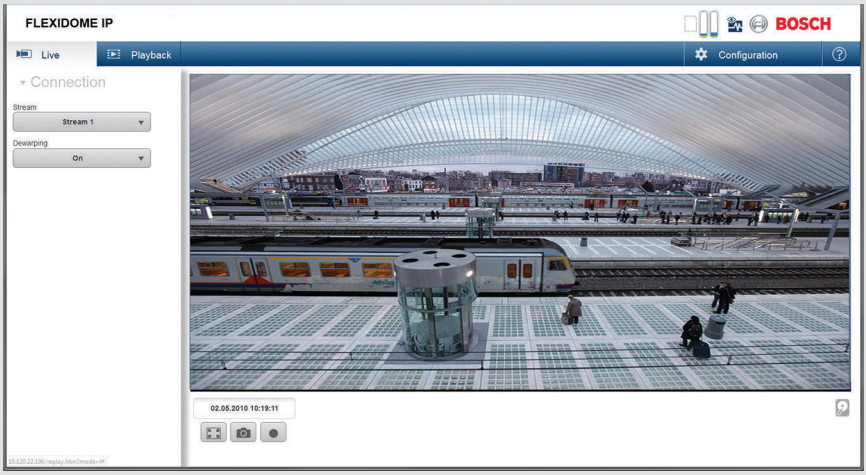

Camera Browser Interface

FLEXIDOME IP panoramic 5000 MP

use-IP
www.use-ip.co.uk
01304 827609

BOSCH

en Software manual

Table of contents

1	**Browser connection**	**10**
1.1	System requirements	10
1.2	Establishing the connection	10
1.2.1	Password protection in camera	11
1.3	Protected network	11
2	**System overview**	**12**
2.1	Live page	12
2.2	Playback	12
2.3	Configuration	12
3	**Operation via the browser**	**14**
3.1	Live page	14
3.1.1	Dewarping	14
3.1.2	Image selection	14
3.1.3	Image orientation	14
3.1.4	Recording status	15
3.1.5	Saving snapshots	15
3.1.6	Recording live video	15
3.1.7	Full-screen display	15
3.1.8	Storage, CPU and network status	16
3.1.9	Status icons	17
3.2	Playback	18
3.2.1	Selecting the recording stream	18
3.2.2	Searching for recorded video	18
3.2.3	Exporting recorded video	19
3.2.4	Controlling playback	19
4	**General settings**	**21**
4.1	Identification	21
4.1.1	Naming	21
4.1.2	ID	21
4.1.3	iSCSI Initiator extension	21
4.2	Password	22
4.2.1	Enter Password	22
4.2.2	Confirm password	22

4.3	Date/Time	23
4.3.1	Date format	23
4.3.2	Device date / Device time	23
4.3.3	Device time zone	23
4.3.4	Daylight saving time	23
4.3.5	Time server IP address	24
4.3.6	Time server type	24
4.4	Display Stamping	25
4.4.1	Camera name stamping	25
4.4.2	Logo stamping	25
4.4.3	Time stamping	25
4.4.4	Display milliseconds	25
4.4.5	Alarm mode stamping	26
4.4.6	Alarm message	26
4.4.7	Transparent background	26
4.4.8	Video authentication	26
4.5	GB/T 28181	26
5	**Web Interface**	**28**
5.1	Appearance	28
5.1.1	Website language	28
5.1.2	Company logo	28
5.1.3	Device logo	28
5.1.4	Show VCA metadata	28
5.1.5	Show overlay icons	28
5.1.6	JPEG size, interval and quality	29
5.2	LIVE Functions	30
5.2.1	Transmit audio	30
5.2.2	Allow snapshots	30
5.2.3	Allow local recording	30
5.2.4	I-frames-only stream	30
5.2.5	Path for JPEG and video files	30
5.2.6	Video file format	30
6	**Camera**	**31**
6.1	Installer Menu	31
6.1.1	Base frame rate	31

6.1.2	Positioning	31
6.1.3	Reboot device	31
6.1.4	Factory defaults	31
6.2	Picture settings – Scene mode	32
6.2.1	Current mode	32
6.2.2	Mode ID	32
6.2.3	Copy mode to	32
6.2.4	Restore Mode Defaults	32
6.2.5	Scene mode factory defaults	32
6.3	Picture settings – Color	34
6.3.1	White balance	34
6.4	Picture settings – ALC	36
6.4.1	ALC mode	36
6.4.2	ALC level	36
6.4.3	Exposure/frame rate	36
6.5	Picture settings – Enhance	37
6.5.1	Sharpness level	37
6.5.2	Backlight Compensation	37
6.5.3	Contrast enhancement	37
6.5.4	Intelligent DNR	37
6.5.5	Intelligent defog	37
6.6	Picture settings – Scene mode scheduler	38
6.7	Encoder Settings	39
6.8	Privacy Masks	40
6.9	Audio	41
6.9.1	Select input	41
6.9.2	Adjust level	41
6.9.3	Recording format	41
6.10	Pixel Counter	42
7	**Encoder Settings**	**43**
7.1	Introduction to encoder settings	43
7.2	Encoder Profile	44
7.2.1	Pre-defined profiles	44
7.2.2	Changing a profile	44
7.2.3	Profile name	44

7.2.4	Target bit rate	45
7.2.5	Maximum bit rate	45
7.2.6	Encoding interval	45
7.2.7	Expert Settings	45
7.2.8	Default	47
7.3	Encoder Streams	48
7.3.1	H.264 settings	48
7.3.2	JPEG stream	48
7.4	Encoder Regions	49
8	**Recording**	**50**
8.1	Introduction to recording	50
8.2	Storage Management	51
8.2.1	Device manager	51
8.2.2	Recording media	51
8.2.3	Activating and configuring storage media	52
8.2.4	Formatting storage media	52
8.2.5	Deactivating storage media	53
8.3	Recording Profiles	54
8.3.1	Recording track selection	54
8.3.2	Standard recording	55
8.3.3	Alarm recording	55
8.4	Maximum Retention Time	57
8.5	Recording Scheduler	58
8.5.1	Weekdays	58
8.5.2	Holidays	58
8.5.3	Profile names	59
8.5.4	Activate recording	59
8.5.5	Recording status	59
8.6	Recording Status	59
9	**Alarm**	**60**
9.1	Alarm Connections	60
9.1.1	Connect on alarm	60
9.1.2	Number of destination IP address	60
9.1.3	Destination IP address	60
9.1.4	Destination password	60

9.1.5	Video transmission	61
9.1.6	Stream	61
9.1.7	Remote port	61
9.1.8	Video output	61
9.1.9	Decoder	62
9.1.10	SSL encryption	62
9.1.11	Auto-connect	62
9.1.12	Audio	62
9.1.13	Default camera	62
9.2	Video Content Analyses (VCA)	63
9.3	Audio Alarm	64
9.3.1	Audio alarm	64
9.3.2	Name	64
9.3.3	Signal Ranges	64
9.3.4	Threshold	64
9.3.5	Sensitivity	64
9.4	Alarm E-Mail	65
9.4.1	Send alarm e-mail	65
9.4.2	Mail server IP address	65
9.4.3	SMTP user name	65
9.4.4	SMTP password	65
9.4.5	Format	65
9.4.6	Image size	65
9.4.7	Attach JPEG from camera	66
9.4.8	Destination address	66
9.4.9	Sender name	66
9.4.10	Test e-mail	66
9.5	Alarm Task Editor	67
10	**Setting up VCA**	**68**
10.1	VCA - Silent VCA	68
10.2	VCA - Profiles	68
10.2.1	Aggregation time [s]	68
10.2.2	Analysis type	69
10.2.3	Tamper detection	69
10.3	VCA - Scheduled	73

10.3.1	Weekdays	73
10.3.2	Holidays	73
10.4	VCA - Event triggered	75
10.4.1	Trigger	75
10.4.2	Trigger active	75
10.4.3	Trigger inactive	75
10.4.4	Delay [s]	75
11	**Network**	**76**
11.1	Network Access	76
11.1.1	Automatic IP assignment	76
11.1.2	IP V4 address	76
11.1.3	IP V6 address	77
11.1.4	DNS server address	77
11.1.5	Video transmission	77
11.1.6	HTTP browser port	77
11.1.7	HTTPS browser port	77
11.1.8	RCP+ port 1756	78
11.1.9	Telnet support	78
11.1.10	Interface mode ETH	78
11.1.11	Network MSS [Byte]	78
11.1.12	iSCSI MSS [Byte]	79
11.1.13	Network MTU [Byte]	79
11.2	DynDNS	80
11.2.1	Enable DynDNS	80
11.2.2	Provider	80
11.2.3	Host name	80
11.2.4	User name	80
11.2.5	Password	80
11.2.6	Force registration now	80
11.2.7	Status	81
11.3	Advanced	82
11.3.1	Cloud-based Services	82
11.3.2	RTSP port	82
11.3.3	Authentication (802.1x)	82
11.3.4	TCP metadata input	82

11.4	Network Management	83
11.4.1	SNMP	83
11.4.2	UPnP	83
11.4.3	Quality of Service	84
11.5	Multicast	85
11.5.1	Enable	85
11.5.2	Multicast Address	85
11.5.3	Port	86
11.5.4	Streaming	86
11.5.5	Multicast packet TTL	86
11.6	Image Posting	87
11.6.1	JPEG posting	87
11.7	Accounts	88
11.8	IPv4 Filter	89
12	**Service**	**90**
12.1	Maintenance	90
12.1.1	Update server	90
12.1.2	Firmware	90
12.1.3	Upload History	91
12.1.4	Configuration	91
12.1.5	Maintenance log	91
12.2	Licenses	92
12.3	Certificate Store	92
12.4	System Overview	93
13	**Appendices**	**94**
13.1	Copyright notices	94

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

- Network access (Intranet or Internet)
- Microsoft Internet Explorer version 9 (32-bit)
- Screen resolution at least 1024 × 768 pixels
- 16- or 32-bit color depth

The Web browser must be configured to enable Cookies from the IP address of the unit.

In Windows Vista, deactivate protected mode on the **Security** tab under **Internet Options**.

Note:

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

Notice!

Megapixel cameras can generate high bitrate streams. Ensure that your network can handle high volume traffic and that you use a powerful, high performance computer.

1.2 Establishing the connection

The unit must have a valid IP address to operate on your network and a compatible subnet mask. By default, DHCP is preset at the factory to **On** and so your DHCP server assigns an IP address. With no DHCP server the default address is 192.168.0.1

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 Bosch Video Management System.

1.2.1 Password protection in camera

A unit offers the option of limiting access across various authorization levels. If the unit is password-protected, a message to enter the password appears.

1. Enter the user name and the associated password in the appropriate fields.
2. Click **OK**. If the password is correct, the desired page is displayed.

1.3 Protected 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 items:

– **LIVE**,

– **PLAYBACK**,
This link is only visible if a storage medium has been configured for recording. (With VRM recording this option is not active.)

– **Configuration**.

Getting help
To get context sensitive help for a particular page, click the help icon .

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.

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.

3.1.1 Dewarping

To view a circular or dewarped live view image:

1. On the left side of the browser, expand the **Connection** group if necessary.
2. Click the **Dewarping** arrow to see the options.
3. Select **E-PTZ** or **Off**.

3.1.2 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** arrow to see the options.
3. Select the stream you wish to view.

3.1.3 Image orientation

With dewarping on, you can manipulate the image with the mouse.

– Place the cursor within the image.
– Click an arrow to orientate the image.
– Use the scroll wheel to zoom in and out.

To see the correct orientation of the image, ensure that the mount position and height have been filled-in correctly in the **Installer** menu.

3.1.4 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.

3.1.5 Saving snapshots

Individual images from the displayed live video stream can be saved locally in JPEG format on the computer's hard drive.

– Click the photo camera icon to save a single image.
  – The storage location depends on the configuration of the camera.

3.1.6 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.

3.1.7 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.

3.1.8 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.

3.1.9 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

Click **PLAYBACK** in the application bar to view, search or export recordings. This link is only visible if a direct iSCSI or memory card has been configured for recording. (With VRM recording this option is not active.)

The panel on the left has 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 video input channel:

1. Click the **Video Input** to see the options.
2. Select the video channel you wish to view.

To view a circular or dewarped image for the full image circle:

1. Click the **Dewarping** arrow to see the options.
2. Select **E-PTZ** or **Off**.

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 start and stop date and times.
2. Select an option from the drop-down box to define a search parameter.
3. Click **Start 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.
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 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. The display can span a range from two months to a few seconds.
– 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 time code is displayed on the left above the full-screen icon.
The buttons have the following functions:

- Start/Pause playback
- Select the playback speed using the speed regulator
- Jump to start of active sequence or to previous sequence
- Jump to start of the next video sequence in the list

4 General settings

4.1 Identification

4.1.1 Naming

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.

4.1.2 ID

Each device should be assigned a unique identifier that can be entered here as an additional means of identification.
Each video channel can be given a name. Click the + sign to add an extra line.

4.1.3 iSCSI 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.)

4.2 Password

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 always have to start from the highest authorization level when assigning passwords.
You can define and change a password for each authorization level if you are logged in as service or if the unit is not password protected.
Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters and no special characters are allowed.
The device has three authorization levels: service, user, and live.

- service is the highest authorization level. Entering the correct password gives access to all the functions and allows all configuration settings to be changed.
- user is the middle authorization level. At this level you can operate the device, play back recordings, and also control camera, for example, but you cannot change the configuration.
- live is the lowest authorization level. At this level you can only view the live video image and switch between the different live image displays.

4.2.1 Enter Password

Define and change a separate password for each level. Enter the password (19 characters maximum; no special characters) for the selected level.

4.2.2 Confirm password

Re-enter the new password to ensure that there are no typing mistakes.

4.3 Date/Time

4.3.1 Date format

Select the required date format.

4.3.2 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.

4.3.3 Device time zone

Select the time zone in which the system is located.

4.3.4 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. Select the region or the city which is closest to the system's location from the list box below the table.
3. Click **Generate** to fill the table with the preset values from the unit.
4. Click one of the entries in the table to make changes. The entry is highlighted.
5. Click **Delete** to remove the entry from the table.
6. Choose other values from the list boxes under the table, to change the selected entry. Changes are immediate.
7. 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.
8. When finished, click **OK** to save and activate the table.

4.3.5 Time server IP 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.

4.3.6 Time server type

Select the protocol that is supported by the selected time server. It is recommended to select the **SNTP server** protocol. This protocol provides high accuracy and is required for special applications and future function extensions.

Select **Time server** if the server uses the RFC 868 protocol.

4.4 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.

4.4.1 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.

4.4.2 Logo stamping

To place a logo on the image, select and upload an uncompressed .bmp file with a maximum size of 128x128 pixels and 256 colors to the camera. Its position on the image can then be selected.

4.4.3 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.

4.4.4 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.

4.4.5 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.

4.4.6 Alarm message

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

4.4.7 Transparent background

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

4.4.8 Video authentication

Select a method for verifying the integrity of the video in the **Video authentication** drop-down box.
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.
Enter the interval (in seconds) between insertions of the digital signature.

4.5 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.

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.

5 Web Interface

5.1 Appearance

You can adapt the appearance of the web interface and change the website language to meet your requirements.
GIF or JPEG images can be used to replace the company and device logos. The image can be stored on a web server (for example, http://www.myhostname.com/images/logo.gif). Ensure that a connection to the web server is always available to display the image. The image files are not stored on the unit.
To restore the original graphics, delete the entries in the **Company logo** and **Device logo** fields.

5.1.1 Website language

Select the language for the user interface.

5.1.2 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.

5.1.3 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.

5.1.4 Show VCA metadata

When video analysis is activated, additional information from the video content analysis (VCA) function is displayed in the live video image. With the MOTION+ analysis type, for example, the sensor fields in which motion is recorded are marked with rectangles.

5.1.5 Show overlay icons

When selected, various status icons are displayed as an overlay on the video images.

5.1.6 JPEG size, interval and quality

Select the size, update interval and quality of the M-JPEG image displayed on the livepage. The highest quality is **1**. When **Best possible** is selected for size, the unit determines the quality based on the network capacity.

5.2 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**. The selected elements are checked.
2. Check to see if the desired items are shown.

5.2.1 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.
(Only available for cameras with audio functions)

5.2.2 Allow snapshots

Select the type of player to be used for live mode viewing.

5.2.3 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.

5.2.4 I-frames-only stream

Select to display an additional tab on the **LIVE** page where only I-frames can be viewed. Ensure that I-frame quality is not set to **Auto** or no updates will occur.

5.2.5 Path for JPEG and video files

Enter the path for the storage location of individual images and video sequences saved from the **LIVE**.

5.2.6 Video file format

Select a file format for the live page display. The MP4 format does not include metadata.

6 Camera

6.1 Installer Menu

6.1.1 Base frame rate

Select the base frame rate for the camera.

Note:
Shutter times and frame rates, and the analog output (if present) are affected by this value.

6.1.2 Positioning

Select the type of positioning you require: The **Mount position** allows you to select wall, ceiling or custom mounting positions.

6.1.3 Reboot device

Click **Reboot** to restart the camera.

6.1.4 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.

6.2 Picture settings – Scene mode

A scene mode is a collection of image parameters that are set in the camera when that particular mode is selected (installer menu settings are excluded). Several pre-defined modes are available for typical scenarios. After a mode has been selected, additional changes can be made through the user interface.

6.2.1 Current mode

Select the mode you wish to use from the drop-down menu.

6.2.2 Mode ID

The name of the selected mode is displayed.

6.2.3 Copy mode to

Select the mode from the drop-down menu to which you wish to copy the active mode.

6.2.4 Restore Mode Defaults

Click **Restore Mode Defaults** to restore the factory default modes. Confirm you decision.

6.2.5 Scene mode factory defaults

Indoor

This mode is similar to the outdoor mode but it avoids the limitations imposed by the sun or street lighting.

Outdoor

This mode covers most situations. It should be used in applications where the lighting changes from day to night. It takes into account sun highlights and street (sodium vapor) lighting.

Traffic
This mode is used for monitoring the traffic movement on roads or parking lots. It can also be used for industrial applications where fast moving objects are to be monitored. Motion artifacts are minimized. This mode should be optimized for a sharp and detailed picture in color and black/white.

Night-optimized
This mode is optimized for sufficient details at low light. It requires more bandwidth and can introduce motion judder.

BLC
This mode is optimized for scenes with people moving in front of a bright background.

Vibrant
This mode has enhanced contrast, sharpness and saturation.

Low bit rate
This mode reduces the bitrate for installations with restricted network bandwidth and storage.

Sports and gaming
This mode is for high-speed capture, and improved color rendition and sharpness.

Retail
This mode has improved color rendition and sharpness with reduced bandwidth requirements.

6.3 Picture settings – Color

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.

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

6.3.1 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 vapor 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** mode the Red, Green, and Blue gain can be manually set to a desired position.

Hold
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** white balance mode, adjust the red gain slider to offset the factory white point alignment (reducing red introduces more cyan).

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

B-gain
In **Manual** 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.

6.4 Picture settings – ALC

6.4.1 ALC mode

Select the mode for automatic light-level control:

- Fluorescent 50 Hz
- Fluorescent 60 Hz
- Outdoor

6.4.2 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.

6.4.3 Exposure/frame rate

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 minimum frame rate for automatic exposure. (The values available depend on the value set for the **Base frame rate** in the **Installer Menu**.)

Default shutter

The default shutter improves the motion performance in auto exposure mode.

- Select a default shutter speed.

Fixed exposure

Select to set a fixed shutter speed.

- Select the shutter speed for fixed exposure. (The values available depend on the value set for the ALC mode.)

6.5 Picture settings – Enhance

6.5.1 Sharpness level

The slider adjusts the sharpness level between -15 and +15. Zero position of the slider corresponds to the factory default level.
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.

6.5.2 Backlight Compensation

Select **Off** to switch off backlight compensation.
Select **On** to capture details in high-contrast and extremely bright-dark conditions.

6.5.3 Contrast enhancement

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

6.5.4 Intelligent DNR

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

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.

6.5.5 Intelligent defog

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

6.6 Picture settings – Scene mode scheduler

The scene mode scheduler is used to determine which scene mode should be used during the day and which scene mode should be used during the night.

1. Select the mode you wish to use during the day from **Day mode** drop-down box.
2. Select the mode you wish to use during the night from **Night mode** drop-down box.
3. Use the two slider buttons to set the **Day time range**.

6.7 Encoder Settings

The encoder settings allow you to adapt the video data transmission characteristics for your operating environment (network structure, bandwidth, data load). The device simultaneously generates two H.264 video streams and an M-JPEG stream for transmission. Select the compression settings of these streams individually, for example, one setting for transmissions to the Internet and one for LAN connections.
Refer to Encoder Profile for more information on setting up the encoder profile.
Refer to Encoder Streams for more information on setting up the encoder streams.
Refer to Encoder Regions for more information on setting up the encoder regions.

6.8 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.
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.

6.9 Audio

(Only available for cameras with audio functions)
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**.

6.9.1 Select input

Select the audio input from the drop-down list.

6.9.2 Adjust level

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

6.9.3 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/)

6.10 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.

7 Encoder Settings

7.1 Introduction to encoder settings

The encoder settings determine the characteristics of the four streams generated by the camera. The types of streams that can be generated are:

- HD streams
- SD streams
- I-frame only streams for recording
- M-JPEG streams

The bit rates, the encoding interval, and the Group-of-Pictures (GOP) structure and quality, are defined and stored for eight different profiles on the **Encoder Profile** page. The SD (Standard Definition) resolution is also selected here.

The resolution of the two H.264 streams and the pre-defined profile to be used for each stream is selected on the **Encoder Streams** page. The maximum frame rate and quality of the JPEG stream is also selected here.

The streams and profiles for recording are selected on the **Recording Profiles** page.

The **Encoder Regions** page allows you to select different quality levels for various areas of the image. This can help in reducing the bit rate. For example, important objects can be selected to provide higher quality encoding than selected background areas.

7.2 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.

7.2.1 Pre-defined profiles

Eight definable profiles are available. The pre-defined profiles give priority to different parameters.

- **Profile 1**
  High resolution for high bandwidth connections
- **Profile 2**
  High resolution with lower data rate
- **Profile 3**
  High resolution for low bandwidth connections
- **Profile 4**
  Standard resolution for high bandwidth connections
- **Profile 5**
  Standard resolution with lower data rate
- **Profile 6**
  Standard resolution for low bandwidth connections
- **Profile 7**
  Standard resolution for DSL connections
- **Profile 8**
  Low resolution for mobile phone connections

7.2.2 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.

7.2.3 Profile name

If required, enter a new name for the profile.

7.2.4 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.

7.2.5 Maximum bit rate

This maximum data rate is not exceeded under any circumstances. Depending on the video quality settings for the I-frames and P-frames, this can result in individual images being skipped.
The value entered here must be at least 10% higher than the value entered in the **Target bit rate** field. If the value entered here is too low, it is automatically adjusted.

7.2.6 Encoding interval

The **Encoding interval** slider determines the interval at which images are encoded and transmitted. This can be particularly advantageous with low bandwidths. The image rate in ips (images per second) is displayed next to the slider.

7.2.7 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).

Averaging period

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

I-frame distance

Use the slider to set the distance between I-frames to **Auto** or to between **3** and **60**. An entry of 3 means that every third image is an I-frame.The lower the number, the more I-frames are generated.

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.

7.2.8 Default

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

7.3 Encoder Streams

7.3.1 H.264 settings

Select H.264 Settings

1. Select a codec algorithm **Property** for stream 1 from the drop-down box.
2. Select the **Non-recording profile** for stream 1 from the eight profiles that have been defined.
   – This profile is not used for recording. When a stream is used for recording, the profile selected on the **Recording Profiles** page is used.
3. Select a codec algorithm **Property** for stream 2 (the available choices depend on the algorithm selected for stream 1).
4. Select the **Non-recording profile** for stream 2 from the eight profiles that have been defined.
   – This profile is not used for recording. When a stream is used for recording, the profile selected on the **Recording Profiles** page is used.

7.3.2 JPEG stream

Set the parameters for the M-JPEG stream.

– Select the **Resolution**.
– Select the **Max. frame rate** in images per second (ips).
– 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.

7.4 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.

8 Recording

8.1 Introduction to 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.

8.2 Storage Management

8.2.1 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.

8.2.2 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 (not available on some cameras).

– To use the SD card for ANR, check the box.
– 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. An SD card of Class 6 or higher is recommended.

8.2.3 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:
A 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.

8.2.4 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.

8.2.5 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.

8.3 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.)

8.3.1 Recording track selection

Standard and alarm recording can be defined for the two recording tracks. You must first select the track before setting up the standard and alarm recording parameters.

1. Click the **Recording 1** entry in the list.
2. Set up the standard and alarm recording parameters for track 1 as described below.
3. Click the **Recording 2** entry in the list.
4. Set up the standard and alarm recording parameters for track 2 as described below.

Recording includes

Specify whether additional data, such as audio (if available) or metadata (for example, alarms or VCA data) should also be recorded. (If audio is available, you can change the global audio format by clicking the audio format link.)

Note:

Including metadata could make subsequent searches of recordings easier but it requires additional memory capacity. Without metadata, it is not possible to include video content analysis in recordings.

8.3.2 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**

8.3.3 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 an alarm recording:

– **Alarm input**
– **Analysis alarm**
– **Video loss**

Select the **Virtual alarm** 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.

8.4 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.

Make sure that the retention time does not exceed the available recording capacity.

8.5 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.

8.5.1 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. Use the right mouse button to deselect any of 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.

8.5.2 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.

Delete user-defined holidays as follows:

1. Click **Delete** in the **Holidays** tab. A new window opens.

2. Click the date to be deleted.
3. Click **OK**. The selection is removed from the table and the window is closed.
4. Repeat for any other dates to be deleted.

8.5.3 Profile names

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.

8.5.4 Activate 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.

8.5.5 Recording status

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

8.6 Recording Status

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

9 Alarm

9.1 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.

9.1.1 Connect on alarm

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

9.1.2 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.

9.1.3 Destination IP address

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

9.1.4 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.

9.1.5 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).

9.1.6 Stream

Select a stream to be transmitted.

9.1.7 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**.

9.1.8 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.

9.1.9 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.

9.1.10 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 **Maintenance** 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).

9.1.11 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.

9.1.12 Audio

Select **On** to transmit the audio stream with an alarm connection.

9.1.13 Default camera

Select the video channel that you wish to send.

9.2 Video Content Analyses (VCA)

The camera has integrated Video Content Analyses (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 analyses.

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.

9.3 Audio Alarm

(Only available for cameras with audio functions)
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.

9.3.1 Audio alarm

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

9.3.2 Name

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

9.3.3 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.

9.3.4 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.

9.3.5 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.

9.4 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.

9.4.1 Send alarm e-mail

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

9.4.2 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**).

9.4.3 SMTP user name

Enter a registered user name for the chosen mail server.

9.4.4 SMTP password

Enter the required password for the registered user name.

9.4.5 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.

9.4.6 Image size

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

9.4.7 Attach JPEG from camera

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

9.4.8 Destination address

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

9.4.9 Sender name

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.

9.4.10 Test e-mail

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

9.5 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.

10 Setting up VCA

Several VCA configurations are available.

- **Off**
- Silent VCA
- **Profile #1**
- **Profile #2**
- **Scheduled**
- **Event triggered**

10.1 VCA - 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.

10.2 VCA - Profiles

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.

10.2.1 Aggregation time [s]

Set an aggregation time of between 0 and 20 seconds. The aggregation time always starts when an alarm event occurs. It extends the alarm event by the value set. This prevents alarm

events that occur in quick succession from triggering several alarms and successive events in a rapid sequence. No further alarm is triggered during the aggregation time.
The post-alarm time set for alarm recordings only starts once the aggregation time has expired.

10.2.2 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.
Click **Configuration** to set up the analysis type.

10.2.3 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.
Sensitivity and **Trigger delay [s]** can only be changed if **Reference check** is selected.

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 **Select Area** and select the areas in the reference image that are to be monitored.

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, and the selected areas are marked in yellow.
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.

Selecting the area

Select the image areas in the reference image that are to be monitored. The video image is subdivided into square fields. Activate or deactivate each of these fields individually.
Select only those areas for reference monitoring in which no movement takes place and that are always evenly lit, as false alarms could otherwise be triggered.

1. Click **Select Area** to configure the sensor fields. A new window opens.
2. If necessary, click **Clear All** first to clear the current selection (fields marked yellow).
3. Left-click the fields to be activated. Activated fields are marked yellow.
4. If necessary, click **Select All** to select the entire video-frame for monitoring.
5. Right-click any fields to deactivate.
6. Click **OK** to save the configuration.
7. Click the close button (**X**) in the window title bar to close the window without saving the changes.

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 **Select Area**. 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.

Global change

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

Scene too bright

Activate this function if tampering associated with exposure to extreme light (for instance, shining a flashlight directly on the objective) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Scene too dark

Activate this function if tampering associated with covering the objective (for instance, by spraying paint on it) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Scene too noisy

Activate this function if tampering associated with EMC interference (noisy scene as the result of a strong interference signal in the vicinity of the video lines) should trigger an alarm.

10.3 VCA - 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.
The current alarm status is displayed for information purposes.

10.3.1 Weekdays

Link any number of 15-minute intervals with the VCA profiles for each day of the week. Moving the mouse cursor over the table displays the time below it. This aids orientation.

1. Click the profile to link in the **Time periods** field.
2. Click in a field in the table, hold down the mouse button and drag the cursor over all the periods to be assigned to the selected profile.
3. Use the right mouse button to deselect any of the intervals.
4. Click **Select All** to link all time intervals to the selected profile.
5. Click **Clear All** to deselect all of the intervals.
6. When finished, click **Set** to save the settings in the device.

10.3.2 Holidays

Define holidays on which a profile should be active that are different to the standard weekly schedule.

1. Click the **Holidays** tab. Any days that have already been selected are shown in the table.
2. Click **Add**. A new window opens.
3. Select the desired date from the calendar. Select several consecutive calendar days by holding down the mouse button. These will later be displayed as a single entry in the table.
4. Click **OK** to accept the selection. The window closes.
5. Assign the individual holidays to the VCA profiles, as described above.

Deleting Holidays

Delete defined holidays at any time:

1. Click **Delete**. A new window opens.
2. Click the date to delete.
3. Click **OK**. The item is deleted from the table and the window closes.
4. The process must be repeated for deleting additional days.

10.4 VCA - 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.
The current alarm status is displayed for information purposes.

10.4.1 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.

10.4.2 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.

10.4.3 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.

10.4.4 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.

11 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.

11.1 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.

11.1.1 Automatic IP assignment

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

11.1.2 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).

11.1.3 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).

11.1.4 DNS server address

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.

11.1.5 Video transmission

If the device is used behind a firewall, TCP (Port 80) 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.

11.1.6 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.

11.1.7 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, the RCP+ port, and Telnet support. 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.

11.1.8 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.

11.1.9 Telnet support

Activating Telenet support allows unencrypted connections on this port. To allow only encrypted connections, set the **Off** option to deactivate telnet support, making telnet connections impossible.

11.1.10 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.

11.1.11 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.

11.1.12 iSCSI MSS [Byte]

Specify a higher MSS value for a connection to the iSCSI system than for the other data traffic via the network. The potential value depends on the network structure. A higher value is only useful if the iSCSI system is located in the same subnet as the camera.

11.1.13 Network MTU [Byte]

Specify a maximum value in bytes for the package size (including IP header) to optimize data transmission.

11.2 DynDNS

11.2.1 Enable 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.

11.2.2 Provider

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

11.2.3 Host name

Enter the host name registered for the unit.

11.2.4 User name

Enter the user name you registered.

11.2.5 Password

Enter the password you registered.

11.2.6 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.

11.2.7 Status

The status of the DynDNS function is displayed here for information purposes; these settings cannot be changed.

11.3 Advanced

11.3.1 Cloud-based Services

The operation mode determines how the camera communicates with Cloud-based Security and Services.

- Select **Auto** to allow the camera to poll the server a few times; if no contact is made, it stops polling.
- Select **On** to constantly poll the server.
- Select **Off** to block polling.

11.3.2 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.

11.3.3 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.

11.3.4 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**.

11.4 Network Management

11.4.1 SNMP

The camera supports the SNMP V1 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. It supports SNMP MIB II in the unified code.
If **On** is selected for the SNMP parameter and a SNMP host address is not entered, the device does not send the traps automatically and will only reply to SNMP requests. If one or two SNMP host addresses are entered, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

SNMP host addresses

To send SNMP traps automatically, enter the IP address of one or two target devices here.

SNMP traps

To choose which traps are sent:

1. Click **Select**. A dialog box appears.
2. Click the check boxes of the appropriate traps.
3. Click **Set** to close the window and send all of the checked traps.

11.4.2 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.

11.4.3 Quality of Service

The priority of the different data channels can be set by defining the DiffServ Code Point (DSCP). Enter a number between 0 and 252 as a multiple of four. For alarm video you can set a higher priority than for regular video and you can define a Post Alarm Time over which this priority is maintained.

11.5 Multicast

The camera 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. Switch between the streams by clicking the appropriate tabs.
The video channels can be individually selected for each stream.

11.5.1 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.

11.5.2 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.

11.5.3 Port

Enter the port address for the stream here.

11.5.4 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.)

11.5.5 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.

11.6 Image Posting

A target account must first be defined to use JPEG posting and for the export of recordings.

11.6.1 JPEG posting

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

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, ensure that the date and time of the device are always set correctly. For eample, the file snap011005_114530.jpg was stored on October 1, 2005 at 11.45 and 30 seconds.

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.

11.7 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 on FTP server
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.

11.8 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.

12 Service

12.1 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.

12.1.1 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.

12.1.2 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.
If the operating status LED lights up red, the upload has failed and must be repeated. To perform the upload, switch to a special page:

1. In the address bar of your browser, enter /main.htm after the device IP address, for example: 192.168.0.10/main.htm
2. Repeat the upload.

12.1.3 Upload History

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

12.1.4 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 **Upload**; 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.
   The progress bar allows monitoring of the transfer.

To save the camera settings:

1. Click **Download**; a dialog box appears.
2. Enter a file name if required and save.

12.1.5 Maintenance log

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

12.2 Licenses

This window is for the activation of additional functions by entering activation codes. An overview of installed licenses is shown. The installation code of the unit is also displayed here.

12.3 Certificate Store

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.”

EAP-TLS trusted
Select the trusted certificate for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).
To add a certificate, click the plus sign.
To delete a certificate, click the trashcan icon to the right of the certificate. **Note:** You can delete only certificates that you have added; you cannot delete the default certificate.

File list

Add a certificate/file to the file list
1. Click **Add**. The Add certificate window appears.
2. Click **Choose File** to navigate to the required file.
3. Click **Upload**.

Delete a certificate from the file list
Click the trashcan icon. The Delete Trusted certificate window appears. To confirm deletion, click OK. To cancel deletion, click Cancel.

Download a certificate
Click the disk icon.

12.4 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.

13 Appendices

13.1 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.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
The Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2015