-3

- Click the **+** button (green icon, right column) to assign the user to the group.
- Click the **–** button (red icon, left column) to remove the user from the group.

Delete Group

- Click the "X" button (red icon next to a group name) to delete the group.

Note that the predefined user groups – **admin**, **user**, and **guest** – cannot be deleted.

16.3 RIGHTS MANAGEMENT

Each user group, and therefore the users assigned to it, can be granted individual rights (privileges).

- Open the **Rights management** tab.

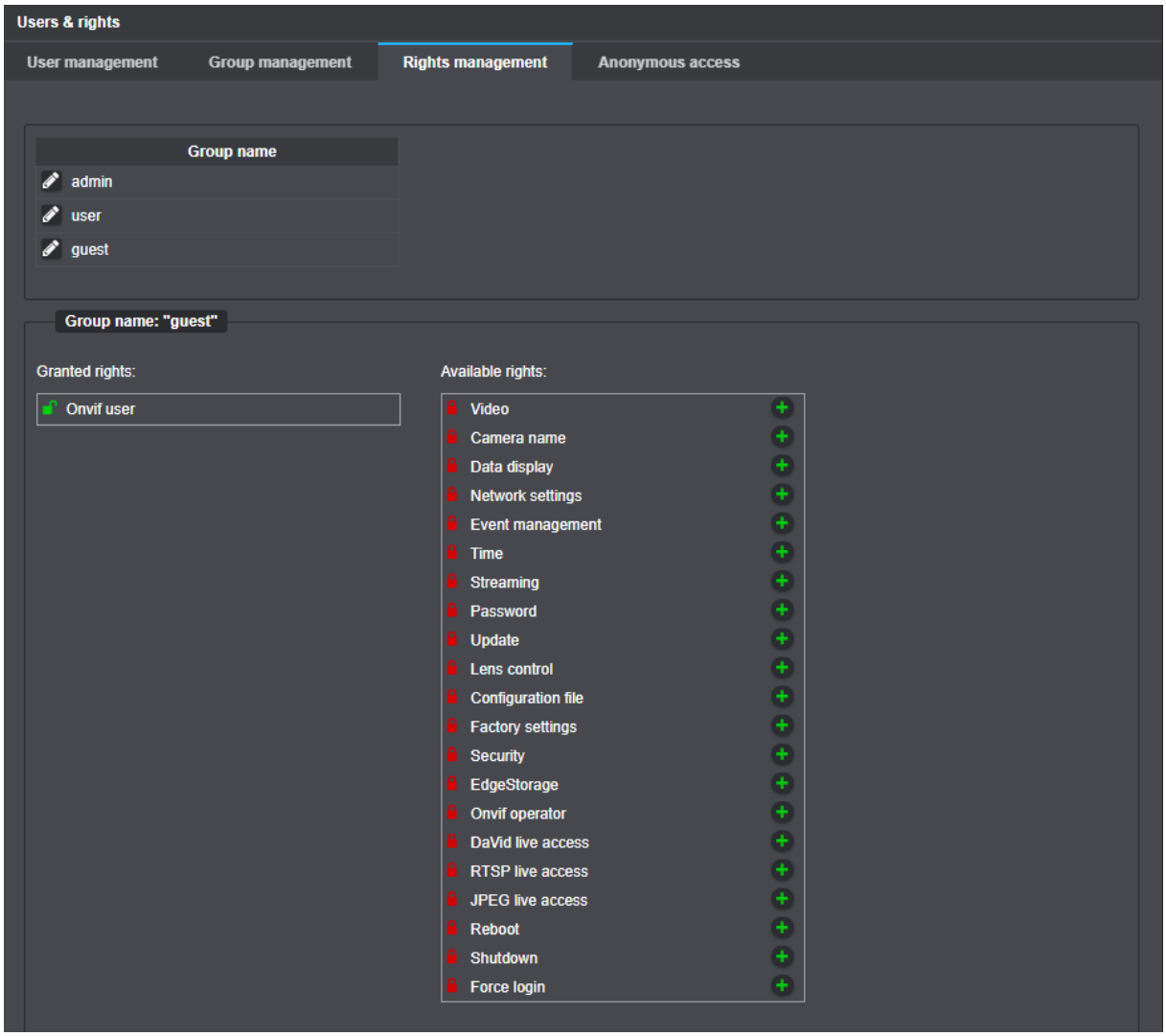

Fig. 16-4

- Click the **Pencil** button (to the left of the group name) to edit the rights (privileges) of the group.
- Click the **+** button (green, right column) to grant a privilege to the group.
- Click the **–** button (red, left column) to remove a privilege from the group.

Note that the privileges of the predefined **admin** user group cannot be restricted.

16.4 ANONYMOUS ACCESS

Anonymous access defines how image transmission without prior user authentication is handled (see “Image Transmission” on page 145).

- Open the **Anonymous access** tab.

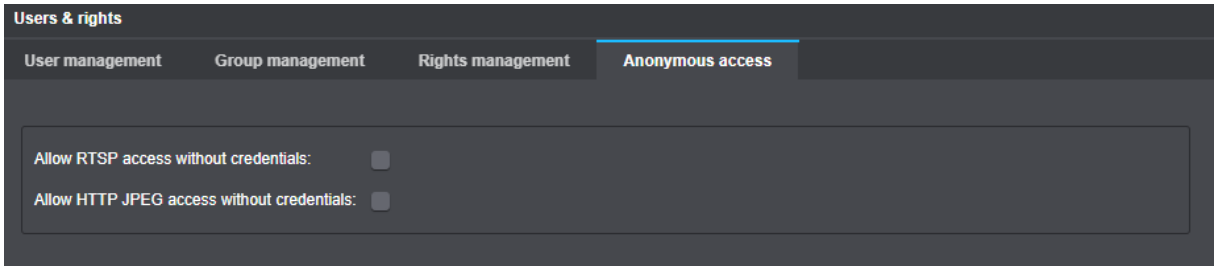

Fig. 16-5

- Select the required checkboxes.

SERVICE

▶ Click the **Service** menu item in the navigation menu.

The **Service** dialog is displayed.

17.1 CONFIGURATION FILE

17.1.1 Export

The device configuration can be exported (fully or in part) and saved as a .cfg file for later reuse.

NOTICE

IP address conflicts due to incorrect network settings

If you want to import the saved configuration file into other cameras (of the same type) in your existing network later on, do not export the **Network settings** to the .cfg file in order to avoid IP address duplicates.

▶ Click the **Configuration file** tab.

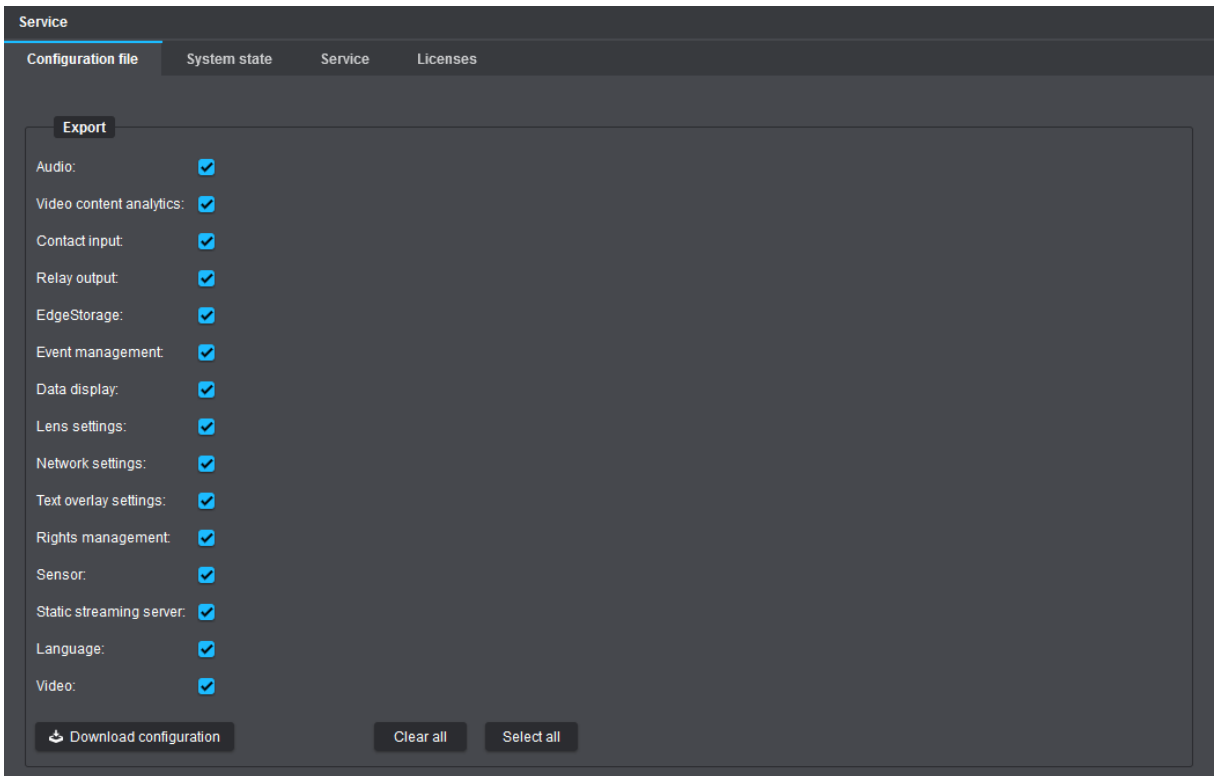

Fig. 17-1

► Under the **Export** section, select the required settings to be exported to the configuration file, such as:

Audio
Exports the audio settings (see chapter "Audio" on page 43).

Video Content Analytics
Exports the video content analysis settings (see chapter "Edge Analytics & AI Apps" on page 100).

Contact Input
Exports the interface settings for the contact inputs (see section "Contact Inputs" on page 73).

Relay Output
Exports the interface settings for the relay outputs (see section "Relay Outputs" on page 72).

EdgeStorage
Exports the EdgeStorage settings (see chapter "EdgeStorage" on page 75).

Event Management
Exports the event management settings (see chapter "Event Management" on page 76).

Data Display
Exports the settings for embedding external texts and interface data (see chapter "Data Display" on page 97).

Lens Settings
Exports the settings for

- Day/Night mode (see section "Day/Night" on page 25),
- Aperture mode and iris position (see section "Exposure Settings" on page 23).

Network Settings
Exports the network settings (see chapter "Network" on page 50).

Text Overlay Settings
Exports the text overlay settings (see section "Text Overlay" on page 31).

Rights Management
Exports the settings for the users and rights management (see chapter "Users & Rights" on page 131).

Sensor
Exports the settings for

- Camera presets (see section "Presets" on page 17),
- Image optimization (see section "Image Optimization" on page 20),
- Corridor mode (see section "Sensor Settings" on page 35).

Static Streaming Server
Exports the settings for the static streaming server (see section "Streaming" on page 55).

Language
Exports the language setting (see chapter “General Settings (Language)” on page 16).

Video
Exports the sensor and the stream/encoder settings (see chapter “Video” on page 35).
Note, however, that the **Corridor mode** setting is exported only by selecting the **Sensor** checkbox.

- Click **Download configuration**.
- Select a folder for saving the configuration file and confirm with **OK**.

> *For later easier identification of the configuration file, the file name consists of the product name and IP address of your device by default.*
> *Unless you specify a different path/folder for saving downloaded files, the .cfg file is saved in the default download folder that you have defined in your web browser.*

17.1.2 Import

Importing configuration files saves time when configuring more complex video security and surveillance systems that use many Dallmeier cameras of the same system design.

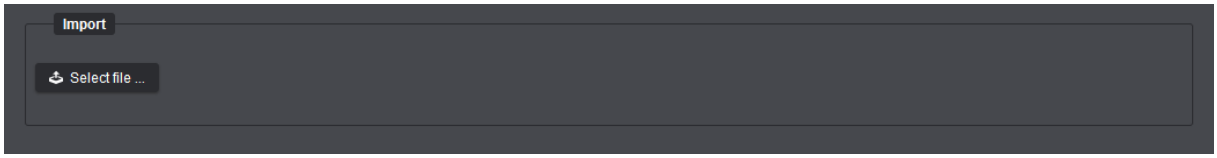

Fig. 17-2

- Under the **Import** section, click **Select file**.
- Using the displayed file explorer, locate and select the configuration file (.cfg) to be imported.
- Click **Open** and confirm with **OK**.

The configuration file is then transferred to the camera.

17.2 SYSTEM STATE

The device can be reset to the factory default settings at any time, if necessary, or rebooted in the unlikely event of a system error or unexpected system behavior.

- Click the **System state** tab.

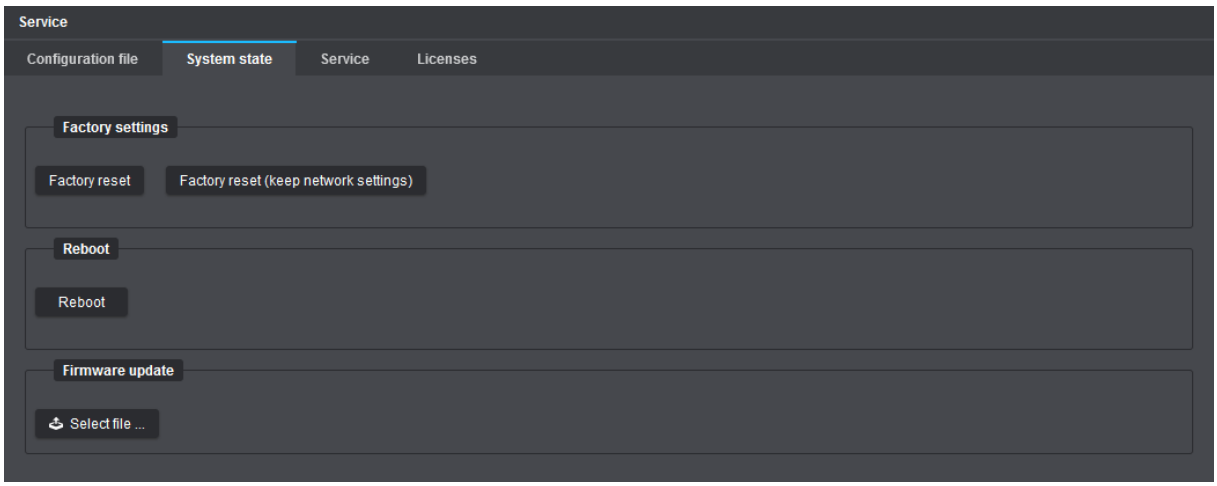

Fig. 17-3.

17.2.1 Factory Settings

- Click **Factory reset** to restore all factory default settings, delete created user accounts, and reset the administration password as well as the network settings (IP address, subnet mask, gateway, etc.), ...

  or

- click **Factory reset (keep network settings)** to restore all factory default settings, but without deleting the created user accounts or resetting the administration password and network settings.

> *Licenses remain valid (until expiration) after resetting the device.*

17.2.2 Reboot

- Click **Reboot** to reboot the device, e.g. in the event of an unexpected system behavior.

17.2.3 Firmware Update

- Regularly check the Dallmeier website at https://www.dallmeier.com/ for the latest release version of Domera® OS (especially with regard to security updates or patches).
- Click **Select file** to transfer an update file (with the .bin file extension) valid for your product model to the camera and start the update process.

17.3 SERVICE

The **Service** tab is intended for special service purposes only and allows you to download the support information regarding your device as a .dat file for the Dallmeier Support if required.

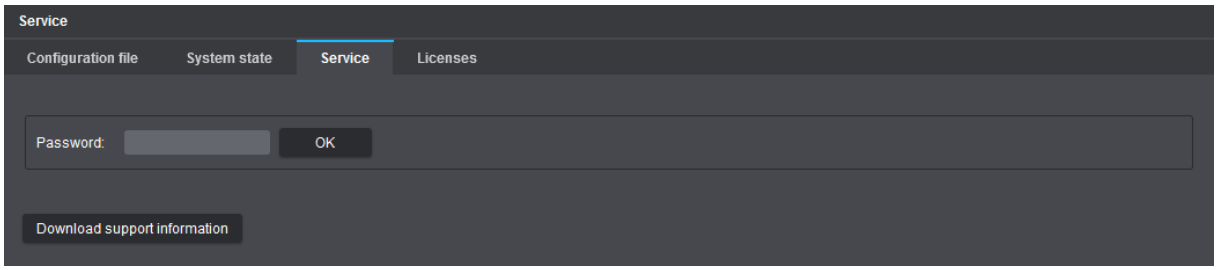

Fig. 17-4

- Click **Download support information**.
- Select a folder for saving the support file and confirm with **OK**.
- If necessary, contact the Dallmeier Support for further instructions.

For later easier identification of the support file, the file name consists of the product name and IP address of your device by default.
Unless you specify a different path/folder for saving downloaded files, the .dat file is saved in the default download folder that you have defined in your web browser.

17.4 LICENSES

On the **Licenses** tab, you can activate optional extra features (additional functions) for your camera or extend the software maintenance license for your camera.

Information on available extra features and software maintenance licenses can be found in the product specification of your camera on the Dallmeier website at https://www.dallmeier.com/.

To purchase a valid license code for a specific extra feature or for extending the software maintenance license, contact your Dallmeier sales partner.

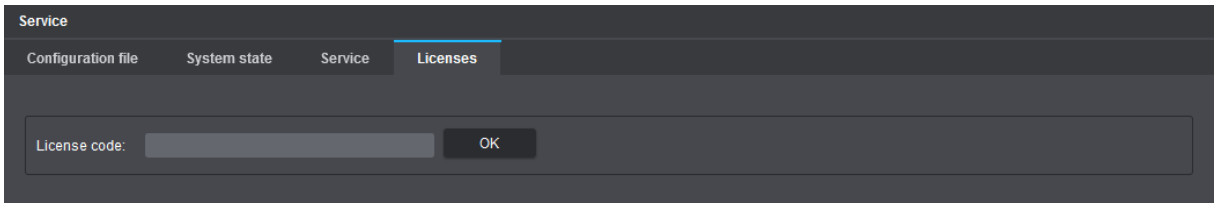

Fig. 17-5

- Enter a valid **License code**.
- Confirm with **OK**.

Depending on the license code entered, either the corresponding extra feature is enabled on your camera and can then be used immediately, or the software maintenance license is automatically extended according to the service package purchased.

> *Information regarding active licenses on your camera, as well as details about the expiration date and time of the software maintenance license currently in use (**Service interval end**) can be found in the **Information** dialog on the **General Information** tab (see section "General Information" on page 142).*

- Note the additional information about software maintenance licenses on the next page.

Important Notes on Software Maintenance Licenses

By default, cameras with Domera® OS come with a free software maintenance license that covers a period of 12 months. This term of validity can be extended either at the time of camera ordering or at a later date by entering a purchased software maintenance license code.

Continuous Licensing History
A continuous software maintenance licensing history is crucial for the ability to successfully update your camera.

For example:
Your camera needs to be updated to a new version of Domera® OS, which will be released in the third year of camera operation. In this case, continuous licensing is required for year 1 (free license), year 2 (first license) and year 3 (second license).

Release Date of the Update File
The release date of the update file is crucial for the ability to successfully update your camera. It must be within a continuous software maintenance licensing period.

For example:
A camera with software maintenance licenses that only cover year 1 + year 2 can still be updated in year 3 of camera operation if the update file was released before the expiration date of the year 2 license.

The term of the free software maintenance license ex works does not start to expire until your camera has been in operation for 500 hours.
Details about the expiration date and time of the software maintenance license currently in use can be accessed via the ***Dallmeier Device Manager****.*

INFORMATION

The **Information** dialog displays various information about the device.

► Click the **Information** menu item in the navigation menu.

18.1 GENERAL INFORMATION

The **General information** tab displays the general information about the device.

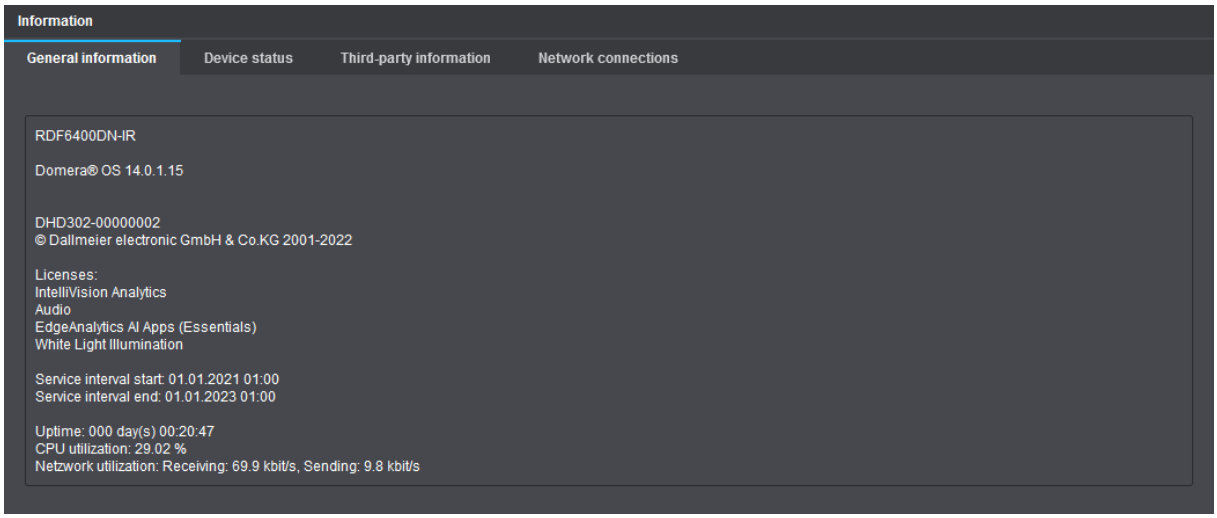

Fig. 18-1

The following data is provided:

- Product model name
- Version number of the installed Domera® OS
- Serial number of the device
- Additional functions currently enabled via license codes (including a possible expiration date)
- Service interval with start and end date (validity of software maintenance license)
- Uptime (elapsed time since the last system start of the device)
- CPU utilization of the device
- Network utilization of the device (current receiving and sending rate)

*With the help of the **Event management** on the camera and the Dallmeier client software **PGuard advance**, you can be automatically notified at an early stage before the service interval of the software maintenance license expires (see section "PGuard Messages" on page 93).*

18.2 DEVICE STATUS

The **Device status** tab displays information about the general status of the device and, if present, information about cyber or IT security issues that need to be addressed.

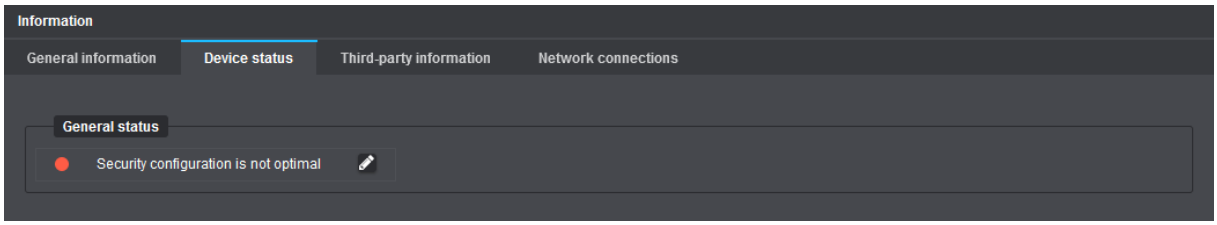

Fig. 18-2

18.3 THIRD-PARTY INFORMATION

The **Third-party information** tab displays information about the used third-party software licenses on the device.

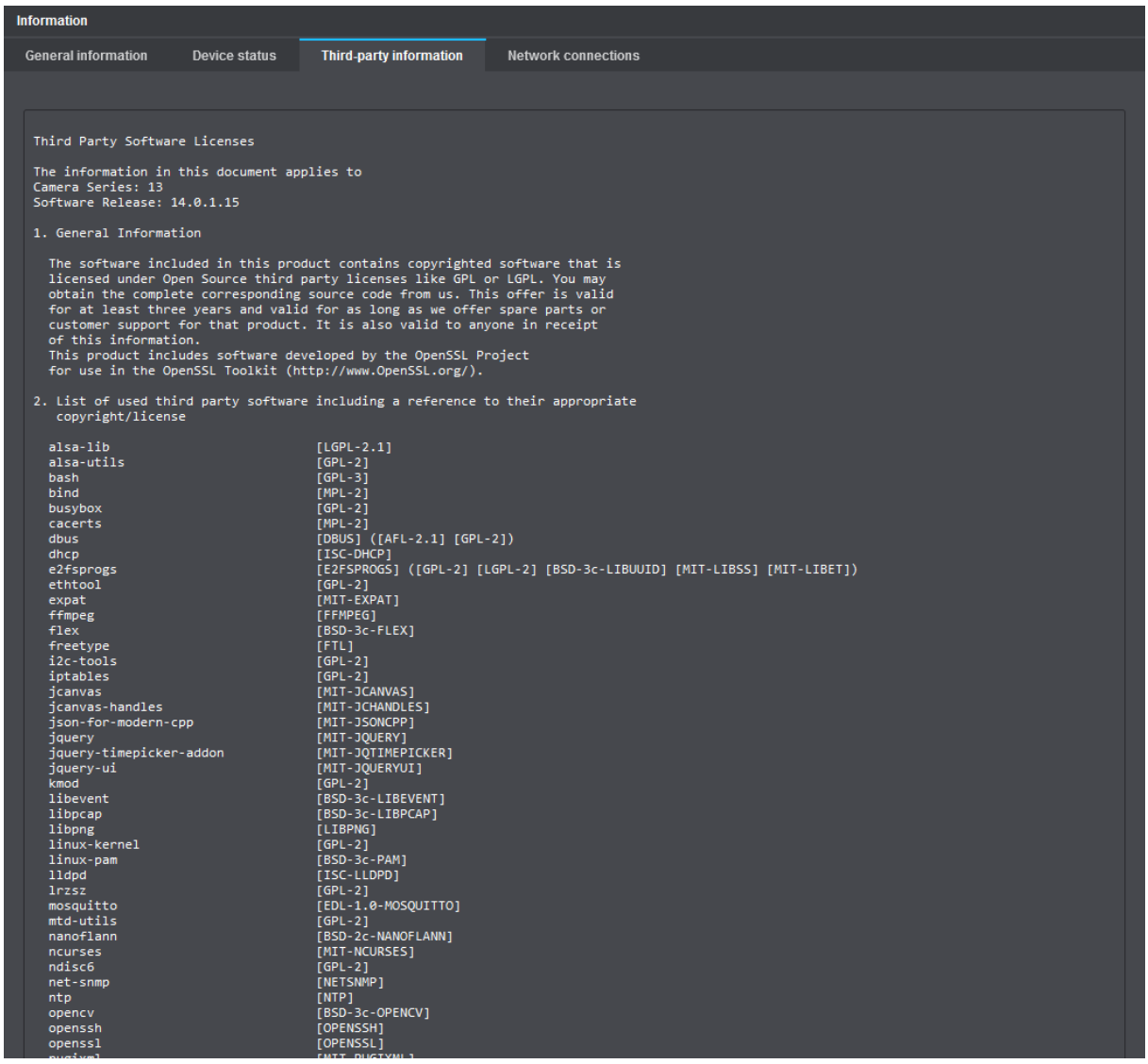

Fig. 18-3

18.4 NETWORK CONNECTIONS

The **Network connections** tab displays information about the currently active network connections that are established to the camera.

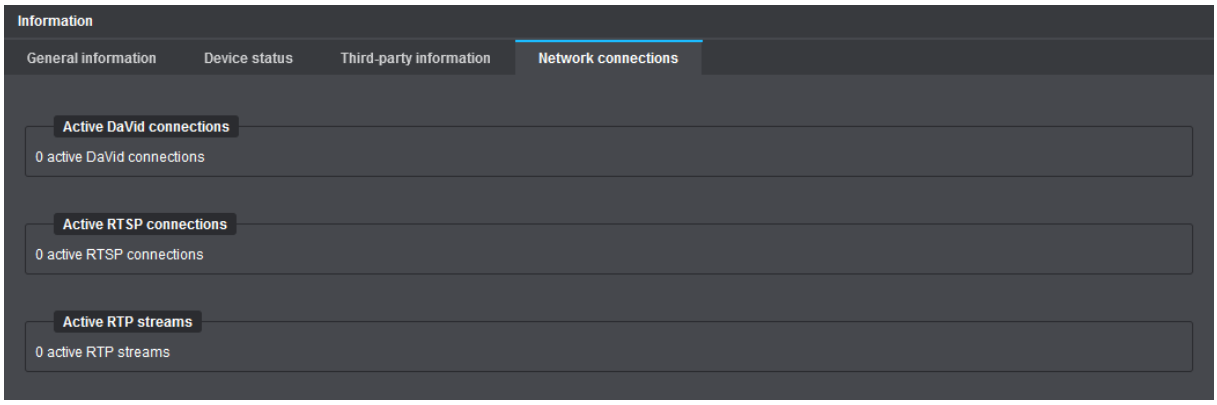

Fig. 18-4

IMAGE TRANSMISSION

The camera can be configured as an active network element for continuous transmission of the generated video data (unicast or multicast streaming) without prior request by a client (see section "Streaming" on page 55).
In addition, as a passive network element, the camera can be requested by external clients and applications to initiate the transmission of the generated video data via various transport, transmission and control protocols.

19.1 STILL IMAGES (JPEG)

Current video data can be requested as still images (JPEG) by any web browser.

Transport protocol:	TCP
Transmission protocol:	HTTP
Port:	80

Note that

- the requested stream must be enabled (**Stream 1** is always enabled).
- the requested stream must be configured for **MJPEG** encoding (otherwise, regardless of the requested stream, only an anamorphic thumbnail/preview image with an aspect ratio of 4:3 and a size of 640×480 pixels is displayed, which looks squeezed in the horizontal dimension and stretched in the vertical dimension).

Also note that either

- the **JPEG live access** right/permission must be granted to a specific user so that any access to the still images is only allowed after prior user authentication (see section "Rights Management" on page 133), ...

  or

- the **Allow JPEG access without credential** checkbox must be selected if you want to allow displaying the still images without prior user authentication (see section "Anonymous Access" on page 134).

Use one of the following HTTP requests for the required stream:

```
[Stream 1]: http://192.168.2.28/live/image0.jpg
[Stream 2]: http://192.168.2.28/live/image1.jpg
[Stream 3]: http://192.168.2.28/live/image2.jpg
```

The default IP address mentioned above is only exemplary and must be replaced with the IP address of your camera.

The displayed still image (JPEG) can be manually refreshed at any time (e.g. by pressing the F5 key on your keyboard).
The HTTP request can also be embedded in an HTML (JavaScript) page that automatically refreshes the image.

19.2 RTSP APPLICATION

The live video can be actively requested by RTSP-capable applications (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 62.

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

RTSP and RTP over HTTP Tunneling

Transmission protocol:	HTTP
Port:	80

Note that

- the requested stream must be enabled (**Stream 1** is always enabled).
- the **RTSP** server in the camera must be enabled (see section "Network Services" on page 62).

Also note that either

- the **RTSP live access** right/permission must be granted to a specific user so that any access to the live video is only allowed after prior user authentication (see section "Rights Management" on page 133), ...

  or

- the **Allow RTSP access without credentials** checkbox must be selected if you want to allow displaying the live video without prior user authentication (see section "Anonymous Access" on page 134).

Use one of the following RTSP requests for the required stream:

```
[Stream 1]: rtsp://192.168.2.28:554/encoder1
[Stream 2]: rtsp://192.168.2.28:554/encoder2
[Stream 3]: rtsp://192.168.2.28:554/encoder3
```

The default IP address mentioned above is only exemplary and must be replaced with the IP address of your camera.

Make sure that after changing the default RTSP port number **554** (see section "Network Services" on page 62), this must also be explicitly changed in the RTSP request.

Example for **Stream 1** with new RTSP port number **1024**:

```
[Stream 1]: rtsp://192.168.2.28:1024/encoder1
```

The available streams 1 to 3 can be requested by three applications simultaneously.
This allows you to realize a so-called “Dual- or Tri-Streaming” functionality (up to three streams with different quality).

If multiple applications are requesting the data of a single stream, the network load and, thus, the required bandwidth increases proportionally. In this case, a multicast configuration should be preferred since this only requires the bandwidth for one stream.

HEADQUARTERS

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

tel +49 941 8700 0
fax +49 941 8700 180
mail info@dallmeier.com

https://www.dallmeier.com/