FLEXIDOME IP micro 3000i - outdoor | FLEXIDOME IP turret 3000i IR - outdoor

NDE-3502-F02 | NDE-3502-F03 | NDE-3503-F02 | NDE-3503-F03 | NTE-3502-F02L | NTE-3502-F03L | NTE-3503-F02L | NTE-3503-F03L

en User manual

Table of contents

1	**Browser connection**	**5**
1.1	System requirements	**5**
1.2	Establishing connection	**5**
1.3	Password Network	**6**
2	**System overview**	**7**
2.1	Live page	**7**
2.2	Playback	**7**
2.3	Configuration	**7**
2.4	Dashboard	**8**
3	**Operation via the browser**	**9**
3.1	Live page	**9**
3.2	Playback page	**11**
3.2.1	Selecting the recording stream	**11**
3.2.2	Searching for recorded video	**12**
3.2.3	Exporting recorded video	**12**
3.2.4	Track list	**12**
3.2.5	Controlling playback	**12**
3.3	Dashboard	**12**
4	**Configuration**	**14**
4.1	General	**14**
4.1.1	Identification	**14**
4.1.2	User Management	**14**
4.1.3	Date/Time	**15**
4.1.4	Display Stamping	**16**
4.1.5	GB/T 28181	**18**
4.2	Web Interface	**18**
4.2.1	Appearance	**18**
4.2.2	'Live' functions	**20**
4.3	Connectivity	**21**
4.3.1	Cloud services	**21**
4.3.2	Accounts	**21**
4.3.3	DynDNS	**22**
4.4	Camera	**22**
4.4.1	Installer Menu	**22**
4.4.2	Color	**26**
4.4.3	ALC	**27**
4.4.4	Enhance	**28**
4.4.5	Encoder Profile	**29**
4.4.6	Encoder Streams	**30**
4.4.7	Encoder Statistics	**31**
4.4.8	Encoder Regions	**31**
4.4.9	Privacy Masks	**32**
4.4.10	Audio	**32**
4.4.11	Pixel Counter	**32**
4.5	Recording	**33**
4.5.1	Storage Management	**33**
4.5.2	Recording Profiles	**34**
4.5.3	Maximum Retention Time	**36**

4.5.4	Recording Scheduler	**36**
4.5.5	Recording Status	**37**
4.5.6	Recording Statistics	**37**
4.5.7	Image Posting	**37**
4.5.8	SD Card Status	**37**
4.6	Alarm	**38**
4.6.1	Alarm Connections	**38**
4.6.2	Video Content Analysis (VCA)	**39**
4.6.3	Audio Alarm	**43**
4.6.4	Alarm E-Mail	**43**
4.6.5	Alarm Inputs	**44**
4.6.6	Alarm Outputs	**45**
4.6.7	Alarm Task Editor	**45**
4.7	Network	**46**
4.7.1	Network Services	**46**
4.7.2	Network Access	**46**
4.7.3	Advanced	**48**
4.7.4	Network Management	**48**
4.7.5	Multicast	**50**
4.7.6	IPv4 filter	**51**
4.8	Service	**51**
4.8.1	Maintenance	**51**
4.8.2	Licenses	**52**
4.8.3	Certificates	**52**
4.8.4	Logging	**53**
4.8.5	System Overview	**53**
5	**Troubleshooting**	**54**
5.1	Physical reset button	**54**
6	**Appendices**	**55**
6.1	Copyright notices	**55**

1 Browser connection

A computer with Microsoft Internet Explorer is used to receive live images, control the unit, and replay stored sequences. The unit is configured over the network using the browser.

1.1 System requirements

Our recommendations are:

- Computer with Dual core HyperThreading processor or better
- Graphic card with performance that matches or is better than the resolution of the camera
- Windows 7 or later operating system
- Network access
- Internet Explorer version 11 or later

  – or –

  Application software, for example, Video Security Client, Bosch Video Client or BVMS.

Note:
To see live images in your browser it might be necessary to download and install the MPEG-ActiveX from the Bosch download store.

1.2 Establishing connection

The unit must have a valid IP address to operate on your network and a compatible subnet mask.
By default, DHCP is pre-set at the factory to **On plus Link-Local** so a DHCP server assigns an IP address or, if no DHCP server is available, a link-local address (auto-IP) is assigned within the range 169.254.1.0 to 169.254.254.255.
You can use IP Helper or Configuration Manager to find the IP address. Download the software from http://downloadstore.boschsecurity.com.

1. Start the Web browser.
2. Enter the IP address of the unit as the URL.
3. During initial installation, confirm any security questions that appear.

Note:
If you cannot connect, the unit may have reached its maximum number of connections. Depending on the device and network configuration, each unit can have up to 50 web browser connections, or up to 100 connections via Bosch Video Client or BVMS.

Password protection in the device
The device is password protected across various authorization levels.
You must set a password for the ‘service’ authorization level to get access to the device.
Make sure the password obeys these conditions:

- 8 to 19 characters in length
- Upper and lower case letters
- Minimum of 1 digit
- Minimum of 1 special character

  These special characters are not allowed: ‘@’, ‘&’, ‘<’, ‘>’, ‘:’, ‘+’

1. Enter the password in the two text fields.
2. Click **Set**. If the password is valid, you get access to the device.

1.3 Password Network

If a RADIUS server is used for network access control (802.1x authentication), the unit must be configured first. To configure the unit, connect it directly to a computer using a network cable and configure the two parameters, **Identity** and **Password**. Only after these have been configured can communication with the unit via the network occur.

2 System overview

When a connection is established, the **Live** page is initially displayed.
The application bar displays the following icons:

	Live	Click this icon to view the live video stream.
	Playback	Click this icon to play back recorded sequences. This link is only visible if a storage medium has been configured for recording. (With VRM recording, this option is not active.)
	Configuration	Click this icon to configure the device.
	Dashboard	Click this icon to see detailed system information.
	Links	Click this icon to navigate to the Bosch download store.
	Logout	Click this icon to log out of the device.
		Click this icon to get context-sensitive help for the page you are browsing.

2.1 Live page

The **Live** page is used to display the live video stream and control the unit.

2.2 Playback

The **Playback** page is used for playing back recorded sequences.

2.3 Configuration

The **Configuration** page is used to configure the unit and the application interface.

Making Changes

Each configuration screen shows the current settings. You can change the settings by entering new values or by selecting a predefined value from a list field.
Not every page has a **Set** button. Changes to pages without a **Set** button are set immediately.
If a page does show a **Set** button, you must click the **Set** button for a change to take effect.

Notice!
Save each change with the associated **Set** button.
Clicking the **Set** button saves the settings only in the current field. Changes in any other fields are ignored.

Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.

2. Click the **Set and Reboot** button. The camera reboots and the changed settings are activated.

2.4 Dashboard

The **Dashboard** page is used to display detailed information about the device.
The **Dashboard** is only visible in the application bar if the **Show 'Dashboard'** option is enabled by a service-level user in the **Configuration** -> **Web Interface** -> **Appearance** page.

3 Operation via the browser

3.1 Live page

After the connection is established, the **Live** page is initially displayed. It shows the live video image on the right of the browser window. Depending on the configuration, various text overlays may be visible on the live video image.

Other information may also be shown next to the live video image. The items shown depend on the settings on the **'Live' functions** page.

Connection

In the **Connection** group, you can configure the **Stream** option.

Image selection

To view a live stream:

1. On the left side of the browser, expand the **Connection** group if necessary.
2. Click the **Stream** drop-down arrow to see the options.
3. Select the stream you wish to view.

ROI

If **Stream 2** is set to **SD ROI**, the **ROI** and **Pre-positions** groups become available.

– Navigate to **Configuration** -> **Camera** -> **Encoder Streams**
– Set **Stream 2** to **SD ROI**
– Click **Set** to save the settings
– Go back to the **Live** page
– In the **Connection** group, click the **Stream** drop down arrow to see the options
– Select **Stream 2**

The **ROI** and **Pre-positions** groups are now enabled.

To use the **ROI** functionality, follow these steps:

– On the left side of the browser, expand the **ROI** group if necessary.
– Use the controls to move around the image.
– Click **+** to zoom and **-** to zoom out.

Pre-Positions

Six pre-position files can be defined for views generated by the region of interest (ROI) controls.

1. On the left side of the browser, expand the **Pre-positions** group if necessary.
2. Use the ROI controls to define a particular view.
3. To store this view, click the icon of one of the six pre-position buttons.
   – If a pre-position is already stored, a dialog box displays a message. Click **OK** to overwrite or **Cancel** to cancel the operation
4. To recall a stored pre-position, click a pre-position button.

Digital I/O

Depending on the configuration of the unit, the alarm input and the output are displayed next to the image. Expand the Digital I/O group if necessary.

The alarm symbol is for information and indicates the status of an alarm input:

– The symbol lights when the input alarm is active.

The alarm output allows the operation of an external device (for example, a light or a door opener).

– To activate the output, click the checkmark symbol.
  – The symbol lights when the output is activated.

Recording status

The hard drive icon below the live camera image changes during an automatic recording. The icon lights up and displays a moving graphic to indicate a running recording. If no recording is taking place, a static icon is displayed.

Full-screen display

Click the full-screen icon to view the selected stream in full-screen mode; press **Esc** on the keyboard to return to the normal viewing window.

Saving snapshots

Individual images from the displayed live video stream can be saved locally in JPEG format on the computer's hard drive. The storage location depends on the configuration of the camera.

– Click the photo camera icon to save a single image.

Recording live video

Video sequences from the displayed live video stream can be saved locally on the computer's hard drive. The sequences are recorded at the resolution specified in the encoder configuration. The storage location depends on the configuration of the camera.

1. Click the recording icon to record video sequences.
   – Saving begins immediately. The red dot on the icon indicates that a recording is in progress.
2. Click the recording icon again to stop recording.

Start Video Security app

To start the Video Security app, click .

Show latest event

Click the **Show latest event** icon to watch the last recorded important events. The **Playback** page opens.

Storage, CPU and network status

When accessing the unit with a browser, the local storage, processor and network status icons are shown in the upper right of the window.

When a local storage card is available, the memory card icon changes color (green, orange or red) to indicate the local storage activity. If you hover over this icon with the mouse the storage activity is shown as a percentage.

If you hover over the middle icon, the CPU load is shown.

If you hover over the right-hand icon, the network load is shown.

This information can help with problem solving or when fine tuning the unit. For example:

– if the storage activity is too high, change the recording profile,
– if the CPU load is too big, change the VCA settings,
– if the network load is too big, change the encoder profile to reduce bitrate.

Status icons

Various overlays in the video image provide important status information. The overlays provide the following information:

Decoding error

The frame might show artifacts due to decoding errors.

Alarm flag

Indicates that an alarm has occurred.

Communication error

A communication error, such as a connection failure to the storage medium, a protocol violation or a timeout, is indicated by this icon.

Gap

Indicates a gap in the recorded video.

Watermark valid

The watermark set on the media item is valid. The color of the check mark changes according to the video authentication method that has been selected.

Watermark invalid

Indicates that the watermark is not valid.

Motion alarm

Indicates that a motion alarm has occurred.

Storage discovery

Indicates that recorded video is being retrieved.

3.2 Playback page

Click **Playback** in the application bar to view, search or export recordings. This link is only visible when a direct iSCSI or memory card is configured for recording (with Video Recording Manager (VRM) recording this option is not active).

On the left side of the screen, there are four groups:

- **Connection**
- **Search**
- **Export**
- **Track list**

3.2.1 Selecting the recording stream

On the left side of the browser, expand the **Connection** group if necessary.

To view a recording stream:

1. Click the **Recording** arrow to see the options.
2. Select recording stream 1 or 2.

3.2.2 Searching for recorded video

On the left side of the browser, expand the **Search** group if necessary.

1. To limit the search to a particular time range, enter the date and times for the start and stop points.
2. Select an option from the drop-down box to define a search parameter.
3. Click **Search**.
4. The results are shown.
5. Click a result to play it back.
6. Click **Back** to define a new search.

3.2.3 Exporting recorded video

On the left side of the browser, expand the **Export** group if necessary.

1. Select a track in the track list or in the search results (or click on the timeline below the video window and drag the buttons to mark the sequence you want to export).
2. The start and stop date and time are filled-in for the selected track. If required, change the times.
3. In the **Time lapse** drop-down box, select the original or a condensed speed.
4. In the **Location** drop-down box, select a target.
5. Click **Export** to save the video track.

Note:
The target server address is set on the **Network** / **Accounts** page.

3.2.4 Track list

The **Track list** shows all the available recordings.

3.2.5 Controlling playback

The time bar below the video image allows quick orientation. The time interval associated with the sequence is displayed in the bar in gray. Arrows indicate the position of the image currently being played back within the sequence.
The time bar offers various options for navigation in and between sequences.

– If required, click in the bar at the point in time at which the playback should begin.
– Change the time interval displayed by clicking the plus or minus icons or use the mouse scroll wheel. The display can span a range from six months to one minute.
– Click the alarm jump buttons to go from one alarm event to the next or to the previous one. Red bars indicate the points in time where alarms were triggered.

Controls
Control playback by means of the buttons below the video image.
The buttons have the following functions:

– Start/Pause playback
– Select the playback (forward or backward) speed using the speed regulator
– Step forward or backward frame-by-frame when paused (small arrows)

3.3 Dashboard

The **Dashboard** page shows information on 4 topics:

– **Device status**
– **Recording status**
– **Connection Status**
– **Services**

You can also download a .JSON file with information about the device:

1. At the bottom of the page, locate the **Export** button
2. Click the **Export** button
3. Select a location in your hard drive to store the file

4 Configuration

4.1 General

4.1.1 Identification

Device name

Assign a unique name to assist in identification. This name simplifies the management of multiple devices in more extensive systems.

The name is used for remote identification, for example, in the event of an alarm. Choose a name that makes it as easy as possible to identify the location unambiguously.

Device ID

Each device should be assigned a unique identifier that can be entered here as an additional means of identification.

Video name

Each video channel can be given a name. Click the + sign to add an extra line.

Host name

Enter the host name registered for the device.

Initiator extension

Add text to an initiator name to make identification easier in large iSCSI systems. This text is added to the initiator name, separated from it by a full stop. (You can see the initiator name in the System Overview page.)

Click **Set** to apply the changes.

4.1.2 User Management

A password prevents unauthorized access to the device. You can use different authorization levels to limit access.

Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you must always start from the highest authorization level when assigning passwords.

You can define and change a password for each authorization level if you are logged into the “service” user account.

Authentication modes

The section **Authentication modes** provides information about the authentication modes set in the camera. A checkmark appears in the checkbox to the left of the mode if the mode is set. If the mode is not set, the phrase “No certificate installed” appears to the right of the mode name.

This device has three authentication modes:

– **Password** indicates a password is set for the camera. It prevents unauthorized access to the device, and can use different authorization levels to limit access.
  Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you must always start from the highest authorization level when assigning passwords.
  You can define and change a password for each authorization level if you are logged into the service user account.
– **Certificate**. A check mark in this check box indicates that at least one certificate is loaded onto the device.
  The Trusted certificate is a root certificate for Bosch Security Systems that proves that the device meets the following criteria:

  - It originates from a Bosch factory that is a secure environment.
  - It has not been tampered with.

  The Trusted certificate is issued by Escrypt. Escrypt is a Bosch company and Certificate Authority (CA).
- **Active Directory server (AD FS)**. A check mark in this check box indicates that the device uses an active directory server.

Creating a new user

To create a new user, click **Add** in the section below **Authentication modes**.

In the box **User**, fill in the fields:

1. User name: Enter a name with a minimum of 5 and a maximum of 31 characters.
2. **Group**, select the appropriate authorization level:
   - live is the lowest authorization level. At this level, it is only possible to view the live video image, and switch between the different live image displays.
   - user is the middle authorization level. At this level, it is possible to operate the device and playback recordings, but configuration changes are not possible.
   - service is the highest authorization level. Entering the correct password gives access to all the functions, and allows all configuration settings to be changed.
3. **Type**, select either:
   - **Password** for a new password.
     Use a minimum of 8 and a maximum of 19 characters. The password must have upper-case and lower-case letters, one or more numerical digits and one or more of these special characters ! ? ” # $ % ( ) { } [ ] * - = . , ; ^ _ | ~ \
     Special characters such as space @ : < > ‘ & + are not valid.
     In this case, enter the new password a second time to eliminate typing mistakes.
   - **Certificate** for a certificate that the new user is authorized to use.
4. Click **Set** to confirm and create a new user.

4.1.3 Date/Time

Date format

Select the required date format.

Device date/Device time

If there are multiple devices operating in your system or network, it is important to synchronize their internal clocks. For example, it is only possible to identify and correctly evaluate simultaneous recordings when all devices are operating on the same time.

1. Enter the current date. Since the device time is controlled by the internal clock, it is not necessary to enter the day of the week – it is added automatically.
2. Enter the current time or click **Sync to PC** to apply the system time from your computer to the device.

Note:

It is important that the date/time is correct for recording. An incorrect date/time setting could prevent correct recording.

Device time zone

Select the time zone in which the system is located.

Daylight saving time

The internal clock can switch automatically between normal and daylight saving time (DST). The unit already contains the data for DST switch-overs for many years in advance. If the date, time and zone have been set up correctly, a DST table is automatically created.

If you decide to create alternative daylight saving time dates by editing the table, note that values occur in linked pairs (DST start and end dates).

First, check the time zone setting. If it is not correct, select the appropriate time zone and click **Set**.

1. Click **Details** to edit the DST table.
2. Click **Generate** to fill the table with the preset values from the unit.
3. Click one of the entries in the table to make changes. The entry is highlighted.
4. Click **Delete** to remove the entry from the table.
5. Choose other values from the list boxes under the table, to change the selected entry. Changes are immediate.
6. If there are empty lines at the bottom of the table, for example after deletions, add new data by marking the row and selecting values from the list boxes.
7. When finished, click **OK** to save and activate the table.

Time server address

The unit can receive the time signal from a time server using various time server protocols and then use it to set the internal clock. The device polls the time signal automatically once every minute.

Enter the IP address of a time server.

Overwrite by DHCP

Select this checkbox to have the DHCP server give the time server date.

Time server type

- Select **Time protocol** if the server uses the RFC 868 protocol.
- Select the protocol that is supported by the selected time server. It is recommended to select the **SNTP protocol**. This protocol provides high accuracy and is required for special applications and future function extensions.
- Select the **TLS protocol** if the server uses the RFC 5246 protocol.

Click **Set** to apply the changes.

4.1.4 Display Stamping

Various overlays or stamps in the video image provide important supplementary information. These overlays can be enabled individually and arranged on the image in a clear manner.

Camera name stamping

Select the position of the camera name overlay in the drop-down box. It can be displayed at the **Top**, at the **Bottom**, or at a position of choice using the **Custom** option, or it can be set to **Off** for no overlay information.

If the **Custom** option is selected, enter values in the X and Y position fields.

Optionally, tick the **Underlay with full-width bar** box to place a full-width background-bar beneath the time stamp.

Logo

To place a logo on the image, select and upload an uncompressed .bmp file with a maximum size of 300x300 pixels and 256 colors to the camera. Its position on the image can then be selected.

Logo position
This option becomes available when the **Camera name stamping** option is enabled. Select:
- **Off** : This option is disabled.
- **To the left of the name**: The logo will be positioned to the left of the **Camera name stamping**
- **To the right of the name**: The logo will be positioned to the right of the **Camera name stamping**
- **Logo only**: The logo will be shown without the **Camera name stamping**.

Time stamping
Select the position of the time and date overlay in the drop-down box. It can be displayed at the **Top**, at the **Bottom**, or at a position of choice using the **Custom** option, or it can be set to **Off** for no overlay information.
If the **Custom** option is selected, enter values in the X and Y position fields.

Display milliseconds
If necessary, display milliseconds for **Time stamping**. This information can be useful for recorded video images; however, it does increase the processor's computing time. Select **Off** if displaying milliseconds is not needed.

Live video indicator
Select **On** to display the **Live video indicator**, an icon that pulses on the OSD to show that the video stream is live.
Select **Off** to hide the **Live video indicator**.

Alarm mode stamping
Select **On** in the drop-down box for a text message to be displayed in the event of an alarm. It can be displayed at a position of choice using the **Custom** option, or it can be set to **Off** for no overlay information.
If the **Custom** option is selected, enter values in the X and Y position fields.

Alarm message
Enter the message to be displayed on the image in the event of an alarm. The maximum text length is 31 characters.

Transparent background
Check this box to make transparent the stamp background on the image.

Text color
Select the color for the alarm message to be displayed in.

Background color
Select the background color for the alarm message to be displayed in.
If you have enabled the **Transparent background** option, the background color is not displayed in the OSD.

Stamping size
Select the desired font size of the overlays on the OSD: **Normal** or **Large**.

Video authentication
Select from the **Video authentication** drop-down box a method for verifying the integrity of the video.
If you select **Watermarking**, all images are marked with an icon. The icon indicates if the sequence (live or saved) has been manipulated.
If you want to add a digital signature to the transmitted video images to ensure their integrity, select one of the cryptographic algorithms for this signature.

Signature interval [s]
For certain **Video authentication** modes, enter the interval (in seconds) between insertions of the digital signature.
Click **Set** to apply the changes.

4.1.5 GB/T 28181

This page allows you to set the parameters for conformance to the GB/T 28181 national standard “Security and protection video monitoring network system for information transport, switch and control”. This standard is specifically for China.

Enable
Select this checkbox to enable the system to use the other parameters on this page in accordance with the GB/T 28181 national standard.

H.264 elementary stream
Select this checkbox to select or to enable the H.264 elementary stream.

Registration timeout
Enter a value (in milliseconds) for the registration timeout. The default is 3600.

Heartbeat timeout
Enter the value (in seconds) for the heartbeat timeout. The default is 15.

Server ID
Enter the ID of the server.

Server IP address
Enter the server IP address.

Server port
Enter the number of the server port. The default is 0.

Device ID
Enter the ID of the device.

Device port
Enter the number of the device port. The default is 5060.

Password
Enter the appropriate password.

Alarm device ID
Enter the ID of the alarm device.
Click **Set** to apply the changes.

4.2 Web Interface

4.2.1 Appearance

You can adapt the appearance of the web interface and change the website language to meet your requirements.
You can use GIF or JPEG images to replace the company and device logos. The image can be stored on a web server.
Make sure that a connection to the web server is always available to display the image. The image files are not stored on the device.
To use the original graphics, delete the entries in the **Company logo** and **Device logo** fields.

Website language
Select the language for the user interface.

Company logo
To replace the company's logo in the top-right part of the window, enter the path to a suitable image in this field. The image file must be stored on a web server.

Device logo
To replace the device name in the top-left part of the window, enter the path to a suitable image in this field. The image file must be stored on a web server.

Show VCA metadata
When video content analysis (VCA) is activated, additional information is displayed in the live video stream. With the MOTION+ analysis type, for example, the sensor fields in which motion is recorded are marked with yellow rectangles.
Using Essential Video Analytics, the outlines of detected objects are displayed in following colors:
– Red: Objects that generate an alarm event under the current settings appear on the camera image inside a red outline.
– Orange: An object that has triggered one alarm event but does not generate another appears inside an orange outline (example: object has crossed a line). During forensic search, an object that triggers an alarm event has an orange outline from the beginning.
– Yellow: Objects that are detected as moving but do not generate an alarm event under the current settings appear inside a yellow outline.

Show VCA trajectories
When video content analysis (VCA) is activated, check this item to show additional information that traces the path of objects, if the corresponding analysis type provides this data.

Show overlay icons
Select this check box to show overlay icons on the live video image.

Show VCA items
Select this checkbox to show VCA items on the live video image.
Shows alarm fields, lines and routes configured for the video analytics in the following colors:
– Green: Fields, lines and routes used in a task are displayed in green. They can be edited but not deleted.
– Red: Fields, lines and routes currently in alarm mode are displayed in red.

Show 'Dashboard'
Select this checkbox to enable the **Dashboard** in the application bar.

Secure cookies
Select this checkbox to secure the cookies sent through the camera.

Notice!
If cookies are secured, authentication forwarding to MPEG ActiveX and the Video Security App is prohibited.

Video player
Select the type of player to be used for live mode viewing.
Latency mode
Select the required latency mode:
– **Low delay:** Default mode. Provides marginal buffering to display fluent video under normal network conditions.
– **Smooth video:** Allows the buffer to automatically adjust to cover network jitter, inducing higher latency.

– **No buffering**: Shows video as it is received by the decoder with minimum latency. Allows the video to jerk if there is network jitter.

Video buffer
The value shown is calculated from the **Latency mode** setting. It cannot be changed.

JPEG resolution
You can specify the size of the JPEG image on the **Live** page. Options are **Small**, **Medium**, **Large**, 720p, 1080p, and "**Best possible**" (default).

JPEG interval
You can specify the interval at which the individual images should be generated for the M-JPEG image on the **Live** page.

JPEG quality
You can specify the quality at which the JPEG images appear on the **Live** page.
Click **Set** to apply the changes.

4.2.2 'Live' functions

You can adapt the **Live** page functions to meet your requirements. Choose from a variety of different options for displaying information and controls.

1. Select the check boxes for the functions to be displayed on the **Live** page. The selected elements are checked.
2. Check to see if the desired items are shown.

Transmit audio
When selected, the audio from the camera (if set to **On** on the **Audio** page) is sent to the computer. This setting applies only to the computer on which the selection is made. Transmitting audio data requires additional network bandwidth.

Lease time [s]
The lease time in seconds determines the time beyond which a different user is authorized to control the camera after no further control signals are received from the current user. After this time interval, the camera is automatically available for another user.

Auto logout time [min]
Set a time frame (in minutes) for the automatic logout. Default value is 0 (no automatic logout).

Show alarm inputs
The alarm inputs are displayed next to the video image as icons along with their assigned names. If an alarm is active, the corresponding icon changes color.

Show alarm outputs
Alarm outputs are shown next to the video image as icons along with their assigned names. If an output is switched, the icon changes color.

Allow snapshots
Specify whether the icon for saving individual images should be displayed below the live image. Individual images can only be saved if this icon is visible.

Allow local recording
Specify whether the icon for saving video sequences locally should be displayed below the live image. Video sequences can only be saved locally on your hard disk if this icon is visible.

I-frames-only stream
When this checkbox is enabled, the **I-frames** stream option on the **Connection** tab of the **Live** page becomes available.

Show 'Pre-positions'
Select to display or hide the pre-positions widget on the live page.

Path for JPEG and video files
Enter the path for the storage location of individual images and video sequences saved from the **Live** page.

Video file format
Select a file format for the live page display. The MP4 format does not include metadata.
Click **Set** to apply the changes.

4.3 Connectivity

4.3.1 Cloud services

Bosch Remote Portal
Operation
The operation mode determines how the camera communicates with the Bosch Remote Portal.
– Select **On** to poll the server constantly.
– Select **Off** to block polling.

Connectivity state
This field indicates the device's connectivity state with Bosch Remote Portal.
– If the device is registered and the operation mode is set to **On**, the state will indicate that the device is Connected (to the cloud service).
Note: The **Visit Remote Portal** button will become active.

– If the device is not registered or the operation mode is set to **Off**, the state will indicate that the device is **Not available**.
Note: The **Register** button will become active only if you have not registered the device to the Bosch Remote Portal.

Stratocast
Enter the Stratocast **Registration code** to connect with the Genetec's Stratocast cloud.
Click **Register** to activate the account.

4.3.2 Accounts

Four separate accounts can be defined for posting and recording export.

Type
Select either FTP or Dropbox for the account type.
Before using a Dropbox account ensure that the time settings of the device have been correctly synchronized.

Account name
Enter an account name to be shown as the target name.

FTP server IP address
For an FTP server, enter the IP address.

FTP server login
Enter your login name for the account server.

FTP server password
Enter the password that gives access to the account server. Click Check to confirm that it is correct.

Path
Enter an exact path to post the images on the account server. Click **Browse...** to browse to the required path.

Maximum bit rate
Enter the maximum bit rate in kbps that will be allowed when communicating with the account.

Encryption
Tick the box to use a secure FTP over TLS connection.
Click **Set** to apply the changes.

4.3.3 DynDNS

A dynamic Domain Name Service (DNS) allows you to select the unit via the Internet using a host name, without having to know the current IP address of the unit. You can enable this service here. To do this, you must have an account with one of the dynamic DNS providers and you must register the required host name for the unit on that site.

Note:
For information about the service, registration process and available host names refer to the provider.

Provider
Select your dynamic DNS Provider from the drop-down list.

Host name
Enter the host name registered for the unit.

User name
Enter the user name you registered.

Password
Enter the password you registered.

Force registration now
Force the registration by transferring the IP address to the DynDNS server. Entries that change frequently are not provided in the Domain Name System. It is a good idea to force the registration when setting up the device for the first time. Only use this function when necessary and no more than once a day, to avoid the possibility of being blocked by the service provider. To transfer the IP address of the device, click the **Register** button.

Status
The status of the DynDNS function is displayed here for information purposes; these settings cannot be changed.
Click **Set** to apply the changes.

4.4 Camera

4.4.1 Installer Menu

Sensor mode
The **Sensor mode** specifies the quality of the image for each situation. Fast moving scenes use more frame rates for better image quality than slow moving scenes. Adjust this setting as necessary.

Image rotation
Select the required angle (0°, 90°, 180° or 270°) to output the correct image orientation.

Mirror image
Select **On** to output a mirror image of the camera picture.

Coding standard
Select the encoding mode:
– H.264
– H.265

Camera LED
Disable the **Camera LED** on the camera to switch it off.

Analog output
Select an aspect ratio format to activate the analog output.
Select **Permanently inactive** to deactivate the analog output.
Note: **Automatic mode** is selected by default for installation purposes upon first connecting the device.

Reboot device
Click **Reboot** to restart the device.

Factory defaults
Click **Defaults** to restore the factory defaults for the camera. A confirmation screen appears. Allow several seconds for the camera to optimize the picture after a reset.

Positioning
The **Positioning** feature describes the location of the camera and the perspective in the camera's field of view.
Perspective information is essential to Video Analytics, as it enables the system to compensate for the illusory smallness of distant objects.
Only through use of perspective information is it possible to distinguish objects such as persons, bicycles, cars and trucks, and accurately compute their real size and speeds as they move through 3D space.
However, to calculate perspective information accurately, the camera must be directed at a single, flat horizontal plane. Multiple and inclined planes, hills, stairs can falsify perspective information and produce incorrect object information such as size and speed.

Mounting position
The mounting position describes the perspective information that is also often called calibration.
In general, the mounting position is determined by the parameters of the camera such as height, roll angle, tilt angle, and focal length.
The height of the camera must always be entered manually. Whenever possible, roll angle and tilt angle are provided by the camera itself. The focal length is provided, if the camera has a built-in lens.

Tilt angle [°]
Enter the tilt angle if the value is not determined by the camera.
The tilt angle describes the angle between the horizontal and the camera.
A tilt angle of 0° means that the camera is mounted parallel to the ground.
A tilt angle of 90° means that the camera is mounted vertically in bird's eye view perspective.
The flatter the tilt angle is set, the less accurate the estimate of object sizes and speeds will be. The settings must be between 0° and 90°. Estimates are no longer possible when you have reached 0°.

Roll angle [°]
Enter the roll angle if the value is not determined by the camera.
The roll angle describes the angle between the roll axis and the horizontal plane. The angle can deviate from the horizontal by up to 45°.

Height [m]
Enter the height in meters of the position of the camera.
The height describes the vertical distance from the camera to the ground plane of the captured image. Typically the elevation of the mounted camera above the ground.

Focal length [mm]
Enter the focal length in millimeters of the position of the camera if the value is not determined by the camera.
The focal length is determined by the lens. The shorter the focal length, the wider the field of view. The longer the focal length, the narrower the field of view and the higher the magnification.

Show sensor values...
Click to automatically see the camera parameters, for example, **Tilt angle [°]**, **Roll angle [°]** and **Focal length [mm]**. These calibration values are measured by the device sensors. Click **OK** to transfer them to the **Positioning** settings page.

Sketch
Click to improve the automatic calibration. The **Sketch-based calibration** window is displayed.
The **Sketch** functionality offers an additional, half-automatic calibration method. This calibration method allows you to describe the perspective in the camera's field of view by drawing vertical lines, ground lines, and ground angles in the camera image and entering the correct size and angle. Use the **Sketch** functionality if the result of the automatic calibration is not sufficient.
You can also combine this manual calibration with the values for roll angle, tilt angle, height and focal length calculated by the camera or entered manually.
Select the **Calculate** check box to obtain the roll angle, tilt angle, height and focal length from the sketched calibration elements - vertical lines, ground lines and angles - you have placed in the camera.
Clear the **Calculate** check box to enter a value manually or to refresh to the values provided by the camera itself.

Calibrating cameras using the Sketch-based calibration window
To determine non-automatically set values:

1. Enter the value for tilt angle, roll angle, height and focal length if the value is known, for example, by measuring the height of the camera above the ground, or reading the focal length from the lens.
2. For each value that is still unknown, select the **Calculate** check box, then place a calibration element on the camera image. Use these calibration elements to trace individual outlines of the displayed environment in the camera image and define the position and size of these lines and angles.
   - Click to place a vertical line across the image.
     A vertical line corresponds to a line that is perpendicular to the ground plane, such as a door frame, edge of a building or a lamp post.
   - Click to place a line across the ground in the image.
     A line on ground corresponds to a line that is on the ground plane, such as a road marking.

– Click to place an angle on the ground in the image.
The angle on ground represents an angle lying on the horizontal ground plane, such as the corner of a carpet or parking bay markings.

3. Adjust the calibration elements to the situation:
   – Enter the real size of a line or angle. To do this, select the line or angle, then enter the size in the corresponding box.
   Example: You have placed a line on ground across the lower side of an automobile. You know that the automobile is 4 m long. Enter 4 m as the length of the line.
   – Adjust the position or length of a line or angle. To do this, drag the line or angle or move the end points to the desired position in the camera image.
   – Remove a line or angle. To do this, select the line or angle, then click the trash can icon.

Note:
Blue lines indicate calibration elements added by you.
White lines represent the element as it should be positioned on the camera image based on the current calibration results or the determined calibration data.

Notice!
If the distance to the camera (geolocation) is not relevant, it is enough to determine height and focal length in relation to each other. This allows a simple calibration by marking 2-3 persons - each with a vertical line - and setting their size. 1,80 m (71 in.) for all is sufficient. Use at least one person in the front and one person in the background of the image for best results.

Coordinate system
Select the coordinate system and enter the appropriate values in the additional input fields that appear depending on the coordinate system selected.
The **Coordinate system** feature describes the position of the camera in a local **Cartesian** or the global **WGS 84** coordinate system. The camera and the objects tracked by the video analytics are displayed on a map.

Cartesian
The Cartesian coordinate system describes each point in the space by a combination of the position on three orthogonal axes X, Y and Z. A right-handed coordinate system is used, where X and Y span the ground plane and Z describes the elevation of the ground plane.

X [m]
The location of the camera on the ground on the X-axis.

Y [m]
The location of the camera on the ground on the Y-axis.

Z [m]
The elevation of the ground plane. To determine the elevation of the camera, add the **Z [m]** value and the **Height [m]** value of the camera.

WGS 84
The WGS 84 coordinate system is a spherical coordinate system description of the world and used in many standards including GPS.

Latitude
Latitude is the north-south position of the camera in the spherical coordinate system WGS 84.

Longitude
Longitude is the east-west position of the camera in the spherical coordinate system WGS 84.

Ground level [m]
The elevation of the ground above sea level. To determine the elevation of the camera, add the **Ground level [m]** value and the **Height [m]** value of the camera.

Azimuth [°]
The orientation of the camera in a counter-clockwise angle starting with 0° in the east (WGS 84) or on the X-axis (**Cartesian**). If the camera is directed towards the north (WGS 84) or the Y-axis (Cartesian), the azimuth is 90°.
Click **Set** to apply the changes.

4.4.2 Color

Brightness (0...255)
Adjust the brightness with the slider from 0 to 255.

Contrast (0...255)
Adjust the contrast with the slider from 0 to 255.

Saturation (0...255)
Adjust the color saturation with the slider from 0 to 255.

White balance
- **Basic auto** mode allows the camera to continually adjust for optimal color reproduction using an average reflectance method. This is useful for indoor light sources and for colored LED light illumination.
- **Standard auto** mode allows the camera to continually adjust for optimal color reproduction in an environment with natural light sources.
- **Sodium lamp auto** mode allows the camera to continually adjust for optimal color reproduction in an environment with sodium vapor light sources (street lighting).
- **Dominant color auto** mode takes into account any dominant color in the image (for example, the green of a football pitch or of a gaming table) and uses this information to obtain a well balanced color reproduction.
- In **Manual RGB** mode, the Red, Green, and Blue gain can be set manually to a desired position.

Apply white balance
Click **Hold** to put ATW on hold and save the current color settings. The mode changes to manual.

RGB-weighted white balance
In an auto mode, **RGB-weighted white balance** can be switched On or Off. When On, additional fine tuning of the automatic color reproduction can be made with the R, G and B weight sliders.

R-gain
In **Manual RGB** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

G-gain
In **Manual RGB** white balance mode, adjust the green gain slider to offset the factory white point alignment (reducing green introduces more magenta).

B-gain
In **Manual RGB** white balance mode, adjust the blue gain slider to offset the factory white point alignment (reducing blue introduces more yellow).

Note:
It is only necessary to change the white point offset for special scene conditions.

Default
Click **Default** to set all video values to their factory setting.

4.4.3 ALC

ALC mode
Select the mode for automatic light-level control:
– Fluorescent 50 Hz
– Fluorescent 60 Hz
– Standard

ALC level
Adjust the video output level (-15 to 0 to +15).
Select the range within which the ALC will operate. A positive value is more useful for low-light conditions; a negative value is more useful for very bright conditions.

Exposure

Automatic exposure
Select to let the camera automatically set the optimum shutter speed. The camera tries to maintain the selected shutter speed as long as the light level of the scene permits.
– Select the **Maximum shutter [s]** for automatic exposure. (The values available depend on the value set for the **Sensor mode** in the **Installer Menu**).

Fixed exposure
Select the **Fixed shutter [s]** for fixed exposure. (The values available depend on the value set for the ALC mode).

Day/Night
Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.
Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.
Color - the camera always produces a color signal regardless of light levels.

Night-to-day switchover
Adjust the slider to set the video level at which the camera in **Auto** mode switches from monochrome to color operation (-15 to +15).
A low (negative) value means that the camera switches to color at a lower light level. A high (positive) value means that the camera switches to color at a higher light level.
(The actual switch-over point might change automatically to avoid instable switching.)

Note:
To ensure stability when using IR illuminators, use the alarm interface for reliable Day/Night switching.

IR function
(Only applicable to FLEXIDOME IP turret 3000i IR - outdoor)
Select the control setting for IR illumination:
– **Auto**: the camera automatically switches the IR illumination.
– **On**: the IR illumination is always on.
– **Off**: the IR illumination is always off.

Intensity level
(Only applicable to FLEXIDOME IP turret 3000i IR - outdoor)
Set the intensity of the IR beam (0 to 30).

4.4.4 Enhance

High dynamic range

Choose between these options:

Off: to disable High Dynamic Range (HDR)

Auto: for automatic HDR. Depending on the scene, the camera can capture multiple exposures to increase the Dynamic Range

Extreme: similar to Auto, but with even higher Dynamic Range. Use this only in quiet scenes and with low light levels. Artifacts can occur depending on the light level and movement in the scene.

Notice!

Do not use HDR in scenes with fluorescent lighting.

HDR can only be active if Auto exposure is selected, and there is a match between the base frame rate (selected in the installer menu) and the ALC fluorescent mode frequency. If there is a conflict, a pop-up window will suggest a solution and adjust the appropriate settings.

Backlight compensation

Select **Off** to switch off backlight compensation.

Select **On** to capture details in high-contrast and extremely bright-dark conditions.

Contrast enhancement

Select **On** to increase the contrast in low contrast conditions.

Intelligent Defog

Select this to activate the automatic intelligent defog feature. This feature continuously adjusts image parameters to provide the best picture possible under foggy or misty conditions.

Intelligent Dynamic Noise Reduction

Select **On** to activate intelligent Dynamic Noise Reduction (DNR) which reduces noise based on motion and light levels.

Sharpness level

Adjusts the **Sharpness level** between -15 and +15. A low (negative) value makes the picture less sharp. Increasing sharpness brings out more detail. Extra sharpness can enhance the details of license plates, facial features and the edges of certain surfaces but can increase bandwidth requirements.

Temporal noise filtering

Adjusts the **Temporal noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

Spatial noise filtering

Adjusts the **Spatial noise filtering** level between -15 and +15. The higher the value, the more noise filtering.

Intelligent streaming

The sharpness level, **Temporal noise filtering** and **Spatial noise filtering** can be automatically adjusted here, through the encoder, for optimum intelligent streaming results.

Dynamic sharpness & noise filtering

Enable or disable the automatic adjustment of the encoder.

Priority encoder stream

Select stream 1, 2 or **Auto** as the priority stream for the encoder. **Auto** automatically selects the optimal stream.

4.4.5 Encoder Profile

Profiles are rather complex and include a number of parameters that interact with one another, so it is generally best to use the pre-defined profiles. Only change a profile if completely familiar with all the configuration options.

Changing a profile

To change a profile, select it by clicking its tab and then change the parameters within that profile.

If a setting outside the permitted range for a parameter is entered, the nearest valid value is substituted when the settings are saved.

Profile name

If required, enter a new name for the profile.

Bit rate optimization

Select the necessary bit rate optimization setting.

Maximum bit rate

The encoder maintains the maximum bit rate over a number of GOPs (group-of-pictures), limiting image quality when necessary. To ensure long-term stability of the maximum bit rate, use the **Averaging period**.

The value entered in this field must be at least 10% higher than the value entered in the field **Target bit rate**. If the value entered here is too low, it will be adjusted automatically.

The value in this field is not to be interpreted as the network transmission bit rate.

Averaging period

Select the appropriate averaging period as a means of stabilizing the long term bit rate.

Target bit rate

To optimize use of the bandwidth in the network, limit the data rate for the device. The target data rate should be set according to the desired picture quality for typical scenes with no excessive motion.

For complex images or frequent changes of image content due to frequent movements, this limit can temporarily be exceeded up to the value entered in the **Maximum bit rate** field.

Frame rate

The **Frame rate** slider determines the interval at which images are encoded and transmitted. This can be particularly advantageous with low bandwidths. The image rate is displayed next to the slider.

Video resolution

Select the desired resolution for the video image for Standard Definition (SD) streams. This setting is not used by High Definition (HD) streams.

Expert Settings

If necessary, use the expert settings to adapt the I-frame quality and the P-frame quality to specific requirements. The setting is based on the H.264 quantization parameter (QP).

I-frame distance

Use the slider to set the distance between I-frames to **Auto** or to between **3** and **255**. An entry of 3 means that every third image is an I-frame. The lower the number, the more I-frames are generated.

Allow enhanced prediction

This function allows for multiple references in H.264 and H.265 streams, which can reduce bitrate. Some decoders do not support this feature and therefore can be disabled.

Min. P-frame QP

In the H.264-protocol, the Quantization Parameter (QP) specifies the degree of compression and thus the image quality for every frame. The lower the QP value, the higher the encoding quality. A higher quality produces a higher data load. Typical QP values are between 18 and 30. Define the lower limit for the quantization of the P-frames here, and thus the maximum achievable quality of the P-frames.

I/P-frame delta QP

This parameter sets the ratio of the I-frame QP to the P-frame QP. For example, you can set a lower value for I-frames by moving the slide control to a negative value. Thus, the quality of the I-frames relative to the P-frames is improved. The total data load will increase, but only by the portion of I-frames.

To obtain the highest quality at the lowest bandwidth, even in the case of increased movement in the picture, configure the quality settings as follows:

1. Observe the coverage area during normal movement in the preview images.
2. Set the value for **Min. P-frame QP** to the highest value at which the image quality still meets your needs.
3. Set the value for **I/P-frame delta QP** to the lowest possible value. This is how to save bandwidth and memory in normal scenes. The image quality is retained even in the case of increased movement since the bandwidth is then filled up to the value that is entered under **Maximum bit rate**.

Background delta QP

Select the appropriate encoding quality level for a background region defined in Encoder Regions. The lower the QP value, the higher the encoding quality.

Object delta QP

Select the appropriate encoding quality level for an object region defined in Encoder Regions. The lower the QP value, the higher the encoding quality.

Default

Click **Default** to return the profile to the factory default values.

Click **Set** to apply the changes.

4.4.6 Encoder Streams

When this menu is accessed while the device is recording, the following message appears at the top of the page: “Recording is currently active. At ‘Active profile’ the stream profile used for recording is displayed, and overrules the ‘Non-recording profile’.”

Property

Select one of the resolutions from the drop-down menu for each stream.

Non-recording profile

Select one of the following profiles for each stream:

Profile number	Description
Profile 1	For a high resolution image, the video bit rate and frame quality are adjusted to ensure that the picture quality is the priority.
Profile 2	For a high resolution image, the video bit rate and frame quality are adjusted to a median profile for everyday use.
Profile 3	For a high resolution image, the video bit rate and frame quality are adjusted to ensure that the bit rate is the priority.

Profile 4	For a low resolution image, the video bit rate and frame quality are adjusted to ensure that the picture quality is the priority.
Profile 5	For a low resolution image, the video bit rate and frame quality are adjusted to a median profile for everyday use.
Profile 6	For a low resolution image, the video bit rate and frame quality are adjusted to ensure that the bit rate is the priority.
Profile 7	Ideal for encoding on a DSL uplink where bit rate limitations are critical.
Profile 8	Ideal for encoding on a 3G uplink where bit rate limitations are critical.

JPEG stream

Set the parameters for the M-JPEG stream.

- Select the **Resolution**.
  - **Note:** The **Resource based** option sets the maximum frame rate at the maximum resolution based on the available system-resources.
- Select the **Max. frame rate** in frames per second (fps).
- The **Picture quality** slider allows adjustment of the M-JPEG image quality from **Low** to **High**.

Note:

The M-JPEG frame rate can vary depending on system loading.

Click **Set** to apply the changes.

4.4.7 Encoder Statistics

Stream

Identifies the current stream (1, 2, or JPEG).

Zoom

Identifies the current zoom factor of the camera (1x, 2x, 4x, or 8x).

Averaging period

Identifies how often (in seconds, minutes, hours, days or weeks) the encoder time is synchronized to the actual time.

4.4.8 Encoder Regions

Encoder regions are used to increase or decrease the encoding quality for selectable areas of the image. They can be used to give better control of the bitrate by enhancing the encoding quality of important regions (objects) and decreasing the encoding quality of less important regions (background).

Eight encoder regions can be defined:

1. Select one of the eight available regions from the drop-down box.
2. Click the + box to add an area.
3. Use the mouse to define the area covered by the region.
   - Drag the center, corner points, or sides of the shaded area.
   - Double-click on a side to add additional points to the area.
4. Select the encoder quality to be used for the defined area. (Object and background quality levels are defined in the **Expert Settings** section of the **Encoder Profile** page.)
5. If required, select another region and repeat the steps.
6. To remove a region, select the area and click the waste bin icon.
7. Click **Set** to apply the region settings.

4.4.9 Privacy Masks

Privacy masking is used to block a specific area of a scene from being viewed. Eight privacy mask areas can be defined.

1. Select the pattern color for the masks.
2. Select the mask you wish to define in the drop-down box.
3. Check the **Enabled** box to activate the mask, or click the + button to add the mask.
4. Use the mouse to move the mask; drag the corner points to resize.
5. Click **Set**.
6. To remove a mask, select it and click the waste bin icon.

Note:
To add an additional adjustment point to the area, double-click on a side.
Click **Set** to apply the changes.

4.4.10 Audio

You can set the gain of the audio signals to suit your specific requirements. The live video image is shown in the window to help you check the audio source. Your changes are effective immediately.
If you connect via Web browser, you must activate the audio transmission on the **'Live' functions** page. For other connections, the transmission depends on the audio settings of the respective system.
The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data is encoded according to the selected format and requires additional bandwidth. If you do not want any audio data to be transmitted, select **Off**.

Audio
Enable or disable the audio recording option.

Input volume
Adjust the audio level with the slider(s). Adjust so that the indicator does not go into the red zone.

Line Out
Adjust the audio level with the slider(s). Adjust so that the indicator does not go into the red zone.

Recording format
Select a format for audio recording. The default value is **AAC 48 kbps**. You can select **AAC 80 kbps**, G.711 or L16 depending on the required audio quality or sampling rate.
AAC audio technology is licensed by Fraunhofer IIS.
(http://www.iis.fraunhofer.de/amm/)

Send audio
Audio can be sent via the **Send audio** button if the unit supports audio. The button activates the audio backchannel connection.

1. Click and hold the **Send audio** button to send an audio signal to the unit.
2. Release the button to stop sending audio.

You must have a speaker or similar connected to the line out of the camera in order to send the audio.
Click **Set** to apply the changes.

4.4.11 Pixel Counter

The number of horizontal and vertical pixels covered by the highlighted area is displayed below the picture. With these values you can check whether the requirements for specific functions, for example, identification tasks, are fulfilled.

1. Click **Freeze** to freeze the camera image if the object that you want to measure is moving.
2. To reposition a zone, place the cursor over the zone, hold down the mouse button and drag into position.
3. To change the shape of a zone, place the cursor over the edge of the zone, hold down the mouse button and drag the edge of the zone to the required position.

4.5 Recording

Images can be recorded to an appropriately configured iSCSI system or, for devices with an SD slot, locally to an SD card.

SD cards are the ideal solution for shorter storage times and temporary recordings. They can be used for local alarm recording or to improve the overall reliability of video recording.
For long-term authoritative images use an appropriately sized iSCSI system.

Two recording tracks are available (**Recording 1** and **Recording 2**). The encoder streams and profiles can be selected for each of these tracks for both standard and alarm recordings.
Ten recording profiles are available where these recording tracks can be defined differently.
These profiles are then used for building schedules.

A Video Recording Manager (VRM) can control all recording when accessing an iSCSI system.
The VRM is an external program for configuring recording tasks for video servers.

4.5.1 Storage Management

Device manager

The Device manager indicates if storage is controlled locally or by a VRM system.
An external Video Recording Manager (VRM) system for the unit is configured via the Configuration Manager.

Recording media

Select a media tab to connect to the available storage media.

iSCSI Media

To use an **iSCSI system** as the storage medium, a connection to the desired iSCSI system is required to set the configuration parameters.
The storage system selected must be available on the network and completely set up. It must have an IP address and be divided into logical drives (LUNs).

1. Enter the IP address of the required iSCSI destination in the **iSCSI IP address** field.
2. If the iSCSI destination is password protected, enter the password into the **Password** field.
3. Click **Read**.
   – The connection to the IP address is established.

The **Storage overview** field displays the logical drives.

Local Media

An SD card inserted in the camera can be used for local recording.

- If the SD card is password protected, enter the password into the **Password** field.

The **Storage overview** field displays the local media.
Note: SD card recording performance is highly dependent on the speed (class) and performance of the SD card. It is recommended to use an industrial SD card with health monitoring.

Local storage

To activate the ANR settings, **Recording 1** must be assigned to an iSCSI target and **Recording 2** to a local storage.
This function enables recording to the iSCSI target. If there is a network disconnection, the video is recorded to the local storage. When the network is recovered, the video recorded to the local storage is transferred to the iSCSI target and completes the missing information.

Activating and configuring storage media
Available media or iSCSI drives must be transferred to the **Managed storage media** list, activated, and configured for storage.

Note:
An iSCSI target storage device can only be associated with one user. If a target is being used by another user, ensure that the current user no longer needs the target before decoupling that user.

1. In the **Storage overview** section, double-click a storage medium, an iSCSI LUN or one of the other available drives.
   – The medium is added as a target in the **Managed storage media** list.
   – Newly added media is shown as **Not active** in the **Status** column.
2. Click **Set** to activate all media in the **Managed storage media** list.
   – The **Status** column shows all media as **Online**.
3. Check the box in the **Rec. 1** or **Rec. 2** column to specify the recording tracks to be recorded on the target selected.

Formatting storage media
All recordings on a storage medium can be deleted at any time. Check the recordings before deleting and back-up important sequences on the computer's hard drive.
1. Click a storage medium in the **Managed storage media** list to select it.
2. Click **Edit** below the list.
3. Click **Format** in the new window to delete all recordings in the storage medium.
4. Click **OK** to close the window.

Deactivating storage media
A storage medium in the **Managed storage media** list can be deactivated. It is then no longer used for recordings.
1. Click a storage medium in the **Managed storage media** list to select it.
2. Click **Remove** below the list. The storage medium is deactivated and removed from the list.

Click **Set** to apply the changes.

4.5.2 Recording Profiles

A recording profile contains the characteristics of the tracks that are used for recording. These characteristics can be defined for ten different profiles. The profiles can then be assigned to days or times of day on the **Recording Scheduler** page.

Each profile is color-coded. The names of the profiles can be changed on the **Recording Scheduler** page.
To configure a profile click its tab to open its settings page.
– To copy the currently visible settings to other profiles, click **Copy Settings**. A window opens to select the target profiles for the copied settings.
– If you change a profile’s settings, click **Set** to save.
– If necessary, click **Default** to return all settings to their factory defaults.

Stream profile settings

Select the encoder profile setting that is to be used with stream 1 and 2 when recording. This selection is independent of the selection for live stream transmission. (The properties of the encoder profiles are defined on the **Encoder Profile** page.)

Select the ROI pre-position scene that is to be used for recording. (The ROI pre-positions for stream 2 are configured on the **Live** page.)

Settings for selected recordings

Recording includes

Select what is to be included in the recordings:

- **Audio**: If audio is not enabled, **Off** is shown. Click on **Off** and the page is redirected to the **Audio** section.
- **Metadata**.

Standard recording

Select the mode for standard recordings:

- **Continuous**: the recording proceeds continuously. If the maximum recording capacity is reached, older recordings are overwritten automatically.
- **Pre-alarm**: recording takes place in the pre-alarm time, during the alarm and during the post-alarm time only.
- **Off**: no automatic recording takes place.

Stream

Select the stream to be used for standard recordings:

- **Stream 1**
- **Stream 2**
- **I-frames only**

Alarm recording

Select a period for the **Pre-alarm time** from the list box.

Select a period for the **Post-alarm time** from the list box.

Alarm stream

Select the stream to be used for alarm recordings:

- **Stream 1**
- **Stream 2**
- **I-frames only**

Check the **encoding interval and bit rates from profile:** box and select an encoder profile to set the associated encoding interval for alarm recording.

Alarm triggers

Select the alarm type that is to trigger a recording:

- **Alarm input**
- **Analysis alarm**
- **Virtual alarm**: select one of the sensors that are to trigger a recording, via RCP+ commands or alarm scripts, for example.

Export to account

Select an account from the drop-down box to export to an account. If an account has not yet been defined, click **Configure accounts** to jump to the **Accounts** page where the server information can be entered.

Click **Set** to apply the changes.

4.5.3 Maximum Retention Time

Recordings are overwritten when the retention time entered here has expired.
Enter the required retention time in days for each recording track.
Click **Set** to apply the changes.

4.5.4 Recording Scheduler

The recording scheduler allows you to link the created recording profiles to the days and times at which the camera's images are to be recorded. Schedules can be defined for weekdays and for holidays.

Weekdays

Assign as many time periods (in 15-minute intervals) as needed for any day of the week. Move the mouse cursor over the table - the time is displayed.

1. Click the profile to be assigned in the **Time periods** box.
2. Click a field in the table and, while holding down the left mouse button, drag the cursor across all of the fields to be assigned to the selected profile.
3. Click the **No recordings** profile in the **Time periods** box to deselect the intervals.
4. Click **Select All** to select all of the intervals to be assigned to the selected profile.
5. Click **Clear All** to deselect all of the intervals.
6. When finished, click **Set** to save the settings to the device.

Holidays

Define holidays whose settings will override the settings for the normal weekly schedule.

1. Click the **Holidays** tab. Days that have already been defined are shown in the table.
2. Click **Add**. A new window opens.
3. Select the desired **From** date from the calendar.
4. Click in the **To** box and select a date from the calendar.
5. Click **OK** to accept the selection which is handled as a single entry in the table. The window closes.
6. Assign the defined holidays to the recording profile as described above.
7. To delete a user-defined holiday, click on the trashcan of the respective holiday.

Click **Set** to apply the changes.

Time periods

Change the names of the recording profiles listed in the **Time periods** box.

1. Click a profile.
2. Click **Rename**.
3. Enter the new name and click **Rename** again.

Recording status

The graphic indicates the recording activity. An animated graphic is displayed when recording is taking place.

Activating recording

After completing configuration, activate the recording schedule and start scheduled recording. Once activated, the **Recording Profiles** and the **Recording Scheduler** are deactivated and the configuration cannot be modified. Stop scheduled recording to modify the configuration.

1. Click **Start** to activate the recording schedule.
2. Click **Stop** to deactivate the recording schedule. Recordings that are currently running are interrupted and the configuration can be modified.

Click **Set** to apply the changes.

4.5.5 Recording Status

Details of the recording status are displayed here for information. These settings cannot be changed.

4.5.6 Recording Statistics

The bit rate of the recorded video (blue) and other data (grey), such as audio and metadata, are shown in the graphic.

Recording

Identifies the current recording profile (1 or 2).

Zoom

Identifies the current zoom factor of the camera (1x, 2x, 4x, or 8x).

Averaging period

Select the appropriate averaging period as a means of stabilizing the long term bit rate.

4.5.7 Image Posting

Save individual JPEG images on an FTP server at specific intervals.

JPEG

Image size

Select the size of the JPEG images that are to be sent from the camera. JPEG resolution corresponds to the highest setting from the two data streams.

File name

Select how file names are created for the individual images that are transmitted.

- **Overwrite**: The same file name is always used and any existing file will be overwritten by the current file.
- **Increment**: A number from 000 to 255 is added to the file name and automatically incremented by 1. When it reaches 255, it starts again from 000.
- **Date/time suffix**: The date and time are automatically added to the file name. When setting this parameter, make sure that the date and time of the device are always set correctly. For example, the file snap011005_114530.jpg was stored on October 1, 2005 at 11:45 and 30 seconds.

VCA overlays

If you have enabled the display of VCA overlays on the **Appearance** page, select the **VCA overlays** check box to have the overlays also visible in the JPEG image.

Posting interval

Enter the interval in seconds at which the images are sent to an FTP server. Enter zero for no images to be sent.

Target

Select the target account for JPEG posting.

Notice!

You must configure an account in order to have functionality for **Image Posting**. Click on **Configure accounts** to do so.

Click **Set** to apply the changes.

4.5.8 SD Card Status

This section identifies the details about the SD card installed in the device:

- **Manufacturer**

– **Product**
– **Size**
– **State**
– **Lifespan**.

Lifespan check

When checked, the **Lifespan** status is shown in the details of the SD cards.

Lifespan alarm

Set the alarm warning to a defined percentage of the lifespan.

If a SD card is not installed, '**SD card not found**' is shown.

It is recommended to use an industrial SD card with health monitoring and enhanced performance. For non-industrial SD cards, the lifespan options are not available.

4.6 Alarm

4.6.1 Alarm Connections

In the event of an alarm, the unit can automatically connect to a pre-defined IP address. The unit can contact up to ten IP addresses in the order listed until a connection is made.

Connect on alarm

Select **On** so that the unit automatically connects to a pre-defined IP address in the event of an alarm.

Select **Follows input 1** so that the unit maintains the connection for as long as an alarm exists on alarm input 1.

Auto-connect

Select **On** to automatically re-establish a connection to one of the previously specified IP addresses after each reboot, connection breakdown, or network failure.

Number of destination IP address

Specify the numbers of the IP addresses to be contacted in the event of an alarm. The unit contacts the remote locations one after the other in the numbered sequence until a connection is made.

Destination IP address

For each number, enter the corresponding IP address for the desired remote station.

Destination password

If the remote station is password protected, enter the password here.

Only ten passwords can be defined here. Define a general password if more than ten connections are required. The unit connects to all remote stations protected by the same general password. To define a general password:

1. Select 10 in the **Number of destination IP address** list box.
2. Enter 0.0.0.0 in the **Destination IP address** field.
3. Enter the password in the **Destination password** field.
4. Set the user password of all the remote stations to be accessed using this password.

Setting destination 10 to the IP-address 0.0.0.0 overrides its function as the tenth address to try.

Video transmission

If the unit is operated behind a firewall, select **TCP (HTTP port)** as the transfer protocol. For use in a local network, select **UDP**.

To enable multicast operation, select **UDP** for the **Video transmission** parameter here and on the **Network Access** page.

Note:
In the event of an alarm, a larger network bandwidth is sometimes required for additional video streams (if multicast operation is not possible).

Stream
Select a stream to be transmitted.

Remote port
Select an appropriate browser port depending on the network configuration.
The ports for HTTPS connections are only available if **SSL encryption** is set to **On**.

Video output
If a hardware receiver is used, select the analog video output to which the signal should be switched. If the destination device is unknown, select **First available**. This places the image on the first video output with no signal.
The connected monitor only displays images when an alarm is triggered.

Note:
Refer to the destination unit documentation for more information on image display options and available video outputs.

Decoder
If a split image is set for the selected video output, select a decoder to display the alarm image. The decoder selected determines the position in the split image.

SSL encryption
SSL encryption protects data used for establishing a connection, such as the password. By selecting **On**, only encrypted ports are available for the **Remote port** parameter. SSL encryption must be activated and configured on both sides of a connection.
The appropriate certificates must also have been uploaded. (Certificates can be uploaded on the **Certificates** page.)
Configure and activate encryption for media data (such as video, metadata or audio when available) on the **Encryption** page (encryption is only available if the appropriate license is installed).

Audio
Select **On** to transmit the audio stream with an alarm connection.
Click **Set** to apply the changes.

4.6.2 Video Content Analysis (VCA)

The camera has integrated Video Content Analysis (VCA) which detects and analyzes changes in the picture using image processing algorithms. Such changes can be due to movements in the camera's field of view. Detection of movement can be used to trigger an alarm and to transmit metadata.

Various VCA configurations can be selected and adapted to your application, as required.

Refer to Setting up VCA for more information on setting up video content analysis.

Note:
If there is not enough computing power, priority is given to live images and recordings. This can lead to impairment of the VCA system. Observe the processor load and optimize the encoder settings or the VCA settings if necessary, or turn off VCA completely.

Setting up VCA

Notice!
You should configure VCA using the Bosch Configuration Manager application. If you do not have the application, download it by clicking **Links** in the application bar.
You can also configure VCA in a browser with MPEG-ActiveX installed and by disabling **Secure cookies** in **Web Interface** -> **Appearance**.

Several VCA configurations are available.
- **Off**
- **Silent VCA**
- **Profile #1**
- **Profile #2**
- **Scheduled**
- **Event triggered**

Silent VCA
In this configuration, metadata is created to facilitate searches of recordings, however, no alarm is triggered.
- In the **VCA configuration** drop-down list, select **Silent VCA**.

No parameters can be changed for this selection.

Profile # 1/ Profile # 2
Two profiles can be set up with different VCA configurations
1. In the **VCA configuration** drop-down list, select profile 1 or 2 and enter the required settings.
2. If necessary, click **Default** to return all settings to default values.

To rename a profile:
1. To rename the file, click the icon to the right of the list field and enter the new profile name in the field.
2. Click the icon again. The new profile name is saved.

The current alarm status is displayed for information purposes.

Scenario
Scenarios are applications with pre-defined settings that are adapted to specific use cases. All relevant settings, from tasks to metadata, are set automatically by the system.
The following scenarios are available:
- Intrusion (one field)
- Intrusion (two fields)
- People counting
- Traffic incidents
- Traffic wrong way

Notice!
A camera calibration is required for all scenarios.
Using the scenarios will reset the VCA configuration to the scenario defaults.
All values (**Metadata Generation** and **Tasks**) can be edited after activating the scenario defaults.
Delete tasks that do not fit your use cases.

Analysis type
Select the required analysis algorithm. Motion+ offers a motion detector and essential recognition of tampering.
Metadata is always created for a video content analysis, unless this is explicitly excluded. Depending on the analysis type selected and the relevant configuration, additional information overlays the video image in the preview window next to the parameter settings. With the Motion+ analysis type, for example, the sensor fields in which motion is recorded are marked with rectangles.

Alarm status
The alarm status is displayed here for information purposes. This means you can check the effects of your settings immediately.
Click **Configuration** to set up the analysis type.

Tamper detection
Detect tampering of cameras and video cables by means of various options. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

Reference check
Save a reference image that can be continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This detects tampering that would otherwise not be detected, for example, if the camera is turned.

1. Click **Reference** to save the currently visible video image as a reference.
2. Click **Add mask** and select the areas in the reference image that are to be ignored. Click **Set** to apply.
3. Check the box **Reference check** to activate the on-going check. The stored reference image is displayed in black and white below the current video image.
4. Select the **Disappearing edges** or **Appearing edges** option to specify the reference check once again.

Sensitivity
The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject. The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected.

Trigger delay [s]
Set delayed alarm triggering here. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This avoids false alarms triggered by short-term changes, for example, cleaning activities in the direct field of vision of the camera.

Disappearing edges
The area selected in the reference image should contain a prominent structure. If this structure is concealed or moved, the reference check triggers an alarm. If the selected area is too homogenous, so that concealing and moving the structure would not trigger an alarm, then an alarm is triggered immediately to indicate the inadequate reference image.

Appearing edges
Select this option if the selected area of the reference image includes a largely homogenous surface. If structures appear in this area, then an alarm is triggered.

Global change

Activate this function if the global change, as set with the Global change slide control, should trigger an alarm.

Global change (slider)

Set how large the global change in the video image must be for an alarm to be triggered. This setting is independent of the sensor fields selected under **Mask...**. Set a high value if fewer sensor fields need to change to trigger an alarm. With a low value, it is necessary for changes to occur simultaneously in a large number of sensor fields to trigger an alarm. This option allows detection, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mount bracket, for example.

Current brightness

For information, the current brightness of the camera scene is displayed. The brighter the scene, the higher the value. Use this value as an indicator when defining a corresponding threshold.

Scene too bright

Activate this function if tampering associated with exposure to extreme light (for instance, shining a flashlight directly on the lens) should trigger an alarm.
Use the slider to set the threshold of the alarm trigger.

Scene too dark

Activate this function if tampering associated with covering the lens (for instance, by spraying paint on it) should trigger an alarm.
Use the slider to set the threshold of the alarm trigger.

Scheduled

A scheduled configuration allows you to link a VCA profile with the days and times at which the video content analysis is to be active.

- In the **VCA configuration** drop-down list, select **Scheduled**.

Schedules can be defined for weekdays and for holidays.
Assign as many time periods (in 15-minute intervals) as needed for any day of the week. Move the mouse cursor over the table - the time is displayed.

1. Click the profile to be assigned in the **Time periods** box.
2. Click a field in the table and, while holding down the left mouse button, drag the cursor across all of the fields to be assigned to the selected profile.
3. Click **None** in the **Time periods** box to deselect the intervals.
4. Click **Select All** to select all of the intervals to be assigned to the selected profile.
5. Click **Clear All** to deselect all of the intervals.
6. When finished, click **Set** to save the settings to the device.

Define holidays whose settings will override the settings for the normal weekly schedule.

1. Click the **Holidays** tab. Days that have already been defined are shown in the table.
2. Click **Add**. A new window opens.
3. Select the desired **From** date from the calendar.
4. Click in the **To** box and select a date from the calendar.
5. Click **OK** to accept the selection which is handled as a single entry in the table. The window closes.
6. Assign the defined holidays to the VCA profiles as described above.
7. To delete a user-defined holiday, click on the trashcan of the respective holiday.

Event triggered

This configuration allows you to stipulate that the video content analysis is only to be activated when triggered by an event.

- In the **VCA configuration** drop-down list, select **Event triggered**.

As long as no trigger is activated, the **Silent VCA** configuration in which metadata is created is active; this metadata facilitates searches of recordings, but does not trigger an alarm.

Trigger
Select a physical alarm or a virtual alarm as a trigger. A virtual alarm is created using software, with RCP+ commands or alarm scripts, for example.

Trigger active
Select the VCA configuration here that is to be enabled via an active trigger. A green check mark to the right of the list field indicates that the trigger is active.

Trigger inactive
Select the VCA configuration here that is to be activated if the trigger is not active. A green check mark to the right of the list field indicates that the trigger is inactive.

Delay [s]
Select the delay period for the reaction of the video content analysis to trigger signals. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. A delay period may be useful in avoiding false alarms or frequent triggering. During the delay period, the **Silent VCA** configuration is always enabled.

4.6.3 Audio Alarm

Alarms can be generated based on audio signals. Configure signal strengths and frequency ranges so that false alarms, for example, machine noise or background noise, are avoided. Set up normal audio transmission before configuring the audio alarm.

Audio alarm
Select **On** for the device to generate audio alarms.

Name
The name makes it easier to identify the alarm in extensive video monitoring systems. Enter a unique and clear name here.

Signal Ranges
Exclude particular signal ranges in order to avoid false alarms. For this reason the total signal is divided into 13 tonal ranges (mel scale). Check or uncheck the boxes below the graphic to include or exclude individual ranges.

Threshold
Set up the threshold on the basis of the signal visible in the graphic Set the threshold using the slide control or, alternatively, move the white line directly in the graphic using the mouse.

Sensitivity
Use this setting to adapt the sensitivity to the sound environment and effectively suppress individual signal peaks. A high value represents a high level of sensitivity.
Click **Set** to apply the changes.

4.6.4 Alarm E-Mail

Alarm states can be documented by e-mail. The camera automatically sends an e-mail to a user-defined e-mail address. This makes it possible to notify a recipient who does not have a video receiver.

Send alarm e-mail
Select **On** for the device to automatically send an alarm e-mail in the event of an alarm.

Mail server IP address
Enter the IP address of a mail server that operates on the SMTP standard (Simple Mail Transfer Protocol). Outgoing e-mails are sent to the mail server via the address entered. Otherwise, leave the box blank (**0.0.0.0**).

SMTP port
Select the appropriate SMTP port.

SMTP user name
Enter a registered user name for the chosen mail server.

SMTP password
Enter the required password for the registered user name.

Format
Select the data format of the alarm message.
– **Standard (with JPEG)**: e-mail with JPEG image file attachment.
– **SMS**: e-mail in SMS format to an e-mail-to-SMS gateway without an image attachment.
When a mobile phone is used as the receiver, make sure to activate the e-mail or SMS function, depending on the format, so that these messages can be received. Obtain information on operating your mobile phone from your mobile phone provider.

Image size
Select the size of the JPEG images that are to be sent from the camera.

Attach JPEG from camera
To send a JPEG image from a particular video channel, check the appropriate box.

VCA overlays
Select the **VCA overlays** check box, to place the outline of the object that triggered an alarm into the camera image sent as snapshot via e-mail.

Destination address
Enter the e-mail address for alarm e-mails here. The maximum address length is 49 characters.

Sender address
Enter a unique name for the e-mail sender, for example, the location of the device. This makes it easier to identify the origin of the e-mail.

Test e-mail
Click **Send Now** to test the e-mail function. An alarm e-mail is immediately created and sent.
Click **Set** to apply the changes.

4.6.5 Alarm Inputs

Active
Configure the alarm triggers for the unit.
Select **N.C.** (Normally Closed) if the alarm is to be triggered by opening the contact.
Select **N.O.** (Normally Open) if the alarm is to be triggered by closing the contact.
Select **N.C.S.** (Normally Closed Supervised) if the alarm is to be triggered by opening the contact.
Select **N.O.S.** (Normally Open Supervised) if the alarm is to be triggered by closing the contact.
A supervised alarm transmits both the alarm condition and the tamper condition. Depending on how the alarm is configured, a short or a break in the alarm's circuit can trigger the tamper signal.

Name
Enter a name for the alarm input. This is then displayed below the icon for the alarm input on the **Live** page (if configured).

Action
Select a type of action to be performed when an alarm input occurs:
– **None**
– **Monochrome**
This switches the camera to the monochrome mode.
Click **Set** to apply the changes.

4.6.6 Alarm Outputs

Configure the switching behavior of the output.
Select different events that automatically activate an output. For example, turn on a floodlight by triggering a motion alarm and then turn the light off again when the alarm has stopped.

Idle state
Select **Open** for the output to operate as a normally open contact, or select **Closed** if the output is to operate as a normally closed contact.

Operating mode
Select the way the output works.
For example, if you want an activated alarm to stay on after the alarm ends, select **Bistable**. If you wish an activated alarm to stay on for ten seconds for example, select **10 s**.

Output follows
Select the event that triggers the output.

Output name
The alarm output can be assigned a name here. This name appears on the Live page.

Toggle
Click the button to switch the alarm output manually (for example, for testing purposes or to operate a door opener).
Click **Set** to apply the changes.

4.6.7 Alarm Task Editor

Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.
To edit this page, you should have programming knowledge and be familiar with the information in the Alarm Task Script Language document and the English language.

As an alternative to the alarm settings on the various alarm pages, enter the desired alarm functions in script form here. This will overwrite all settings and entries on the other alarm pages.

1. Click **Examples** under the Alarm Task Editor field to see some script examples. A new window opens.
2. Enter new scripts in the Alarm Task Editor field or change existing scripts in line with your requirements.
3. When finished, click **Set** to transmit the scripts to the device. If the transfer was successful, the message **Script successfully parsed.** is displayed over the text field. If it was not successful, an error message is displayed with further information.

4.7 Network

The settings on these pages are used to integrate the device into a network. Some changes only take effect after a reboot. In this case **Set** changes to **Set and Reboot**.

1. Make the desired changes.
2. Click **Set and Reboot**.

The device is rebooted and the changed settings are activated.

4.7.1 Network Services

This page shows an overview of all available network services. Use the checkbox to activate or deactivate a network service. Click on the settings symbol next to the network service to go to the settings page for this network service.

Click **Set** to apply the changes.

4.7.2 Network Access

If the IP address, subnet mask, or gateway address is changed, then the device is only available under the new addresses after the reboot.

Automatic IPv4 assignment

If the network has a DHCP server for the dynamic assignment of IP addresses, select **On** or **On plus Link-Local** to automatically accept the DHCP-assigned IP address.

If no DHCP server is available select **On plus Link-Local** to automatically assign a Link-Local (Auto-IP) address.

For certain applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

Ethernet

The Ethernet options are defined in this section.

IP V4 address

IP address

Enter the desired IP address for the camera. The IP address must be valid for the network.

Subnet mask

Enter the appropriate subnet mask for the set IP address.

Gateway address

For the device to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise, this field can remain empty (0.0.0.0).

IP V6 address

IP address

Enter the desired IP address for the camera. The IP address must be valid for the network.

Prefix length

Enter the appropriate prefix length for the set IP address.

Gateway address

For the device to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise, this field can remain empty (0.0.0.0).

DNS server address 1/DNS server address 2

The device is easier to access if it is listed on a DNS server. For example, to establish an Internet connection to the camera, it is sufficient to enter the name given to the device on the DNS server as a URL in the browser. Enter the DNS server's IP address. Servers are supported for secure and dynamic DNS.

Video transmission
If the device is used behind a firewall, TCP (HTTP port) should be selected as the transmission protocol. For use in a local network, choose UDP.
Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.

UDP encryption
Enable this option to encrypt the User Datagram Protocol (UDP) connection. UDP with encryption can also be used in multicast networks.

TCP rate control
Select **On** if you want to allow Adaptive Bit Rate encoding.

HTTP browser port
Select a different HTTP browser port from the list if required. The default HTTP port is 80. To limit connection to HTTPS, deactivate the HTTP port. To do this, activate the **Off** option.

HTTPS browser port
To limit browser access to encrypted connections, choose an HTTPS port from the list. The standard HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports and limit connections to unencrypted ports.
The camera uses the TLS 1.0 protocol. Ensure that the browser has been configured to support this protocol. Also ensure that Java application support is activated (in the Java Plug-in Control Panel of the Windows Control Panel).
To limit connections to SSL encryption, set the **Off** option in the HTTP browser port and the RCP+ port. This deactivates all unencrypted connections allowing connections on the HTTPS port only.
Configure and activate encryption for media data (video, audio, metadata) on the **Encryption** page.

Minimum TLS version
Select the version for minimum Transport Layer Security (TLS).

Allow HTTP basic authentication
Select **On** if you want to allow HTTP basic authentication. This is a less secure authentication option where passwords are transmitted in clear text. This option should only be used if the network and system are otherwise secured.

HSTS
Select this option to use the web security policy HTTP Strict Transport Security (HSTS) to provide secure connections.

RCP+ port 1756
Activating RCP+ port 1756 allows unencrypted connections on this port. To allow only encrypted connections, set the **Off** option to deactivate the port.

Discovery port (0 = Off)
Enter the number of the port that you want to discover.
To deactivate the port, enter 0.

Interface mode ETH
If necessary, select the Ethernet link type for interface ETH. Depending on the device connected, it may be necessary to select a special operation type.

Network MSS [Byte]
Set the maximum segment size for the IP packet's user data here. This gives the option to adjust the size of the data packets to the network environment and to optimize data transmission. In UDP mode, comply with the MTU value set below.

Network MTU [Byte]
Specify a maximum value in bytes for the package size (including IP header) to optimize data transmission.
Click **Set** to apply the changes.

4.7.3 Advanced

RTSP port
If necessary, select a different port for the exchange of the **RTSP** data from the list. The standard **RTSP port** is 554. Select **Off** to deactivate the **RTSP** function.

Authentication (802.1x)
To configure Radius server authentication, connect the unit directly to a computer using a network cable. If a Radius server controls access rights over the network, select **On** to activate authentication to communicate with the unit.
1. Enter the user name that the Radius server uses for the unit in the **Identity** field.
2. Enter the **Password** that the Radius server expects from the unit.

TCP metadata input
The device can receive data from an external TCP sender, for example an ATM or POS device, and store it as metadata. Select the port for TCP communication. Select **Off** to deactivate the function. Enter a valid **Sender IP address**.

Syslog

Server IP address
Enter the appropriate IP address of the server.

Server port (0 = Off)
Enter the number of the server port.

Protocol
Select the appropriate protocol: **UDP**, **TCP**, or **TLS**.

LLDP power configuration

Requested for camera
The value in this field identifies the number of watts requested for the camera.

Additional Power
Enter the number of additional watts that you want the camera to use.

Requested total
The value in this field is the total number of watts from the fields **Requested for camera** and **Additional Power**.

Allocated power
The value in this field is the number of watts of allocated power to the camera.
Click **Set** to apply the changes.

4.7.4 Network Management

SNMP
The camera supports two versions of Simple Network Management Protocol (SNMP) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The unit supports SNMP MIB II in the unified code.
Select either of the options that follow for the **SNMP** parameter:
– **SNMP v1 legacy**
– **SNMP v3**

If you select either of the SNMP version, but do not enter an SNMP host address, the camera does not send messages (traps) automatically, but only replies to SNMP requests.
Select **Off** to deactivate the SNMP function.

1. SNMP host address / 2. SNMP host address
If you wish to send SNMP traps automatically, enter the IP addresses of one or two required target units here.

SNMP v1 legacy
When you select **SNMP v1 legacy** in the field **SNMP**, the field **SNMP traps** appears.

SNMP traps
You can select which traps are to be sent.
1. Click **Select**. A list is opened.
2. Click the checkboxes to select the required traps. All the checked traps will be sent.
3. Click **Set** to accept the selection.

SNMP v3
When you select **SNMP v3** in the field **SNMP**, the tabs **User** and **Trap user** show.
The same fields show in both tabs.
User name
Enter the appropriate user name.
Authentication protocol
Select the appropriate authentication protocol: None, MD5, or SHA1.
Authentication password
Enter the appropriate password for authentication.
Privacy protocol
Select the appropriate privacy protocol: None, DES, or AES.
Privacy password
Enter the appropriate password.
Read-only
To make this information read-only, select this check box.

UPnP
Select **On** to activate UPnP communication. Select **Off** to deactivate it.
When the Universal Plug-and-Play (UPnP) function is activated, the unit responds to requests from the network and is automatically registered on the requesting computers as a new network device. This function should not be used in large installations due to the large number of registration notifications.

Note:
To use the UPnP function on a Windows computer, both the Universal Plug-and-Play Device Host and the SSDP Discovery Service must be activated.

Quality of service
The camera offers Quality of Service (QoS) configuration options to ensure fast network response to PTZ data and images. Quality of Service (QoS) is the set of techniques to manage network resources. QoS manages the delay, delay variation (jitter), bandwidth, and packet loss parameters to guarantee the ability of a network to deliver predictable results. QoS identifies the type of data in a data packet and divides the packets into traffic classes that can be prioritized for forwarding.
Consult with your network administrator for assistance configuring the **Audio**, **Video**, **Control**, and the **Alarm video** settings, and to select the appropriate **Post-alarm time**.

Post-alarm time has a time period from 0 s [seconds] to 3 h [hours]; 15 s [seconds] is the default option.
Click **Set** to apply the changes.

4.7.5 Multicast

The device can enable multiple receivers to receive the video signal simultaneously. The stream is either duplicated and then distributed to multiple receivers (Multi-unicast), or it is sent as a single stream to the network, where it is simultaneously distributed to multiple receivers in a defined group (**Multicast**).

Multicast operation requires a multicast-enabled network that uses **UDP** and the Internet Group Management protocol (**IGMP** V2). The network must support group IP addresses. Other group management protocols are not supported. The **TCP** protocol does not support multicast connections.

A special IP address from 225.0.0.0 to 239.255.255.255 (class D address) must be configured for multicast operation in a multicast-enabled network. The multicast address can be the same for multiple streams, however, it is necessary to use a different port in each case.

The settings must be made individually for each stream. Enter a dedicated multicast address and port for each stream.
The video channels can be individually selected for each stream.

Enable
Enable simultaneous data reception on receivers that need to activate the multicast function. To do this, check the box and enter the multicast address.

Multicast Address
Enter a valid multicast address to be operated in multicast mode (duplication of the data stream in the network).

With a 0.0.0.0 setting, the encoder for the stream operates in multi-unicast mode (copying of data stream in device). The camera supports multi-unicast connections for up to five simultaneously connected receivers.

Duplication of data places a heavy demand on the CPU and can lead to impairment of the image quality under certain circumstances.

Port
Enter the port address for the stream here.

Streaming
Click the checkbox to activate multicast streaming mode. An activated stream is marked with a check. (Streaming is typically not required for standard multicast operation.)

Metadata
You can enable multicast metadata here. The configuration follows the same pattern as for video multicast, but without the streaming option.
Define a multicast address and define a port.

Audio
You can enable multicast audio for different encoders here. The configuration follows the same pattern as for video multicast, but without the streaming option.
Define a multicast address and define a port for the different encoders.

Multicast packet TTL
A value can be entered to specify how long the multicast data packets are active on the network. If multicast is to be run via a router, the value must be greater than 1.

IGMP version
Set the multicast IGMP version to comply with the device.
Click **Set** to apply the changes.

4.7.6 IPv4 filter

To restrict the range of IP addresses within which you can actively connect to the device, fill-in an IP address and mask. Two ranges can be defined.

- Click **Set** and confirm to restrict access.

If either of these ranges are set, no IP V6 addresses are allowed to actively connect to the device.

The device itself may initiate a connection (for example, to send an alarm) outside the defined ranges if it is configured to do so.

4.8 Service

4.8.1 Maintenance

Notice!
Before starting a firmware update, make sure to select the correct upload file.
Do not interrupt the firmware installation. Even changing to another page or closing the browser window leads to interruption.
Uploading the wrong files or interrupting the upload can result in the device no longer being addressable, requiring it to be replaced.

The camera functions and parameters can be updated by uploading new firmware. To do this, the latest firmware package is transferred to the device via the network. The firmware is installed there automatically. Thus, a camera can be serviced and updated remotely without requiring a technician to make changes to the device on site. The latest firmware can be obtained from your customer service center or from the download area.

Update server
The address of the update server appears in the address box.
1. Click **Check** to make a connection to this server.
2. Select the appropriate version for your camera to download the firmware from the server.

Firmware
To update the firmware:
1. First, store the firmware file on your hard disk.
2. Enter the full path for the firmware file in the field or click **Browse...** to locate and select the file.
3. Click **Upload** to begin transferring the file to the device. The progress bar allows monitoring of the transfer.

The new firmware is unpacked and the Flash memory is reprogrammed. The time remaining is shown by the message going to reset Reconnecting in ... seconds. When the upload is completed successfully, the device reboots automatically.

Upload history
Click **Show** to view the firmware upload history.

Configuration

Save configuration data for the device to a computer and load saved configuration data from a computer to the device.

To load configuration data from the computer to the device:

1. Click **Browse...**. A dialog box appears.
   Make certain that the file to be loaded comes from the same device type as the device to be reconfigured.
2. Locate and open the desired configuration file. If the configuration file is password-protected, enter the password.
3. Click **Upload**.
   The progress bar allows monitoring of the transfer. The time remaining is shown by the message going to reset Reconnecting in ... seconds. When the upload is completed successfully, the device reboots automatically.

To save the camera settings:

1. Click **Download**. A dialog box appears.
2. Enter a password to protect the configuration file.
3. Enter a file name if required and save the file.

Maintenance log

Download an internal maintenance log from the device to send it to Customer Service for support purposes. Click **Download** and select a storage location for the file.

4.8.2 Licenses

This window activates more functions with use of an **Activation key**. An overview of the **Installed licenses** is shown. Also, the **Installation code** of the unit is shown.

4.8.3 Certificates

This section shows the installed certificates.

Usage list

HTTPS server

Select the default certificate for the HTTPS server.

EAP-TLS client

Select the client for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).
Note: The only option may be “None.”

TLS-DATE trusted

Select the trusted certificate for TTLS-DATE.

Stratocast

Select the trusted certificate for Stratocast.

CBS certificates

Select the trusted certificate for CBS.

SYSLOG client

Select the client for SYSLOG.

File list

Add a certificate/file to the file list

Click **Add**.

In the Add certificate window choose either:

- **Upload certificate** to select a file that is already available:
  - Click **Browse** to navigate to the required file.
  - Click **Upload**.

- **Generate signing request** for a signing authority to create a new certificate:
  - Fill in all the required fields and click **Generate**.
- **Generate certificate** to create a new self-signed certificate:
  - Fill in all the required fields and click **Generate**.

Delete a certificate from the file list

Click the trashcan icon to the right of the certificate. The Delete file window appears. To confirm deletion, click OK. To cancel deletion, click Cancel.

Note: You can only delete certificates that you have added; you cannot delete the default certificate.

Download a certificate

Click on the download icon and a window opens with base64 encoded text of the certificate. Click **Set** to apply the changes.

4.8.4 Logging

Event Logging

Current log level

Select the level of event for which to display log entries or to log.

Number of displayed entries

Select the number of entries to display.

Software Sealing

Enable software sealing

Select this check box to enable software protection that prevents users from adjusting camera settings. This function also protects the camera from unauthorized access.

Debug Logging

Retrieves detailed information of the active logs.

Diagnostics

Retrieves diagnostics information.

Reload

Reloads the displayed entries.

Download log

Save a copy of the entries from the device to a computer.

To save the entries:

1. Click **Download log**; a dialog box appears.

Enter a file name if required and save

4.8.5 System Overview

This window is for information only and cannot be modified. Keep this information at hand when seeking technical support.

Select the text on this page with a mouse and copy it so that it can be pasted into an e-mail if required.

5 Troubleshooting

5.1 Physical reset button

Each camera has a hardware reset button. You may need to press the reset button to reset the camera to factory defaults if you encounter the following circumstances:

- You can power up the camera but cannot log on to the camera using the web browser.
- The camera doesn't start up, or fails to power up via PoE.
- The camera cannot search an IP address.
- The camera's firmware crashed.
- You forgot the password to access the camera.
- The image becomes frozen.
- You cannot update the firmware.
- The camera disconnects from the network at random and needs a reboot.
- The camera no longer finds pre-positions (preset positions).
- You cannot configure the camera using the web browser.
- The camera has no video out.

Notice!
A factory default deletes all camera settings including passwords, network settings, and image settings.
Complete the following sequence of steps only if you have no other option to restore operation to the camera.

Steps to complete a hardware reset for all camera models

1. Apply power to the camera. Search for the IP address, and then log on to the camera using the web browser. (**Note**: You can use Configuration Manager to identify the IP address.)
2. Find the hardware reset button on the camera block. (See each section below to locate the reset button for your camera model.)
3. Push and hold the reset button for more than 8 seconds. The red LED indicator on the PCBA board will come on to show that the hardware reset started.
4. Let the camera complete a self-check. When the self-check completes, the red LED will go off.
5. Search again for the IP address. Access the camera using the web browser. Set the initial password for the camera.

For FLEXIDOME IP micro 3000i - outdoor, the reset button is on the opposite side of the **SD card** slot. To access the reset button, remove the camera bubble.

For FLEXIDOME IP turret 3000i IR - outdoor, the reset button is in a slot in the back of the camera module. To access the reset button, remove the cover.

6 Appendices

6.1 Copyright notices

The firmware uses the fonts "Adobe-Helvetica-Bold-R-Normal--24-240-75-75-P-138-ISO10646-1" and "Adobe-Helvetica-Bold-R-Normal--12-120-75-75-P-70-ISO10646-1" under the following copyright:
Copyright 1984-1989, 1994 Adobe Systems Incorporated.
Copyright 1988, 1994 Digital Equipment Corporation.
Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both those copyright notices and this permission notice appear in supporting documentation, and that the names of Adobe Systems and Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

This software is based in part on the work of the Independent JPEG Group.
Stratocast is a trademark of Genetec, Inc.
Dropbox is a trademark of Dropbox, Inc.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2020

202012091737