VIP X1 XF

VIPX1XF

BOSCH

en Installation and Operating Manual

Table of Contents

1 Preface

1.1 About this Manual

This manual is intended for persons responsible for the installation and operation of the VIP X1 XF. International, national and any regional electrical engineering regulations must be followed at all times. Relevant knowledge of network technology is required. The manual describes the installation and operation of the unit.

1.2 Conventions in this Manual

In this manual, the following symbols and notations are used to draw attention to special situations:

CAUTION!
This symbol indicates that failure to follow the safety instructions described may endanger persons and cause damage to the unit or other equipment.
It is associated with immediate, direct hazards.

NOTICE!
This symbol refers to features and indicates tips and information for easier, more convenient use of the unit.

1.3 Intended Use

The VIP X1 XF network video server transfers video, audio and control signals over data networks (Ethernet LAN, Internet). There are various memory options for recording the images captured by the connected camera. The unit is intended for use with CCTV systems. Various functions can be triggered automatically by incorporating external alarm sensors. Other applications are not permitted.
In the event of questions concerning the use of the unit which are not answered in this manual, please contact your sales partner or:
Bosch Sicherheitssysteme GmbH
Werner-von-Siemens-Ring 10
85630 Grasbrunn
Germany
www.boschsecurity.com

1.4 EU Directives

The VIP X1 XF network video server complies with the requirements of EU Directives 89/336 (Electromagnetic Compatibility) and 73/23, amended by 93/68 (Low Voltage Directive).

1.5 Rating Plate

For exact identification, the model name and serial number are inscribed on the bottom of the housing. Please make a note of this information before installation, if necessary, so as to have it to hand in case of questions or when ordering spare parts.

2 Safety Information

2.1 Electric Shock Hazard

- Never attempt to connect the unit to any power network other than the type for which it is intended.
- Use only power supply units with UL approval and a power output according to LPS or NEC Class 2.
- Never open the housing.
- Never open the housing of the power supply unit.
- If a fault occurs, disconnect the power supply unit from the power supply and from all other units.
- Install the power supply and the unit only in a dry, weather-protected location.
- If safe operation of the unit cannot be ensured, remove it from service and secure it to prevent unauthorized operation. In such cases, have the unit checked by Bosch Security Systems.

  Safe operation is no longer possible in the following cases:
  - if there is visible damage to the unit or power cables,
  - if the unit no longer operates correctly,
  - if the unit has been exposed to rain or moisture,
  - if foreign bodies have penetrated the unit,
  - after long storage under adverse conditions, or
  - after exposure to extreme stress in transit.

2.2 Installation and Operation

- The relevant electrical engineering regulations and guidelines must be complied with at all times during installation.
- Relevant knowledge of network technology is required to install the unit.
- Before installing or operating the unit, make sure you have read and understood the documentation for the other equipment connected to it, such as cameras. The documentation contains important safety instructions and information about permitted uses.
- Perform only the installation and operation steps described in this manual. Any other actions may lead to personal injury, damage to property or damage to the equipment.

2.3 Maintenance and Repair

- Never open the housing of the VIP X1 XF. The unit does not contain any user-serviceable parts.
- Never open the housing of the power supply unit. The power supply unit does not contain any user-serviceable parts.
- Ensure that all maintenance or repair work is carried out only by qualified personnel (electrical engineers or network technology specialists).

3 Product Description

3.1 Scope of Delivery

- VIP X1 XF network video server
- 2 terminal blocks
- 4 self-adhesive elastic bumpers
- 1 wall-mounting panel
- 2 screws
- 2 wall plugs
- 1 Quick Installation Guide
- Product CD with the following content:
  - Quick Installation Guide
  - Manual
  - System Requirements document
  - Further documentation on Bosch Security Systems products
  - Configuration Manager
  - MPEG ActiveX control
  - Player and Archive Player
  - DirectX control
  - Sun JVM
  - Adobe Acrobat Reader

NOTICE!
Check that the delivery is complete and in perfect condition. Arrange for the unit to be checked by Bosch Security Systems if you find any damage.

3.2 System Requirements

General Requirements

- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Screen resolution at least 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).
The Web browser must be configured to enable Cookies to be set from the IP address of the unit.
In Windows Vista, deactivate protected mode on the **Security** tab under **Internet Options**.
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

Additional Configuration Requirements

- Microsoft Internet Explorer (version 7.0 or higher)
  or
- Installed Configuration Manager program (version 3.1 or higher)

Additional Operational Requirements

- Microsoft Internet Explorer (version 7.0 or higher)
  or
- Receiver software, for example VIDOS (version 4.01 or higher) or Bosch Video Management System (version 2.2 or higher)
  or
- H.264 compatible hardware decoder from Bosch Security Systems (for example VIP XD) as a receiver and connected video monitor
- For playing back recordings: connection to storage medium

3.3 Overview of Functions

Network Video Server

The VIP X1 XF is a compact network video server for a connected video source. It is primarily designed for encoding video, audio and control data for transfer over an IP network. With its encoding in the H.264 format, the VIP X1 XF is ideally suited for making existing analog CCTV cameras IP-compatible and for remote access to digital VCRs and multiplexers.
The use of existing networks means that integration with CCTV systems or local networks can be achieved quickly and easily.
Two units, for example a VIP X1 XF as a sender and a VIP XD as a receiver, can create a standalone system for data transfer without a PC. Video images from a single sender can be received simultaneously on multiple receivers. Audio signals can also be transmitted from and to compatible units.

Receiver

Compatible H.264 enabled hardware decoders (for example the VIP XD) can be used as receivers. Computers with decoding software such as VIDOS or computers with the Microsoft Internet Explorer Web browser can also be used as receivers.

Video Encoding

The VIP X1 XF uses the H.264 video compression standard. Thanks to efficient encoding, the data rate remains low even with high image quality and can also be adapted to local conditions within wide limits.

Dual Streaming

Dual Streaming allows the incoming data stream to be encoded simultaneously according to two different, individually customized profiles. This feature creates two data streams that can serve different purposes, for example one for recording and one optimized for live transmission over the LAN.

Multicast

In suitably configured networks, the multicast function enables simultaneous real-time video transmission to multiple receivers. The UDP and IGMP V2 protocols must be implemented on the network for this function.

Encryption

The VIP X1 XF offers a variety of options for protection against unauthorized reading. Web browser connections can be protected using HTTPS. You can protect the control channels via the SSL encryption protocol. With an additional license, the user data itself can be encrypted.

Remote Control
For remote control of external units such as pan or tilt heads for cameras or motorized zoom lenses, control data is transmitted via the VIP X1 XF's bidirectional serial interface. This interface can also be used to transmit transparent data.

Video Content Analysis and Tamper Detection
The VIP X1 XF offers a wide range of configuration options for alarm signaling in the event of tampering with the connected camera. An algorithm for detecting movement in the video image is also part of the scope of delivery and can optionally be extended to include special video analysis algorithms.

Snapshots
Individual video frames (snapshots) from the VIP X1 XF can be called up as JPEG images, stored on the computer's hard drive or displayed in a separate browser window.

Recordings
Various local memory options enable the VIP X1 XF to be used as a digital VCR. A connection to an appropriately configured iSCSI system enables long-term recordings with high image quality over the network.

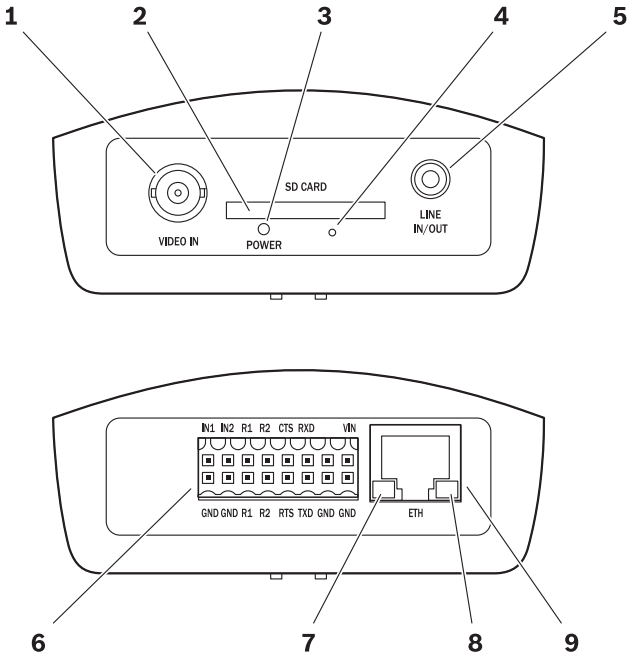
Backup
A function for storing the video images displayed on the hard drive of your computer is available on the **LIVEPAGE** as well as on the **RECORDINGS** page. Video sequences can be stored by means of a mouse click and can be redisplayed using the Player program supplied as part of the scope of delivery.

Summary

The VIP X1 XF provides the following main functions:

- Video and data transmission over IP data networks
- Dual Streaming function for the encoder for simultaneous encoding with two individually definable profiles
- Multicast function for simultaneous image transmission to multiple receivers
- One analog BNC composite video input (PAL/NTSC)
- Video encoding to international standard H.264
- Integrated Ethernet port (10/100 Base-T)
- SD slot for SD cards for local storage
- Transparent, bidirectional data channel via RS-232/RS-422/RS-485 serial interface
- Configuration and remote control of all internal functions via TCP/IP, also secured via HTTPS
- Password protection to prevent unauthorized connection or configuration changes
- Extensive, flexible storage options
- Two alarm inputs and two relay outputs
- Built-in video sensor for motion and tamper alarms
- Event-controlled automatic connection
- Convenient maintenance via uploads
- Flexible encryption of control and data channels
- Authentication according to international standard 802.1x
- Bidirectional audio (mono) for line connections
- Audio encoding to international standard G.711

3.4 Connections, Controls and Displays



1 **VIDEO IN** video input
BNC socket for connecting the video source

2 **SD CARD** slot
for an SD card

3 **POWER** LED
lights up green when ready for operation

4 Factory reset button
to restore factory default settings

5 **LINE IN/OUT** audio connection (mono)
3.5 mm / 1/8 in stereo socket line-out for connecting an audio connection

6 Terminal Block
for alarm inputs, relay outputs, serial interface and power supply

7 Green LED
lights up when the unit is connected to the network

8 Orange LED
lights up during data transmission

9 **ETH** RJ45 socket
for connecting to an Ethernet LAN (local network), 10/100 MBit Base-T

NOTICE!
For more information about the LEDs, see *Section 8.4 LEDs, page 108*.
For terminal block assignment, see *Section 8.8 Terminal Block, page 110*.

4 Installation

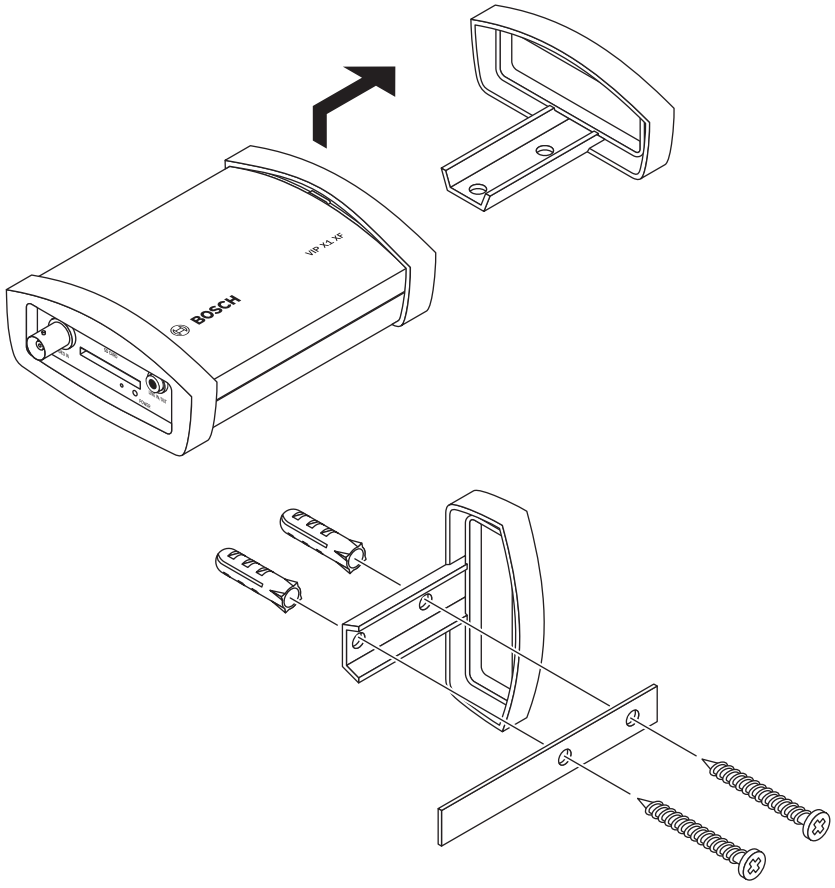
4.1 Preparations

CAUTION!
The unit is intended for use indoors or in housings.
Select a suitable location for installation that guarantees to meet the environmental conditions. The ambient temperature must be between 0 and +50 °C (+32 and +122 °F). The relative humidity must not exceed 95%.
The VIP X1 XF generates heat during operation, so you should ensure that there is adequate ventilation and enough clearance between the unit and heat-sensitive objects or equipment.

Please ensure the following installation conditions:

- Do not install the unit close to heaters or other heat sources. Avoid locations exposed to direct sunlight.
- Allow sufficient space for running cables.
- Ensure that the unit has adequate ventilation.
- When making connections, use only the cables supplied or use appropriate cables immune to electromagnetic interference.
- Position and run all cables so that they are protected from damage, and provide adequate cable strain relief where needed.
- Avoid impacts, blows and severe vibrations that exceed the specification limits (see *Section 9 Specifications, page 114*), as these can irreparably damage the unit.

4.2 Mounting



You can secure the VIP X1 XF to walls, below ceilings or any other load-bearing locations using the wall-mounting panel, in either a vertical or a horizontal position.

CAUTION!

The mounting location must be able to reliably hold the unit. The load-bearing capacity must be adequate for four times the weight of the unit.
If mounting the unit in a vertical position, you will need to use the lower plastic frame and then place the unit onto the frame from above. If mounting the unit in a horizontal position, you can use either of the two frames.

- Lift the plastic frame on one side of the housing and carefully remove it from the unit.
- Screw the plastic frame in the required position together with the wall-mounting panel.
- Check that the plastic frame is secure.
- Place the unit on the wall-mounting panel, with the panel positioned between the housing and the second plastic frame.
- Slide the unit into the plastic frame until you feel it lock securely into place.
- Finally, check that the unit is securely attached in the installation location.

4.3 Connections

Camera

You can connect a video source to the VIP X1 XF. Any cameras and other video sources that produce a standard PAL or NTSC signal are suitable.

1. Connect the camera or another video source to the BNC **VIDEO IN** socket using a video cable (75 Ohm, BNC plug).
2. If the video signal is not looped through, termination is performed by a software setting if necessary (see *Section 5.17 Advanced Mode: Video Input, page 43*).

Audio Connection

The VIP X1 XF has an audio port for audio line signals (input and output, both mono).
The audio signals are transmitted two-way and in sync with the video signals. As a result, you can connect a speaker or door intercom system at the destination point, for example. The following specifications should be complied with in all cases.

1 × **LINE IN**:	Impedance 9 kOhm typ., 5.5 V_{p-p} max. input voltage
1 × **LINE OUT**:	Impedance 16 Ohm min., 3 V_{p-p} max. output voltage

The stereo plug must be connected as follows:

Contact	**Function**
Tip	Line Out
Middle ring	Line In
Lower ring	Ground

▶ Connect an audio source with line level to the LINE IN/OUT socket of the VIP X1 XF with a 3.5 mm stereo plug.

Network

You can connect the VIP X1 XF to a 10/100 Base-T network using a standard UTP category 5 cable with RJ45 plugs.

▶ Connect the VIP X1 XF to the network via the **ETH** socket.

SD Slot

You can insert an SD card into the **SD CARD** slot to enable recordings to be saved locally. SD cards are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions.

NOTICE!
The release letter for the current firmware version includes a list of compatible SD cards.

Playing back recordings is also possible using a different VIP X1 XF.

CAUTION!
If the card is formatted, all existing data is deleted from the card.
You should therefore check whether the SD card contains any data that needs to be backed up before it is inserted.

1. Carefully slide the SD card into the slot as far as it will go, until it locks into place.
2. To remove the SD card, push carefully in the direction of insertion until the mechanical catch releases and then remove the card.

Data Interface

The bidirectional data interface is used to control units connected to the VIP X1 XF, such as a dome camera with a motorized lens. The connection supports the RS-232, RS-422 and RS-485 transmission standards.

The VIP X1 XF offers the serial interface via the orange terminal block (see *Section 8.8 Terminal Block, page 110*).

The range of controllable equipment is expanding constantly. The manufacturers of the relevant equipment provide specific information on installation and control.

CAUTION!

Please take note of the appropriate documentation when installing and operating the unit to be controlled.

The documentation contains important safety instructions and information about permitted uses.

NOTICE!

A video connection is necessary to transmit transparent data.

Alarm Inputs

The VIP X1 XF has two alarm inputs on the orange terminal block (see *Section 8.8 Terminal Block, page 110*). The alarm inputs are used to connect to external alarm devices such as door contacts or sensors. With the appropriate configuration, an alarm sensor can automatically connect the VIP X1 XF to a remote location, for example.

A zero potential closing contact or switch can be used as the actuator.

NOTICE!

If possible, use a bounce-free contact system as the actuator.

▶ Connect the lines to the appropriate terminals on the orange terminal block (**IN1** and **IN2**) and check that the connection is secure.

Relay Outputs

The VIP X1 XF has two relay outputs for switching external units such as lamps or alarm sirens. You can operate these relay outputs manually while there is an active connection to the VIP X1 XF. The outputs can also be configured to automatically activate sirens or other alarm units in response to an alarm signal. The relay outputs are also located on the orange terminal block (see *Section 8.8 Terminal Block, page 110*).

CAUTION!

A maximum load of 30 V_{p-p} and 200 mA (SELV) may be applied to the relay contacts.

▶ Connect the lines to the appropriate terminals on the orange terminal block (**R1** and **R2**) and check that the connection is secure.

4.4 Power On/Power Off

Power Supply

The VIP X1 XF does not have a power switch. Power is supplied via a separate unit. Connect the VIP X1 XF to the power supply unit and plug this into the mains. The unit is now ready for use. The VIP X1 XF does not come supplied with a power supply unit.

CAUTION!

Use only power supply units with UL approval and a power output according to LPS or NEC Class 2.

Where necessary, use suitable equipment to ensure that the power supply is free from interference such as voltage surges, spikes or voltage drops.

Do not connect the VIP X1 XF to the power supply until all other connections have been made.

1. Plug the terminal block with the PSU cable connected to it into the orange socket on the VIP X1 XF.
2. Connect the power supply unit to the mains. The VIP X1 XF is ready for use as soon as the **POWER** LED changes from a red light, indicating the start-up procedure, to a green light.

Provided the network connection has been correctly made, the green **ETH** LED also lights up. The lit orange **ETH** LED signals that data packets are being transmitted via the network.

4.5 Setup Using Configuration Manager

The **Configuration Manager** program can be found on the product CD contained in the scope of delivery. This program allows you to implement and set up new video servers in the network quickly and conveniently.

NOTICE!

Using Configuration Manager to set all parameters in the VIP X1 XF is an alternative to configuration by means of a Web browser, as described in chapter 5 of this manual.

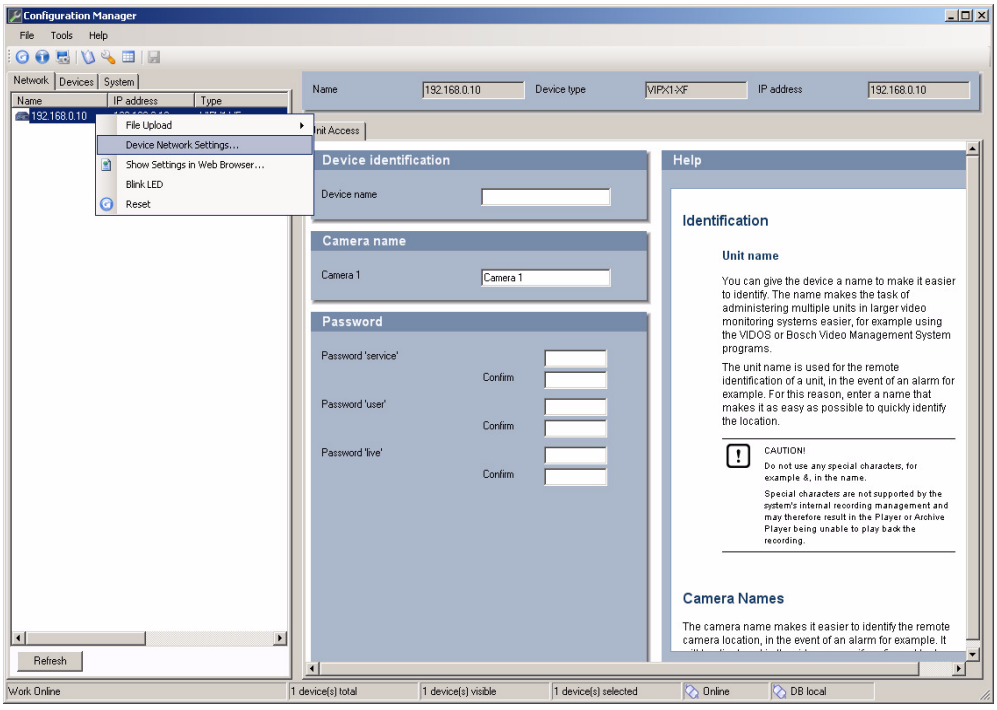
Installing the Program

1. Insert the CD into the computer's CD-ROM drive.
2. If the CD does not start automatically, open the **Configuration Manager** directory using Windows Explorer and double-click **Setup.exe**.
3. Follow the on-screen instructions.

Configuring the VIP X1 XF

You can start Configuration Manager immediately after installation.

1. Double-click the icon on the desktop or start the program via the Start menu. After the program has started, the network is immediately searched for compatible video servers.



2. You can start the configuration if a VIP X1 XF is shown in the list in the left section of the window. To do this, right-click the entry for the unit.
3. Click **Device Network Settings...** in the popup menu.
4. In the **Device IP address** field, enter a valid IP address to operate on your network (for example **192.168.0.10**) and click **OK**. The unit reboots and the IP address is valid.
5. If required, enter an appropriate subnet mask for the IP address, and additional network data.

NOTICE!
You must reboot to activate the new IP address, a new subnet mask or a gateway IP address.

Reboot

You can trigger the reboot directly with the assistance of Configuration Manager.

▶ Right-click the entry for the unit in the list in the left section of the window and select the **Reset** command from the context menu.

Additional Parameters

You can check and set additional parameters with the assistance of Configuration Manager. You can find detailed information on this in the documentation for this program.

5 Configuration Using a Web Browser

5.1 Connecting

The integrated HTTP server in the VIP X1 XF provides you with the option to configure the unit over the network with a Web browser. This option is an alternative to configuration using the Configuration Manager program and is considerably richer in function and more convenient than configuration using the terminal program.

System Requirements

- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 7.0 or higher)
- Screen resolution at least 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).
The Web browser must be configured to enable Cookies to be set from the IP address of the unit.
In Windows Vista, deactivate protected mode on the **Security** tab under **Internet Options**.
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

Installing MPEG ActiveX

Suitable MPEG ActiveX software must be installed on the computer to allow the live video images to be played back. If necessary, you can install the program from the product CD supplied.

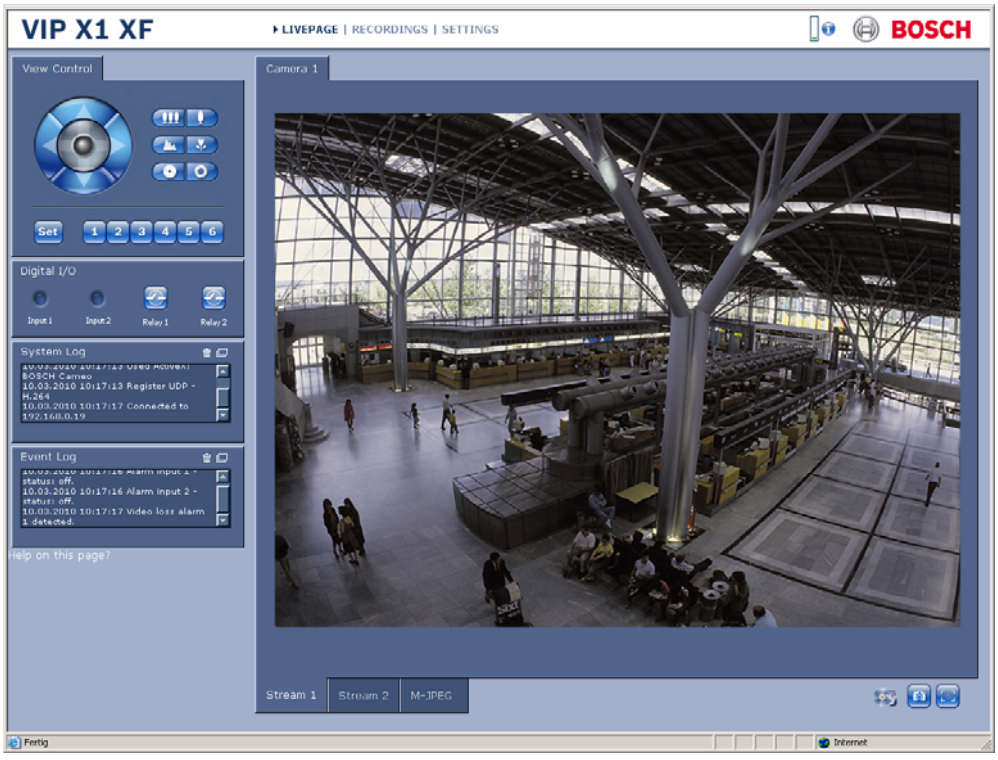
1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

Establishing the Connection

Before you can operate the VIP X1 XF within your network, it must have a valid IP address for your network and a compatible subnet mask.

The following default address is preset at the factory: **192.168.0.1**

1. Start the Web browser.
2. Enter the IP address of the VIP X1 XF as the URL. The connection is established and after a short time you will see the **LIVEPAGE** with the video image.



Maximum Number of Connections

If you do not connect, the unit may have reached its maximum number of connections. Depending on the unit and network configuration, each VIP X1 XF can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

Protected VIP X1 XF

If the VIP X1 XF is password protected against unauthorized access, the Web browser displays a corresponding message and prompts you to enter the password when you attempt to access protected areas.

NOTICE!

The VIP X1 XF offers the option to limit the extent of access using various authorization levels (see *Section 5.11 Advanced Mode: Password, page 34*).

1. Enter the user name and associated password in the corresponding text fields.
2. Click **OK**. If the password is entered correctly, the Web browser displays the page that was called up.

Protected Network

If a RADIUS server is employed in the network for managing access rights (802.1x authentication), the VIP X1 XF must be configured accordingly, otherwise no communication is possible.

To configure the unit, you must connect the VIP X1 XF directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated (see *Section Authentication, page 83*).

5.2 Configuration Menu

The **SETTINGS** page provides access to the configuration menu, which contains all the unit's parameters arranged in groups. You can view the current settings by opening one of the configuration screens. You can change the settings by entering new values or by selecting a predefined value from a list field.

There are two options for configuring the unit or checking the current settings:

– Basic Mode
– Advanced Mode

In **Basic Mode** the most important parameters are arranged in seven groups. This allows you to change the basic settings with just a few entries and then put the device into operation.

Advanced Mode is recommended for expert users or system support personnel. You can access all device parameters in this mode. Settings that affect the fundamental functionality of the device (such as firmware updates) can only be altered in Advanced Mode.

All parameter groups are described in this chapter in the order in which they are listed in the configuration menu, from the top of the screen to the bottom.

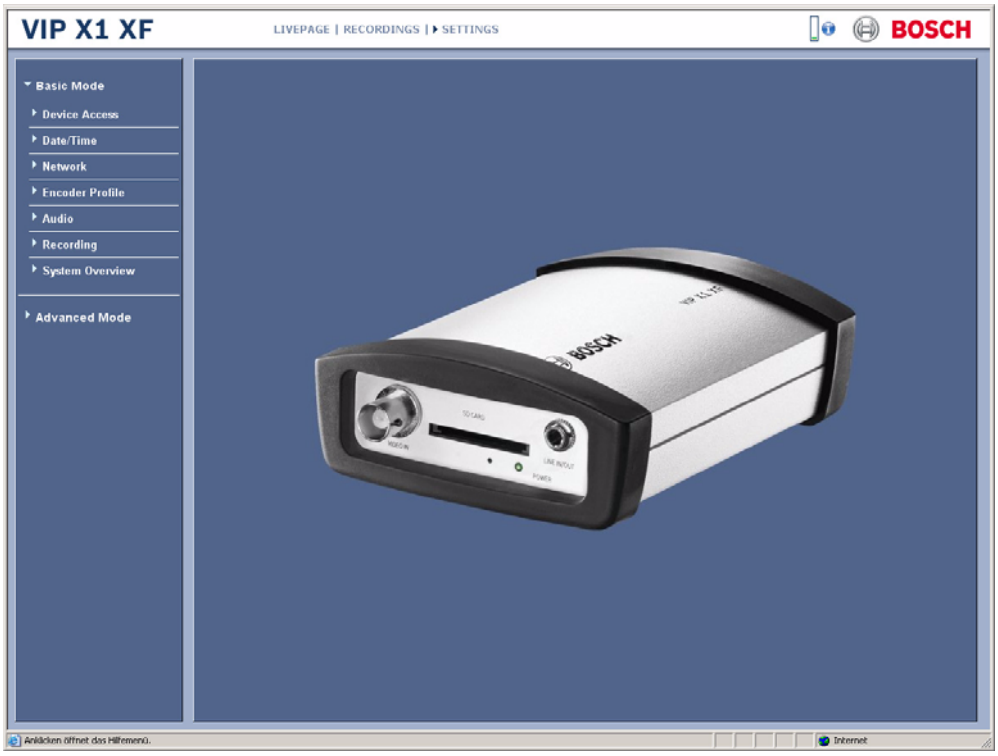
CAUTION!

The settings in the advanced mode should only be processed or modified by expert users or system support personnel.

All settings are backed up in the VIP X1 XF memory so they are not lost even if the power fails. The exception is the time settings, which are lost after 72 hours without power if no central time server is selected (see *Section 5.4 Basic Mode: Date/Time, page 27*).

Starting Configuration

▶ Click the **SETTINGS** link in the upper section of the window. The Web browser opens a new page with the configuration menu.



Navigation

1. Click one of the menu items in the left window margin. The corresponding submenu is displayed.
2. Click one of the entries in the submenu. The Web browser opens the corresponding page.

Making Changes

Each configuration screen shows the current settings. You can change the settings by entering new values or by selecting a predefined value from a list field.

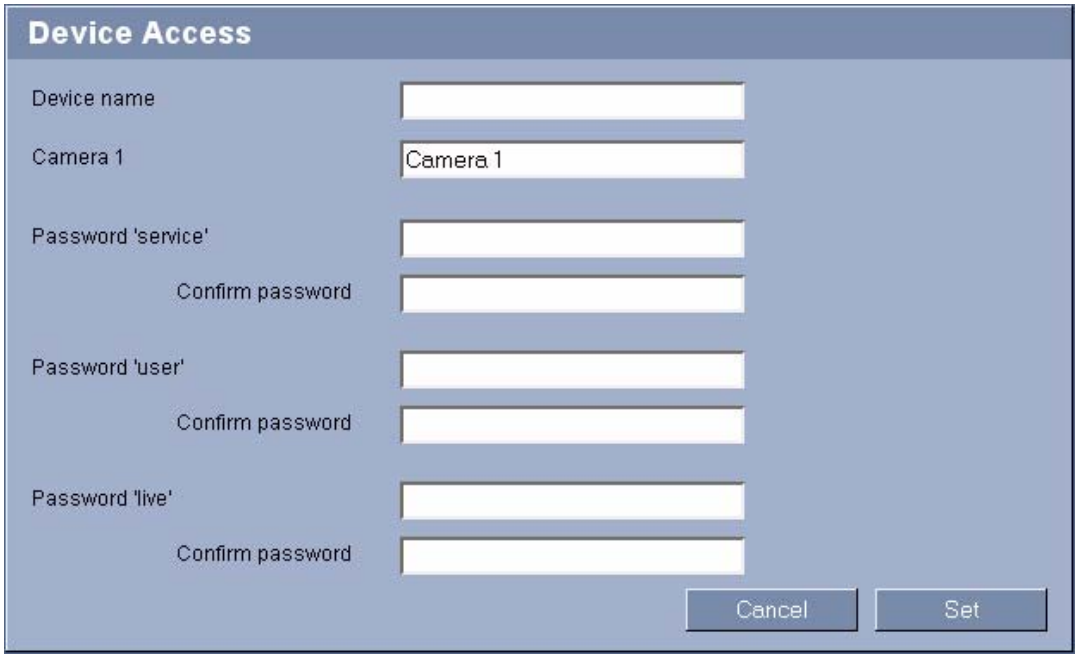
▶ After each change, click **Set** to save the change.

CAUTION!

Save each change with the associated **Set** button.

Clicking the **Set** button saves the settings only in the current field. Changes in any other fields are ignored.

5.3 Basic Mode: Device Access



Device name

You can give the VIP X1 XF a name to make it easier to identify. The name makes the task of administering multiple units in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.

The device name is used for the remote identification of a unit, in the event of an alarm for example. For this reason, enter a name that makes it as easy as possible to quickly identify the location.

CAUTION!

Do not use any special characters, for example **&**, in the name.

Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player programs being unable to play back the recording.

Camera 1

The camera name makes it easier to identify the remote camera location, in the event of an alarm for example. It will be displayed in the video screen if configured to do so (see *Section Camera name stamping, page 37*). The camera name makes the task of administering cameras in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.

Enter a unique, unambiguous name for the camera in this field.

CAUTION!

Do not use any special characters, for example **&**, in the name.

Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player programs being unable to play back the recording.

Password

A VIP X1 XF is generally protected by a password to prevent unauthorized access to the unit. You can use different authorization levels to limit access.

The VIP X1 XF operates with three authorization levels: **service**, **user** and **live**.

The highest authorization level is **service**. After entering the correct password, you can access all the functions of the VIP X1 XF and change all configuration settings.

With the **user** authorization level, you can operate the unit, play back recordings and also control cameras, for example, but you cannot change the configuration.

The lowest authorization level is **live**. It can only be used to view the live video image and switch between the different live image displays.

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.

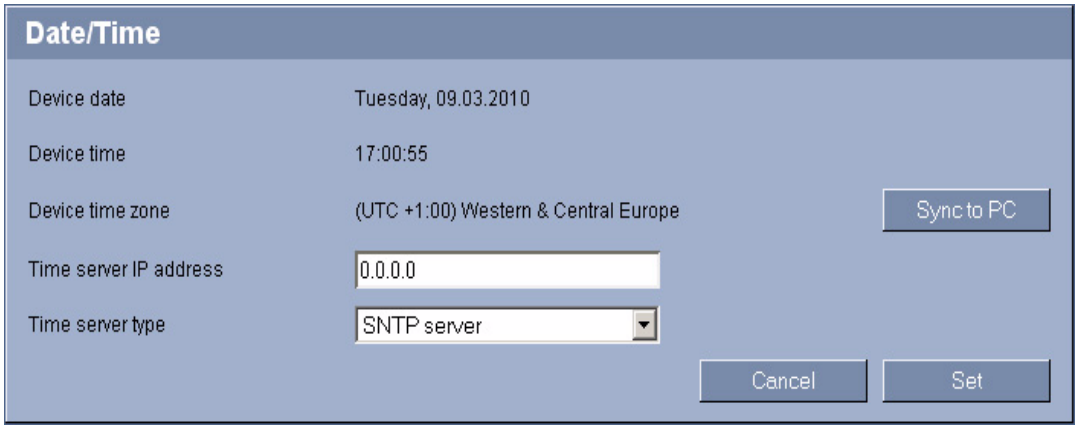
NOTICE!

Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. If a **live** password is assigned, for example, a **service** and a **user** password must also be set. When assigning passwords, you should therefore always start from the highest authorization level, **service**, and use different passwords.

Confirm password

In each case, enter the new password a second time to eliminate typing mistakes.

5.4 Basic Mode: Date/Time



Device date / Device time / Device time zone

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 units are operating on the same time. If necessary, you can synchronize the unit with your computer's system settings.

▶ Click the **Sync to PC** button to copy your computer's system time to the VIP X1 XF.

Time server IP address

The VIP X1 XF can receive the time signal from a time server using various time server protocols, and then use it to set the internal clock. The unit polls the time signal automatically once every minute.

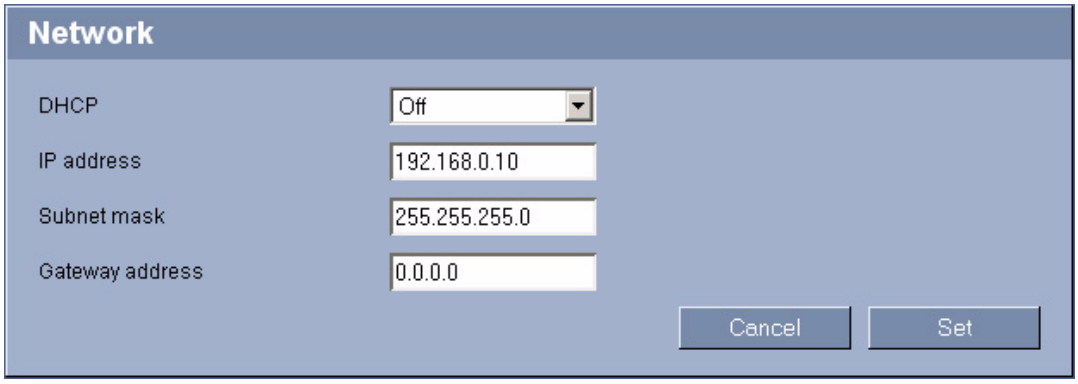
▶ Enter the IP address of a time server here.

Time server type

Select the protocol that is supported by the selected time server. Preferably, you should select the **SNTP server** as the protocol. This supports a high level of accuracy and is required for special applications and subsequent function extensions.

Select **Time server** for a time server that works with the protocol RFC 868.

5.5 Basic Mode: Network



The settings on this page are used to integrate the VIP X1 XF into an existing network.
Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.
2. Click the **Set and Reboot** button. The VIP X1 XF is rebooted and the changed settings are activated.

CAUTION!
If you change the IP address, subnet mask or gateway address, the VIP X1 XF is only available under the new addresses after the reboot.

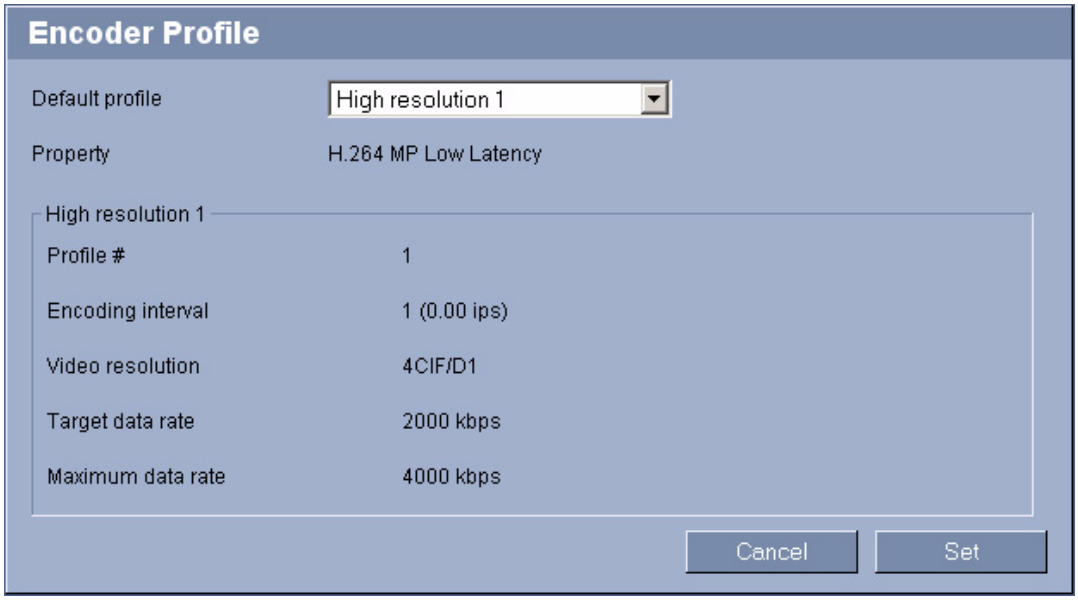
DHCP
If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the VIP X1 XF.
Certain applications (VIDOS, Bosch Video Management System, Archive Player, Configuration Manager) use the IP address for the unique assignment of the unit. If you use these 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 VIP X1 XF in this field. The IP address must be valid for the network.

Subnet mask
Enter the appropriate subnet mask for the selected IP address here.

Gateway address
If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise leave the box blank (**0.0.0.0**).

5.6 Basic Mode: Encoder Profile



Default profile

You can select a profile for encoding the video signal.

You can use this to adapt the video data transmission to the operating environment (for example network structure, bandwidth, data load).

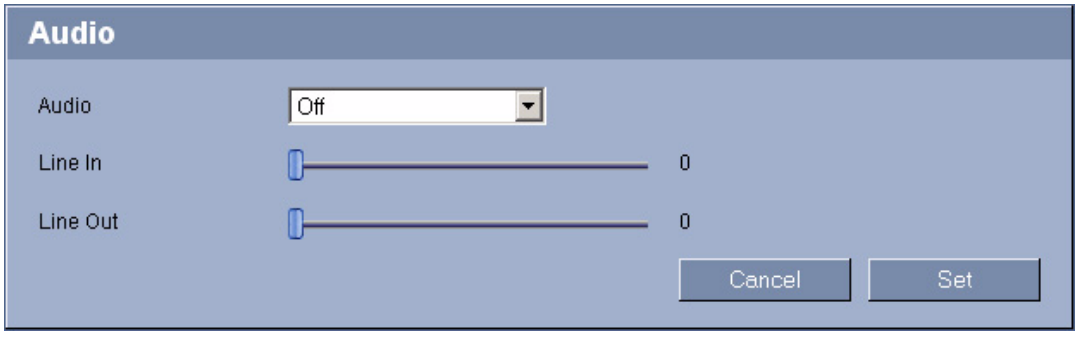
Pre-programmed profiles are available, each giving priority to different perspectives. When selecting a profile, details are displayed in the list field. Below is a brief description of the factory default settings for the encoder profiles.

NOTICE!

The names and the technical details for the encoder profiles depend on the configuration of the device.

- **High resolution 1**
  High quality, connections with the highest bandwidth, resolution 704 × 576/480 pixels
- **High resolution 2**
  High quality, connections with high bandwidth, resolution 704 × 576/480 pixels
- **Low bandwidth**
  High resolution, connections with low bandwidth, resolution 704 × 576/480 pixels
- **DSL**
  DSL connections with 500 kbps, resolution 352 × 288/240 pixels
- **ISDN (2B)**
  ISDN connections via two B-channels, resolution 352 × 288/240 pixels
- **ISDN (1B)**
  ISDN connections via one B-channel, resolution 352 × 288/240 pixels
- **MODEM**
  Analog modem connections with 20 kbps, resolution 352 × 288/240 pixels
- **GSM**
  GSM connections with 9,600 baud, resolution 352 × 288/240 pixels

5.7 Basic Mode: Audio



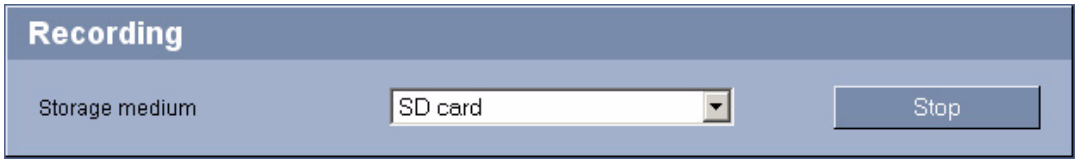
You can set the gain of the audio signals to suit your specific requirements. Your changes are effective immediately.
If you connect via Web browser, you must activate the audio transmission on the **LIVEPAGE Functions** page (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*). For other connections, the transmission depends on the audio settings of the respective system.

Audio
The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approx. 80 kbps for each connection. If you do not want any audio data to be transmitted, select **Off**.

Line In
You can set the line input gain.

Line Out
You can set the line output gain.

5.8 Basic Mode: Recording

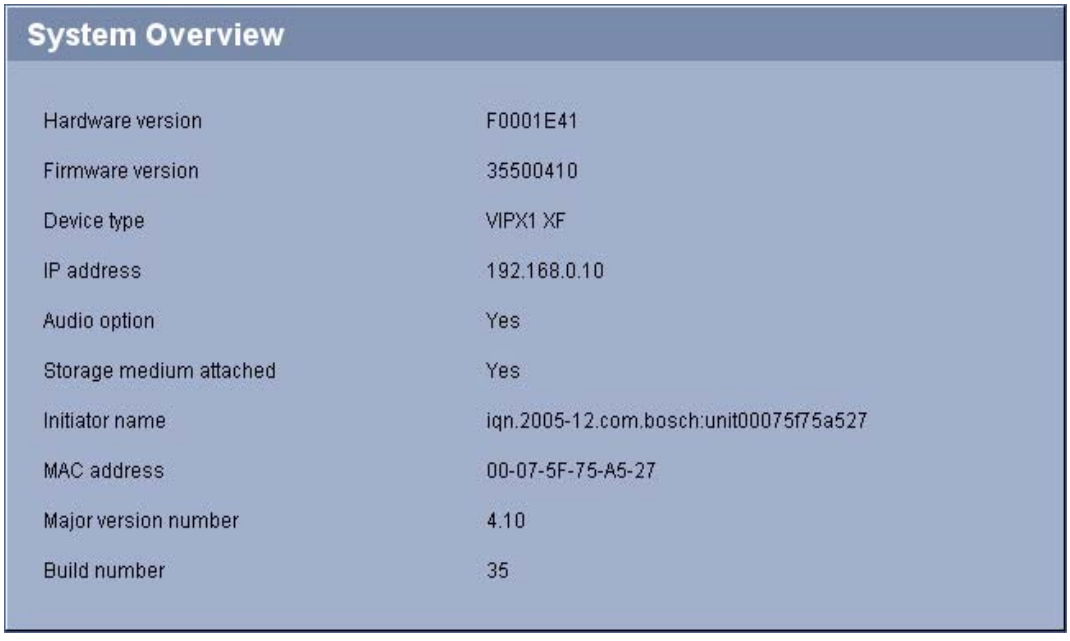


You can record the images from the camera connected to the VIP X1 XF on the local SD card or on an appropriately configured iSCSI system.
SD cards (see *Section SD Slot, page 17*) are the ideal solution for shorter storage times.
For long-term, authoritative images, it is essential that you use an appropriately sized iSCSI system.
Here you can select a storage medium and immediately start or stop the recording.

Storage medium

1. Select the required storage medium from the list.
2. Click the **Start** button to start the recording immediately.

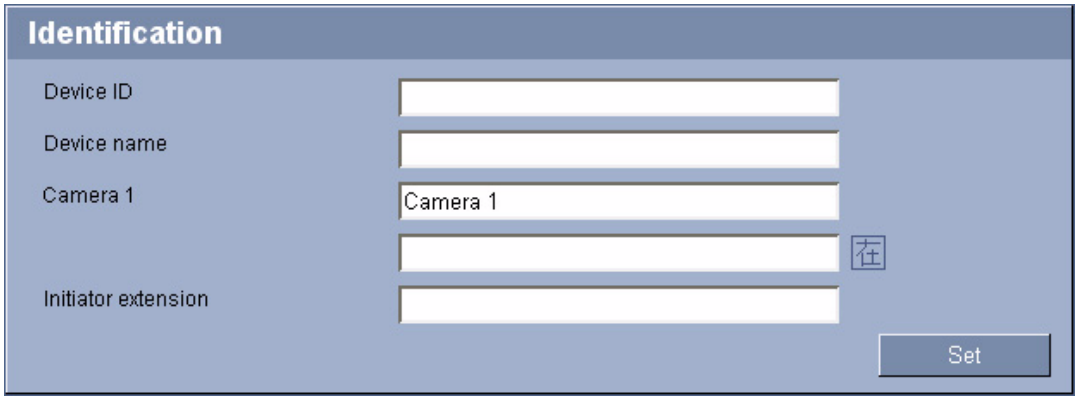
5.9 Basic Mode: System Overview



The data on this page are for information purposes only and cannot be changed. Keep a record of these numbers in case technical assistance is required.

NOTICE!
You can select all required text on this page with the mouse and copy it to the clipboard with the [Ctrl]+[C] key combination, for example if you want to send it via e-mail.

5.10 Advanced Mode: Identification



Device ID
Each VIP X1 XF should be assigned a unique identifier that you can enter here as an additional means of identification.

Device name
You can give the VIP X1 XF a name to make it easier to identify. The name makes the task of administering multiple units in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.
The device name is used for the remote identification of a unit, in the event of an alarm for example. For this reason, enter a name that makes it as easy as possible to quickly identify the location.

CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player programs being unable to play back the recording.

Camera 1
The camera name makes it easier to identify the remote camera location, in the event of an alarm for example. It will be displayed in the video screen if configured to do so (see *Section Camera name stamping, page 37*). The camera name makes the task of administering cameras in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.
Enter a unique, unambiguous name for the camera in this field. You can use both lines for this.

CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player programs being unable to play back the recording.

You can use the second line for entering additional characters; these can be selected from a table.

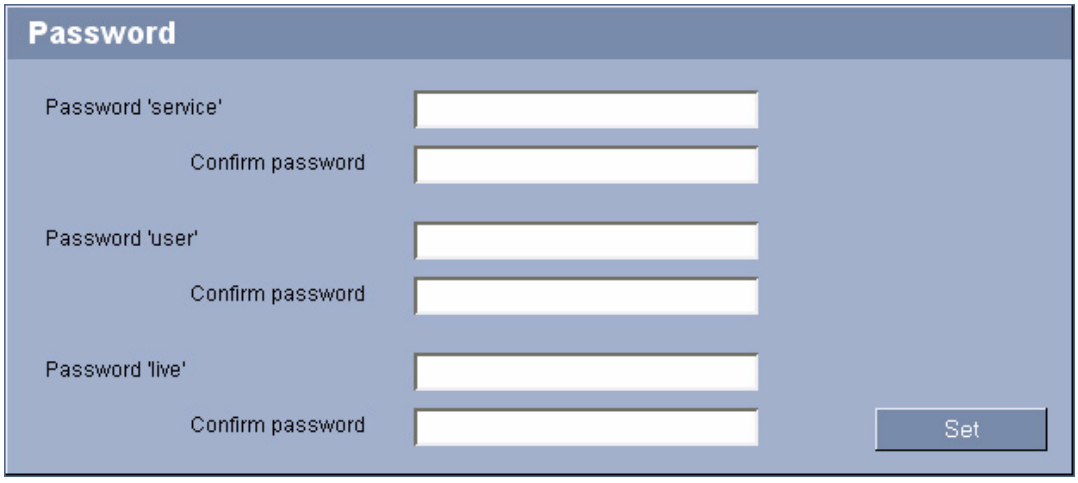
1. Click the icon next to the second line. A new window with the character map is opened.
2. Click the required character. The character is inserted into the **Result** field.
3. In the character map, click the **<<** and **>>** icons to move between the different pages of the table, or select a page from the list field.

4. Click the **<** icon to the right of the **Result** field to delete the last character, or click the **X** icon to delete all characters.
5. Now click the **OK** button to apply the selected characters to the second line of the **Camera 1** parameters. The window will close.

Initiator extension

You can attach your own text to the initiator name of the VIP X1 XF to make the unit easier to identify 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 (see *Section 5.9 Basic Mode: System Overview, page 31*).

5.11 Advanced Mode: Password



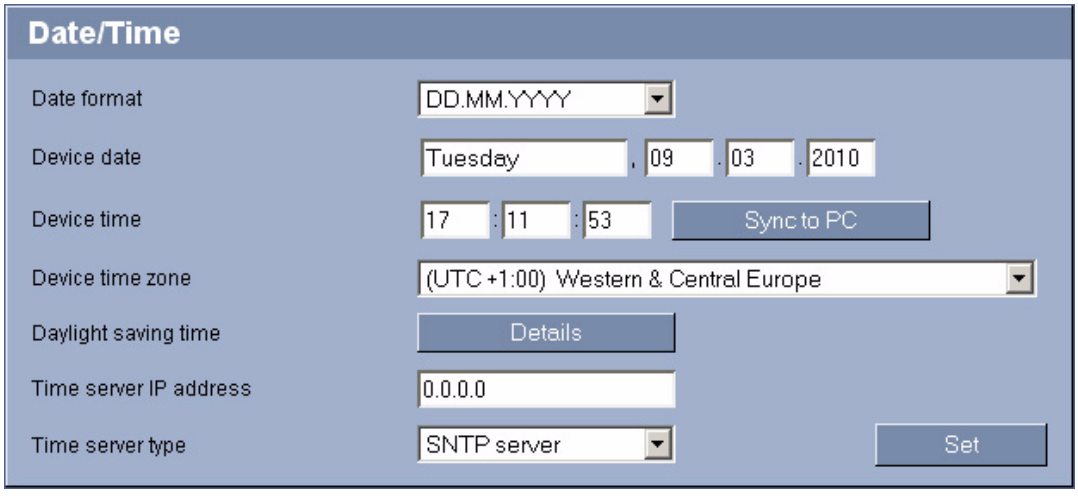
A VIP X1 XF is generally protected by a password to prevent unauthorized access to the unit. You can use different authorization levels to limit access.

NOTICE!
Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. If a **live** password is assigned, for example, a **service** and a **user** password must also be set. When assigning passwords, you should therefore always start from the highest authorization level, **service**, and use different passwords.

Password
The VIP X1 XF operates with three authorization levels: **service**, **user** and **live**.
The highest authorization level is **service**. After entering the correct password, you can access all the functions of the VIP X1 XF and change all configuration settings.
With the **user** authorization level, you can operate the unit, play back recordings and also control cameras, for example, but you cannot change the configuration.
The lowest authorization level is **live**. It can only be used to view the live video image and switch between the different live image displays.
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.

Confirm password
In each case, enter the new password a second time to eliminate typing mistakes.

5.12 Advanced Mode: Date/Time



Date format
Select your required date format.

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

1. Enter the current date. Since the unit time is controlled by the internal clock, there is no need to enter the day of the week – it is added automatically.
2. Enter the current time or click the **Sync to PC** button to copy your computer's system time to the VIP X1 XF.

Device time zone
Select the time zone in which your system is located.

Daylight saving time
The internal clock can switch automatically between normal and daylight saving time (DST). The unit already contains the data for DST switch-overs up to the year 2018. You can use these data or create alternative time saving data if required.

NOTICE!
If you do not create a table, there will be no automatic switching. When changing and clearing individual entries, remember that two entries are usually related to each other and dependent on one another (switching to summer time and back to normal time).

1. First check whether the correct time zone is selected. If it is not correct, select the appropriate time zone for the system, and click the **Set** button.
2. Click the **Details** button. A new window will open and you will see the empty table.
3. Select the region or the city that is closest to the system's location from the list field below the table.
4. Click the **Generate** button to generate data and enter this into the table.
5. Make changes by clicking an entry in the table. The entry is selected.
6. Clicking the **Delete** button will remove the entry from the table.
7. Select other values from the list fields below the table to change the entry. Changes are made immediately.

8. If there are empty lines at the bottom of the table, for example after deletions, you can add new data by marking the row and selecting required values from the list fields.
9. Now click the **OK** button to save and activate the table.

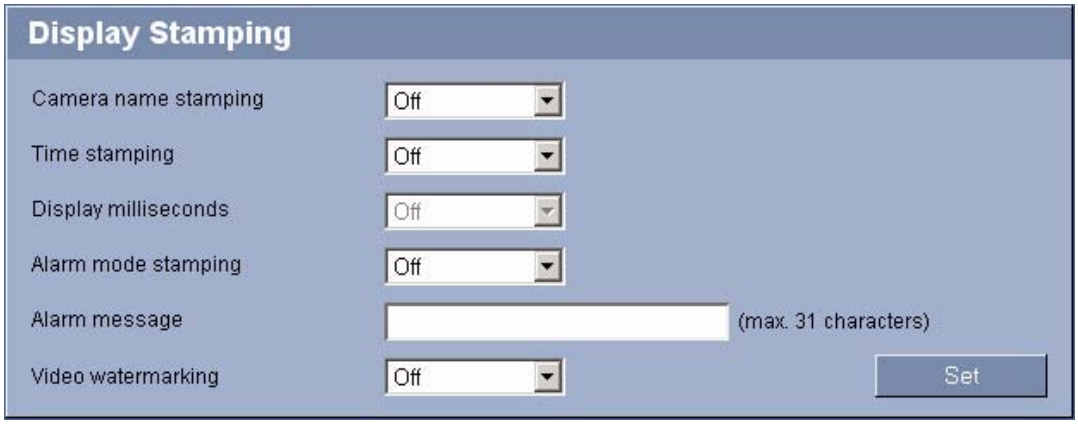
Time server IP address

The VIP X1 XF can receive the time signal from a time server using various time server protocols, and then use it to set the internal clock. The unit polls the time signal automatically once every minute.
Enter the IP address of a time server here.

Time server type

Select the protocol that is supported by the selected time server. Preferably, you should select the **SNTP server** as the protocol. This supports a high level of accuracy and is required for special applications and subsequent function extensions.
Select **Time server** for a time server that works with the protocol RFC 868.

5.13 Advanced Mode: Display Stamping



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

Camera name stamping

This field sets the position of the camera name overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

Time stamping

This field sets the position of the time overlay. It can be displayed at the **Top**, at the **Bottom** or at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

Display milliseconds

You can only select this option if the **Time stamping** function is activated. If necessary, you can also display milliseconds. This information can be useful for recorded video images; however, it does increase the processor's computing time. Select **Off** if you do not need to display milliseconds.

Alarm mode stamping

Select **On** to display a text message overlay in the event of an alarm. It can be displayed at a position of your choice that you can then specify using the **Custom** option. Or it can be set to **Off** for no overlay information.

1. Select the desired option from the list.
2. If you select the **Custom** option, additional fields are displayed where you can specify the exact position (**Position (XY)**).
3. In the **Position (XY)** fields, enter the values for the desired position.

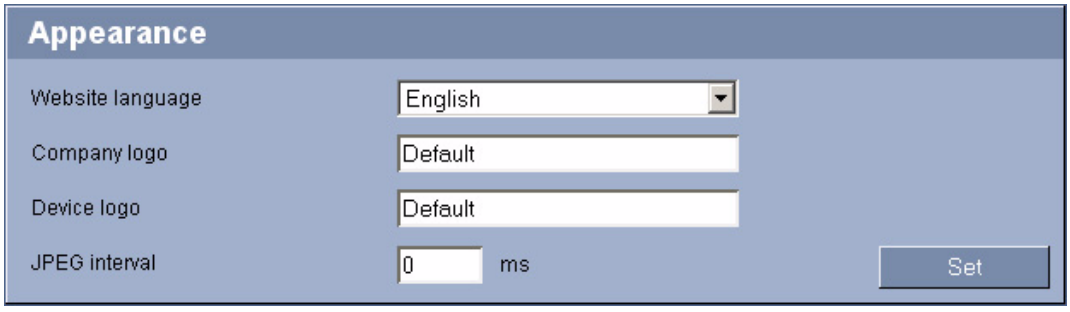
Alarm message

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

Video watermarking

Choose **On** if you wish the transmitted video images to be "watermarked". After activation, all images are marked with a green **W**. A red **W** indicates that the sequence (live or saved) has been manipulated.

5.14 Advanced Mode: Appearance



On this page you can adapt the appearance of the web interface and change the website language to meet your requirements. If necessary, you can replace the manufacturer's logo (top right) and the product name (top left) in the top part of the window with individual graphics.

NOTICE!
You can use either GIF or JPEG images. The file paths must correspond to the access mode (for example **C:\Images\Logo.gif** for access to local files, or **http://www.mycompany.com/images/logo.gif** for access via the Internet/Intranet). When accessing via the Internet/Intranet, ensure that a connection is always available to display the image. The image file is not stored in the VIP X1 XF.

Website language
Select the language for the user interface here.

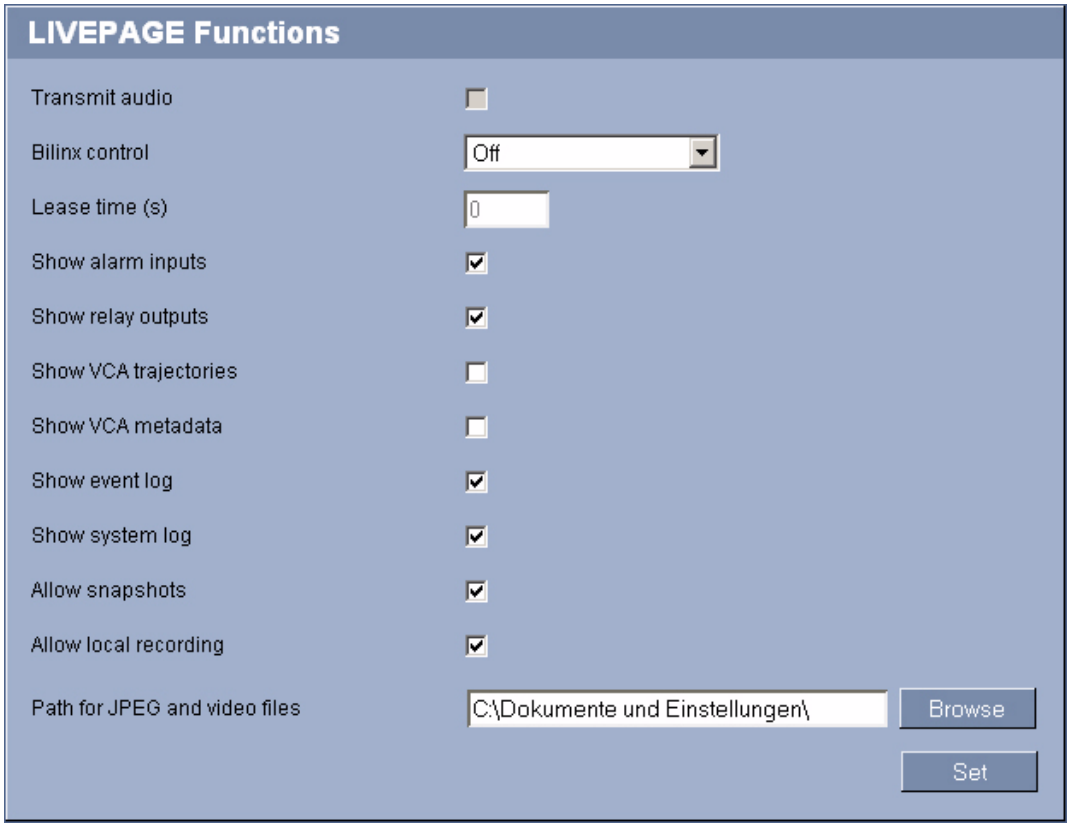
Company logo
Enter the path to a suitable graphic if you want to replace the manufacturer's logo. The image file can be stored on a local computer, in the local network or at an Internet address.

Device logo
Enter the path to a suitable graphic if you want to replace the product name. The image file can be stored on a local computer, in the local network or at an Internet address.

NOTICE!
If you want to use the original graphics again, simply delete the entries in the **Company logo** and **Device logo** fields.

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

5.15 Advanced Mode: LIVEPAGE Functions



On this page you can adapt the **LIVEPAGE** functions to your requirements. You can choose from a variety of different options for displaying information and controls.

1. Check the box for the items that are to be made available on the **LIVEPAGE**. The selected items are indicated by a check mark.
2. Check whether the required functions are available on the **LIVEPAGE**.

Transmit audio

You can only select this option if audio transmission is actually switched on (see *Section Audio, page 50*).

The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approx. 80 kbps for each connection.

Bilinx control

Next to the field for view control at the top left of the **LIVEPAGE**, an additional field is displayed for the special Bosch Security Systems Bilinx control.

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 enabled.

Show alarm inputs

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

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

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 (see *Section 5.31 Advanced Mode: VCA Event triggered, page 70*).

Show VCA metadata
When the analysis function is activated, the additional information from the video content analysis (VCA) will be displayed in the live video image (see *Section 5.31 Advanced Mode: VCA Event triggered, page 70*). With the **MOTION+** analysis type, for example, the sensor fields in which motion is recorded will be marked with rectangles.

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

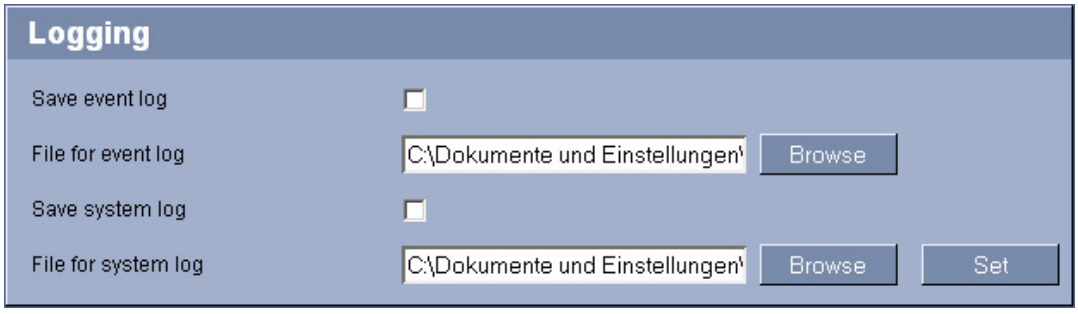
Show system log
The system messages are displayed along with the date and time in a field next to the video image and provide information about establishing and ending connections, for example.

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

Allow local recording
Here you can specify whether the icon for saving video sequences on the local memory should be displayed below the live image. Video sequences can only be saved if this icon is visible.

Path for JPEG and video files
1. Enter the path for the storage location of individual images and video sequences that you can save from the **LIVEPAGE**.
2. If necessary, click **Browse** to find a suitable directory.

5.16 Advanced Mode: Logging



Save event log

Check this option to save event messages in a text file on your local computer.
You can then view, edit and print this file with any text editor or the standard Office software.

File for event log

1. Enter the path for saving the event log here.
2. If necessary, click **Browse** to find a suitable directory.

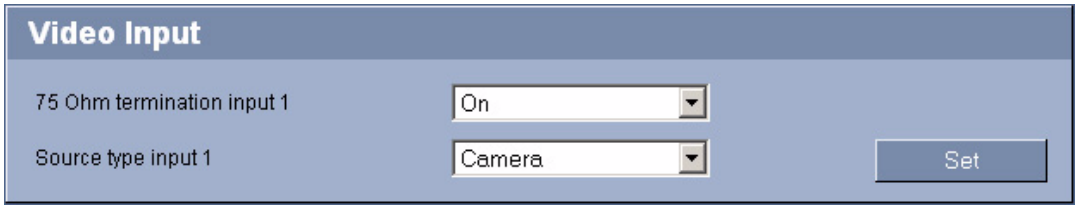
Save system log

Check this option to save system messages in a text file on your local computer.
You can then view, edit and print this file with any text editor or the standard Office software.

File for system log

1. Enter the path for saving the system log here.
2. If necessary, click **Browse** to find a suitable directory.

5.17 Advanced Mode: Video Input



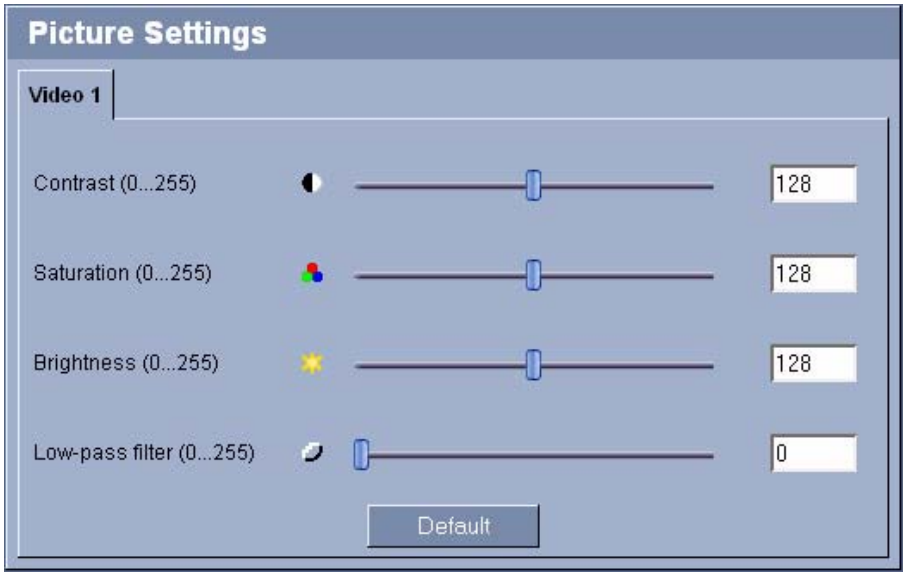
You can activate the 75 Ohm terminating resistance for the video input of the VIP X1 XF. The terminating resistance must be deactivated for the video signal to be looped through. Every video input is closed at the time of delivery.

75 Ohm termination
Select **Off** if the video signal is to be looped through.

Source type
To allow VCRs to be connected as a video source, you can change the characteristic of the video source from the preset value of **Camera** to **VCR**. VCRs require a more tolerant setting for the internal PLL as a result of jitter effects caused by the mechanical components of a VCR.

NOTICE!
In some cases, selecting the **VCR** option can lead to an improvement in the video image even with a camera connected.

5.18 Advanced Mode: Picture Settings



You can set the video image of the camera to suit your requirements. The current video image is displayed in the small window next to the slide controls as confirmation. Your changes are effective immediately.

1. Move the slide control to the required position.
2. Click **Default** to reset all settings to their default value.

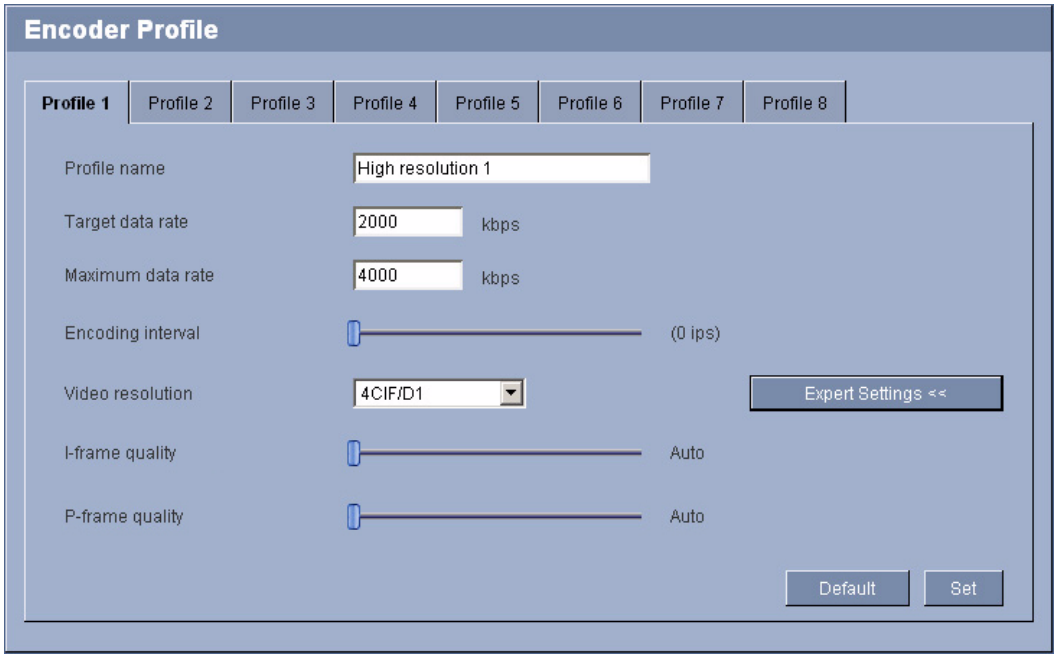
Contrast (0...255)
You can use this function to adapt the contrast of the video image to your working environment.

Saturation (0...255)
You can use this function to adjust the color saturation so as to make the reproduction of colors on your monitor as realistic as possible.

Brightness (0...255)
You can use this function to adapt the brightness of the video image to your working environment.

Low-pass filter (0...255)
You can use this function to filter very fine noise from the image. This reduces and optimizes the bandwidth necessary for image transmission over the network. The image resolution may be impaired.
The higher the value set with the slide control, the flatter the image signal. Check your setting in the image window next to the slide controls.
Also observe the processor load indicator that appears at the top of the window near the manufacturer's logo (see *Section 8.5 Processor Load, page 109*).

5.19 Advanced Mode: Encoder Profile



You can change the names and individual parameter values for the encoder profiles.
You can use this to adapt the video data transmission to the operating environment (for example network structure, bandwidth, data load).
Pre-programmed profiles are available, each giving priority to different perspectives. Below is a brief description of the factory default settings for the encoder profiles.

- **High resolution 1**
  High quality, connections with the highest bandwidth, resolution 704 × 576/480 pixels
- **High resolution 2**
  High quality, connections with high bandwidth, resolution 704 × 576/480 pixels
- **Low bandwidth**
  High resolution, connections with low bandwidth, resolution 704 × 576/480 pixels
- **DSL**
  DSL connections with 500 kbps, resolution 352 × 288/240 pixels
- **ISDN (2B)**
  ISDN connections via two B-channels, resolution 352 × 288/240 pixels
- **ISDN (1B)**
  ISDN connections via one B-channel, resolution 352 × 288/240 pixels
- **MODEM**
  Analog modem connections with 20 kbps, resolution 352 × 288/240 pixels
- **GSM**
  GSM connections with 9,600 baud, resolution 352 × 288/240 pixels

CAUTION!
Change the profiles only once you are fully familiar with all the configuration options. In the default setting, Stream 1 is transmitted for alarm connections and automatic connections. Bear this fact in mind when assigning the profile.

NOTICE!
All parameters combine to make up a profile and are dependent on one another. If you enter a setting that is outside the permitted range for a particular parameter, the nearest permitted value will be substituted when the settings are saved.

Profile name
You can enter a new name for the profile. The name is then displayed in the **Default profile** list field on the **Encoder Streams** page in the lists of selectable profiles.

Target data rate
You can limit the data rate for the VIP X1 XF to optimize utilization of the bandwidth in your network. 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 be temporarily exceeded up to the value you enter in the **Maximum data rate** field.

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

Encoding interval
The setting selected here determines the interval at which images are encoded and transmitted. The image rate in ips (images per second) is displayed next to the text field.

Video resolution
Here you can select the desired resolution for the video image. The following resolutions are available:
– **CIF**
  352 × 288/240 pixels
– **4CIF/D1**
  704 × 576/480 pixels

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

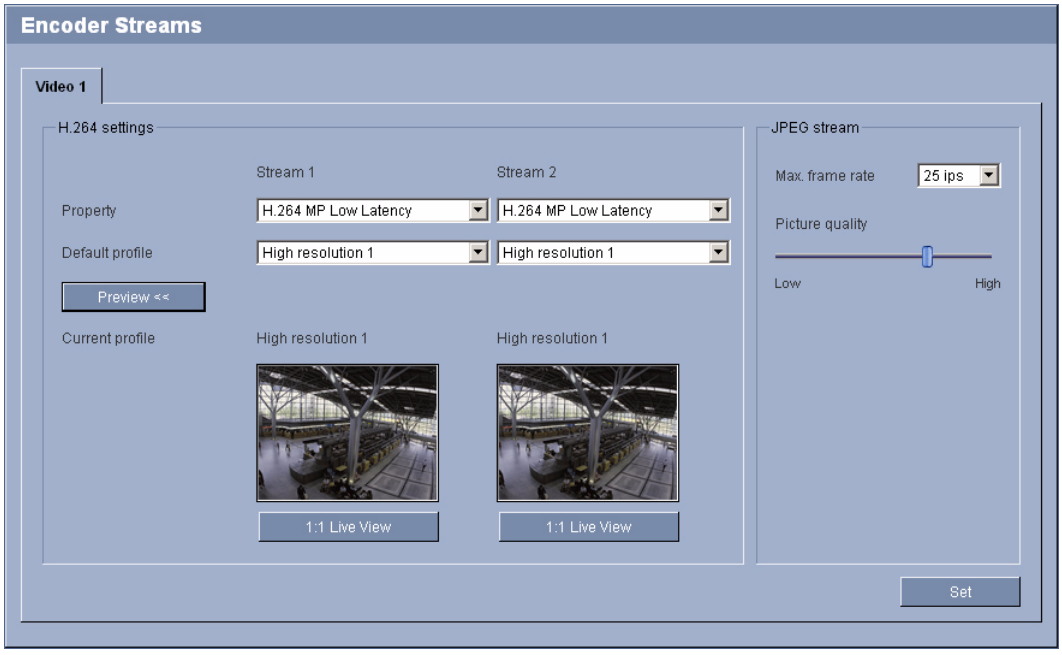
I-frame quality
This setting allows you to adjust the image quality of the I-frames. The basic setting **Auto** automatically adjusts the quality to the settings for the P-frame video quality. Alternatively, you can use the slide control to set a value between 9 and 51. The value **9** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **51** results in a very high refresh rate and lower image quality.

P-frame quality
This setting allows you to adjust the maximum image quality of the P-frames. The basic setting **Auto** automatically adjusts to the optimum combination of movement and image definition (focus). Alternatively, you can use the slide control to set a value between 9 and 51. The value **9** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **51** results in a very high refresh rate and lower image quality.

Default

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

5.20 Advanced Mode: Encoder Streams



The VIP X1 XF simultaneously generates two data streams (Dual Streaming); you can select the relevant property for these here and connect them to an encoder profile, for example one for transmissions to the Internet and one for LAN connections.
Two settings with different encoder properties are available:

– **H.264 BP+ (HW decoder)**
  Select this setting when using hardware decoders or the Divar XF digital video recorder.
  CABAC: off
  CAVLC: on
  GOP structure: IP
  I-frame distance: 15
  Deblocking filter: on

– **H.264 MP Low Latency**
  Select this setting when using software decoders, PTZ and for rapid movements in the images.
  CABAC: on
  CAVLC: off
  GOP structure: IP
  I-frame distance: 30
  Deblocking filter: on

1. Select the required encoder properties and one of the encoder profiles for each data stream.
2. Click the **Preview** button. The preview screens for both data streams are shown.
3. Click the **1:1 Live View** button below the preview screen to open a new window with the original data stream and to check the image quality and the transmission rate.

Property
Select the required encoder properties for the relevant data stream here.

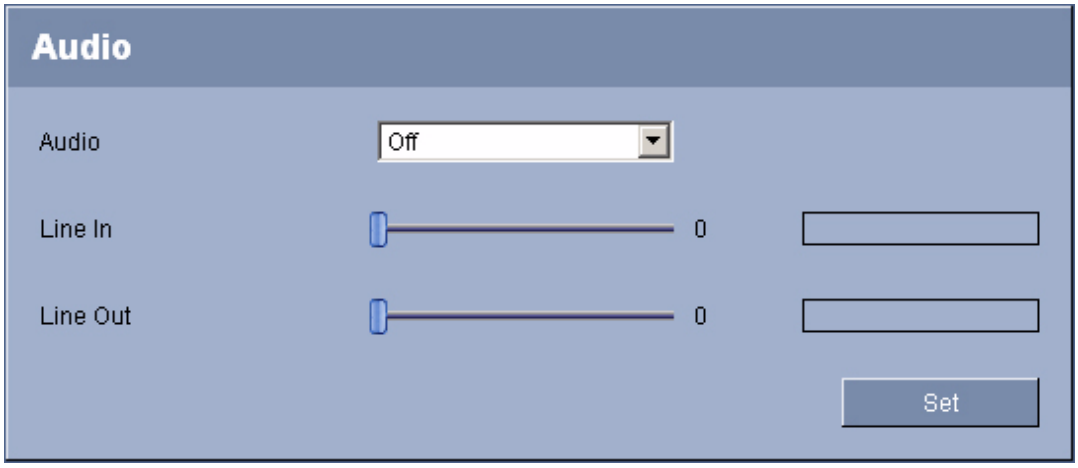
Default profile
Select the required encoder profile here. The properties of the profiles are defined on the **Encoder Profile** page (see *Section 5.19 Advanced Mode: Encoder Profile, page 45*).

JPEG stream
You can set up the separate JPEG stream in this area. These settings are independent of the H.264 settings. The resolution corresponds to the highest setting from the two data streams.

Max. frame rate
You can select the frame rate for transmitting the JPEG images.

Picture quality
This setting allows you to define the picture quality. Low quality requires a lower bandwidth in the network.

5.21 Advanced Mode: Audio



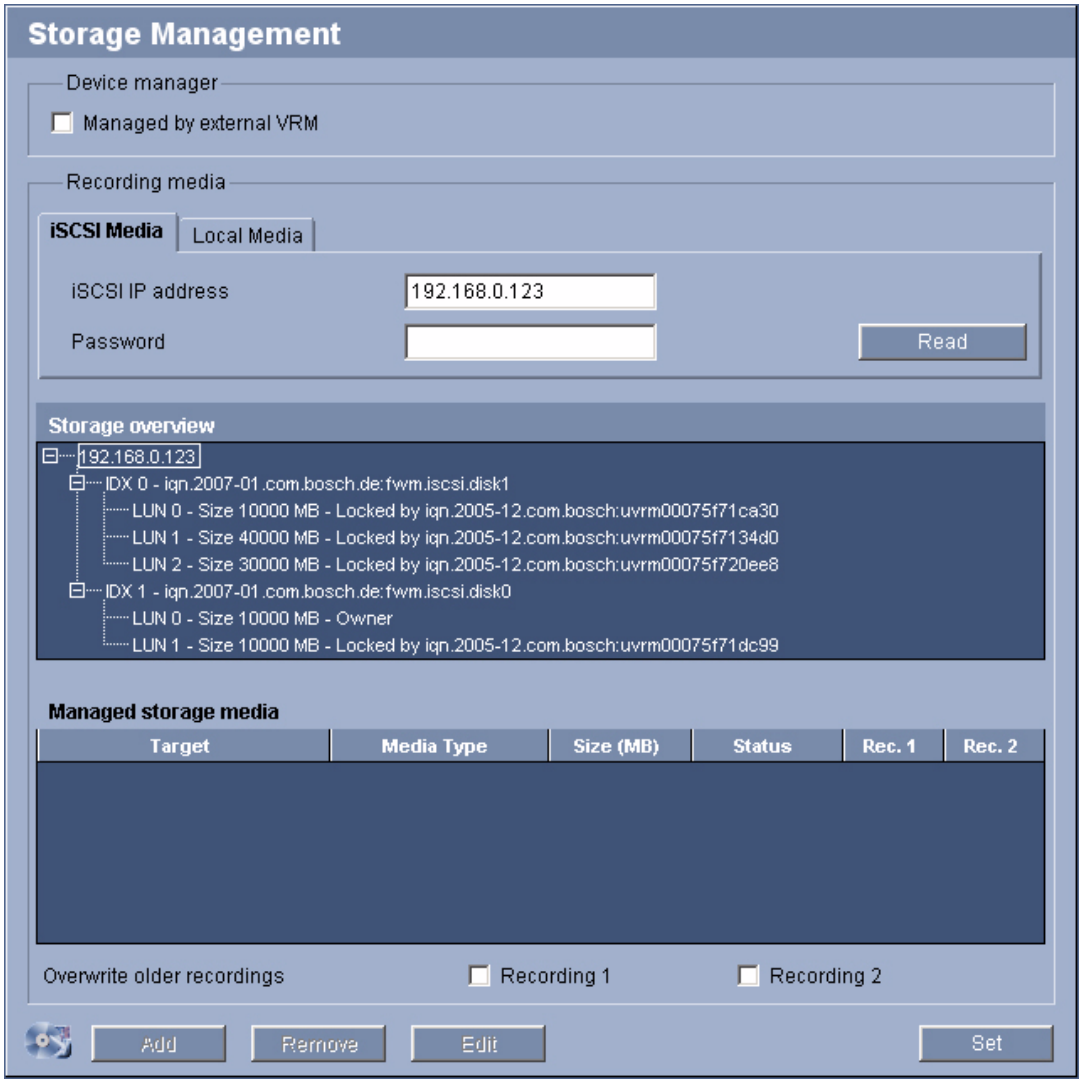
You can set the gain of the audio signals to suit your specific requirements. The current video image is shown in the small window next to the slide controls to help you check the audio source and improve assignments. Your changes are effective immediately.
If you connect via Web browser, you must activate the audio transmission on the **LIVEPAGE Functions** page (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*). For other connections, the transmission depends on the audio settings of the respective system.

Audio
The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approx. 80 kbps for each connection. If you do not want any audio data to be transmitted, select **Off**.

Line In
You can set the line input gain. Make sure that the display does not go beyond the green zone during modulation.

Line Out
You can set the line output gain. Make sure that the display does not go beyond the green zone during modulation.

5.22 Advanced Mode: Storage Management



You can record the images from the camera connected to the VIP X1 XF on the local SD card or on an appropriately configured iSCSI system.
SD cards (see *Section SD Slot, page 17*) are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions.
For long-term, authoritative images, it is essential that you use an appropriately sized iSCSI system.
It is also possible to let the VRM Video Recording Manager control all recording when accessing an iSCSI system. This is an external program for configuring recording tasks for video servers. For further information please contact your local customer service at Bosch Security Systems.

Device manager
If you activate the **VRM** option in this screen, the VRM Video Recording Manager will manage all recording and you will not be able to configure any further settings here.

CAUTION!
Activating or deactivating VRM causes the current settings to be lost; they can only be restored through reconfiguration.

Recording media
Select the required recording media here so that you can then activate them and configure the recording parameters.

iSCSI Media
If you want to use an **iSCSI system** as a recording medium, you must set up a connection to the required iSCSI system and set the configuration parameters.

NOTICE!
The iSCSI storage system selected must be available on the network and completely set up. Amongst other things, it must have an IP address and be divided into logical drives (LUN).

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 this into the **Password** field.
3. Click the **Read** button. The connection to the IP address will be established. In the **Storage overview** field, you can see the corresponding logical drives.

Local Media
The supported local recording media are displayed in the **Storage overview** field.

Activating and Configuring Storage Media
The storage overview displays the available storage media. You can select individual media or iSCSI drives and transfer these to the **Managed storage media** list. You can activate the storage media in this list and configure them for storage.

CAUTION!
Each storage medium can only be associated with one user. If a storage medium is already being used by another user, you can decouple the user and connect the drive with the VIP X1 XF. Before decoupling, make absolutely sure that the previous user no longer needs the storage medium.

1. In the **Recording media** section, click the **iSCSI Media** and **Local Media** tabs to display the applicable storage media in the overview.
2. In the **Storage overview** section, double-click the required storage medium, an iSCSI LUN or one of the other available drives. The medium is then added to the **Managed storage media** list. In the **Status** column, newly added media are indicated by the status **Not active**.
3. Click the **Set** button to activate all media in the **Managed storage media** list. In the **Status** column, these are indicated by the status **Online**.
4. Check the box in the **Rec. 1** or **Rec. 2** column to specify which data stream should be recorded on the storage media selected. **Rec. 1** stores Stream 1, **Rec. 2** stores Stream 2. This means that you can record the standard data stream on a hard drive and record alarm images on the local SD card, for example.
5. Check the boxes for the **Overwrite older recordings** option to specify which older recordings can be overwritten once the available memory capacity has been used. **Recording 1** corresponds to Stream 1, **Recording 2** corresponds to Stream 2.

CAUTION!
If older recordings are not allowed to be overwritten when the available memory capacity has been used, the recording in question will be stopped. You can specify limitations for overwriting old recordings by configuring the retention time (see *Section 5.24 Advanced Mode: Retention Time, page 56*).

Formatting Storage Media
You can delete all recordings on a storage medium at any time.

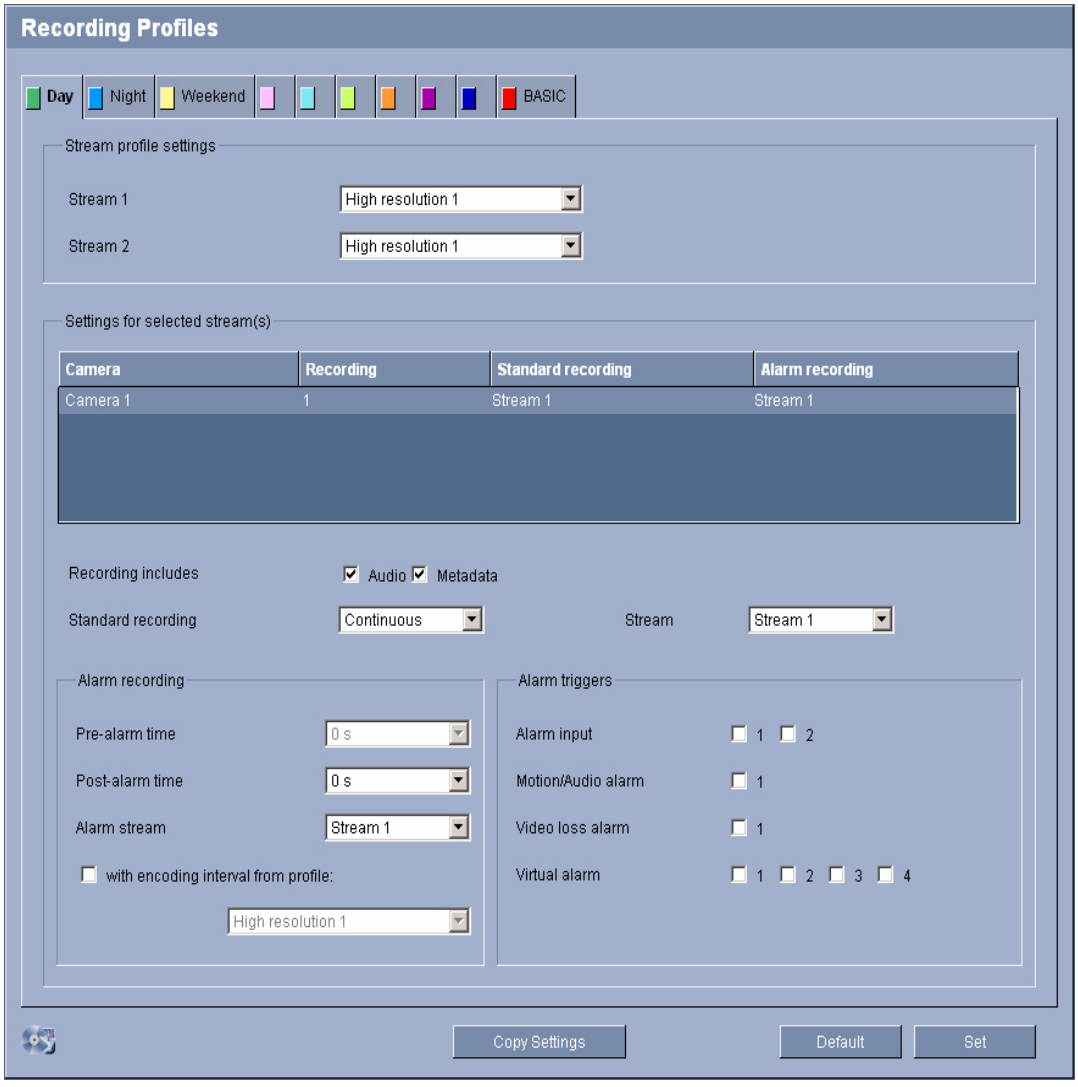
CAUTION!
Check the recordings before deleting and back up important sequences on the computer's hard drive.

1. Click a storage medium in the **Managed storage media** list to select it.
2. Click the **Edit** button below the list. A new window will open.
3. Click the **Formatting** button to delete all recordings in the storage medium.
4. Click **OK** to close the window.

Deactivating Storage Media
You can deactivate any storage medium from the **Managed storage media** list. It is then no longer used for recordings.

1. Click a storage medium in the **Managed storage media** list to select it.
2. Click the **Remove** button below the list. The storage medium is deactivated and removed from the list.

5.23 Advanced Mode: Recording Profiles



You can define up to ten different recording profiles. You will then use these recording profiles in the recording scheduler, where they are linked with the individual days and times (see *Section 5.25 Advanced Mode: Recording Scheduler, page 57*).

NOTICE!
You can change or add to the recording profile description on the tabs on the **Recording Scheduler** page (see *Section Time periods, page 58*).

1. Click one of the tabs to edit the corresponding profile.
2. If necessary, click the **Default** button to return all settings to their default values.
3. Click the **Copy Settings** button if you want to copy the currently visible settings to other profiles. A new window will open and you can select the profiles in which you want to copy the settings.
4. For each profile, click the **Set** button to save the settings in the unit.

Stream profile settings
You can select the profile setting that is to be used for each data stream in the event of recordings. This selection is independent of the selection for live data stream transmission (see *Section 5.20 Advanced Mode: Encoder Streams, page 48*).
The properties of the profiles are defined on the **Encoder Profile** page (see *Section 5.19 Advanced Mode: Encoder Profile, page 45*).

Recording includes
You can specify whether, in addition to video data, audio data and metadata (for example alarms, VCA data and serial data) should also be recorded. Including metadata could make subsequent searches of recordings easier but it requires additional memory capacity.

CAUTION!
Without metadata, it is not possible to include video content analysis in recordings.

Standard recording
Here you can select the mode for standard recordings.
If you select **Continuous**, the recording proceeds continuously. If the maximum memory capacity is reached, older recordings will automatically be overwritten. If you select the **Pre-alarm** option, recording will only take place in the pre-alarm time, during the alarm and during the set post-alarm time.
If you select **Off**, no automatic recording takes place.

CAUTION!
You can specify limitations for overwriting older recordings in **Continuous** mode by configuring the retention time (see *Section 5.24 Advanced Mode: Retention Time, page 56*).

Stream
Here you can select the data stream that is to be used for standard recordings. You can select the data stream for alarm recordings separately and independently of this (see *Section Alarm stream, page 55*).

Pre-alarm time
You can select the required pre-alarm time from the list field.

Post-alarm time
You can select the required post-alarm time from the list field.

Alarm stream
Here you can select the data stream that is to be used for alarm recordings. You can select the data stream for standard recordings separately and independently of this (see *Section Stream, page 55*).

with encoding interval from profile
You can select an alternative encoding interval for the data stream for alarm recordings. Otherwise the encoding interval that corresponds to the default profile allocated to the data stream is used (see *Section 5.20 Advanced Mode: Encoder Streams, page 48*).

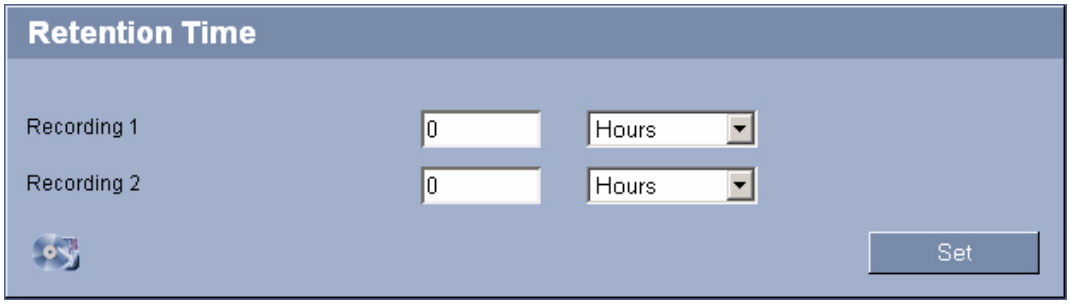
Alarm input / Motion/Audio alarm / Video loss alarm
Here you can select the alarm sensor that is to trigger a recording.

NOTICE!
The alarm inputs are configured and activated on the **Alarm Inputs** page (see *Section 5.35 Advanced Mode: Alarm Inputs, page 75*).
The numbering of the checkboxes for the alarm inputs corresponds to the labeling of the alarm inputs on the VIP X1 XF.
The motion alarm is configured and activated on the **VCA** page (see *Section 5.28 Advanced Mode: VCA, page 62* onwards).
The audio alarm is configured and activated on the **Audio Alarm** page (see *Section 5.32 Advanced Mode: Audio Alarm, page 71*).

Virtual alarm
Here you can select the virtual alarm sensors that are to trigger a recording, via RCP+ commands or alarm scripts, for example.

NOTICE!
For more information, please see the **Alarm Task Script Language** document and the RCP+ documentation. These documents can be found on the product CD supplied.

5.24 Advanced Mode: Retention Time

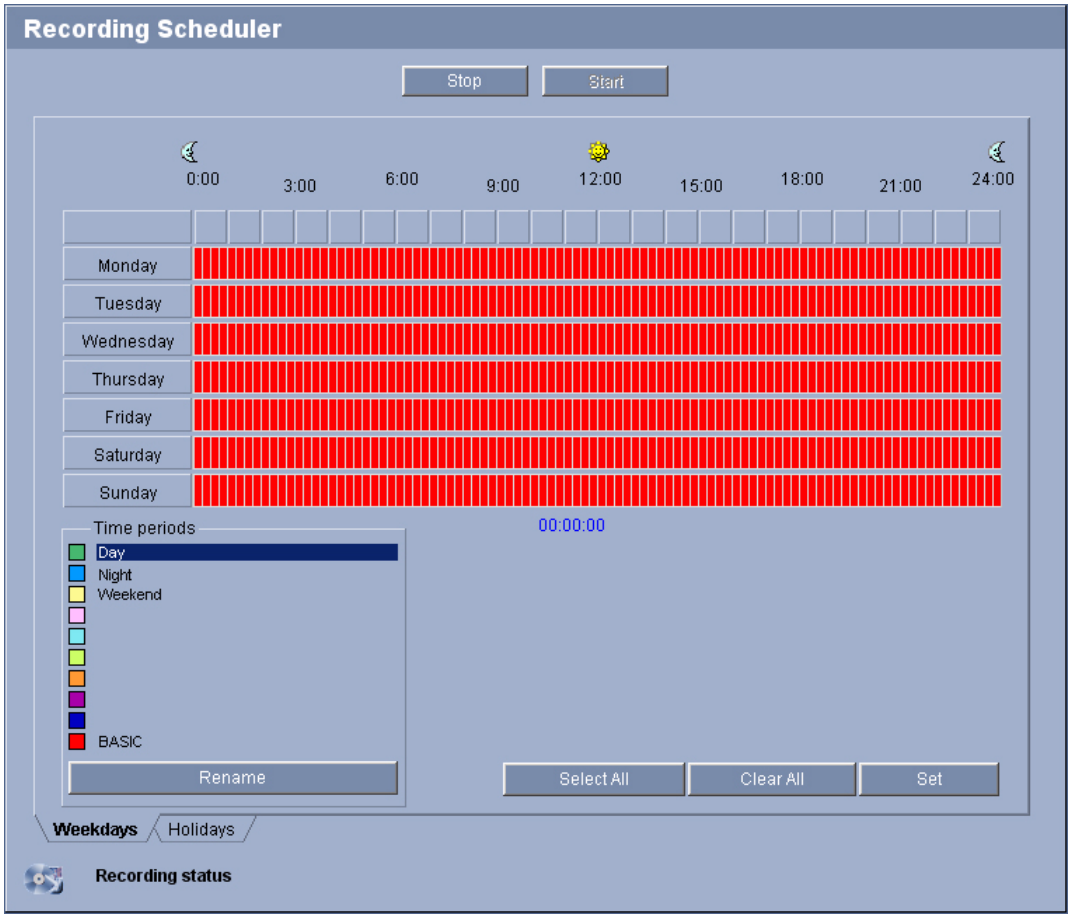


You can specify the retention times for recordings. If the available memory capacity of a medium has been used, older recordings are only overwritten if the retention time entered here has expired.

NOTICE!
Make sure that the retention time corresponds with the available memory capacity. A rule of thumb for the memory requirement is as follows: 1 GB per hour retention time with 4CIF for complete frame rate and high image quality.

Recording 1 / Recording 2
Enter the required retention time in hours or days for each recording. **Recording 1** corresponds to Stream 1, **Recording 2** corresponds to Stream 2.

5.25 Advanced Mode: Recording Scheduler



The recording scheduler allows you to link the created recording profiles with the days and times at which the camera's images are to be recorded in the event of an alarm.
You can link any number of 15-minute intervals with the recording profiles for each day of the week. Moving the mouse cursor over the table displays the time below it. This aids orientation.
In addition to the normal weekdays, you can define holidays that are not in the standard weekly schedule on which recordings are to apply. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

1. Click the profile you want 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 the **Select All** button to link all time intervals to the selected profile.
5. Click the **Clear All** button to deselect all of the intervals.
6. When you are finished, click the **Set** button to save the settings in the unit.

Holidays

You can define holidays that are not in the standard weekly schedule on which recordings are to apply. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

1. Click the **Holidays** tab. Any days that have already been selected will be shown in the table.
2. Click the **Add** button. A new window will open.
3. Select the desired date from the calendar. You can 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 will close.
5. Assign the individual holidays to the recording profiles, as described above.

Deleting Holidays

You can delete holidays you have defined yourself at any time.

1. Click the **Delete** button. A new window will open.
2. Click the date you wish to delete.
3. Click **OK**. The item will be deleted from the table and the window will close.
4. The process must be repeated for deleting additional days.

Time periods

You can change the names of the recording profiles.

1. Click a profile and then the **Rename** button.
2. Enter your chosen name and then click the **Rename** button again.

Activating the Recording

After completing configuration you must activate the recording scheduler and start the recording. Once recording is underway, the **Recording Profiles** and **Recording Scheduler** pages are deactivated and the configuration cannot be modified.

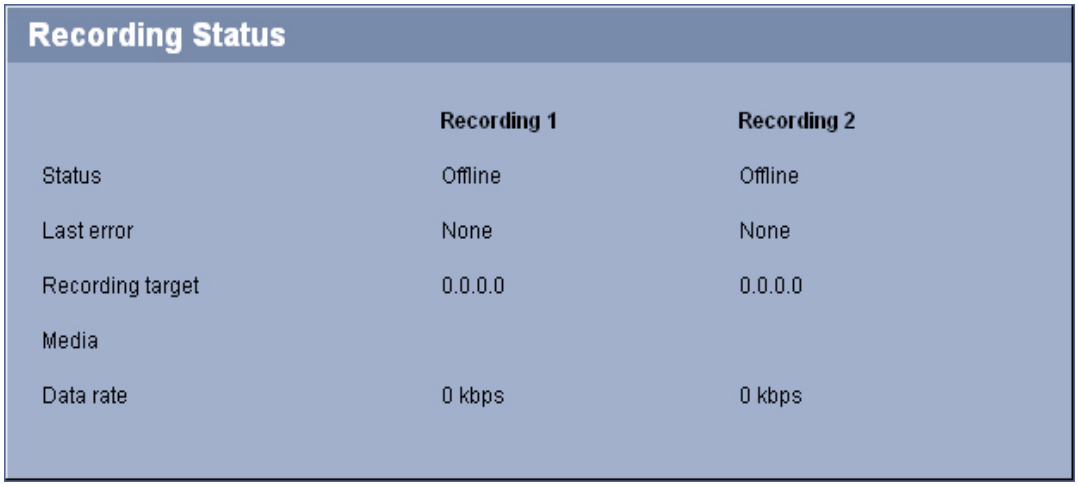
You can stop the recording activity at any time and modify the settings.

1. Click the **Start** button to activate the recording scheduler.
2. Click the **Stop** button to deactivate the recording scheduler. Running recordings are interrupted and the configuration can be changed.

Recording status

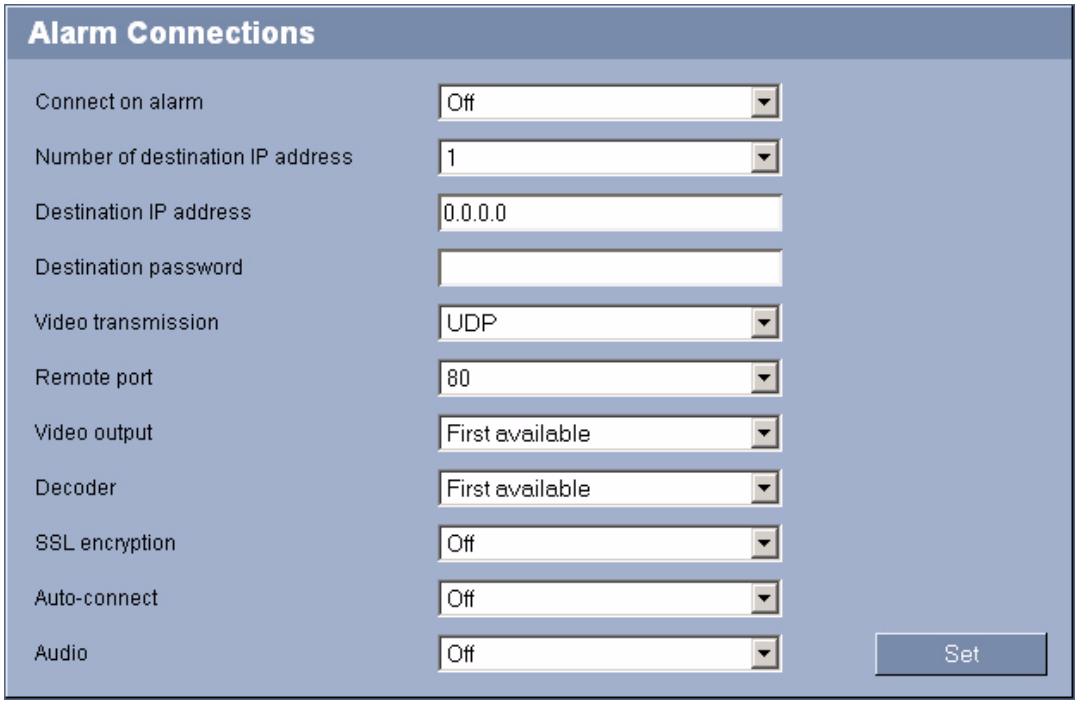
The graphic indicates the recording activity of the VIP X1 XF. You will see an animated graphic while recording is taking place.

5.26 Advanced Mode: Recording Status



Certain details on the recording status are displayed here for information purposes. You cannot change any of these settings.

5.27 Advanced Mode: Alarm Connections



You can select how the VIP X1 XF responds to an alarm. In the event of an alarm, the unit can automatically connect to a pre-defined IP address. You can enter up to ten IP addresses to which the VIP X1 XF will connect in sequence in the event of an alarm, until a connection is made.

Connect on alarm
Select **On** so that the VIP X1 XF automatically connects to a predefined IP address in the event of an alarm.

By setting **Follows input 1** the unit maintains the connection that has been automatically established for as long as an alarm exists on alarm input 1.

NOTICE!
In the default setting, Stream 1 is transmitted for alarm connections. Bear this fact in mind when assigning the profile (see *Section 5.19 Advanced Mode: Encoder Profile, page 45*).

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 stations one after the other in the numbered sequence until a connection is made.

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

Destination password
If the remote station is password protected, enter the password here.
In this page, you can save a maximum of ten destination IP addresses and hence up to ten passwords for connecting to remote stations. If connections to more than ten remote stations are to be possible, for example when initiating connections via higher-ranking systems such as VIDOS or Bosch Video Management System, you can store a general password here. The VIP X1 XF can use this general password to connect to all remote stations protected with the same password. In this case, proceed as follows:

1. Select **10** from the **Number of destination IP address** list field.
2. Enter the address **0.0.0.0** in the **Destination IP address** field.
3. Enter your chosen password in the **Destination password** field.
4. Define this password as the **user** password for all remote stations to which a connection is to be possible.

NOTICE!
If you enter the destination IP address 0.0.0.0 for destination 10, the VIP X1 XF will no longer use this address for the tenth attempt at automatic connection in the event of an alarm. The parameter is then used only to save the general password.

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

CAUTION!
Please note that in some circumstances, a larger bandwidth must be available on the network for additional video images in the event of an alarm, in case Multicast operation is not possible. To enable Multicast operation, select the **UDP** option for the **Video transmission** parameter here and on the **Network** page (see *Section Video transmission, page 79*).

Remote port
Depending on the network configuration, select a browser port here. The ports for HTTPS connections will be available only if the **On** option is selected in the **SSL encryption** parameter.

Video output
If you know which unit is being used as the receiver, you can select the analog video output to which the signal should be switched. If the destination unit is unknown, it is advisable to select the **First available** option. In this case, the image is placed on the first free video

output. This is an output on which there is no signal. The connected monitor only displays images when an alarm is triggered. If you select a particular video output and a split image is set for this output on the receiver, you can also select from **Decoder** the decoder in the receiver that is to be used to display the alarm image.

NOTICE!
Refer to the destination unit documentation concerning image display options and available video outputs.

Decoder
Select a decoder of the receiver to display the alarm image. The decoder selected has an impact on the position of the image in a split screen. For example, you can specify that the upper-right quadrant should be used to display the alarm image on a VIP XD by selecting decoder 2.

SSL encryption
The data for the connection, for example the password, can be securely transmitted with SSL encryption. If you have selected the **On** option, only encrypted ports are offered in the **Remote port** parameter.

NOTICE!
Please note that the SSL encryption must be activated and configured at both ends of a connection. This requires the appropriate certificates to be uploaded onto the VIP X1 XF (see *Section SSL certificate, page 87*).

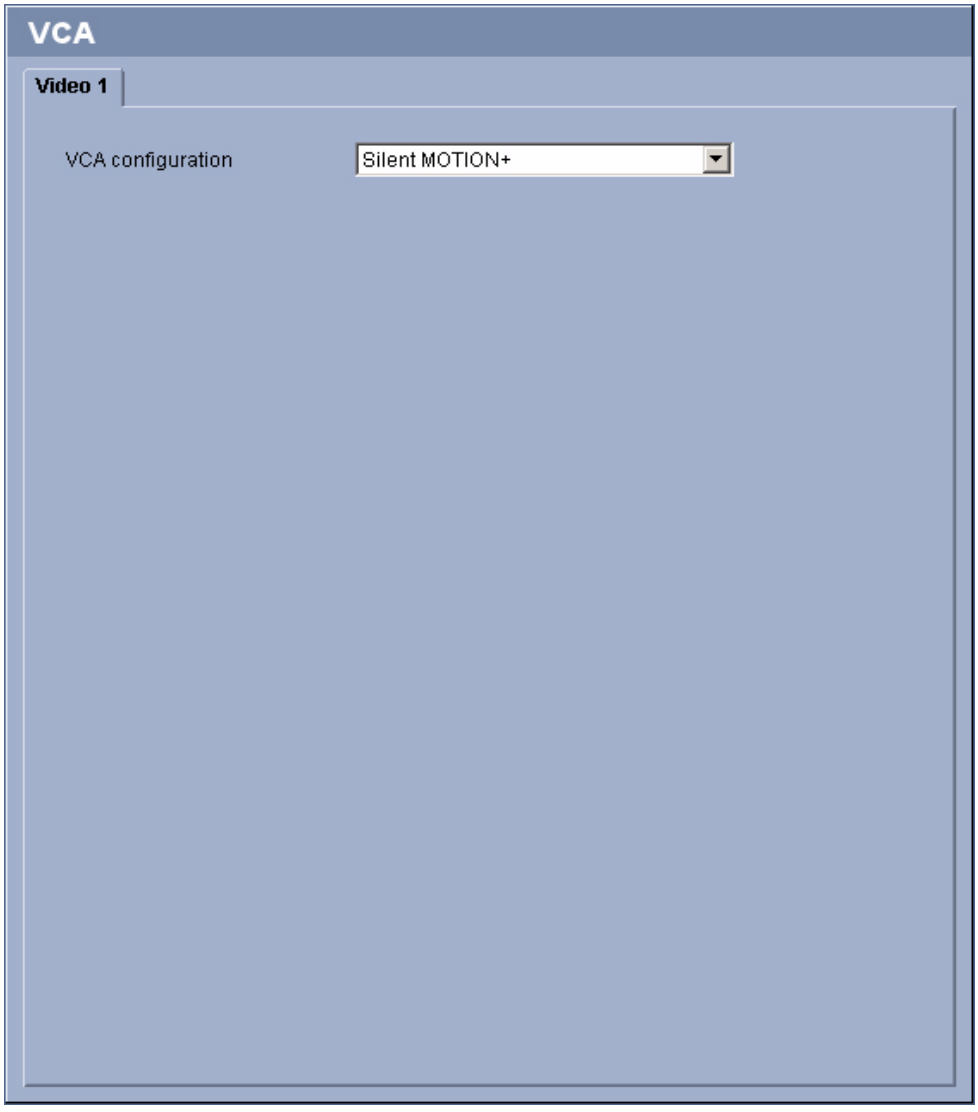
You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.42 Advanced Mode: Encryption, page 85*).

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

NOTICE!
In the default setting, Stream 1 is transmitted for automatic connections. Bear this fact in mind when assigning the profile (see *Section 5.19 Advanced Mode: Encoder Profile, page 45*).

Audio
Select the **On** option if you wish to additionally transmit a standalone G.711 encoded audio stream with alarm connections.

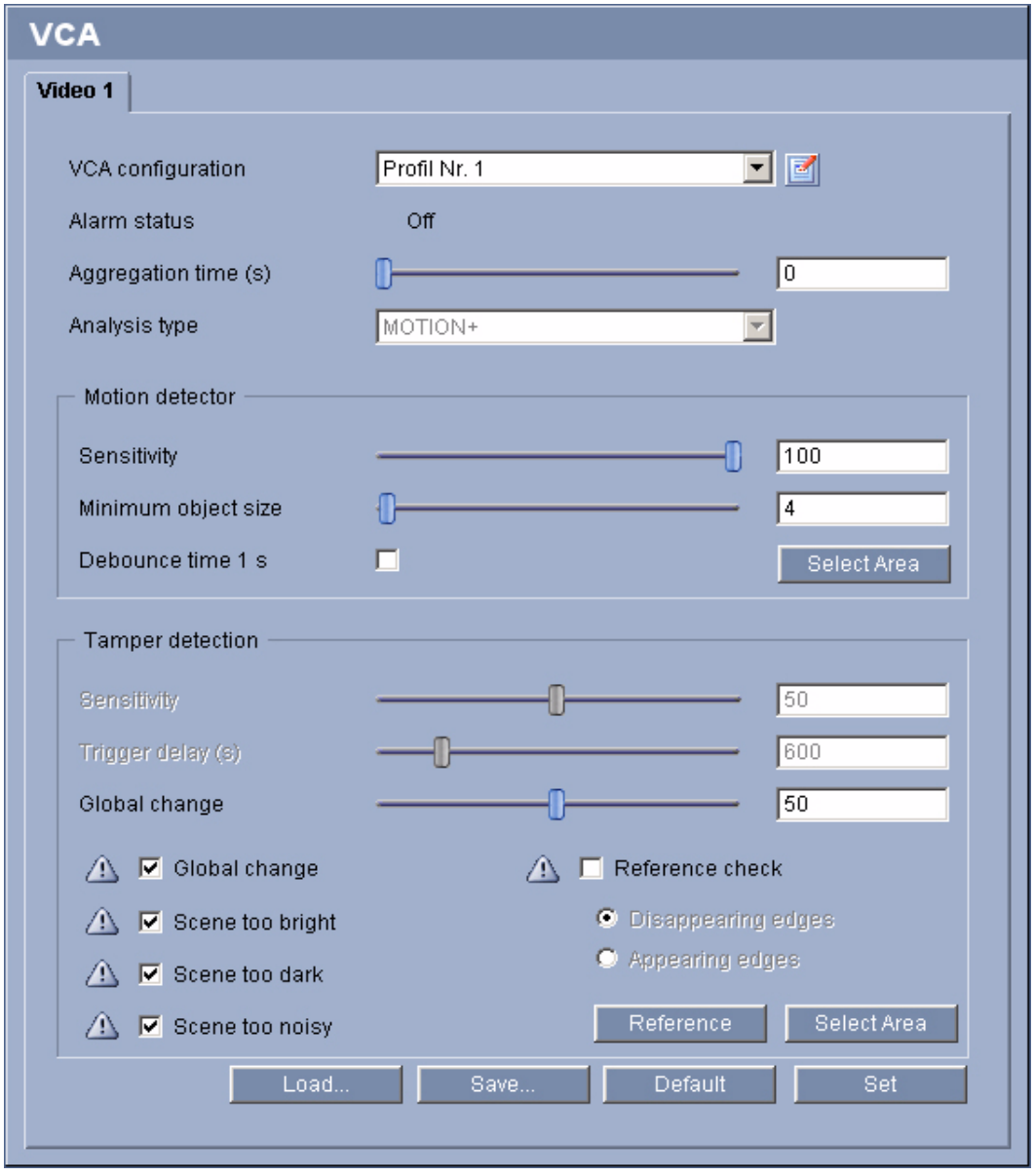
5.28 Advanced Mode: VCA



The VIP X1 XF contains an integrated video content analysis (VCA), which can detect and analyze changes in the signal using image processing algorithms. Such changes can be due to movements in the camera's field of view.
You can select various VCA configurations and adapt these to your application as required.
The **Silent MOTION+** configuration is active by default. In this configuration, metadata is created to facilitate searches of recordings; however, no alarm is triggered.
You can switch off the video content analysis completely if the device's full power is to be made available for the encoder.

1. Select a VCA configuration and make the required settings.
2. If necessary, click the **Default** button to return all settings to their default values.

5.29 Advanced Mode: VCA Profiles



You can configure two profiles with different VCA configurations. You can save profiles on your computer's hard drive and load saved profiles from there. This can be useful if you want to test a number of different configurations. Save a functioning configuration and test new settings. You can use the saved configuration to restore the original settings at any time.

NOTICE!
If computing power becomes short, the highest priority is always the live images and recordings. This can lead to impairment of the video content analysis. You should therefore observe the processor load and optimize the encoder settings or the video content analysis settings as necessary.

1. Select a VCA profile and enter the required settings.
2. If necessary, click the **Default** button to return all settings to their default values.

3. Click the **Save...** button to save the profile settings to another file. A new window is opened, in which you can specify where you want to save the file and what name you want to save it under.
4. Click the **Load...** button to load a saved profile. A new window opens in which you can select the profile file and specify where to save the file.

VCA configuration

Select one of the profiles here to activate it or edit it.

You can rename the 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.

Alarm status

The alarm status is displayed here for information purposes. This means you can check the effects of your settings immediately.

Aggregation time (s)

You can set an aggregation time of between 0 and 20 seconds if necessary. 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 (see *Section 5.23 Advanced Mode: Recording Profiles, page 54*).

Analysis type

Select the required analysis algorithm. By default, only **MOTION+** is available – this offers a motion detector and essential recognition of tampering.

NOTICE!

Additional analysis algorithms with comprehensive functions, such as IVMD and IVA, are available from Bosch Security Systems.

If you select one of these algorithms, you can set the corresponding parameters here directly. You can find information on this in the relevant documents on the product CD supplied.

Metadata is always created for a video content analysis, unless this was 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 will be marked with rectangles.

NOTICE!

On the **LIVEPAGE Functions** page, you can also enable additional information overlays for the **LIVEPAGE** (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).

Motion detector (MOTION+ only)

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.

CAUTION!

Reflections of light (off glass surfaces, etc.), switching lights on or 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 (MOTION+ only)

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 (MOTION+ only)

You can specify the number of sensor fields that a moving object must cover to generate an alarm. This is to prevent 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 (MOTION+ only)

The debounce time is intended to prevent 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.

Select Area (MOTION+ only)

The areas of the image to be monitored by the motion detector can be selected. The video image is subdivided into square sensor fields. Each of these fields can be activated or deactivated individually. If you wish to exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, etc.), the relevant fields can be deactivated.

1. Click **Select Area** to configure the sensor fields. A new window will open.
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 you wish 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.

Tamper detection

You can reveal the 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.

NOTICE!
The options for tamper detection can only be set for fixed cameras. Dome cameras or other motorized cameras cannot be protected in this manner as the movement of the camera itself causes changes in the video image that are too great.

Sensitivity

NOTICE!
This and the following parameter are only accessible if the reference check is activated.

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)
You can set delayed alarm triggering. 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 allows you to avoid false alarms triggered by short-term changes, for example cleaning activities in the direct field of vision of the camera.

Global change
You can 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 you to detect, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mount bracket, for instance.

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 lens) 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 lens (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), as an example, should trigger an alarm.

Reference check

You can save a reference image that is 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 allows you to detect 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 on-going matching. 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.

Select Area

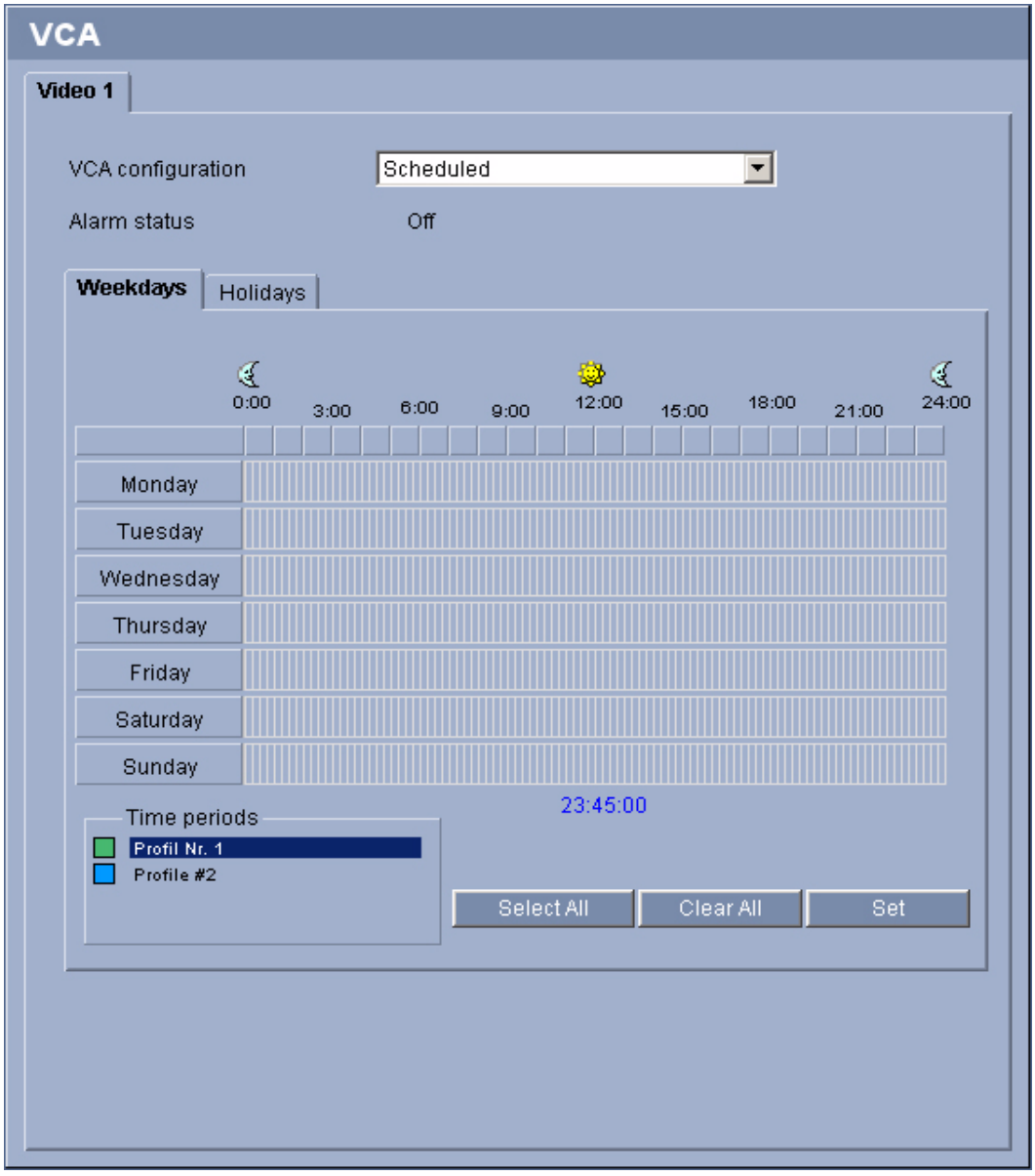
You can select the image areas in the reference image that are to be monitored. The video image is subdivided into square fields. Each of these fields can be activated or deactivated individually.

NOTICE!

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 will open.
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 you wish 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.

5.30 Advanced Mode: VCA Scheduled



This configuration allows you to link the created VCA profile with the days and times at which the video content analysis is to be active.
You can 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.
In addition to the normal weekdays, you can define holidays that are not in the standard weekly schedule on which recordings are to apply. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

1. Click the profile you want 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 the **Select All** button to link all time intervals to the selected profile.
5. Click the **Clear All** button to deselect all of the intervals.
6. When you are finished, click the **Set** button to save the settings in the unit.

Holidays

You can define holidays on which a profile should be active that are different to the standard weekly schedule. This allows you to apply a schedule for Sundays to other days with dates that fall on varying weekdays.

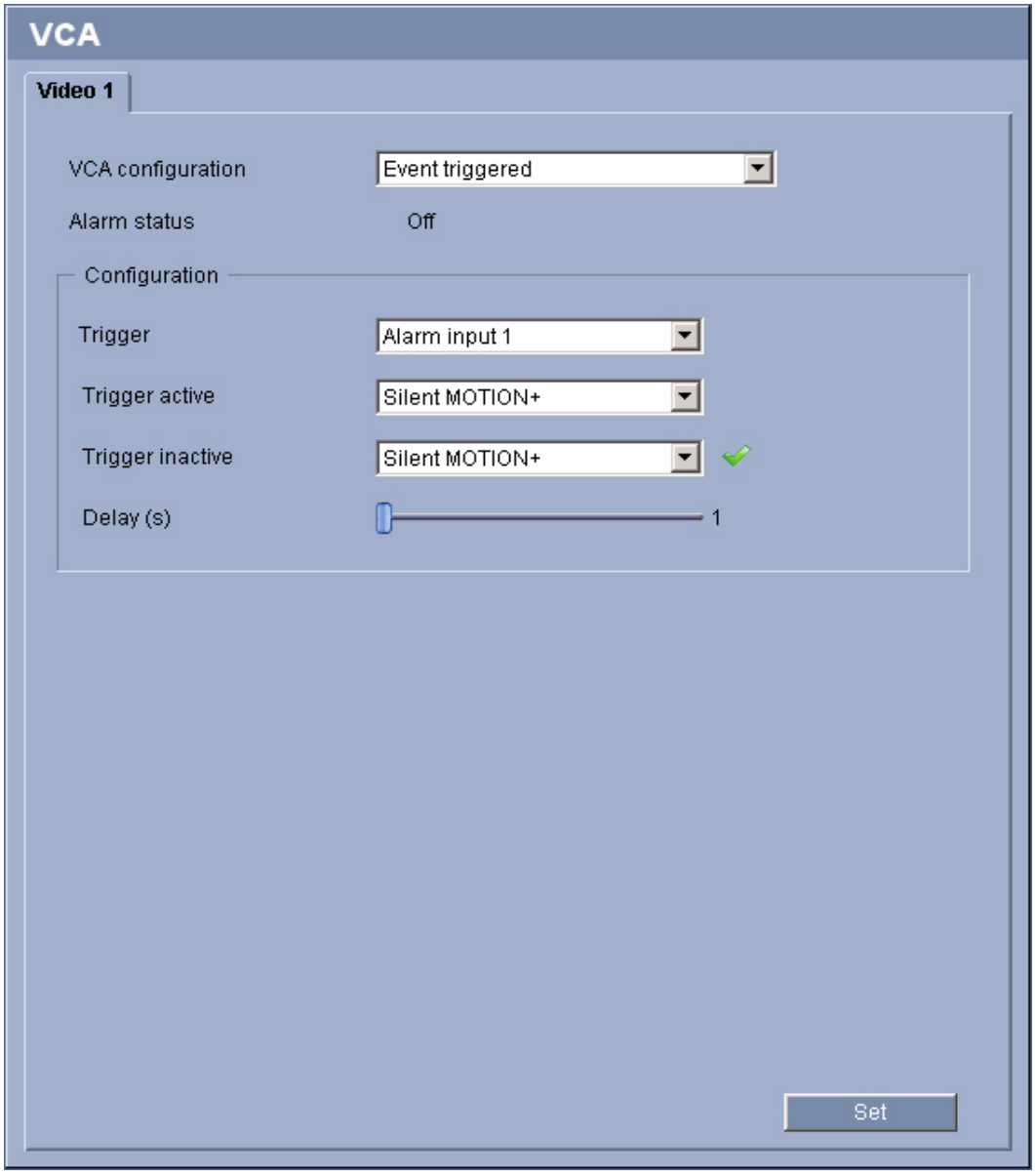
1. Click the **Holidays** tab. Any days that have already been selected will be shown in the table.
2. Click the **Add** button. A new window will open.
3. Select the desired date from the calendar. You can select several consecutive calendar days by holding down the mouse button. These will later be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

Deleting Holidays

You can delete holidays you have defined yourself at any time.

1. Click the **Delete** button. A new window will open.
2. Click the date you wish to delete.
3. Click **OK**. The item will be deleted from the table and the window will close.
4. The process must be repeated for deleting additional days.

5.31 Advanced Mode: VCA Event triggered



This configuration allows you stipulate that the video content analysis is only to be activated when triggered by an event. As long as no trigger is activated, the **Silent MOTION+** configuration in which metadata is created is active; this metadata facilitates searches of recordings, but does not trigger an alarm.

Trigger
You can select one of the physical alarms on the device's alarm inputs or one of the virtual alarms as a trigger. A virtual alarm is created using software, with RCP+ commands or alarm scripts, for example.

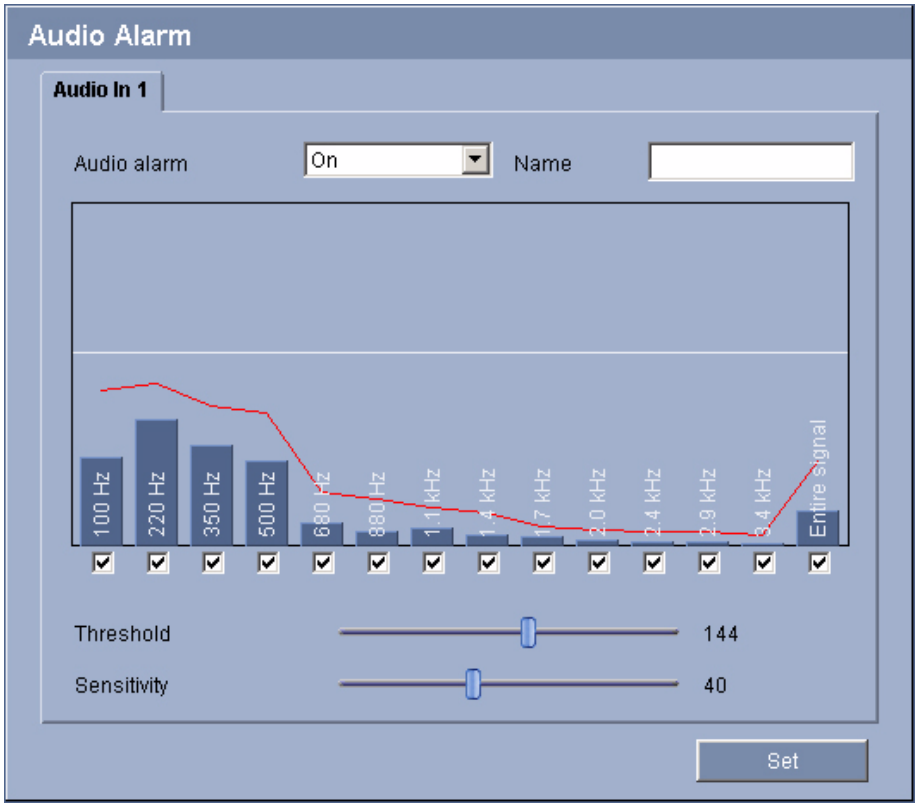
NOTICE!
For more information, please see the **Alarm Task Script Language** document and the RCP+ documentation. You can find these documents on the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).

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

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

Delay (s)
Select the delay period here 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, for example. During the delay period, the **Silent MOTION+** configuration is always enabled.

5.32 Advanced Mode: Audio Alarm



The VIP X1 XF can create alarms on the basis of audio signals. You can configure signal strengths and frequency ranges in such a way that false alarms, for example due to machine noise or background noise, are avoided.

NOTICE!
First set up normal audio transmission before you configure the audio alarm here (see *Section 5.21 Advanced Mode: Audio, page 50*).

Audio alarm
Select **On** if you want the device to generate audio alarms.

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

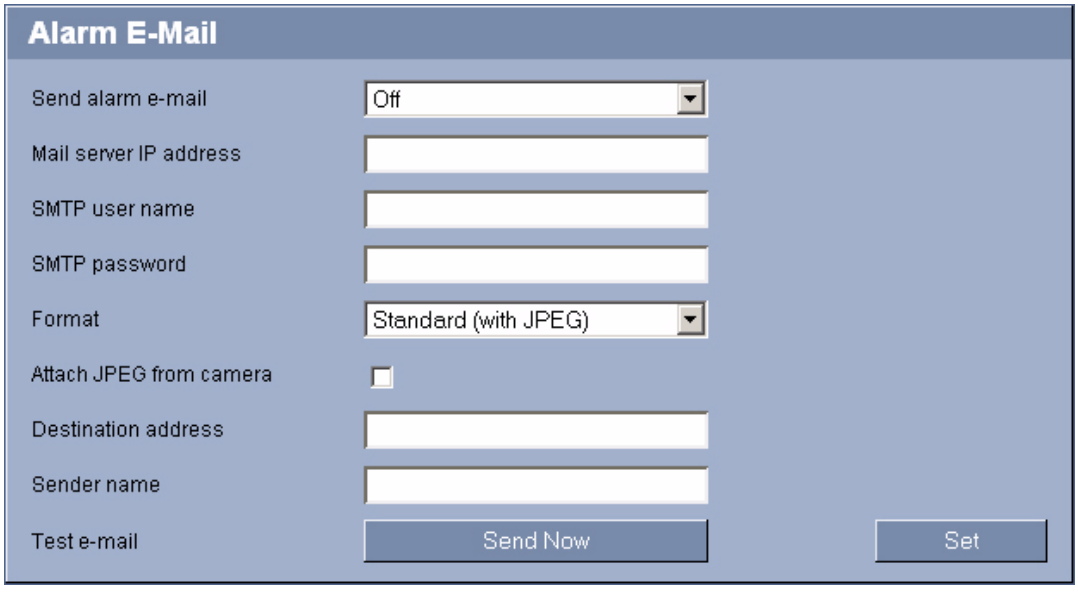
CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal recording management and may therefore result in the Player or Archive Player programs being unable to play back the recording.

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

Sensitivity
You can use this setting to adapt the sensitivity to the sound environment. You can effectively suppress individual signal peaks. A high value represents a high level of sensitivity.

Signal Ranges
You can 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.

5.33 Advanced Mode: Alarm E-Mail



As an alternative to automatic connecting, alarm states can also be documented by e-mail. In this way it is possible to notify a recipient who does not have a video receiver. In this case, the VIP X1 XF automatically sends an e-mail to a previously defined e-mail address.

Send alarm e-mail
Select **On** if you want the unit to automatically send an alarm e-mail in the event of an alarm.

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

SMTP user name
Enter a registered user name for the chosen mailserver here.

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

Format
You can select the data format of the alarm message.

- **Standard (with JPEG)**
  E-mail with attached JPEG image file.
- **SMS**
  E-mail in SMS format to an e-mail-to-SMS gateway (for example to send an alarm by cellphone) without an image attachment.

CAUTION!
When a cellphone 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.
You can obtain information on operating your cellphone from your cellphone provider.

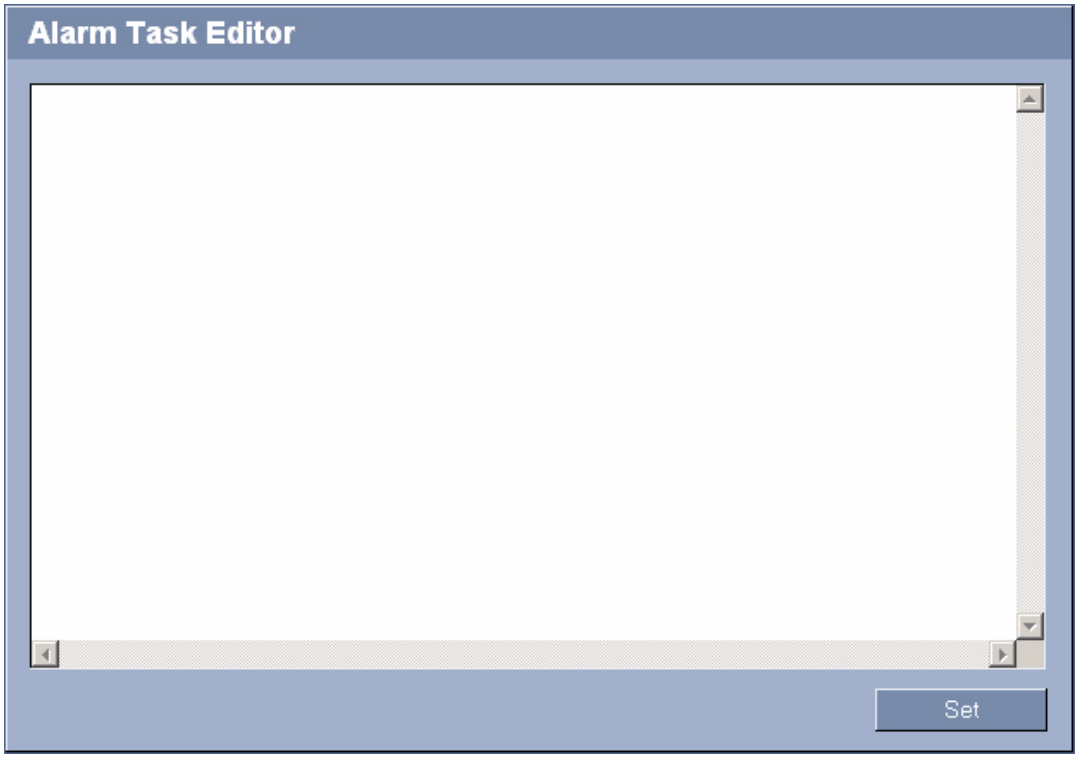
Attach JPEG from camera
Click the checkbox to specify that JPEG images are sent from the camera. An enabled video input is indicated by a check mark.

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

Sender name
Enter a unique name for the e-mail sender, for example the location of the unit. This will make it easier to identify the origin of the e-mail.

Test e-mail
You can test the e-mail function by clicking the **Send Now** button. An alarm e-mail is immediately created and sent.

5.34 Advanced Mode: Alarm Task Editor

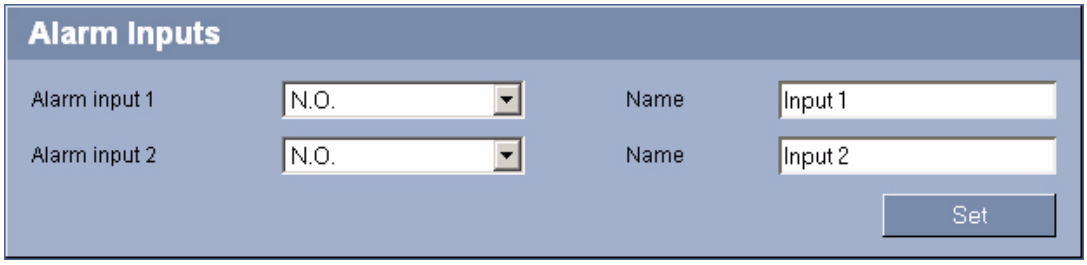


CAUTION!
Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.
In order to edit this page, you must have programming knowledge and be familiar with the information in the **Alarm Task Script Language** document. You can find the document on the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).

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

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

5.35 Advanced Mode: Alarm Inputs

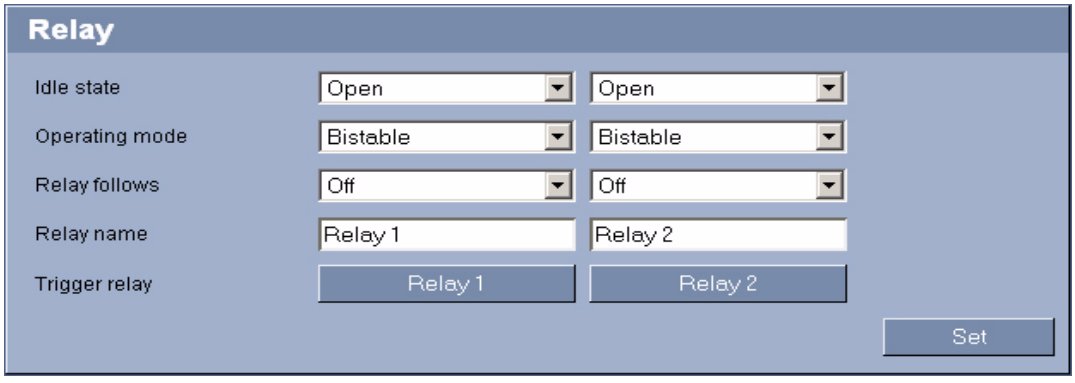


You can configure the alarm inputs of the VIP X1 XF.

Alarm input
Select **N.O.** if the alarm is to be triggered when the contact closes. Select **N.C.** if the alarm is to be triggered when the contact opens.

Name
You can enter a name for each alarm input, which is then displayed below the icon for the alarm input on the **LIVEPAGE** if configured correctly (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).

5.36 Advanced Mode: Relay



You can configure the switching behavior of the relay outputs. For each relay, you can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).
You can also specify whether an output should operate as a bistable or monostable relay. In bistable mode, the triggered state of the relay is maintained. In monostable mode, you can set the time after which the relay will return to the idle state.
You can select different events that automatically activate an output. It is possible, for example, to turn on a floodlight by triggering a motion alarm and then turning the light off again when the alarm has stopped.

Idle state
Select **Open** if you want the relay to operate as an NO contact, or select **Closed** if the relay is to operate as an NC contact.

Operating mode
Select an operating mode for the relay.

For example, if you want an alarm-activated lamp to stay on after the alarm ends, select **Bistable**. If you wish an alarm-activated siren to sound for ten seconds, for example, select **10 s**.

Relay follows

If required, select a specific event that will trigger the relay. The following events are possible triggers:

- **Off**
  Relay is not triggered by events
- **Connection**
  Trigger whenever a connection is made
- **Video alarm**
  Trigger by interruption of the video signal
- **Motion alarm**
  Trigger by motion alarm, as configured on the **VCA** page (see *Section 5.31 Advanced Mode: VCA Event triggered, page 70*)
- **Local input**
  Trigger by the corresponding external alarm input
- **Remote input**
  Trigger by remote station's corresponding switching contact (only if a connection exists)

NOTICE!
The numbers in the lists of selectable events relate to the corresponding connections on the unit, **Video alarm 1**, for example to the **VIDEO IN** connection.

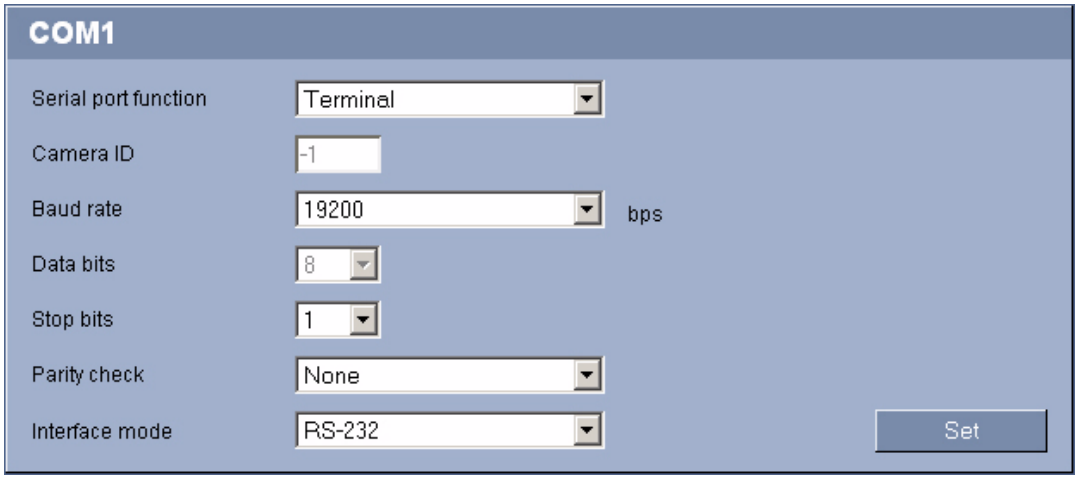
Relay name

You can assign a name for the relay here. The name is shown on the button next to **Trigger relay**. The Livepage can also be configured to display the name under the relay icon.

Trigger relay

Click the button to trigger the relay manually (for testing or to operate a door opener, for example).

5.37 Advanced Mode: COM1



You can configure the serial interface parameters (orange terminal block) to meet your requirements.

NOTICE!
If the VIP X1 XF is working in multicast mode (see *Section 5.40 Advanced Mode: Multicasting, page 83*), the first remote location to establish a video connection to the unit is also assigned the transparent data connection. However, after about 15 seconds of inactivity the data connection is automatically terminated and another remote location can exchange transparent data with the unit.

Serial port function
Select a controllable unit from the list. If you wish to use the serial port to transmit transparent data, select **Transparent**. Select **Terminal** if you wish to operate the unit from a terminal.

NOTICE!
After selecting a unit, the remaining parameters in the window are set automatically and should not be changed.

Camera ID
If necessary, enter the ID of the peripheral you wish to control (for example a dome camera or pan/tilt head).

Baud rate
Select the value for the transmission rate in bps.

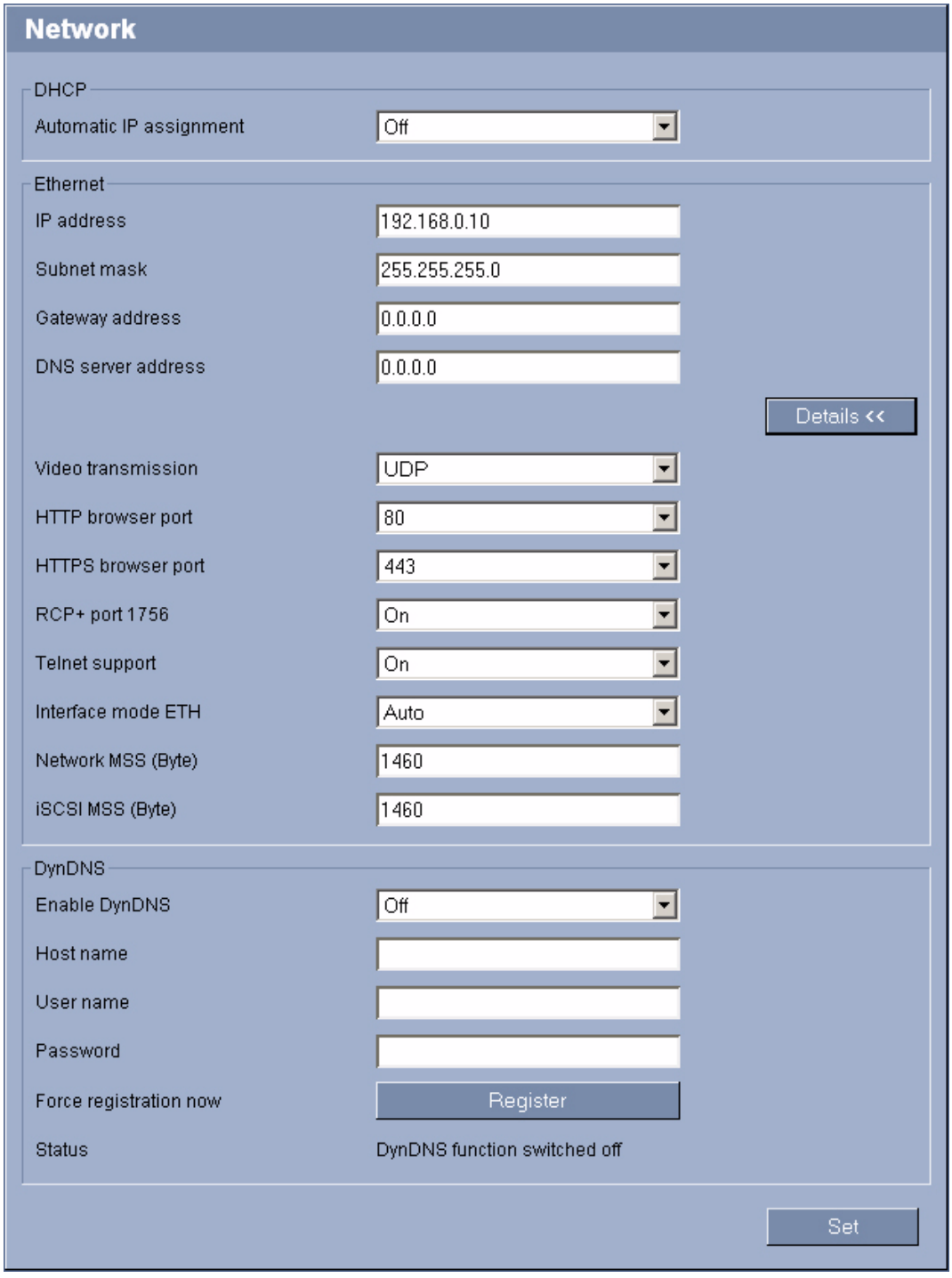
Data bits
The number of data bits per character cannot be changed.

Stop bits
Select the number of stop bits per character.

Parity check
Select the type of parity check.

Interface mode
Select the desired protocol for the serial interface.

5.38 Advanced Mode: Network



The settings on this page are used to integrate the VIP X1 XF into an existing network. Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.
2. Click the **Set and Reboot** button. The VIP X1 XF is rebooted and the changed settings are activated.

CAUTION!
If you change the IP address, subnet mask or gateway address, the VIP X1 XF is only available under the new addresses after the reboot.

Automatic IP assignment
If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the VIP X1 XF.
Certain applications (VIDOS, Bosch Video Management System, Archive Player, Configuration Manager) use the IP address for the unique assignment of the unit. If you use these 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 VIP X1 XF in this field. The IP address must be valid for the network.

Subnet mask
Enter the appropriate subnet mask for the selected IP address here.

Gateway address
If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise leave the box blank (**0.0.0.0**).

DNS server address
The unit can use a DNS server to trigger an address specified as a name. Enter the IP address of the DNS server here.

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

CAUTION!
Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.
The MTU value in UDP mode is 1,514 bytes.

HTTP browser port
Select a different HTTP browser port from the list if required. The default HTTP port is 80. If you want to allow only secure connections via HTTPS, you must deactivate the HTTP port. In this case, select **Off**.

HTTPS browser port
If you wish to allow browser access on the network via a secure connection, select an HTTPS browser port from the list if necessary. The default HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports; only unsecured connections will now be possible.
The VIP X1 XF uses the TLS 1.0 encryption protocol. You may have to activate this protocol via your browser configuration. You must also activate the protocol for the Java applications (via the Java control panel in the Windows control panel).

NOTICE!
If you want to allow only secure connections with SSL encryption, you must select the **Off** option for each of the parameters **HTTP browser port**, **RCP+ port 1756** and **Telnet support**. This deactivates all unsecured connections. Connections will then only be possible via the HTTPS port.

You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.42 Advanced Mode: Encryption, page 85*).

RCP+ port 1756
To exchange connection data, you can activate the unsecured RCP+ port 1756. If you want connection data to be transmitted only when encrypted, select the **Off** option to deactivate the port.

Telnet support
If you want to allow only secure connections with encrypted data transmission, you must select the **Off** option to deactivate Telnet support. The unit will then no longer be accessible using the Telnet protocol.

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

Network MSS (Byte)
You can set the maximum segment size for the IP packet's user data. This gives you the option to adjust the size of the data packets to the network environment and to optimize data transmission. Please comply with the MTU value of 1,514 bytes in UDP mode.

iSCSI MSS (Byte)
You can 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 VIP X1 XF.

Enable DynDNS
DynDNS.org is a DNS hosting service that stores IP addresses in a database ready for use. It allows you to select the VIP X1 XF 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 DynDNS.org and you must have registered the required host name for the unit on that site.

NOTICE!
Information about the service, registration process and available host names can be found at DynDNS.org.

Host name
Enter the host name registered on DynDNS.org for the VIP X1 XF here.

User name
Enter the user name you registered at DynDNS.org here.

Password
Enter the password you registered at DynDNS.org here.

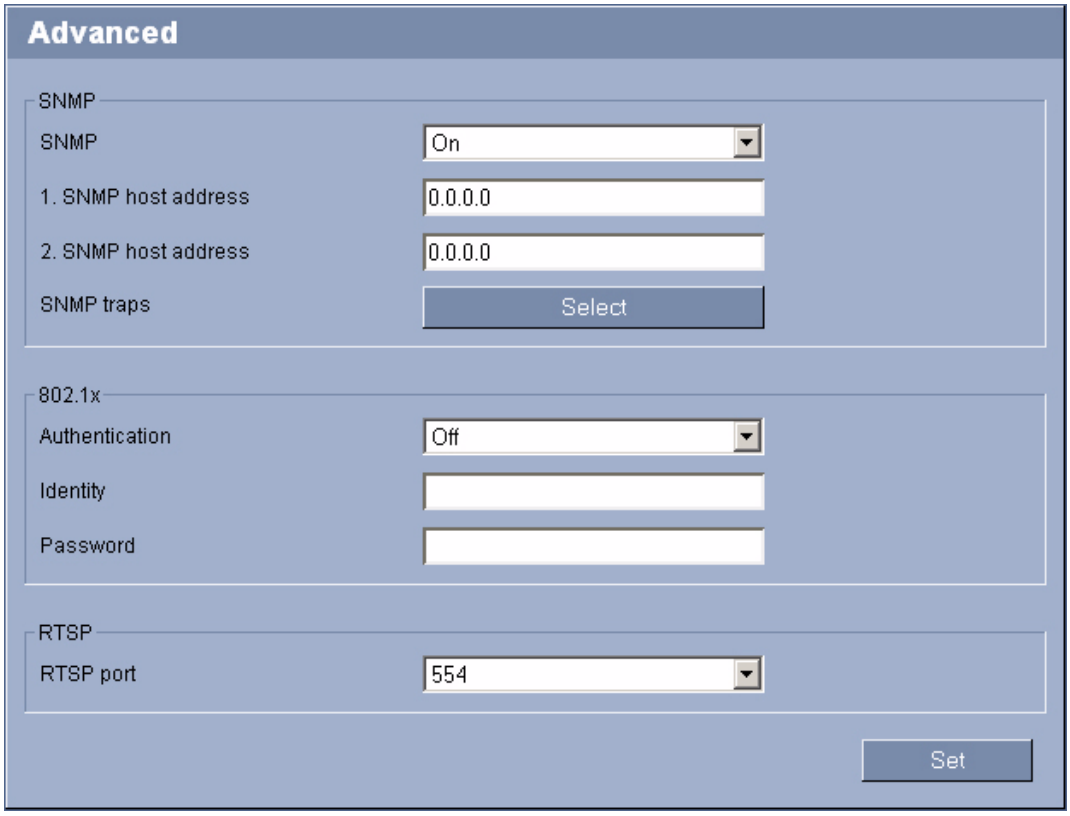
Force registration now

You can 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 you are 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 VIP X1 XF, click the **Register** button.

Status

The status of the DynDNS function is displayed here for information purposes. You cannot change any of these settings.

5.39 Advanced Mode: Advanced



The settings on this page are used to implement advanced settings for the network.
Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.
2. Click the **Set and Reboot** button. The VIP X1 XF is rebooted and the changed settings are activated.

SNMP

The VIP X1 XF supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The unit supports SNMP MIB II in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target devices here.
If you select **On** for the **SNMP** parameter and do not enter an SNMP host address, the VIP X1 XF does not send the SNMP traps automatically, but only replies to SNMP requests. If you enter one or two SNMP host addresses, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

1. SNMP host address / 2. SNMP host address

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

SNMP traps

You can select which traps are to be sent.

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

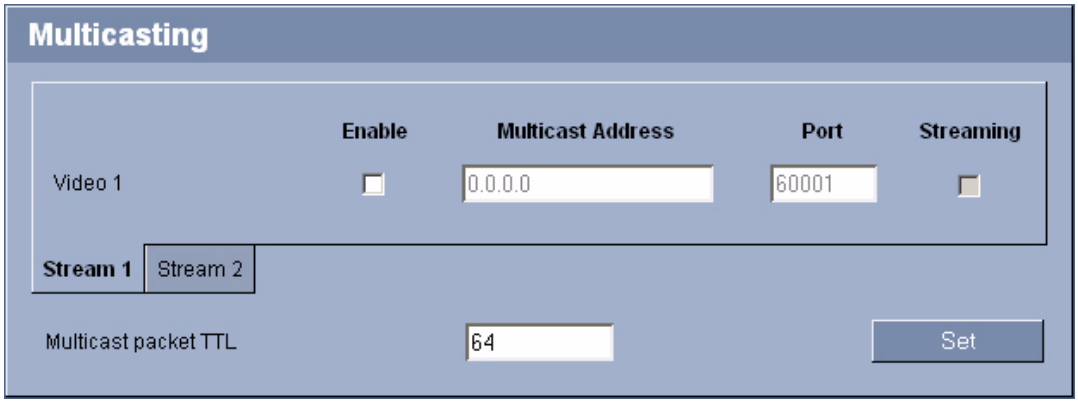
Authentication
If a RADIUS server is employed in the network for managing access rights, authentication must be activated here to allow communication with the unit. The RADIUS server must also contain the corresponding data.
To configure the unit, you must connect the VIP X1 XF directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated.

Identity
Enter the name that the RADIUS server is to use for identifying the VIP X1 XF.

Password
Enter the password that is stored in the RADIUS server.

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.

5.40 Advanced Mode: Multicasting



In addition to a 1:1 connection between an encoder and a single receiver (unicast), the VIP X1 XF can enable multiple receivers to receive the video signal from an encoder simultaneously. The device either duplicates the data stream itself and then distributes it to multiple receivers (Multi-unicast) or it sends a single data stream to the network, where the data stream is simultaneously distributed to multiple receivers in a defined group (Multicast). You can enter a dedicated multicast address and port for each stream. You can switch between the streams by clicking the appropriate tabs.

NOTICE!
Multicast operation requires a multicast-enabled network that uses the UDP and the Internet Group Management IGMP protocols. Other group management protocols are not supported. The TCP protocol does not support multicast connections.

A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network.
The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255.
The multicast address can be the same for multiple streams. However, it will be necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and multicast address.

NOTICE!
The settings must be made individually for each stream.

Enable
To enable simultaneous data reception on several receivers you need to activate the multicast function. To do this, check the box. You can then enter the multicast address.

Multicast Address
Enter a valid multicast address for each stream to be operated in multicast mode (duplication of the data streams in the network).
With the setting **0.0.0.0** the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in the unit). The VIP X1 XF supports multi-unicast connections for up to five simultaneously connected receivers.

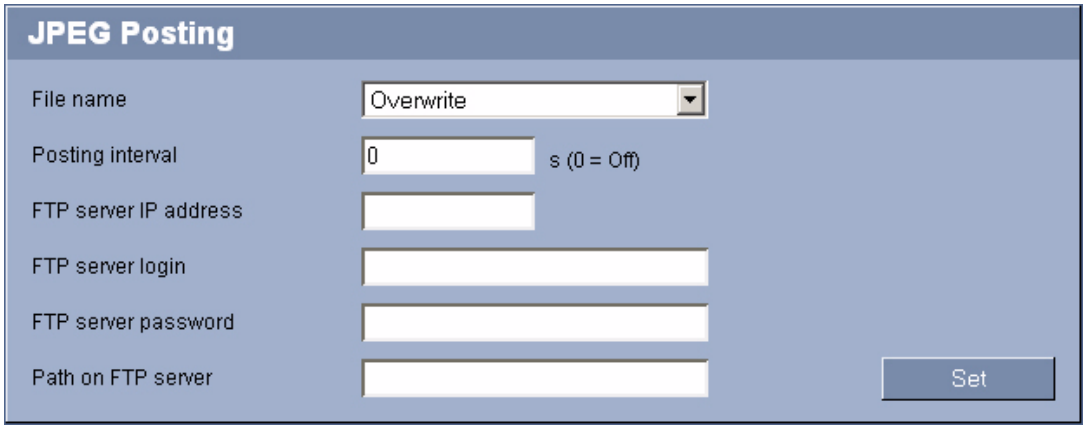
NOTICE!
Duplication of data places a heavy demand on the unit and can lead to impairment of the image quality under certain circumstances.

Port
Assign a different port to each data stream if there are simultaneous data streams at the same multicast address.
Enter the port address of the required stream here.

Streaming
Click the checkbox to activate multicast streaming mode for the relevant stream. An enabled stream is indicated by a check mark.
Streaming is typically not required for standard multicast operation.

Multicast packet TTL
You can enter a value to specify how long the multicast data packets are active on the network. This value must be greater than one if multicast is to be run via a router.

5.41 Advanced Mode: JPEG Posting



You can save individual JPEG images on an FTP server at specific intervals. You can then retrieve these images at a later date to reconstruct alarm events if required. The resolution corresponds to the highest setting from the two data streams.

File name

You can select how file names will be created for the individual images that are transmitted.

- **Overwrite**
  The same file name is always used and any existing file will be overwritten with 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 unit's date and time are always correctly set. Example: 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 will be sent to an FTP server. Enter zero if you do not want any images to be sent.

FTP server IP address

Enter the IP address of the FTP server on which you wish to save the JPEG images.

FTP server login

Enter your login name for the FTP server.

FTP server password

Enter the password that gives you access to the FTP server.

Path on FTP server

Enter the exact path on which you wish to post the images on the FTP server.

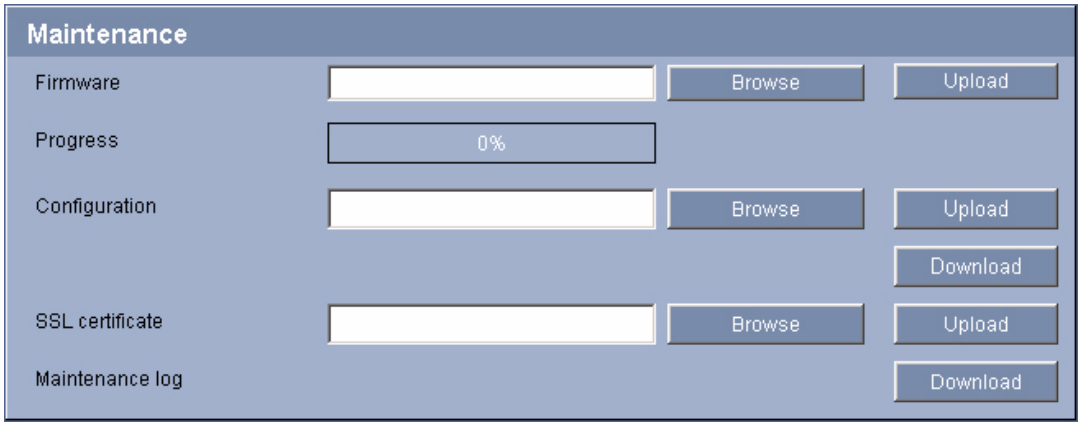
NOTICE!

The creation of JPEG images has a lower priority than video encoding and image analysis. This can result in JPEG images being created with a delay of up to several seconds after the triggering event. If reliable, real-time recording of the alarm is required, ensure that the encoder has enough computing power available.

5.42 Advanced Mode: Encryption

A special license, with which you will receive a corresponding activation key, is required to encrypt user data. You can enter the activation key to release the function on the **Licenses** page (see *Section 5.44 Advanced Mode: Licenses, page 88*).

5.43 Advanced Mode: Maintenance



Firmware

The VIP X1 XF is designed in such a way that its functions and parameters can be updated with firmware. To do this, transfer the current firmware package to the unit via the selected network. It will then be automatically installed there.

In this way, a VIP X1 XF can be serviced and updated remotely without a technician having to change the installation on site.

You obtain the current firmware from your customer service or from the download area at www.boschsecurity.com.

CAUTION!

Before launching the firmware upload make sure that you have selected the correct upload file. Uploading the wrong files can result in the unit no longer being addressable, in which case you must replace the unit.

You should never interrupt the installation of firmware. An interruption can lead to the flash-EPROM being incorrectly programmed. This in turn can result in the unit no longer being addressable, in which case it will have to be replaced. Even changing to another page or closing the browser window leads to an interruption.

1. First store the firmware file on your hard drive.
2. Enter the full path of the firmware file in the field or click **Browse** to locate and select the file.
3. Next, click **Upload** to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

The new firmware is unpacked and the Flash EPROM is reprogrammed. The time remaining is shown in the message **going to reset Reconnecting in ... seconds**. The unit reboots automatically once the upload has successfully completed.

If the **POWER** LED then flashes red, the upload has failed and must be repeated. To perform the upload you must now switch to a special page:

1. In the address bar of your browser, enter **/main.htm** after the IP address of the VIP X1 XF (for example **192.168.0.10/main.htm**).
2. Repeat the upload.

Configuration

You can save configuration data for the VIP X1 XF on a computer and then load saved configuration data from a computer to the unit.

Upload

1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Make certain that the file to be loaded comes from the same unit type as the unit you want to configure.
3. Next, click **Upload** to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

Once the upload is complete, the new configuration is activated. The time remaining is shown in the message **going to reset Reconnecting in ... seconds**. The unit reboots automatically once the upload has successfully completed.

Download

1. Click the **Download** button. A dialog box opens.
2. Follow the on-screen instructions to save the current settings.

SSL certificate

To be able to work with an SSL encrypted data connection, both ends of a connection must hold the relevant certificates. You can upload the SSL certificate, comprising one or multiple files, onto the VIP X1 XF.

If you wish to upload multiple files onto the VIP X1 XF, you must select them consecutively.

NOTICE!

The certificate must be created in the format *.pem so that it can be accepted by the unit.

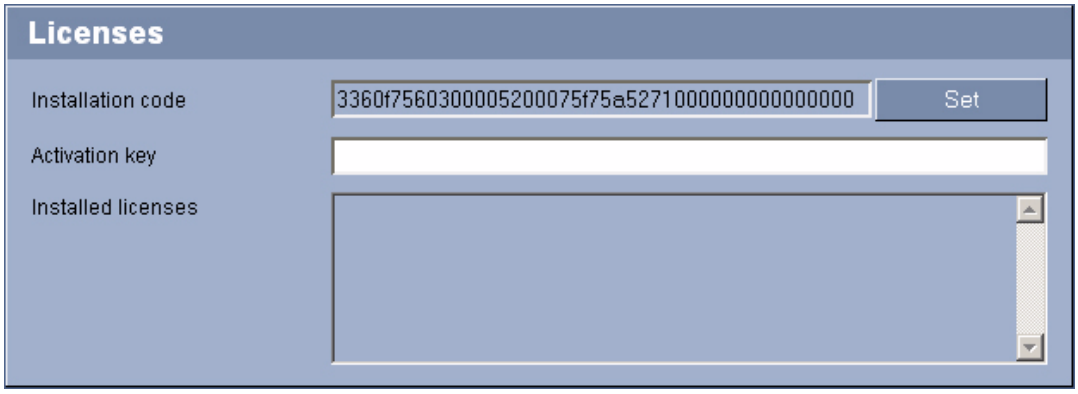
1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Next, click **Upload** to begin transferring the file to the unit.
3. Once all files have been successfully uploaded, the unit must be rebooted. In the address bar of your browser, enter **/reset** after the IP address of the VIP X1 XF (for example **192.168.0.10/reset**).

The new SSL certificate is valid.

Maintenance log

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

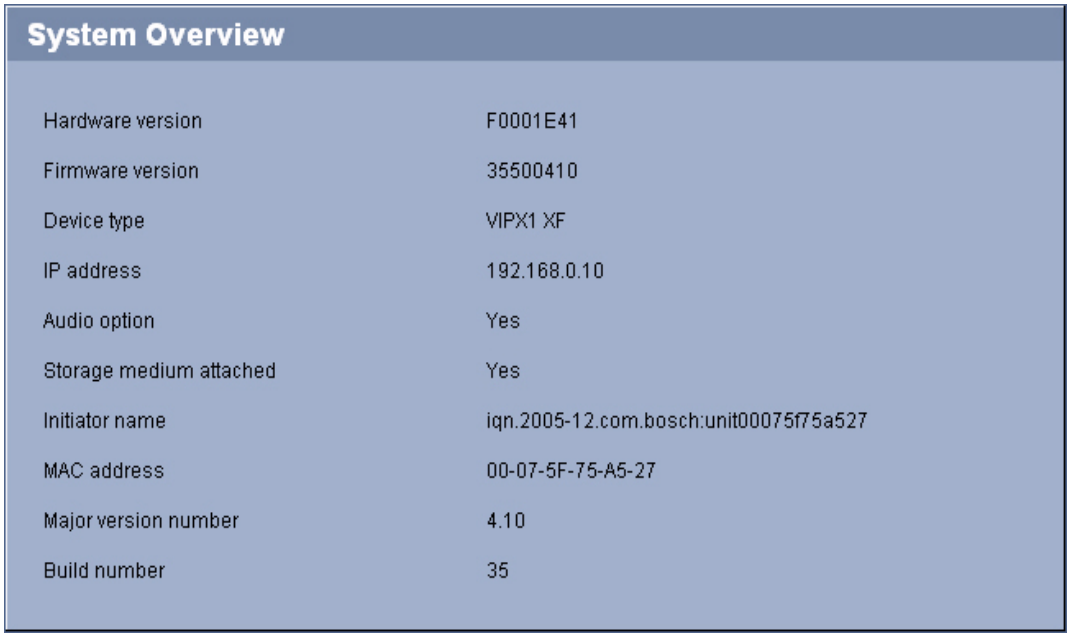
5.44 Advanced Mode: Licenses



You can enter the activation key to release additional functions or software modules.

NOTICE!
The activation key cannot be deactivated again and is not transferable to other units.

5.45 Advanced Mode: System Overview



The data on this page are for information purposes only and cannot be changed. Keep a record of these numbers in case technical assistance is required.

NOTICE!
You can select all required text on this page with the mouse and copy it to the clipboard with the [Ctrl]+[C] key combination, for example if you want to send it via e-mail.

5.46 Function Test

The VIP X1 XF offers a variety of configuration options. You should therefore check that it is functioning correctly after installation and configuration.
The function test is the only way to ensure that the VIP X1 XF operates as expected in the event of an alarm.
Your check should include the following functions:

- Can the VIP X1 XF be called up remotely?
- Does the VIP X1 XF transmit all the required data?
- Does the VIP X1 XF respond to alarm events as required?
- Do the recordings occur as intended?
- Is it possible to control peripherals if necessary?

6 Operation

6.1 Operation with Microsoft Internet Explorer

A computer with Microsoft Internet Explorer (version 7.0 or higher) can receive live images from the VIP X1 XF, control cameras or other peripherals and replay stored video sequences.

System Requirements

- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 7.0 or higher)
- Screen resolution at least 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM
- For playing back recordings: connection to storage medium

NOTICE!
Also note the information in the **System Requirements** document on the product CD supplied. If necessary, you can install the required programs and controls from the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).
The Web browser must be configured to enable Cookies to be set from the IP address of the unit.
In Windows Vista, deactivate protected mode on the **Security** tab under **Internet Options**.
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

Installing MPEG ActiveX

Suitable MPEG ActiveX software must be installed on the computer to allow the live video images to be played back. If necessary, you can install the program from the product CD supplied.

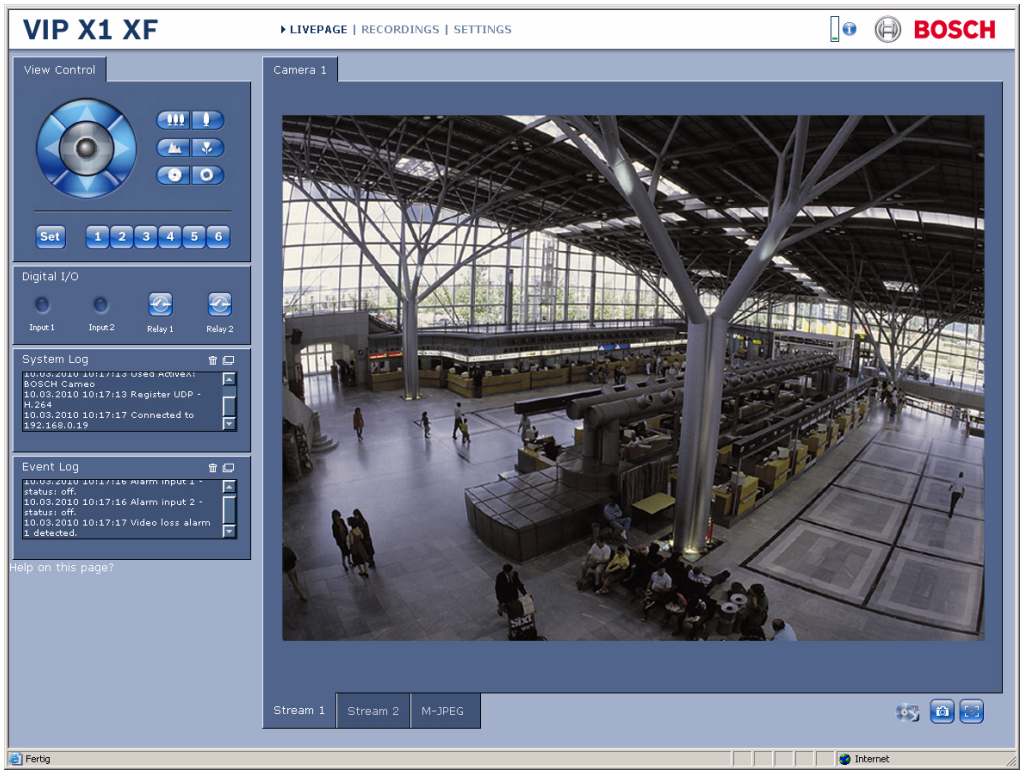
1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

Establishing the Connection

Before you can operate the VIP X1 XF within your network, it must have a valid IP address for your network and a compatible subnet mask.

The following default address is preset at the factory: **192.168.0.1**

1. Start the Web browser.
2. Enter the IP address of the VIP X1 XF as the URL. The connection is established and after a short time you will see the **LIVEPAGE** with the video image.



6.2 The LIVEPAGE

Once the connection is established, the Web browser displays the **LIVEPAGE**. 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 (see *Section 5.13 Advanced Mode: Display Stamping, page 37*).
Other information may be shown next to the live video image on the **LIVEPAGE**. The display depends on the settings on the **LIVEPAGE Functions** page (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).

Maximum Number of Connections
If you do not connect, the unit may have reached its maximum number of connections. Depending on the unit and network configuration, each VIP X1 XF can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

Protected VIP X1 XF
If the VIP X1 XF is password protected against unauthorized access, the Web browser displays a corresponding message and prompts you to enter the password when you attempt to access protected areas.

NOTICE!
A VIP X1 XF offers the option to limit the extent of access using various authorization levels (see *Section 5.11 Advanced Mode: Password, page 34*).

1. Enter the user name and associated password in the corresponding text fields.
2. Click **OK**. If the password is entered correctly, the Web browser displays the page that was called up.

Protected Network
If a RADIUS server is employed in the network for managing access rights (802.1x authentication), the VIP X1 XF must be configured accordingly, otherwise no communication is possible (see *Section Authentication, page 83*).

Image Selection
You can view the image of the camera in different displays.

▶ Click one of the tabs **Stream 1**, **Stream 2** or **M-JPEG** below the video image to toggle between the different displays of the camera image.

View Control

Control options for peripherals (for example a pan/tilt head or dome camera) depend on the type of unit installed and on the configuration of the VIP X1 XF.
If a controllable unit is configured and connected to the VIP X1 XF, the controls for the peripheral are displayed next to the video image.

1. To control a peripheral, click the appropriate controls.
2. Move the mouse cursor over the video image. Additional options for controlling peripherals are displayed with the mouse cursor.

Digital I/O

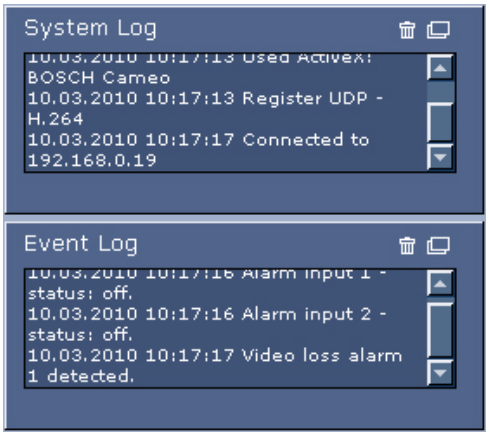
The alarm icons **Input 1** and **Input 2** are for information purposes and indicate the status of an alarm input: When an alarm is triggered, the corresponding icon lights up blue. The unit's configuration determines whether the alarm is displayed, as well as additional details (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).

Triggering Relay

You can switch connected units using the relays in the VIP X1 XF (for example lights or door openers).

▶ To activate this, click the icon for the corresponding relay next to the video image. The icon will be red when the relay is activated.

System Log / Event Log



The **System Log** field contains information about the operating status of the VIP X1 XF and the connection. You can save these messages automatically in a file (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).
Events such as the triggering or end of alarms are shown in the **Event Log** field. You can save these messages automatically in a file (see *Section 5.15 Advanced Mode: LIVEPAGE Functions, page 40*).

1. If you want to delete the entries, click the delete icon in the top right-hand corner of the relevant field.
2. If you want to view a detailed log, click the icon in the top right-hand corner of the relevant field. A new window will open.

Audio Function

Depending on the configuration, the VIP X1 XF can send and receive audio signals. All users who are connected by browsers receive the audio signals sent by the VIP X1 XF.
Audio signals can only be sent to the VIP X1 XF by the user who connects to the unit first.

1. On the **LIVEPAGE**, click anywhere next to the video image to remove the focus from the ActiveX.
2. Hold down the **F12** key to establish a voice connection with the VIP X1 XF. The browser's status bar displays the message **Send Audio ON**.
3. Release the **F12** key when you want to stop sending audio signals to the VIP X1 XF. The status bar in Internet Explorer displays the message **Send Audio OFF**.

NOTICE!
When the connection maintaining voice contact with the VIP X1 XF is broken, the next user to make a connection to the VIP X1 XF can send audio data to the VIP X1 XF.

6.3 Saving Snapshots

You can save individual images from the video sequence currently shown on the **LIVEPAGE** in JPEG format on your computer's hard drive. The icon for recording single images is only visible if the unit is configured to enable this process (see *Section Allow snapshots, page 41*).

▶ Click the icon. The image is saved at a resolution of 704 × 576 pixels (4CIF). The storage location depends on the configuration of the VIP X1 XF (see *Section Path for JPEG and video files, page 41*).

6.4 Recording Video Sequences

You can save sections of the video sequence currently shown on the **LIVEPAGE** on your computer's hard drive. The icon for recording video sequences is only visible if the unit is configured to enable this process (see *Section Allow local recording, page 41*).

1. Click the icon to start recording. The storage location depends on the configuration of the VIP X1 XF (see *Section Path for JPEG and video files, page 41*). A red dot in the icon indicates that recording is in progress.

2. Click the icon again to stop recording.

NOTICE!
You can play back saved video sequences using the Player program from Bosch Security Systems, which can be installed from the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).

Image Resolution
Sequences are saved at the resolution that has been preset in the configuration for the encoder (see *Section 5.19 Advanced Mode: Encoder Profile, page 45*).

6.5 Running Recording Program

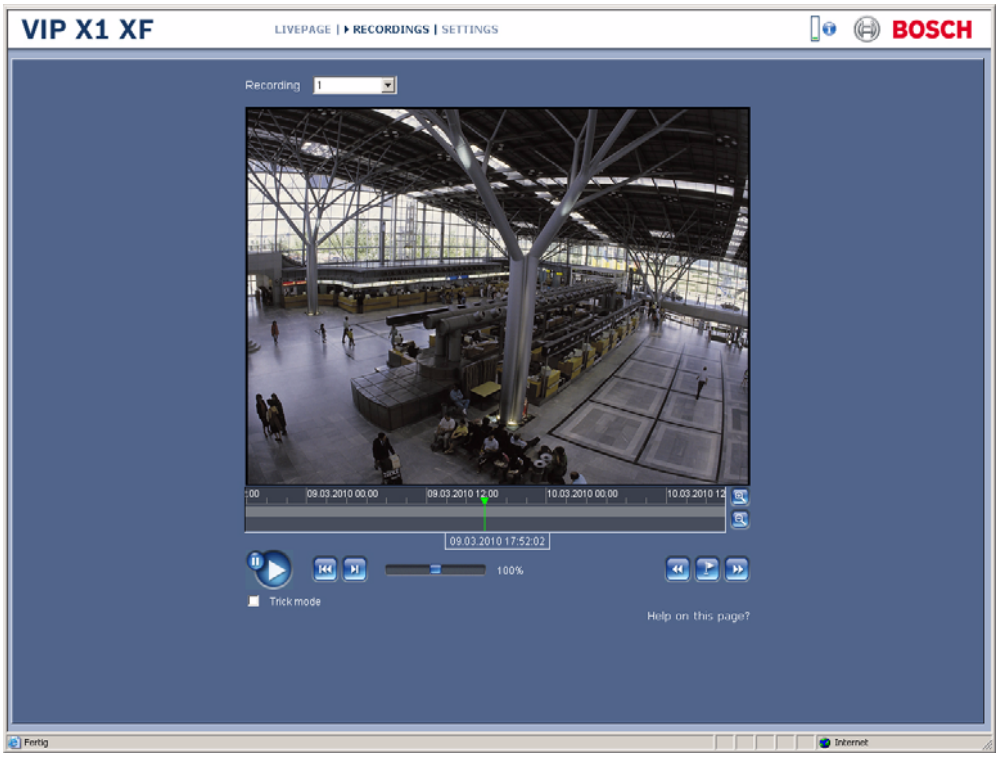
The hard drive icon below the camera images on the **LIVEPAGE** changes during an automatic recording.

A moving graphic will appear to indicate a running recording. If no recording is taking place, a static icon is displayed.

6.6 The RECORDINGS Page

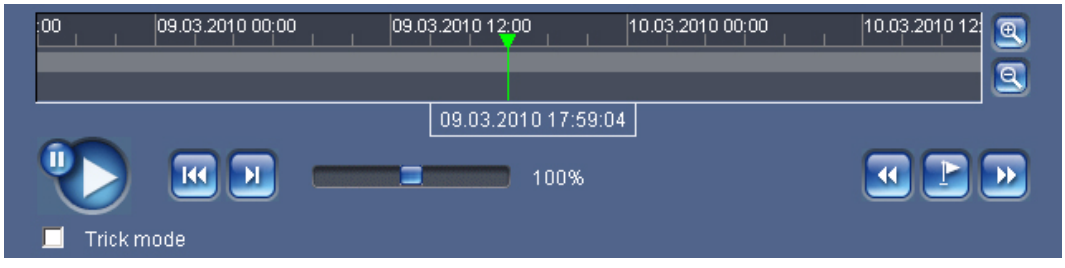
The **RECORDINGS** page for playing back recorded video sequences can be accessed from the **LIVEPAGE** and from the **SETTINGS** menu.
The **RECORDINGS** link is only visible if a storage medium has been selected (see *Section 5.22 Advanced Mode: Storage Management, page 51*).

▶ Click the **RECORDINGS** link in the navigation bar in the upper section of the window. The playback page appears.



Recording
Here you can select the recording that you want to view. Playback of the recording starts immediately in the video window. The contents of the recordings are identical. The quality or the storage location can vary.

Controlling a Playback



You will see a time bar below the video image for quick orientation. 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.
Red bars indicate the points in time where alarms were triggered. Drag the green arrow to navigate to these points quickly.

1. You can change the time interval by clicking the zoom keys (magnifying glass icons). The display can span a range from two months to a few seconds.
2. Drag the green arrow to the point in time at which playback should begin. The date and time display below the bar provides orientation to the second.

Buttons

You can control playback by means of the buttons below the video image. The buttons have the following functions:

Start or pause playback

Leap to the start of the active video sequence or to the previous sequence

Leap to the start of the next video sequence

Slide Control

You can use the slide control to control playback speed.

Bookmarks

In addition, you can set markers in the sequences, so-called bookmarks, and leap directly to these. 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

NOTICE!

Bookmarks are only valid while you are in the **RECORDINGS** page; they are not saved with the sequences. As soon as you leave the page all bookmarks are deleted.

Trick Mode

If you are using a mouse with a scroll wheel, you can view recordings frame by frame in trick mode. To do this, place the mouse cursor in the timeline below the timescale and turn the scroll wheel. Playback is automatically stopped (paused) during scrolling. Trick mode requires significantly higher memory capacity and computing power. For this reason, the number of cameras used in this mode can be restricted in the Configuration Manager program.

6.7 Installing Player

You can play back saved video sequences using the Player program from Bosch Security Systems, which can be found on the product CD supplied (see *Section 3.1 Scope of Delivery, page 9*).

NOTICE!
In order to play back saved sequences using Player, suitable MPEG ActiveX software must be installed on the computer.

1. Insert the CD into the computer's CD-ROM drive. If the CD does not start automatically, open the CD in Windows Explorer and double-click the **index.html** file to start the menu.
2. From the list field at the top, select the language you require and click **Tools** in the menu.
3. Click the **Archive Player** entry. The installation will start. Follow the instructions in the installation program. Archive Player is installed at the same time as Player.
4. After successful installation, you will find two new icons on your desktop for Player and Archive Player.
5. Start Player by double-clicking the **Player** icon.

6.8 Hardware Connections Between Video Servers

A VIP X1 XF with a camera connected to it can be used as a sender and a compatible hardware decoder (such as the VIP XD) with a connected monitor as a receiver using an Ethernet network connection. In this way it is possible to cover long distances without the need for major installation or cabling work.

NOTICE!
The sender and receiver must be located in the same subnet to establish a hardware connection.

Installation
Compatible video servers are designed to connect to one another automatically, provided they are correctly configured. They only need to be part of a closed network. Proceed as follows to install the units:

1. Connect the units to the closed network using Ethernet cables.
2. Connect them to the power supply.

NOTICE!
Make sure that the units are configured for the network environment and that the correct IP address for the remote location to be contacted in the event of an alarm is set on the **Alarm Connections** configuration page (see *Section 5.27 Advanced Mode: Alarm Connections, page 59*).

Connecting
There are three options for establishing a connection between a sender and a compatible receiver in a closed network:

– an alarm,
– a terminal program, or
– Internet Explorer.

NOTICE!
Connecting with a Web browser is described in the manual of the relevant unit that is to be used as the receiver, for example VIP XD.

Connecting on Alarm
With the appropriate configuration, a connection between a sender and a receiver is made automatically when an alarm is triggered (see *Section 5.27 Advanced Mode: Alarm Connections, page 59*). After a short time the live video image from the sender appears on the connected monitor.
This option can also be used to connect a sender and a compatible receiver using a switch connected to the alarm input. You do not need a computer to make the connection in this case.

Connecting with a Terminal Program

Various requirements must be met in order to operate with a terminal program (see *Section 8.9 Communication with Terminal Program, page 111*).

1. Start the terminal program and enter the command **4** in the main menu to switch to the **Rcp+** menu.
2. Enter the command **c** in the **Rcp+** menu to change the remote IP address, then enter the IP address of the unit you wish to connect to.
3. In the **Rcp+** menu, enter command **1** to activate automatic connection.

Closing the Connection with a Terminal Program

1. Start the terminal program and enter the command **4** in the main menu to switch to the **Rcp+** menu.
2. In the **Rcp+** menu, enter command **3** to deactivate automatic connection.

6.9 Operation Using Software Decoders

The video server VIP X1 XF provides a highly efficient systems solution together with the VIDOS software.
VIDOS is a software package for operating, controlling and managing CCTV installations (such as surveillance systems) at remote locations. It runs under Microsoft Windows operating systems. It is primarily designed for decoding video, audio and control data received from a remote sender.
There are many options available for operation and configuration when using a VIP X1 XF with VIDOS. Please refer to the software documentation for more details.

Another program that supports the VIP X1 XF is Bosch Video Management System.
Bosch Video Management System is an IP video security solution that enables the seamless management of digital video, audio and data over any IP network. It was developed for use with Bosch CCTV products as one component of an extensive video security management system. It allows you to integrate your existing components into a simple-to-control system or into the entire Bosch range, benefiting from a complete security solution based on the latest technology and years of experience.

The VIP X1 XF video server is also designed for use with the DiBos 8 digital recorder.
DiBos 8 records up to 32 video and audio streams and is available as IP software or hybrid DVR with additional analog camera and audio inputs. DiBos supports the most diverse functions on the VIP X1 XF video server, for example relay activation, remote control of peripherals and remote configuration. DiBos 8 can use the alarm inputs for event triggering and, on release of the MOTION+ motion detector, record the activated cells to enable intelligent motion search.

7 Maintenance and Upgrades

7.1 Testing the Network Connection

You can use the **ping** command to check the connection between two IP addresses. This allows you to test whether a unit in the network is active.

1. Open the DOS command prompt.
2. Type **ping** followed by the IP address of the unit.

If the unit is found, the response appears as **Reply from ...** followed by the number of bytes sent and the transmission time in milliseconds. If not, the unit cannot be accessed over the network. This might be because:

– The unit is not correctly connected to the network. Check the cable connections in this case.
– The unit is not correctly integrated into the network. Check the IP address, subnet mask and gateway address.

7.2 Unit Reset

You can use the Factory Reset button to restore the unit to its original settings. Any changes to the settings are overwritten by the factory defaults. A reset may be necessary, for example, if the unit has invalid settings that prevent it from functioning as desired.

CAUTION!
All configured settings will be discarded during a reset.
If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.43 Advanced Mode: Maintenance, page 86*).

NOTICE!
After a reset, the unit can only be addressed via the factory default IP address. The IP address can be changed as described in the **Installation** chapter (see *Section 4.5 Setup Using Configuration Manager, page 19*).

1. If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.43 Advanced Mode: Maintenance, page 86*).
2. Using a pointed object, press the Factory Reset button located below the SD slot until the **POWER** LED flashes red (see *Section 3.4 Connections, Controls and Displays, page 14*). All settings will revert to their defaults.
3. Change the IP address of the VIP X1 XF if necessary.
4. Configure the unit to meet your requirements.

7.3 Repairs

CAUTION!
Never open the housing of the VIP X1 XF.
The unit does not contain any user-serviceable parts.

Ensure that all maintenance or repair work is carried out only by qualified personnel (electrical engineers or network technology specialists). In case of doubt, contact your dealer's technical service center.

7.4 Transfer and Disposal

The VIP X1 XF should only be passed on together with this installation and operating manual. Your Bosch product is designed and manufactured with high-quality materials and components which can be recycled and reused.

This symbol means that electrical and electronic equipment, at their end-of-life, should be disposed of separately from your household waste.
In the European Union, there are separate collection systems for used electrical and electronic products. Please dispose of this equipment at your local community waste collection/recycling center.

8 Appendix

8.1 Troubleshooting

If you are unable to resolve a malfunction, please contact your supplier or systems integrator, or go directly to Bosch Security Systems Customer Service.
You can view a range of information about your unit version on the **System Overview** page (see *Section 5.45 Advanced Mode: System Overview, page 88*). Make a note of this information before contacting Customer Service. You can download an internal maintenance log from the unit on the **Maintenance** page if you wish to send it to Customer Service by e-mail (see *Section Maintenance log, page 87*).

The following tables are intended to help you identify the causes of malfunctions and correct them where possible.

8.2 General Malfunctions

Malfunction	Possible causes	Recommended solution
No connection between the unit and terminal program.	Incorrect cable connections.	Check all cables, plugs, contacts, terminals and connections.
	The computer's serial interface is not connected.	Check the other serial interface.
	Interface parameters do not match.	If necessary select a different interface and make sure that the computer's interface parameters match those of the unit. Try the following standard parameters: 19,200 baud, 8 data bits, no parity, 1 stop bit. Next, disconnect the unit from the power supply and reconnect it again after a few seconds.
No image transmission to remote station.	Camera error.	Connect local monitor to the camera and check the camera function.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
	Incorrect encoder stream property set for connection to hardware decoder.	Select the **H.264 BP+ (HW decoder)** option on the **Encoder Streams** configuration page.
No connection established, no image transmission.	The unit's configuration.	Check all configuration parameters.
	Faulty installation.	Check all cables, plugs, contacts and connections.
	Wrong IP address.	Check the IP addresses (terminal program).
	Faulty data transmission within the LAN.	Check the data transmission with **ping**.
	The maximum number of connections has been reached.	Wait until there is a free connection and then call the sender again.
No audio transmission to remote station.	Hardware fault.	Check that all connected audio units are operating correctly.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
	Incorrect configuration.	Check audio parameters on the **Audio** configuration and **LIVEPAGE Functions** pages.
	The audio voice connection is already in use by another receiver.	Wait until the connection is free and then call the sender again.

Malfunction	Possible causes	Recommended solution
The unit does not report an alarm.	Alarm source is not selected.	Select possible alarm sources on the **Alarm Inputs** configuration page.
	No alarm response specified.	Specify the desired alarm response on the **Alarm Connections** configuration page, change the IP address if necessary.
Control of cameras or other units is not possible.	The cable connection between the serial interface and the connected unit is not correct.	Check all cable connections and ensure all plugs are properly fitted.
	The interface parameters do not match those of the other unit connected.	Make sure that the settings of all units involved are compatible.
The unit is not operational after a firmware upload.	Power failure during programming by firmware file.	Have the unit checked by Customer Service and replace if necessary.
	Incorrect firmware file.	Enter the IP address of the unit followed by **/main.htm** in your Web browser and repeat the upload.
Placeholder with a red cross instead of the ActiveX components.	JVM not installed on your computer or not activated.	Install Sun JVM from the product CD.
Web browser contains empty fields.	Active proxy server in network.	Create a rule in the local computer's proxy settings to exclude local IP addresses.
The **POWER** LED flashes red.	Firmware upload failed.	Repeat firmware upload.

8.3 Malfunctions with iSCSI Connections

Malfunction	Possible causes	Recommended solution
After connecting to the iSCSI destination, no LUNs are displayed.	Incorrect LUN mapping during iSCSI system configuration.	Check the iSCSI system configuration and reconnect.
After connecting to the iSCSI destination, "LUN FAIL" appears below a node.	The LUN list could not be read, as it was assigned to the wrong network interface.	Check the iSCSI system configuration and reconnect.
LUN mapping is not possible.	Some iSCSI systems do not support the use of an initiator extension.	Delete the initiator extension on the **Identification** configuration page.

8.4 LEDs

The VIP X1 XF network video server has LEDs on its front and rear panels that show the operating status and can give indications of possible malfunctions:

POWER LED

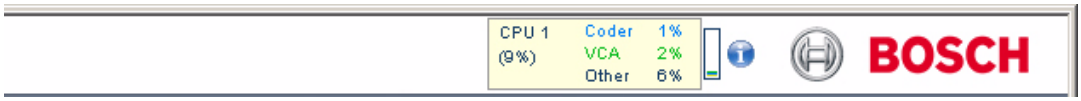
Does not light up:	VIP X1 XF is switched off.
Lights up green:	VIP X1 XF is switched on.
Lights up red:	Startup in progress.
Flashes green:	Video connection established.
Flashes red:	VIP X1 XF is faulty, for example following failed firmware upload.

10/100 Base-T RJ45 Socket

Green LED lights up:	Network connection established.
Orange LED lights up:	Data transmission via network connection.

8.5 Processor Load

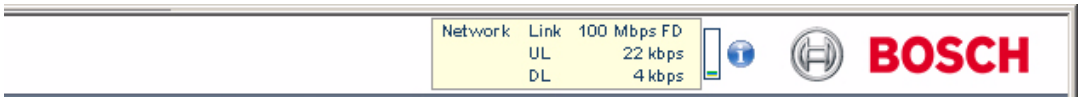
If the VIP X1 XF is accessed via the Web browser, you will see the processor load indicator in the top left of the window next to the manufacturer's logo.



You can obtain additional information to help you when troubleshooting or fine tuning the unit. The values indicate the proportions of the individual functions on the encoder load, shown as percentages.

▶ Move the cursor over the graphic indicator. Some additional numerical values are also displayed.

8.6 Network Connection



You can display information about the network connection. To do this, move the cursor over the **i** icon.

Link	Ethernet link type
UL	Uplink, speed of the outgoing data traffic
DL	Downlink, speed of the incoming data traffic

8.7 Serial Interface

Options for using the serial interface include transferring transparent data, controlling connected units or operating the unit with a terminal program.
The serial interface supports the RS-232, RS-422 and RS-485 transmission standards. The mode used depends on the current configuration (see *Section 5.37 Advanced Mode: COM1, page 77*). Connection is via the terminal block.

8.8 Terminal Block

The terminal block has several contacts for:

– 2 alarm inputs
– 2 relay outputs
– Serial data transmission

Pin Assignment

The pin assignment of the serial interface depends on the interface mode used (see *Section 5.37 Advanced Mode: COM1, page 77*).

Contact	RS-232 mode	RS-422 mode	RS-485 mode
CTS	—	RxD- (receive data minus)	
TXD	TxD (transmit data)	TxD- (transmit data minus)	Data-
RTS	—	TxD+ (transmit data plus)	Data+
RXD	RxD (receive data)	RxD+ (receive data plus)	
GND	GND (ground)	—	—

Contact	Function
IN1	Input alarm 1
IN2	Input alarm 2
GND	Ground
R1	Relay output 1
R2	Relay output 2
GND	Ground
VIN	9 to 30 V DC (power supply)
GND	Ground

Connect each alarm input to a ground contact (GND) when connecting alarm inputs.

8.9 Communication with Terminal Program

Data Terminal

If a VIP X1 XF cannot be found in the network or the connection to the network is interrupted, you can connect a data terminal to the VIP X1 XF for initial setup and setting of important parameters. The data terminal consists of a computer with a terminal program.

You require a serial transmission cable with a 9-pin Sub-D plug to connect to the computer and open ends for connection to the terminal block of the VIP X1 XF (see *Section Pin Assignment, page 110*).

HyperTerminal, a communications accessory included with Microsoft Windows, can be used as the terminal program.

NOTICE!

Information on installing and using HyperTerminal can be found in the manuals or in the online help for Microsoft Windows.

1. Disconnect the VIP X1 XF from the Ethernet network before working with the terminal program.
2. Connect the serial interface of the VIP X1 XF using any available serial interface on the computer.

Configuring the Terminal

Before the terminal program can communicate with the VIP X1 XF, the transmission parameters must be matched. Make the following settings for the terminal program:

– 19,200 bps
– 8 data bits
– No parity check
– 1 stop bit
– No protocol

Command Inputs

After the connection has been established, you must log on to the VIP X1 XF to access the main menu. Other submenus and functions can be accessed using the on-screen commands.

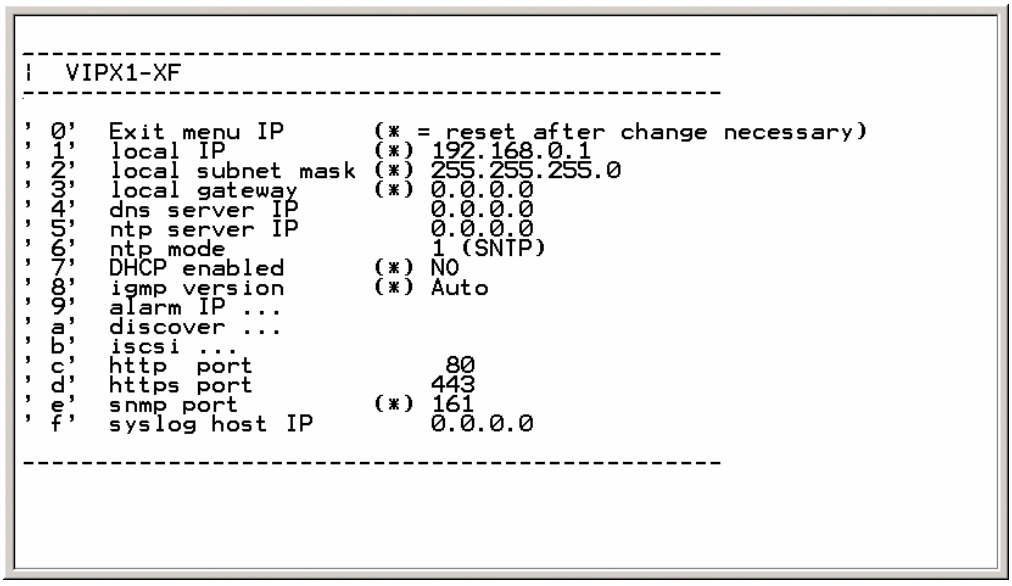
1. If necessary, turn off the local echo so that entered values are not repeated on the display.
2. Enter one command at a time.
3. When you have entered a value, such as the IP address, check the characters you have entered before pressing Enter to transfer the values to the VIP X1 XF.

Assigning an IP Address

Before you can operate a VIP X1 XF in your network you must first assign it an IP address that is valid for your network.

The following default address is preset at the factory: **192.168.0.1**

1. Start a terminal program such as HyperTerminal.
2. Enter the user name **service**. The terminal program displays the main menu.
3. Enter command **1** to open the **IP** menu.



4. Enter **1** again. The terminal program displays the current IP address and prompts you to enter a new IP address.
5. Enter the desired IP address and press Enter. The terminal program displays the new IP address.
6. Use the displayed commands for any additional settings you require.

NOTICE!

You must reboot to activate the new IP address, a new subnet mask or a gateway IP address.

Reboot

Briefly interrupt the power supply to the VIP X1 XF for a reboot (disconnect the power supply unit from the mains supply and switch on again after a few seconds).

Additional Parameters

You can use the terminal program to check other basic parameters and modify them where necessary. Use the on-screen commands in the various submenus to do this.

8.10 Copyrights

The firmware 4.1 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.

9 Specifications

9.1 Unit

Operating voltage	9 to 30 V DC, power supply via external unit
Power consumption	Approx. 5 VA
LAN interfaces	1 × Ethernet 10/100 Base-T, automatic adjustment, half/full duplex, RJ45
Data interfaces	1 × RS-232/RS-422/RS-485, bidirectional, push-in terminal
SD Slot	1 × SD CARD, for standard SD cards or SDHC up to 32 GB
Alarm inputs	2 × push-in terminals (non-isolated closing contact), maximum activation resistance 10 Ohm
Relay outputs	2 × push-in terminals, 30 V_{p-p}, 200 mA (SELV), 4 contacts
Video Input	1 × BNC socket 0.7 to 1.2 V_{p-p}, 75 Ohm, PAL/NTSC
Audio input (LINE IN)	1 × 3.5 mm stereo socket 5.5 V_{p-p} max., impedance 9 kOhm typ.
Audio output (LINE OUT)	1 × 3.5 mm stereo socket 3.0 V_{p-p} max., impedance 16 kOhm min.
Displays	1 × LED (operation) on the front panel, 2 × LED (network connection, data transfer) on the rear panel
Thermal value	17 BTU/h max.
Operating conditions	Temperature: 0 to +50 °C / +32 to +122 °F relative humidity: 0 to 95%, non-condensing
Approvals	IEC 60950-1; EN 50130-4; EN 50130-5; EN 50130-4/13; EN 50121; EN 55103-1; EN 55103-2; EN 55022; EN 61000-3-2; EN 61000-3-3; EN 61000-4-5; FCC 47 CFR Chapter B Part 15; AS/NZS CISPR22
Dimensions (H × W × D)	36 × 88 × 118 mm / 1.4 × 3.5 × 4.7 in, including BNC connections
Weight	Approx. 0.25 kg / 0.55 lb

9.2 Protocols/Standards

Video standards	PAL, NTSC
Video coding protocols	H.264 MP (Main Profile), H.264 BP+, M-JPEG, JPEG
Video data rate	9.6 kbps to 6 Mbps
Image resolutions (PAL/NTSC)	704 × 576/480 pixels (4CIF) 352 × 288/240 pixels (CIF)
Total delay	120 ms (PAL/NTSC, H.264, no network delay)
Image refresh rate	25/30 ips max.
Network protocols	RTP, Telnet, UDP, TCP, IP, HTTP, HTTPS, FTP, DHCP, IGMP V2, IGMP V3, ICMP, ARP, SMTP, SNTP, SNMP, 802.1x
Audio coding protocol	G.711, 300 Hz to 3.4 kHz
Audio sampling rate	8 kHz
Audio data rate	80 kbps

Glossary

0...9

10/100/1000 Base-T	IEEE-802.3 specification for 10, 100 or 1000 Mbps Ethernet
802.1x	The IEEE 802.1x standard provides a general method for authentication and authorization in IEEE-802 networks. Authentication is carried out via the authenticator, which checks the transmitted authentication information using an authentication server (*see* RADIUS server) and approves or denies access to the offered services (LAN, VLAN or WLAN) accordingly.

A

ARP	Address Resolution Protocol: a protocol for mapping MAC and IP addresses

B

Baud	Unit of measure for the speed of data transmission
bps	Bits per second, the actual data rate
BVIP	Bosch Video over IP unit

C

CF	CompactFlash; interface standard, for digital storage media amongst other things. Used in computers in the form of CF cards, digital cameras and Personal Digital Assistants (PDA).
CIF	Common Intermediate Format, video format with 352 × 288/240 pixels

D

DHCP	Dynamic Host Configuration Protocol: uses an appropriate server to enable dynamic assignment of an IP address and other configuration parameters to computers on a network (Internet or LAN)
DNS	Domain Name System, mainly used for converting domain names to IP addresses
DynDNS	DNS hosting service that works according to RFC 2845 and stores the IP addresses of its clients in a database, ready for use

F

FTP	File Transfer Protocol
Full duplex	Simultaneous data transmission in both directions (sending and receiving)

G

GBIC	GigaBit Interface Converter; applied in network technology to render interfaces flexible, for converting an electrical interface into an optical interface, for example. This enables flexible operation of an interface as a Gigabit Ethernet via twisted-pair cables or fiber optic cables.
GOP	Group of Pictures

H

H.264	Standard for high-efficiency video compression, based on the predecessors MPEG-1, MPEG-2 and MPEG-4. H.264 typically achieves a coding efficiency around three times as high as MPEG-2. This means that comparable quality can be achieved at around a third of MPEG-2 data quantity.
HTTP	Hypertext Transfer Protocol: protocol for transmitting data over a network
HTTPS	Hypertext Transfer Protocol Secure: encrypts and authenticates communication between Web server and browser

I

ICMP	Internet Control Message Protocol
ID	Identification: a machine readable character string
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
Internet Protocol	The main protocol used on the Internet, normally in conjunction with the Transfer Control Protocol (TCP): TCP/IP
IP	*See* Internet Protocol
IP address	A 4-byte number uniquely defining each unit on the Internet. It is usually written in dotted decimal notation, for example "209.130.2.193"
iSCSI	Storage over IP process for storage networks; specifies how storage protocols are operated over IP
ISDN	Integrated Services Digital Network

J

JPEG	An encoding process for still images (Joint Photographic Experts Group)

K

kbps	Kilobits per second, the actual data rate

L

LAN	*See* Local Area Network
Local Area Network	A communications network serving users within a limited geographical area such as a building or university campus. It is controlled by a network operating system and uses a transfer protocol.
LUN	Logical Unit Number; logical drive in iSCSI storage systems

M

MAC	Media Access Control

MIB	Management Information Base; a collection of information for remote servicing using the SNMP protocol
MPEG-2	Improved video/audio compression standard, compression on highest level allows images in studio quality; now established as broadcast standard
MPEG-4	A further development of MPEG-2 designed for transmitting audiovisual data at very low transfer rates (for example over the Internet)
MSS	Maximum Segment Size; maximum byte figure for the user data in a data packet

N

Net mask	A mask that explains which part of an IP address is the network address and which part is the host address. It is usually written in dotted decimal notation, for example "255.255.255.192."
NTP	Network Time Protocol; a standard for synchronizing computer system clocks via packet-based communication networks. NTP uses the connectionless network protocol UDP. This was developed specifically for enabling time to be reliably transmitted over networks with variable packet runtime (Ping).

O

OF	Optical Fiber; now used predominantly as the transmission medium for line-borne telecommunication processes (glass fiber cable)

P

Parameters	Values used for configuration

Q

QCIF	Quarter CIF, video format with 176 × 144/120 pixels

R

RADIUS server	Remote Authentication Dial-In User Service: a client/server protocol for the authentication, authorization and accounting of users with dial-up connections on a computer network. RADIUS is the de-facto standard for central authentication of dial-up connections via Modem, ISDN, VPN, Wireless LAN (*see* 802.1x) and DSL.
RFC 868	A protocol for synchronizing computer clocks over the Internet
RS-232/-422/-485	Standards for serial data transmission
RTP	Real-Time Transport Protocol; a transmission protocol for real-time video and audio
RTSP	Real-Time Streaming Protocol; network protocol for controlling the continuous transmission of audiovisual data (streams) or software over IP-based networks

S

SD card	Secure Digital Memory Card; digital memory card that works on the flash principle

SFP	Small Form-factor Pluggable; small, standardized module for network connections, designed as a plug connector for high-speed network connections
SNIA	Storage Networking Industry Association; association of companies for defining the iSCSI standard
SNMP	Simple Network Management Protocol; a protocol for network management, for managing and monitoring network components
SNTP	Simple Network Time Protocol; a simplified version of NTP (*see* NTP)
SSL	Secure Sockets Layer; an encryption protocol for data transmission in IP-based networks
Subnet mask	*See* Net mask

T

TCP	Transmission Control Protocol
Telnet	Login protocol with which users can access a remote computer (Host) on the Internet
TLS	Transport Layer Security; TLS 1.0 and 1.1 are the standard advanced developments of SSL 3.0 (*see* SSL)
TTL	Time-To-Live; life cycle of a data packet in station transfers

U

UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair

W

WAN	*See* Wide Area Network
Wide Area Network	A long distance link used to extend or connect remotely located local area networks

Index

N

O

P

R

S

T

U

V

W

Bosch Sicherheitssysteme GmbH
Werner-von-Siemens-Ring 10
85630Grasbrunn
Germany
www.boschsecurity.com