Camera Browser Interface

DINION IP 5000 MP

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

BOSCH

en Software manual

Table of contents

1	**Browser connection**	**11**
1.1	System requirements	11
1.2	Establishing the connection	11
1.2.1	Password protection in camera	12
1.3	Protected network	12
2	**System overview**	**13**
2.1	Live page	13
2.2	Playback	13
2.3	Settings	13
3	**Operation via the browser**	**14**
3.1	Live page	14
3.1.1	Image selection	14
3.1.2	View Control ROI	15
3.1.3	Digital I/O	16
3.1.4	System Log / Event Log	16
3.1.5	Recording status	16
3.1.6	Saving snapshots	16
3.1.7	Recording video sequences	17
3.1.8	Full-screen display	17
3.1.9	Audio communication	17
3.1.10	Storage, CPU and network status	18
3.1.11	Status icons	19
3.2	Playback	20
3.2.1	Selecting recordings for playback	20
3.2.2	Exporting tracks	20
3.2.3	Searching for tracks	21
3.2.4	Controlling playback	21
4	**Basic Mode**	**23**
4.1	Device Access	23
4.1.1	Name	23
4.1.2	Password	23
4.2	Date/Time	24
4.3	Network	25

4.4	Encoder	25
4.5	Audio	26
4.6	Recording	26
4.7	System Overview	26
5	**General settings**	**27**
5.1	Identification	27
5.1.1	Naming	27
5.1.2	ID	27
5.1.3	iSCSI Initiator extension	27
5.2	Password	28
5.2.1	Enter Password	28
5.2.2	Confirm password	28
5.3	Date/Time	29
5.3.1	Date format	29
5.3.2	Device date / Device time	29
5.3.3	Device time zone	29
5.3.4	Daylight saving time	29
5.3.5	Time server IP address	30
5.3.6	Time server type	30
5.4	Display Stamping	31
5.4.1	Camera name stamping	31
5.4.2	Time stamping	31
5.4.3	Display milliseconds	31
5.4.4	Alarm mode stamping	31
5.4.5	Alarm message	32
5.4.6	Transparent stamping	32
5.4.7	Video authentication	32
5.5	GB/T 28181	32
6	**Web Interface**	**33**
6.1	Appearance	33
6.1.1	Website language	33
6.1.2	Company logo	33
6.1.3	Device logo	33
6.1.4	Show VCA metadata	33
6.1.5	Show VCA trajectories	34

6.1.6	Show overlay icons	34
6.1.7	Select video player	34
6.1.8	JPEG size, interval and quality	34
6.2	LIVE Functions	35
6.2.1	Transmit audio	35
6.2.2	Lease time [s]	35
6.2.3	Show alarm inputs	35
6.2.4	Show alarm outputs	35
6.2.5	Show event log	35
6.2.6	Show system log	36
6.2.7	Allow snapshots	36
6.2.8	Allow local recording	36
6.2.9	I-frames-only stream	36
6.2.10	Show Intelligent Tracking	36
6.2.11	Path for JPEG and video files	36
6.3	Logging	37
6.3.1	Save event log	37
6.3.2	Save system log	37
7	**Camera**	**38**
7.1	Installer Menu	38
7.1.1	Base frame rate	38
7.1.2	Camera LED	38
7.1.3	Mirror image	38
7.1.4	Flip image	38
7.1.5	Menu button	38
7.1.6	Analog output	38
7.1.7	Reboot device	38
7.1.8	Factory defaults	38
7.1.9	Lens Wizard	39
7.2	Picture settings – Scene mode	40
7.2.1	Current mode	40
7.2.2	Mode ID	40
7.2.3	Copy mode to	40
7.2.4	Restore Mode Defaults	40
7.2.5	Scene mode factory defaults	40

7.3	Picture settings – Color	42
7.3.1	White balance	42
7.4	Picture settings – ALC	44
7.4.1	ALC mode	44
7.4.2	ALC level	44
7.4.3	Exposure/frame rate	44
7.4.4	Day/night	44
7.5	Picture settings – Enhance	46
7.5.1	Sharpness level	46
7.5.2	Backlight Compensation	46
7.5.3	Contrast enhancement	46
7.5.4	Intelligent DNR	46
7.6	Picture settings – Scene mode scheduler	47
7.7	Encoder Settings	48
7.8	Privacy Masks	49
7.9	Audio	50
7.9.1	Select input	50
7.9.2	Adjust level	50
7.9.3	Recording format	50
7.10	Pixel Counter	51
8	**Encoder Settings**	**52**
8.1	Encoder Profile	53
8.1.1	Pre-defined profiles	53
8.1.2	Changing a profile	53
8.1.3	Profile name	53
8.1.4	Target bit rate	54
8.1.5	Maximum bit rate	54
8.1.6	Encoding interval	54
8.1.7	Standard definition video resolution	54
8.1.8	Expert Settings	54
8.1.9	Default	56
8.2	Encoder Streams	57
8.2.1	H.264 settings	57
8.2.2	JPEG stream	58
8.3	Encoder Regions	59

8.3.1	Regions	59
9	**Recording**	**60**
9.1	Storage Management	60
9.1.1	Device manager	60
9.1.2	Recording media	60
9.1.3	Activating and configuring storage media	61
9.1.4	Formatting storage media	62
9.1.5	Deactivating storage media	62
9.2	Recording Profiles	63
9.2.1	Recording track selection	63
9.2.2	Standard recording	64
9.2.3	Alarm recording	64
9.3	Maximum Retention Time	66
9.4	Recording Scheduler	67
9.4.1	Weekdays	67
9.4.2	Holidays	67
9.4.3	Profile names	68
9.4.4	Activate recording	68
9.4.5	Recording status	68
9.5	Recording Status	69
10	**Alarm**	**70**
10.1	Alarm Connections	70
10.1.1	Connect on alarm	70
10.1.2	Number of destination IP address	70
10.1.3	Destination IP address	70
10.1.4	Destination password	70
10.1.5	Video transmission	71
10.1.6	Stream	71
10.1.7	Remote port	71
10.1.8	Video output	71
10.1.9	Decoder	72
10.1.10	SSL encryption	72
10.1.11	Auto-connect	72
10.1.12	Audio	72
10.2	Video Content Analyses (VCA)	73

10.3	Audio Alarm	74
10.3.1	Audio alarm	74
10.3.2	Name	74
10.3.3	Signal Ranges	74
10.3.4	Threshold	74
10.3.5	Sensitivity	74
10.4	Alarm E-Mail	75
10.4.1	Send alarm e-mail	75
10.4.2	Mail server IP address	75
10.4.3	SMTP user name	75
10.4.4	SMTP password	75
10.4.5	Format	75
10.4.6	Image size	75
10.4.7	Attach JPEG from camera	76
10.4.8	Destination address	76
10.4.9	Sender name	76
10.4.10	Test e-mail	76
10.5	Alarm Task Editor	77
11	**Setting up VCA**	**78**
11.1	VCA - Silent VCA	78
11.2	VCA - Profiles	79
11.2.1	Aggregation time [s]	79
11.2.2	Analysis type	79
11.2.3	Motion detector	80
11.2.4	Tamper detection	81
11.3	VCA - Scheduled	85
11.3.1	Weekdays	85
11.3.2	Holidays	85
11.4	VCA - Event triggered	87
11.4.1	Trigger	87
11.4.2	Trigger active	87
11.4.3	Trigger inactive	87
11.4.4	Delay [s]	87
12	**Interfaces**	**88**
12.1	Alarm input	88

12.1.1 Name 88
12.1.2 Action 88
12.2 Alarm output 89
12.2.1 Idle state 89
12.2.2 Operating mode 89
12.2.3 Output follows 89
12.2.4 Output name 89
12.2.5 Trigger output 89
13 Network 90
13.1 Network Access 90
13.1.1 Automatic IP assignment 90
13.1.2 IP V4 address 90
13.1.3 IP V6 address 91
13.1.4 DNS server address 91
13.1.5 Video transmission 91
13.1.6 HTTP browser port 91
13.1.7 HTTPS browser port 91
13.1.8 RCP+ port 1756 92
13.1.9 Telnet support 92
13.1.10 Interface mode ETH 92
13.1.11 Network MSS [Byte] 92
13.1.12 iSCSI MSS [Byte] 93
13.1.13 Network MTU [Byte] 93
13.2 DynDNS 94
13.2.1 Enable DynDNS 94
13.2.2 Provider 94
13.2.3 Host name 94
13.2.4 User name 94
13.2.5 Password 94
13.2.6 Force registration now 94
13.2.7 Status 95
13.3 Advanced 96
13.3.1 Cloud-based Services 96
13.3.2 RTSP port 96
13.3.3 Authentication (802.1x) 96

13.3.4	TCP metadata input	96
13.4	Network Management	97
13.4.1	SNMP	97
13.4.2	UPnP	97
13.4.3	Quality of Service	98
13.5	Multicast	99
13.5.1	Enable	99
13.5.2	Multicast Address	99
13.5.3	Port	100
13.5.4	Streaming	100
13.5.5	Multicast packet TTL	100
13.6	Image Posting	101
13.6.1	JPEG posting	101
13.7	Accounts	102
13.8	IPv4 Filter	103
13.9	Encryption	104
14	**Service**	**105**
14.1	Maintenance	105
14.1.1	Update server	105
14.1.2	Firmware	105
14.1.3	Upload History	106
14.1.4	Configuration	106
14.1.5	SSL certificate	106
14.1.6	Maintenance log	107
14.2	Licenses	108
14.3	System Overview	109
15	**Appendices**	**110**
15.1	Copyright notices	110

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
- JVM installed

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**.

To play back live video images, an appropriate ActiveX must be installed on the computer. If necessary, install
Bosch Video Client. This can be downloaded from the following address:
http://downloadstore.boschsecurity.com/

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 title bar displays three items: **LIVE**, **PLAYBACK**, **SETTINGS**.

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

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 Settings

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

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 Image selection

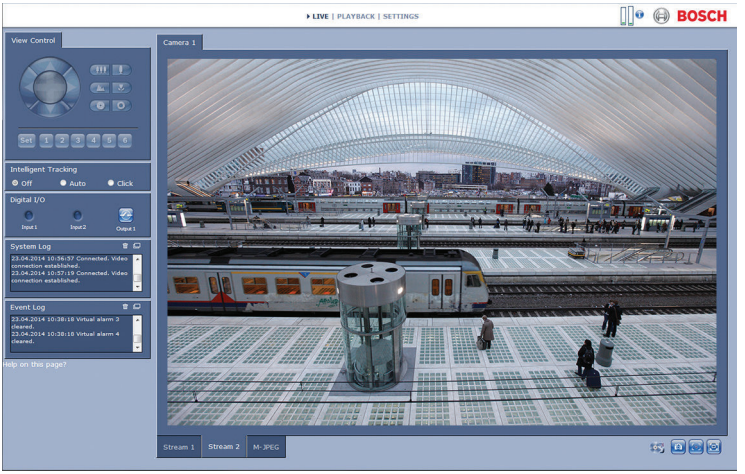


Figure 3.1: Live page

Click a tab below the video image to display a camera image stream.

3.1.2 View Control ROI

When the **Stream 2** encoder stream is set for Region of Interest (ROI), a specific type of **View Control** panel is activated for electronic pan, tilt and zoom control (E-PTZ).
Refer to Encoder Streams for more information on setting up **Stream 2**. (If dual ROI is available, open the camera in a second browser window to set up the ROI on **Stream 2**.)

Zoom

To zoom in on a region of the stream 2 image:

1. Click and hold to zoom in; click and hold to zoom out.
2. Click to see the full image.

Select an area

To select a particular region of the image:

1. Click and hold the arrows to move up and down, and from side to side through the image.
2. Click and hold the center area to move in all directions.

Set positions

To store the current view:

1. Select a region of interest.
2. Click **Set**.
3. Click a number.

To display a pre-set region of interest, click one of the buttons numbered one to six.

3.1.3 Digital I/O

Depending on the configuration of the unit, the alarm input and the output are displayed next to the image.
The alarm symbol is for information and indicates the status of an alarm input:

– Active 1 = Symbol lights
– Active 0 = Symbol not lit.

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

▸ To operate, click the relay symbol.

The symbol is red when the output is activated.

3.1.4 System Log / Event Log

The **System Log** field contains information about the operating status of the camera and the connection.
Events such as the triggering or the end of alarms are shown in the **Event Log** field.

1. To view, filter and save these messages to a file, click in the top right-hand corner.
2. To clear the log, click in the top right-hand corner of the relevant field.

3.1.5 Recording status

The hard drive icon below the camera images on the **LIVE** page 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.

3.1.6 Saving snapshots

Individual images from the video sequence that is currently being shown can be saved in JPEG format on the computer's hard drive.

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

3.1.7 Recording video sequences

Sections of the video sequence that is currently being shown on the **LIVE** page can be saved 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.

Play back saved video sequences using the Player from Bosch Security Systems.

3.1.8 Full-screen display

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

3.1.9 Audio communication

Audio can be sent and received via the **LIVE** page if the unit and the computer support audio.

1. Press and hold the F12 key on the keyboard to send an audio signal to the unit.
2. Release the key to stop sending audio.

All connected users receive audio signals sent from the unit but only the user who first pressed the F12 key can send audio signals; others must wait for the first user to release the key.

3.1.10 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 next to the Bosch logo.
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 IVA settings,
- if the network load is too big, change the encoder profile to reduce bitrate.

3.1.11 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 title 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.)

A collapsible panel on the left of the display has four tabs:

- **Track list**
- **Export**
- **Search**
- **Search results**

Select the recording number to be shown in the **Recording** drop-down menu at the top of the window.

3.2.1 Selecting recordings for playback

To see all saved sequences:

1. Click the track list tab .
2. A list of tracks with a number assigned is displayed. Start time and stop time, recording duration, number of alarms and recording type are shown for each track.
3. At the bottom of the window, select the maximum number of tracks to be displayed in the list.
4. Use the arrow buttons at the bottom to browse the list.
5. To view tracks beginning from a particular time, enter the time code and click **Get Tracks**.
6. Click a track. The playback for the selected track starts.

3.2.2 Exporting tracks

1. Select a track in the track list.
2. Click the export tab .

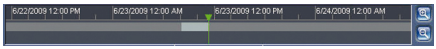
3. The start and stop time are filled-in for the selected track. If required, change the times.
4. Select a target.
5. Select the original or a condensed speed.
6. Click the save icon .

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

3.2.3 Searching for tracks

1. Click the search tab .
2. Click one of the **Search mode** options to define the search parameters.
3. To limit the search to a particular time range, enter the start and stop times.
4. Click **Start Search**.
5. The results are shown in the search results tab .
6. Click a result to play it back.
7. Click the search tab again to define a new search.

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. A green arrow above the bar indicates the position of the image currently being played back within the sequence.
The time bar offers various options for navigation in and between sequences.

– 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.
– If required, click in the bar at the point in time at which the playback should begin.
– Red bars indicate the points in time where alarms were triggered.

To view the current live image, click **Now**.

Controls

Control playback by means of the buttons below the video image.

Use the jog dial to quickly scan the sequences. The time code is displayed above it.

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

Bookmarks

You can set markers in a sequence and jump to these directly. These bookmarks are indicated as small yellow arrows above the time interval. Use the bookmarks as follows:

Jump to the previous bookmark

Set bookmark

Jump to the following bookmark

Bookmarks are only valid while in the **Recordings** page; they are not saved with the sequences. All bookmarks are deleted when you leave the page.

4 Basic Mode

4.1 Device Access

4.1.1 Name

Assign a unique name to assist in identification. This name simplifies the management of multiple devices in more extensive systems.
The name is used for remote identification, for example, in the event of an alarm. Choose a name that makes it as easy as possible to identify the location unambiguously.

4.1.2 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.

Define and change a separate password for each level. Enter the password (19 characters maximum; no special characters) for the selected level.
Re-enter the new password to ensure that there are no typing mistakes.

4.2 Date/Time

If there are multiple devices operating in the 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.
Device time, date and time zone are shown.

▸ 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.

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.
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.

4.3 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.
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.

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).

4.4 Encoder

Select a profile for encoding the video signal on stream 1 (this is not a selection of the recording profile).
Pre-programmed profiles are available that give priority to different parameters and they should be selected based on your operating environment.
When a profile is selected, its details are displayed.

4.5 Audio

Switch the camera audio **On** or **Off**.
Use the slider to adjust the level for the applicable audio signal.

4.6 Recording

Record the images from the camera to a storage medium. For long-term authoritative images, it is essential to use VRM or an appropriately sized iSCSI system.

Storage medium

1. Select the required storage medium from the list.
2. Click **Start** to start recording or **Stop** to end recording.

4.7 System Overview

This page provides general information on the hardware and firmware system, including version numbers. No items can be changed on this page but they can be copied for information purposes when troubleshooting.

5 General settings

5.1 Identification

5.1.1 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.

You can use additional lines to enter kanji characters.

1. Click the + sign to add a new line
2. Click the icon next to the new line. A window with a character map opens.
3. Click the required character. The character is inserted into the **Result** field.
4. In the character map, click the << and >> icons to move between the different pages of the table, or select a page from the list field.
5. Click the < icon to the right of the **Result** field to delete the last character, or click the X icon to delete all characters.
6. Click the **OK** button to apply the selected characters to the new line of the name. The window closes.

5.1.2 ID

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

5.1.3 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.)

5.2 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.

5.2.1 Enter Password

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

5.2.2 Confirm password

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

5.3 Date/Time

5.3.1 Date format

Select the required date format.

5.3.2 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.

5.3.3 Device time zone

Select the time zone in which the system is located.

5.3.4 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.

5.3.5 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.

5.3.6 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.

5.4 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.

5.4.1 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.

5.4.2 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.

5.4.3 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.

5.4.4 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.

5.4.5 Alarm message

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

5.4.6 Transparent stamping

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

5.4.7 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.

5.5 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”.

6 Web Interface

6.1 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.

6.1.1 Website language

Select the language for the user interface.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.1.5 Show VCA trajectories

The trajectories (motion lines of objects) from the video content analysis are displayed in the live video image if a corresponding analysis type is activated.

6.1.6 Show overlay icons

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

6.1.7 Select video player

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

6.1.8 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.

6.2 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.

6.2.1 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.

6.2.2 Lease time [s]

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

6.2.3 Show alarm inputs

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

6.2.4 Show alarm outputs

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

6.2.5 Show event log

The event messages are displayed with the date and time in a field next to the video image.

6.2.6 Show system log

The system messages are displayed with the date and time in a field next to the video image and provide information about the establishment and termination of connections, and other system-level messages.

6.2.7 Allow snapshots

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

6.2.8 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.

6.2.9 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.

6.2.10 Show Intelligent Tracking

Select to display or hide the intelligent tracker panel on the live page.

6.2.11 Path for JPEG and video files

Enter the path for the storage location of individual images and video sequences saved from the **LIVE**. If necessary, click **Browse...** to find a suitable folder.

6.3 Logging

6.3.1 Save event log

Select this option to save event messages in a text file on the local computer. This file can be viewed, edited, and printed with any text editor or standard office software.

File for event log

Enter the path for saving the event log. If necessary, click **Browse...** to find a suitable folder.

6.3.2 Save system log

Select this option to save system messages in a text file on the local computer. This file can be viewed, edited, and printed with any text editor or standard office software.

File for system log

Enter the path for saving the system log. If necessary, click **Browse...** to find a suitable folder.

7 Camera

7.1 Installer Menu

7.1.1 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.

7.1.2 Camera LED

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

7.1.3 Mirror image

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

7.1.4 Flip image

Select **On** to output an upside down camera image.

7.1.5 Menu button

Select **Disabled** to prevent access to the install wizard via the menu button on the camera itself.

7.1.6 Analog output

Select an aspect ratio format to activate the analog output of the camera.

7.1.7 Reboot device

Click **Reboot** to restart the camera.

7.1.8 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.

7.1.9 Lens Wizard

Click **Lens Wizard...** to open a separate window which can be used to focus the camera lens (not for all cameras).

7.2 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.

7.2.1 Current mode

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

7.2.2 Mode ID

The name of the selected mode is displayed.

7.2.3 Copy mode to

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

7.2.4 Restore Mode Defaults

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

7.2.5 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.

7.3 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.

7.3.1 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.
- **SON/SOX auto** mode allows the camera to continually adjust for optimal color reproduction in an environment with sodium vapor light sources (street lighting).
- 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.

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.

7.4 Picture settings – ALC

7.4.1 ALC mode

Select the mode:

- Fluorescent 50 Hz
- Fluorescent 60 Hz
- Outdoor

7.4.2 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.

7.4.3 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.)

7.4.4 Day/night

Auto - the camera switches the IR cut-off filter on and off depending on the scene illumination level.

Monochrome - the IR cut-off filter is removed, giving full IR sensitivity.
Color - the camera always produces a color signal regardless of light levels.

Switch level
Set the video level at which the camera in **Auto** mode switches to monochrome operation (-15 to 0 to +15).
A low (negative) value means that the camera switches to monochrome at a lower light level. A high (positive) value means that the camera switches to monochrome at a higher light level.

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

7.5 Picture settings – Enhance

7.5.1 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.

7.5.2 Backlight Compensation

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

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

7.5.3 Contrast enhancement

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

7.5.4 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.

7.6 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**.

7.7 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.

7.8 Privacy Masks

Privacy masking is used to block a specific area of a scene from being viewed. Four privacy mask areas can be defined. The activated masked areas are filled with the selected pattern in live view.

1. Select the pattern to be used for all masks.
2. Check the box of the mask you wish to activate.
3. Use the mouse to define the area for each of the masks.

7.9 Audio

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

7.9.1 Select input

Select the audio input from the drop-down list.

7.9.2 Adjust level

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

7.9.3 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/)

7.10 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.

8 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.

8.1 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.

8.1.1 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

8.1.2 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.

8.1.3 Profile name

If required, enter a new name for the profile.

8.1.4 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.

8.1.5 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.

8.1.6 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.

8.1.7 Standard definition video resolution

Select the desired resolution for the standard definition video image.

Note:
These resolutions are not used by a HD stream.

8.1.8 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.

8.1.9 Default

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

8.2 Encoder Streams

8.2.1 H.264 settings

Select H.264 Settings

1. Select a codec algorithm **Property** for stream 1 from the drop-down box.
2. Select a codec algorithm **Property** for stream 2 (the available choices depend on the algorithm selected for stream 1).
3. Select the **Non-recording profile** for each stream 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.

Preview >>

Previews of streams 1 and 2 can be shown.

1. Click **Preview>>** to display a preview of the video for streams 1 and 2. The current profile is shown above the preview.
2. Click **1:1 Live View** below a preview to open a viewing window for that stream. Various additional items of information are shown across the top of the window.
3. Click **Preview <<** to close the preview displays.

Note:

Deactivate the display of the video images if the performance of the computer is adversely affected by the decoding of the data stream.

Regions of Interest (ROI)

If you select an ROI property for stream 2, you can set up a region of interest on the **LIVE** page.

8.2.2 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.

8.3 Encoder Regions

8.3.1 Regions

1. Select one of the eight available regions from the drop-down box.
2. Use the mouse to define the area for that region by dragging the center or sides of the shaded window.
3. Select the encoder quality to be used for the defined area. (Object and background quality levels are defined on the **Expert Settings** section of the **Encoder Profile** page.)
4. If required, select another region and repeat steps 2 and 3.
5. Click **Set** to apply the region settings.

Preview

Click to open a viewing window where a 1:1 live image and the bit rate for the region settings can be previewed.

9 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. For further information, contact your local customer service at Bosch Security Systems.

9.1 Storage Management

9.1.1 Device manager

An external Video Recording Manager (VRM) system for the unit is configured via the Configuration Manager. The **Managed by VRM** box is only an indicator; it cannot be changed here.
If the **Managed by VRM** box is checked, you are not able to configure any further recording settings on this page.

9.1.2 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).

- 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.

9.1.3 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.

9.1.4 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.

9.1.5 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.

9.2 Recording Profiles

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

Each profile is color-coded. The names of the profiles can be changed on the **Recording Scheduler** page.
To configure a profile click its tab to open its settings page.

– To copy the currently visible settings to other profiles, click **Copy Settings**. A window opens to select the target profiles for the copied settings.
– If you change a profile's settings, click **Set** to save.
– If necessary, click **Default** to return all settings to their factory defaults.

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

9.2.1 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.

9.2.2 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**

9.2.3 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.

Check the **Export to account** box to send standard H.264 files to the target whose address is displayed.
If the target has not yet been defined, click **Configure accounts** to jump to the **Accounts** page where the server information can be entered.

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.

9.3 Maximum Retention Time

Recordings are overwritten when the retention time entered here has expired.

- Enter the required retention time in days for each recording track.

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

9.4 Recording Scheduler

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

9.4.1 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.

9.4.2 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.

9.4.3 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.

9.4.4 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.

9.4.5 Recording status

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

9.5 Recording Status

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

10 Alarm

10.1 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.

10.1.1 Connect on alarm

Select **On** so that the unit automatically connects to a pre-defined IP address in the event of an alarm.
Select **Follows input 1** so that the unit maintains the connection for as long as an alarm exists on alarm input 1.

10.1.2 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.

10.1.3 Destination IP address

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

10.1.4 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, for example, when connections are initiated by a controlling system such as Bosch Video Client or Bosch Video Management System. 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.

10.1.5 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).

10.1.6 Stream

Select a stream to be transmitted.

10.1.7 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**.

10.1.8 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.

10.1.9 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.

10.1.10 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).

10.1.11 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.

10.1.12 Audio

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

10.2 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.

10.3 Audio Alarm

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

10.3.1 Audio alarm

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

10.3.2 Name

The name makes it easier to identify the alarm in extensive video monitoring systems, for example with the Bosch Video Client and the Bosch Video Management System. Enter a unique and clear name here.

10.3.3 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.

10.3.4 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.

10.3.5 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.

10.4 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.

10.4.1 Send alarm e-mail

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

10.4.2 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**).

10.4.3 SMTP user name

Enter a registered user name for the chosen mail server.

10.4.4 SMTP password

Enter the required password for the registered user name.

10.4.5 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.

10.4.6 Image size

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

10.4.7 Attach JPEG from camera

Check the box to specify that JPEG images are sent from the camera.

10.4.8 Destination address

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

10.4.9 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.

10.4.10 Test e-mail

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

10.5 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.

11 Setting up VCA

Several VCA configurations are available.

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

11.1 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.

11.2 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.

11.2.1 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.

11.2.2 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.

Note:
For suitable devices, additional analysis algorithms with comprehensive functions, such as IVMD and IVA, are also available. Refer to the IVA documentation for more information on using these.

11.2.3 Motion detector

Motion detection is available for the Motion+ analysis type. For the detector to function, the following conditions must be met:

- Analysis must be activated.
- At least one sensor field must be activated.
- The individual parameters must be configured to suit the operating environment and the desired responses.
- The sensitivity must be set to a value greater than zero.

Note:
Reflections of light (from glass surfaces, etc.), lights switching on and off, or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended. For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Sensitivity
Sensitivity is available for the Motion+ analysis type. The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject. The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

Minimum object size
Specify the number of sensor fields that a moving object must cover to generate an alarm. This setting prevents objects that are too small from triggering an alarm. A minimum value of 4 is recommended. This value corresponds to four sensor fields.

Debounce time 1 s

The debounce time prevents very brief alarm events from triggering individual alarms. If the **Debounce time 1 s** option is activated, an alarm event must last at least 1 second to trigger an alarm.

Selecting the area

Select the areas of the image to be monitored by the motion detector. The video image is subdivided into square sensor fields. Activate or deactivate each of these fields individually. To exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, for example), the relevant fields can be deactivated.

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 red).
3. Left-click the fields to be activated. Activated fields are marked red.
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.

11.2.4 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.

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.

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.

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.

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.

11.3 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.

11.3.1 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.

11.3.2 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.

11.4 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.

11.4.1 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.

11.4.2 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.

11.4.3 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.

11.4.4 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.

12 Interfaces

12.1 Alarm input

Configure the alarm triggers for the unit.
Select **N.C.** (Normally Closed) if the alarm is to be triggered by opening the contact.
Select **N.O.** (Normally Open) if the alarm is to be triggered by closing the contact.

12.1.1 Name

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

12.1.2 Action

Select a type of action to be performed when an alarm input occurs:

- **None**
- **Monochrome**
  This switches the camera to the monochrome mode.
- **Switch mode**
  When this is selected, you can select the **Scene Mode** to be used for the active and inactive period of the alarm.

12.2 Alarm output

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

12.2.1 Idle state

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

12.2.2 Operating mode

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

12.2.3 Output follows

Select the event that triggers the output.

12.2.4 Output name

The relay can be assigned a name here. The name is shown on the button next to **Trigger output**. The **LIVE** page can also be configured to display the name next to the relay icon.

12.2.5 Trigger output

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

13 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.

13.1 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.

13.1.1 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.

13.1.2 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).

13.1.3 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).

13.1.4 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.

13.1.5 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.

13.1.6 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.

13.1.7 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.

13.1.8 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.

13.1.9 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.

13.1.10 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.

13.1.11 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.

13.1.12 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.

13.1.13 Network MTU [Byte]

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

13.2 DynDNS

13.2.1 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.

13.2.2 Provider

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

13.2.3 Host name

Enter the host name registered for the unit.

13.2.4 User name

Enter the user name you registered.

13.2.5 Password

Enter the password you registered.

13.2.6 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.

13.2.7 Status

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

13.3 Advanced

13.3.1 Cloud-based Services

The operation mode determines how the camera communicates with Bosch Cloud-based Security and Services. For more information about these services and their availability, visit: http://cloud.boschsecurity.com

- 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.

13.3.2 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.

13.3.3 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.

13.3.4 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**.

13.4 Network Management

13.4.1 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.

13.4.2 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.

13.4.3 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.

13.5 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.

13.5.1 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.

13.5.2 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.

13.5.3 Port

Enter the port address for the stream here.

13.5.4 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.)

13.5.5 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.

13.6 Image Posting

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

13.6.1 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.

13.7 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.

13.8 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.

13.9 Encryption

If an encryption license is installed, this submenu gives access to the encryption parameters.

14 Service

14.1 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 Bosch Security Systems download area.

14.1.1 Update server

The address of the Bosch 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.

14.1.2 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.

14.1.3 Upload History

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

14.1.4 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 **Load From...** ; 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 **Save As...**; a dialog box appears.
2. Enter a file name if required and save.

14.1.5 SSL certificate

To work with an SSL connection, both sides of the connection must have the appropriate certificates. Upload one or more certificate files, one at a time, to the camera.

1. Enter the full path of the file to upload or click **Browse...** to locate the file.
2. Click **Upload** to start the file transfer.

Once all files have been successfully uploaded, the device must be rebooted. In the address field of the browser, enter /reset after the camera's IP address, for example:
192.168.0.10/reset
The new SSL certificate is valid.

14.1.6 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.

14.2 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.

14.3 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.

15 Appendices

15.1 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