

VIP X1



Security Systems

EN | Installation and Operating Manual
Network Video Server

BOSCH

Copyright

This manual is copyrighted material of Bosch Security Systems. All rights reserved. Without express written permission from Bosch Security Systems no portion of this document may be reproduced or transmitted for any reasons, regardless of the means or manner employed, mechanical or electronic.

Issue: December 2006 (Version 2.5)

© Copyright 2006 Bosch Security Systems

Note

This manual was prepared with care and all information contained herein was reviewed. At the time of printing, the description was complete and correct. As the result of product improvements, the contents of this manual may change without notice. Bosch Security Systems assumes no liability for damage, either direct or indirect, arising from mistakes, incompleteness or discrepancies between this manual and the product described.

Trade marks

All names used in this manual for hardware and software are probably registered trade marks and should be treated as such.

Contents

Chapter 1 Preface	
Conventions	7
Intended use	8
EU Directives	8
Rating plate	8
Chapter 2 Safety information	
Electric shock hazard	9
Installation and operation	10
Maintenance and repair	10
Chapter 3 Product description	
Components supplied	11
System requirements for setup	11
Configuration requirements	12
Operational requirements	12
Overview of functions	13
Connections on the front panel	16
Connections on the rear panel	17
Chapter 4 Installation	
Connections	20
Power on/Power off	24
Setup using the Configuration Manager	25
Chapter 5 Configuration using a Web browser	
Connecting	27
Configuration menu	30
Unit identification	32
Password	32
Language	34
Date and time	34
Time server	35
Camera name	36
Display stamping	37
Picture settings	39
MPEG-4 encoder	41

Video input	46
Audio settings (audio version only)	47
JPEG posting	48
Storage medium	50
iSCSI settings	52
Partitioning	56
Recording profiles	63
Recording scheduler	66
Alarm sources	69
Alarm connections	70
VCA	73
Alarm e-mail	79
Relay	81
COM1	83
Network	85
Multicasting	89
Encryption	91
Version information	93
Livepage configuration	94
Licenses	97
Maintenance	98
Function test	101

Chapter 6 Operation

Operation with Microsoft Internet Explorer	103
The LIVEPAGE	105
Saving snapshots	108
Recording video sequences	108
The RECORDINGS page	110
Backup	114
Installing Player	115
Replaying USB hard drive recordings on PC	116
Hardware connections between video servers	118
Operation with decoder software	120

Chapter 7 Maintenance and upgrades

Testing the network connection	121
Unit reset	121
Repairs	122
Transfer and disposal	122

Chapter 8 Appendix

Troubleshooting	123
LEDs.	126
Processor load	126
Serial interface	127
Terminal block	127
Communication with terminal program.	129
Glossary	132
Specifications	135

Chapter 9 Index

1

Preface

This manual is intended for persons responsible for the installation and operation of the VIP X1. 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.

Conventions

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.



Note

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

Intended use

The VIP X2 network video server transmits video and control signals over data networks (Ethernet LAN, Internet). Audio signals can also be transmitted with the audio version of the unit. The units are designed for use in 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 units which are not answered in this manual, please contact your sales partner or:

Bosch Sicherheitssysteme GmbH
Robert-Koch-Straße 100
85521 Ottobrunn
Germany

www.bosch-sicherheitssysteme.de

EU Directives

The VIP X2 network video server complies with the requirements of EU Directives 89/336 (Electromagnetic Compatibility) and 73/23, amended by 93/68 (Low Voltage Directive).

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

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 unit provided.
- Never open the housing.
- Never open the housing of the power supply unit.
- If a fault occurs, disconnect the power supply unit from the power supply and from all other units.
- Install the power supply and the unit only in a dry, weather-protected location.
- If safe operation of the unit cannot be ensured, remove it from service and secure it to prevent unauthorized operation. 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.

In such cases, have the unit checked by Bosch Security Systems.

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.

Maintenance and repair

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

3

Product description

Components supplied

- VIP X1 network video server (basic version or audio version)
- Power supply unit with four primary adapters
- Configuration cable
- Quick Installation Guide
- Product CD with the following content:
 - Quick Installation Guide
 - Manual
 - System Requirements document
 - Configuration Manager
 - MPEG ActiveX control
 - Player and Archive Player
 - DirectX control
 - Microsoft Internet Explorer
 - Sun JVM
 - Adobe Acrobat Reader

Note

Check that the delivery is complete and in perfect condition. Have your unit checked by Bosch Security Systems if you detect any damage.

System requirements for setup

- Computer with Windows 2000/XP operating system, access to a network and Microsoft Internet Explorer (version 6.0 or higher)
- or
- Computer with Windows 2000/XP operating system, access to a network and an installed Configuration Manager program

Configuration requirements

- Computer with Windows 2000/XP operating system, access to a network and Microsoft Internet Explorer (version 6.0 or higher)
or
- Computer with Windows 2000/XP operating system, access to a network and an installed Configuration Manager program

Note

Take also note of the information in the **System Requirements** document on the product CD supplied. Make sure the graphics card is set to 16- or 32-bit color depth and that Sun JVM is installed and activated on your PC. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11).

Operational requirements

- Computer with Windows 2000/XP operating system, access to a network and Microsoft Internet Explorer (version 6.0 or higher)
or
- Computer with Windows 2000/XP operating system, access to a network and receiver software, for example VIDOS or Bosch Video Management System
or
- MPEG-4 compatible hardware decoder from Bosch Security Systems (for example VIP X1D) as a receiver and connected video monitor
- For recording and playback: Access to an iSCSI server that is configured and ready for operation

Note

Take also note of the information in the **System Requirements** document on the product CD supplied. Make sure the graphics card for reception on the computer monitor is set to 16- or 32-bit color depth and that Sun JVM is installed and activated on your PC. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11).

Overview of functions

Network video server

The VIP X1 is an ultra-compact network video server for one connected video source. It is primarily designed for encoding video and control data for transfer over an IP network. With its encoding in the MPEG-4 format, the VIP X1 is ideally suited for making existing analog CCTV cameras IP-compatible and for remote access to digital video recorders and multiplexers.

The VIP X1 is small enough to be easily integrated into small housings as well. The use of existing networks means that integration with CCTV systems or local networks can be achieved quickly and easily.

Two units, a VIP X1 as a sender and a VIP XD as a receiver for example, can create a standalone system for data transfer without a PC. Video images from a single sender can be received simultaneously on multiple receivers. The audio version of the VIP X1 also allows the transmission of audio signals from and to compatible units. The PoE version (Power-over-Ethernet) of the VIP X1 enables power to be supplied via the network cable without an external power adapter. This requires a network infrastructure that supports PoE standard IEEE 802.11af.

Receiver

Compatible MPEG-4 enabled hardware decoders (such as VIP XD) can be used as receivers. Computers with decoding software installed, such as VIDOS, or computers with the Microsoft Internet Explorer Web browser can also be used as receivers.

Video encoding

The VIP X1 uses the MPEG-4 video compression standard. Thanks to efficient encoding, the data rate remains low even with high image quality and can also be adapted to local conditions within wide limits.

Dual Streaming

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

Multicast

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

Encryption

To prevent unauthorized access, the authentication process, as well as the actual data transmissions can be encrypted. Web browser connections can be protected using HTTPS.

Remote control

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

Tampering recognition and motion detectors

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

Snapshots

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

Backup

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

Summary

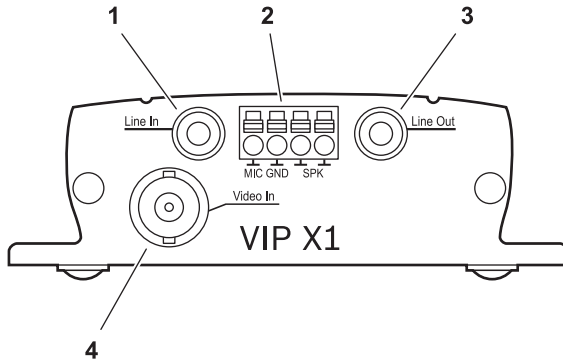
The VIP X1 provides the following main functions:

- Video and data transmission over IP data networks
- Dual Streaming function for the encoder for simultaneous encoding with two individually definable profiles
- Multicast function for simultaneous picture transmission to multiple receivers
- Analog BNC composite video input (PAL/NTSC)
- Video encoding to international standard MPEG-4
- Integrated Ethernet port (10/100 Base-T)
- Transparent, bidirectional data channel with an RS232/RS422/RS485 serial interface
- Configuration and remote control for all internal functions with TCP/IP, also secured via HTTPS
- Password protection to prevent unauthorized connection or configuration changes
- Extensive, flexible recording options
- Four alarm inputs and one relay output
- Built-in video sensor for motion and tamper alarms
- Event-driven automatic connection
- Convenient maintenance via uploads
- Flexible control and data channel encryption
- Authentication according to international standard 802.1x
- PoE power supply according to IEEE standard 802.11af (variant)

The audio version also offers:

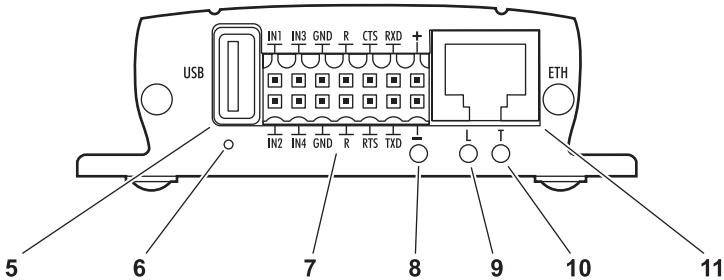
- Transmission and receipt of audio signals
- Bidirectional audio (mono) for line or microphone/speaker links
- Audio encoding to international standard G.711

Connections on the front panel



- 1** Audio line input **Line In** (audio version only)
3.5 mm stereo jack socket for connecting one audio line input signal
- 2** Terminal connector (audio version only)
for microphone and loudspeaker connections
- 3** Audio line output **Line Out** (audio version only)
3.5 mm stereo jack socket for connecting an audio line output signal
- 4** Video input **Video In**
BNC socket for connecting a video source

Connections on the rear panel



- 5 USB port**
for connecting a USB storage medium (external hard drive)
- 6 Factory reset button**
to restore factory default settings
- 7 Terminal block**
for alarm inputs, relay output, serial interface and power supply
- 8 Operating status LED**
lights up green when ready for operation
- 9 LED L**
lights up green when the unit is connected to the network
- 10 LED T**
flashes orange when data is being transmitted over the network
- 11 RJ45 socket **ETH****
for connecting to an Ethernet LAN (local network),
10/100 MBit Base-T

For more information about the LEDs see page 126. For information about the terminal block connections see page 127.

4

Installation

Thanks to its ultra-compact dimensions, the VIP X1 is particularly well suited to installation in cabinets.



Caution

The unit is intended for use indoors or in housings. Select a suitable location for installation where the unit will not be subjected to conditions of extreme temperature or humidity. The ambient temperature must be between 0 and +50°C (+32 and +122°F); the relative humidity must not exceed 80%.

The unit generates heat during operation, so you should ensure that there is adequate ventilation and enough clearance between the unit and heat-sensitive objects or equipment.

Please ensure the following installation conditions:

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

Connections

Cameras

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

- Connect the camera or another video source with a video cable (75 Ohm, BNC connector) to the BNC **Video In** sockets.
- If the video signal is not looped through, termination is performed by a software setting if necessary (see **Video input**, page 46).

Audio connections (audio version only)

The audio version of the VIP X1 has two audio ports for audio line signals as well as a microphone input and a loudspeaker output.

The audio signals are transmitted two-way and in sync with the video signals. As a result, you can connect a speaker or door intercom system at the destination point, for example.

Note

If possible you should use the line ports of the intercom for transmitting audio signals on the intercom systems. The following specifications should be complied with in all cases.

Line In:	Impedance 9 kOhm typ., 5.5 V _{p-p} max. input voltage
Line Out:	Impedance 16 Ohm min., 3 V _{p-p} max. output voltage
MIC (microphone):	Impedance 2 kOhm typ., 2.8 V _{p-p} max. input voltage, -20 dB in, supply 2.3 V typ.
SPK (speaker):	Impedance 4 Ohm min., 6 V _{p-p} max. output voltage, power output RMS 1 W

The stereo jack plugs must be connected as follows:

Contact	Function
Tip	Channel 1 (camera)
Middle ring	Not used
Lower ring	Ground

- Connect an audio source with line level to the **Line In** jack socket of the VIP X1 with a 3.5 mm stereo jack plug.
- Connect a unit with line-in connection to the **Line Out** jack socket of the VIP X1 with a 3.5 mm stereo jack plug.

If you wish to connect a microphone and a loudspeaker directly:

- Connect the microphone cords to the **MIC** and **GND** connections on the push-in terminal.
- Connect the loudspeaker cords to the **SPK** connections on the push-in terminal.

Data interface

The bidirectional data interface is used to control units connected to the VIP X1, such as a dome camera with a motorized lens.

The interface supports the RS232, RS422 and RS485 transmission standards. The interface is made up of four terminals of the ST500 jack (for pin assignment, see page 127).

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.



Note

A video connection is necessary to transmit transparent data.

Network

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

- Connect the unit to the network using the **ETH** socket.

Alarm inputs

The VIP X1 has four alarm inputs on the orange terminal block (for pin assignment, see page 127). The alarm inputs are used to connect to external alarm devices such as door contacts or sensors. With the appropriate configuration, an alarm sensor can automatically connect the VIP X1 to a remote location, for example.

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

Note

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

- Connect the lines to the appropriate terminals on the orange terminal block (**IN1** to **IN4**) and check that the connection is secure.

Relay output

The VIP X1 has a relay output for switching external units such as lamps or sirens. This relay output can be activated manually during a connection session with the VIP X1. The output can also be configured to automatically activate sirens or other alarm units in response to an alarm signal. The relay output is also located on the orange terminal block (for pin assignment, see page 128).



Caution

The maximum rating of the relay contact is 30 V and 2 A.

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

USB interface

The USB interface supports the USB 2.0 standard and enables a connection to an external hard drive using a USB interface.

When a connection is first made to a USB hard drive, the VIP X1 checks whether a compatible file system exists on the hard drive. If none is available, the VIP X1 creates a new one. In doing so, all existing data is deleted. If a compatible file system is already present on the hard drive, any data already stored remains on the drive. The drive can then easily be used for further recordings.

A PC can also be used for playing back recordings, irrespective of whether a connection to the VIP X1 exists (see page 116).



Caution

Check whether any other data that should be backed up exists on the drive before plugging in the drive. All other data on the drive is deleted as soon as the VIP X1 is switched on.

- Connect the external drive to the **USB** port of the VIP X1 using a USB cable.

Power on/Power off

Power supply

The VIP X1 comes with a plug-in power supply unit (PSU) with four primary adapters and a terminal block. The VIP X1 does not have a power switch. The unit is ready for operation as soon as it is connected to the power supply.



Caution

The VIP X1 may only be operated using the supplied PSU with the correct primary adapter for your power outlet. Where necessary, use suitable equipment to ensure that the power supply is free from interference such as voltage surges, spikes or voltage drops.

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

- Plug the terminal block with the PSU cable connected into the orange socket on the VIP X1.
- Ensure that the correct primary adapter is attached to the power supply unit and that a suitable power outlet is available.
- Plug the power supply unit into the grounded power outlet. The unit is ready for operation as soon as the "operating status" LED stops flashing red during start-up and lights up green.

Provided the network connection has been correctly made, the green **L** LED also lights up. The flashing orange **T** LED indicates data traffic on the network.

Setup using the Configuration Manager

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

Note

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

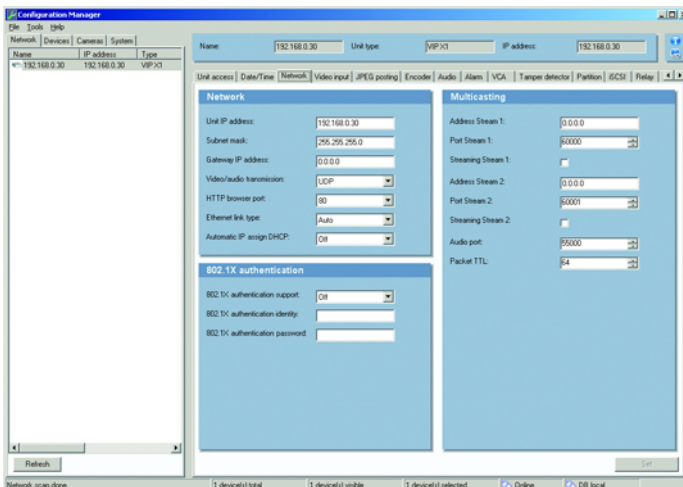
Installing the program

- Insert the CD in the CD-ROM drive of the computer.
- If the CD does not start automatically, open the **Configuration Manager** directory using Windows Explorer and double click **Setup.exe**.
- Follow the on-screen instructions.

Configuring the VIP X1

You can start the Configuration Manager immediately after installation.

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



- You can start the configuration if a VIP X1 is shown in the list in the left section of the window. To do this, click the entry for the unit.
- Click the **Network** tab in the right section of the window. The current network settings are displayed.
- In the IP address field, enter the required IP address (for example 192.168.0.30) and click the **Set** button at the bottom right of the window. The new IP address is valid the next time you start the unit.
- If required, enter a new subnet mask and additional network data.

**Note**

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

Restart

You can trigger the restart directly with the assistance of the Configuration Manager:

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

Additional parameters

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

5

Configuration using a Web browser

Connecting

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

Note

Make sure the graphics card is set to 16- or 32-bit color depth and that Sun JVM is installed and activated on your PC. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11).

Instructions for using the Web browser can be found in its online help.

System requirements

- Microsoft Internet Explorer (version 6.0 or higher)
- Monitor resolution 1024 × 768 pixels
- Network access (Intranet or Internet)

Note

Take also note of the information in the **System Requirements** document on the product CD supplied.

Installing MPEG ActiveX

Note

Suitable MPEG ActiveX software must be installed on the computer to allow the live video images to be played back. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11).

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

Establishing the connection

The VIP X1 must be assigned a valid IP address to operate on your network.

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

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



Maximum number of connections

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

Protected VIP X1

If the VIP X1 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.

Note

The VIP X1 offers the option to limit the extent of access using various authorization levels (see page 32).

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

Protected network

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

For configuration you must connect the VIP X1 directly to a computer using a crossed network cable since communication via the network is only possible when the parameters **Identity** and **Password** have been set and authentication was successful (see page 88).

Configuration menu

You can access the configuration menu via the **SETTINGS** page. This menu displays all the parameters of the unit, 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 in the configuration menu should only be processed or modified by expert users or system support personnel.

All settings are backed up in the VIP X1 memory so they are not lost even if the power fails.

Start configuration

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



Navigation

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

Making changes

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

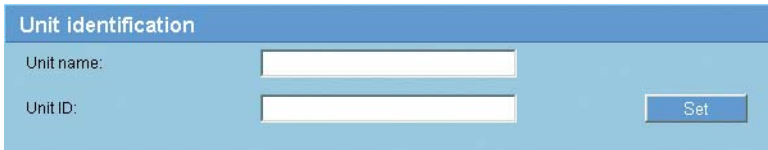
- After each change, click **Set** to save the change.



Caution

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

Unit identification



The screenshot shows a web form titled "Unit identification" with a blue header. Below the header, there are two input fields: "Unit name:" and "Unit ID:". To the right of the "Unit ID:" field is a blue "Set" button.

Unit name:

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

Note

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

Unit ID:

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

Password



The screenshot shows a web form titled "Password" with a blue header. Below the header, there are three input fields: "User name:" with a dropdown menu showing "user", "Password:", and "Confirm password:". To the right of the "Password:" field is a red error message: "No 'user' password set!". To the right of the "Confirm password:" field is a blue "Set" button.

A VIP X1 is generally protected by a password to prevent unauthorized access to the unit. You can use different authorization levels (**User name:**) to control access.

 **Note**

Proper password protection is only guaranteed when all higher authorization levels are also protected with a password. If a **live** password is assigned for example, a **service** and a **user** password must also be set. As a result, you should always assign passwords beginning with the highest authorization level **service**.

User name:

The VIP X1 operates with three user names: **service**, **user** and **live**, which correspond to different authorization levels.

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

The **user** user name is the middle authorization level. You use it to operate the unit and also to control cameras, but you cannot change the configuration.

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

Password:

You can define and change a separate password for each user name if you are logged in as **service** or if the unit is not password protected.

Enter the password for the selected user name here.

Confirm password:

Enter the new password a second time to eliminate typing mistakes.

 **Note**

The new password is only saved when you click the **Set** button. You should therefore click the **Set** button immediately after entering and confirming a password, even if you also wish to subsequently assign a password to another user name.

Language



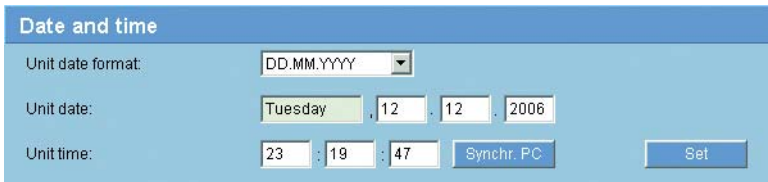
Language

Website language: English

Website language:

Select the language for the user interface here.

Date and time



Date and time

Unit date format: DD.MM.YYYY

Unit date: Tuesday, 12, 12, 2006

Unit time: 23 : 19 : 47

Unit date format:

Select your required date format.

Unit date and Unit 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.

- 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.
- Enter the current clock time or click the **Synchr. PC** button to apply the system time from your computer to the VIP X1.

Time server

Time server

Unit time zone:

Daylight saving time:

Time server IP address:

Time server type:

The VIP X1 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.

Unit time zone:

Select the time zone in which your system is located.

Daylight saving time:

The internal clock can automatically switch between normal and daylight saving time (DST). The unit already contains the data for DST-switchovers up to the year 2015. These can be used or modified, if required.

Note

If you do not create a table, there will be no automatic switching. When editing the table, please note that the values generally occur in linked pairs (DST start and end dates).

- First check the timezone setting. If it is not correct, select the appropriate timezone for the system, and click the **Set** button.
- Click the **Details** button. A new window will open showing an empty table.
- Select the region or the city which is closest to the system's location from the list box below the table.
- Click the **Generate** button to fill the table with the preset values from the unit.
- Click one of the entries in the table to make changes. The entry will be highlighted.
- Clicking the **Delete** button will remove the entry from the table.
- Choose other values from the list boxes under the table, to change the selected entry. Changes are immediate.

- 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 values from the list boxes.
- When you are finished, click the **OK** button to save and activate the table.

Time server IP address:

Enter the IP address of the time server here.

Time server type:

Choose the protocol used by the selected time server. Always choose **SNTP server** as protocol, if it is supported by the time server. This protocol provides higher accuracy and is required for certain applications, as well as for later additions.

Choose **Time server**, if the server uses RFC 868 as protocol.

Camera name



Camera name

Camera 1:

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

Camera 1:

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

Display stamping

Display stamping

Camera name stamping: Position (XY): / (0..255)

Time stamping:

Alarm mode stamping:

Displayed alarm message: (max. 31 characters)

Video watermarking:

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

Camera name stamping:

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

Time stamping:

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

Alarm mode stamping:

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

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

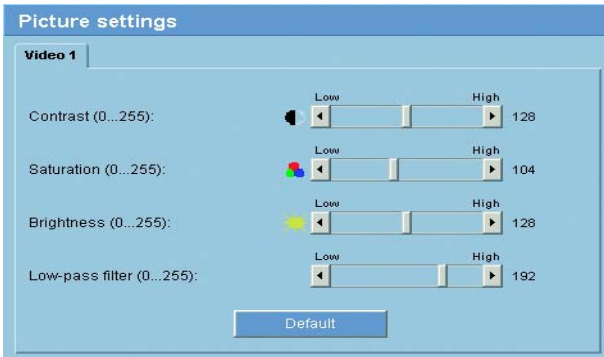
Displayed alarm message:

Enter the message to be displayed for an alarm. The maximum text length is 31 characters.

Video watermarking:

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

Picture settings



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

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

Contrast (0...255):

You can use this function to adapt the contrast of the video image to your working environment.

Saturation (0...255):

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

Brightness (0...255):

You can use this function to adapt the brightness of the video image to your working environment.

Low-pass filter (0...255):

You can use this function to filter fine-grained noise out of the image. Thus you reduce and optimize the bandwidth necessary for image transmission over the network. This may reduce the image resolution.

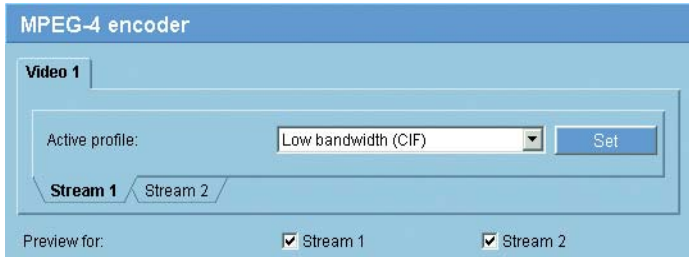
The higher the value given by the slide control the smoother the image signal. Check your settings controlling the video window next to the slide controls.

Also watch the indicator for the processor load displayed on top of the window on the left of the unit name (compare page 126).

MPEG-4 encoder

For encoding the video signal you can select two profiles and change the pre-sets for the profiles.

Selecting a profile



You can adapt the MPEG-4 data transmission to the operating environment (for example network structure, bandwidth, data load). To this end, the VIP X1 simultaneously generates two data streams (Dual Streaming), which compression settings you can select individually, for example one setting for transmissions to the Internet and one for LAN connections.

Pre-programmed profiles are available, each giving priority to different perspectives.

- **Profile 1: Low bandwidth (CIF)**
High quality for low bandwidth connections,
resolution 352 × 288/240 pixels
- **Profile 2: Low delay (2/3 D1)**
High quality with low delay,
resolution 464 × 576/480 pixels
- **Profile 3: High resolution (4CIF/D1)**
High resolution for high bandwidth connections,
resolution 704 × 576/480 pixels
- **Profile 4: DSL**
For DSL connections at 500 kBit/s,
resolution 352 × 288/240 pixels
- **Profile 5: ISDN (2B)**
For ISDN connections via two B channels,
resolution 352 × 288/240 pixels

■ Profile 6: ISDN (1B)

For ISDN connections via one B channel,
resolution 352 × 288/240 pixels

■ Profile 7: Modem

For analog modem connections at 20 kBit/s,
resolution 352 × 288/240 pixels

■ Profile 8: GSM

For GSM connections at 9,600 baud,
resolution 176 × 144/120 pixels

Active profile:

Here you can select the desired profile for each of the two streams. You will see a preview for each data stream in the right section of the window. The preview of the data stream currently selected is marked by a green frame. Above the previews, various additional items of information regarding data transmission are displayed and continually updated.

- Click a tab at the bottom to select the associated stream.
- Select the desired setting from the list.

**Note**

Stream 2 is always transmitted for alarm connections and automatic connections. Bear this fact in mind when assigning the profile.

Preview for:

Select which video data stream should be displayed in the previews. You can deactivate the display of the video images if the performance of the computer is affected too strongly by the decoding of the data streams.

Check the box for the required data stream.

Profile configuration

Profile configuration

Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 | Profile 7 | Profile 8

Profile name:

Target data rate: kBit/s

Encoding interval: (0.00 fps)

Video resolution:

Details

Max. data rate: kBit/s High Low

P-frame quality: High Low

I-frame quality: High Low

I-frame distance:

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



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.



Note

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

Profile name:

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

Target data rate:

You can limit the data rate for the VIP X1 to optimize utilization of the bandwidth in your network. The target data rate should be set according to the desired picture quality for typical scenes with no excessive motion.

For complex images or frequent changes of image content due to frequent movements, this limit can be temporarily exceeded up to the value you enter in the **Max. data rate** field.

Encoding interval:

The figure selected here determines the interval at which images are encoded and transmitted. For example, entering **4** means that only every fourth image is encoded, the following three are skipped - this can be particularly advantageous with low bandwidths. The image rate in ips (images per second) is displayed beside the text box.

Video resolution:

Here you can select the desired resolution for the MPEG-4 video image. The following resolutions are available:

- **QCIF** 176 × 144/120 pixels
- **CIF** 352 × 288/240 pixels
- **1/2 D1** 352 × 576/480 pixels
- **2CIF** 704 × 288/240 pixels
- **4CIF/D1** 704 × 576/480 pixels
- **2/3 D1** 464 × 576/480 pixels

Default

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

Details

After clicking the **Details >>** button, further settings for image quality and communication parameters are displayed.

These settings require familiarity with MPEG and video encoding standards. Incorrect settings could result in useless video images.

Max. data rate:

This maximum data rate is not exceeded under any circumstances. Depending on the video quality settings for the I- and P-frames, this fact can result in skipping of individual images.

The value entered here should be at least 10% higher than the value entered in the **Target data rate** field.

P-frame quality:

This setting allows you to adjust the image quality of the P-frames depending on the movement within the image. The **Auto** option automatically adjusts to the optimum combination of movement and image definition (focus). Selecting **Manual** allows you to set a value between 4 and 31 on the slide control. The value **4** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **31** results in a very high refresh rate and lower image quality.

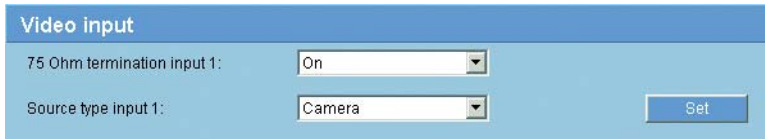
I-frame quality:

This setting allows you to adjust the image quality of the I-frames. The **Auto** option automatically adjusts the quality to the settings for the P-frame video quality. Selecting **Manual** allows you to set a value between 4 and 31 on the slide control. The value **4** represents the best image quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of **31** results in a very high refresh rate and lower image quality.

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 when necessary. An entry of **1** indicates that I-frames are continuously generated. An entry of **2** indicates that only every second image is an I-frame, and **3** only every third image etc.; the frames in between are coded as P-frames.

Video input



Video input	
75 Ohm termination input 1:	<input type="text" value="On"/>
Source type input 1:	<input type="text" value="Camera"/> <input type="button" value="Set"/>

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

75 Ohm termination:

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

Source type:

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

Note

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

Audio settings (audio version only)

	Gain	Peak	Selection
Line In 1:	<input type="range"/>	13	<input checked="" type="radio"/>
Microphone (MIC):	<input type="range"/>	0	<input type="radio"/>
Line Out/Speaker (SPK):	<input type="range"/>	30	<input type="radio"/>

You can set the gain of the audio signals to suit your specific requirements. The current video image is shown in the small window next to the slide controls to help you check the selected audio source and improve assignments. Your changes are effective immediately.

If you connect via Web browser you must activate the audio transmission on the **Livepage configuration** page (see page 94). For other connections the transmission depends on the audio settings of the respective system.

Line In 1: / Microphone (MIC):

You can set the gain of the audio signal for the line input and for the microphone input. Make sure that the display does not go beyond the green zone during modulation.

Line Out/Speaker (SPK):

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

Selection

Click one of the option boxes and then click **Set** to display the level of the respective audio input for orientation and to set the gain.

JPEG posting

You can save individual JPEG images on an FTP server at certain intervals. You can then retrieve these images at a later date to reconstruct alarm events if required.

JPEG format:

Select the resolution you wish the JPEG images to have:

- **Small** 176 × 144/120 pixels (QCIF)
- **Medium** 352 × 288/240 pixels (CIF)
- **Large** 704 × 576/480 pixels (4CIF)

File name:

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

- **Overwrite:** The same file name is always used and any existing file will be overwritten with the current file.
- **Increment:** A number from 000 to 255 is added to the file name and automatically incremented by 1. When it reaches 255 it starts again from 000.
- **Date/time suffix:** The date and time are automatically added to the file name. When setting this parameter, ensure that the unit's date and time are always correctly set. Example: the file snap011005_114530.jpg was stored on October 1, 2005 at 12.45 p.m. and 30 seconds.

JPEG posting interval:

Enter the interval in seconds at which the images will be sent to an FTP server.
Enter zero if you do not want any images to be sent.

FTP server IP address:

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

FTP server login:

Enter your login name for the FTP server.

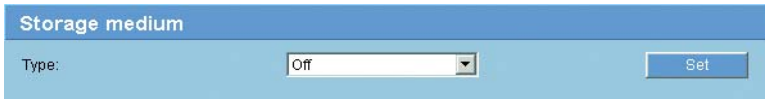
FTP server password:

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

Path on FTP server:

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

Storage medium



Storage medium

Type:

You can record the images from the camera connected to the VIP X1 on an external USB hard drive (see page 23) or in an appropriately configured iSCSI storage device.

It is also possible to let the Video Recording Manager (**VRM**) control all recording, when accessing an iSCSI server. The VRM is an external program for configuring recording tasks for video servers. For further information, please contact your local customer service at Bosch Security Systems.

Type:

Select the desired storage medium to subsequently configure the recording parameters.

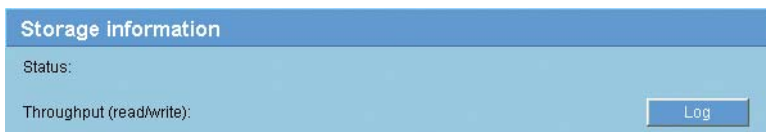
If you select **VRM**, the Video Recording Manager will manage all recording, and you will not be able to make any further configurations here.



Caution

If you switch the storage medium from **iSCSI server** to **USB hard drive**, the settings on the **iSCSI settings** page will be lost and can only be restored by reconfiguring them.

Storage information



The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

- Click **Log** to view a status report with logged actions. A new window will open.
- In this window, click **Delete** to delete all entries. The entries will be deleted immediately; you cannot undo this process.
- Click the **Close** button to close the window.

iSCSI settings

iSCSI settings

iSCSI IP address:

iSCSI LUN map

- iqn.2002-10.com.infortrend:raid.sn6800876.00
- iqn.2002-10.com.infortrend:raid.sn6800876.01
- iqn.2002-10.com.infortrend:raid.sn6800876.02
- iqn.2002-10.com.infortrend:raid.sn6800876.03

Target IP address:

Target node:

Target LUN:

Target password:

Initiator name:

Initiator extension:

If you select type **iSCSI server** as the storage medium, you then need to set up a connection to the desired iSCSI storage device and set the configuration parameters.

Note

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

iSCSI IP address:

- Enter the IP address of the required iSCSI server here.
- Click the **Read** button. The connection to the IP address will be established. The **iSCSI LUN map** field contains the corresponding logical drives.

iSCSI LUN map

The LUN map displays the logical drives configured for the iSCSI storage device. The current user is displayed for each drive.

- Double-click a free drive (LUN). The associated information is called up and automatically displayed in the fields below the map.
- If the logical drive is password protected, you must first enter the password in the **Target password** field and click the **Set** button.

Note

In cases where the information cannot be read due to the network topology, you must enter the data manually, so that the VIP X1 can access the drive. In this case you should ensure that the entries correspond exactly with the configuration of the iSCSI device.

- After entering all the settings in the relevant fields, click **Set**. The VIP X1 attempts to create a connection to the required drive using this data.

As soon as a connection has been established, the selected drive is used for recordings.

Target IP address:

Enter the IP address of the required iSCSI server here.

Target node:

Enter the number of the iSCSI server target node.

Target LUN:

Enter the LUN of the required drive.

Target password:

If the drive is password protected, enter the password.

Note

You may not enter a new password. This is only possible by configuring the iSCSI storage device.

Initiator name:

The initiator name is automatically displayed after a connection has been established.

Initiator extension:

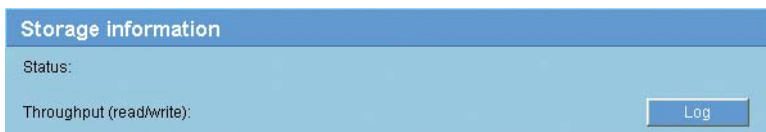
Enter the initiator extension. For the sake of clarity, you can enter a name or the existing extension with a comment, for example "- Camera 1"

Decoupling the drive in use

Each drive can only be associated with one user. If a drive is already being used by another person, you can decouple the drive and connect the drive with the VIP X1.

- Double-click a drive that is already being used in the LUN map. You will see a warning message.
- Confirm the decoupling of the current user. The drive is released and can now be connected to the VIP X1.

Storage information



The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

- Click **Log** to view a status report with logged actions. A new window will open.
- In this window, click **Delete** to delete all entries. The entries will be deleted immediately; you cannot undo this process.
- Click the **Close** button to close the window.

Partitioning

Partitioning

Camera	Partition name	Alarm tracks	Type	Size (MByte)
01	Partition 1	4 alarm track(s) with 102 MByte(s)	Linear mode	43000

Create partition
Edit partition
Partition status
Delete all partitions

Total memory: 44032.0 MByte(s)

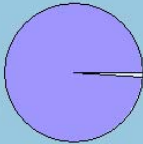
Internally used memory: 456.0 MByte(s)

Available memory: 43576.0 MByte(s)

Number of partitions: 1 of 1 partitions created

Partitioned memory: 43000.0 MByte(s)

Unpartitioned memory: 576.0 MByte(s)



partitioned
 unpartitioned

One partition can be set up for recordings of the camera connected to the VIP X1, in a similar manner to the partitioning often found on computer hard drives. Parameters such as size, quality and type of video recording or compression standard used can be specified for each partition. Modifying these parameters leads to reorganization, during which stored data is lost.

One partition is already pre-configured in the default configuration.

The partition is listed in the table on the page **Partitioning** together with the number of the video input (**Camera**), its partition name, alarm tracks, type and size.

In addition, the page provides you with an overview of the drive data; for example total memory and partitioned memory. A pie chart indicates how much memory space is partitioned for recordings.

Creating a partition

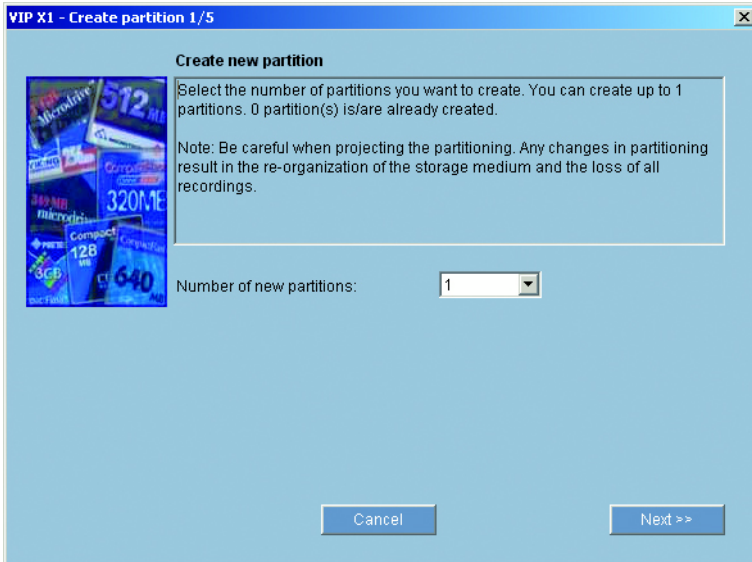
Note

You can set up only one partition.

Creating a new partition is performed using separate windows in which information is presented to you and you are led step by step through the necessary settings.

The process must be completed once.

- Click the **Create partition** button to start the assistant for creating partitions. The first window appears.



- You should always first read the information text in the upper section of the window.
- Click in the text fields to enter values or use the other controls that are available, such as buttons, checkboxes or list fields.
- Click the **Next >>** button in the lower section of the window to continue with the next step.
- Click the **<< Back** button in the lower section of the window to view the previous step again.
- Click the **Cancel** button to cancel the process and close the help.

Saving changes

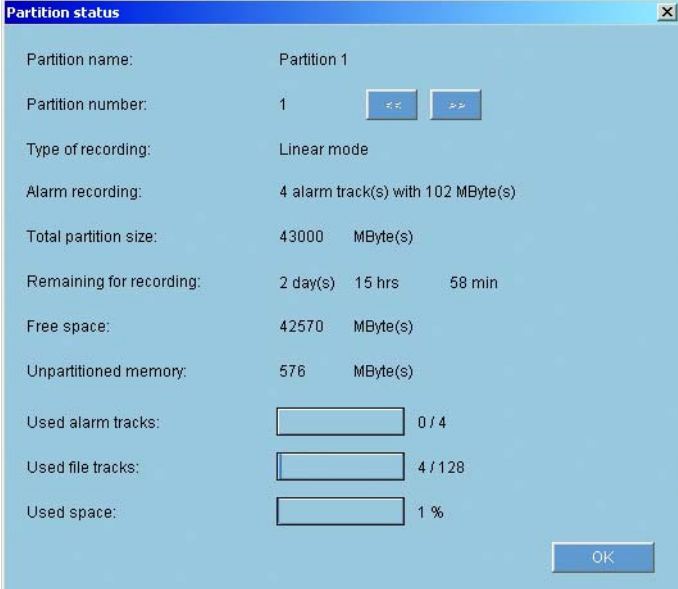
After you have made all necessary settings, you must transfer the settings to the unit and save them. To do this, you need to quit the help in the last window using the **Finish** button.

**Caution**

All modifications to settings are only effective if you complete the configuration in the last window by clicking **Finish**.

- Switch to the last window if necessary.
- Click **Finish** to complete the configuration. All settings are now transferred to the unit and subsequently become effective.

Partition status



The screenshot shows a window titled "Partition status" with a close button (X) in the top right corner. The window displays the following information:

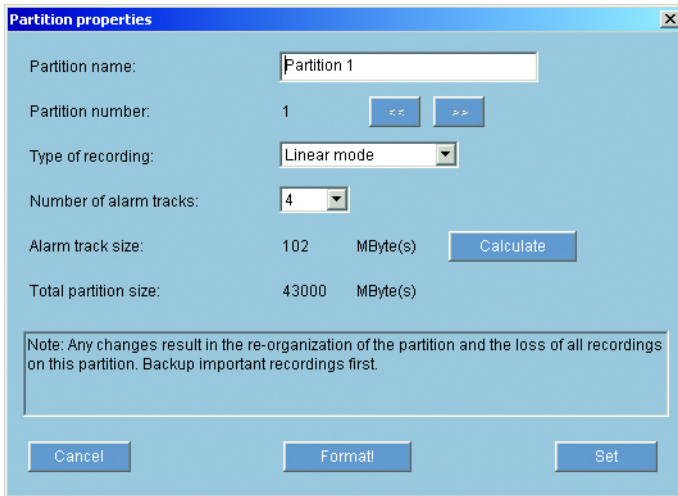
Partition name:	Partition 1		
Partition number:	1	<input type="button" value="←"/>	<input type="button" value="→"/>
Type of recording:	Linear mode		
Alarm recording:	4 alarm track(s) with 102 MByte(s)		
Total partition size:	43000 MByte(s)		
Remaining for recording:	2 day(s) 15 hrs 58 min		
Free space:	42570 MByte(s)		
Unpartitioned memory:	576 MByte(s)		
Used alarm tracks:	<input type="text" value="0"/> / 4		
Used file tracks:	<input type="text" value="4"/> / 128		
Used space:	<input type="text" value="1"/> %		

An "OK" button is located in the bottom right corner of the window.

This window provides information about the current configuration of the partition. No changes can be made here.

- In the list, click the partition to highlight it.
- Click the **Partition status** button. A window will open showing information on the partition.
- Click **OK** to close the window.

Editing a partition



Partition properties

Partition name:

Partition number:

Type of recording:

Number of alarm tracks:

Alarm track size: MByte(s)

Total partition size: MByte(s)

Note: Any changes result in the re-organization of the partition and the loss of all recordings on this partition. Backup important recordings first.

You can modify the configuration of the partition at any time.



Caution

Changes to the partition lead to a reorganization of the partition, resulting in the loss of all sequences stored on it. Consequently, you should back up all important sequences on the computer's hard drive before modifying the partition.

You can perform the required modifications in the **Partition properties** window.

- In the list, click the partition to highlight it.
- Click the **Edit partition** button. A new window with the entries for the partition is opened.
- Enter the necessary changes.
- Click the **Set** button to save the modifications.
- After closing the window, click the **Set** button in the main window to transfer the changes to the unit and to save them.

Type of recording:

Select the required recording type.

In the case of **Ring mode** the recording proceeds continuously. If the maximum hard drive space has been reached, the oldest recordings are automatically overwritten.

In the case of **Linear mode** the recording proceeds until the entire hard drive space is full. The recording is then stopped until old recordings have been deleted.

Number of alarm tracks:



Caution

Alarm tracks must be set up in the partition for alarm recording.

The unit uses a special recording mode during alarm recording for optimal usage of storage capacity: as soon as a time gap for alarm recording begins, a recording is continuously made on one segment, which is the size of a complete alarm sequence (pre- and post-alarm time).

This segment in the partition functions in a similar manner to a ring buffer and is overwritten until an alarm is actually triggered. Recording occurs on the segment only for the duration of the preset post-alarm time and a new segment subsequently used in the same manner.

Select the number of alarm tracks to be used in the partition. One alarm event can be recorded in each alarm track. Accordingly, the number of alarms entered can be recorded and archived. A partition can contain a maximum of 128 alarm recordings.

If the option **Ring mode** (see page 61) is set for a partition, the latest alarm recordings are always saved in the preset number. If the option **Linear mode** is selected, the recording is stopped as soon as the total number of alarm tracks has been recorded.

Alarm track size:

The size for an alarm track can be calculated according to various parameters. The calculated size applies to all alarm tracks for the partition.

- Click the **Calculate** button. A window will open.
- Select the appropriate setting for each parameter from the list boxes.

Click the **Set** button to accept the calculated value.

Format!

You can delete all recordings in the partition at any time.



Caution

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

- Click the **Format!** button to delete all recordings in the partition.

Delete all partitions

You can delete the partition at any time.



Caution

Deleting the partition leads to the entire hard drive being reorganized and the loss of all sequences stored on the drive. Consequently, you should check the recordings before deleting any partition and back up important sequences on the computer's hard drive.

- Click the **Delete all partitions** button. The line remains in the display containing the number **01**, the partition name is deleted and the size is indicated as **0**.
- Click the **Set** button to transfer the changes to the unit and to save them.

Recording profiles

You can define up to ten separate recording profiles. You then assign these to individual days or times of day in the recording scheduler (see page 63).



Note

You can modify the names of the recording profiles on the tabs in the **Recording scheduler** page (see page 63).

Recording profiles

Day Night Weekend

Camera	Standard profile	Encoder	Post-alarm profile
Camera 1	Low bandwidth (CIF)	Stream 1	Standard profile

Settings for selected camera(s)

Standard recording

Standard profile: Low bandwidth (CIF)

Encoder: Stream 1

Pre-alarm recording

Alarm track recording: 4 alarm track(s) with 102 MByte(s)

Pre-alarm time: 0 sec

Post-alarm recording

Post-alarm time: 0 sec

Post-alarm profile: Standard profile

Alarm input: 1 2 3 4

Motion alarm: 1

Video loss alarm: 1

Default

Copy settings

Set

- Click one of the tabs to edit the corresponding profile.
- In the list click the name of the camera input to edit the settings.
- Click the **Default** button to return all settings to their defaults, if appropriate.
- Click the **Copy settings** button if you want to copy the currently visible settings to another profile. A dialog will appear, and you can select the target profile for the copied settings.
- Click the **Set** button in each profile tab to save the settings in the device.

Standard profile:

You can select the encoder profile to use for continual recording (compare page .42).

 **Note**

The recording profile can deviate from the standard setting **Active profile** and is only used during an active recording.

Encoder:

You can select which data stream to record here.

Alarm track recording: **Note**

This parameter is only active, if the alarm tracks have been configured (see page 61).

- Click the checkbox to activate alarm track recording. The pre-alarm time gap will be displayed automatically.

Post-alarm time:

You can select the post-alarm time gap from the list box.

Post-alarm profile:

You can select the encoder profile to use for recording during the post-alarm time (compare page 42). The **Standard profile** option sets this to the same as the standard profile.

Alarm input/Motion alarm/Video loss alarm:

You can select the alarm sensor that is to trigger a recording.

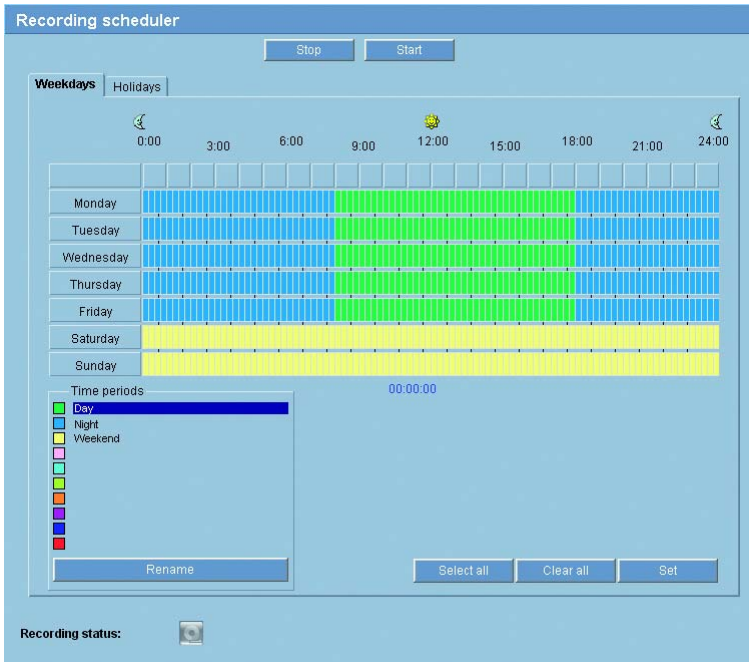
Note

The alarm sensor must be active to be able to trigger the recording.

The alarm inputs and video loss alarm are activated on the page **Alarm sources** (see page 69). The motion alarm is configured and activated on the page **VCA** (see page 73).

The numbering of the check boxes for the alarm inputs corresponds to the labeling of the alarm inputs on the VIP X1.

Recording scheduler



In the recording scheduler you can assign weekdays and times to the recording profiles you have created during which images from the camera should be recorded in the event of an alarm.

You can assign as many time periods (in 15-minute intervals) for any day of the week to a profile. When you move the mouse cursor over the table, the time is displayed.

In addition to weekdays, you can also define holidays which differ from the regular scheduling for the week. This allows you to apply the settings for Sundays to other dates that fall on varying weekdays.

- Click the profile in the **Time periods** field that you want to assign intervals to.
- Click a field in the table, and holding the left mouse button down drag the cursor across all of the fields to be assigned to the selected profile.
- Use the right mouse button to deselect any of the intervals.
- Click the **Select all** button to select all of the intervals to be assigned to the selected profile.

- Click the **Clear all** button to deselect all of the intervals.
- When you are finished, click the **Set** button to save the settings in the device.

Holidays

You can define holidays, which will override the settings for the normal weekly schedule. This allows you to apply the settings for Sundays to other dates that fall on varying weekdays.

- Click the **Holidays** tab. Any days, which have already been defined, will be shown in the table.
- Click the **Add** button. This will open a new window.
- Select the desired date from the calendar. By dragging the mouse you can select a range of dates. These are handled as a single entry in the table.
- Click **OK** to accept the selection. The window will close.
- Assign the defined holidays to the recording profile as described above.

Delete holidays

You can delete user-defined holidays at any time.

- Click the **Delete** button. This will open a new window.
- Click the date to be deleted.
- Click **OK**. The selection is removed from the table and the window closed.
- Repeat for any other dates to be deleted.

Time periods

You can change the names of the recording profiles.

- Select a profile by clicking and then click **Rename**.
- Enter the desired name and click **Rename** again.

Activate recording

After configuration, you must activate the recording scheduler and start the recording.

After starting, the pages **Recording profiles** and **Recording scheduler** are deactivated, and the configuration cannot be modified.

You can terminate recording at any time and modify settings.

- Click the **Start** button to activate the recording scheduler.
- Click the **Stop** button to deactivate the recording scheduler. Recordings that are currently running will be interrupted and the configuration can be modified.

Recording status:

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

Alarm sources

Alarm sources		
Alarm input 1:	<input type="button" value="Off"/> <input type="button" value="Active high"/>	Name: <input type="text" value="Input 1"/>
Alarm input 2:	<input type="button" value="Off"/> <input type="button" value="Active high"/>	Name: <input type="text" value="Input 2"/>
Alarm input 3:	<input type="button" value="Off"/> <input type="button" value="Active high"/>	Name: <input type="text" value="Input 3"/>
Alarm input 4:	<input type="button" value="Off"/> <input type="button" value="Active high"/>	Name: <input type="text" value="Input 4"/>
Video loss alarm:	<input type="checkbox"/> 1	<input type="button" value="Set"/>

You can configure the possible alarm triggers for the VIP X1 (for example, the alarm inputs).

Alarm input 1: to Alarm input 4:

Select the option **On** to activate the alarm by the corresponding external alarm sensor. Otherwise, select **Off**.

Select **Active high** if the alarm is to be triggered by closing the contact.

Select **Active low** if the alarm is to be triggered by opening the contact.

Name:

You can enter a name for each alarm input, which is then displayed below the icon for the alarm input on the **LIVEPAGE** if configured correctly (see **Livepage configuration**, page 94).

Video loss alarm:

Activate the checkbox if you want an interruption of the video signal to also trigger an alarm.

Alarm connections

Alarm connections

Connect on alarm:	<input type="text" value="Off"/>
Number of destination IP address:	<input type="text" value="1"/>
Destination IP address:	<input type="text" value="0.0.0.0"/>
Destination password:	<input type="text"/>
Remote port:	<input type="text" value="80"/>
SSL encryption:	<input type="text" value="Off"/>
Auto-connect:	<input type="text" value="Off"/>
Audio:	<input type="text" value="Off"/>

You can select how the VIP X1 responds to an alarm. In the event of an alarm, the unit can automatically connect to a pre-defined IP address. You can enter up to 10 IP addresses to which the VIP X1 will connect in sequence in the event of an alarm, until a connection is made.

Connect on alarm:

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

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

Note

Stream 2 is always transmitted for alarm connections. Bear this fact in mind when assigning the profile (see page 42).

Number of destination IP address:

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

Destination IP address:

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

Destination password:

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

You can save up to ten target IP-addresses on this page. This means that also only ten passwords for connections can be defined here. If more than ten connections are necessary, for example when connections are initiated by a controlling system, such as VIDOS or Bosch Video Management System, you can define a general password. The VIP X1 can make connections with this general password to all devices protected by that same password. In such cases, proceed as follows:

- Select **10** in the **Number of destination IP address** list box.
- Enter **0.0.0.0** in the **Destination IP address** field.
- Enter the password in the **Destination password** field.
- Set the **user** password of all the devices to be connected to this password.

Note

Setting target 10 to the destination IP address 0.0.0.0 will override its function as the tenth address to try for auto-connect by the VIP X1 on alarm. Instead the parameter is used only to store the general password.

Remote port:

Choose the browser-port, depending on the network configuration. Port 443 for HTTPS connections is only available if the **On** option in **SSL encryption** is active.

SSL encryption:

SSL encryption can be used to protect data, such as the password, used for connection establishment. If you activate the **On** option, only encrypted ports are available for the **Remote port** parameter.

Note

SSL encryption must be activated and configured on both sides of a connection. The appropriate certificates must also have been uploaded to the VIP X1 (see page 99).

You can configure and activate encryption for media data (video, audio, meta-data) on the **Encryption** page (see page 91).

Auto-connect:

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

**Note**

Stream 2 is always transmitted for automatic connections. Bear this fact in mind when assigning the profile (see page 42).

Audio: (audio version only)

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

VCA

VCA

Video 1

Analysis:

Analysis type: Alarm state: Off

Motion detector

Sensitivity:

Min. object size:

Global change %:

Tamper detection

Sensitivity:

Trigger delay (Sec):

Scene too bright Scene too noisy

Scene too dark Reference check

The VIP X1 contains an integrated video content analysis (VCA), which can detect and analyze changes in the signal on the basis of image processing. Such changes can be due to movements in the camera's field of view.

- Enter the desired settings.
- If necessary, click the **Default** button to return all settings to their default values.

Analysis:

Select the option **On** to activate the video content analysis.

As soon as the video content analysis is activated, metadata are created. Depending on the **Analysis type** selected and the relevant configuration, additional information overlays the video image in the preview window next to the parameter settings. If you have selected **MOTION+** analysis, for example, the sensor fields in which movement is registered are marked by rectangles.

 **Note**

On the **Livepage configuration** page, you can enable additional information overlays for the live video image too (see page 96).

Analysis type:

Select the required analysis algorithm. By default, only **MOTION+** is available – this offers a motion detector and essential recognition of tampering. The current alarm status is displayed for information purposes.

 **Note**

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

Motion detector (MOTION+ only)

For the detector to function, the following conditions must be met:

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

**Caution**

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

For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Sensitivity: (MOTION+ only)

The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject.

The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

Min. object size: (MOTION+ only)

You can specify the number of sensor fields that a moving object must cover to generate an alarm. This setting prevents objects that are too small from triggering an alarm.

A minimum value of **4** is recommended. This value corresponds to four sensor fields.

Global change %: (MOTION+ only)

You can define the percentage of sensor fields that must register a change simultaneously before generating an alarm. This setting is independent of the sensor fields selected under **Select area**.

This option allows you to detect, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mounting bracket, for instance.

Selecting the area (MOTION+ only)

The areas of the image to be monitored by the motion detector can be selected. The video image is subdivided into 858 square sensor fields. You can activate or deactivate each of these fields individually. If you wish to exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, etc.), the relevant fields can be deactivated.

- Click **Select area** to configure the sensor fields. A new window will open.
- If necessary, click **Clear all** first to clear the current selection (fields marked red).
- Left-click the fields to be activated. Activated fields are marked red.
- If necessary, click **Select all** to select the entire video frame for monitoring.
- Right-click any fields you wish to deactivate.
- Click **OK** to save the configuration.
- Click the close button (**X**) in the window title bar to close the window without saving the changes.

Tamper detection

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

Note

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

Sensitivity:

Note

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

The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject.

The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected.

Trigger delay (sec):

You can set delayed alarm triggering. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This allows you to avoid false alarms triggered by short-term changes, for example cleaning activities in the direct field of vision of the camera.

Scene too bright

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

Scene too dark

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

Scene too noisy

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

Reference check

You can save a reference image that is continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This allows you to detect tampering that would otherwise not be detected, for example if the camera is turned.

- Click **Reference** to save the currently visible video image as a reference.
- Click **Select area** and select the areas in the reference image that are to be monitored.
- Check the box **Reference check** to activate on-going matching. The stored reference image is displayed in black and white below the current video image, and the selected areas are marked in red.

Selecting the area

You can select the image areas in the reference image that are to be monitored. The video image is subdivided into 858 square fields. You can activate or deactivate each of these fields individually.

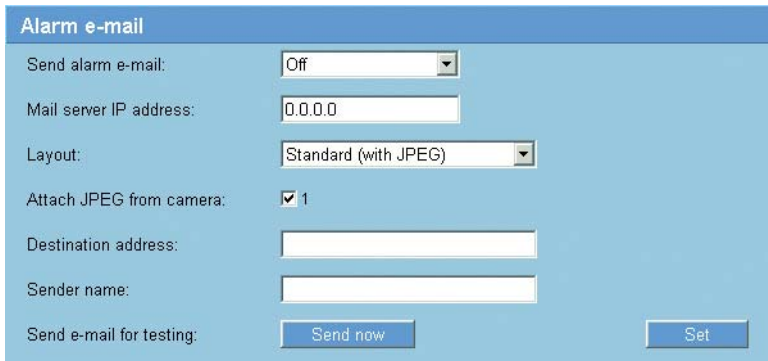


Note

Select only those areas for reference monitoring in which no movement takes place and that are always evenly lit, as false alarms could otherwise be triggered.

- Click **Select area** to configure the sensor fields. A new window will open.
- If necessary, click **Clear all** first to clear the current selection (fields marked red).
- Left-click the fields to be activated. Activated fields are marked red.
- If necessary, click **Select all** to select the entire video frame for monitoring.
- Right-click any fields you wish to deactivate.
- Click **OK** to save the configuration.
- Click the close button (**X**) in the window title bar to close the window without saving the changes.

Alarm e-mail



The screenshot shows a web-based configuration interface for "Alarm e-mail". It features a blue header with the title "Alarm e-mail". Below the header, there are several configuration fields: "Send alarm e-mail:" with a dropdown menu set to "Off"; "Mail server IP address:" with a text input field containing "0.0.0.0"; "Layout:" with a dropdown menu set to "Standard (with JPEG)"; "Attach JPEG from camera:" with a checked checkbox and the number "1"; "Destination address:" with an empty text input field; "Sender name:" with an empty text input field; and "Send e-mail for testing:" with a "Send now" button. A "Set" button is located at the bottom right of the form.

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

Layout:

You can select the data format of the alarm message.

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

**Caution**

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

Attach JPEG from camera:

Click the checkbox to enable the attachment of JPEG images of the camera.

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.

Send e-mail for testing:

Test the e-mail function by clicking the **Send now** button. An alarm e-mail is immediately created and sent.

Relay

Idle state:	Open
Operating mode:	Bistable
Relay follows:	Off
Relay name:	Relay 1
Trigger relay:	Relay 1 Set

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 the output. It is possible, for example, to turn on a floodlight by triggering a motion alarm and then turning the light off again when the alarm has stopped.

Idle state:

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

Operating mode:

Select an operating mode for the relay.

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

Relay follows:

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

■ Off

Relay is not triggered by events

■ Connection

Trigger whenever a connection is made

■ Video alarm 1

Trigger by interrupting the video signal

■ Motion alarm 1

Trigger by means of motion alarm as configured on the page **VCA** (see page 73)

■ Local input 1

Trigger by external alarm input 1

■ Remote input 1

Trigger by remote station's switching contact (only if a connection exists)

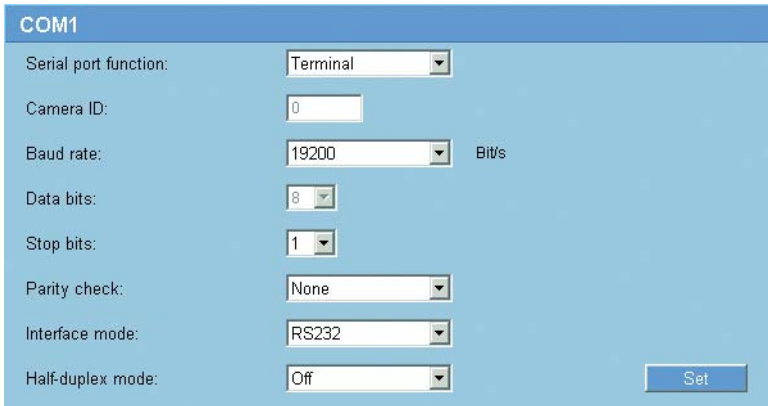
Relay name:

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

Trigger relay:

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

COM1



The screenshot shows a configuration window titled "COM1" with a light blue background. It contains several settings, each with a label and a dropdown menu or text input field:

- Serial port function: Terminal
- Camera ID: 0
- Baud rate: 19200 Bits
- Data bits: 8
- Stop bits: 1
- Parity check: None
- Interface mode: RS232
- Half-duplex mode: Off

A "Set" button is located at the bottom right of the configuration area.

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

Note

If the VIP X1 is working in multicast mode (see page 89), the first remote location to establish a video connection to the unit is also assigned the transparent data connection. However after about 15 seconds of inactivity the data connection is automatically terminated and another remote location can exchange transparent data with the unit.

Serial port function:

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

Note

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

Camera ID:

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

Baud rate:

Select the value for the transmission rate in bit/s.

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.

Half-duplex mode:

Choose the setting appropriate for your application.

Network

Network

Ethernet

IP address: [Reboot after 'Set' necessary!](#)

Subnet mask: [Reboot after 'Set' necessary!](#)

Gateway address: [Reboot after 'Set' necessary!](#)

Video transmission:

HTTP browser port:

HTTPS browser port:

RCP+ port 1756: [Reboot after 'Set' necessary!](#)

Telnet support: [Reboot after 'Set' necessary!](#)

Ethernet link type:

[Details <<](#)

SNMP

1. SNMP host address:

2. SNMP host address:

SNMP traps:

802.1x

Authentication:

Identity:

Password:

DHCP

Automatic IP assignment: [Reboot after 'Set' necessary!](#)

The settings in this screen are used to integrate the VIP X1 into an existing network.



Caution

Some changes, for example to the IP address, subnet mask or gateway address are transferred to the unit by clicking **Set**. However, they only take effect after the unit is restarted!

Note the indicator **Reboot after 'Set' necessary!**

- Click **Set** after entering a new IP address.
- To restart the unit, enter the old IP address followed by `/reset` (for example `192.168.0.30/reset`) in the address bar of your Web browser. The VIP X1 restarts, after which it can only be accessed at the new IP address.

IP address:

Enter the desired IP address for the VIP X1 in this field. The IP address must be valid for the network.

Subnet mask:

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

Gateway address:

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

Video transmission:

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



Caution

Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections.



Note

The MTU value in UDP mode is 1514 bytes.

HTTP browser port:

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

HTTPS browser port:

To limit browser access to encrypted connections, choose an HTTPS port from the list. The standard HTTPS port is 443. By activating the **Off** option, you can deactivate HTTPS ports and limit connections to unencrypted ports.

The VIP X1 uses the TLS 1.0 encryption protocol. Ensure that the browser has been configured to support this protocol. Also ensure that Java application support is activated (in the Java Plug-in Control Panel of the Windows Control Panel).

Note

If you want to limit connections to SSL encryption, you must set the **Off** option in the **HTTP browser port**, the **RCP+ port 1756**, and **Telnet support**. This deactivates all unencrypted connections allowing connections on the HTTPS port only.

You can configure and activate encryption for media data (video, audio, meta-data) on the **Encryption** page (see page 91).

RCP+ port 1756:

You can activate the unencrypted RCP+ port 1756 for exchanging connection data. If you want to allow only encrypted connections, you must set the **Off** option to deactivate the port.

Telnet support:

If you want to allow only encrypted connections, you must set the **Off** option to deactivate Telnet support, making Telnet connections impossible.

Ethernet link type:

Choose the setting appropriate for your application.

1. SNMP host address: / 2. SNMP host address:

The VIP X1 supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. It supports SNMP MIB II in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target devices here.

SNMP traps:

You can choose, which traps are sent.

- Click **Select**. A dialog box appears.
- Click the check boxes of the appropriate traps.
- Click **OK** to close the window and send all of the checked traps.

Authentication:

If a RADIUS server controls access rights in the network, you must activate authentication here. Otherwise there will be no communication with the device. The respective data must also be stored in the RADIUS server.

For configuration you must connect the VIP X1 directly to a computer using a crossed network cable since communication via the network is only possible when the parameters **Identity** and **Password** have been set and authentication was successful.

Identity:

Enter the user name that the RADIUS server uses for identification of the VIP X1.

Password:

Enter the password that is stored in the RADIUS server.

Automatic IP assignment:

If the network has a DHCP server for dynamic IP allocation, you can activate the acceptance of the automatically assigned IP address here. In this case, the IP entered above on this page will be overwritten the next time the unit boots (restart).

**Caution**

The DHCP server must support the allocation of static IP addresses based on MAC addresses and must be configured accordingly, so that the unit receives the same IP address after each restart. If not, the unit may no longer be accessible via its IP address, or controlling systems, such as VIDOS or Bosch Video Management System lose the allocations.

Multicasting

Multicasting

Multicast address video 1: Port: Streaming

Stream 1 / Stream 2

Multicast packet TTL:

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

Note

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

A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network.

The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255.

The multicast address can be the same for multiple streams. However it will be necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and multicast address.

Multicast address video 1:

Enter a valid multicast address for each stream to be operated in multicast mode (duplication of the data streams in the network).

With the setting **0.0.0.0** the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in the unit). The VIP X1 supports multi-unicast connections for up to five simultaneously connected receivers.

 **Note**

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

Port:

Assign a different port to each data stream if there are simultaneous data streams at the same multicast address.

Enter the port address of the required stream here.

Streaming

Click the checkbox to activate multicast streaming mode for the relevant stream. An enabled stream is indicated by a check mark.

Multicast packet TTL:

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

Encryption

Encryption

Encryption: Off Keys <<

Automatic key interchange:

Encryption:

Data channel	Encryption keys
Video 1 Stream 1	00000000000000000000000000000000
Video 1 Stream 2	00000000000000000000000000000000
Video 1 metadata	00000000000000000000000000000000
Video 1 recording	00000000000000000000000000000000
Video 1 recording metadata	00000000000000000000000000000000
Audio 1	00000000000000000000000000000000
Audio 3 recording	00000000000000000000000000000000
Audio 2	00000000000000000000000000000000

Decryption:

Data channel	Decryption keys
Audio decoder 1	00000000000000000000000000000000

Edit
Generate keys
Clear keys

Set

Encryption:

You can activate the encryption of media data (video, audio, meta data) here. Activation here also causes the exchange of connection data (RCP+) to be encrypted.



Caution

If you want to have encrypted data channels, you should only allow secured Web browser connections via SSL. To do this, you must deactivate all open ports and protocols (see page 87). Connections then are possible via an HTTPS port only.

You can select data channels individually for encryption. As soon as a key has been generated, only encrypted data is transmitted in the respective channel. If you delete the key, unencrypted data is transmitted in the respective channel.



Note

Encrypting video data requires a lot of computing power.

- Select **On** in the **Encryption:** list box to activate encryption. Activation generates keys for all channels.
- Click the **Keys >>** button to display a list of data channels and associated keys.
- Click an entry to select it.
- Hold the [Ctrl] key down to mark multiple entries.
- Click the **Clear keys** button to delete the keys for the marked channel. The data in this channel is no longer encrypted.
- Click the **Generate keys** button to generate a new key for a marked channel.
- Click the **Edit** button to enter a key for a marked entry manually.

Automatic key exchange:

You can activate an automatic key exchange between two devices (or a device and a software decoder) across an encrypted connection. If the checkbox is marked keys are exchanged automatically.

Version information

Version information	
Hardware version:	F0000143
Firmware version:	17000250
Device type:	VIP X1
Audio option:	Yes
Storage medium attached:	Yes
MAC address:	00-07-5F-70-12-A3
Major version number:	2.50
Build number:	17

The details in this window are for information only and cannot be changed. Keep a record of these numbers in case technical assistance is required.



Note

You can use the mouse to mark and copy the firmware and hardware version numbers, for example to send them via e-mail.

Livepage configuration

Livepage configuration

URL for logo:	<input type="text" value="Default"/>	<input type="button" value="Browse"/>	
URL for device logo:	<input type="text" value="Default"/>	<input type="button" value="Browse"/>	
Transmit audio:	<input type="checkbox"/>		
Show alarm inputs:	<input checked="" type="checkbox"/>		
Show relay output:	<input checked="" type="checkbox"/>		
Show VCA metadata:	<input type="checkbox"/>		
Show VCA trajectories:	<input type="checkbox"/>		
Show event log:	<input checked="" type="checkbox"/>		
Show system log:	<input checked="" type="checkbox"/>		
Save event log:	<input checked="" type="checkbox"/>		
Save system log:	<input checked="" type="checkbox"/>		
File for event log:	<input type="text" value="C:\Event.bt"/>	<input type="button" value="Browse"/>	
File for system log:	<input type="text" value="C:\General.bt"/>	<input type="button" value="Browse"/>	
Path for JPEG and MPEG files:	<input type="text" value="C:\"/>	<input type="button" value="Browse"/>	<input type="button" value="Set"/>

In this window you can customize the appearance of the **LIVEPAGE** to suit your requirements. You can opt to have selected information and controls displayed in addition to the video image.

If necessary, you can also replace the manufacturer's logo (upper left) and the product name (upper right) in the upper window area (banner) by individual graphics.

Note

You can use either GIF or JPEG images. The file paths must correspond to the access mode (for example `C:\Images\Logo.gif` for access to local files, or `http://www.mycompany.com/images/logo.gif` for access via the Internet/Intranet).

For access via the Internet/Intranet, ensure that a connection is always available to display the image. The image file is not stored in the VIP X1.

- Check the box for the items that are to be displayed on the **LIVEPAGE**. The selected items are indicated by a check mark.

- Go to the **LIVEPAGE** to check whether and how the required items are displayed.

URL for logo:

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

If necessary, click **Browse** to search for an appropriate graphic in the local network.

URL for device logo:

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

- If necessary, click **Browse** to search for an appropriate graphic in the local network.

Note

If you want to use the original graphics again, simply delete the entries in the fields **URL for logo** and **URL for device logo**.

Transmit audio: (audio version only)

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

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 output:

The relay output is shown next to the video image as an icon, along with its assigned name. If the relay is switched, the icon changes color.

Show VCA metadata:

Additional information from the video content analysis VCA are displayed in the live video image, if the analysis is activated (see page 73). If you have selected **MOTION+** analysis, for example, the sensor fields in which movement is registered are marked by rectangles.

Show VCA trajectories: (IVMD 2.0 only)

The trajectories (motion lines of objects) generated by the video content analysis with IVMD 2.0 algorithm are displayed in the live video image, if this analysis type is activated (see page 73).

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 the establishment and termination of connections, etc.

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.

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 event log:

Enter the path to save the event log here.

- If necessary, click **Browse** to find a suitable folder.

File for system log:

Enter the path to save the system log here.

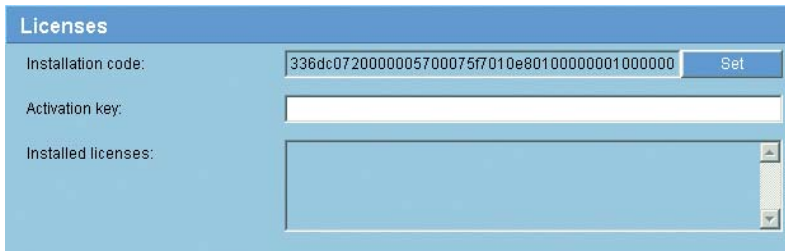
- If necessary, click **Browse** to find a suitable folder.

Path for JPEG and MPEG files:

Enter the path for the storage location of individual images and video sequences that you can save from the **LIVEPAGE**.

- If necessary, click **Browse** to find a suitable folder.

Licenses



The screenshot shows a web interface for license management. It features a blue header with the word "Licenses". Below this, there are three main sections: "Installation code:" with a text box containing a long alphanumeric string and a "Set" button; "Activation key:" with an empty text box; and "Installed licenses:" with an empty list area and a scrollbar on the right.

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

Note

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

Maintenance

Maintenance			
Firmware upload:	<input type="text"/>	<input type="button" value="Durchsuchen..."/>	<input type="button" value="Upload"/>
Upload progress:	<input type="text" value="0%"/>		
Configuration download:			<input type="button" value="Download"/>
Configuration upload:	<input type="text"/>	<input type="button" value="Durchsuchen..."/>	<input type="button" value="Upload"/>
SSL certificate upload:	<input type="text"/>	<input type="button" value="Durchsuchen..."/>	<input type="button" value="Upload"/>

Firmware upload:

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

In this way, a VIP X1 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 on our Internet site.



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 faulty programming of the flash-EPROM. This in turn can result in the unit no longer being addressable, in which case it will have to be replaced.

- First store the firmware file on your hard drive.
- Enter the full path of the firmware file in the field or click **Browse...** button to locate and select the file.
- 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 by the message **going to reset Reconnecting in ... seconds**. The unit restarts automatically once the upload has successfully completed.

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

- In the address bar of your browser, enter `/main.htm` after the IP address of the VIP X1 (for example `192.168.0.30/main.htm`).
- Repeat the upload.

Configuration download:

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

- Click the **Download** button. The computer displays a dialog box.
- Follow the on-screen instructions to save the current settings.

Configuration upload:

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

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

SSL certificate upload:

In order to work with an SSL connection, both sides of the connection must possess the appropriate certificates. You can upload a certificate consisting of one or more files to the VIP X1 here.

Files must be uploaded one at a time.

- Enter the complete path name of the file you wish to upload, or click **Browse...** to locate the file.
- Click **Upload** to start the file transfer.

- After successful upload of all files you must reboot the device. Enter the IP address of the VIP X1 followed by `/reset` (for example `192.168.0.30/reset`) in the address bar of your Web browser.

The new SSL certificate is valid.

Function test

The VIP X1 offers a variety of configuration options. You should therefore check that it is functioning correctly after installation and configuration.

The function test is the only way to ensure that the VIP X1 operates as expected in the event of an alarm.

Your check should include the following functions:

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

6

Operation

Operation with Microsoft Internet Explorer

A computer with Microsoft Internet Explorer (version 6.0 or higher) can receive live images from the VIP X1, control cameras or other peripherals and replay stored video sequences.

 **Note**

Make sure the graphics card is set to 16- or 32-bit color depth and that Sun JVM is installed and activated on your PC. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11). You can find notes on using Internet Explorer in the online help in Internet Explorer.

System requirements

- Computer with Windows 2000/XP operating system, access to a network and Microsoft Internet Explorer (version 6.0 or higher)
- Monitor resolution 1024 × 768 pixels, 16- or 32-bit color depth
- For playing back recordings: connection to iSCSI server

 **Note**

Take also note of the information in the **System Requirements** document on the product CD supplied.

Installing MPEG ActiveX

 **Note**

Suitable MPEG ActiveX software must be installed on the computer to allow the live video images to be played back. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11).

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

Establishing the connection

The VIP X1 must be assigned a valid IP address to operate on your network.

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

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



The LIVEPAGE

Once the connection is established, the Web browser displays the **LIVEPAGE**. It shows the live video image on the right of the browser window. Depending on the configuration, various text overlays may be visible on the live video image (see **Display stamping**, page 37).

Other information may be shown next to the live video image on the **LIVEPAGE**. What is shown will depend on the settings you have made on the **Livepage configuration** screen (see page 94).

Maximum number of connections

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

Protected VIP X1

If the VIP X1 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.

Note

The VIP X1 offers the option to limit the extent of access using various authorization levels (see page 32).

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

Image selection

You can view the image from the camera in different displays.

- Click one of the tabs **MPEG-4 Stream 1**, **MPEG-4 Stream 2** or **M-JPEG** below the video image to toggle between the different displays of the camera image.

Camera control

Control options for peripherals (for example a pan/tilt head or a dome camera) depend on the type of unit installed and on the configuration of the VIP X1.

If a controllable unit is configured and connected to the VIP X1, the controls for the unit are displayed next to the video image.



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

Digital I/O



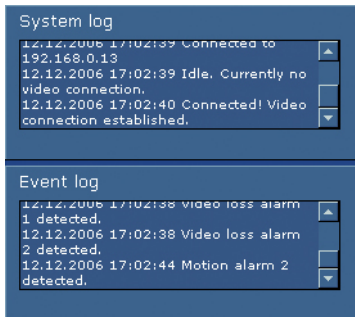
The alarm icons **Input 1 ... Input 4** are for information purposes and indicate the status of an alarm input: When an alarm is triggered the respective icon lights up in green. The unit's configuration determines whether the alarm is displayed, as well as additional details (see **Livepage configuration**, page 94).

Trigger relay

You can switch a connected unit by means of the relay in the VIP X1 (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 VIP X1 and the connection. You can save these messages automatically in a file (see page 96).

Events such as the triggering or end of alarms are shown in the **Event log** field. You can save these messages automatically in a file (see page 96).

Audio function (audio version only)

Depending on the configuration, the VIP X1 can send and receive audio signals. All users who are connected by browsers receive the audio signals sent by the VIP X1.

Audio signals can only be sent to the VIP X1 by the user who connects to the unit first.

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

Note

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

Saving snapshots

You can save individual images from the video sequence currently shown on the **LIVEPAGE** in JPEG format on your computer's hard drive.

- Click the icon for saving single images. The image is saved at a resolution of 704 × 576 pixels (4CIF). The storage location depends on the configuration of the VIP X1 (see page 97).



Recording video sequences

You can save sections of the video sequence currently shown on the **LIVE-PAGE** on your computer's hard drive.

- Click the icon for recording video sequences to start recording. The storage location depends on the configuration of the VIP X1 (see page 97). The flashing red dot in the icon indicates that recording is in progress.



- Click the icon for recording video sequences again to stop recording.

Note

You can play back saved video sequences using the Player from Bosch Security Systems which can be installed from the product CD supplied (see page 115).

Image resolution

Sequences are saved at the resolution that has been preset in the configuration for the encoder (see page 44).

Running recording program

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



The icon lights up green and displays a moving graphic to indicate a running recording. If no recording is taking place, a gray icon is displayed.

The RECORDINGS page

You can access the **RECORDINGS** page for playing back recorded video sequences from the **LIVEPAGE** as well as from the **SETTINGS** menu.

The **RECORDINGS** link is only visible if a storage medium has been selected (see page 50).

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

The screenshot displays the Bosch VIP X1 RECORDINGS page. The top navigation bar includes 'BOSCH', 'LIVEPAGE | RECORDINGS | SETTINGS', and 'VIP X1'. The main content area is divided into several sections:

- Partition:** Partition 1
- Table:** A table listing recorded tracks with columns for Track, Start time, Stop time, Duration, Alarm, and Type.

Track	Start time	Stop time	Duration	Alarm	Type
0	26.11.2006 07:16:08	26.11.2006 07:21:23	00:05:15		Time
1	29.11.2006 23:50:38	30.11.2006 00:37:19	00:46:40		Time
2	13.12.2006 00:27:20	13.12.2006 00:50:44	00:13:14		Time
3	13.12.2006 18:28:43	13.12.2006 18:50:20	00:21:37		Time
- Screenshots:** A section for displaying screenshots, currently empty.
- Video Playback:** A large window showing a live video feed of an indoor arena. Below the video is a timeline with markers at 16:25:00, 16:30:00, 16:35:00, 16:40:00, and 16:45:00. The current playback position is 13.12.2006 16:33:55. Playback controls include play/pause, stop, previous, next, and full screen buttons. A progress bar shows 100% completion.
- Help on this page?** A link for user assistance.

At the bottom of the window, a status bar shows 'Connected: Video connection successfully established.' and 'Internet' connectivity.

Selecting recordings

All sequences that are saved in the partition are displayed in the list. A running number (track) is assigned to each sequence. Start time and stop time, recording duration, number of alarms, and recording type are displayed.

- Click a list entry. The playback for the selected sequence starts immediately in the video window.

Controlling a playback



You will see a time bar below the video image for quick orientation. If a particular sequence has been selected for playback by means of click, the selected sequence appears in the list in blue with a green border. The associated time interval is displayed in the bar in gray. A green arrow above the bar indicates the position of the image currently being played back within the sequence.

The time bar offers various options for navigation in and between sequences.

- You can change the time interval displayed by moving the gray area to the left or right while holding down the mouse button.
- You can change the time interval displayed by clicking the zoom keys (magnifying glass icons). The display can span a range from two months to a few seconds.
- You can select a different sequence for playback by clicking on the corresponding gray marking.

- If required, drag the green arrow to the point in time at which the playback should begin. Alternatively you can double-click directly in the gray time interval or in the timescale to jump to the position selected in this manner. The date and time display below the bar provides orientation to the second.

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



Start playback
or pause



Jump to the start of active video sequence or
to the previous sequence in the list



Jump to the end of active video sequence or
to the next sequence in the list

You can use the slide control to control playback speed and fast forward/rewind: positioning in the middle indicates playback at recording speed, left indicates rewind, and right fast forward. The fast forward or rewind speed changes, depending on how far you move the slide control toward the runner icons.



You can continuously select playback speed by means of the speed regulator:



Red bars within the gray sequence fields indicate the points in time where alarms were triggered. Drag the green arrow to navigate to these points quickly.

In addition, you can set markers in the sequences, so-called bookmarks, and jump directly to these. These bookmarks are indicated as small yellow arrows above the time interval. Use the bookmarks as follows:



Jump to the previous bookmark



Set bookmark



Jump to the following bookmark

– Right-click a bookmark to delete it.



Note

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

Backup

You can back up the video sequences or single images stored on the hard drive of the VIP X1 to the computer's hard drive.

First select the required sequence as described in the previous section. The following buttons are available for the backup:



Back up a sequence to the computer's hard drive



Back up a single image to the computer's hard drive

- Start playback of the sequence that you want to save either completely or partially on the computer's hard drive.
- Click the icon for the sequence backup. The backup starts immediately – this process is displayed by a flashing red dot in the icon.
- Click the sequence backup icon again to end the backup.

This procedure can be repeated many times within the sequence to back up multiple extracts from a longer sequence.

- Click the button for backing up a single image to back up only snapshots from the running sequence to your computer's hard drive.

The single images are immediately displayed in the **Screenshots** area after clicking.

The storage location for the sequences and single images can be specified in the configuration of the VIP X1 (see page 97).

Installing Player

You can play back saved video sequences using the Player from Bosch Security Systems which can be found on the product CD supplied (see **Components supplied**, page 11).



Note

Suitable MPEG ActiveX software must be installed on the computer in order to play back saved video sequences using the Player.

- Insert the CD in the CD-ROM drive of the computer. If the CD does not start automatically, open the CD in Windows Explorer and double click the **index.html** file to start the menu.
- Select a language from the list box at the top and click **Tools** in the menu.
- Click **Archive Player**; the installation starts. Follow the instructions in the installation program. The Player is installed together with the Archive Player.
- After a successful installation, two new icons for the Player and the Archive Player appear on the desktop.
- Double click the **Player** icon to start the Player.

Replaying USB hard drive recordings on PC

If you store recordings on an external USB hard drive (see pages 23 and 50), you can connect this drive to a PC and view the recordings there.

System requirements

- Computer with Windows 2000/XP operating system and Microsoft Internet Explorer (version 6.0 or higher)
- Available USB 2.0 port
- Monitor resolution 1024 × 768 pixels

Note

Make sure the graphics card is set to 16- or 32-bit color depth and that Sun JVM is installed and activated on your PC. If necessary, you can install the required software and controls from the product CD supplied (see **Components supplied**, page 11). You can find notes on using Internet Explorer in the online help in Internet Explorer.

Installing MPEG ActiveX

Note

Suitable MPEG ActiveX software must be installed on the computer to allow the video images to be played back. If necessary, you can install the required software and controls from the product CD supplied (see page 103).

Playback

- End all running recording programs on the VIP X1.
- Detach the USB drive from the VIP X1.
- Connect the drive to a free USB port in the computer using a USB cable.
- Open the directory for the drive using Explorer and double-click on the **video-jet.exe** file.

The software of a virtual video server is started, and you can access the playback page on this unit by entering the IP address of your own computer in Internet Explorer (for example 192.168.0.1).

- Start Internet Explorer.
- Enter the IP address of your computer as the URL. The Web browser opens the page for playing back recordings.

You can select recordings and control playback, in the same way as when accessing a normal VIP X1 (see page 111).

**Note**

You must restart the virtual video server software if you restart the computer or if you change the USB drive, by double-clicking on the **video-jet.exe** file again.

Hardware connections between video servers

You can easily connect a VIP X1 with connected camera as a sender, and a suitable MPEG-4 compatible hardware decoder (for example VIP XD) with a connected monitor as a receiver via an Ethernet network. In this way it is possible to cover long distances without the need for major installation or cabling work.

Installation

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

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

Note

Make sure that the units are configured for the network environment and that the correct IP address for the remote location to be contacted in the event of an alarm is set on the **Alarm connections** configuration page (see page 70).

Connecting

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

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

Note

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

Connect on alarm

With the appropriate configuration, a connection between a sender and a receiver is made automatically when an alarm is triggered (see page 70). After a short time the live video image from the sender appears on the connected monitor.

This option can also be used to connect a sender and a compatible receiver using a switch connected to the alarm input. You do not need a computer to make the connection in this case.

Connecting with a terminal program

Various requirements must be met in order to operate with a terminal program (see page 129).

- Start the terminal program and enter the command 1 in the main menu to switch to the **IP** menu.
- Enter the command 4 in the **IP** menu to change the remote IP address, then enter the IP address of the unit you wish to connect to.
- Return to the main menu by entering the command 0. Then enter the command 4 to switch to the **Rcp+** menu.
- In the **Rcp+** menu, enter the command 5 to activate the automatic connection.

Closing the connection with a terminal program

- Start the terminal program (see page 129) and enter the command 4 in the main menu to switch to the **Rcp+** menu.
- In the **Rcp+** menu, enter the command 5 to deactivate the automatic connection.

Operation with decoder software

The VIP X1 video server combines with VIDOS to provide a high-performance system solution.

VIDOS is a software package for operating, controlling and managing of CCTV installations (such as surveillance systems) at remote locations. It runs under Microsoft Windows operating systems. It is primarily designed for decoding video, audio and control data received from a remote sender.

Many options are provided for operation and configuration when using a VIP X1 with VIDOS. Please refer to the software documentation for more details.

Another software supporting the VIP X1 is Bosch Video Management System.

Bosch Video Management System is a unique enterprise IP video security solution that provides seamless management of digital video, audio and data across any IP network. It is designed to work with Bosch CCTV products as part of a total video security management system. Now you can integrate your existing components into one easy-to-manage system, or use Bosch's full-line capabilities and benefit from a complete security solution based on cutting-edge technology and years of experience.

The video server VIP X1 is also designed for use with DiBos 8 Video Recorders.

DiBos 8 can record up to 32 video and audio streams, and is available as software or as a hybrid DVR with additional analog camera and audio inputs. DiBos supports various functions of the video server VIP X1, such as controlling relays, remote control of peripheral devices and remote configuration. DiBos 8 can use alarm inputs to trigger actions and, when motion detection MOTION+ is active, can record the relevant cells, making intelligent motion detection possible.

7

Maintenance and upgrades

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.

- Open the DOS command prompt.
- 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 properly 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.

Unit reset

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



Caution

All configured settings will be discarded during a reset. If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see page 98).



Note

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 chapter "**Installation**" (see page 25).

- If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see page 98).

- Using a pointed object, press the Factory reset button located below the USB port until the LED flashes red (see page 17). All settings will revert to their defaults.
- Change the IP address of the VIP X1 if necessary.
- Configure the unit to meet your requirements.

Repairs



Caution

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

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

Transfer and disposal

The VIP X1 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

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.

The version numbers of the internal processors can be viewed on a special page. Make a note of this information before contacting Customer Service.

- In the address bar of your browser, enter `/version.htm` after the IP address of the unit (for example `192.168.0.30/version.htm`).
- Write down the information or print out the page.

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

General malfunctions

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

Malfunction	Possible causes	Solution
The unit does not report an alarm.	Alarm source is not selected.	Select possible alarm sources on the Alarm sources configuration page.
	No alarm response specified.	Specify the desired alarm response on the Alarm connections configuration page, change the IP address if necessary.
Control of cameras or other units is not possible.	The cable connection between the serial interface and the connected unit is not correct.	Check all cable connections and ensure all plugs are properly fitted.
	The interface parameters do not match those of the other unit connected.	Make sure that the settings of all units involved are compatible.
The unit is not operational after a firmware upload.	Power failure during programming by firmware file.	Have the unit checked by Customer Service and replace if necessary.
	Incorrect firmware file.	Enter the IP address of the unit followed by <code>/main.htm</code> in your Web browser and repeat the upload.

iSCSI connections malfunctions

Malfunction	Possible causes	Solution
No LUNs are displayed after connection to the iSCSI server.	Incorrect LUN mapping during iSCSI server configuration.	Check the iSCSI server configuration and reconnect.
„LUN FAIL“ is displayed below a node after connection to the iSCSI server.	The LUN map was not readable as it was assigned to the wrong network interface.	Check the iSCSI server configuration and reconnect.
LUN mapping is not possible.	Some iSCSI systems don't support initiator extensions.	Delete the initiator extension on the iSCSI settings configuration page.

LEDs

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

Operating status LED

Not lit:	VIP X1 is switched off.
Lit green:	VIP X1 is switched on.
Flashes green:	VIP X1 is being accessed.
Lit red (briefly):	Startup in progress.
Lit red (continuously):	Defect in VIP X1, firmware upload failed.

LED L

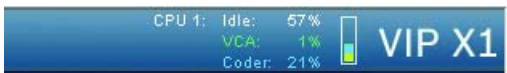
Lit green:	Connected to the network.
------------	---------------------------

LED T

Flashing orange:	Data transfer via the network.
------------------	--------------------------------

Processor load

When accessing the VIP X1 with a Web browser the indicator for the processor load is displayed in the upper left of the window next to the device name.



Move the mouse cursor over the icon to display numerical values for the processor. This information can help with problem solving or when fine tuning the device.

Serial interface

Options for using the serial interface include transferring transparent data, controlling connected units or operating the unit with a terminal program.

The serial interface supports the RS232, RS422 and RS485 transmission standards. The standard used depends on the current configuration (see page 83). Connection is via the terminal connector.

Terminal block

The terminal block has several contacts for:

- 4 alarm inputs
- 1 relay output
- Serial data transmission

Pin assignment

The pin assignment for the serial interface depends on the interface mode that is used (see page 84):

Contact	RS232 function	RS422/485 function
IN1	Alarm input 1	Alarm input 1
IN2	Alarm input 2	Alarm input 2
IN3	Alarm input 3	Alarm input 3
IN4	Alarm input 4	Alarm input 4
GND	GND (ground)	GND (ground)
GND	GND (ground)	GND (ground)
R (top)	Relay	Relay
R (bottom)	Relay	Relay
CTS	CTS (clear to send)	RxD- (receive data minus)
RTS	RTS (ready to send)	TxD- (transmit data minus)
RXD	RxD (receive data)	RxD+ (receive data plus)
TXD	TxD (transmit data)	TxD+ (transmit data plus)
+	12 V (power supply)	12 V (power supply)
-	GND (ground)	GND (ground)

To operate the alarm inputs, connect each alarm input to a ground contact (GND) via a trigger contact.

Communication with terminal program

Data terminal

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

You require a serial transmission cable with a 9-pin Sub-D connector to connect to the computer and open ends for connection to the terminal plug of the VIP X1 (pin assignment see page 127).

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

Note

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

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

Configuring the terminal

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

- 19,200 bit/s
- 8 data bits
- No parity check
- 1 stop bit
- No protocol

Command inputs

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

- If necessary, turn off the local echo so that entered values are not repeated on the display.
- Enter one command at a time.
- When you have entered a value, such as an IP address, check your input again before pressing the [ENTER] key to transfer the values to the VIP X1.

Assigning an IP Address

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

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

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

```

-----
|  VIP_X
-----
* 0' Exit menu IP      (* = reset after change necessary)
* 1' local IP         (**) 192.168.0.1
* 2' local subnet mask (**) 255.255.0.0
* 3' local gateway   (**) 0.0.0.0
* 4' remote IP       0.0.0.0
* 5' ntp server       0.0.0.0
* 6' ntp mode         1 (SNTP)
* 7' DHCP enabled    (**) NO
* 8' igmp version     (**) Auto
* 9' alarm IP ...
* a' discover ...
* b' iscsi ...
* c' http port        80
* d' https port       443
* e' ftp server IP    0.0.0.0
* f' syslog host IP   0.0.0.0
-----

```

Verbunden 00:00:26 Autom. Erkenn. Autom. Erkenn. RF GROSS NF Aufzeichnen Druckerecho

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

**Note**

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

Restart

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

Additional parameters

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

Glossary

Brief explanations of some of the terms and abbreviations used in this manual are given below.

10/100 Base-T	IEEE-802.3 specification for 10 or 100 MBit/s Ethernet
802.1x	The IEEE standard, 802.1x, provides a general method of access control and authorization for IEEE 802-based networks. An authenticator provides authentication by accessing an authentication server (see RADIUS server) to check connection requests, and grants or refuses access to the available services (LAN, VLAN, WLAN).
ARP	Address Resolution Protocol: a protocol for mapping MAC and IP addresses
Baud	Unit of measure for the speed of data transmission
Bit/s	Bits per second, the actual data rate
CIF	Common Intermediate Format, video format with 352 × 288/240 pixels
DHCP	Dynamic Host Configuration Protocol allows a network device to receive a dynamically allocated IP address and other network parameters from a server in a network.
DNS	Domain Name Service
FTP	File Transfer Protocol
Full duplex	Simultaneous data transmission in both directions (sending and receiving)
GoP	Group of Pictures
HTTP	Hypertext Transfer Protocol: protocol for transmission of data over a network
HTTPS	Hypertext Transfer Protocol. Secure provides secure transfer of data between web server and web browser.
ICMP	Internet Control Message Protocol
ID	Identification: a machine readable character string
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
Internet Protocol	The main protocol used on the Internet, normally in conjunction with the Transfer Control Protocol (TCP): TCP/IP
IP	See Internet Protocol
IP address	A 4-byte number uniquely defining each unit on the Internet. It is usually written in dotted decimal notation, for example "209.130.2.193"

iSCSI	Storage over IP process for storage networks; specifies how storage protocols are operated over IP.
ISDN	Integrated Services Digital Network
JPEG	An encoding process for still images (Joint Photographic Experts Group)
kBit/s	Kilobits per second, the actual data rate
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)
MAC	Media Access Control
MIB	Management Information Base; a collection of information for remote servicing using the SNMP protocol
MPEG-4	A further development of MPEG-2 designed for transmitting audiovisual data at very low transfer rates (for example over the Internet)
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 is a standard for synchronizing the system clocks in computers in packet switching networks. NTP uses the stateless protocol, UDP. NTP was designed to provide dependable time synchronization in networks with variable latency (ping times).
Parameters	Values used for configuration
QCIF	Quarter CIF, video format with 176 × 144/120 pixels
RADIUS server	Remote Authentication Dial-in User Service is a client-server protocol for authentication, authorization, and accounting of users in dial-in connections for computer networks. RADIUS is the de-facto standard for centralized authentication of dial-ins for modems, ISDN, VPN, wireless LAN (see 802.1x), and DSL.
RFC 868	A protocol for synchronizing computer clocks over the Internet
RS232/RS422/RS485	Standards for serial data transmission
RTP	Realtime Transport Protocol; a transmission protocol for real-time video and audio
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 is a simplified version of NTP (see NTP)
SSL	Secure Sockets Layer is an encryption protocol for data transmission in IP-based networks
Subnet mask	See Net mask
TCP	Transfer Control Protocol
Telnet	Login protocol with which users can access a remote computer (Host) on the Internet
TLS	Transport Layer Security versions 1.0 and 1.1 are standardized enhancement of the SSL 3.0 protocol (see SSL)
TTL	Time-To-Live; life cycle of a data packet in station transfers
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
WAN	See Wide area network
Wide area network	A long distance link used to extend or connect remotely located local area networks

Specifications

Device

Operating voltage	12 ... 24 V DC, power supply unit with various primary adapters included PoE: IEEE 802.11af, class 2
Power consumption	Approx. 6 VA
LAN interface	1 × Ethernet 10/100 Base-T, automatic adjustment, half/full duplex, RJ45
Data interfaces	1 × RS232/RS422/RS485, bidirectional, ST500 1 × USB 2.0
Alarm inputs	4 × push-in terminals (non-isolated closing contact), maximum trip resistance 10 Ohm
Relay output	1 × push-in terminal, 30 V _{p-p} , 2 A
Video input	1 × BNC jacks 0.7 ... 1.2 V _{p-p} , 75 Ohm, PAL/NTSC
Audio input (Line In)	1 × 3.5 mm stereo jack socket, 5.5 V _{p-p} max., impedance 9 kOhm typ.
Audio output (Line Out)	1 × 3.5 mm stereo jack socket, 3 V _{p-p} max., impedance 16 Ohm min.
Microphone input	1 × push-in terminal, 2.8 V _{p-p} max. at -20 dB, impedance 2 kOhm typ., supply 2.3 V typ.
Speaker output	1 × push-in terminal, 6 V _{p-p} max., 1 W rms, impedance 4 Ohm min.
Displays	3 × LED (operating voltage, network connection, data transfer) in rear panel
Operating conditions	Temperature: 0 ... +50°C (+32 ... +122°F) relative humidity: 20 ... 80%, non-precipitating
Regulatory approvals	CE: IEC 60950; UL 1950; AS/NZS 3548; EN 55103-1, -2; EN 55130-4; EN 55022; EN 55024; EN 61000-3-2; EN 61000-3-3; FCC 47 CFR Chapter 1 Part 15

Dimensions (w × h × l)	98 × 85 × 26 mm (3.86 × 3.35 × 1.02 in.) including feet and BNC connections	
Weight	Basic version:	approx. 170 g
	Audio version:	approx. 195 g

Protocols/standards

Video standards	PAL, NTSC
Video coding protocols	MPEG-4, JPEG
Video data rate	9,600 kBit/s ... 10 MBit/s
Image resolutions (PAL/NTSC)	704 × 576/480 pixels (4CIF/D1)
	704 × 288/240 pixels (2CIF)
	464 × 576/480 pixels (2/3 D1)
	352 × 576/480 pixels (1/2 D1)
	352 × 288/240 pixels (CIF)
	176 × 144/120 pixels (QCIF)
Total delay	120 ms (PAL/NTSC, MPEG-4, no network delay)
Image refresh rate	1 ... 50/60 fields/s variable (PAL/NTSC), Field/image-based encoding
Network protocols	RTP, Telnet, TCP, UDP, IP, HTTP, HTTPS, DHCP, IGMP V2, IGMP V3, ICMP, ARP, SNMP V2, 802.1x

Audio version only:

Audio coding protocol	G.711
Audio sampling rate	8 kHz
Audio data rate	80 kBit/s

9

Index

A

Activate recording 68
Activation key 97
Actuator 22
Alarm 37, 106
Alarm e-mail 79
Alarm input 22
Alarm message 38
Alarm sources 69
Alarm track recording 64
Audio connections 20
Audio settings 47
Audio source selection 47
Audio stream on alarm 72
Auto-connect 72
Automatic key exchange 92

B

Backup 114
Banner 94
Baud rate 84
Brightness 39
Browser window 105

C

Camera 83
Camera name 36
Camera selection 105
Cameras 20
Changes 31, 57

Changes in light level 74
Color depth 12, 27, 103, 116
COM1 83
Components supplied 11
Configuration 27, 99
Configuration download 99
Configuration mode 30
Connecting 27, 118
Connecting on alarm 70
Connections 29
Continual recording 64
Contrast 39
Control 83
Control functions 106
Controlling playback 111
Conventions 7
Creating a partition 56

D

Danger 9
Data bits 84
Data interface 21
Data terminal 129
Date 34
Date format 34
Daylight saving time 35
Default settings 63
Defaults 44, 73
Defaults recording profiles 63
Deleting partitions 62

Deleting recordings 62

Device reset 121

Display stamping 37

Dome camera 21

Dual Streaming 13, 41

E

Echo 130

Editing a partition 60

Electromagnetic compatibility 8

E-mail 79

Encoding 13

Encryption 91

Encryption protocol 87

EPROM 98

Establishing the connection 28, 104

Event log 96, 107

F

False alarms 74

Firewall 86

Firmware upload 98

Firmware version 93

Formatting 62

Front panel 16, 17

FTP server 48, 49

Function test 101

G

Gateway 86

General password 71

H

Half-duplex mode 84

Hardware version 93

Holidays 67

I

Identification 8, 32

IEEE 802.1x 88

IGMP V2 89

Image quality 90

Image resolution 108

Image selection 105

Indicator processor load 126

Installation 10

Installation conditions 19

Installation location 19

Interface 127

Interface mode 84

Internal clock 34

IP address 86, 130

iSCSI settings 52

J

JPEG format 48

JPEG posting 48

JPEG posting interval 49

L

Language 34

Licenses 97

Linear mode 61

Live video images 27, 103

Livepage 94

Loudspeaker 21, 47

Low Voltage Directive 8

Low-pass filter 40

M

Main functions 15
Maintenance 10
Make contact 22
Manufacturer logo 94
Marker 113
maximum number 29
Media playback 110
Microphone 21, 47
Monitor resolution 27, 103, 116
Motion detector 73
Motion detector defaults 73
Motion detector object size 75
Motion detector sensitivity 74, 76
MPEG ActiveX 27, 103, 115, 116
MPEG viewer 115
MPEG-4 encoder 41
MTU value 86
Multicast 89
Multicast address 89
Multicast connection 86, 89
Multicast function 14
Multicasting 89
Multi-unicast 89

N

Navigation 31
Network 22, 85
Network check 121
Network connection 24
Number of connections 29, 105

O

Operation 9, 103

Overview of functions 13

P

Parameters 26, 131
Parity 84
Partition 56
Partition status 59
Partitioning 56
Password 29, 32, 33, 105
Peripheral device control 106
Picture settings 39
Pin assignment 128
Playback 110
Playback button 112
Playback on PC 116
Port 86, 90
Post-alarm profile 64
Post-alarm time 64
Power off 24
Power on 24
Power supply 9
Power switch 24
Power-over-Ethernet 13
Processor load 126
Product name 94
Profile settings 43
Profiles 41
Protocol 84
Protocols 136

R

RADIUS 88
Rear panel 17
Receiver 13

Receiver password 71
Recording activity 68
Recording program 109
Recording scheduler 63, 66
Recording video sequences 108
Reflections of light 74
Regulations 7
Relay 81
Relay output 22, 81
Remote control 14
Repair 10, 122
Reset 121
Reset of profile 44
Restart 26, 131
Ring mode 61
Router 90

S

Safety 9
Saturation 39
Saving event log 96
Saving system log 96
Selecting a profile 41
Selecting the area 75, 77, 78
Sensor fields 75, 78
Serial number 8
Serial port function 83
Setup 11
Signal source 22
Size alarm track 61
SMS 79
Snapshots 14, 108
SNMP 87
SNTP server 36

Software decoder 120
Source type 46
Specifications 135
SSL certificate 99
Standards 136
Stop bits 84
Storage information 51, 55
Storage medium 50
Streaming 90
Subnet mask 86
Symbols 7
Synchronize 34
System log 96, 97, 107
System requirements 27

T

Tamper detection 76
Target data rate 44
TCP 86
Terminal 83
Termination 46
Test 101
Time 34, 37
Time server 35
Time server IP address 36
Time server protocol 35
Time server type 36
Time signal 35
Time zone 35
TLS 87
Transmission parameters 129
Transmission protocol 86
Transmission rate 84
Transmission standards 21, 127

Transmit audio 95

Transparent 83

Traps 88

Trigger relay 82

TTL 90

U

UDP 86

Unicast 89

Unit date 34

Unit ID 32

Unit identification 32

Unit name 32

Unit time 34

URL 28, 104, 117

User name 33

V

VCA metadata 73, 96

VCR 46

Version 93

Video content analysis 73

Video input 16, 46

Video loss alarm 69

Video recorder 46

Video sensor 73

Video signal interruption 69

W

Watermarking 38

Bosch Sicherheitssysteme GmbH
Robert-Koch-Straße 100
85521 Ottobrunn
Germany
www.bosch-sicherheitssysteme.de

Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven
The Netherlands
www.boschsecuritysystems.com

© 2006 Bosch Sicherheitssysteme GmbH
Subject to change.
2501B/1206/en/4

BOSCH