VideoJet XTC XF

VJT-XTCXF

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 VideoJet XTC XF transcoder. 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 VideoJet XTC XF video transcoder transfers video and control signals over data networks (Ethernet LAN, Internet). It enables HD video to be seen over wide area networks or through mobile access in original quality. 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
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

1.4 EU Directives

The VideoJet XTC XF video transcoder 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 the power supply provided or 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.
- When installing in a switch cabinet, ensure that the unit and the power supply units have sufficient grounding.
- 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.
- 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. Bear the total heat output in mind, particularly when installing multiple units in a switch cabinet.
  - 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.
  - When installing in a switch cabinet, ensure that the screw joints are free of tension and subject to as little mechanical stress as possible. Ensure that the unit and the power supply units have sufficient grounding.

2.3 Maintenance and repair

- Never open the housing of the unit. 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). In case of doubt, contact your dealer's technical service center.

3 Product description

3.1 Parts included

- 1 VideoJet XTC XF video transcoder
- 2 terminal blocks (6-pin, 8-pin)
- 4 self-adhesive elastic bumpers
- 1 wall-mounting panel
- 2 screws
- 2 wall plugs
- 1 power supply unit with 3 primary adapters (EU, US, UK)
- 1 Quick Installation Guide
- 1 Safety Hints document

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 7 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 **Releaseletter** document for the respective firmware. For the latest version of the firmware, required programs and controls, and the current version of the Bosch Video Client (BVC) management software, access your Bosch product catalog on the Internet.
The Web browser must be configured to enable cookies to be set from the IP address of the unit.
In Windows 7, 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 9.0 or higher)
  or
- Installed Configuration Manager application (latest version)

Additional operational requirements

- Microsoft Internet Explorer (version 9.0 or higher)
  or
- Receiver software, for example the latest version of
  - Bosch Video Client
  - Bosch Video Management System
  - Bosch Video Security iPad app
- For playing back recordings: connection to storage medium

3.3 Overview of functions

Network video server
The VideoJet XTC XF is a compact video transcoder that enables HD video to be seen over wide area networks or through mobile access in original quality. It provides two independent transcoded streams, enabling live viewing access to two HD cameras or playback of their recordings simultaneously, regardless of the network bandwidth. Having found an event or a point of interest, pausing the replay causes Instant Display Enhancement to present the HD image in its original recording quality.
Its Dynamic Transcoding functionality makes it the ideal entrance door for central monitoring systems to remote HD camera sites, or for remote clients to small business HD video surveillance installations.
Its transcoding services seamlessly integrate with VRM Video Recording Manager installations, enabling e.g. mobile access for on-site guards to HD video, both live and playback.

Flexibility
VideoJet XTC XF transcoders offer local recording for up to four connected HD cameras on CompactFlash, or network-attached RAID iSCSI storage devices. The built-in iSCSI support enables the VideoJet XTC XF transcoders to act as conventional DVRs while providing transcoded HD video across any bandwidth-type of network.

Transcoding
The transcoder features eight profiles that can be predefined for various types of network connections. These profiles, selectable on the playback page, provide a quick and easy adaptation to the available bandwidth.

Viewing
View the VideoJet XTC XF transcoder video with the Bosch Video Security app for iOS devices like Apple iPad, on a PC using a Web browser, in the Bosch Video Management System, or integrate it into another video management system.
Adaptive Bit Rate encoding enables viewing from remote sites over bandwidth-limited connections and wireless connections to mobile clients.
Latest HTML5 technologies provide easy access from Android, Windows Phone and iOS based mobile devices.

Region of interest (ROI)
Get every detail even on lower bandwidth or smaller video window by panning, tilting and zooming a region-of-interest cut-out from the full image. ROI is possible on both live viewing and playback of recordings.

Advanced remote playback
Bosch’s latest enhancements—Adaptive Bit Rate encoding and transcoding—allow replay of recordings over bandwidth-limited connections with smooth browsing through the footage while not missing any detail. Be it a remote guard searching for a specific evidence or alerted by alarm notification, quick access to the relevant recording is easily achieved, and recorded images are presented in original quality even over weak links.

Access security
The VideoJet XTC XF transcoders offer various security levels for accessing the network, the unit, and the data channels. As well as password protection with three levels, they support 802.1x authentication using a RADIUS server for identification. You can secure Web browser access by HTTPS using a SSL certificate that is stored in the unit. For total data protection,

each communication channel—video or serial I/O—can be independently AES encrypted with 128-bit keys, once the Encryption Site License has been applied.

Forensic Search

The VideoJet XTC XF transcoders provide Forensic Search in the recordings of its assigned IVA-enabled cameras. Simple line and field definitions, drawn over the video image, allow quick and efficient search through the metadata of camera recordings.Forensic Search is possible via the Bosch Video Security app as well as the Web browser playback interface.

ONVIF conformance

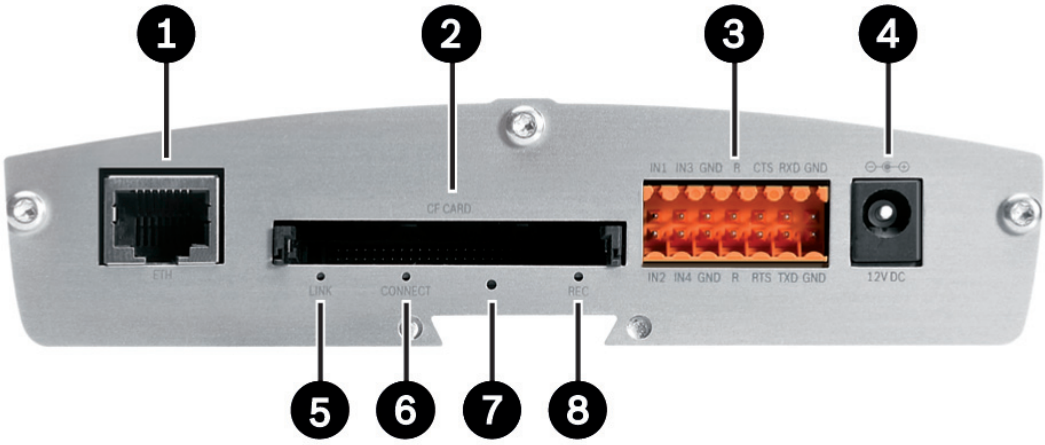
VideoJet XTC XF conforms to ONVIF 1.02 and ONVIF Profile S, providing interoperability between network video products regardless of manufacturer. In addition, its firmware supports all applicable features of the ONVIF 2.2 specification.
ONVIF conformant devices are able to exchange live video, audio, metadata and control information and ensure that they are automatically discovered and connected to network applications such as video management systems.

Summary

The VideoJet XTC XF transcoders provide the following main functions:

- Video and data transmission over IP data networks especially for bandwidth-limited links
- Two independent transcoder channels
- Video transcoding to international standard H.264
- Integrated Ethernet port (10/100 Base-T)
- CF slot for standard Type I/II CompactFlash memory card 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
- Four alarm inputs and one relay output
- Convenient maintenance via uploads
- Flexible encryption of control and data channels
- Authentication according to international standard 802.1x

3.4 Connections, controls and displays



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

2 **CF CARD** slot
for one standard Type I/II CompactFlash memory card

3 Terminal block
for alarm inputs, relay output and serial interface

4 **12V DC** power connector
for connecting the power supply unit

5 **LINK** LED
lights up when the unit is connected to the network

6 **CONNECT** LED
lights up when supplied with power and during data transmission

7 Factory reset button
to restore factory default settings

8 **REC** LED
flashes during recordings

Further topics:

– *Section 8.4 LEDs, page 67*
– *Section 8.7 Terminal block, page 68*

4 Installation

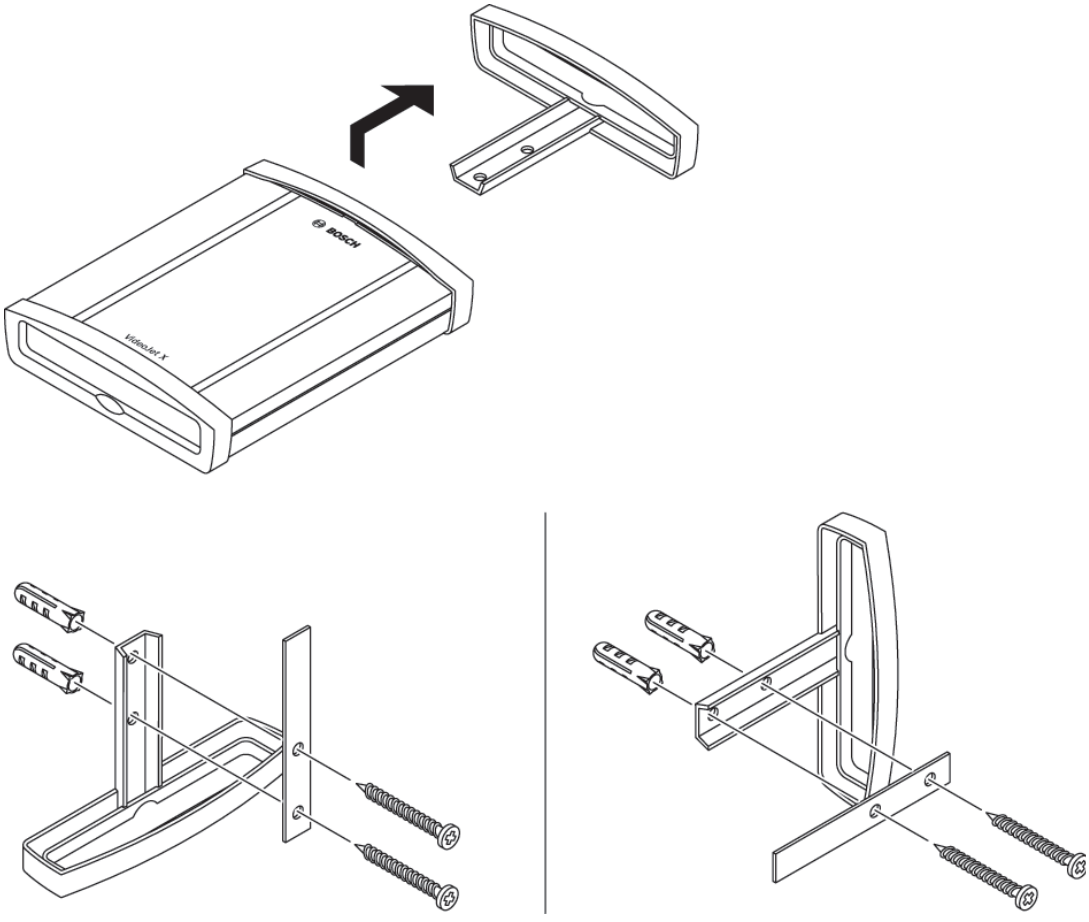
4.1 Preparations

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 for the delivered power supply unit must be between 0 and +40 °C (+32 and +104 °F). The relative humidity must be between 20% and 80%, non-condensing. The ambient temperature for the VideoJet XTC XF transcoder must be between 0 and +50 °C (+32 and +122 °F). The relative humidity must not exceed 90%, non-condensing. The transcoder 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. During installation, please note the maximum heat value of 31 BTU/h per unit without the power supply.

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. Bear the total heat output in mind, particularly when installing multiple units in a switch cabinet.
- 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.
- When installing in a switch cabinet, ensure that the screw joints are free of tension and subject to as little mechanical stress as possible. Ensure that the unit and the power supply units have sufficient grounding.
- Avoid impacts, blows and severe vibrations that exceed the specification limits, as these can irreparably damage the unit.

Further topics:
- *Section 9 Specifications, page 70*

4.2 Mounting



You can secure the VideoJet XTC XF transcoder 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 Installing in a switch cabinet

4.3.1 Preparations

The VideoJet XTC XF transcoder can be installed in a 19-inch rack. A Rack Mount Kit for the installation of up to three units can be obtained from Bosch. For more information access your Bosch product catalog on the Internet.

CAUTION!

When installing in a switch cabinet, ensure that there is sufficient ventilation for the unit. The transcoder generates heat during operation. During installation, please note the maximum heat value of 31 BTU/h per unit without the power supply.

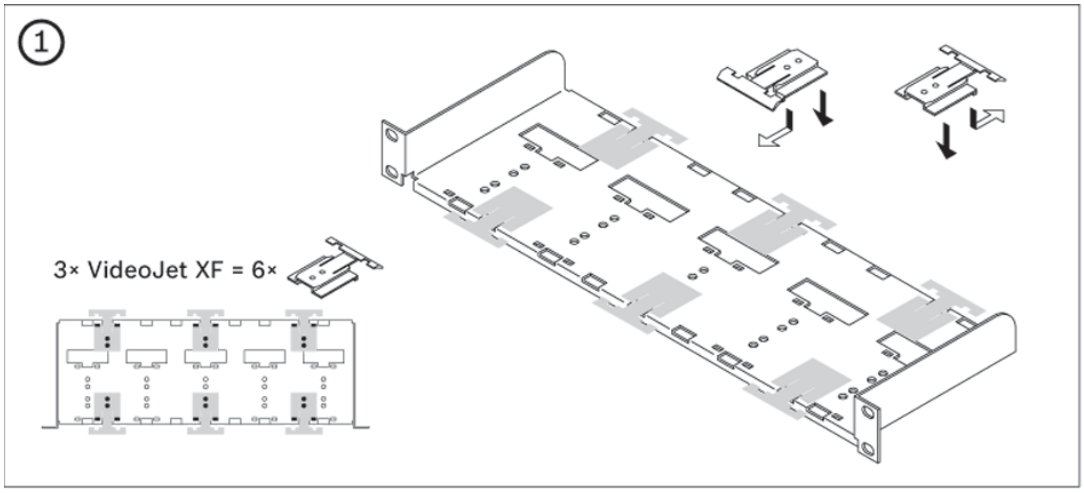
The ambient temperature for the delivered power supply unit must be between 0 and +40 °C (+32 and +104 °F). The relative humidity must be between 20% and 80%, non-condensing.

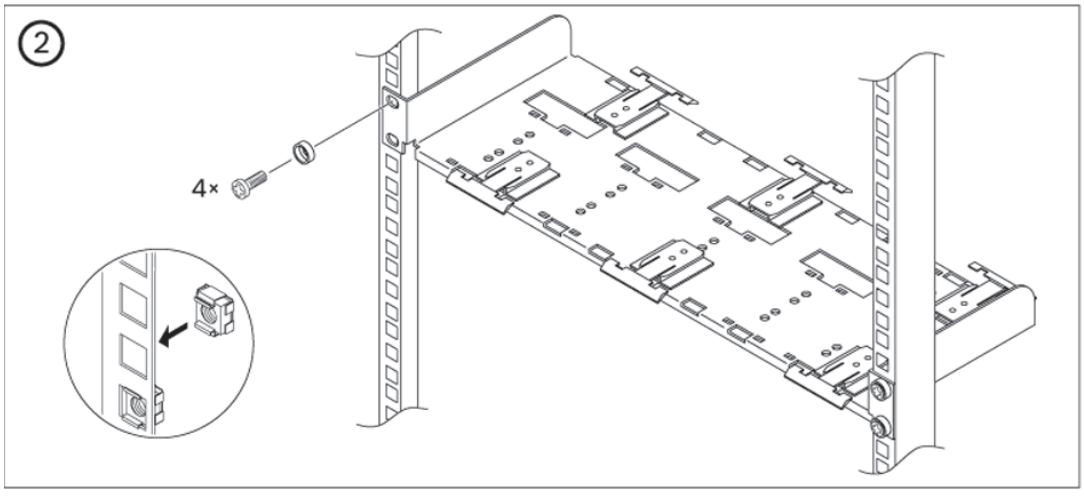
The ambient temperature for the VideoJet XTC XF transcoder must be between 0 and +50 °C (+32 and +122 °F). The relative humidity must not exceed 90%, non-condensing.

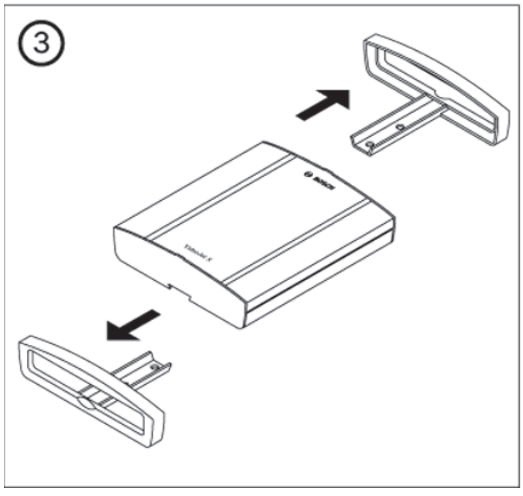
When installing in a switch cabinet, ensure that the screw joints are free of tension and subject to as little mechanical stress as possible. Ensure that the unit and the power supply units have sufficient grounding.

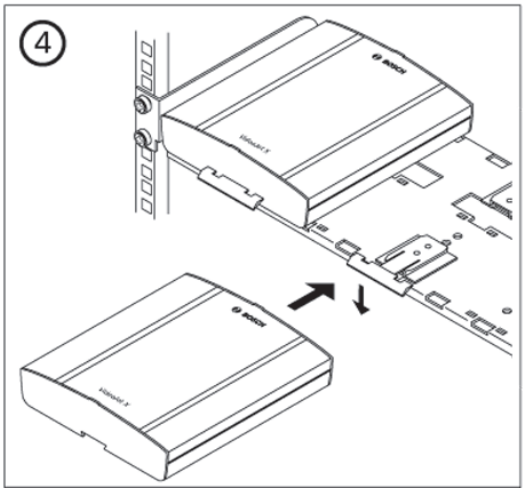
4.3.2 Installing the unit

1. Install the required number of fixing plates, two for each unit.
2. Prepare the switch cabinet in such a manner that you are easily able to insert the rack mount frame directly at the installation point.
3. Place the cage nuts in the corresponding drillings or spaces in the switch cabinet frame.
4. Lift the empty rack mount frame into the switch cabinet frame and insert the fastening screws together with the washers.
5. Tighten the screws one after the other and then check once more that all the screws are tight.
6. Remove the plastic frames from both sides of each unit to be installed.
7. Slide each unit onto the corresponding fixing plates until you feel it lock securely into place.


1
3× VideoJet XF = 6×


2
4×


3


4

4.4 Connections

Network

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

▶ Connect the unit to the network via the **ETH** socket.

CF slot

You can insert a standard Type I/II CompactFlash memory card into the **CF CARD** slot to enable recordings to be saved locally. CF cards are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings of the connected cameras.

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

1. Carefully slide the CF card into the slot as far as it will go, until it locks into place.
2. To remove the CF card, pull and remove the card.

Data interface

The connection supports the RS-232, RS-422 and RS-485 transmission standards. A video connection is necessary to transmit transparent data.
The transcoder offers the serial interface via the orange terminal block.
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.

Further topics:

– *Section 8.7 Terminal block, page 68*

Alarm inputs

The VideoJet XTC XF transcoder has four alarm inputs on the orange terminal block. The alarm inputs are used to connect to external alarm devices such as door contacts or sensors. Sophisticated alarm handling requires scripting using Alarm Task Editor.
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 **IN1** to **IN4** on the orange terminal block and check that the connections are secure.

Further topics:

– *Section 8.7 Terminal block, page 68*

Relay output

The VideoJet XTC XF transcoder has one relay output for switching external units such as lamps or alarm sirens. You can operate the relay output manually while there is an active connection to the transcoder. The relay output is also located on the orange terminal block.

CAUTION!

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

▶ Connect the lines to the appropriate terminals **R** on the orange terminal block and check that the connections are secure.

Further topics:

– *Section 8.7 Terminal block, page 68*

4.5 Power on/Power off

Power supply

The VideoJet XTC XF transcoder does not have a power switch. Power is supplied via a separate unit. Connect the transcoder to the power supply unit and plug this into the mains. The unit is now ready for use. The transcoder comes supplied with an appropriate power supply unit.

CAUTION!

Use only the power supply unit provided or another power suppply unit 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 VideoJet XTC XF transcoder to the power supply until all other connections have been made.

1. Connect the power supply unit to the **12V DC** socket on the transcoder.
2. Connect the power supply unit to the mains. The transcoder is ready for use as soon as the **CONNECT** 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 **LINK** LED also lights up. The flashing green LED **CONNECT** signals that data packets are being transmitted via the network.

4.6 Setup using Bosch Video Client

For the current version of the Bosch Video Client (BVC) management software, access your Bosch product catalog on the Internet. This program allows you to implement and set up the unit in the network quickly and conveniently.

Installing the program

1. Download Bosch Video Client from the Bosch product catalog on the Internet.
2. Unzip the file.
3. Double-click the installer file.
4. Follow the instructions on the screen to complete the installation.

Configuring the unit

You can start Bosch Video Client immediately after installation.

1. Double-click the 

icon on the desktop to start the program. Alternatively, start the application via the **Start** button and the **Programs** menu (path: Start/Programs/Bosch Video Client/Bosch Video Client).
2. When the program is started for the first time, a wizard opens to help you detect and configure devices on the network.
3. If the wizard does not start automatically, click  to open the Configuration Manager application. Then, click **Configuration Wizard...** on the **Tools** menu.
4. Follow the instructions given in the **Configuration Wizard** window.

Additional parameters

You can check and set additional parameters with the assistance of the Configuration Manager application in Bosch Video Client. You can find detailed information on this in the documentation for these applications.

5 Configuration using a Web browser

5.1 Connecting

The integrated HTTP server in the VideoJet XTC XF transcoder 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 application.

System requirements

- Computer with Windows XP or Windows 7 operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 9.0 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 **Releaseletter** document for the respective firmware. For the latest version of the firmware, required programs and controls, access your Bosch product catalog on the Internet.

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

In Windows 7, 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.

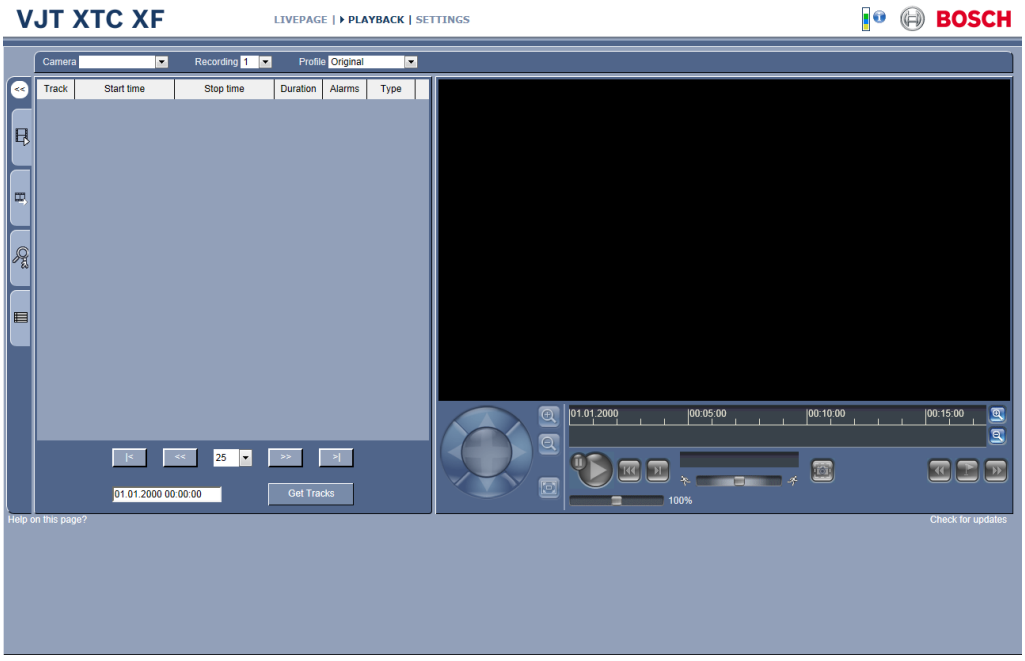
Establishing the connection

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

As a default DHCP is enabled in the unit's network settings. With an active DHCP server in the network you must know the IP address assigned by the DHCP server to operate the unit.

If DHCP address assignment is not successful use the following default IP address preset at the factory: **192.168.0.1**

1. Start the Web browser.
2. Enter the IP address of the unit as the URL.
3. During initial installation, confirm the security questions that appear. The connection is established and after a short time you will see the **PLAYBACK** page.
4. If the unit requires a newer software decoder to display the video, a pop-up window informs you on how to proceed.



Maximum number of transcoding connections

Only up to two transcoder channels are available per unit. If you do not connect, the unit may have reached its maximum number of connections. Wait for one of the transcoder channels to get free and try again.

Protected VideoJet XTC XF

The VideoJet XTC XF offers the option to limit the extent of access using various authorization levels. If the VideoJet XTC 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.

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.

Further topics:

– *Section 5.4 General > Password, page 25*

Protected network

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

To configure the unit, you must connect the VideoJet XTC 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.

Further topics:

– *Section Authentication, page 49*

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.
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 should only be processed or modified by expert users or system support personnel.

All settings are backed up in the VideoJet XTC 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.

Further topics:

– *Section 5.5 General > Date/Time, page 26*

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.

The following menu items are available:

General	Identification
	Password
	Date/Time
Web Interface	Appearance
	LIVEPAGE Functions

	Logging
Transcoder	Transcoder Setup
	Transcoder Profile
Recording	Storage Management
	Remote Video Device
Alarm	Alarm E-Mail
	Alarm Task Editor
Interfaces	Alarm Inputs
	Relay
	COM1
Network	Network Access
	Advanced
	Accounts
	IPv4 Filter
	Encryption
Service	Installer Menu
	Maintenance
	Licenses
	System Overview

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 General > Identification

Device name

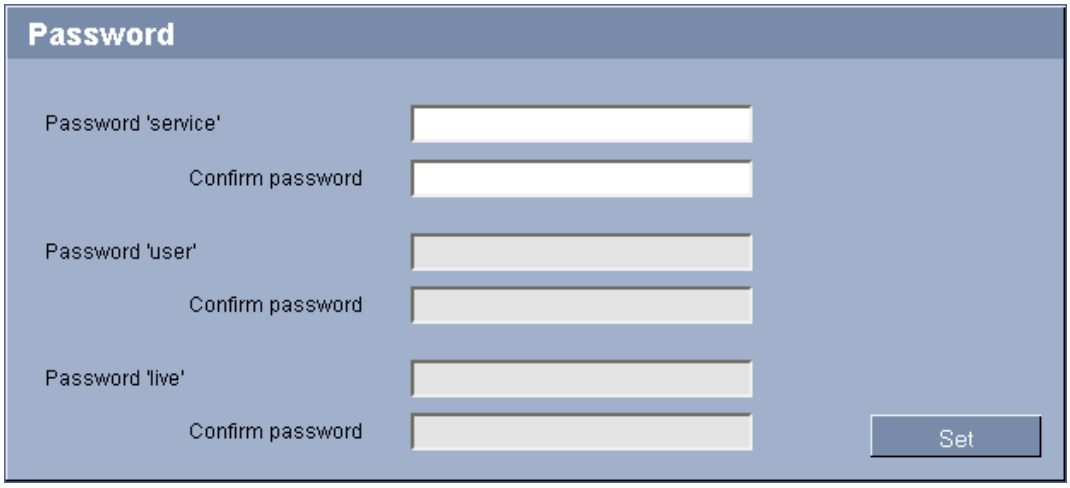
You can give the VideoJet XTC XF transcoder a name to make it easier to identify. The name makes the task of administering multiple units in larger video monitoring systems easier, for example using the Bosch Video Client or Bosch Video Management System programs.

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 management.

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

5.4 General > Password



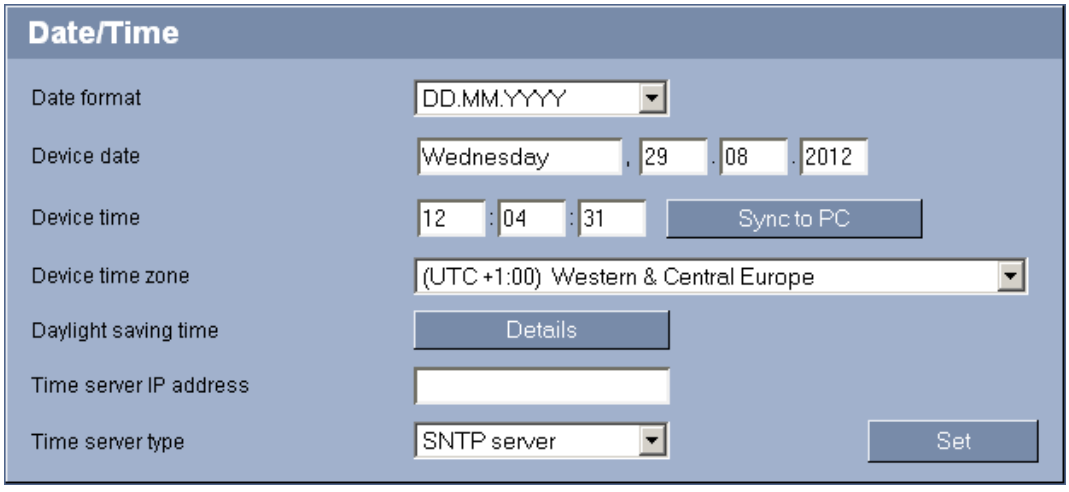
A VideoJet XTC XF transcoder is generally protected by a password to prevent unauthorized access to the unit. You can use different authorization levels to limit access.

Password
The VideoJet XTC XF transcoder 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 unit 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.
Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. Therefore, you always have to start from the highest authorization level when assigning passwords.
You can define and change a password for each authorization level if you are logged in as **service** or if the unit is not password protected.
Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters.

CAUTION!
Do not use any special characters, for example **&**, in the password.
Special characters are not supported by the system's internal management.

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

5.5 General > 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 VideoJet XTC XF transcoder.

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).

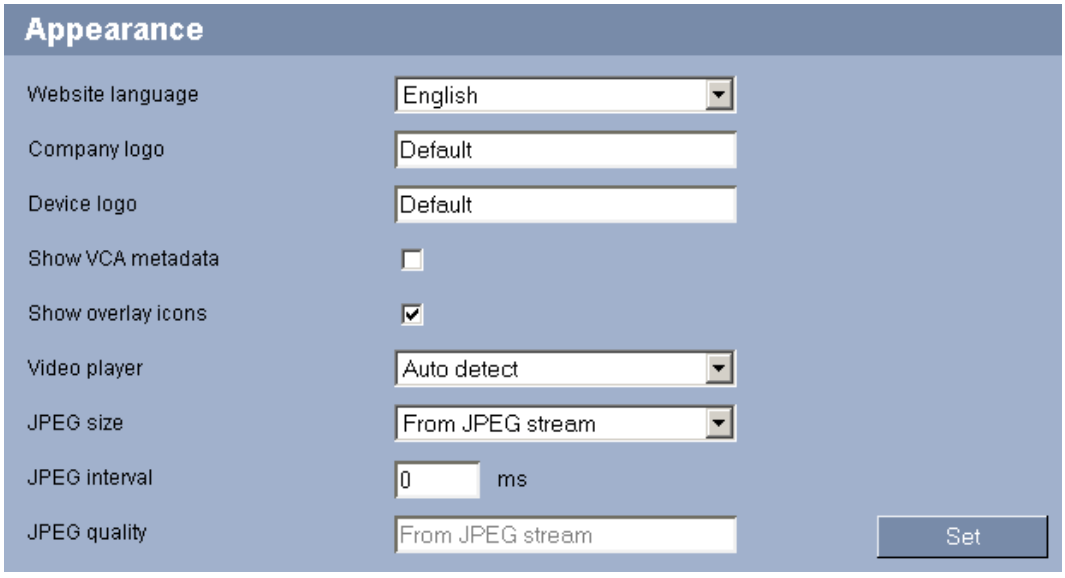
1. First check whether the correct time zone is selected. If it is not correct, select the appropriate time zone for the system, and click the **Set** button.
2. Click the **Details** button. A new window will open and you will see the empty table.
3. Select the region or the city that is closest to the system's location from the list field below the table.
4. Click the **Generate** button to generate data and enter it 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 apply and activate the table.

Time server IP address
The VideoJet XTC XF transcoder 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 **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.

5.6 Web Interface > 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 stored on a web server (for example **http://www.mycompany.com/images/logo.gif**).
Ensure that a connection to the web server is always available to display the image. The image file is not stored in the VideoJet XTC XF transcoder.
If you want to use the original graphics again, simply delete the entries in the **Company logo** and **Device logo** fields.

Website language
Select the language for the user interface here.

There are always two languages to choose from: English and another language. If the language you require is not available for selection, you can download the current firmware with another language combination from the Bosch product catalog on the Internet.

Company logo
Enter the path to a suitable graphic if you want to replace the manufacturer's logo. The image file must be stored on a web server.

Device logo
Enter the path to a suitable graphic if you want to replace the product name. The image file must be stored on a web server.

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

Show overlay icons
Various overlays or "stamps" in the video image provide important status information.

Further topics:
– *Section Display stamping, page 61*

Video player
Select the player you want to use for the **PLAYBACK** page. Choose **Auto detect** to have the player selected automatically. The first available player in the list will be used. Note that if you decide for JPEG images even the live view is no video stream.

JPEG size
Select the image size for displaying the M-JPEG on the **LIVEPAGE**. If the **From JPEG stream** option is selected, both the image size and quality defined in the encoder profile are used. Other options are:
– **Small**
  176 × 144/120 pixels (QCIF)
– **Medium**
  352 × 288/240 pixels (CIF)
– **Large**
  704 × 576/480 pixels (4CIF)
– **720p**
  1280 × 720 pixels
– **1080p**
  1920 × 1080 pixels

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

JPEG quality
You can specify the image quality for displaying the M-JPEG on the **LIVEPAGE**. If the **From JPEG stream** option is selected for the **JPEG size** parameter, this setting is automatically taken over and cannot be changed here.

5.7 Web Interface > 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 for the **LIVEPAGE** user. The selected items are indicated by a check mark.
2. Check whether the required functions are available for the **LIVEPAGE** user.

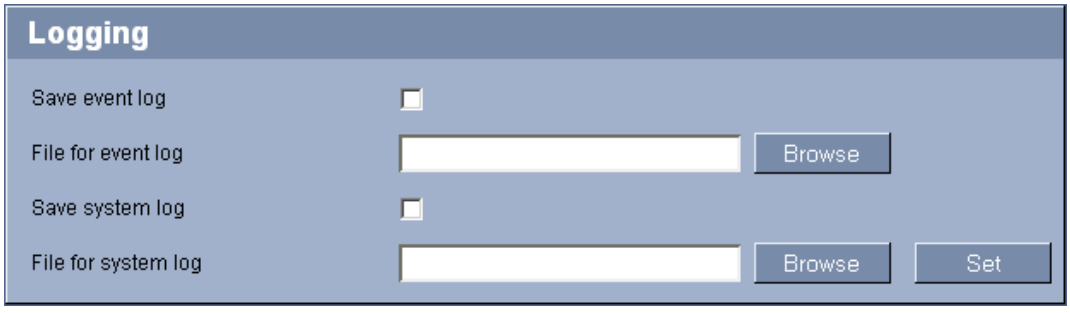
Show alarm inputs
Alarm inputs are shown next to the video image as icons, along with their assigned names. If an alarm is active, the corresponding icon changes color.

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 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.

5.8 Web Interface > 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.

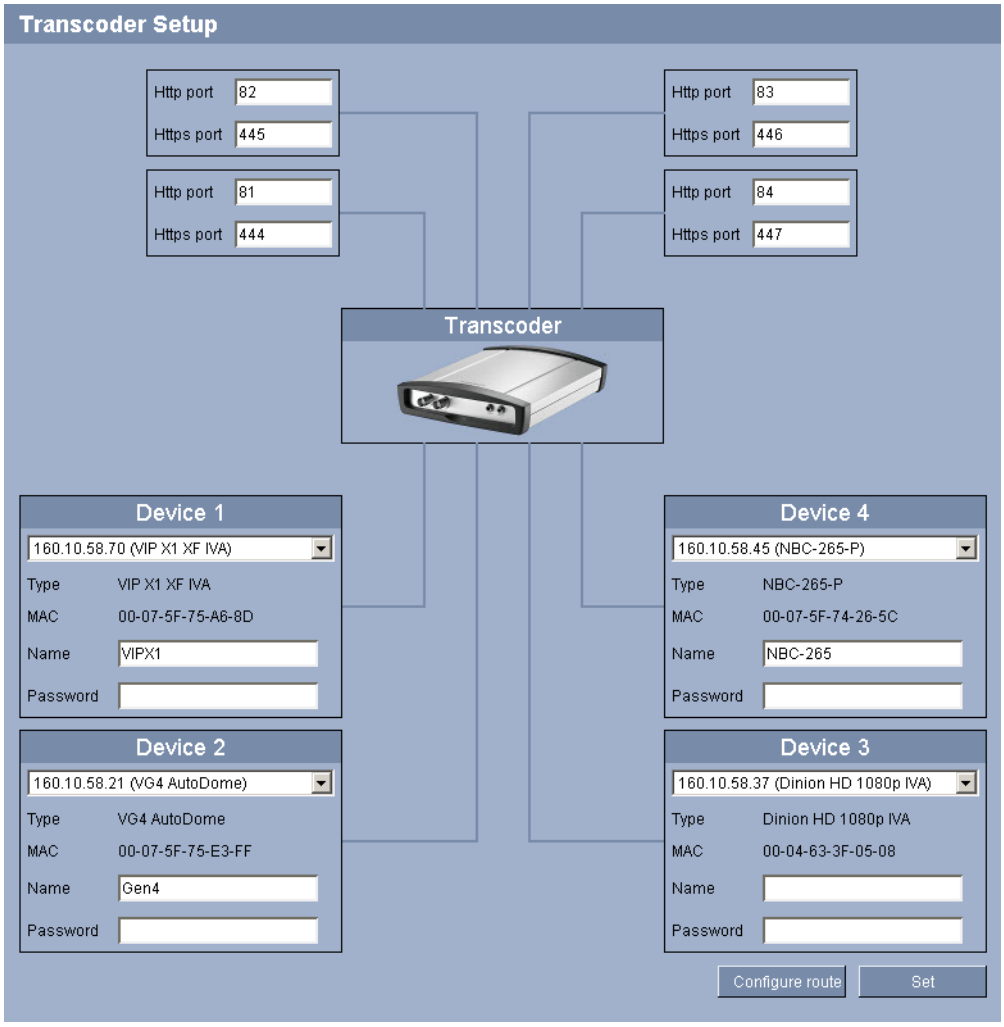
Save system log

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.

5.9 Transcoder > Transcoder Setup



Define up to four cameras for which you want to offer transcoded video. Transcoding is only available for recorded video. Therefore, make sure that these cameras will have recordings either by configuring the cameras accordingly or by having the transcoder managing it.
For information, the HTTP and HTTPS port of the transcoder are displayed. These can be changed on the **Network Access** page.

To setup a camera do the following:

1. Click a drop-down box. The system is automatically scanned for available cameras which are listed for selection. This includes analog cameras which are integrated into your system through a single-channel encoder. In this case, the corresponding encoder is listed for selection.

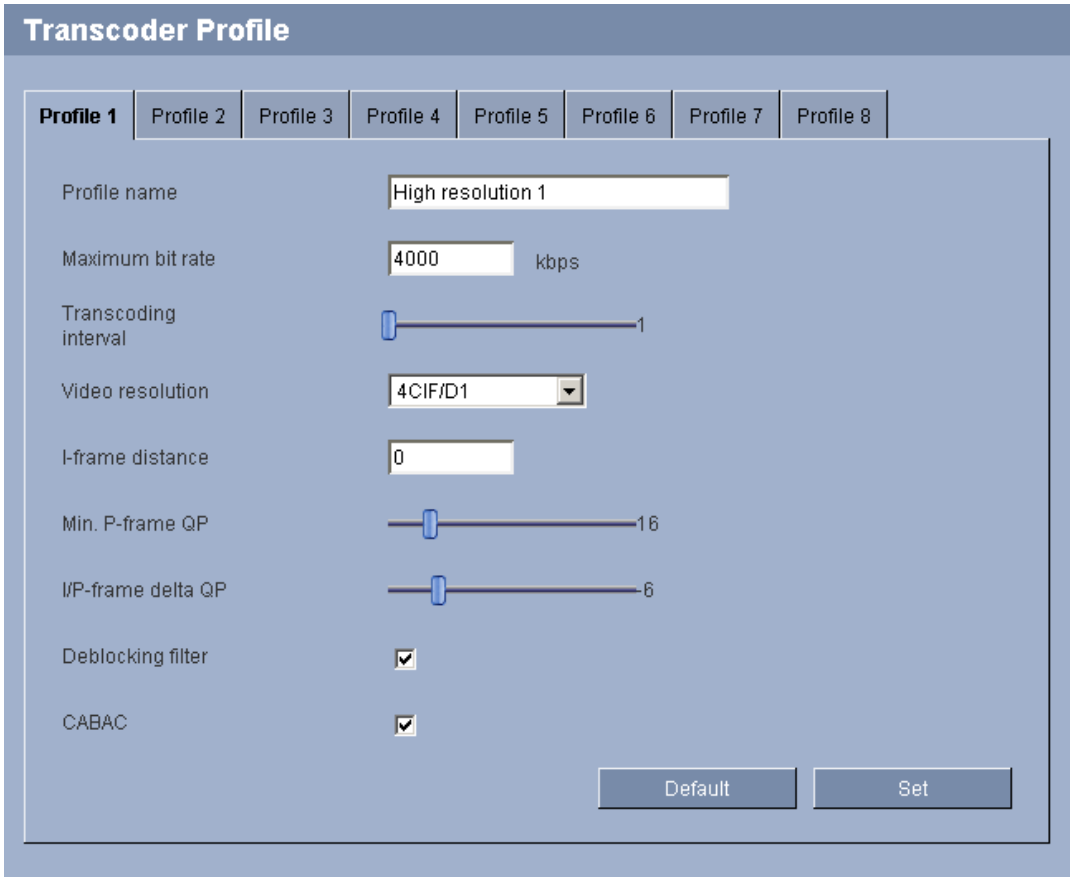
2. Select the desired camera from the list. The **Type**, **MAC**, and **Name** parameters are displayed, if available.
3. You may change the name. Do not use any special characters, for example **&**. Special characters are not supported by the system's internal management.
   Note that the name here is only used for the transcoder operation. Changes here will not overwrite the name assigned to camera or encoder on the corresponding **SETTINGS** page of the respective unit. The name you enter here will be displayed in the title bar of the transcoder Web pages and in the list of available cameras on the **PLAYBACK** page. If you leave the field empty the IP address of the unit is displayed.
4. In the **Password** field, enter the service password of the selected camera.
5. By default, the **HTTP port** and **HTTPS port** numbers for the camera are set automatically for each camera as an offset to the transcoder ports. The corresponding fields are marked by the white outline and the highlighted connection line. You may change the numbers, if necessary.
6. Repeat the procedure for each camera you want to add.
7. Click **Set** to save the settings. For each connected camera a link is added in the title bar next to the **SETTINGS** link stating the camera number **1** to **4** and its name or IP address.
8. If your router has UPnP enabled, click **Configure Router** to save the settings to the router. Otherwise, configure your router manually.

The cameras are now available for selection on the **PLAYBACK** page. Transcoding will only be possible once recordings for the cameras are available.

Further topics:

– *Section 5.18 Network > Network Access, page 44*
– *Section 6.2.1 Links, page 57*

5.10 Transcoder > Transcoder Profile



For video transcoding, you can select a profile on the **PLAYBACK** page to adapt the video data transmission to the operating environment (for example network structure, bandwidth, data load). You can configure the presets for the profiles on this page.
Pre-programmed profiles are available, each giving priority to different perspectives. Below is a brief description of the factory default settings for the transcoder profiles.

- **High resolution 1**
  High quality for connections with the highest bandwidth
- **High resolution 2**
  High quality for high bandwidth connections
- **Low bandwidth**
  High resolution for low bandwidth connections
- **DSL**
  For DSL connections with 500 kbps
- **ISDN (2B)**
  For ISDN connections via two B-channels
- **ISDN (1B)**
  For ISDN connections via one B-channel
- **Modem**
  For analog modem connections with 20 kbps
- **GSM**
  For GSM connections at 9,600 baud

You can change individual parameter values of a profile and you can also change the name. You can switch between profiles by clicking the appropriate tabs.
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.

CAUTION!
The profiles are rather complex. They include a large number of parameters that interact with one another, so it is generally best to use the default profiles.
Change the profiles only once you are fully familiar with all the configuration options.

Profile name
You can enter a new name for the profile here. The name is then displayed in the list of available profiles.

CAUTION!
Do not use any special characters, for example **&**, in the name.
Special characters are not supported by the system's internal management.

Maximum bit rate
This maximum bit 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.

Transcoding interval
The setting here determines the interval at which images are coded and transmitted. For example, entering **4** means that only every fourth image is coded, the following three are skipped — this can be particularly advantageous with low bandwidths.

Base resolution
Define the desired size for the video image. The actual resolution depends on the settings of the connected unit.
The following tables provide an overview on available resolutions for small and large image sizes for the various CPP (Common Product Platform) devices:

Base resolution: Small (resolution in pixels)

	CPP3	CPP4	CPP-ENC
1080p	352 × 240	512 × 288	—
720p	352 × 240	512 × 288	—
PAL	352 × 288	—	352 × 288
NTSC	352 × 240	—	352 × 240

Base resolution: Large (resolution in pixels)

	CPP3	CPP4	CPP-ENC
1080p	704 × 480	768 × 432	—
720p	704 × 480	768 × 432	—
PAL	704 × 576	—	704 × 576
NTSC	704 × 480	—	704 × 480

Thanks to Instant Display Enhancement, when you pause the video the image will be enhanced to the next higher resolution, if available. Thus, in pause mode you can get up to 1920 × 1080 pixels for a connected HD device that is configured accordingly.

I-frame distance
This parameter allows you to set the intervals in which the I-frames will be coded. **0** means auto mode, whereby the video server inserts I-frames as necessary. An entry of **3** indicates that only every third image is an I-frame.

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

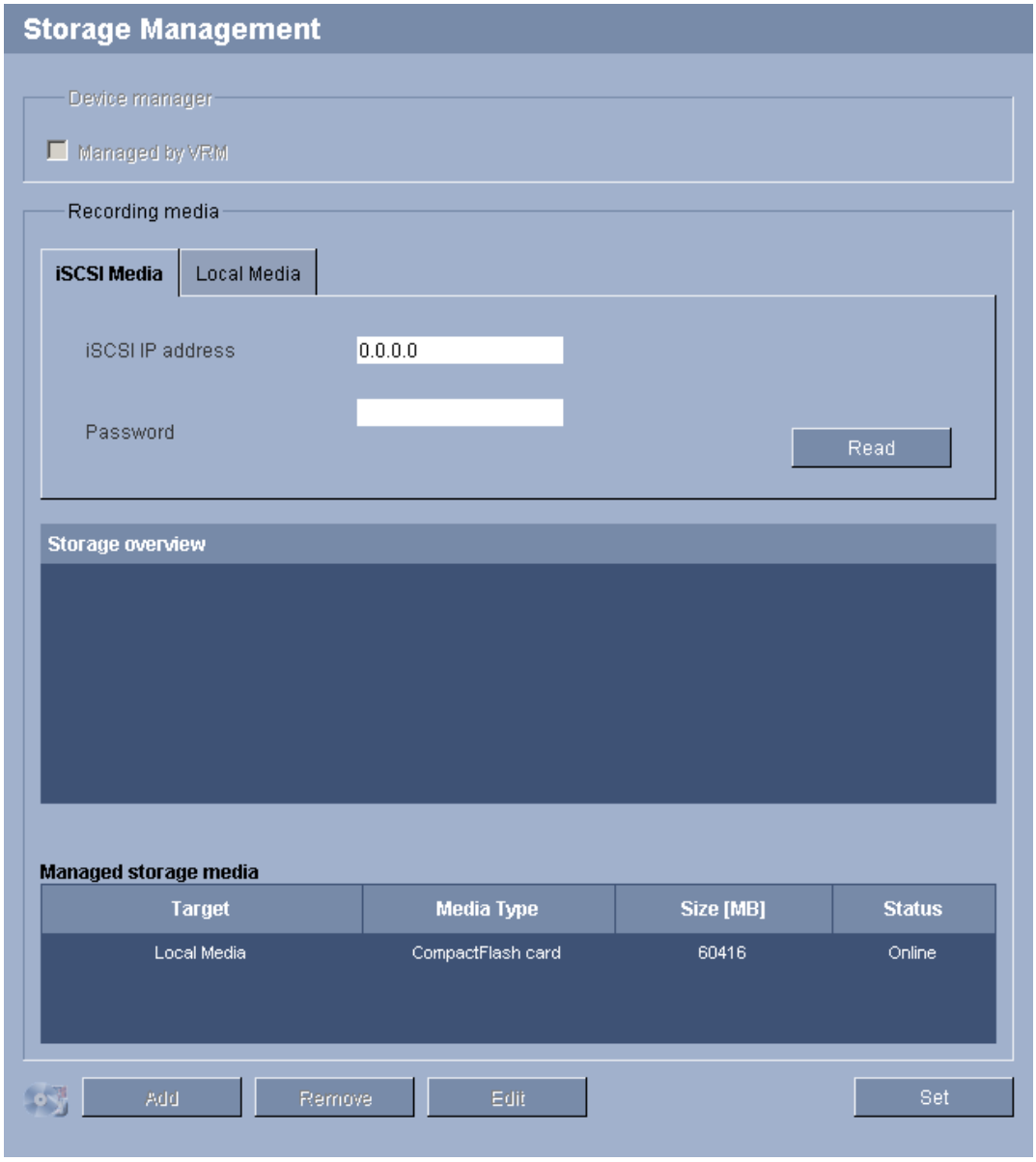
I/P-frame delta QP
This parameter sets the ratio of the I-frame QP to the P-frame QP. For example, you can set a lower value for I-frames by moving the slide control to a negative value. Thus, the quality of the I-frames relative to the P-frames is improved. The total data load will increase, but only by the portion of I-frames.
As default, a value of **-6** is set which should work for most applications. If necessary, you may change this value as follows:
– If you find the transcoded video to be jerky, the QP value is too high and should be reduced.
– If you find the transcoded video to be pumping, the QP value is too low and should be increasced.

Deblocking filter
You can activate a filter that reduces blocking in the image, thereby providing a smoother image. Please note that this option requires additional computing power.

CABAC
You can activate an additional lossless compression of the video data. The same image quality is retained while the data rate is reduced. This compression necessitates high computing power.

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

5.11 Recording > Storage Management



The VideoJet XTC XF can also manage the recordings for the connected cameras. In order to have the recordings managed by the transcoder, you need to define the storage media here and to initialize the recording for the desired camera on the **Remote Video Device** page.
You can record the images on the local CF card or on an appropriately configured iSCSI system.
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 recordings 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 have added the device to a VRM system, the VRM Video Recording Manager will manage all recording. In this case the **Managed by VRM** box is checked and you will not be able to configure any further settings here.

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 for the connected devices, 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 target in the **iSCSI IP address** field.
2. If the iSCSI target 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 VideoJet XTC XF transcoder. 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**.

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 **Format** 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.

5.12 Recording > Remote Video Device

This page provides information on the current recording status of the cameras connected to the transcoder, for example the recording bit rate. For easy identification, the name respectively IP address of the connected camera is displayed as heading for the corresponding information block. The status information may be followed by an icon. Move the cursor over the icon to show more details. In particular, the recording target for the respective camera is displayed which is also the source for the recordings available to you on the **PLAYBACK** page.

NOTICE!
Note that the connected camera respectively its encoder needs to run at least firmware version 5.60 if you also want to be able to playback and transcode video that is stored by the remote video device itself. If it has firmware version 5.52 only recordings managed by the transcoder can be played back and transcoded. Earlier firmware versions are not supported.

If you want the recordings to be managed by the transcoder you have to initialize the recordings here. Otherwise, the recording settings of the camera itself apply. Furthermore, you have the possibility to start and stop recordings and to overwrite the recording settings for the connected cameras.

1. To take over the recording management for a single camera, click **Initialize Recording...** for the respective device. Click **Initialize All...** to do so for all connected devices at once.
2. In the **Configuration** window, mark the **SETTINGS** pages of the remote video device that you want to overwrite with the transcoder defaults. Generally, this means that a simple basic configuration is set which grants you most effective recording that also supports forensic search:

   Recording Profiles

   Select the desired recording mode as it affects the defaults to be set. Note that only the **Day** tab on the **Recording Profiles** page is overwritten, that is the tab marked green.

   - **Pre-alarm**

     The best stream profile and the maximum pre-alarm time for RAM recording together with a minimum post-alarm time are selected, all available alarm triggers are activated, and metadata is included in recording.

   - **Continuous**

     The best stream profile is selected for recording, pre- and post-alarm times are deleted, all available alarm triggers are deactivated, and metadata is included in recording.

   Recording Scheduler

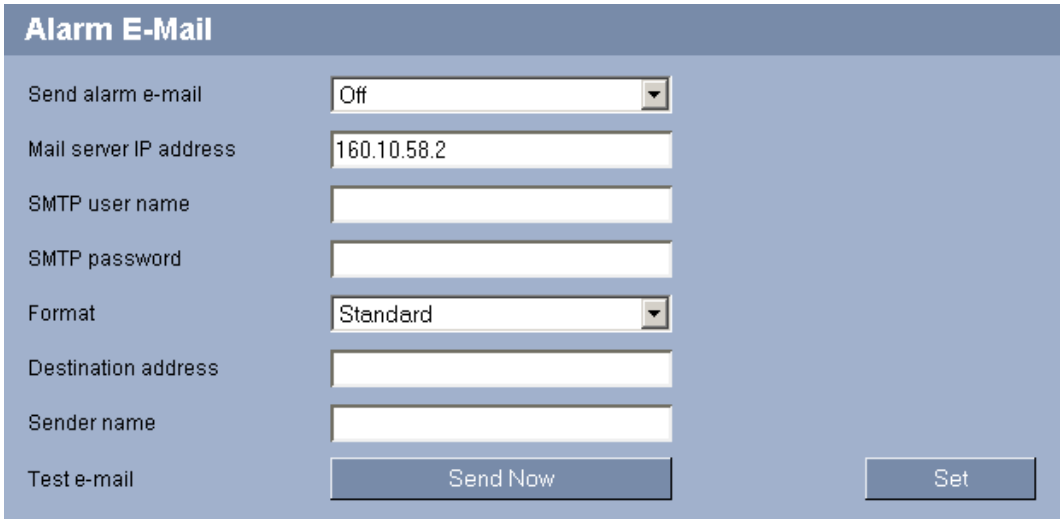
   The scheduler is set to 24/7 recording with the **Day** recording profile.

   VCA

   If the camera supports IVA software, this is set as analysis type and activated to detect any object in the scene. Otherwise, the motion detector is activated configured to monitor the entire area for even small objects with high sensitivity.

3. Click **Set** to save the settings. The recording target is the one defined in the transcoder. Only recordings to this target will now be available on the **PLAYBACK** page.
4. Click the respective button to start or stop the recording for a camera.

5.13 Alarm > 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 unit 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**
  E-mail in standard format
- **SMS**
  E-mail in SMS format to an e-mail-to-SMS gateway (for example, to send an alarm by cell phone)

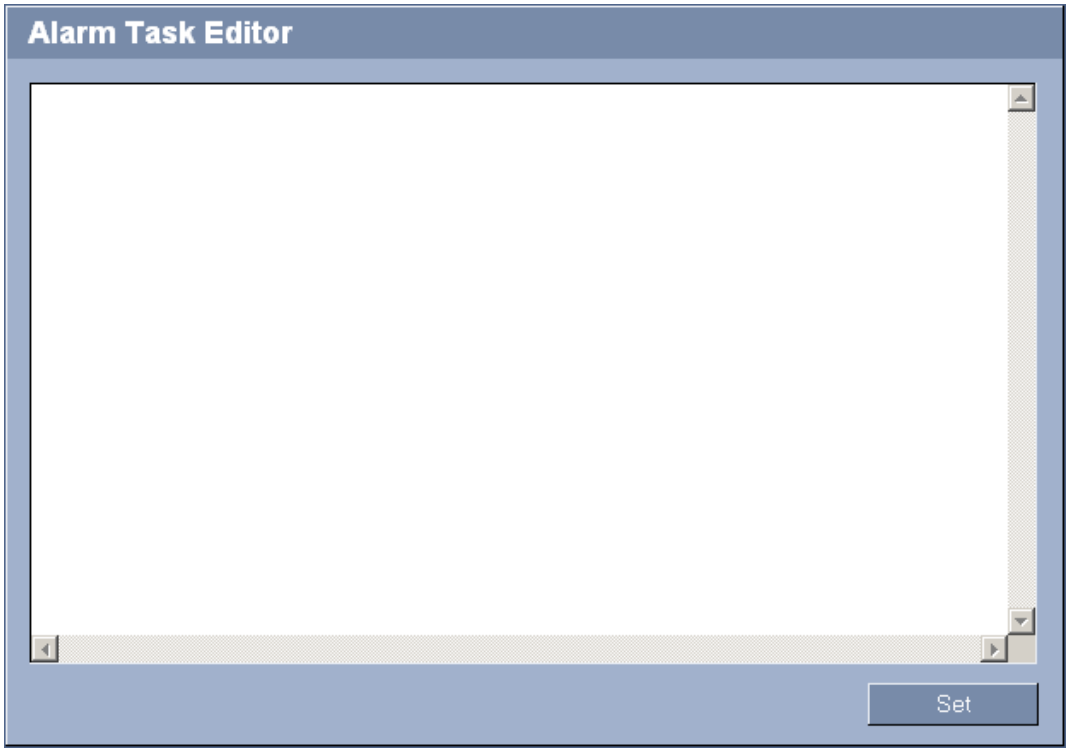
CAUTION!
When a cellphone is used as the receiver, make sure to activate the e-mail or SMS function, depending on the format, so that these messages can be received.
You can obtain information on operating your cellphone from your cellphone provider.

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.

5.14 Alarm > Alarm Task Editor

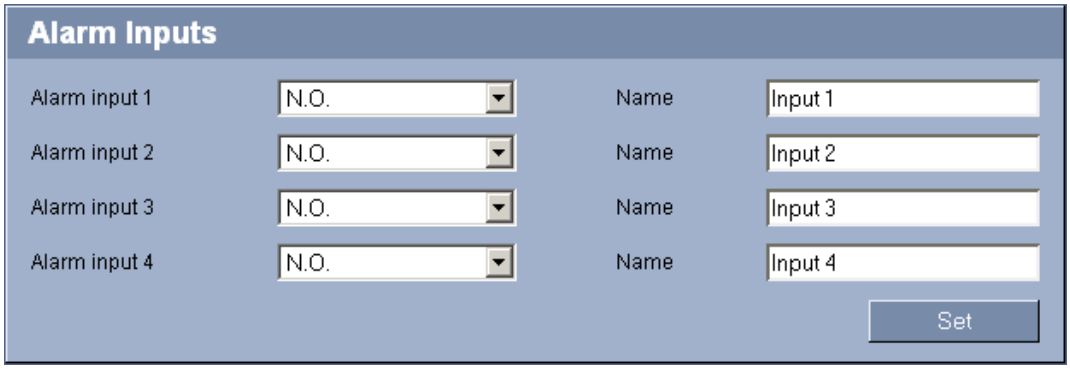


CAUTION!
Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.
In order to edit this page, you must have programming knowledge and be familiar with the information in the **Alarm Task Script Language** document. For the latest version of this document access your Bosch product catalog on the Internet.

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.

5.15 Interfaces > Alarm Inputs



You can configure the alarm inputs of the VideoJet XTC XF transcoder.

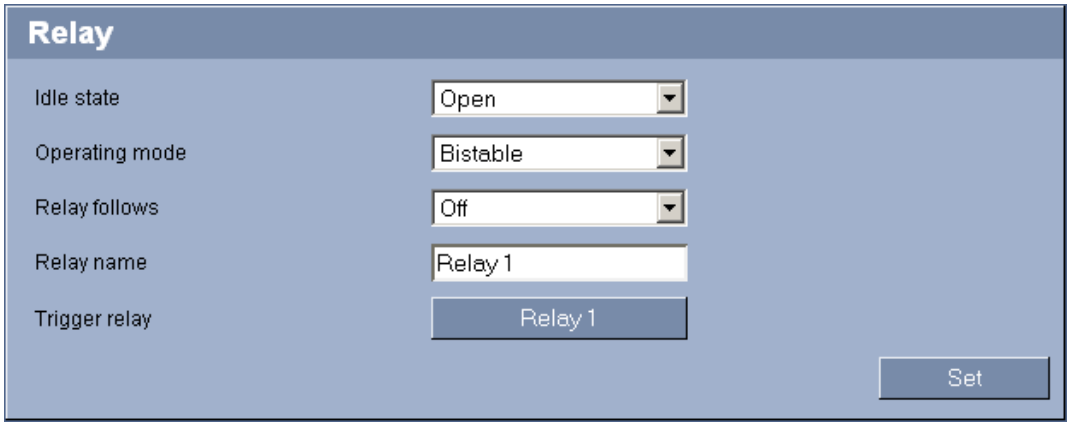
Alarm input
Select **N.O.** if the alarm is to be triggered when the contact closes. Select **N.C.** if the alarm is to be triggered when the contact opens.

Name
You can enter a name for each alarm input. If the **LIVEPAGE** functions are configured accordingly, this name is displayed below the icon for the alarm input. You can also use the name in the Forensic Search program function as a filter option for quick search in recordings. 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 management.

Further topics:
– *Section 5.7 Web Interface > LIVEPAGE Functions, page 29*

5.16 Interfaces > Relay



You can configure the switching behavior of the relay output. You can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).
You can also specify whether the 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 only for a defined period, for example, select the corresponding setting.

Relay follows
Select the event that triggers the relay.

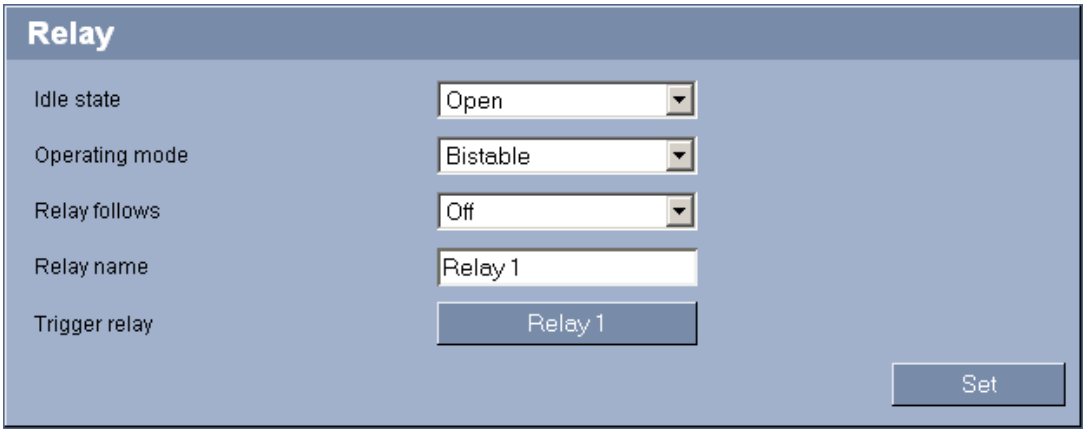
Relay name
You can assign a name for the relay here. The name is shown on the button next to **Trigger relay**. If the **LIVEPAGE** functions are configured accordingly, this name is displayed below the relay icon. You can also use the name in the Forensic Search program function as a filter option for quick search in recordings. 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 management.

Further topics:
– *Section 5.7 Web Interface > LIVEPAGE Functions, page 29*

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

5.17 Interfaces > COM1



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

Serial port function
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.

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

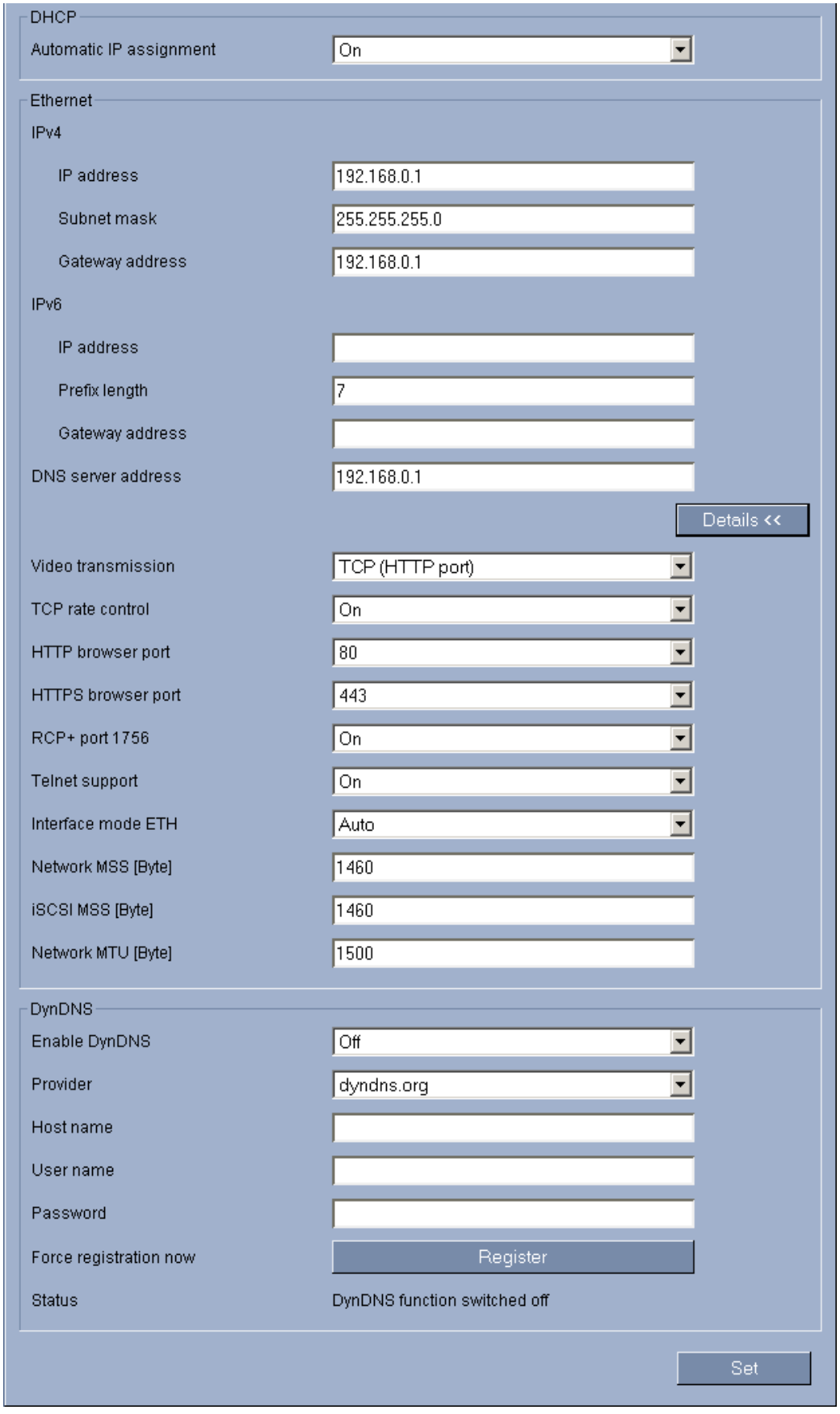
Data bits
The number of data bits per character cannot be changed.

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.

5.18 Network > Network Access



The settings on this page are used to integrate the VideoJet XTC XF transcoder 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 unit is rebooted and the changed settings are activated.

CAUTION!
If you change the IP address, subnet mask, gateway address or the DHCP setting, the unit 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 transcoder.
Certain applications (Bosch Video Client, Bosch Video Management System) 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.

IPv4
For IPv4 connections, fill-in the required information:

1. Enter the desired IP address for the VideoJet XTC XF transcoder in the **IP address** field. The IP address must be valid for the network.
2. Enter the appropriate subnet mask for the selected IP address.
3. If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway in the **Gateway address** field. Otherwise leave the box blank (**0.0.0.0**).

If necessary, you may also enter the parameters for IPv6 connections.

IPv6
For IPv6 connections, fill-in the required information:

1. Enter the desired IP address for the VideoJet XTC XF transcoder in the **IP address** field. The IP address must be valid for the network.
2. Enter the appropriate prefix length for the set IP address.
3. If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway in the **Gateway address** field. Otherwise leave the box blank (**0.0.0.0**).

If necessary, you may also enter the parameters for IPv4 connections.

DNS server address
The unit can use a DNS server to resolve a mail or FTP server 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**.

TCP rate control
Activate this option If you want to allow Adaptive Bit Rate encoding.

HTTP browser port
Select a different HTTP browser port from the list if required. The default HTTP port is 80. 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 VideoJet XTC XF transcoder 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 and metadata) on the **Encryption** page.

Further topics:
– *Section 5.22 Network > Encryption, page 51*

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 network equipment connected, e.g. a switch, 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. In UDP mode, comply with the MTU value set below.

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 transcoder.

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

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

NOTICE!
For information about the service, registration process and available host names please refer to the provider.

Provider
Select your dynamic DNS provider.

Host name
Enter the host name registered for the transcoder.

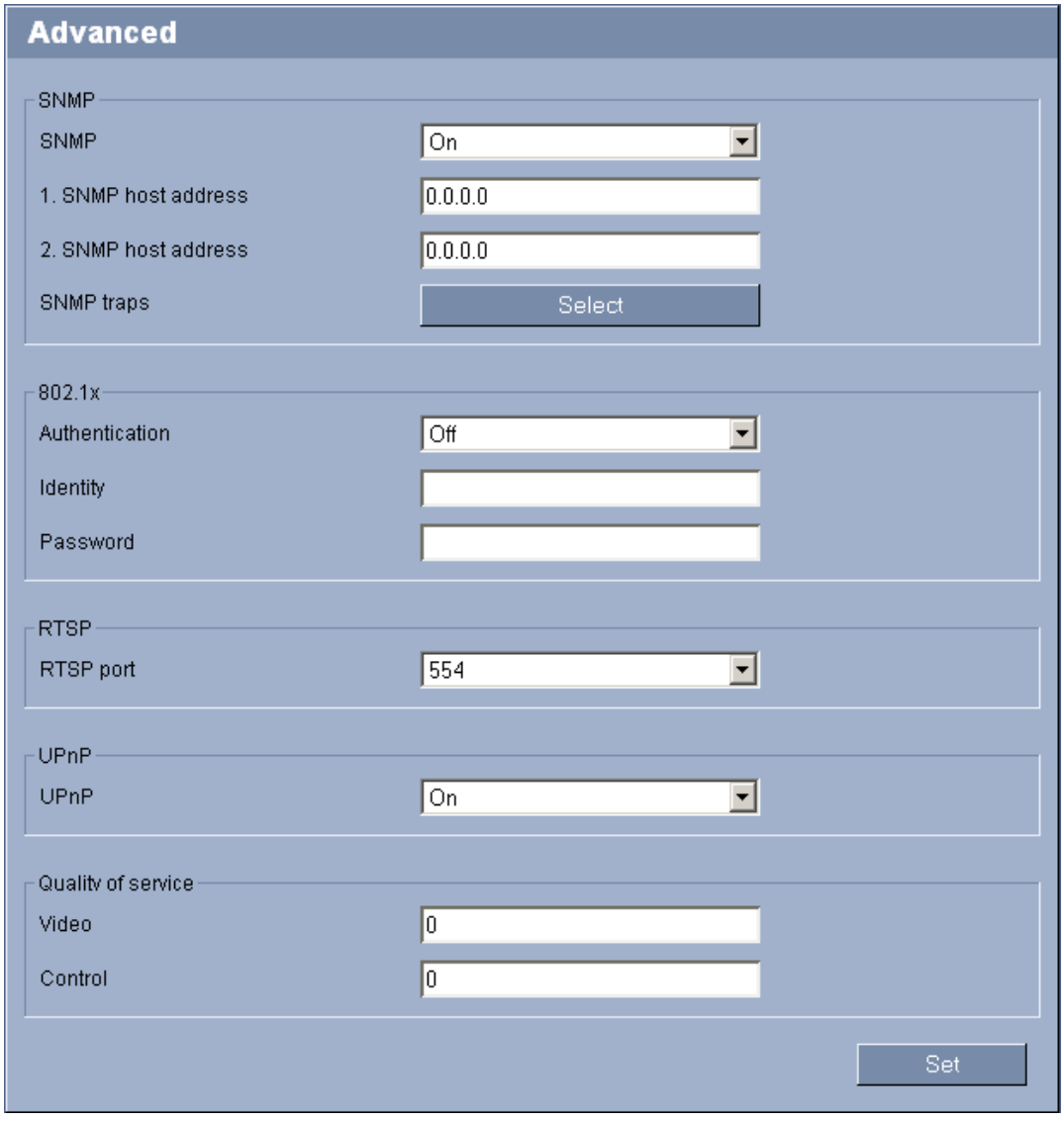
User name
Enter the user name you registered.

Password
Enter the password you registered.

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 transcoder, click the **Register** button.

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

5.19 Network > 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 unit is rebooted and the changed settings are activated.

SNMP

The VideoJet XTC XF transcoder 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 unit 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 transcoder directly to a computer. 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 unit.

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.

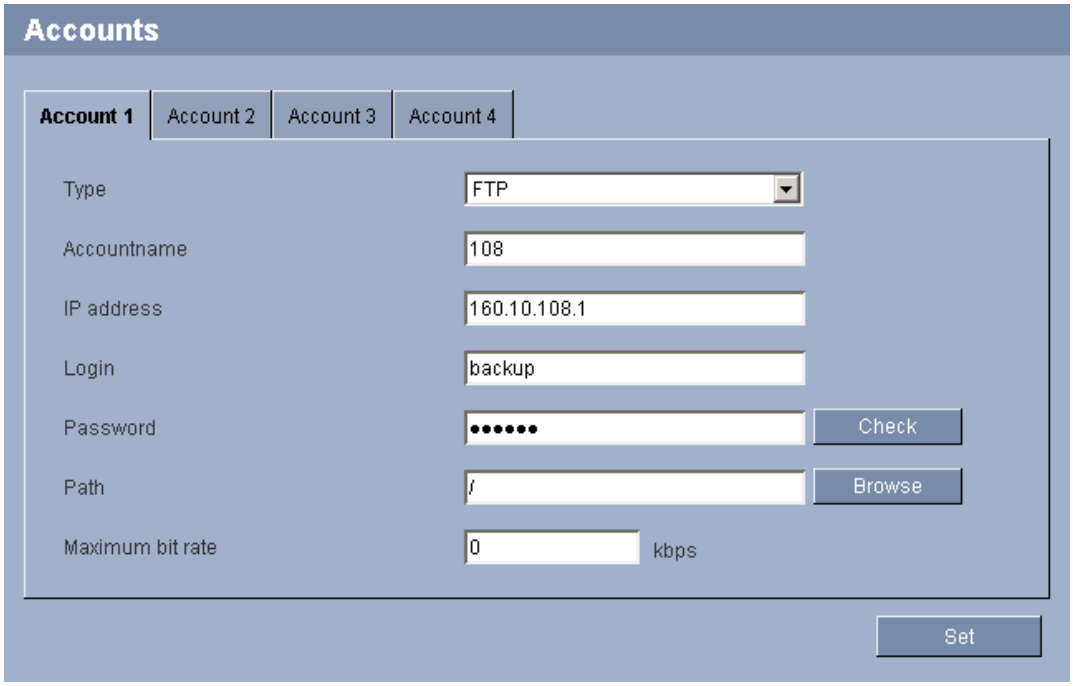
UPnP
You can activate the Universal Plug and Play (UPnP) function. If the function is turned on, the unit responds to requests from the network and is automatically registered on the requesting computers as a new network device. For example, access to the unit can then be made using Windows Explorer without knowledge of the IP address of the unit.

NOTICE!
To use the UPnP function on a computer, both the Universal Plug and Play Device Host and SSDP Discovery Service must be active in Windows XP and Windows 7.

This function should not be used in large installations because of the variety of potential registration notifications.

Video / Control
The quality of service of the different data channels can be set by defining the DiffServ Code Point (DSCP). Enter a number between 0 and 252 as a multiple of four.

5.20 Network > Accounts



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

Type
Select either an FTP server or Dropbox for the account type.

NOTICE!
Make sure to adhere to all existing data protection laws, regulations, and guidelines of the respective country when using a Dropbox account.

For using a Dropbox account, note that the device needs access to the Internet. Click **Connect...**: the Dropbox website opens for you to sign in or to create a new account. Follow the steps described there and allow the Bosch app to connect with your Dropbox. Return to the device's **Accounts** page to get a status message on the Dropbox connection.

Account name
Enter an account name to be shown as the target on the **PLAYBACK** page.

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

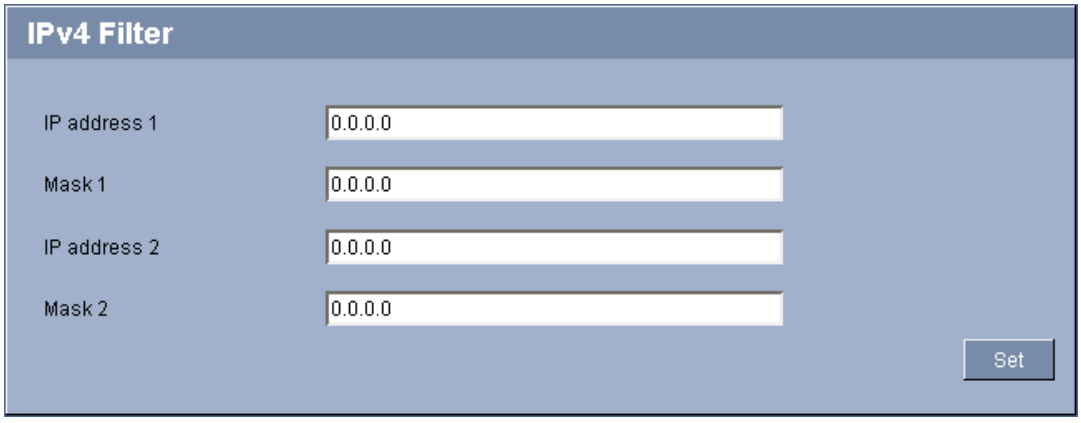
Login
Enter your login name for the account server.

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

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

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

5.21 Network > IPv4 Filter



To restrict the range of IP addresses within which you can actively connect to the device, fill-in an IP address and mask. Two ranges can be defined.
To do so, enter one or two IP addresses and define the range with the help of the corresponding mask. For example: With IP address 192.168.0.0 and corresponding mask 255.255.255.128 only IP addresses in the range from 192.168.0.0 to 192.168.0.127 are allowed to actively connect to the device.
If either of these ranges are set, no IPv6 addresses are allowed to actively connect to the device. The device itself may initiate a connection (for example, to send an alarm) outside the defined ranges if it is configured to do so.

5.22 Network > 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.

Further topics:
– *Section 5.25 Service > Licenses, page 54*

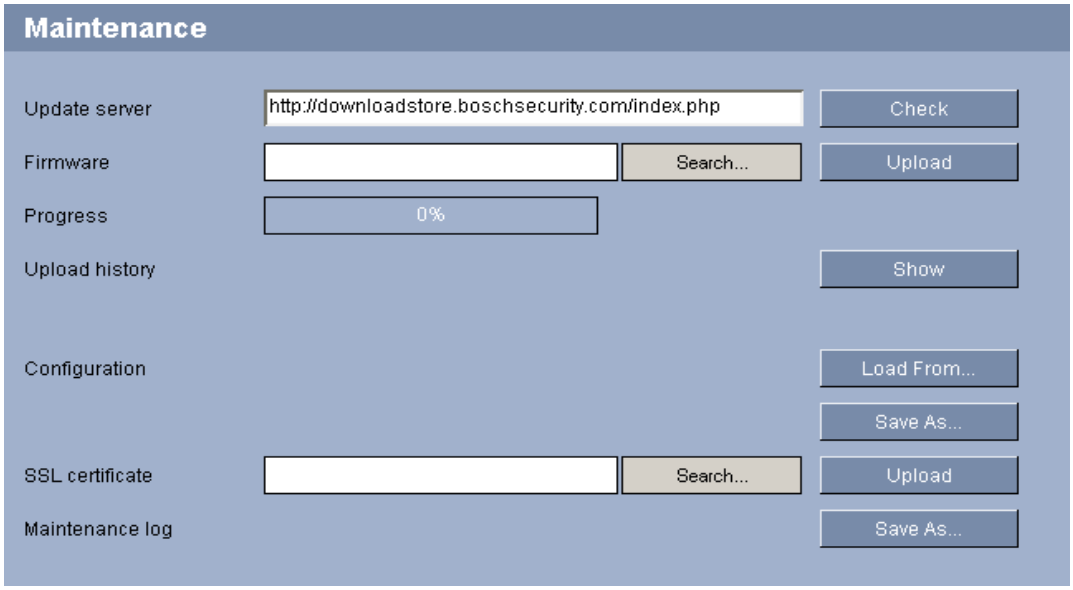
5.23 Service > Installer Menu

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

Factory defaults

Click **Defaults** to restore the factory defaults for the unit. A confirmation screen appears.

5.24 Service > Maintenance



Update server

The address of the Bosch update server appears in the address box.

1. Click **Check** to make a connection to this server. A list of available firmware appears.
2. Select the appropriate version for your unit to download the firmware from the server.
3. If required, check the **Do not show again.** box to avoid this window opening again.

Firmware

The VideoJet XTC XF transcoder 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, the unit 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 **CONNECT** 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 transcoder (for example **192.168.0.10/main.htm**).
2. Repeat the upload.

Upload history

You can lookup information on the last data uploads.

▶ Click **Show** to display the upload history. A new window ist opened showing a list of the last uploads.

Configuration

You can save configuration data for the unit 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 **Load From...** 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 **Save As...** 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 VideoJet XTC XF transcoder.
If you wish to upload multiple files onto the unit, 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 transcoder (for example **192.168.0.10/reset**), or use the **Reboot** button on the **Installer Menu** page.

The new SSL certificate is valid.

Further topics:

– *Section 5.23 Service > Installer Menu, page 51*

Maintenance log

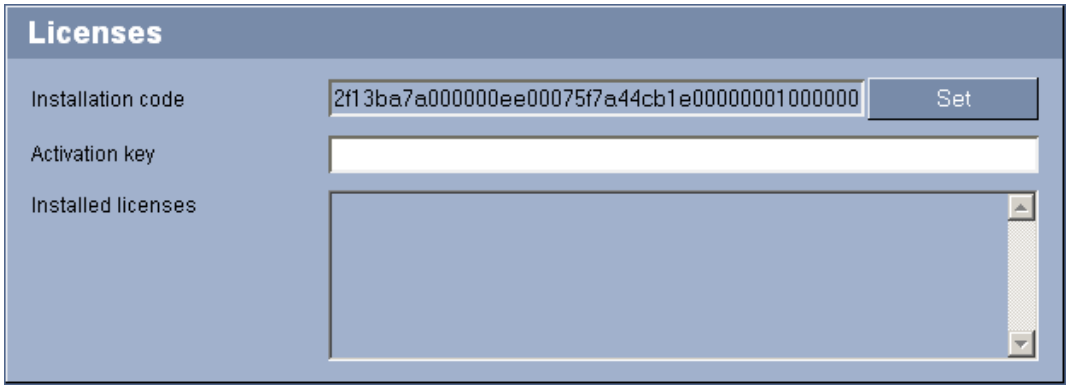
You can download an internal maintenance log from the unit to send it to Customer Service for support purposes. When doing this, ensure that **HTTPS browser port** is not set to **Off** and

TLS 1.0-support is activated for your browser. Click **Save As...** and select a storage location for the file.

Further topics:

– *Section HTTPS browser port, page 46*

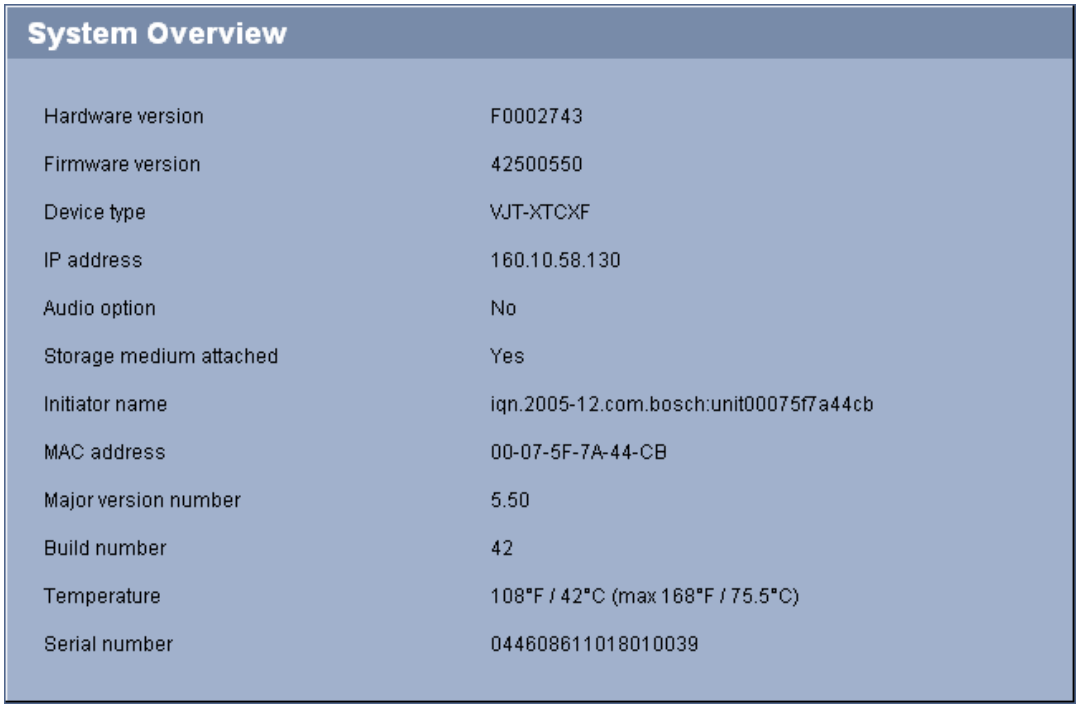
5.25 Service > Licenses



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.

5.26 Service > 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.

5.27 Function test

The VideoJet XTC XF transcoder 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 unit operates as expected.
Your check should include the following functions:

- Can the unit be called up remotely?
- Does the unit transmit all the required data?
- 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 9.0 or higher) can receive images from devices connected to the VideoJet XTC XF transcoder and replay stored video sequences.

System requirements

- Computer with Windows XP or Windows 7 operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 9.0 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 **Releaseletter** document for the respective firmware. For the latest version of the firmware, required programs and controls, access your Bosch product catalog on the Internet.

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

In Windows 7, 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.

Establishing the connection

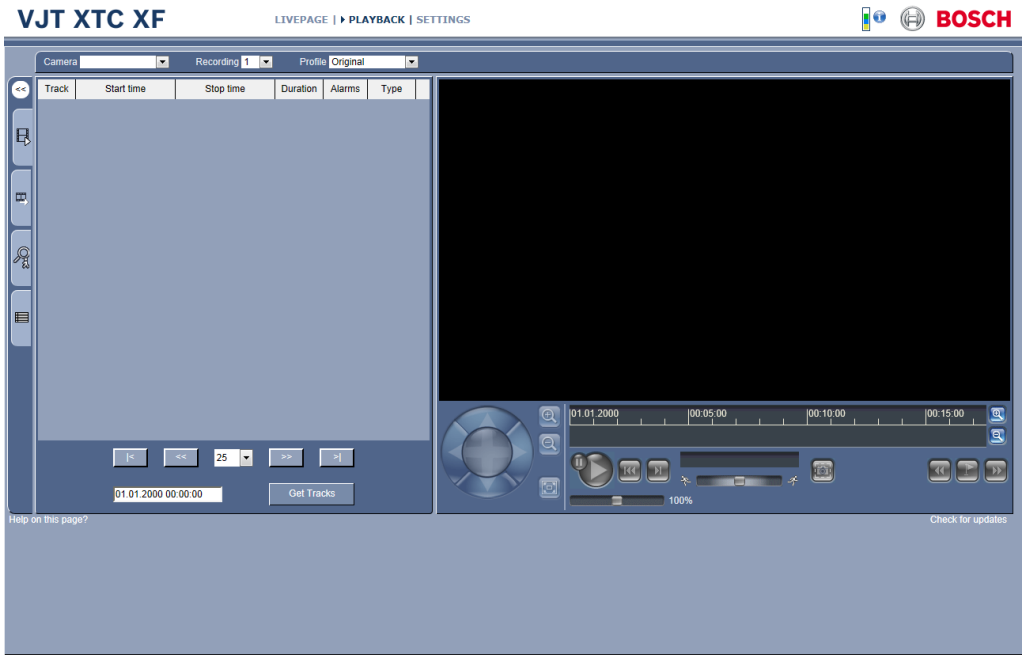
Before you can operate the VideoJet XTC XF transcoder within your network, it must have a valid IP address for your network and a compatible subnet mask.

As a default DHCP is enabled in the unit's network settings. With an active DHCP server in the network you must know the IP address assigned by the DHCP server to operate the unit.

If DHCP address assignment is not successful use the following default IP address preset at the factory: **192.168.0.1**

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 unit as the URL.
3. During initial installation, confirm the security questions that appear. The connection is established and after a short time you will see the **PLAYBACK** page.
4. If the unit requires a newer software decoder to display the video, a pop-up window informs you on how to proceed.



Maximum number of transcoding connections

Only up to two transcoder channels are available per unit. If you do not connect, the unit may have reached its maximum number of connections. Wait for one of the transcoder channels to get free and try again.

Protected unit

The VideoJet XTC XF transcoder offers the option to limit the extent of access using various authorization levels. If the unit 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.

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.

Further topics:

– *Section 5.4 General > Password, page 25*

Protected network

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

Further topics:

– *Section Authentication, page 49*

6.2 The title bar

If the VideoJet XTC XF is accessed via the Web browser, the title bar provides you with various links and information elements.

6.2.1 Links

Depending on the configuration of the unit you have a number of links to easily switch to other web pages. However, password protection may prevent you from displaying certain pages.

1. Click the **LIVEPAGE**, **PLAYBACK** or **SETTINGS** link to switch to the corresponding web page of the unit.
2. If there are already devices connected to the transcoder these are displayed as links in the title bar, too. Click the link to open the **SETTINGS** page of the connected device.

6.2.2 Information elements

In the right part of the title bar you see the processor load indicator next to the information icon. Here you can obtain additional information to help you when troubleshooting or fine tuning the unit.

1. The processor load indicator shows the proportions of the individual functions sorted by color. Move the cursor over the indicator to show the color code and the percentages.
2. Move the cursor over  to display information about the network connection:

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

6.3 The PLAYBACK page

Once the connection is established, the Web browser displays the **PLAYBACK** page.
A collapsible panel on the left of the display has four tabs:

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

On the right of the display you see the playback area with room for the video and a number of buttons and sliders described below to help you control the playback.

6.3.1 Preparing for playback

1. At the top of the window, select the desired camera from the **Camera** drop-down menu. In the **Track list** tab, the list of tracks with a number assigned to each sequence is displayed. Start time and stop time, recording duration, number of alarms, and recording type are shown for each track. Playback of the live video for the selected camera is started.
2. Select 1 or 2 from the **Recording** drop-down menu at the top of the window.
3. To use the built-in transcoding function, select any other than the original profile to guarantee smooth replay and browsing through recordings even for bandwidth-limited connections.
   The electronic pan/tilt/zoom control allows to zoom into a region of interest. Only this cut-out of the original recording will then be transcoded for best use of available bandwidth.
   Thanks to Instant Display Enhancement, when you pause the video the image will be enhanced to the next higher resolution, if available. Thus, in pause mode you can get up to 1920 × 1080 pixels for a connected HD device that is configured accordingly.

Further topics:

- *Section Base resolution, page 33*

6.3.2 Selecting recordings for playback

To see all saved sequences:

1. Click the **Track list** tab.

2. At the bottom of the window, select the maximum number of tracks to be displayed in the list.
3. Use the arrow buttons at the bottom to browse the list.
4. To view tracks beginning from a particular time, enter the time code and click **Get Tracks**.
5. Click a track. The playback for the selected sequence starts.
6. Click **Now** to return to the live video from the selected camera.

6.3.3 Exporting tracks

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

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

6.3.4 Searching for events in tracks

If for the original recording video content analysis was activated, you can do a forensic search for special events:

1. Click the **Search** tab.
2. Select a search mode:
   - **Any motion**
     Returns a result for any motion in the recorded video.
   - **Field**
     Use the mouse to define a field in the preview window for the search to return a result for any motion in that field.
   - **Line crossing**
     Use the mouse to define a line in the preview window for the search to return a result for any crossing of that line.
   - **Recorded alarms**
     Returns a result for any alarm recorded due to the original alarm settings for the recording.
3. To limit the search to a particular time range, enter the start and stop times.
4. Click **Start Search**.
   The results are shown in the **Search results** tab.
5. Click a result to play it back. You can also export JPEGs or mp4 video of the result using the icons below the respective thumbnail.
6. Click the **Search** tab to enter a new search.

6.3.5 Controlling playback

View control

To select a particular region of interest:

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

When you use the electronic pan/tilt on the full image you also zoom into the region of interest automatically.

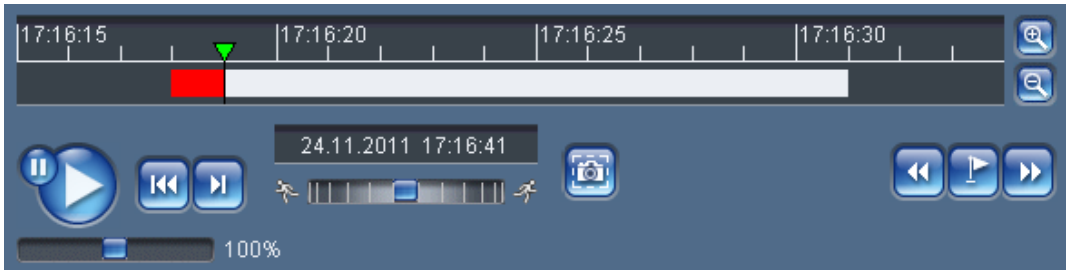
To zoom in on a region of interest:

 Zoom in

 Zoom out

 Reset to full image

Time bar



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

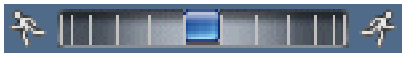
Leap to the start of the active video sequence or to the previous sequence

Leap to the start of the next video sequence

Slide controls

Use the slide control below the Start button to control playback speed. The default value of 100% represents real time speed. Higher values speed up the playback, lower values slow it down.

Use the slide control below the time bar to control playback direction. Drag the rectangle to the right for fast forwarding the playback. Drag it to the left for rewinding.



Making snapshots

You can make a snapshot in JPEG format of the visible area of the sequence currently replayed, e.g. to save them on your computer's hard drive.

▶ Click  to make a snapshot of the visible area.

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

Jump to the previous bookmark

Set bookmark

Jump to the following bookmark

Display stamping

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

Decoding error. The frame might show artefacts due to decoding errors. If subsequent frames reference this corrupted frame, they might also show decoding errors as well but won't be marked with the "decoding error" icon.

Alarm flag set on media item

Communication error. Any kind of communication error is visualized by this icon. Cause can be a connection failure to the storage medium, a protocol violation with a sub component or simply a timeout. An automatic reconnection procedure is started in the background in order to recover from this error.

Gap; no video recorded

Watermarking not valid

Watermarking flag set on media item

Motion flag set on media item

Discovery of storage not completed. If the information about recorded video is not cached, a discovery procedure is started in order find all recorded video. During this time, the “discovery” symbol is shown. While discovery is executed, gaps might be shown in places which the discovery has not yet reached. The gap will automatically be replaced by the true video, as soon as the correct information is available.

Check for updates

You can check for a newer version of the software decoder manually. After clicking the link a new window is opened with instructions on how to proceed.

6.4 The LIVEPAGE

The **LIVEPAGE** page provides an M-JPEG overview of the connected cameras.
Other information may be shown next to the M-JPEG image on the **LIVEPAGE**. The display depends on the settings on the **LIVEPAGE Functions** page.

Further topics:

– *Section 5.7 Web Interface > LIVEPAGE Functions, page 29*

Image selection

▶ Click one of the tabs to toggle between the different cameras or click **Quad View** to see all M-JPEGs at once.

Digital I/O

The alarm icons **Input 1** to **Input 4** 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.

Further topics:

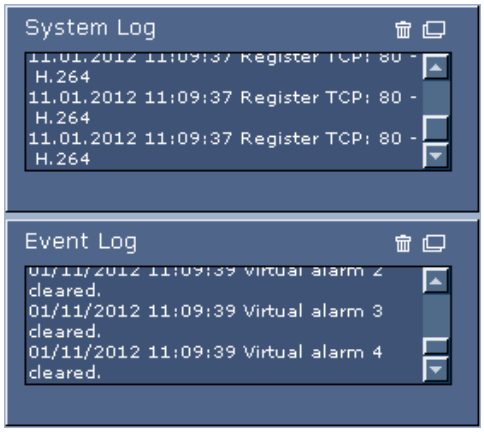
– *Section 5.7 Web Interface > LIVEPAGE Functions, page 29*

Triggering relay

You can switch a connected unit by means of the relay in the VideoJet XTC XF (for example a light or a door opener).

▶ To activate this, click the icon for the 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 VideoJet XTC XF and the connection. You can save these messages automatically in a file.

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.

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.

Further topics:

– *Section 5.7 Web Interface > LIVEPAGE Functions, page 29*

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.

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.

1. If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page.
2. Using a pointed object, press the Factory Reset button located below the CF slot until the **CONNECT** LED flashes red. All settings will revert to their defaults.
3. Change the IP address of the transcoder if necessary.
4. Configure the unit to meet your requirements.

Further topics:

– *Section 5.24 Service > Maintenance, page 52*
– *Section 3.4 Connections, controls and displays, page 13*
– *Section 4.6 Setup using Bosch Video Client, page 19*

7.3 Repairs

– Never open the housing of the unit. 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). In case of doubt, contact your dealer's technical service center.

7.4 Transfer and disposal

The VideoJet XTC XF transcoder 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. 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.

Further topics:
- *Section 5.26 Service > System Overview, page 54*
- *Section Maintenance log, page 53*

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 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.
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.
	Faulty data transmission within the LAN.	Check the data transmission with e.g. **ping**.
	The maximum number of connections has been reached.	Wait until there is a free connection and then call the unit again.
The unit does not report an alarm.	Alarm source is not selected.	Check alarm source settings.
	No alarm response specified.	Specify the desired alarm response, change the IP address, if necessary.
No serial data transmission.	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.

Malfunction	Possible causes	Recommended solution
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 it, 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 Bosch product catalog on the Internet.
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 **CONNECT** 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 target, no LUNs are displayed.	Incorrect LUN mapping during iSCSI system configuration.	Check the iSCSI system configuration and reconnect.
After connecting to the iSCSI target, "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.

8.4 LEDs

The VideoJet XTC XF transcoder has LEDs that show the operating status and can give indications of possible malfunctions:

CONNECT LED

Does not light up:	The unit is switched off.
Lights up green:	The unit is switched on.
Lights up red:	Startup in progress.
Flashes green:	Data packet transmission via network.
Flashes red:	The unit is faulty, for example following failed firmware upload.

LINK LED

Lights up green:	Network connection established.

REC LED

Flashes orange:	Recording in progress.

8.5 Information elements

If the VideoJet XTC XF is accessed via the Web browser, the title bar provides you with various links and information elements.
In the right part of the title bar you see the processor load indicator next to the information icon. Here you can obtain additional information to help you when troubleshooting or fine tuning the unit.

1. The processor load indicator shows the proportions of the individual functions sorted by color. Move the cursor over the indicator to show the color code and the percentages.
2. Move the cursor over  to display information about the network connection:

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

8.6 Serial interface

Options for using the serial interface include transferring transparent data or controlling connected units.
The serial interface supports the RS-232, RS-422 and RS-485 transmission standards. The mode used depends on the current configuration. Connection is via the terminal block.

Further topics:
- *Section 5.17 Interfaces > COM1, page 42*
- *Section 8.7 Terminal block, page 68*

8.7 Terminal block

The terminal block has several contacts for:
- 4 alarm inputs
- 1 relay output
- Serial data transmission

Pin assignment serial interface
The pin assignment of the serial interface depends on the interface mode used.

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)	–	–

Further topics:
- *Section 5.17 Interfaces > COM1, page 42*

Pin assignment I/O

Contact	Function
IN1	Input alarm 1
IN2	Input alarm 2
IN3	Input alarm 3
IN4	Input alarm 4

Contact	Function
GND	Ground
R	Relay output

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

8.8 Copyrights

Fonts

The firmware uses the fonts "Adobe-Helvetica-Bold-R-Normal--24-240-75-75-P-138-ISO10646-1" and "Adobe-Helvetica-Bold-R-Normal--12-120-75-75-P-70-ISO10646-1" under the following copyright:

Software

This software is based in part on the work of the Independent JPEG Group.

9 Specifications

9.1 VideoJet XTC XF

Operating voltage	12 VDC, power supply via external unit polarity: ⊖—C—⊕; jack must fit a pin of 2 mm (0.079 in) in diameter
Current consumption	0.75 A
Power consumption	Approx. 9 W
LAN interfaces	1 × Ethernet 10/100 Base-T, automatic adjustment, half/full duplex, RJ45
COM port	1 × RS-232/RS-422/RS-485, bidirectional, push-in terminal
CF slot	1 × CF CARD, for standard Type I/II CF card, 2 TB max
Alarm inputs	4 × push-in terminals (non-isolated closing contact), maximum activation resistance 10 Ohm
Relay output	1 × push-in terminals, 30 V_{p-p} (SELV), 200 mA
Displays	3 × LED (operation, network connection, data transfer, recording) on the rear panel
Thermal value	31 BTU/h max
Operating conditions	Ambient temperature: 0 to +50 °C (+32 to +122 °F) Relative humidity: 0 to 90%, non-condensing
Approvals	IEC 60950-1; IEC 62676-2; EN 50132-5-2; UL-listed; EN 50130-4; EN 50121-4; EN 55103-1; EN 55103-2; EN 55022; EN 55024; EN 61000-3-2; EN 61000-3-3; FCC 47 CFR Part 15 Subpart B Class B; AS/NZS 3548 Class B
Dimensions (H × W × D)	38 × 146 × 178 mm (1.5 × 5.7 × 7.0 in)
Weight	Approx. 0.6 kg (1.3 lb)

Protocols/standards

Video standards	PAL, NTSC
Video coding protocols	H.264 Main Profile, H.264 Baseline Profile (ISO/IEC 14496-10) M-JPEG, JPEG
Video data rate	9.6 kbps to 10 Mbps per channel
Total delay	120 ms max
Frame rate	1 to 25/30 (PAL/NTSC)
Network protocols	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP, ICMP, RTSP, FTP, Telnet, ARP, DHCP, SNTP, SNMP (V1, MIB-II), 802.1x, SMTP, iSCSI, UPnP (SSDP)
Encryption	TLS 1.0, SSL, AES (optional)

9.2 Power supply unit delivered

Operating voltage	100 to 240 VAC
Operating conditions	Ambient temperature: 0 to +40 °C (+32 to +104 °F) Relative humidity: 20 to 80%, non-condensing
Storage conditions	Ambient temperature: –20 to +80 °C (–4 to +176 °F) Relative humidity: 10 to 95%, non-condensing

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

Adaptive Bit Rate	Adaption of encoder produced bit rate to available bandwidth
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
Dynamic Transcoding	Bosch technology that reencodes IP video for adaptation to the available bandwidth to the viewing client
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
Instant Display Enhancement	Bosch technology that enhances image resolution and quality of paused transcoded video to the maximum extent
Internet Protocol	The main protocol used on the Internet, normally in conjunction with the Transfer Control Protocol (TCP): TCP/IP. Since version 4 (IPv4) has only limited address space, a successor version (IPv6) has already been developed to meet the growing needs for Internet addresses.
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"
IPv4	*See* Internet Protocol
IPv6	*See* Internet Protocol
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

S

T

U

V

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com