



# VIP X1600 XFMD

Decoder Module



**BOSCH**



# Table of Contents

<b>1</b>	<b>Preface</b>	<b>5</b>
1.1	About this Manual	5
1.2	Conventions in this Manual	5
1.3	Intended Use	5
1.4	EU Directives	6
1.5	Rating Plate	6
<b>2</b>	<b>Safety Information</b>	<b>7</b>
2.1	Electric Shock Hazard	7
2.2	Installation and Operation	7
2.3	Maintenance and Repair	7
<b>3</b>	<b>Product Description</b>	<b>9</b>
3.1	Scope of Delivery	9
3.2	System Requirements	9
3.3	Overview of Functions	10
3.4	Connections	12
<b>4</b>	<b>Installation</b>	<b>13</b>
4.1	Preparations	13
4.2	Installing Modules	13
4.3	Connections	15
4.4	Setup Using the Configuration Manager	17
<b>5</b>	<b>Configuration Using a Web Browser</b>	<b>19</b>
5.1	Connecting	19
5.2	Configuration Menu	22
5.3	Identification	23
5.4	Password	23
5.5	Date/Time	24
5.6	Appearance	26
5.7	Decoder Profile	27
5.8	Monitor Display	28
5.9	Audio	28
5.10	Alarm Connections	29
5.11	Audio Alarm	32
5.12	Alarm E-Mail	33
5.13	Alarm Task Editor	35
5.14	Alarm Inputs	36
5.15	Relay	36
5.16	COM1	38
5.17	Network	39
5.18	Advanced	42
5.19	Encryption	43
5.20	Maintenance	44

---

5.21	Licenses	46
5.22	System Overview	46
5.23	Function Test	47
<hr/>		
<b>6</b>	<b>Operation</b>	<b>49</b>
6.1	Connecting	49
6.2	The CONNECTIONS Page	52
6.3	Connections Between the Sender and Receiver	53
6.4	Hardware Connections Between Video Servers	55
6.5	Operation with Management Software	56
<hr/>		
<b>7</b>	<b>Maintenance and Upgrades</b>	<b>57</b>
7.1	Testing the Network Connection	57
7.2	Unit Reset	57
7.3	Repairs	58
7.4	Transfer and Disposal	58
<hr/>		
<b>8</b>	<b>Appendix</b>	<b>59</b>
8.1	Troubleshooting	59
8.2	Processor Load	61
8.3	Network Connection	61
8.4	Serial Interface	62
8.5	Terminal Block	62
8.6	Communication with Terminal Program	63
8.7	Copyrights	65
<hr/>		
<b>9</b>	<b>Specifications</b>	<b>67</b>
9.1	VIP X1600 XFMD Decoder Module	67
9.2	Protocols/Standards	67
<hr/>		
<b>10</b>	<b>Glossary</b>	<b>69</b>
<hr/>		
<b>11</b>	<b>Index</b>	<b>73</b>

# 1 Preface

## 1.1 About this Manual

This manual is intended for persons responsible for the installation and operation of the VIP X1600 XF. International, national and any regional electrical engineering regulations must be followed at all times. Relevant knowledge of network technology is required. The manual describes the installation and operation of the unit.

## 1.2 Conventions in this Manual

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



### **CAUTION!**

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

---



### **NOTICE!**

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

---

## 1.3 Intended Use

The VIP X1600 XF network video server is intended for use with CCTV systems and serves to transfer video and control signals via data networks (Ethernet LAN and Internet). The optional modules for installation determine the range of functions. Encoder modules (senders) and decoder modules (receivers) are available. Audio signals can also be transmitted with the audio versions of the encoder modules. Various functions can be triggered automatically by incorporating external alarm sensors. Other applications are not permitted.

In the event of questions concerning the use of the unit which are not answered in this manual, please contact your sales partner or:

Bosch Security Systems  
Robert-Koch-Straße 100  
85521 Ottobrunn  
Germany  
[www.boschsecurity.com](http://www.boschsecurity.com)

## 1.4 EU Directives

The VIP X1600 XF network video server complies with the requirements of EU Directives 89/336 (Electromagnetic Compatibility) and 73/23, amended by 93/68 (Low Voltage Directive).

## 1.5 Rating Plate

For exact identification, the model name and serial number are inscribed on the rating plate on the bottom of the VIP X1600 XF base and on the rating plates on the circuit boards of the modules. Please make a note of this information before installation, if necessary, so as to have it to hand in case of questions or when ordering spare parts.

## 2 Safety Information

### 2.1 Electric Shock Hazard

- Always install a module in the appropriate VIP X1600 XF base or VIP X1600 B base housing only.
- If a fault occurs, disconnect the VIP X1600 XF from the power supply and from all other units.
- Install the power supply and the unit only in a dry, weather-protected location.
- If safe operation of the unit cannot be ensured, remove it from service and secure it to prevent unauthorized operation. In such cases, have the unit checked by Bosch Security Systems .

Safe operation is no longer possible in the following cases:

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

### 2.2 Installation and Operation

- The relevant electrical engineering regulations and guidelines must be complied with at all times during installation.
- Relevant knowledge of network technology is required to install the unit.
- Before installing or operating the module, please ensure you have read and understood the documentation for the VIP X1600 XF base or VIP X1600 B base and for any other equipment connected to the module, such as monitors. The documentation contains important safety instructions and information about permitted uses.
- Perform only the installation and operation steps described in this manual. Any other actions may lead to personal injury, damage to property or damage to the equipment.

### 2.3 Maintenance and Repair

- Never open the housing of a VIP X1600 XF base or VIP X1600 B base. The unit does not contain any user-serviceable parts. Remove only the supplied cover when installing a module.
- Do not change any components in a VIP X1600 XF base or VIP X1600 B base or a module. The units do not contain any user-serviceable parts.
- Never open the housing of the power supply unit. The power supply unit does not contain any user-serviceable parts.
- Ensure that all maintenance or repair work is carried out only by qualified personnel (electrical engineers or network technology specialists).





## 3 Product Description

### 3.1 Scope of Delivery

- VIP X1600 XFMD decoder module
- Mounting kit for installation in the VIP X1600 XF base
- Terminal plugs
- Quick Installation Guide

**NOTICE!**

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

---

### 3.2 System Requirements

**General Requirements**

- VIP X1600 XF base or VIP X1600 B base housing
- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM

**NOTICE!**

Also note the information in the **System Requirements** document on the product CD supplied with the VIP X1600 XF base. If necessary, you can install the required programs and controls from the product CD.

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

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

You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

---

**Additional Configuration Requirements**

- Microsoft Internet Explorer (version 6.0 or higher)  
or
- Installed Configuration Manager program (version 2.0 or higher)

**Additional Operational Requirements**

- Microsoft Internet Explorer (version 6.0 or higher)  
or
- Management software, for example VIDOS (version 3.11 or higher) or Bosch Video Management System (version 2.02 or higher)

## 3.3 Overview of Functions

### Network Video Decoder

The VIP X1600 XFMD decoder module is a network video receiver for simultaneous reception of up to ten video streams in MPEG-4 format or up to four video streams in MPEG-2 D1 VES format. It is primarily designed for decoding video data after transfer over an IP network and for transmitting control data. When connected to up to four monitors and used in conjunction with compatible video servers, the module is ideally suited for making existing analog CCTV systems IP-compatible. Two units, for example a VideoJet X40 as a sender and a VIP X1600 XF with decoder module as a receiver, can create a standalone system for data transfer without a PC. Video images from a single sender can be received simultaneously on multiple receivers. In addition to video streams in MPEG-4 format, audio signals can also be transmitted from and to compatible units. The module is designed for installation in the VIP X1600 XF base and the VIP X1600 B base. Installing the units is a quick and easy operation that does not require any additional tools. All modules are hot swappable and can be exchanged while the system is running.

### Sender

Compatible hardware encoders can be used as senders, for example VIP X1600 or VideoJet X40. Computers with installed VIDOS software are suitable for convenient connection of the required senders to the respective receivers.

### Multicast

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

### Encryption

The VIP X1600 XFMD encoder module offers a variety of options for protection against unauthorized reading. Web browser connections can be protected using HTTPS. You can protect the control channels via the SSL encryption protocol. With an additional license, the user data itself can be encrypted.

### Configuration

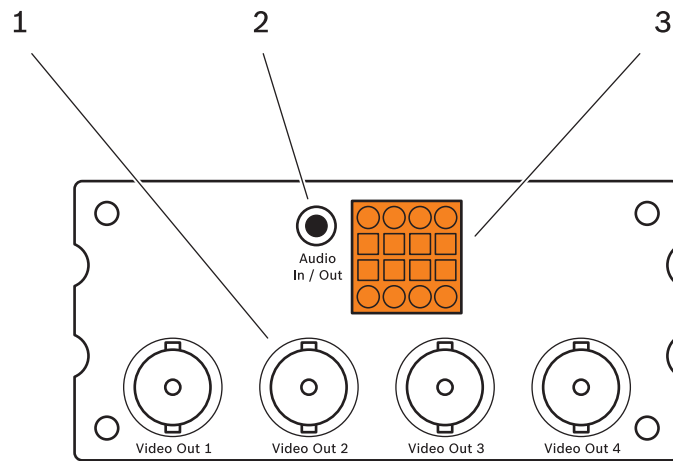
The module can be configured with a Web browser on the local network (Intranet) or via the Internet. Alternatively, you can perform the configuration using the Configuration Manager program contained on the product CD, which comes supplied with the VIP X1600 XF base. In the same way, firmware updates and fast loading of device configurations are possible.

**Summary**

The VIP X1600 XFMD decoder module provides the following main functions:

- Video and data reception over IP data networks
- Quad view function with simultaneous decoding of four video streams
- Four BNC composite video outputs (PAL/NTSC) for connecting four analog monitors
- Video decoding using MPEG-4 and MPEG-2
- Transparent, bidirectional data channel via RS-232/RS-422/RS-485 serial interface
- Configuration and remote control of all internal functions via TCP/IP, also secured via HTTPS
- Password protection to prevent unauthorized connection or configuration changes
- Alarm inputs for external sensors (such as a door contact)
- Relay output for switching external units (such as lamps or sirens)
- Event-controlled automatic connection
- Convenient maintenance via uploads
- Flexible encryption of control and data channels
- Authentication according to international standard 802.1x
- Transmission and receipt of audio signals
- Bidirectional audio (mono) for line connections
- Audio encoding to international standard G.711

## 3.4 Connections



- 1** Video outputs **Video Out 1** to **Video Out 4**  
BNC sockets for connecting video monitors
- 2** Audio connection (mono) **Audio In / Out**  
3.5 mm / 1/8 in. stereo socket line-out for connecting an audio connection
- 3** Terminal block  
for alarm input, relay output and serial interface

## 4 Installation

### 4.1 Preparations

The module is exclusively designed for installation in the VIP X1600 XF base and the VIP X1600 B base. Installing the units is a quick and easy operation that does not require any additional tools.

### 4.2 Installing Modules

Installing the different VIP X1600 XF modules in the VIP X1600 XF base or the VIP X1600 B base is described in the relevant Quick Installation Guide. Please also take note of the following basic notes when installing a unit.

**CAUTION!**

Do not install a module in a different housing and do not operate the unit outside of the VIP X1600 XF base or the VIP X1600 B base. The ambient temperature during installation and operation must be between 0 und +50 °C (+32 und +122 °F), and the relative humidity must not exceed 80% (non-condensing).

---

**Installation Sequence and Capacity of the VIP X1600 XF Base****CAUTION!**

Ensure that Slot 1 is always populated by a module, even when modifying the installation. Malfunctions may occur when the VIP X1600 XF is switched on without a functional module in Slot 1.

You can install up to four modules in a VIP X1600 XF base. Slot 1 must always be the first slot that is populated. The remaining slots can be populated in any order desired. It is also possible to install and remove modules during operation.

**Cooling****CAUTION!**

Whenever the installation is modified, or modules are exchanged or supplemented, it is essential that all unpopulated slots are properly covered on the rear side of the VIP X1600 XF base.

The installed modules generate a high volume of heat during operation. As a result, it is essential that a functional heat dissipation system is in place for problem-free operation of a VIP X1600 XF.

**Rating Plates**

Every module has a label on the circuit board containing a printed MAC address by which the module can be uniquely identified. Take note of this MAC address and the location in the VIP X1600 XF base before installation so that you can later identify the module, even after it has been inserted, for example when performing fault diagnosis.

**Removing and Exchanging Modules**

It is also possible to install, remove and exchange modules during operation.

**CAUTION!**

Ensure that Slot 1 is always populated by a module, even when modifying the installation. Malfunctions may occur when the VIP X1600 XF is switched on without a functional module in Slot 1.

1. Before removing a module, terminate all recordings currently running in this module.
2. When installing a module, please ensure that the cover is kept for future use.
3. When removing a module, it is essential that the corresponding slot be closed with the cover if a module is no longer to be used in this slot. The opening must be closed to ensure that the unit remains cool.

## 4.3 Connections

### Monitors

You can connect up to four analog video monitors (PAL/NTSC) to each decoder module.

- ▶ Connect an analog video monitor to each of the BNC sockets **Video Out 1** to **Video Out 4** using a video cable (75 Ohm, BNC plug).

### Audio Connection

The decoder module has an audio connection for audio line signals (input and output, both mono).

The audio signals are transmitted two-way and in sync with the MPEG-4 video signals. As a result, you can connect a speaker or door intercom system at the destination point, for example. It is not possible to simultaneously transmit audio signals when transmitting MPEG-2 video signals.

<b>Line In:</b>	Impedance 9 kOhm typ., 5.5 V <sub>p-p</sub> max. input voltage
<b>Line Out:</b>	Impedance 16 Ohm min., 3 V <sub>p-p</sub> max. output voltage

The stereo plug must be connected as follows:

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

- ▶ Connect an audio source with line level and a unit with line-in connection to the **Audio In / Out** socket with a 3.5 mm / 1/8 in stereo plug.

### Data Interface

The bidirectional data interface of the decoder module is used to control connected units, for example a control panel for dome cameras with motorized lens. The connection supports the RS-232, RS-422 und RS-485 transmission standards.

The connection is managed using the orange terminal block (see *Section Pin Assignment, page 62*).

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



### CAUTION!

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

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



### NOTICE!

A video connection is necessary to transmit transparent data.

**Alarm Input**

The module offers an alarm input via the orange terminal block (see *Section Pin Assignment, page 62*). The alarm input is used to connect to external alarm devices such as door contacts or sensors. When configured appropriately, an alarm device can, for example, trigger the module to automatically establish a connection with a remote station.

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

**NOTICE!**

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

- 
- ▶ Connect the lines to the **IN** and **GND** terminals of the orange terminal block and check that the connection is secure.

**Relay Output**

The module has a relay output for switching external units such as lamps or sirens. You can operate this relay output manually while there is an active connection to the module. 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 (see *Section Pin Assignment, page 62*).

**CAUTION!**

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

- 
- ▶ Connect the lines to both **REL** terminals of the orange terminal block and check that the connection is secure.



## 4.4 Setup Using the Configuration Manager

The **Configuration Manager** program can be found on the product CD supplied with the VIP X1600 XF base. This program allows you to implement and set up new modules quickly and conveniently.



### NOTICE!

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

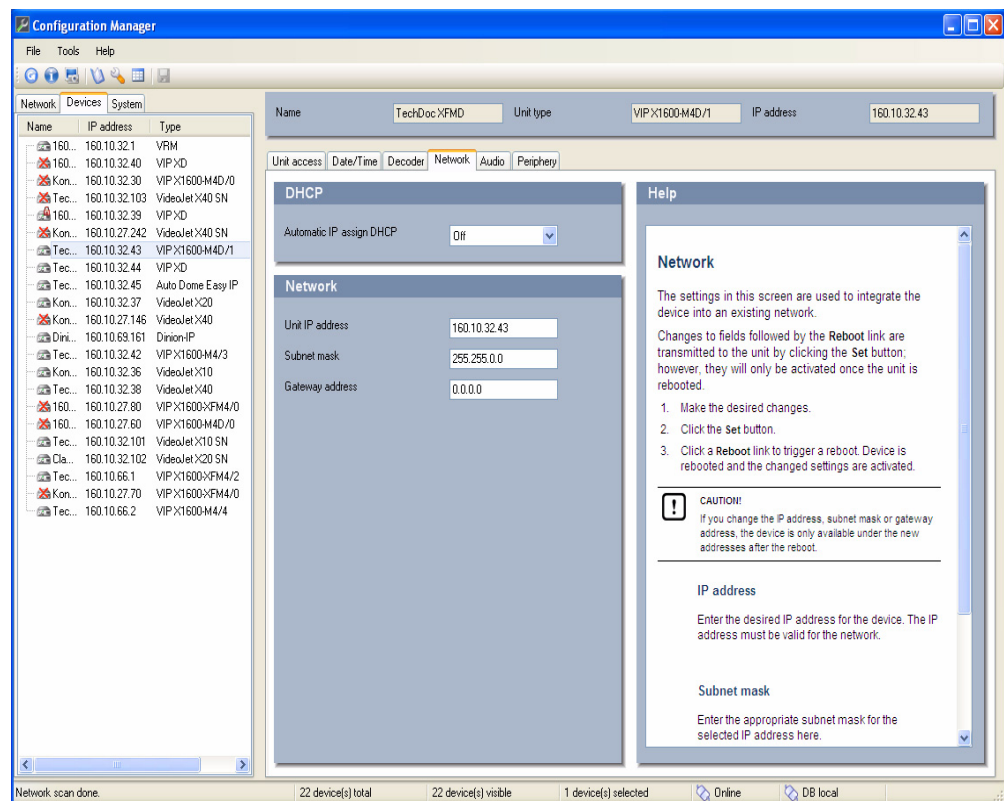
### Installing the Program

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

### Configuring the Module

You can start the Configuration Manager immediately after installation.

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



2. You can start the configuration if the module is shown in the list in the left section of the window. To do this, right-click the entry for the module.
3. Click **Unit network settings...** in the context menu.
4. In the **Unit IP address** field, enter a valid IP address for your network (for example **192.168.0.16**) and click **OK**. The unit reboots and the IP address is valid.
5. If required, enter an appropriate subnet mask for the IP address, and additional network data.

**NOTICE!**

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

---

**Reboot**

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

- ▶ Right click the entry for the module 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

### 5.1 Connecting

The integrated HTTP server in the VIP X1600 XF offers you the option of configuring the unit over the network with a Web browser. This option is an alternative to configuration using the Configuration Manager program and is considerably richer in function and more convenient than configuration using the terminal program.

#### System Requirements

- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 6.0 or higher)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM



#### NOTICE!

Also note the information in the **System Requirements** document on the product CD supplied with the VIP X1600 XF base. If necessary, you can install the required programs and controls from the product CD.

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

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

You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

#### Installing MPEG ActiveX

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

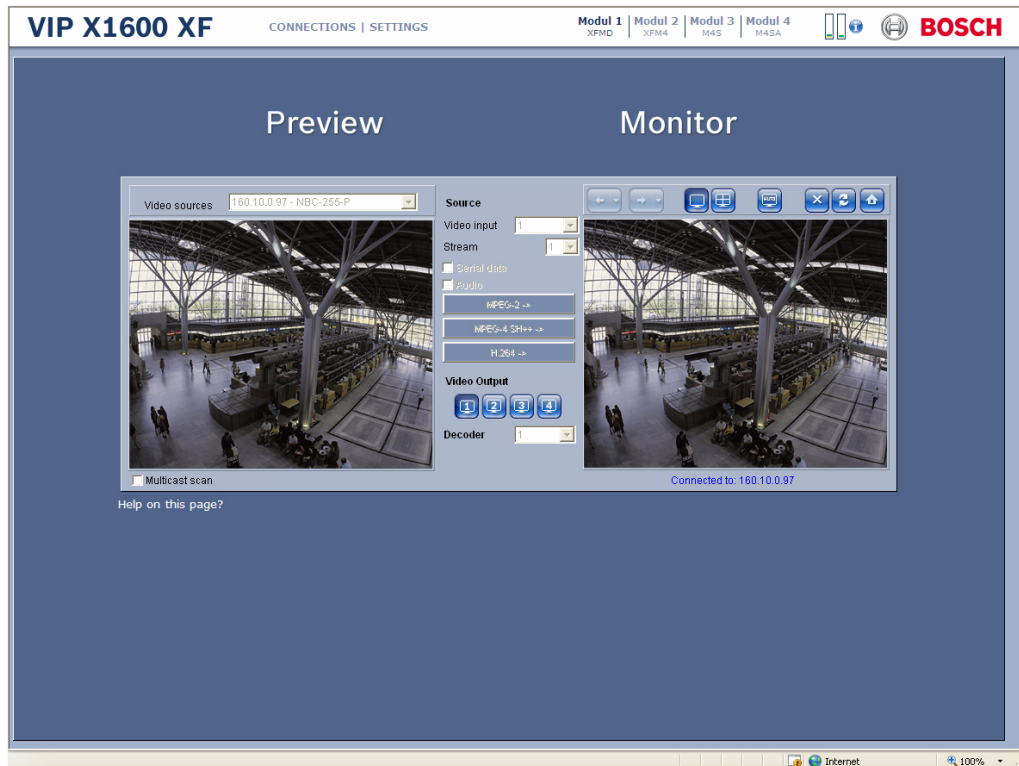
1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

### Establishing the Connection

At least the module in Slot 1 must be assigned a valid IP address and a compatible subnet mask to operate the VIP X1600 XF on your network.

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

1. Start the Web browser.
2. Enter the module's IP address as the URL. The connection is established and after a short time you will see the **CONNECTIONS** page.



### Maximum Number of Connections

If you do not connect, the unit may have reached its maximum number of connections.

Depending on the unit and network configuration, each module can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

---

**Protected Module**

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

**NOTICE!**

The modules offer the option to limit the extent of access using various authorization levels (see *Abschnitt 5.4 Password, Seite 23*).

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

**Protected Network**

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

To configure the unit, you must connect the VIP X1600 XF directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated (see *Abschnitt Authentication, Seite 43*).

**CAUTION!**

The switch used for the network must support the multi-host operation when using 802.1x authentication and must be configured so that a VIP X1600 XF with several modules can try several hosts for communicating over the network.

---

## 5.2 Configuration Menu

The **SETTINGS** page provides access to the configuration menu, which contains all the unit's parameters arranged in groups.

You can view the current settings by opening one of the configuration screens. You can change the settings by entering new values or by selecting a predefined value from a list field. All parameter groups are described in this chapter in the order in which they are listed in the configuration menu, from the top of the screen to the bottom.



### CAUTION!

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

---

All settings are stored in the module's memory so that they are retained even if the power supply is interrupted.

### Navigation

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

### Making Changes

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

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



### CAUTION!

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

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

---

### 5.3 Identification



#### Device ID

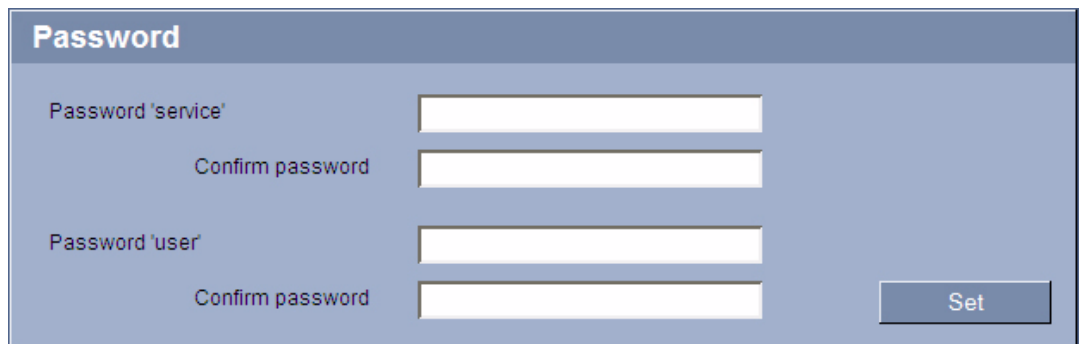
Each module should be assigned a unique identifier that you can enter here as an additional means of identification.

#### Device name

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

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

### 5.4 Password



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



#### NOTICE!

Proper password protection with a **user** password is only guaranteed when the higher authorization level **service** is also password protected. When assigning passwords, you should therefore always start from the highest authorization level, **service**, and use different passwords.

### Password

The module operates with two authorization levels: **service** and **user**.

The highest authorization level is **service**. After entering the correct password, this user name allows you to use all the functions of the module and change all configuration settings.

You can use the **user** authorization level to connect the unit to a sender in the network and to disconnect it, but you cannot change the configuration.

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

Enter the password for the appropriate authorization level here.

### Confirm password

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



#### NOTICE!

A 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.

## 5.5

### Date/Time



#### NOTICE!

The module in Slot 1 is the time server for the module in Slot 2 to Slot 4. Consequently, these settings are only possible for the module in Slot 1.

#### Date format

Select your required date format.

#### Unit date / Unit time

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

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

#### Unit time zone

Select the time zone in which your system is located.



### Daylight saving time

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



#### NOTICE!

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

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

### Time server IP address

Enter the IP address of a time server.

### Time server type

The VIP X1600 XFMD 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.

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

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

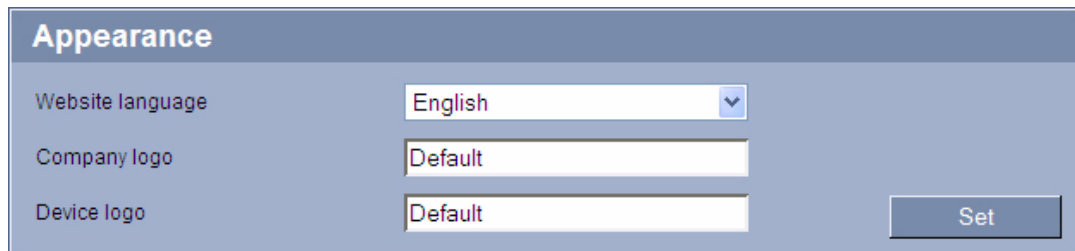


#### NOTICE!

Select the same time server type for the modules in Slot 2 to Slot 4 as for the module in Slot 1.

---

## 5.6 Appearance



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



### NOTICE!

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

When accessing via the Internet/Intranet, ensure that a connection is always available to display the image. The image file is not saved in the module.

### Website language

Select the language for the user interface here.



### NOTICE!

There are always two languages to choose from: English and another language. If the language you require is not available for selection, you can download the current firmware with another language combination from the website [www.boschsecurity.com](http://www.boschsecurity.com).

### Company logo

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

### Device logo

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



### NOTICE!

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

## 5.7 Decoder Profile

**Decoder Profile**

Monitor 1

Monitor name:

Standard:

Window layout:  Single view  Quad view

Monitor 2

Monitor name:

Standard:

Monitor 3

Monitor name:

Standard:

Window layout:  Single view  Quad view

Monitor 4

Monitor name:

Standard:

In this screen you can set the various options for the display of video images on the monitors.

### Monitor name

You can give the connected monitors names to make them easier to identify. The names make the task of administering multiple units in larger video monitoring systems easier, for example using the VIDOS or Bosch Video Management System programs.

The monitor name allows you to remotely identify the monitor location. For this reason, enter a name that makes it as easy as possible to quickly identify the location.

### Standard

You can adapt the video output signal to the monitor you are using. PAL and NTSC options are available for this.

### Window layout

You can specify the standard window layout for monitors 1 and 3. The image layout can also be selected at any time during operation on the **CONNECTIONS** page.

## 5.8 Monitor Display

The screenshot shows a configuration panel titled "Monitor Display". It contains three rows of settings:

- Display transmission disturbance:** A dropdown menu currently set to "Off".
- Disturbance sensitivity:** A slider control with a numerical input field set to "0".
- Disturbance notification text:** A text input field containing the word "FREEZE".

A "Set" button is located in the bottom right corner of the panel.

The VIP X1600 XFMD can recognize transmission interruptions and display a warning on the monitor if set accordingly. With Quad view, the warning is displayed in the relevant quadrant. The settings here apply to all monitors and connections.

### Display transmission disturbance

Select **On** if the appropriate monitor is to display a warning in the event of a transmission interruption.

### Disturbance sensitivity

You can set the level of interruption at which the display should be triggered.

### Disturbance notification text

Enter the text that the VIP X1600\_XFMD should display on the monitor. The maximum text length is 31 characters.

## 5.9 Audio

The screenshot shows a configuration panel titled "Audio". It contains three rows of settings:

- Audio:** A dropdown menu currently set to "On".
- Line In:** A slider control with a numerical input field set to "21".
- Line Out:** A slider control with a numerical input field set to "53".

A "Set" button is located in the bottom right corner of the panel.

You can set the gain of the audio signals to suit your specific requirements. Your changes are effective immediately.

If you connect via Web browser you must activate the audio transmission on the **CONNECTIONS** page (see *Section 6.2 The CONNECTIONS Page, page 52*). For other connections, the transmission depends on the audio settings of the respective system.

### Audio

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

**Line In**

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

**Line Out**

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

**5.10 Alarm Connections**

Alarm Connections	
Connect on alarm	Off
Number of destination IP address	1
Destination IP address	0.0.0.0
Destination password	
Video transmission	UDP
Remote port	80
Video output	First available
Decoder	First available
SSL encryption	Off
Auto-connect	Off
Audio	Off
Default camera	1

You can select how the VIP X1600 XFMD responds to an alarm. In the event of an alarm, the unit can automatically connect to a pre-defined IP address. You can enter up to ten IP addresses to which the VIP X1600 XFMD will connect in sequence in the event of an alarm, until a connection is made.

**Connect on alarm**

Select **On** so that the VIP X1600 XFMD automatically connects to a predefined IP address in the event of an alarm.

By setting **Follows input 1**, the VIP X1600 XFMD automatically connects to a remote station and holds the connection as long as an alarm exists on the alarm input. This option can also be used to connect two units (sender and receiver) via a switch connected to the VIP X1600 XFMD. You do not need a computer to make the connection in this case.



**NOTICE!**

In the default setting, Stream 2 is transmitted for automatic connections. Bear this fact in mind when assigning the profile to the corresponding sender.

**Number of destination IP address**

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

**Destination IP address**

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

**Destination password**

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

In this page, you can save a maximum of ten destination IP addresses and hence up to ten passwords for connecting to remote stations. If connections to more than ten remote stations are to be possible, for example when initiating connections via higher-ranking systems such as VIDOS or Bosch Video Management System, you can store a general password here. The VIP X1600 XFMD can use this general password to connect to all remote stations protected with the same password. In this case, proceed as follows:

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

**NOTICE!**

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

---

**Video transmission**

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

---

**CAUTION!**

Please note that in some circumstances, a larger bandwidth must be available on the network for additional video images in the event of an alarm, in case Multicast operation is not possible. To enable Multicast operation, select the **UDP** option for the **Video transmission** parameter here and on the **Network** page (see *Section Video transmission, page 40*).

---

**Remote port**

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

**Video output**

Select a video output to display the alarm image. The video output selected defines whether the image can be displayed on a split screen. Display on a split screen is only possible for the video outputs 1 and 3.

**Decoder**

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

---

**SSL encryption**

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

**NOTICE!**

Please note that the SSL encryption must be activated and configured at both ends of a connection. This requires the appropriate certificates to be uploaded onto the VIP X1600 XFMD (see *Section Delete decoder logo, page 45*).

You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.19 Encryption, page 43*).

**Auto-connect**

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

**NOTICE!**

In the default setting, Stream 2 is transmitted for automatic connections. Bear this fact in mind when assigning the profile to the corresponding sender.

**Audio**

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

**Default camera**

Here you can select the camera whose image will be automatically displayed first on the receiver when the alarm connection is made. Depending on the system configuration, you can then select the other cameras as well.

**NOTICE!**

The numbering follows the labeling of the video inputs on the corresponding sender.

---

## 5.11 Audio Alarm

The VIP X1600 XFMD can create alarms on the basis of audio signals. You can configure signal strengths and frequency ranges in such a way that false alarms, for example due to machine noise or background noise, are avoided.



### NOTICE!

First set up normal audio transmission before you configure the audio alarm here (see *Section 5.9 Audio, page 28*).

### Audio alarm

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

### Name

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



### CAUTION!

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

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

### Threshold

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



**Sensitivity**

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

**Signal Ranges**

You can exclude particular signal ranges in order to avoid false alarms. For this reason the total signal is divided into 13 tonal ranges (mel scale). Check or uncheck the boxes below the graphic to include or exclude individual ranges.

**5.12 Alarm E-Mail**

The screenshot shows a configuration window titled "Alarm E-Mail". It contains the following fields and controls:

- Send alarm e-mail:** A dropdown menu currently set to "Off".
- Mail server IP address:** An empty text input field.
- SMTP user name:** An empty text input field.
- SMTP password:** An empty text input field.
- Format:** A dropdown menu currently set to "Standard".
- Destination address:** An empty text input field.
- Sender name:** An empty text input field.
- Test e-mail:** A button labeled "Send Now".
- Set:** A button labeled "Set".

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 X1600 XFMD automatically sends an e-mail to a previously defined e-mail address.

**Send alarm e-mail**

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

**Mail server IP address**

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

**SMTP user name**

Enter a registered user name for the chosen mailserver here.

**SMTP password**

Enter the required password for the registered user name here.

**Format**

You can select the data format of the alarm message.

- **Standard**  
E-mail.
- **SMS**  
E-mail in SMS format to an e-mail-to-SMS gateway (for example to send an alarm by cellphone).

**CAUTION!**

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

You can obtain information on operating your cellphone from your cellphone provider.

---

**Destination address**

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

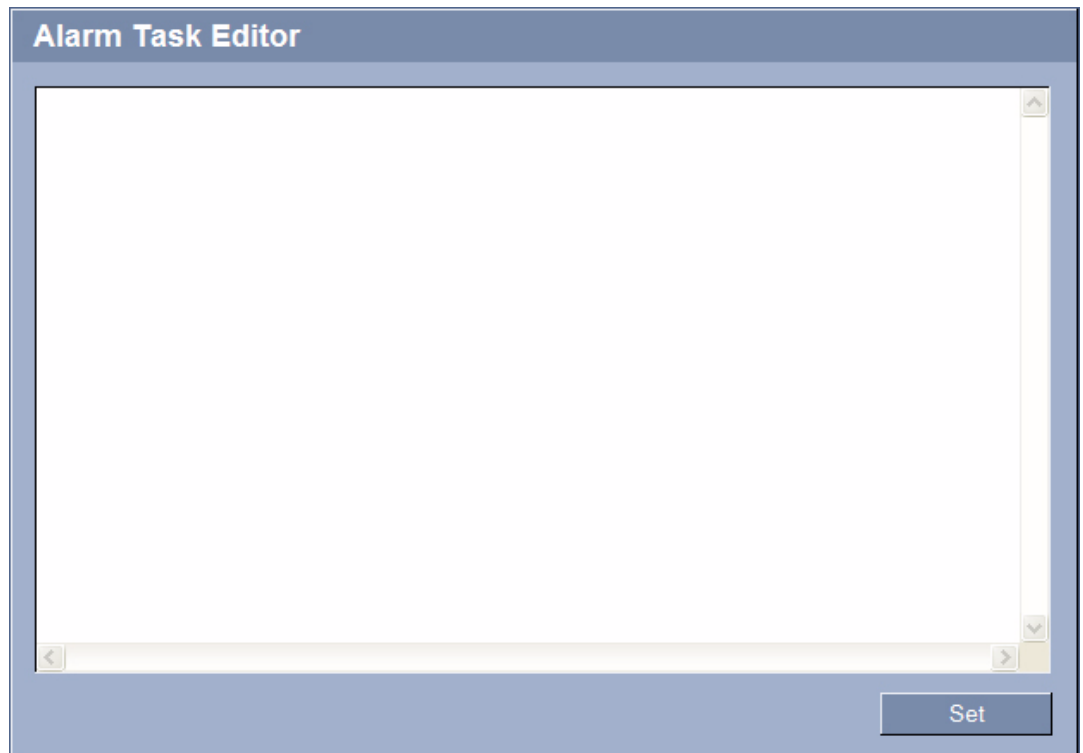
**Sender name**

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

**Test e-mail**

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

## 5.13 Alarm Task Editor



### CAUTION!

Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.

In order to edit this page, you must have programming knowledge and be familiar with the information in the **Alarm Task Script Language** document. You can find the document on the product CD supplied with the VIP X1600 XF base (see *Section 3.1 Scope of Delivery, page 9*).

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

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

## 5.14 Alarm Inputs

You can configure the alarm input of the module.

### Alarm input

Select **Active high** if the alarm is to be triggered when the contact closes. Select **Active low** if the alarm is to be triggered when the contact opens.

### Name

For easier identification, you can enter a name for the alarm input.

## 5.15 Relay

You can configure the switching behavior of the relay output. You can specify an open switch relay (normally closed contact) or a closed switch relay (normally open contact).

You can also specify whether the output should operate as a bistable or monostable relay. In bistable mode, the triggered state of the relay is maintained. In monostable mode, you can set the time after which the relay will return to the idle state.

You can select different events that automatically activate 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 ten seconds, for example, select **10 s**.

**Relay follows**

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

- **Off**  
Relay is not triggered by events
- **Connection**  
Trigger whenever a connection is made
- **Local input 1**  
Trigger by external alarm input 1
- **Remote input 1**  
Trigger by remote station's switching contact 1 (only if a connection exists)

**Relay name**

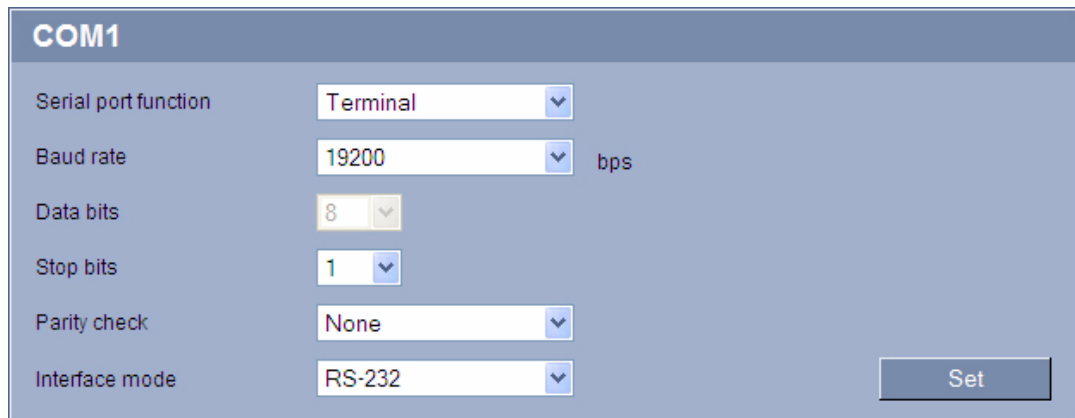
You can assign a name for the relay here. The name is shown on the button next to **Trigger relay**.

**Trigger relay**

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

## 5.16

### COM1



The screenshot shows a configuration window titled "COM1" with the following settings:

Parameter	Value
Serial port function	Terminal
Baud rate	19200 bps
Data bits	8
Stop bits	1
Parity check	None
Interface mode	RS-232

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.

#### Serial port function

Select the desired serial port function from the list. If you wish to use the serial port to transmit transparent data, when using a control desk for example, select **Transparent**. Select **Terminal** if you wish to operate the unit from a terminal.

#### Baud rate

Select the value for the transmission rate in bps.

#### Data bits

The number of data bits per character cannot be changed.

#### Stop bits

Select the number of stop bits per character.

#### Parity check

Select the type of parity check.

#### Interface mode

Select the desired protocol for the serial interface.

## 5.17 Network

### Network

**DHCP**

Automatic IP assignment Off

**Ethernet**

IP address

Subnet mask

Gateway address

DNS server address

Video transmission UDP

HTTP browser port 80

HTTPS browser port 443

RCP+ port 1756 On

Telnet support On

Interface mode ETH 1 Auto

Interface mode ETH 2 Auto

Interface mode ETH 3 Auto

Network MSS (Byte)

**DynDNS**

Enable DynDNS Off

Host name

User name

Password

Force registration now

Status DynDNS function switched off

The settings on this page are used to integrate the VIP X1600 XFMD into an existing network. Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.

- Click the **Set and Reboot** button. The VIP X1600 XFMD is rebooted and the changed settings are activated.

**CAUTION!**

If you change the IP address, subnet mask or gateway address, the VIP X1600 XFMD is only available under the new addresses after the reboot.

---

**Automatic IP assignment**

If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the VIP X1600 XFMD. Certain applications (VIDOS, Bosch Video Management System, Archive Player, Configuration Manager) use the IP address for the unique assignment of the unit. If you use these applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

**IP address**

Enter the desired IP address for the VIP X1600 XFMD in this field. The IP address must be valid for the network.

**Subnet mask**

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

**Gateway address**

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

**DNS server address**

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

**Video transmission**

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

---

**CAUTION!**

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

The MTU value in UDP mode is 1,514 bytes.

---

**HTTP browser port**

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

**HTTPS browser port**

If you wish to allow browser access on the network via a secure connection, select an HTTPS browser port from the list if necessary. The default HTTPS port is 443. Select the **Off** option to deactivate HTTPS ports; only unsecured connections will now be possible.

The VIP X1600 XFMD uses the TLS 1.0 encryption protocol. You may have to activate this protocol via your browser configuration. You must also activate the protocol for the Java applications (via the Java control panel in the Windows control panel).



**NOTICE!**

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

---

You can activate and configure encryption of the media data (video, audio and metadata) on the **Encryption** page (see *Section 5.19 Encryption, page 43*).

**RCP+ port 1756**

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

**Telnet support**

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

**Interface mode ETH 1/ETH 2/ETH 3 (only for the module in Slot 1)**

If required, select the Ethernet link type for the **ETH 1**, **ETH 2** and **ETH 3** interfaces on the VIP X1600 XF. Depending on the unit connected, it may be necessary to select a special operation type. These settings can only be configured for the module in Slot 1.

**Network MSS (Byte)**

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

**Enable DynDNS**

DynDNS.org is a DNS hosting service that stores IP addresses in a database ready for use. It allows you to select the VIP X1600 XFMD via the Internet using a host name, without having to know the current IP address of the unit. You can enable this service here. To do this, you must have an account with DynDNS.org and you must have registered the required host name for the unit on that site.

---

**NOTICE!**

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

---

**Host name**

Enter the host name registered on DynDNS.org for the VIP X1600 XFMD here.

**User name**

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

**Password**

Enter the password you registered at DynDNS.org here.

**Force registration now**

You can force the registration by transferring the IP address to the DynDNS server. Entries that change frequently are not provided in the Domain Name System. It is a good idea to force the registration when you are setting up the device for the first time. Only use this function when necessary and no more than once a day, to avoid the possibility of being blocked by the service provider. To transfer the IP address of the VIP X1600 XFMD, click the **Register** button.

**Status**

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

**5.18****Advanced**

**Advanced**

SNMP

SNMP

1. SNMP host address

2. SNMP host address

SNMP traps

802.1x

Authentication

Identity

Password

RTSP

RTSP port

The settings on this page are used to implement advanced settings for the network.

Some changes only take effect after the unit is rebooted. In this case, the **Set** button changes to **Set and Reboot**.

1. Make the desired changes.
2. Click the **Set and Reboot** button. The VIP X1600 XFMD is rebooted and the changed settings are activated.

## SNMP

The VIP X1600 XFMD supports the SNMP V2 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. The unit supports SNMP MIB II in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target units here.

If you select **On** for the **SNMP** parameter and do not enter an SNMP host address, the VIP X1600 XFMD does not send them automatically, but only replies to SNMP requests. If you enter one or two SNMP host addresses, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

### 1. SNMP host address / 2. SNMP host address

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

### SNMP traps

You can select which traps are to be sent.

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

### Authentication

If a RADIUS server is employed in the network for managing access rights, authentication must be activated here to allow communication with the module. The RADIUS server must also contain the corresponding data.



### CAUTION!

The switch used for the network must support the multi-host operation when using 802.1x authentication and must be configured so that a VIP X1600 XF base with several modules can try several hosts for communicating over the network.

---

Settings for authentication are only necessary for the module in Slot 1. This makes for the automatic authentication of the other modules.

To configure the unit, you must connect the VIP X1600 XF base directly to a computer using a network cable. This is because communication via the network is not enabled until the **Identity** and **Password** parameters have been set and successfully authenticated.

### Identity

Enter the name that the RADIUS server is to use for identifying the VIP X1600 XFMD.

### Password

Enter the password that is stored in the RADIUS server.

### RTSP port

If necessary, select a different port for the exchange of the RTSP data from the list. The standard RTSP port is 554. Select **Off** to deactivate the RTSP function.

## 5.19

### Encryption

A special license, with which you will receive a corresponding activation key, is required to encrypt user data. You can enter the activation key to release the function on the **Licenses** page (see *Section 5.21 Licenses, page 46*).

## 5.20

## Maintenance

Maintenance			
Firmware	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Upload"/>
Progress	<input type="text" value="0%"/>		
Configuration	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Upload"/>
			<input type="button" value="Download"/>
SSL certificate	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Upload"/>
Decoder logo	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Upload"/>
Delete decoder logo			<input type="button" value="Delete"/>
Maintenance log			<input type="button" value="Download"/>

**Firmware**

The VIP X1600 XFMD 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 X1600 XFMD 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 flash-EPROM being incorrectly programmed. This in turn can result in the unit no longer being addressable, in which case it will have to be replaced. Even changing to another page or closing the browser window leads to an interruption.

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

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

If the LED of the corresponding module on the front panel of the VIP X1600 XF is showing red, the upload has failed and must be repeated. To perform the upload you must now switch to a special page:

1. In the address bar of your browser, enter **/main.htm** after the IP address of the VIP X1600 XFMD (for example **192.168.0.32/main.htm**).
2. Repeat the upload.

### Configuration

You can save configuration data for the VIP X1600 XFMD on a computer and then load saved configuration data from a computer to the unit.

#### Upload

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

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

#### Download

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

#### SSL certificate

To be able to work with an SSL encrypted data connection, both ends of a connection must hold the relevant certificates. You can upload the SSL certificate, comprising one or multiple files, onto the VIP X1600 XFMD.

If you wish to upload multiple files onto the VIP X1600 XFMD, you must select them consecutively.



#### NOTICE!

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

---

1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Next, click **Upload** to begin transferring the file to the unit.
3. Once all files have been successfully uploaded, the unit must be rebooted. In the address bar of your browser, enter **/reset** after the IP address of the VIP X1600 XFMD (for example **192.168.0.32/reset**).

The new SSL certificate is valid.

#### Decoder logo

If no video camera is selected, the decoder logo is displayed instead of the camera image. It is possible to create your own decoder logo and load it onto the VIP X1600 XFMD.

To create the logo, you need a special program, which is available from Bosch Security Systems. Standard image formats are not supported for the decoder logo.

1. Enter the full path of the file to upload or click **Browse** to select the required file.
2. Click **Upload** to transfer the file to the unit.

#### Delete decoder logo

Click **Delete decoder logo** to remove the decoder logo.

#### Maintenance log

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

## 5.21

## Licenses

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

**NOTICE!**

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

## 5.22

## System Overview

System Overview	
Hardware version	F1001341
Firmware version	35500400
Device type	VIP X1600 XFMD
IP address	160.10.32.43
Audio option	Yes
MAC address	00-07-5F-71-FA-9C
Major version number	4.00
Build number	35
Firmware version of switch	70

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

**NOTICE!**

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

## 5.23 Function Test

The VIP X1600 XF offers a variety of configuration options. You should therefore check that it is functioning correctly after installation and configuration.

The function test is the only way to ensure that the VIP X1600 XF operates as expected in the event of an alarm.

Your check should include the following functions:

- Can the VIP X1600 XF be called up remotely?
- Does the VIP X1600 XF transmit all the required data?
- Does the VIP X1600 XF respond to alarm events as required?
- Is it possible to control peripherals if necessary?





## 6 Operation

### 6.1 Connecting

A computer with Microsoft Internet Explorer (version 6.0 or higher) can establish a connection to a compatible video server and play back the live images received on the monitors connected to the VIP X1600 XFMD.

#### System Requirements

- Computer with Windows XP or Windows Vista operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 6.0 or higher)
- Screen resolution 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Sun JVM



#### NOTICE!

Also note the information in the **System Requirements** document on the product CD supplied with the VIP X1600 XF base. If necessary, you can install the required programs and controls from the product CD.

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

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

You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

---

#### Installing MPEG ActiveX

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

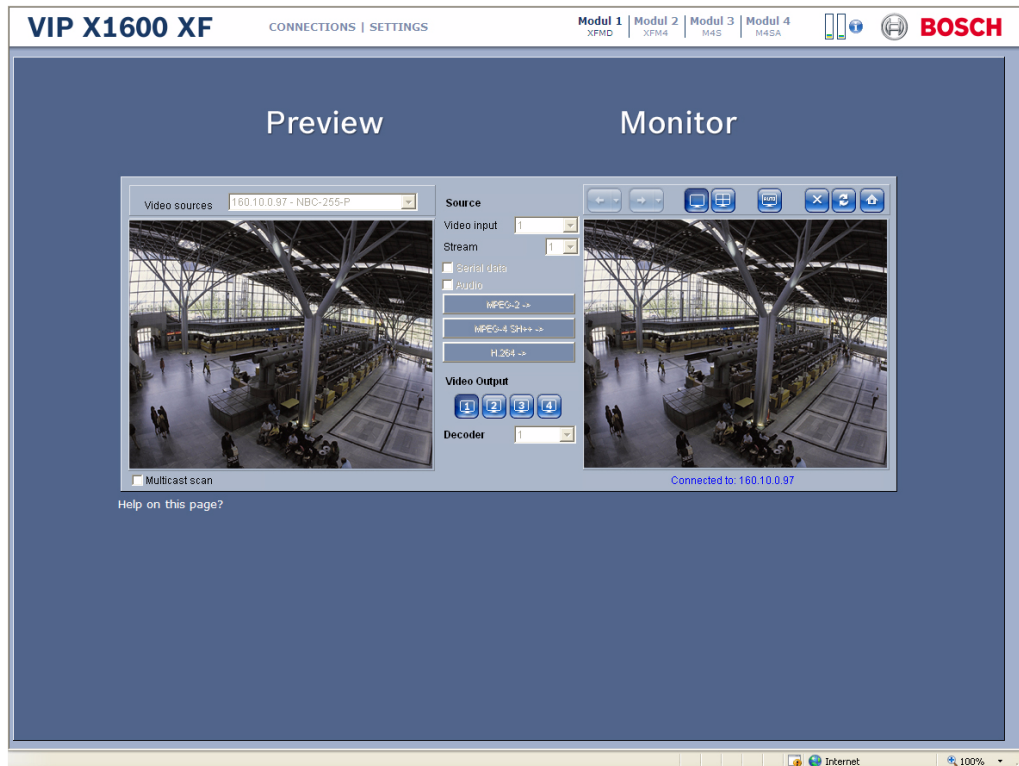
1. Insert the product CD into the computer's CD-ROM drive. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double-click **MPEGAx.exe**.
2. Follow the on-screen instructions.

### Establishing the Connection

At least the module in Slot 1 must be assigned a valid IP address and a compatible subnet mask to operate the VIP X1600 XF on your network.

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

1. Start the Web browser.
2. Enter the IP address of the VIP X1600 XFMD as the URL. The connection is established and after a short time you will see the **CONNECTIONS** page.



### Maximum Number of Connections

If you do not connect, the unit may have reached its maximum number of connections.

Depending on the unit and network configuration, each VIP X1600 XFMD can have up to 25 Web browser connections or up to 50 connections via VIDOS or Bosch Video Management System.

---

**Protected Module**

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

**NOTICE!**

The modules offer the option to limit the extent of access using various authorization levels (see *Section 5.4 Password, page 23*).

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

**Protected Network**

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

**Switching between the Modules**

If multiple modules have been installed in a VIP X1600 XF, you can easily switch between the modules in the same unit.

- ▶ In the upper section of the window, click one of the links **Module 1** to **Module 4** to switch to the corresponding module in the same VIP X1600 XF.

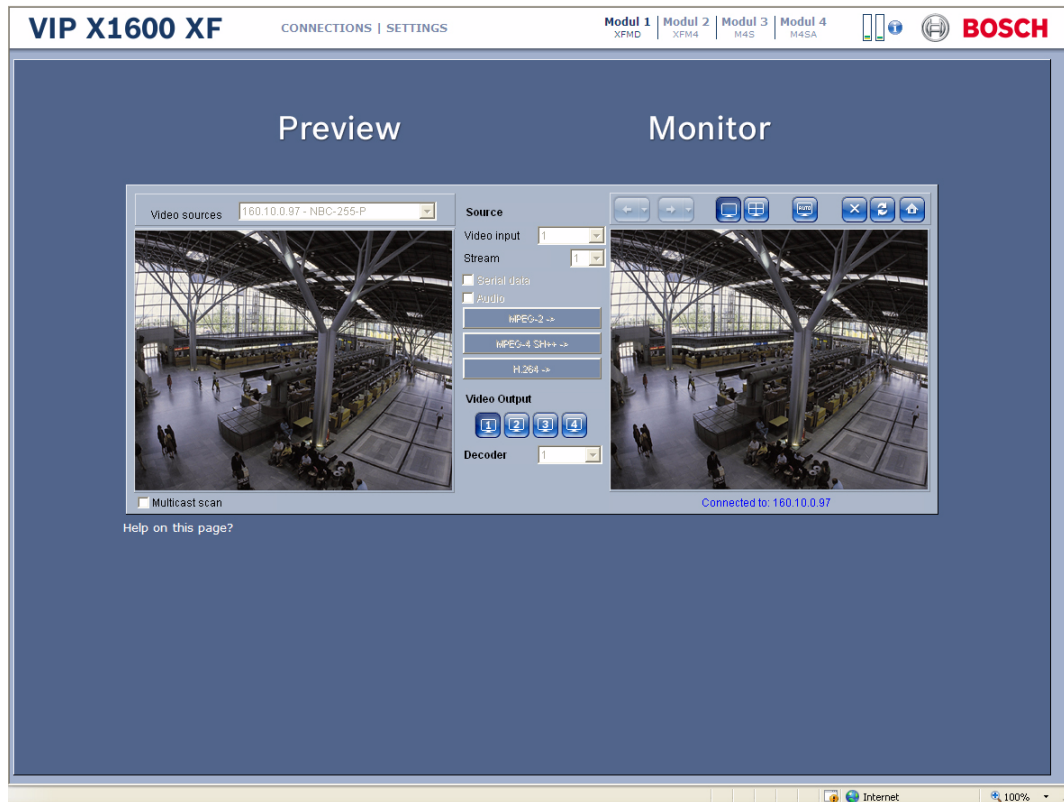
**NOTICE!**

A module that is installed in another base must be selected via its IP address.

---

## 6.2 The CONNECTIONS Page

Once the connection is established, the Web browser first displays the **CONNECTIONS** page and the VIP X1600 XFMD automatically browses the network for available senders.



### Preview

In this area you can select one of the video sources found in the network. You see a snapshot of the video image from the selected source. Besides the unit name, the snapshot provides an additional means of identifying the sender.

### Monitor

As soon as a connection is established, you see the video image from the connected sender. The image is refreshed around once per second.

## 6.3 Connections Between the Sender and Receiver

When you open the **CONNECTIONS** page, the VIP X1600 XFMD automatically scans the network for available senders. As soon as a sender is found in the network, the **Preview** area displays a JPEG snapshot from that sender. All senders found are listed in the **Video sources** list field.



### NOTICE!

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

---

### Establishing the Connection



### NOTICE!

If you do not connect, the unit may have reached its maximum number of connections. The maximum number of connections depends on the unit and network configuration. The **Serial data** and **Audio** checkboxes must be selected before the connection is made in order to activate data and audio transmission. The window displays a green loudspeaker icon in the bottom right corner of the video image the first time an audio connection is made. This icon indicates which sender is holding the active audio link.

---

1. Choose the desired sender from the **Video sources** list field.
2. If necessary, enter the password.
3. Click **OK**. If the password is correct, a JPEG snapshot from the selected video source appears in the **Preview** area.
4. If the sender is a multi-channel unit, for example a VideoJet X40, you can set the **Video input** for playback.
5. If the sender works with Dual Streaming, for example a VideoJet X10, you can select the **Stream** for playback.
6. Check the **Serial data** checkbox if you also want to transmit transparent data. Ensure that the sender and receiver are correctly configured for data transmission.
7. Check the **Audio** checkbox if you also want to transmit audio data. Ensure that the sender and receiver are correctly configured for audio transmission.
8. Click the appropriate checkbox again to deactivate the data or audio connection.
9. Click the **MPEG-2 ->**, **MPEG-4 SH++ ->** or **H.264 ->** button to start displaying the video images on the connected monitor. In the **Monitor** area you will see the video image from the connected sender. The image is refreshed around once per second.
10. Click one of the **Video Output** buttons to show the image on the respective monitor.

### Controlling Connections

You can control the selected connections and the monitor display using the buttons above the video image in the **Monitor** area. The buttons have the following functions:



Switch to the previous connection in the connection history.



Switch to the next connection in the connection history.



Single view display



Quad view



Activate and deactivate auto-connect (see *Section Auto-connect, page 31*).



Disconnect and end display of video images on the connected monitor.



Update display of video image.



Switch to the start-up connection (first connection after selecting VIP X1600 XFMD).

### Selecting Decoder for Quad View

When selecting Quad view, you can select the appropriate decoder for the display. This allows you to freely assign in which quadrant the relevant video image is to be displayed.

1. In the **Monitor** area, click the button for Quad view.
2. Click the desired quadrant. The selected quadrant is marked by a red frame.
3. Establish the connection and start the display on the monitor (see *Section Establishing the Connection, page 53*). The video images are displayed in the selected quadrant.

### Multicast scan

You can use the Multicast scan to search for video sources outside the subnet in which the VIP X1600 XF is located. Check the box in the Preview area to activate the **Multicast scan**.

## 6.4 Hardware Connections Between Video Servers

You can easily connect a VIP X1600 XFMD with a connected monitor as a receiver, together with a compatible sender (for example VideoJet X40) with a connected camera via an Ethernet network. In this way it is possible to cover long distances without the need for major installation or cabling work.



### NOTICE!

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

### Installation

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

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



### NOTICE!

Make sure that the units are configured for the network environment and that the correct IP address for the remote location to be contacted in the event of an alarm is set on the **Alarm Connections** configuration page (see *Section 5.10 Alarm Connections, page 29*).

### 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.

### Connecting on Alarm

With the appropriate configuration, a connection between a sender and a receiver is made automatically when an alarm is triggered (see *Section 5.10 Alarm Connections, page 29*). After a short time the live video image from the sender appears on the selected monitor. This option can also be used to connect a sender and a compatible receiver using a switch connected to the alarm input. You do not need a computer to make the connection in this case.

### Connecting with a Terminal Program

Various requirements must be met in order to operate with a terminal program (see *Section 8.6 Communication with Terminal Program, page 63*).

1. Start the terminal program and enter the command **1** in the main menu to switch to the **IP** menu.
2. 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.
3. Enter the command **0** to return to the main menu and then enter the command **4** to switch to the **Rcp+** menu.
4. In the **Rcp+** menu, enter the command **5** to activate the automatic connection.

### Closing the Connection with a Terminal Program

1. Start the terminal program and enter the command **4** in the main menu to switch to the **Rcp+** menu.
2. In the **Rcp+** menu, enter the command **5** to deactivate the automatic connection.

## 6.5 Operation with Management Software

The use of management software such as VIDOS is recommended for operating larger systems with multiple senders and receivers.

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

Many options are provided for operation and configuration when using a VIP X1600 XF with VIDOS. Please refer to the software documentation for more details.

Another program that supports the VIP X1600 XF is Bosch Video Management System. Bosch Video Management System is an IP video security solution that enables the seamless management of digital video, audio and data over any IP network. It was developed for use with Bosch CCTV products as one component of an extensive video security management system. It allows you to integrate your existing components into a simple-to-control system or into the entire Bosch range, benefiting from a complete security solution based on the latest technology and years of experience.



## 7 Maintenance and Upgrades

### 7.1 Testing the Network Connection

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

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

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

- The VIP X1600 XF is not correctly connected to the network. Check the cable connections in this case.
- The module is not correctly integrated into the network. Check the IP address, subnet mask and gateway address.

### 7.2 Unit Reset

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



#### CAUTION!

All configured settings will be discarded during a reset.

If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.20 Maintenance, page 44*).

---



#### NOTICE!

After a reset, the module can only be addressed via the factory default IP address. The IP address can be changed as described in the **Installation** chapter (see *Section 4.4 Setup Using the Configuration Manager, page 17*).

---

1. If necessary, back up the current configuration using the **Download** button on the **Maintenance** configuration page (see *Section 5.20 Maintenance, page 44*).
2. Using a pointed object, press the Factory Reset button located below the orange terminal block until the module's LED on the front panel of the VIP X1600 XF flashes red. All module settings will revert to their defaults.
3. Change the IP address of the module if necessary.
4. Configure the module to meet your requirements.

## 7.3 Repairs

**CAUTION!**

Do not change any components in the module or the VIP X1600 XF base. The unit does not contain any user-serviceable parts.

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

## 7.4 Transfer and Disposal

A VIP X1600 XF, the VIP X1600 XF base or a module should only be passed on together with this Installation and Operating Manual.

Your Bosch product is designed and manufactured with high-quality materials and components which can be recycled and reused.



This symbol means that electrical and electronic equipment, at their end-of-life, should be disposed of separately from your household waste.

In the European Union, there are separate collection systems for used electrical and electronic products. Please dispose of this equipment at your local community waste collection/recycling center.

## 8 Appendix

### 8.1 Troubleshooting

If you are unable to resolve a malfunction, please contact your supplier or systems integrator, or go directly to Bosch Security Systems Customer Service.

You can view a range of information about your unit version on the **System Overview** page (see *Section 5.22 System Overview, page 46*). Make a note of this information before contacting Customer Service. You can download an internal maintenance log from the unit on the **Maintenance** page if you wish to send it to Customer Service by e-mail (see *Section Maintenance log, page 45*).

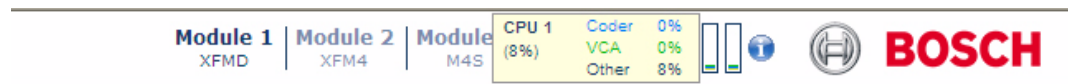
The following table is intended to help you identify the causes of malfunctions and correct them where possible.

Malfunction	Possible causes	Recommended solution
No connection between the unit and terminal program.	Incorrect cable connections.	Check all cables, plugs, contacts, terminals and connections.
	The computer's serial interface is not connected.	Check the other serial interface.
	Interface parameters do not match.	If necessary select a different interface and make sure that the computer's interface parameters match those of the module. 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 on the monitor.	Monitor error.	Connect local camera or other video source to the monitor and check the monitor function.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
No connection established, no image transmission.	The module'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 <b>ping</b> .
	The maximum number of connections has been reached.	Wait until there is a free connection and then call the sender again.

<b>Malfunction</b>	<b>Possible causes</b>	<b>Recommended solution</b>
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 <b>Audio</b> configuration page.
	The audio voice connection is already in use by another receiver.	Wait until the connection is free and then call the sender again.
The module does not report an alarm.	Alarm source is not selected.	Select the alarm source on the <b>Alarm Inputs</b> configuration page.
	No alarm response specified.	Specify the desired alarm response on the <b>Alarm Connections</b> 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 module is not operational after a firmware upload.	Power failure during programming by firmware file.	Have the module checked by Customer Service and replace if necessary.
	Incorrect firmware file.	Enter the IP address of the module followed by <b>/main.htm</b> in your Web browser and repeat the upload.
Placeholders with a red cross are displayed instead of the ActiveX components.	Sun JVM is not installed on the computer or is not enabled.	Install Sun JVM from the product CD.
Web browser contains empty fields.	Active proxy server in network.	Create a rule in the local computer's proxy settings to exclude local IP addresses.
If a sender is connected to the receiver, the first connection remains.	Auto-connect configured.	Deactivate auto-connect.

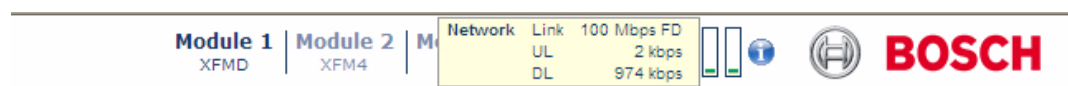
## 8.2 Processor Load

If the VIP X1600 XFMD decoder module is accessed via the Web browser, you will see the processor load indicators in the top right of the window next to the manufacturer's logo.



Moving the mouse cursor over the graphic indicators displays the status of the processor together with the numerical values. This information may help you with troubleshooting or fine tuning the unit.

## 8.3 Network Connection



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

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

## 8.4 Serial Interface

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

The serial interface supports the RS-232/RS-422/RS-485 transmission standards. The mode used depends on the current configuration (see *Section 5.16 COM1, page 38*). Connection is via the terminal block.

## 8.5 Terminal Block

The terminal block has several contacts for:

- 1 alarm input
- 1 relay output
- Serial data transmission

### Pin Assignment

The pin assignment of the serial interface depends on the interface mode used (see *Section 5.16 COM1, page 38*).

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

Contact	Function
IN	Input alarm
GND	Ground
REL	Relay output
REL	Relay output

Connect the **IN** alarm input to the **GND** ground contact when connecting the alarm signal.

## 8.6 Communication with Terminal Program

### Data Terminal

If a module cannot be found in the network or the connection to the network is interrupted, you can connect a data terminal to the VIP X1600 XF for initial setup and setting of important parameters. The data terminal consists of a computer with a terminal program.

You require a serial transmission cable with a 9-pin Sub-D plug to connect to the computer and open ends for connection to the terminal block of the module (see *Section Pin Assignment, page 62*).

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



### NOTICE!

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

---

1. Disconnect the VIP X1600 XF from the Ethernet network before working with the terminal program.
2. Connect the serial interface of the module using any available serial interface on the computer.

### Configuring the Terminal

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

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

### Command Inputs

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

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

### Assigning an IP Address

To use a module in your network you must first assign it an IP address that is valid for your network.

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

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

```

-----
|  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
-----

```

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



#### NOTICE!

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

#### Reboot

Briefly interrupt the power supply to the VIP X1600 XF for a reboot (disconnect the power supply unit from the mains supply and switch on again after a few seconds).

#### Additional Parameters

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



## 8.7 Copyrights

The firmware 4.0 uses the fonts "Adobe-Helvetica-Bold-R-Normal--24-240-75-75-P-138-ISO10646-1" and "Adobe-Helvetica-Bold-R-Normal--12-120-75-75-P-70-ISO10646-1" under the following copyright:

Copyright 1984-1989, 1994 Adobe Systems Incorporated.

Copyright 1988, 1994 Digital Equipment Corporation.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both those copyright notices and this permission notice appear in supporting documentation, and that the names of Adobe Systems and Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

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



## 9 Specifications

### 9.1 VIP X1600 XFMD Decoder Module

Operating voltage	Supply via VIP X1600 XF base housing
Power consumption	Max. 12 W
Data interfaces	1 × RS-232/RS-422/RS-485, bidirectional, push-in terminal
Alarm input	1 × push-in terminal (non-isolated closing contact), maximum activation resistance 10 Ohm
Relay output	1 × push-in terminal, 30 V <sub>p-p</sub> , 2 A (SELV), 2 contacts
Video outputs	4 × BNC socket 0.7 to 1.2 V <sub>p-p</sub> , 75 Ohm, PAL/NTSC
Audio input	1 × 3.5 mm / 1/8 in. stereo socket, 5.5 V <sub>p-p</sub> max., impedance 9 kOhm typ.
Audio output	1 × 3.5 mm / 1/8 in. stereo socket, 5.5 V <sub>p-p</sub> max., impedance 16 Ohm min.
Thermal value	41 BTU/h
Operating conditions	Temperature: 0 to +50 °C / +32 to +122 °F, relative humidity: 20 to 80%, non-condensing
Approvals	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
Weight	approx. 120 g / 0.27 lb

### 9.2 Protocols/Standards

Video standards	PAL, NTSC
Video coding protocols	H.264 BP+, MPEG-4, MPEG-2
Video data rate	9.6 kbps to 6 Mbps per channel
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	25/30 ips max.
Network protocols	RTP, Telnet, UDP, TCP, IP, HTTP, HTTPS, DHCP, IGMP V2, IGMP V3, ICMP, ARP, SNMP (V1/V2c/V3 MIB-II), 802.1x
Audio coding protocol	G.711, 300 Hz to 3.4 kHz
Audio sampling rate	8 kHz
Audio data rate	80 kbps



# 10 Glossary

## Symbols

---

10/100/1000 Base-T IEEE-802.3 specification for 10, 100 or 1000 Mbps Ethernet

---

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

### A

---

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

### B

---

Baud Unit of measurement for the speed of data transmission

---

bps Bits per second, the actual data rate

---

BVIP Bosch Video over IP unit

### C

---

CABAC Context-based Adaptive Binary Arithmetic Coding; an effective way to compress binary data without loss. In the video standard MPEG-4/Part10 (H.264/AVC), CABAC is characterized by high picture quality, a high compression rate and high computing requirements.

---

CF CompactFlash; interface standard, for digital storage media amongst other things. Used in computers in the form of CF cards, digital cameras and Personal Digital Assistants (PDA).

---

CIF Common Intermediate Format, video format with 352 × 288/240 pixels

### D

---

DHCP Dynamic Host Configuration Protocol: uses an appropriate server to enable dynamic assignment of an IP address and other configuration parameters to computers on a network (Internet or LAN)

---

DNS Domain Name System, mainly used for converting domain names to IP addresses

---

DynDNS DNS hosting service that works according to RFC 2845 and stores the IP addresses of its clients in a database, ready for use

### F

---

FTP File Transfer Protocol

---

Full duplex Simultaneous data transmission in both directions (sending and receiving)

**G**

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

**H**

HTTP	Hypertext Transfer Protocol: protocol for transmitting data over a network
HTTPS	Hypertext Transfer Protocol Secure: encrypts and authenticates communication between Web server and browser

**I**

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

**J**

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

**K**

kbps	Kilobits per second, the actual data rate
------	---

**L**

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

---

## M

---

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

---

## N

---

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

---

## O

---

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

---

## P

---

Parameters	Values used for configuration
------------	-------------------------------

---

## Q

---

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

---

## R

---

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

---

**S**

---

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

---

**T**

---

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

---

**U**

---

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

---

**W**

---

WAN	<i>See</i> Wide Area Network
Wide Area Network	A long distance link used to extend or connect remotely located local area networks

---



# 11

## Index

### A

Activation key 46  
Actuator 16  
Alarm 12  
Alarm e-mail 33  
Alarm input 16  
Alarm sources 36  
Audio connection 12  
Audio stream on alarm 31  
Audio transmission 28  
Auto-connect 31

### B

Baud rate 38

### C

Changes 22  
Checking network 57  
Closing contact 16  
COM1 38  
Configuration 19, 45  
Configuration download 45  
Configuration mode 22  
Connect on alarm 29  
Connecting 19, 55  
Conventions 5

### D

Data bits 38  
Data interface 15  
Data terminal 63  
Date 24  
Date format 24  
Daylight saving time 25  
Device ID 23  
Device name 23, 27  
Domkamera 15  
DynDNS 41

### E

Echo 63  
Electromagnetic compatibility 6  
E-mail 33  
Encryption protocol 40  
EPROM 44  
Establishing the connection 50

### F

Firewall 30, 40  
Firmware upload 44  
Function test 47

### G

Gateway 40  
General password 30

### H

HTTP port 40  
HTTPS port 40

### I

Identification 6, 23, 27  
IEEE 802.1x 43  
Installation 7, 13  
Installation conditions 13

Interface 62  
Interface mode 38  
Internal clock 24  
IP address 40, 64

### L

Language 26  
Licenses 46  
Live video images 19, 49  
Low Voltage Directive 6

### M

Main functions 11  
Maintenance 7  
Manufacturer logo 26  
Monitore 15  
MPEG ActiveX 19, 49  
MTU value 40, 41  
Multicast connection 40  
Multicast function 10

### N

Navigation 22  
Network 39, 42  
Network connection 61  
Number of connections 20, 50

### O

Operation 7

### P

Parameters 18, 64  
Parity check 38  
Password 21, 23, 24, 51  
Pin assignment 62  
Playback button 54  
Port 40  
Processor load 61  
Processor load indicator 61  
Product name 26  
Protocol 38

### Q

Quad view 54

### R

RADIUS 43  
Reboot 18, 64  
Receiver password 30  
Regulations 5  
Relay 12, 16  
Relay output 36  
Relay outputs 16  
Repair 7, 58  
Reset 57

### S

Scope of delivery 9  
Screen resolution 9, 19, 49  
Sender 10  
Serial interface 12  
Serial number 6  
Serial port function 38  
Signal source 16  
SMS 34

- SNMP 43
- SNTP server 25
- SSL certificate 45
- SSL encryption 31
- Stop bits 38
- Subnet mask 40
- Summer time 25
- Symbols 5
- Synchronize 24
- System requirements 9, 19, 49

**T**

- TCP 30, 40
- Terminal 38
- Test 47
- Time 24
- Time server 25
- Time server IP address 25
- Time server protocol 25
- Time signal 25
- Time zone 24
- TLS 40
- Transmission interruptions 28
- Transmission parameters 63
- Transmission protocol 30, 40
- Transmission rate 38
- Transmission standards 15, 62
- Transparent 38
- Traps 43
- Trigger relay 37

**U**

- UDP 30, 40
- Unit date 24
- Unit identification 23, 27
- Unit name 23, 27
- Unit reset 57
- Unit time 24
- URL 20, 50
- User name 24

**V**

- Verbindung herstellen 20



**Bosch Security Systems**

Robert-Koch-Straße 100

85521 Ottobrunn

Germany

Telefon 089 6290-0

Fax 089 6290-1020

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems, 2009