



MIC Series IP Power Supply

MIC IP PSU



BOSCH

en User Manual

Table of Contents

1	Safety	6
1.1	About this Manual	6
1.2	Conventions in this Manual	6
1.3	Legal Information	6
1.4	Important safety instructions/notices	7
2	Product Description	10
2.1	Overview of Functions	10
2.2	Summary of Functions	11
3	Installation	12
3.1	Parts List	12
3.1.1	User-Supplied Parts	12
3.1.2	User-Supplied Tools	12
3.2	Dimensions and Layout of MIC IP Power Supplies	13
3.3	MIC Power Supply Units (PSUs) for Non-IR MIC Cameras	14
3.4	MIC Power Supply Units (PSUs) for IR MIC Cameras	15
3.5	Earth Link on the PCB	15
3.6	Fuse Ratings	16
3.7	Installation Instructions	17
3.8	Commissioning the Camera with Heater Option Fitted	25
3.9	Simultaneous IP and Analog Video/Control ("Hybrid" Operation)	26
3.10	Assign an IP Address	26
3.11	Hardware connections between video servers	27
4	Configuration using a Web browser	28
4.1	Connecting	28
4.1.1	System Requirements	28
4.1.2	Additional Operational Requirements	28
4.1.3	Installing MPEG ActiveX	28
4.1.4	Establishing the Connection	28
4.2	Configuration menu	30
4.3	Basic Mode: Device Access	31
4.4	Basic Mode: Date/Time	32
4.5	Basic Mode: Network	33
4.6	Basic Mode: Encoder	34
4.7	Basic Mode: System Overview	35
4.8	Advanced Mode: General	36
4.9	Identification	36
4.10	Password	37
4.11	Date/Time	38
4.12	Display Stamping	39
4.13	Advanced Mode: Web Interface	40
4.14	Appearance	40
4.15	LIVEPAGE Functions	41
4.16	Logging	42

4.17	Video Input	43
4.18	Advanced Mode: Encoder	43
4.19	Picture Settings	43
4.20	Encoder Profile	44
4.21	Encoder Streams	47
4.22	Pixel Counter	48
4.23	Advanced Mode: Camera	48
4.24	Camera Options	48
4.25	Lens	50
4.26	PTZ	52
4.27	Display	52
4.28	Alarm	54
4.28.1	Input Options	54
4.28.2	Output Options	54
4.28.3	Alarm Rules	55
4.28.4	Alarm States	56
4.29	Miscellaneous	56
4.30	Logs	57
4.31	Advanced Mode: Recording	57
4.32	Storage Management	57
4.33	Recording Profiles	60
4.34	Retention Time	62
4.35	Recording Scheduler	63
4.36	Recording Status	64
4.37	Advanced Mode: Alarm	65
4.38	Alarm Connections	65
4.39	VCA	67
4.40	Alarm E-Mail	71
4.41	Alarm Task Editor	72
4.42	Advanced Mode: Network	73
4.43	Network Access	73
4.44	Advanced	75
4.45	Multicast	77
4.46	FTP Posting	79
4.47	IPv4 Filter	80
4.48	Encryption	80
4.49	Advanced Mode: Service	81
4.50	Maintenance	81
4.51	Licenses	83
4.52	System Overview	83
4.53	Function test	84
5	Operation	85
5.1	Function test	85
5.2	The LIVEPAGE	85
5.3	Saving snapshots	87
5.4	Recording video sequences	87
5.5	Running recording program	87
5.6	Processor load	87

5.7	Network connection	88
5.8	The RECORDINGS page	88
5.9	Operation using software decoders	90
<hr/>		
6	Maintenance and upgrades	91
6.1	Testing the network connection	91
6.2	Unit reset	91
6.3	Troubleshooting	91
6.4	General malfunctions	92
6.5	Fiber Optic Module	93
6.6	Malfunctions with iSCSI connections	94
6.7	LEDs	94
6.8	Processor load	94
6.9	Network connection	94
6.10	Terminal block	95
6.11	Communication with terminal program	95
6.12	Transfer and disposal	97
6.13	Repairs	97
6.14	Copyrights	97

1 Safety

1.1 About this Manual

This manual has been compiled with great care and the information it contains has been thoroughly verified. The text was complete and correct at the time of printing. Because of the ongoing development of products, the content of the manual may change without notice. Bosch Security Systems accepts no liability for damage resulting directly or indirectly from faults, incompleteness, or discrepancies between the manual and the product described.

1.2 Conventions in this Manual

The following symbols and notations are used to draw attention to special situations:



DANGER!

This symbol indicates an imminently hazardous situation such as “Dangerous Voltage” inside the product. If not avoided, this will result in an electrical shock, serious bodily injury, or death.



WARNING!

Indicates a potentially hazardous situation. If not avoided, this could result in serious bodily injury or death.



CAUTION!

Medium Risk

Indicates a potentially hazardous situation. If not avoided, this may result in minor or moderate injury. Alerts the user to important instructions accompanying the unit.



CAUTION!

Indicates a potentially hazardous situation. If not avoided, this may result in property damage or risk of damage to the unit.



NOTICE!

This symbol indicates information or a company policy that relates directly or indirectly to the safety of personnel or protection of property.

1.3 Legal Information

Copyright - This manual is the intellectual property of Bosch Security Systems, Inc. and is protected by copyright. All rights reserved.

Trademarks - All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

Notice of Regulatory Compliance

This product complies with the following EC directives:

- EMC Directive (89/336/EC as amended)
- LV Directive (73/23/EC)
- RoHS (Restriction of Hazardous Substances) 2002/95/EC, CIPRA-B and CTIC

1.4 Important safety instructions/notices

Read, follow, and retain for future reference all of the following safety instructions. Heed all warnings on the unit and in the operating instructions before operating the unit.

Installation - Do not install the unit:

- Near any heat sources such as radiators, heaters, stoves, or other equipment (including amplifiers) that produce heat
- Near overhead power lines or power circuits, or where it may contact such power lines or circuits
- In a built-in installation or rack without proper ventilation or adhering to the manufacturer's instructions.

The equipment must not exceed its maximum operating temperature requirements.

Mount the unit properly in a rack to prevent a hazardous condition due to uneven mechanical loading.

Power - Units have power supplied to the unit whenever the power cord is inserted into the power source. The power cord is the main power disconnect device for switching off the voltage to the unit. Disconnect the power before moving the unit or when leaving the unit unattended and unused for long periods.

Protect the power supply cord and plug from foot traffic, from being pinched by items placed on or against them at electrical outlets and at its exit from the unit. For units operating at 230 VAC, 50 Hz, the power cord must comply with the latest versions of *IEC 60227*. For units operating at 120 VAC, 60 Hz, the power cord must comply with the latest versions of *UL 62* and *CSA 22.2 No.49*.

Servicing - Do not attempt to service this unit yourself. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel. If any of the following conditions occur, unplug the unit from the main AC power source and refer servicing to qualified service personnel:

- the power supply cord or plug is damaged;
- exposure to moisture, water, and/or inclement weather (rain, snow, etc.);
- liquid has been spilled in or on the equipment;
- an object has been pushed or has fallen into the unit;
- the unit has been dropped or the unit cabinet is damaged;
- the unit exhibits a distinct change in performance;
- the unit does not operate normally when the user correctly follows the operating instructions.

Ensure that service personnel use replacement parts specified by the manufacturer, or that have the same characteristics as the original parts. Unauthorized substitutions may cause fire, electrical shock, or other hazards. Service personnel should perform safety checks after completion of service or repairs to the unit to ensure proper operating condition.

Modifications - Any change or modification of the equipment, not expressly approved by Bosch, could void the warranty or, in the case of an authorization agreement, authority to operate the equipment.

Electrostatic-sensitive device - Use proper CMOS/MOS-FET handling precautions to avoid electrostatic discharge. Wear required grounded wrist straps and observe proper ESD safety precautions when handling electrostatic-sensitive printed circuit boards.

Fuse rating - For security protection of the device, the branch circuit protection is required. This must be in accordance with NEC800 (CEC Section 60) or other local codes.

Coax grounding:

- Ground the cable system if connecting an outside cable system to the unit.

- Connect outdoor equipment to the unit's inputs only after connecting the grounding plug to a grounded outlet, or its ground terminal is properly connected to a ground source.
- Disconnect the unit's input connectors from outdoor equipment before disconnecting the grounding plug or grounding terminal.
- Follow proper safety precautions such as grounding for any outdoor device connected to this unit.

U.S.A. models only - Section 810 of the *National Electrical Code, ANSI/NFPA No.70*, provides information regarding proper grounding of the mount and supporting structure, grounding of the coax to a discharge unit, size of grounding conductors, location of discharge unit, connection to grounding electrodes, and requirements for the grounding electrode.

Outdoor signals - The installation for outdoor signals, especially regarding clearance from power and lightning conductors and transient protection, must be in accordance with *NEC725* and *NEC800 (CEC Rule 16-224 and CEC Section 60)*.

Power resupply - If the unit is forced to power down due to exceeding the specified operating temperatures, disconnect the power cord, wait for at least 30 seconds, and then reconnect the power cord.



CAUTION!

Connecting System ground to Safety ground may result in ground loops that can disrupt the CCTV system.



NOTICE!

This is a **class B** product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC & ICES Information

(U.S.A. and Canadian Models Only)

This equipment has been tested and found to comply with the limits for a **Class B** digital device, pursuant to *part 15* of the *FCC Rules*. These limits are designed to provide reasonable protection against harmful interference in a **residential installation**. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- reorient or relocate the receiving antenna;
- increase the separation between the equipment and receiver;
- connect the equipment into an outlet on a circuit different from that to which the receiver is connected;
- consult the dealer or an experienced radio/TV technician for help.

Intentional or unintentional modifications, not expressly approved by the party responsible for compliance, shall not be made. Any such modifications could void the user's authority to operate the equipment. If necessary, the user should consult the dealer or an experienced radio/television technician for corrective action.

The user may find the following booklet, prepared by the Federal Communications Commission, helpful: *How to Identify and Resolve Radio-TV Interference Problems*. This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

INFORMATIONS FCC ET ICES

(modèles utilisés aux États-Unis et au Canada uniquement)

Suite à différents tests, cet appareil s'est révélé conforme aux exigences imposées aux appareils numériques de **classe B**, en vertu de la *section 15 du règlement* de la *Commission fédérale des communications des États-Unis (FCC)*, et en vertu de la norme *ICES-003 d'Industrie Canada*. Ces exigences visent à fournir une protection raisonnable contre les interférences nuisibles lorsque l'appareil est utilisé dans le cadre d'une **installation résidentielle**. Cet appareil génère, utilise et émet de l'énergie de radiofréquences et peut, en cas d'installation ou d'utilisation non conforme aux instructions, engendrer des interférences nuisibles au niveau des radiocommunications. Toutefois, rien ne garantit l'absence d'interférences dans une installation particulière. Il est possible de déterminer la production d'interférences en mettant l'appareil successivement hors et sous tension, tout en contrôlant la réception radio ou télévision. L'utilisateur peut parvenir à éliminer les interférences éventuelles en prenant une ou plusieurs des mesures suivantes:

- Modifier l'orientation ou l'emplacement de l'antenne réceptrice;
- Éloigner l'appareil du récepteur;
- Brancher l'appareil sur une prise située sur un circuit différent de celui du récepteur;
- Consulter le revendeur ou un technicien qualifié en radio/télévision pour obtenir de l'aide.

Toute modification apportée au produit, non expressément approuvée par la partie responsable de l'appareil, est strictement interdite. Une telle modification est susceptible d'entraîner la révocation du droit d'utilisation de l'appareil.

La brochure suivante, publiée par la Commission fédérale des communications (FCC), peut s'avérer utile : *How to Identify and Resolve Radio-TV Interference Problems (Comment identifier et résoudre les problèmes d'interférences de radio et de télévision)*. Cette brochure est disponible auprès du U.S. Government Printing Office, Washington, DC 20402, États-Unis, sous la référence n° 004-000-00345-4.

Disclaimer

Underwriter Laboratories Inc. ("UL") has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested fire, shock and/or casualty hazards as outlined in UL's *Standard(s) for Safety for Closed Circuit Television Equipment, UL 2044* and in *Standard(s) for Safety for Information Technology Equipment, UL 60950-1*. UL Certification does not cover the performance or reliability of the security or signaling aspects of this product.

UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY SECURITY OR SIGNALING RELATED FUNCTIONS OF THIS PRODUCT.

2 Product Description

2.1 Overview of Functions

Network video server

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

Receiver

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

Video encoding

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

Audio encoding

The encoder uses the G.711 and L16 audio compression standards. G.711 is the default setting both for live transmission and recording. When configuring with a Web browser, you can select L16 for recording. Using video management systems, L16 is also available for live audio.

Dual Streaming

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

Multicast

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

Encryption

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

Remote control

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

Video content analysis and tamper detection

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

Snapshots

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

Recordings

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

Backup

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

2.2**Summary of Functions**

The encoder provides the following main functions:

- Video and data transmission over IP data networks
- Dual Streaming function for the encoder for simultaneous encoding with two individually definable profiles
- Multicast function for simultaneous image transmission to multiple receivers
- One analog BNC composite video input (PAL/NTSC, 75 ohm)
- Video encoding to international standard H.264
- Integrated Ethernet port (10/100 Base-T)
- SD slot that supports local storage on SD cards (user-supplied) [ideal for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions]
- Transparent, bidirectional data channel via RS-232/RS-422/RS-485 serial interface
- Configuration and remote control of all internal functions via TCP/IP, also secured via HTTPS
- Password protection to prevent unauthorized connection or configuration changes
- Extensive, flexible storage options
- Support for two alarm inputs and two relay outputs
- Built-in video sensor for motion and tamper alarms
- Event-controlled automatic connection
- Convenient maintenance via uploads
- Flexible encryption of control and data channels
- Authentication according to international standard 802.1x
- Bidirectional audio (mono) for line connections; transmitted in sync with the video signal
- Audio encoding to international standards G.711 or L16

3 Installation

Each MIC power supply unit (PSU) provides all of the connections needed for power, video, and telemetry for a single MIC camera. Each MIC PSU has CE and FCC approval and has an aluminum enclosure that is weather-resistant (rated IP67). Features include:

- A built-in encoder for video and data transmission over an IP (standard 10/100 Base-T) network
- A provision for driving various optional interface cards mounted internally to the MIC power supply enclosure (for example, an 8-input alarm card (MIC-ALM))
- A provision for a signal interface card (MIC-BP4) to connect telemetry to Bosch Biphas equipment
- Screw termination of all cables (composite, telemetry, and ancillary) into and out of the enclosure
- Earth isolation and termination within the unit to control video earthing correctly and thus prevent earth loops

The table below summarizes the MIC power supplies and their specifications:

MIC PSU	Voltage	Hz	Power	Output	Applicable MIC Cameras
IP Power Supply Units (Non-IR)					
MIC-IP-PS-115	115 VAC	50/60 Hz	40 VA	18 VAC	MIC550, MIC612
MIC-IP-PS-230	230 VAC	50/60 Hz	40 VA	18 VAC	
MIC-IP-PS-24	24 VAC	50/60 Hz	40 VA	18 VAC	
Dimensions (H x W x D)	330 x 250 x 90.75 mm 13 x 9.8 x 3.6 in.)				
Weight	7.21 kg (15.9 lb)				
IP IR Power Supply Units					
MIC-IPIR-PS-115	115 VAC	50/60 Hz	60 VA	18 VAC	MIC550IR
MIC-IPIR-PS-230	230 VAC	50/60 Hz	60 VA	18 VAC	
MIC-IPIR-PS-24	24 VAC	50/60 Hz	60 VA	18 VAC	
Dimensions (H x W x D)	330 x 250 x 90.75 mm (13 x 9.8 x 3.6 in.)				
Weight	7.3 kg (16.09 lb)				

3.1 Parts List

Each MIC IP PSU ships with the following parts:

- Two (2) M12 cable glands for telemetry and ancillary equipment
- One (1) M16 gland for connection of RJ45 or Fiber cable
- One (1) 1/2 in. NPT cable gland for connection of the shielded composite cable to the MIC camera
- One (1) 1/2 in. NPT cable gland for the power cable connection
- One (1) 1/2 in. NPT and one (1) M12 blanking plug

3.1.1 User-Supplied Parts

Installers must provide the following parts to complete installation of a MIC PSU:

- Power cable in the appropriate length
- Four (4) M6 stainless steel screws and washers
- Metal conduit suitable for containing power cables external to the PSU enclosure
- Ethernet cable (terminated as needed)

3.1.2 User-Supplied Tools

- Ring crimp tool (Davico type DHCR15 or equivalent)
- Phillips-head screwdriver

3.2 Dimensions and Layout of MIC IP Power Supplies

The figures below display the dimensions and the layout of the enclosures of the MIC IP PSUs.

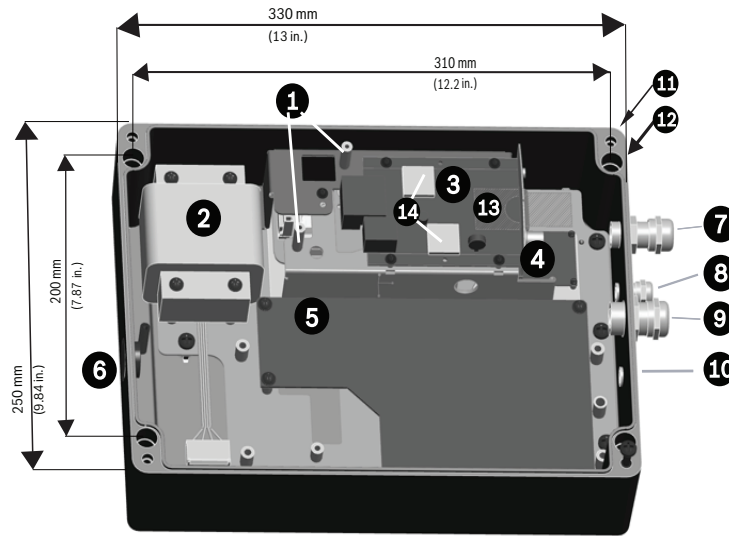


Figure 3.1 Layout of MIC IP PSU (Model numbers: MIC-IP-PS-115, MIC-IP-PS-230, MIC-IP-PS-24)

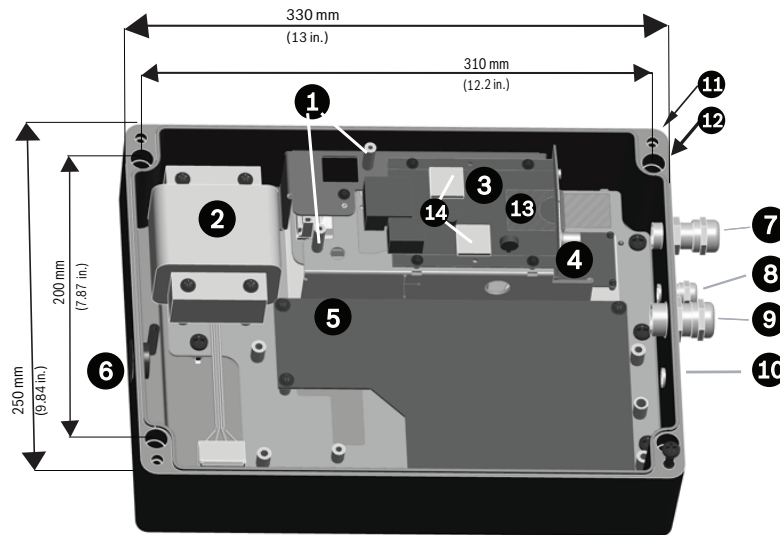


Figure 3.2 Layout of MIC IP IR PSU (Model numbers: MIC-IPIR-PS-115, MIC-IPIR-PS-230, MIC-IPIR-PS-24)

Number	Description
1	Two (2) metal stand-offs for fiber optic module (module sold separately)
2	Transformer
3	Encoder
4	Power board for encoder
5	Main PCB (Different configuration for IR and non-IR models)
6	Blanking plug over hole in enclosure for power cable
7	Cable gland for RJ45 / Fiber cable
8	Cable gland for optional washer drive
9	Cable gland for composite cable (analog connection)
10	For non-thermal cameras: Blanking plug over hole for optional cable gland for alarms For thermal cameras: Blanking plug over hole for output for optional switch video
11	Hole for lid screw
12	Hole for mounting screw
13	Slot for SD card (card is user-supplied)
14	Thermal pads between encoder and inside of lid of enclosure

3.3 MIC Power Supply Units (PSUs) for Non-IR MIC Cameras

The figure below displays the layout of the PCB in the MIC PSUs for non-IR cameras, with call-out numbers to the side of or below the connection/terminal ID or the terminal, and 'on' the fuses. The table below the figure identifies the connections.

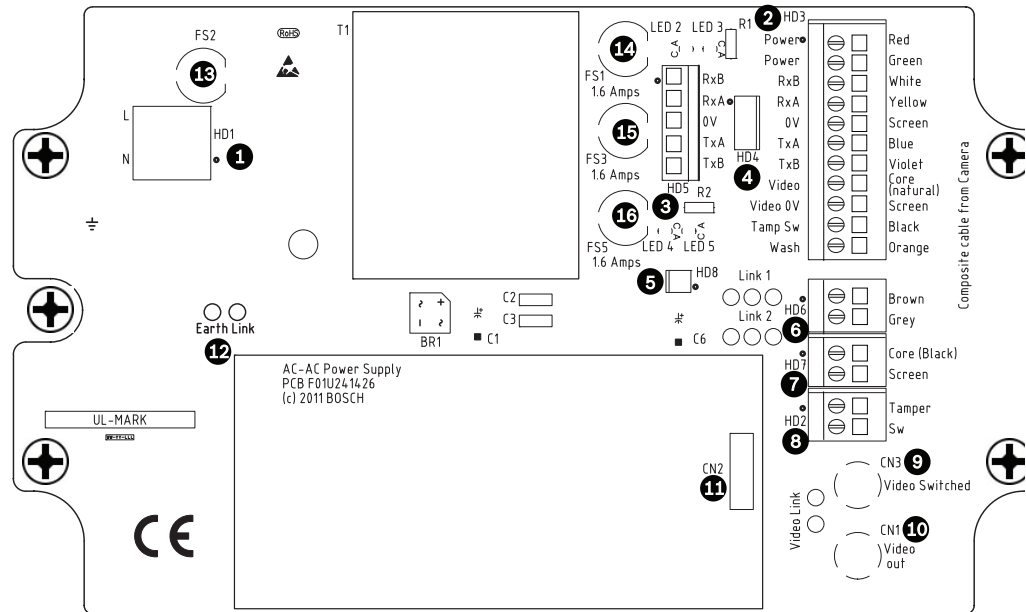


Figure 3.3 Layout of PCB in enclosure of PSU for non-IR MIC cameras

Number	Connection / Terminal ID on PCB	Description/Function of Connection / Terminal	Type of Connection / Terminal
1	HD1	AC Power input	Screw terminal
2	HD3	Shielded composite cable (analog connections to camera)	Screw terminal
3	HD5	RS-485 control	Screw terminal
4	HD4	USB to RS-485 converter	Molex connector
5	HD8	**NOT USED**	Molex connector
6	HD6	[Optional] Auxiliary, heater	Screw terminal
7	HD7	Video (composite cable)	Screw terminal
8	HD2	Tamper switch	Screw terminal
9	CN3 (Video Switched)	Coax connection	BNC socket
10	CN1 (Video Out)	Coax connection	BNC socket
11	CN2	Auxiliary card header	Plug in
12	Earth Link	Earth Link	--
13	FS2	Fuse 2 - Primary protection	--
14	FS1	Fuse 1 - MIC camera protection	--
15	FS3	Fuse 3 - Heater protection 1	--
16	FS5	Fuse 5 - Heater protection 2	--

3.4 MIC Power Supply Units (PSUs) for IR MIC Cameras

The figure below displays the layout of the PCB in the MIC PSUs for IR cameras, with call-out numbers to the side of or below the connection/terminal ID or the terminal, and 'on' the fuses. The table below the figure identifies the connections.

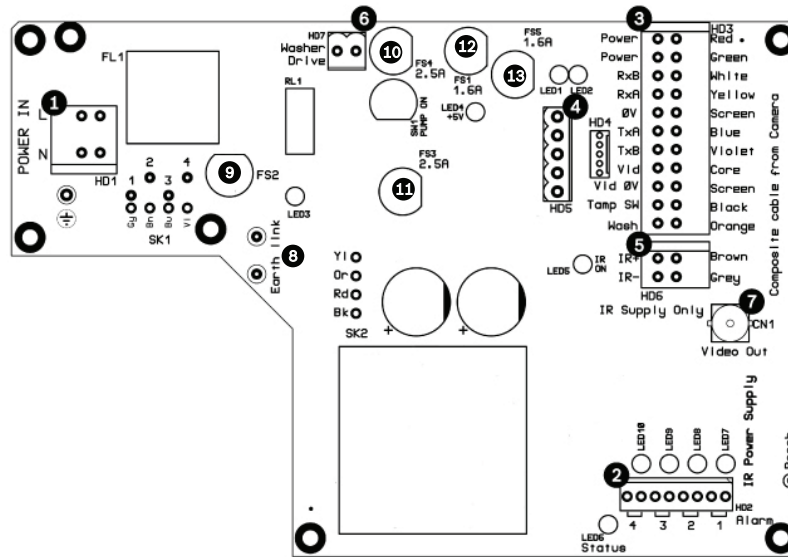


Figure 3.4 Layout of PCB in enclosure of PSU for MIC IR cameras

Number	Connection / Terminal ID	Description/Function of Connection / Terminal	Type of Connection / Terminal
1	HD1	AC Power input	Screw terminal
2	HD2	4-input alarm	Screw terminal
3	HD3	Shielded composite cable (analog connections to camera)	Screw terminal
4	HD4	USB to RS-485 converter	Screw terminal or Molex connector
4	HD5	RS-485 control	
5	HD6	[Optional] Auxiliary, IR lamps	Screw terminal
6	HD7	Washer drive	Screw terminal
7	CN1 (Video Out)	Coax connection	BNC socket
8	Earth Link	Earth Link	--
9	FS2	Fuse 2 - Primary protection	--
10	FS4	Fuse 4 - washer drive	--
11	FS3	Fuse 3 - IR lamps	--
12	FS1	Fuse 1 - MIC camera protection	--
13	FS5	Fuse 5 - MIC camera protection	--

3.5 Earth Link on the PCB

The printed circuit board (PCB) of each MIC PSU (IR and non-IR) has one Earth Link option, near terminal block HD1, to allow the PSU to be set up for different earthing schemes:

- If there is a separate connection between video screen and earth, the Earth Link should be broken. This usually occurs on copper-connected systems where all of the copper video coaxes are taken back to the control room to be connected to a central earth point.
- If fiber optics or other indirect connections are used to get data and video to and from the control room, then the Earth Link should be left intact, as long as it is the only camera-end earth reference point.

3.6 Fuse Ratings

Non-IR MIC power supplies have four (4) off 20 mm fuses (numbers 13 - 16 in *Figure 3.3*) in fuse holders. The ratings for these fuses are fixed on the low voltage secondary side but change with input voltage on the high voltage primary side. The following table shows the fuse values that should be fitted to provide proper protection for the power supplies. **Note:** Fuse FS4 does not exist.

Fuse ID	Fuse Function	Type	Ratings for 240 V Primary	Ratings for 115 V Primary	Ratings for 24 V Primary
FS1	MIC camera protection	Glass	1.6 A anti-surge (T)	1.6 A glass anti-surge (T)	1.6 A glass anti-surge (T)
FS2	Primary protection	Glass	normal 250V 0.5A 5x20mm	normal 250V 0.8A 5x20mm	2.5 A quick blow
FS3	Heater protection 1	Glass	1.6 A anti-surge (T)	1.6 A glass anti-surge (T)	1.6 A glass anti-surge (T)
FS5	Heater protection 2	Glass	1.6 A anti-surge (T)	1.6 A glass anti-surge (T)	1.6 A glass anti-surge (T)

MIC IR power supplies have five (5) 20 mm fuses (see *Figure 3.4*). The following table shows the fuse values that should be fitted to provide proper protection for the power supplies.

Fuse ID	Fuse Function	Type	Ratings for 240 V Primary	Ratings for 115 V Primary	Ratings for 24 V Primary
FS1	MIC camera protection	Glass	1.6 A quick blow	1.6 A quick blow	1.6 A quick blow
FS2	Primary protection	Glass	600 mA quick blow	1.0 A quick blow	2.5 A quick blow
FS3	IR lamps	Glass	2.5 A quick blow	2.5 A quick blow	2.5 A quick blow
FS4	washer drive	Glass	2.5 A quick blow	2.5 A quick blow	2.5 A quick blow
FS5	MIC camera protection	Glass	1.6 A quick blow	1.6 A quick blow	1.6 A quick blow



CAUTION!

Replace only with the same type and rating of fuse for continued protection against the risk of fire, damage or injury. Fitting fuses other than those described above invalidates the product warranty and may result in damage to the product or injury to the installer.

3.7 Installation Instructions



CAUTION!

Installation must be made by qualified personnel and conform to ANSI/NFPA 70 (the National Electrical Code® (NEC)), Canadian Electrical Code, Part I (also called CE Code or CSA C22.1), and all applicable local codes. Bosch Security Systems, Inc. accepts no liability for any damages or losses caused by incorrect or improper installation.



DANGER!

– ELECTRICAL SHOCK HAZARD

To reduce the risk of electrical shock, disconnect power before opening or working on any power supply unit. Power must be disconnected before replacing any fuse in the MIC PSU. Power supply units have power supplied whenever the power cord is inserted into the power source.

- MIC PSUs have a separate internal shield covering the power cable input terminal block (HD1). Only suitably qualified persons should remove this shield and connect the mains power cable. The shield **MUST** be re-installed and fully secured before connecting the power.
- The power supply cable shall have conductors of a maximum size of 12 AWG.
- Branch circuit protection is required. A readily accessible 2-pole disconnect device with a contact separation of at least 3mm must be incorporated externally to the equipment.



WARNING!

To meet UL standards and ratings, all external wires for installation applications **must be** routed through a permanently earthed metal conduit.



CAUTION!

- Do not connect MIC IR units to a MIC PSU with the heater option enabled as this can result in damage to the cameras. Ensure that an IR power supply is used with a MIC IR camera unit. Heaters are available for MIC612 cameras only.
- Except for the Earth Link, heater links (MIC612), and applicable fuse, the MIC PSUs have no user-adjustable parts. MIC cameras have no user-serviceable parts.
- Bosch recommends using an uninterruptible power supply (UPS) in connection with a MIC camera/PSU installation.
- MIC PSU enclosures are not EXD rated and must be replaced with a **certified** enclosure if installed within a hazardous area.



NOTICE!

To maintain the IP (protection) rating of the power supply enclosure, install only listed or recognized conduit hubs or fittings with the same environmental rating as the enclosure in compliance with the installation instruction of the hub or fitting.

To install the power supply, follow these steps:

1. Select the mounting position of the MIC PSU so that the PSU cannot be interfered with either intentionally or accidentally. Bosch recommends using a lockable cabinet.
2. Loosen the four (4) captive Phillips head screws on the top of the lid of the power supply enclosure (item 11, *Figure 3.1*). Lift the lid and set it upside down next to the enclosure.

**NOTICE!**

- Do not stretch or cut, or otherwise disturb, the earth core cable to the inside of the lid and to the earth termination post. (See *Figure 3.6.*)
- Note the position of the thermal pads. They should be sticking onto either the built-in stand-offs on the inside of the lid of the enclosure, or onto designated spots on the encoder. If the pads are not positioned correctly, they can cause the encoder to stop functioning properly. See *Figure 3.9* and *Figure 3.10* for details.

3. Locate the four (4) mounting holes of the PSU (see *Figure 3.5*). The dimensions shown are for the mounting holes only. The other four (4) holes shown are for securing the lid.

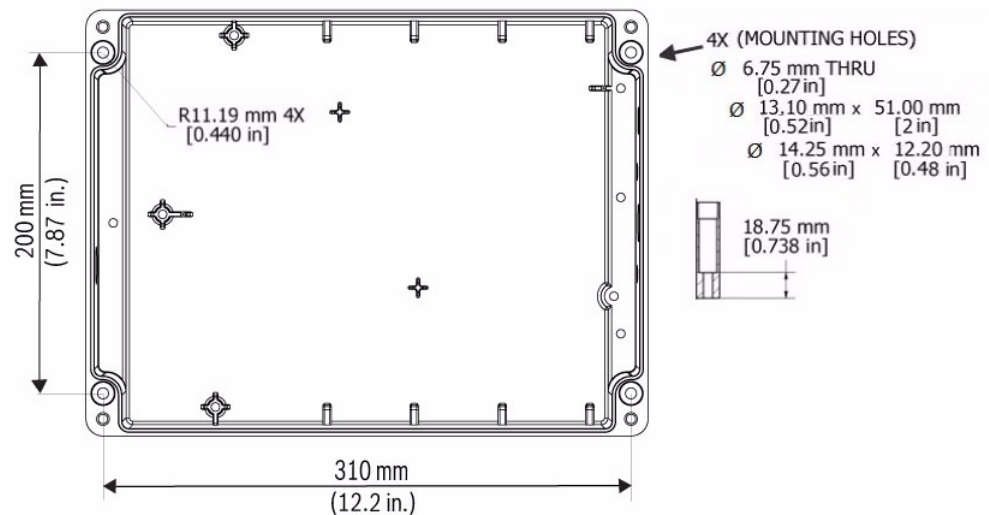


Figure 3.5 MIC IP PSU Mounting Dimensions

4. Drill four (4) holes in the mounting surface for the mounting anchors appropriate for M6 screws (not supplied).
5. Secure the PSU to the mounting surface using four (4) M6 stainless steel screws and washers (not supplied).

**NOTICE!**


If you are securing the power supply enclosure in a vertical position (for example, on a wall), one person should hold the enclosure lid while another secures the enclosure body in place, to avoid damage to any part of the enclosure, and/or injury to the installer(s).

6. Undo the two (2) M3 screws on the internal high voltage input head-end shield (marked with "Danger") covering the power cable terminal HD1; retain the screws.
7. Remove the internal shield and set it nearby, outside of the PSU enclosure.
8. Remove the blanking plug covering the hole for the power cable (item 6, *Figure 3.1*). Install suitable (metal) conduit (not supplied) in the hole. Secure the conduit as recommended by the conduit manufacturer.

**CAUTION!**

Only installations with conduit meet UL standards. If you choose to use a power cord without conduit (not recommended), fit the 1/2 in. NPT cable gland (supplied) in place of the blanking plug. It is easier to fit the power cord through the cable gland outside of the enclosure, and then attach the gland to the enclosure. Ensure that the cable gland has sufficient room to allow for the cable to enter (approximately 60 mm on either side of the enclosure).

9. Prepare the power cable as needed, and then feed the cable into the enclosure.
10. Connect the Live and Neutral cores to the correct screw terminals on terminal block HD1 as identified in the table below and printed on the PCB. Observe polarity and voltage.

PCB Marking	Description
L	Live
N	Neutral
	Earth / Ground

11. Remove the brass nut and copper washer from the earth termination post (item 3, *Figure 3.6*); set these aside.

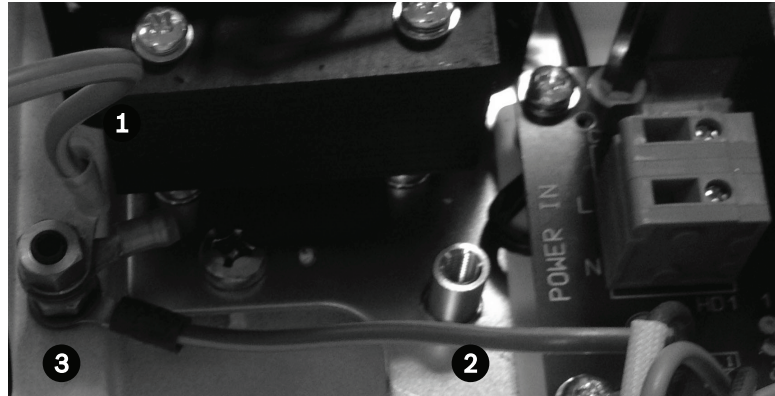


Figure 3.6 Power (mains) input with shield removed, showing terminal block HD1 before wiring

Number	Description
1	Earth core cable to enclosure lid
2	Earth core cable to power supply PCB
3	Earth termination post

12. Remove the ring terminal (supplied).
13. Insert the earth core from the mains cord (item 2, *Figure 3.6*) into the crimp portion (size M6, UL-certified) of the ring terminal and crimp it in place.

Note: The graphic in the figure referenced below is representative of the connections; the layout of the MIC IP PSU differs slightly from that depicted below.
14. Place the ring terminal onto the earth termination post.
15. Replace the copper washer. Secure with the brass nut.
16. Replace the internal shield, taking care to avoid pinching the cables. Tighten the screws.

NOTICE!



For MIC612 cameras only: You must connect the overall shield drain wire of the composite cable to the power supply chassis in order to ground the chassis. Crimp the drain wire to the ring terminal lug attached to the mounting screw of the PCB located to the right of BNC socket CN3 (Video Switched). See *Figure 3.3* for location of the screw.

* If connecting a heater [MIC612 only], see *Section 3.8 Commissioning the Camera with Heater Option Fitted*.

17. *On non-IR models only:* If necessary, connect a tamper switch to terminal block HD2.
18. If simultaneous video (IP and analog (PAL or NTSC)) is desired, follow these steps:
 - a. Disconnect the coax cable between the BNC socket (marked "VIDEO IN") on the encoder and the BNC socket CN1 on the PCB.
 - b. Attach a BNC "T" connector (75 ohm, user-supplied) to the BNC socket CN1 on the PCB.
 - c. Re-attach the coax cable from the encoder to one end of the "T" connector.

- d. Feed your coax cable coming from Bilinx-compatible head-end control system through the top-left M12 cable gland (item 1, *Figure 3.7*).
- e. Attach your coax cable to the other end of the "T" connector.
- f. After the PSU is operational, you must access the menu for Encoder settings and disable the video termination option. See *Section 4.17 Video Input* of the User Manual.

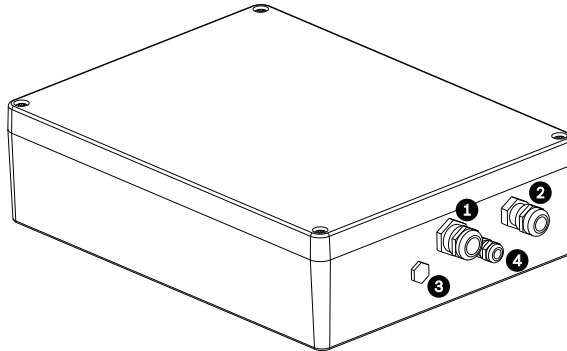


Figure 3.7 Enclosure of MIC IP PSU, with cable glands identified

Number	Description	Cable Gland Size
1	Composite cable (used for analog connections)	1/2 in.
2	RJ45 / Fiber cable	M16
3	For non-thermal cameras: Optional cable gland for alarms For thermal cameras: optional switched video output	M12
4	Cable gland for optional washer drive	M12

19. *On non-IR power supplies for non-thermal cameras:* If connecting to additional add-on cards (for example, a card for 8-input alarms plus washer pump drive (MIC-ALM)), remove the blanking plug that covers the hole for the bottom-left M12 cable gland (item 3, *Figure 3.7*). Attach the supplied M12 gland. Make the appropriate connections to plug-in terminal CN2.
20. Through the top right hole (item 2, *Figure 3.7*) of the enclosure, install conduit necessary to protect standard UTP category 5 cable.

Note: You may need to remove the cable gland first.
21. Feed the category 5 cable through the conduit and into the enclosure.
22. Connect the RJ45 plug of the cable to the ETH socket on the encoder to connect the encoder to the network.

Note: If installing a fiber optic module, see the Fiber Optic Media Converter Installation Guide for instructions for installing the module in the MIC IP PSU.

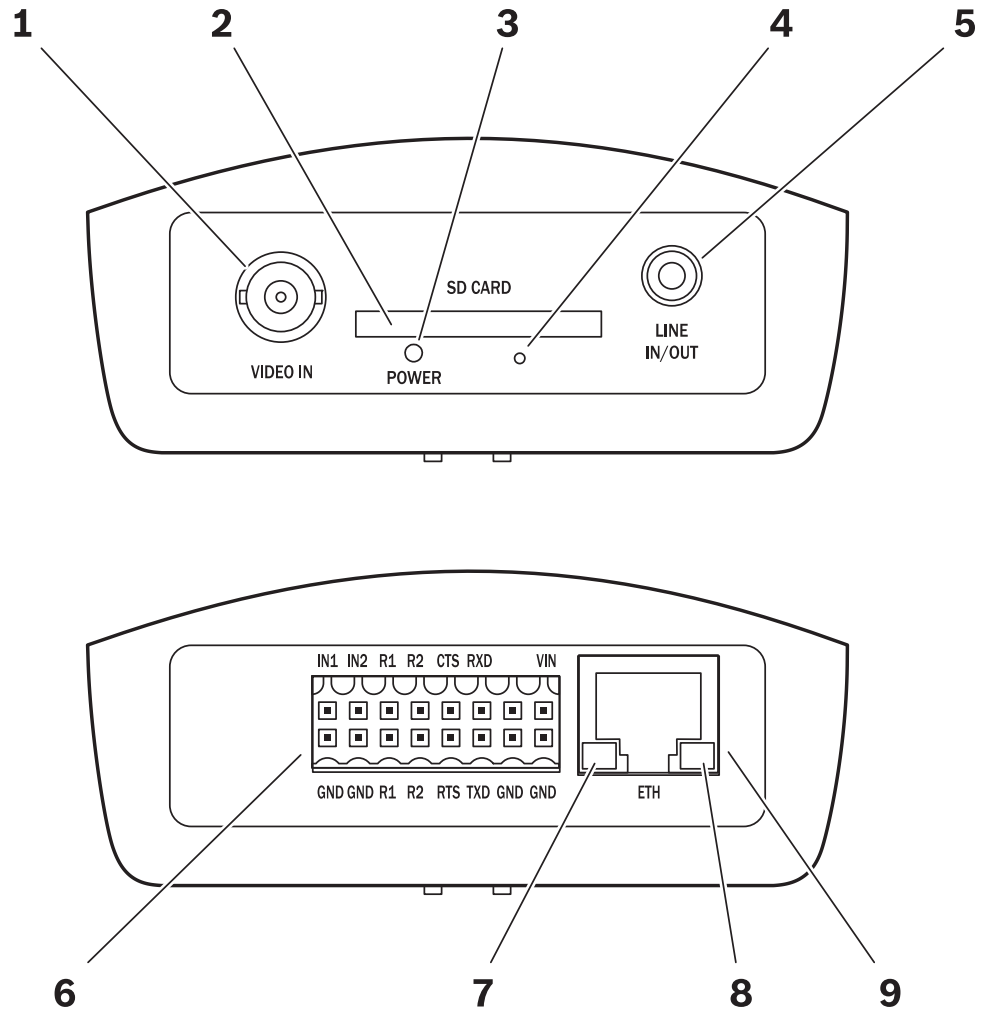


Figure 3.8 Encoder connections front (top half of graphic) and back (bottom half of graphic)

Number	Description
1	VIDEO IN video input BNC socket (75 ohm) for connecting the video source
2	SD CARD slot (The release letter of the current firmware version has a list of compatible cards.)
3	POWER LED lights up green when ready for operation (See "LEDs" in the User Manual for more information about the LEDs.)
4	Factory reset button to restore factory default settings
5	LINE IN/OUT For audio connection (not applicable to MIC cameras)
6	Terminal Block for alarm inputs, relay outputs, serial interface and power supply (See "Terminal block" in the Appendix of the User Manual for details.)
7	Green LED lights up when the unit is connected to the network
8	Orange LED lights up during data transmission
9	ETH RJ45 socket for connecting to an Ethernet LAN (local network), 10/100 MBit Base-T

23. Make the connections for Alarm inputs as needed.

- For IP connections, connect the lines for the alarm inputs (for external devices such as door contacts or sensors) to terminals **IN1** and **IN2** on the orange terminal block (see the section "Terminal block" in the Appendix of the User Manual) of the encoder, and check that the connection is secure. Connect each alarm input to a ground contact (GND). With the appropriate configuration, an alarm sensor can automatically connect the encoder to a remote location, for example.

Note: You can use a zero potential closing contact or switch as the actuator. If possible, use a bounce-free contact system as the actuator.

- For physical alarm connections on MIC IR power supplies, connect alarm input cables to terminal block HD2, as indicated in the table below:

Signal	Pin Number
Alarm 1	1
0 V	2
Alarm 2	3
0 V	4
Alarm 3	5
0 V	6
Alarm 4	7
0 V	8

24. Make the connections for Relay outputs as needed. Connect the lines for the relay outputs (for switching external units such as lamps or alarm sirens) to terminals **R1** and **R2** on the orange terminal block of the encoder, and check that the connection is secure. You can operate these relay outputs manually while there is an active connection to the encoder. The outputs can also be configured to activate sirens or other alarm units automatically in response to an alarm signal.



CAUTION!

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

25. To save recordings locally, insert an SD card into the slot **SD CARD** of the encoder by carefully sliding the card into the slot as far as it will go, until it locks into place. (To remove the card, push carefully in the direction of insertion until the mechanical catch releases, and then remove the card.)



CAUTION!

If the card is formatted already, all existing data will be deleted from the card! Before inserting the card, check whether the SD card contains any data that must be backed up.

26. On MIC IR power supplies, a washer drive is standard. A 24 VAC rated relay is fitted via the onboard fuse FS4 (rated at 2.5 Amps). Make the following washer pump connections to terminal block HD7 (marked Washer Drive on the PCB):

Signal	Pin Number
Washer Pump	1
Washer Pump	2



WARNING!

The washer pump terminal is rated only to 24 VAC or VDC maximum voltage and is not suitable for Mains-operated pumps.

27. Test the washer by pressing the red button marked SW1 PUMP ON on the PCB.
LED 3 illuminates in response to telemetry commands from the control room to turn on the washer. Note that the software in the camera prevents the washer from running more than 10 seconds continuously to prevent emptying the washer bottle.



NOTICE!

For installation of the MIC Washer Kit (MIC-WKT), MIC 8-input Alarm Card (MIC-ALM) or Biphase converters (MIC-BP3 or MIC-BP4), please see their respective manuals.

28. Verify that the thermal pads are in the correct position on the encoder or on the built-in stand-offs on the inside of the lid of the enclosure. Correct positioning of the thermal pads is imperative, or the encoder may not function. See the photos below for the correct positioning.

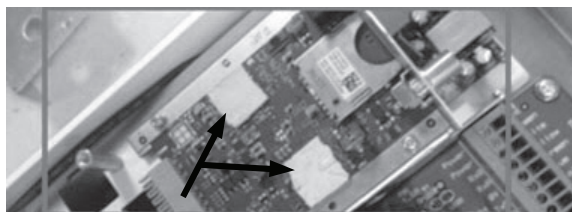


Figure 3.9 Thermal pads in correct position on the encoder

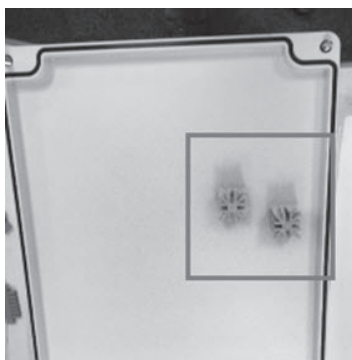


Figure 3.10 Location of correct position for thermal pads on the inside of the lid of the enclosure

29. After all wiring and connections are complete, connect the power supply to the power source. The PSU should now have power and be operational.
30. Verify that the following LEDs are lit on the PCB (depending on the model of MIC PSU):

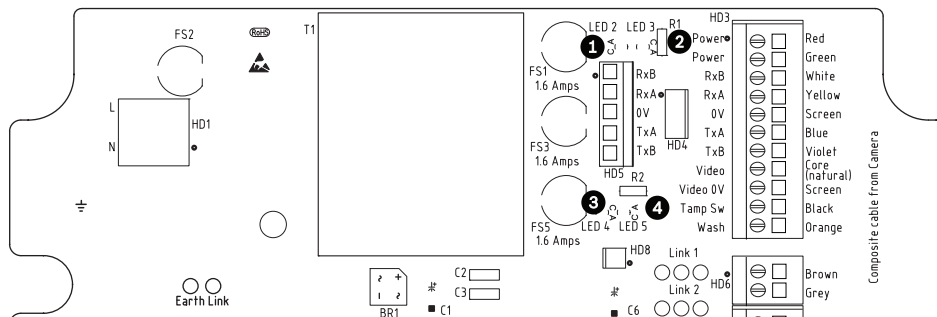


Figure 3.11 MIC Series power supply LED position (at the "top right" of the PCB)

Number	LED	Description
MIC Non-IR models		
1	LED 2	18 VAC power on to camera
2	LED 4	Power on for optional heater
3	LED 3	18 VAC power on camera
4	LED 5	Power on for optional heater

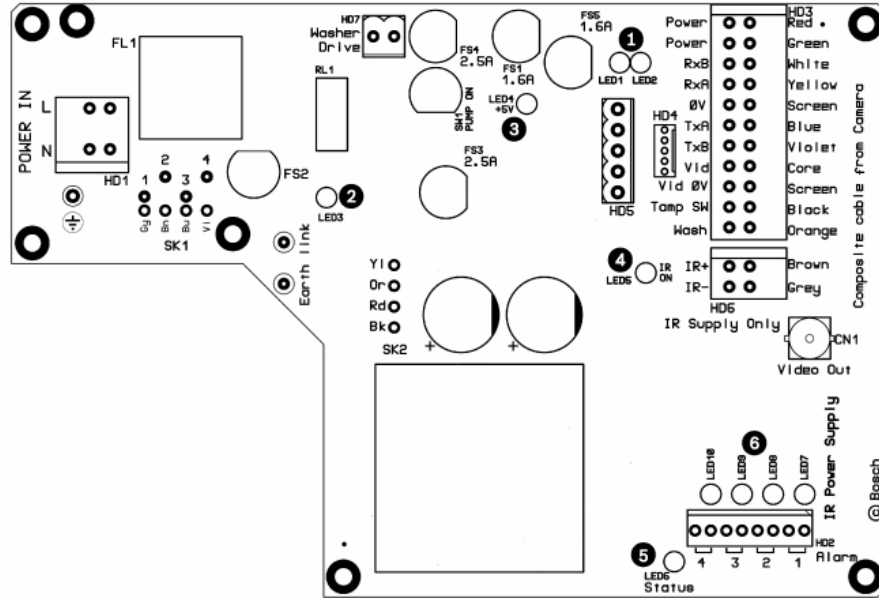


Figure 3.12 MIC Series IR power supply LED positions

Number	LED	Description
MIC IR models		
1	LED 1 LED 2	Indicates that 18 VAC is available from the power supply and that the supply fuses are intact.
2	LED 3	Illuminates when the washer drive is on.
3	LED 4	Monitors the internally generate +5 V.
4	LED 5	Illuminates when the IR lamp supply is turned on by the camera telemetry.
5	LED 6	Status LED. Pulses On/Off when Multi Alarm is selected.
6	LED 7-10	Illuminate when the associated alarm is active.

31. Re-attach the enclosure lid and tighten the four (4) captive screws on the lid to ensure that the enclosure is watertight.

3.8 Commissioning the Camera with Heater Option Fitted

To enable the heaters for MIC612, you must change two links on the PCB of the power supply. Follow these steps:

1. Disconnect the power supply from the power source.
2. Open the power supply enclosure.
3. Locate Link 1 and Link 2 on the PCB, next to terminal block HD6. The default setting is 0V.

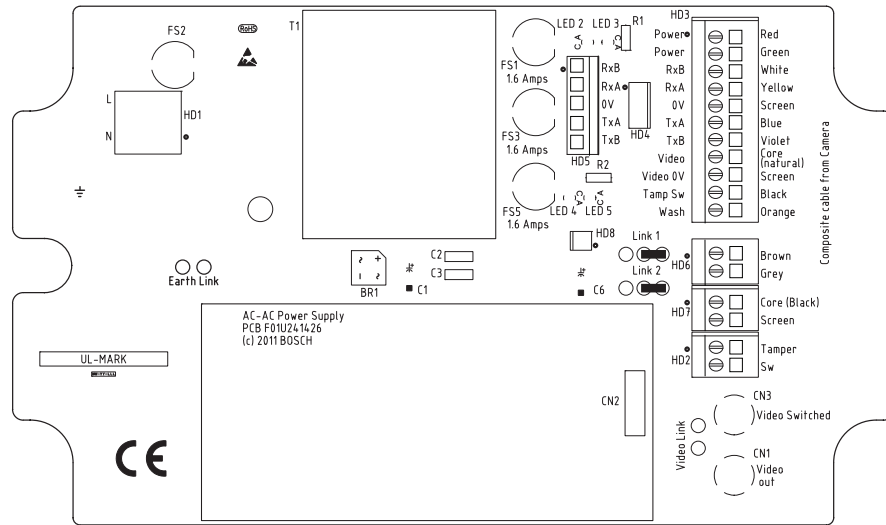


Figure 3.13 PCB links set to 0V

4. Break the two solder links. Remove any excess solder.
5. Solder the links, using TCW link wire, from the left hand pads to the middle pads. The power supply will now deliver 18 VAC to terminal block HD6.

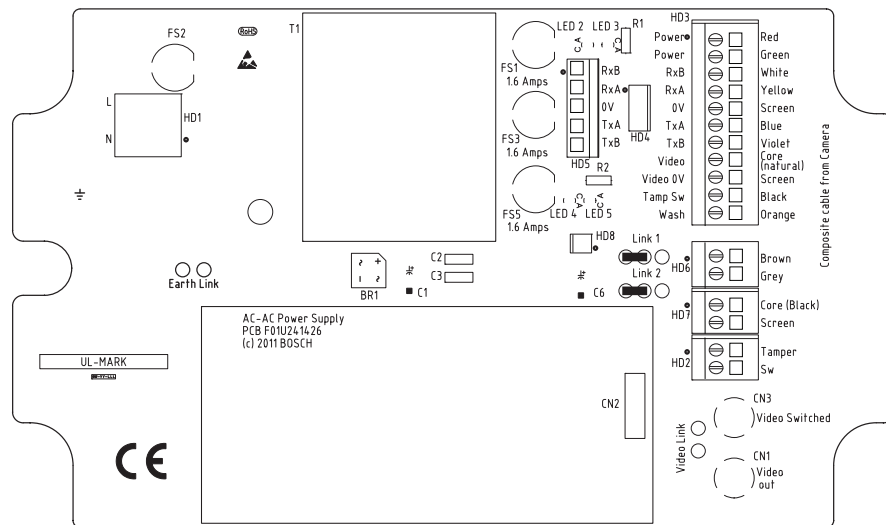


Figure 3.14 PCB links set to 18V

6. Locate the Brown and Grey wires from the composite cable.
7. Connect the heater wires Brown and Grey to terminal block HD6 as labelled on the PCB. The heaters are thermostatically controlled and will automatically turn on at +5 °C (+41 °F) and turn off at +15 °C (+59 °F).
8. Check all connections.
9. Close the PSU enclosure.
10. Reconnect the power supply to the power source.

3.9 Simultaneous IP and Analog Video/Control ("Hybrid" Operation)

The figure below illustrates how to configure your system to achieve simultaneous video and control over both IP and analog connections.

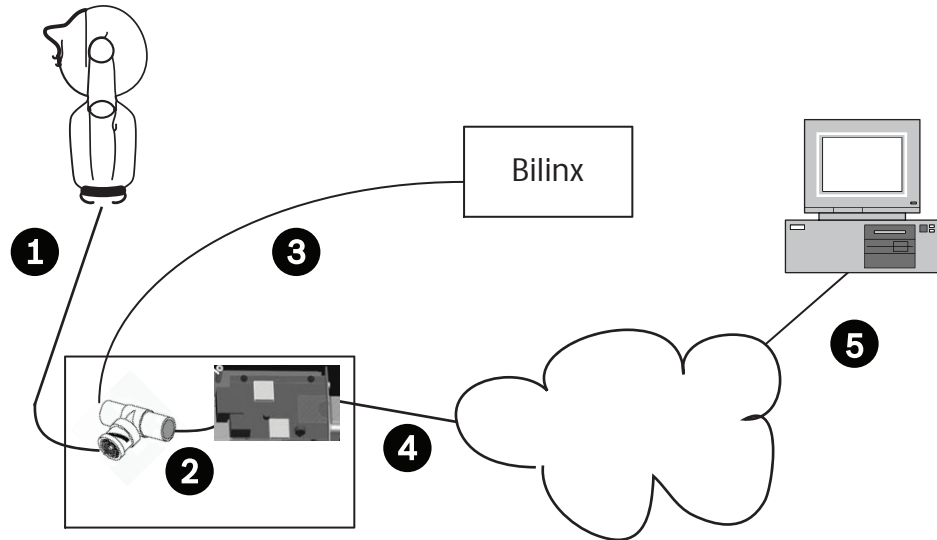


Figure 3.15 System configuration for simultaneous video/control

Number	Description
1	Connection between MIC camera and BNC T-connector in BNC socket on PCB in MIC IP PSU
2	Connection between BNC T-connector and encoder in MIC IP PSU
3	Connection between BNC T-connector and Bilinx-based control (head-end) system
4	Connection between encoder and Local Area Network (LAN) (or the "cloud")
5	Connection between the Local Area Network (LAN) (or the "cloud") and PC connected to video monitor

3.10 Assign an IP Address

Assign an IP address to the encoder. The encoder must have a valid IP address for your network and a compatible subnet mask before you can operate it within your network.

1. If you have not already done so, install the **Configuration Manager** program from the product CD.
2. Start **Configuration Manager**. The system automatically searches the network for compatible units.
3. If the encoder is displayed in the list, right-click the entry, then select Device Network Settings... from the popup menu that appears.
4. In the Device IP address field, enter the required IP address (for example **192.168.0.100**) and click OK. The encoder reboots and the IP address is valid.

3.11 Hardware connections between video servers

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



NOTICE!

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

Installation

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

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



NOTICE!

Make sure that the units are configured for the network environment and that the correct IP address for the remote location to be contacted in the event of an alarm is set on the Alarm Connections configuration page (see *Section 4.38 Alarm Connections, page 65*).

Connecting

There are three options for establishing a connection between a sender and a compatible receiver in a closed network: an alarm, a terminal program, or Internet Explorer.



NOTICE!

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

Connecting on alarm

With the appropriate configuration, a connection between a sender and a receiver is made automatically when an alarm is triggered (see *Section 4.38 Alarm Connections, page 65*). After a short time the live video image from the sender appears on the connected monitor. This option can also be used to connect a sender and a compatible receiver using a switch connected to the alarm input. You do not need a computer to make the connection in this case.

Connecting with a terminal program

Various requirements must be met in order to operate with a terminal program (see *Section 6.11 Communication with terminal program, page 95*).

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

Closing the connection with a terminal program

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

4 Configuration using a Web browser

4.1 Connecting

A computer with Microsoft Internet Explorer (version 7.0 or higher) can receive live images from the encoder, control cameras or other peripherals and replay stored video sequences. Before you can operate the camera via the encoder, you must configure the camera. The integrated HTTP server in the encoder provides you with the option to configure the unit over the network with a Web browser. This option is an alternative to configuration using the Configuration Manager application (version 4.21 or higher) and is considerably richer in function and more convenient than configuration using the terminal program.

4.1.1 System Requirements

- Computer with Windows XP or Windows 7 operating system
- Network access (Intranet or Internet)
- Microsoft Internet Explorer (version 7.0 or higher)
- Screen resolution at least 1,024 × 768 pixels
- 16- or 32-bit color depth
- Installed Java Virtual Machine (JVM)



NOTICE!

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

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

In Windows 7, deactivate protected mode on the **Security** tab under **Internet Options**.

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

4.1.2 Additional Operational Requirements

- Instead of Microsoft Internet Explorer:
Receiver software (such as Bosch Video Management System (version 3.0 or higher)) OR H.264-compatible hardware decoder from Bosch Security Systems (such as VIP XD HD) as a receiver and connected video monitor
- For playing back recordings: connection to storage medium [a different encoder from the one built-in to the power supply enclosure]

4.1.3 Installing MPEG ActiveX

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

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

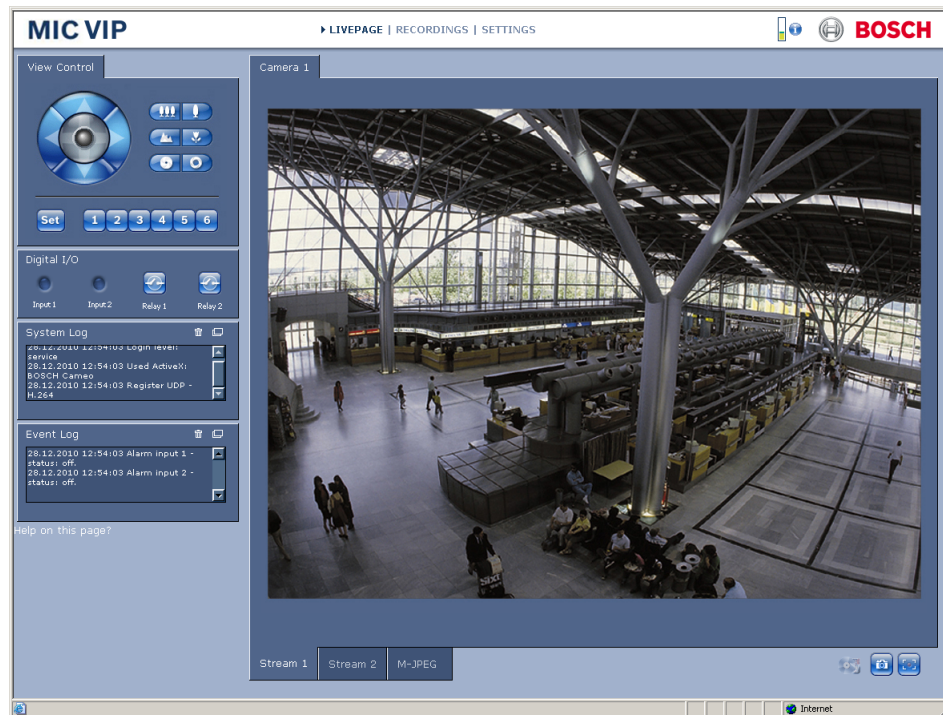
4.1.4 Establishing the Connection

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

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

1. Start the Web browser.
2. Enter the IP address of the encoder as the URL.

3. During initial installation, confirm the security questions that appear. The connection is established and after a short time you will see the LIVEPAGE with the video image.



Maximum number of connections

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

Protected Encoder

If the encoder 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 encoder offers the option to limit the extent of access using various authorization levels (see *Section 4.10 Password, page 37*).

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 encoder must be configured accordingly, otherwise no communication is possible.

To configure the unit, you must connect the encoder directly to a computer using a network cable. This is because communication via the network is not enabled until the Identity and Password parameters have been set and successfully authenticated (see *Section Authentication, page 76*).

4.2 Configuration menu

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

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

- Basic Mode
- Advanced Mode

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

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

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



CAUTION!

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

All settings are backed up in the encoder memory so they are not lost even if the power fails. The exception is the time settings, which are lost after 72 hours without power if no central time server is selected (see *Section 4.4 Basic Mode: Date/Time, page 32*).

Starting configuration

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



Navigation

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

Making changes

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

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

**CAUTION!**

Save each change with the associated Set button.

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

4.3**Basic Mode: Device Access**

Device Access

Camera name

Password 'service'

Confirm password

Password 'user'

Confirm password

Password 'live'

Confirm password

Camera name

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

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

**CAUTION!**

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

Special characters are not supported by the system's internal management.

Password

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

The encoder operates with three authorization levels: **service**, **user** and **live**.

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

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

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

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

Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters.



CAUTION!

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



NOTICE!

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

Confirm password

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

4.4 Basic Mode: Date/Time

Date/Time

Device date	Tuesday, 28.12.2010	
Device time	11:23:19	
Device time zone	(UTC +1:00) Western & Central Europe	<input type="button" value="Sync to PC"/>
Time server IP address	<input type="text"/>	
Time server type	<input type="text" value="SNTP server"/>	

Device date / Device time / Device time zone

If there are multiple devices operating in your system or network, it is important to synchronize their internal clocks. For example, it is only possible to identify and correctly evaluate simultaneous recordings when all units are operating on the same time. If necessary, you can synchronize the unit with your computer's system settings.

- ▶ Click the Sync to PC button to copy your computer's system time to the encoder.

Time server IP address

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

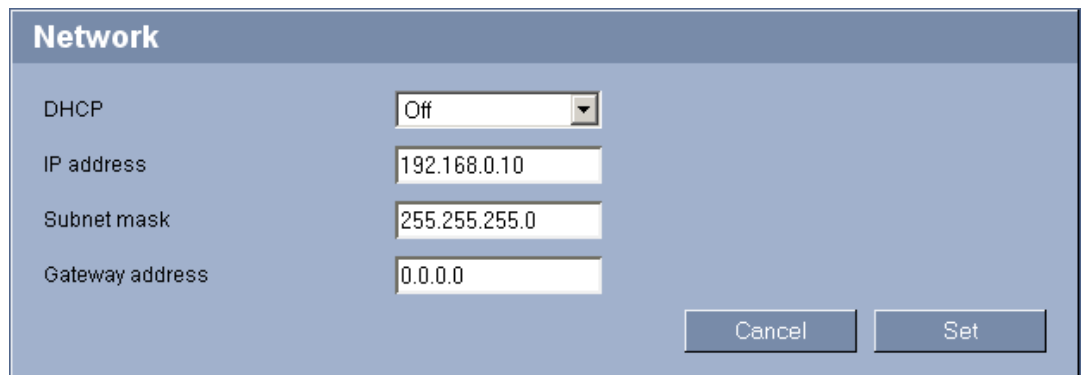
- ▶ Enter the IP address of a time server here.

Time server type

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

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

4.5 Basic Mode: Network



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

1. Make the desired changes.
2. Click the Set and Reboot button. The encoder is rebooted and the changed settings are activated.



CAUTION!

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

DHCP

If a DHCP server is employed in the network for the dynamic assignment of IP addresses, you can activate acceptance of IP addresses automatically assigned to the encoder.

Certain applications (for example, Bosch Video Management System) use the IP address for the unique assignment of the unit. If you use these applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

IP address

Enter the desired IP address for the encoder 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**).

4.6 Basic Mode: Encoder

Encoder

Non-recording profile High resolution 1 ▾

Property H.264 MP SD

High resolution 1

Profile #	1
Encoding interval	1 (0.00 ips)
Video resolution	4CIF/D1
Target bit rate	2000 kbps
Maximum bit rate	4000 kbps

Cancel
Set

Non-recording profile

You can select a profile for encoding the video signal.

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

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



NOTICE!

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

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

4.7 Basic Mode: System Overview

System Overview	
Hardware version	F0004C40
Firmware version	45500551
Device type	MIC VIP
IP address	192.168.0.20
Audio option	No
Storage medium attached	No
Initiator name	iqn.2005-12.com.bosch:unit00075f79d395
MAC address	00-07-5F-79-D3-95
Major version number	5.51
Build number	45
Stream 1	High resolution 1
Stream 2	Low bandwidth
Temperature	100°F / 37.5°C (max 114°F / 45.5°C)
Serial number	044000120105010018

Device Information	
Device model	MIC550IR Series 28X Day/Night
Video type	NTSC
Firmware version camera	02.02.00.38

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.

4.8 Advanced Mode: General

4.9 Identification



CAUTION!

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

Camera name

The camera name makes it easier to identify the remote camera location, in the event of an alarm for example. It will be displayed in the video screen if configured to do so (see *Section Camera name stamping, page 39*). The camera name makes the task of administering cameras in larger video monitoring systems easier, for example using the Bosch Video Management System.

Enter a unique, unambiguous name for the camera in this field. Choose a name that makes it as easy as possible to quickly identify the location. You can use both lines for this.



CAUTION!

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

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

1. Click the icon next to the second line. A new window with the character map is opened.
2. Click the required character. The character is inserted into the Result field.
3. In the character map, click the **<<** and **>>** icons to move between the different pages of the table, or select a page from the list field.
4. Click the **<** icon to the right of the Result field to delete the last character, or click the **X** icon to delete all characters.
5. Now click the OK button to apply the selected characters to the second line of the Camera 1 parameters. The window will close.

Camera ID

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

Initiator extension

You can attach your own text to the initiator name of the encoder to make the unit easier to identify in large iSCSI systems. This text is added to the initiator name, separated from it by a full stop. You can see the initiator name in the system overview (see *Section 4.7 Basic Mode: System Overview, page 35*).

4.10

Password

The screenshot shows a web interface for setting passwords. It is titled 'Password' and contains three rows of input fields. The first row is for 'service', the second for 'user', and the third for 'live'. Each row has a 'Password' field and a 'Confirm password' field. A 'Set' button is positioned at the bottom right of the form area.

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

**NOTICE!**

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

Password

The encoder operates with three authorization levels: **service**, **user** and **live**.

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

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

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

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

Enter the password for the appropriate authorization level here. The maximum password text length is 19 characters.

**CAUTION!**

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

Special characters are not supported by the system's internal management.

Confirm password

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

4.11

Date/Time

The screenshot shows a web-based configuration interface for the Date/Time settings. It features several input fields and buttons:

- Date format:** A dropdown menu set to "DD.MM.YYYY".
- Device date:** Three input fields for day, month, and year, showing "Sunday", "12", and "12", with "2010" in a separate field.
- Device time:** Three input fields for hours, minutes, and seconds, showing "11", "27", and "10". A "Sync to PC" button is next to it.
- Device time zone:** A dropdown menu set to "(UTC +1:00) Western & Central Europe".
- Daylight saving time:** A "Details" button.
- Time server IP address:** An empty text input field.
- Time server type:** A dropdown menu set to "SNTP server".
- Set:** A button at the bottom right to save the configuration.

Date format

Select your required date format.

Device date / Device time

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

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

Device time zone

Select the time zone in which your system is located.

Daylight saving time

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



NOTICE!

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

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

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

Time server IP address

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

Enter the IP address of a time server here.

Time server type

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

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

4.12 Display Stamping

Display Stamping	
Camera name stamping	Off
Time stamping	Off
Display milliseconds	Off
Alarm mode stamping	Off
Alarm message	<input type="text"/> (max. 31 characters)
Video watermarking	Off

Set

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

Camera name stamping

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

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

Time stamping

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

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

Display milliseconds

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

Alarm mode stamping

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

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

Alarm message

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

Video watermarking

Choose On if you wish the transmitted video images to be "watermarked". After activation, all images are marked with an icon. The icon indicates if the sequence (live or saved) has been manipulated (see *Section Display stamping, page 85*).

4.13 Advanced Mode: Web Interface

4.14 Appearance

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

**NOTICE!**

You can use either GIF or JPEG images. The file paths must correspond to the access mode (for example **C:\Images\Logo.gif** for access to local files, or

<http://www.mycompany.com/images/logo.gif> for access via the Internet/Intranet).

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

Website language

Select the language for the user interface here.

Company logo

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

Device logo

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

**NOTICE!**

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

JPEG interval

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

4.15**LIVEPAGE Functions**

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

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

Lease time [s]

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

Show alarm inputs

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

Show VCA trajectories

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

Show VCA metadata

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

Show overlay icons

Select this checkbox to display the overlay icons on the LIVEPAGE.

Show event log

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

Show system log

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

Allow snapshots

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

Allow local recording

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

I-frames-only stream

Select this checkbox to configure the LIVEPAGE to stream I-frames-only video.

Path for JPEG and video files

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

4.16

Logging

Logging		
Save event log	<input type="checkbox"/>	
File for event log	<input type="text" value="C:\Event.txt"/>	<input type="button" value="Browse"/>
Save system log	<input type="checkbox"/>	
File for system log	<input type="text" value="C:\System.txt"/>	<input type="button" value="Browse"/> <input type="button" value="Set"/>

Save event log

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

File for event log

1. Enter the path for saving the event log here.

2. If necessary, click Browse to find a suitable directory.

Save system log

Check this option to save system messages in a text file on your local computer.

You can then view, edit and print this file with any text editor or the standard Office software.

File for system log

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

4.17

Video Input

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

75 Ohm termination

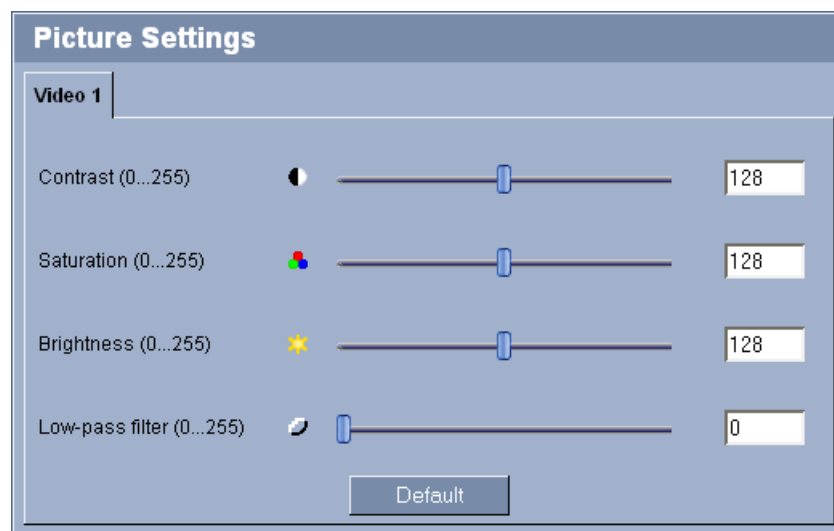
Select Off if the video signal is to be looped through.

4.18

Advanced Mode: Encoder

4.19

Picture Settings



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

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

Contrast (0...255)

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

Saturation (0...255)

You can use this function to adjust color saturation in order to correct unnatural camera signal colors.

Brightness (0...255)

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

Low-pass filter (0...255)

You can use this function to filter very fine noise from the image. This reduces and optimizes the bandwidth necessary for image transmission over the network. The image resolution may be impaired.

The higher the value set with the slide control, the more high-frequency components are filtered from the image. Check your setting in the image window next to the slide controls. Also observe the processor load indicator that appears at the top of the window near the manufacturer's logo (see *Section 6.8 Processor load, page 94*).

4.20**Encoder Profile**

The screenshot shows the 'Encoder Profile' configuration window. At the top, there are tabs for Profile 1 through Profile 8. The 'Profile 1' tab is active. The configuration parameters are as follows:

- Profile name: High resolution 1
- Target bit rate: 2000 kbps
- Maximum bit rate: 2400 kbps
- Encoding interval: Slider control, value 29.97 ips
- Video resolution: 4CIF/D1 (dropdown menu)
- GOP structure: IP (dropdown menu)
- Averaging period: No averaging (dropdown menu)
- I-frame distance: Slider control, value 30 (1.00 I-frames/s)
- Min. P-frame QP: Slider control, value 17
- I/P-frame delta QP: Slider control, value -6

Buttons include 'Expert Settings <<', 'Default', and 'Set'.

You can change the names and individual parameter values for the encoder profiles. You can use this to adapt the video data transmission to the operating environment (for example network structure, bandwidth, data load).

Pre-programmed profiles are available, each giving priority to different perspectives. Below is a brief description of the factory default settings for the encoder profiles.

- **High resolution 1**
High quality for connections with the highest bandwidth, resolution 704 × 576/480 pixels
- **High resolution 2**
High quality for high bandwidth connections, resolution 704 × 576/480 pixels
- **Low bandwidth**
High resolution for low bandwidth connections, resolution 704 × 576/480 pixels
- **DSL**
For DSL connections with 500 kbps, resolution 704 × 576/480 pixels

- **ISDN (2B)**
For ISDN connections via two B-channels, resolution 352 × 288/240 pixels
- **ISDN (1B)**
For ISDN connections via one B-channel, resolution 352 × 288/240 pixels
- **MODEM**
For analog modem connections with 20 kbps, resolution 352 × 288/240 pixels
- **GSM**
For GSM connections at 9,600 baud, resolution 352 × 288/240 pixels

**CAUTION!**

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

**NOTICE!**

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

Profile name

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

**CAUTION!**

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

Target bit rate

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

For complex images or frequent changes of image content due to frequent movements, this limit can be temporarily exceeded up to the value entered in the Maximum bit rate field.

Maximum bit rate

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

Encoding interval

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

Video resolution

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

- CIF
352 × 288/240 pixels
- 4CIF/D1
704 × 576/480 pixels

Expert Settings

Click this button to reveal the additional fields for Encoder Profiles. You can use the expert settings to adapt the I-frame quality and the P-frame quality to specific requirements, if necessary. The setting is based on the H.264 quantization parameter (QP).

GOP structure

Select the structure you require for the Group of Pictures here. Depending on whether you place greater priority on having the lowest possible delay (IP frames only) or using as little bandwidth possible, you can choose between IP, IBP, and IBBP.

Averaging period

This parameter allows you to set the averaging period

Options are: No averaging (default), 1 min, 2 min, 5 min, 10 min, 30 min, 1h, 2h, 5h, 12h, 1 days, 2 days, 3 days, 7 days.

I-frame distance

This parameter allows you to set the intervals in which the I-frames will be coded. With the Auto setting, the encoder inserts I-frames as necessary. An entry of **3** indicates that only every third image is an I-frame; the frames in between are coded as P-frames. Note that if you have selected IBP as GOP structure only even values are supported. If you have selected IBBP as GOP structure only 3 or multiples of 3 are supported as value.

Min. P-frame QP

This setting adjusts the maximum image quality of the P-frames. Auto automatically adjusts to the optimum combination of movement and image definition (focus).

The value **9** represents maximum image quality, a value of **51** represents minimum quality.

With the slide control, define a control range from a chosen value to **51**. The encoder delivers the best possible quality within this control range while maintaining the maximum bit rate.

I/P-frame delta QP

This setting sets the image quality of the I-frames. Select Auto to ensure that the maximum bit rate is not exceeded. Auto automatically follows the P-frame image quality.

Default

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

4.21 Encoder Streams



The encoder simultaneously generates two data streams (Dual Streaming); you can select the relevant property for these here and connect them to an encoder profile, for example one for transmissions to the Internet and one for LAN connections.

Two settings with different encoder properties are available:

- H.264 BP+ bit-rate-limited
Select this setting when using hardware decoders or the Divar XF digital video recorder. The bit rate is limited to 1.2 Mbps.
CABAC: off
CAVLC: on
GOP structure: IP
I-frame distance: 15
Deblocking filter: on
- H.264 MP SD
Select this setting when using software decoders, PTZ and for rapid movements in the images.
CABAC: on
CAVLC: off
GOP structure: IP
I-frame distance: 30
Deblocking filter: on



CAUTION!

Hardware decoders VIP XD and VIP X1600 XFMD can only process algorithm H.264 BP+. Bear this in mind when configuring profile settings.

1. Select the required encoder properties and one of the encoder profiles for each data stream.
2. Click the Preview button. The preview screens for both data streams are shown.

3. Click the 1:1 Live View button below the preview screen to open a new window with the original data stream and to check the image quality and the transmission rate.

Property

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

Non-recording profile

Select the required encoder profile here. The properties of the profiles are defined on the Encoder Profile page (see *Section 4.20 Encoder Profile, page 44*).

JPEG stream

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

Resolution

The video resolution. Options are: CIF, 4CIF/D1.

Max. frame rate

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

Picture quality

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

4.22

Pixel Counter

Counts the number of pixels in a defined image area. The pixel counter allows the installer to easily verify that the camera installation fulfills any regulatory or specific customer requirements, for example, calculating the pixel resolution of the face of a person passing a doorway monitored by the camera.

4.23

Advanced Mode: Camera

4.24

Camera Options

Camera options are sorted into Settings Groups 1 through 4.

Settings Group 1 has the following settings:

White Balance

Adjusts the color settings to maintain the quality of the white areas of the image.

- **ATW:** allows the camera to continuously adjust color reproduction.
- **Indoor:** white balance tracking for indoor use.
- **Outdoor:** white balance tracking for outdoor use.
- **AWB Hold:** places the ATW on hold and saves the color settings.
- **Extended ATW (default):** allows the camera to constantly adjust for optimal color reproduction.
- **Manual:** Red and Blue gain can be manually set to a desired position.
- **Outdoor Auto:** Automatically adjusts the white balance to reduce the dark tones at dawn or dusk.
- **Sodium Lamp Auto:** Automatically adjusts for sodium vapor light to restore objects to their original color.
- **Sodium Lamp:** Optimizes the sodium vapor light to restore objects to their original color.

Red Gain

The red gain adjustment offsets the factory white point alignment (reducing red introduces more cyan).

Blue Gain

The blue gain adjustment offsets the factory white point alignment (reducing blue introduces more yellow). It is only necessary to change the white point offset for special scene conditions.

Gain Control

Adjusts the automatic gain control (AGC). Automatically sets the gain to the lowest possible value needed to maintain a good picture.

- **AGC** (default): electronically brightens dark scenes, which may cause graininess in low light scenes.
- **Fixed**: no enhancement. This setting disables the Max. Gain Level option. If you select this option, the camera makes the following changes automatically:
 - **Night Mode**: switches to Color
 - **Auto Iris**: switches to Constant

Maximum Gain Level

Controls the maximum value the gain can have during AGC operation. To set the maximum gain level, type a value between 1 and 6. The default setting is 4.

Sharpness

Adjusts the sharpness of the picture. To set the sharpness, type a value between 1 and 15 inclusive. The default setting is 12.

Settings Group 2 has the following settings:

Shutter Mode

- **Off**: turns the Auto SensUP Off.
- **AutoSensUp**: increases camera sensitivity by increasing the integration time on the camera. This is accomplished by integrating the signal from a number of consecutive video frames to reduce signal noise. If you select this option, the camera makes the following change automatically:
 - **Auto Iris**: switches to Constant
 - **Shutter**: is disabled

Shutter

Adjusts the electronic shutter speed (AES). Controls the time period for which light is gathered by the collecting device. The default setting is 1/60 second for NTSC and 1/50 for PAL cameras. The range of settings is from 1/1 to 1/10000.

AutoSensUp Maximum

Options are: 15x (default), 7.5x, 4x, 2x.

Night Mode

Selects night mode (B/W) to enhance lighting in low light scenes. Select from the following options:

- **Monochrome**: Forces the camera to stay in Night Mode and transmit monochrome images.
- **Color**: The camera does not switch to Night Mode regardless of ambient light conditions.

- **Auto** (default): The camera switches out of Night Mode after the ambient light level reaches a pre-defined threshold.

Night Mode Threshold

Adjusts the level of light at which the camera automatically switches out of night mode (B/W) operation. Select a value between 10 and 55 (in increments of 5), where 10 is earlier and 55 is later.

Night Mode Color

On or Off

Settings Group 3 has the following settings:

Backlight Compensation

Optimizes the video level for the selected area of the image. Parts outside this area may be underexposed or overexposed. Select On to optimize the video level for the central area of the image. The default setting is Off.

Stabilization

Turns on video stabilization.

Wide Dynamic Range

Turns on the wide dynamic range feature. Wide Dynamic Range improves image reproduction in extreme high-contrast environments. Select from Off, On, or Auto Mode.

Settings Group 4 has the following settings:

Wiper

Controls the wiper of the MIC cameras. Options are:

CONTINUOUS: Wiper wipes continuously until deactivated manually or by the five-minute timeout built in to the system. INTERMITTENT: Wipes twice, then turns off after 15 seconds. ONE SHOT: Wipes five times, then turns off. WASH WIPE: Wiper washes and wipes. OFF: Turns off the wiper.

Wiper/washer

Click Start to start the wiper/washer. Click Stop to stop the wiper/washer.

Illuminator

Controls IR illuminators. When ON, the camera gives a much better image at low light levels. [Valid only for MIC-550IR units.] Options are: On, Off, Auto.

IR focus correction

Optimizes the focus for IR lighting. Options are: On, Off, Auto.

4.25

Lens

Lens options are sorted into Settings Groups 1 through 2.

Settings Group 1 has the following settings:

Auto Focus

Continuously adjusts the lens automatically to the correct focus for the sharpest picture.

- **One Push** (default): activates the Auto Focus feature after the camera stops moving. Once focused, Auto Focus is inactive until the camera is moved again.

- **Auto Focus:** Auto Focus is always active.
- **Manual:** Auto Focus is inactive.

Auto Iris

Automatically adjusts the lens to allow the correct illumination of the camera sensor. This type of lens is recommended for use where there are low light or changing light conditions.

- **Constant** (default): camera constantly adjusts to varying light conditions (default).
If you select this option, the camera makes the following changes automatically:
 - **Gain Control:** switches to AGC.
 - **Shutter Speed:** switches to default.
- **Manual:** camera must be manually adjusted to compensate for varying light conditions.

Auto Iris Level

Increases or decreases brightness according to the amount of light. Type a value between 1 and 15, inclusive. The default setting is 5.

Iris Speed

Controls how fast the Iris will be.

Focus Speed

Controls how fast the Auto focus will readjust when the focus becomes blurred. Select from the following options:

- **Super Slow**
- **Slow** (default)
- **Medium**
- **Fast**

Maximum Zoom Speed

Controls the zoom speed. The default setting is Medium.

Settings Group 2 has the following settings:

Digital Zoom

Digital zoom is a method of decreasing (narrowing) the apparent angle of view of a digital video image. It is accomplished electronically, without any adjustment of the camera's optics, and no optical resolution is gained in the process. Select Off to disable or On to enable this feature. The default setting is On.

Zoom Polarity

Capability to reverse the operation of the zoom button on the controller.

- **Normal** (default): zoom controls operate normally.
- **Reverse:** zoom controls are reversed.

Focus Polarity

- **Normal (default):** focus controls operate normally.
- **Reverse:** focus controls are reversed.

Iris Polarity

Capability to reverse the operation of the iris button on the controller.

- **Normal** (default): iris controls operate normally.
- **Reverse:** iris controls are reversed.

4.26

PTZ

PTZ options are sorted into Settings Groups 1 through 2.

Settings Group 1 has the following settings:

Auto Pan Speed

Continuously pans the camera at a speed between right and left limit settings. Type a value between 1 and 60 (expressed in degrees), inclusive. The default setting is 30.

Standard Tour Period

Select the length of time for a standard tour. Default: 5 s.

PTZ Fixed Speed

Select the desired fixed speed of PTZ functions of the camera. Default value: 4.

Inactivity

Selects the time period the camera must be not controlled until the inactivity event will be executed.

- **Off** (default): camera remains on a current scene indefinitely.
- **Scene 1**: camera returns to Preset 1.
- **Previous Aux**: camera returns to the previous activity.

Inactivity Period

Determines the behavior of the camera when the control for camera is inactive. Select a time period from the pull-down list (3 sec. - 10 min.). The default setting is 2 minutes.

Auto Pivot

The Auto Pivot tilts the camera through the vertical position as the camera is rotated to maintain the correct orientation of the image. Set the Auto Pivot to On (default) to rotate the camera 180° automatically when following a subject traveling directly beneath the camera. To disable this feature, click Off.

Settings Group 2 has the following settings:

Orientation

The orientation of the camera. Options: Normal, Inverted, Canted.

Freeze Frame

Holds a preposition video frame while moving to another preposition. Options: On, Off.

4.27

Display

Display options are sorted into Settings Groups 1 through 3.

Settings Group 1 has the following settings:

Title OSD

Controls how the OSD displays sector or shot titles. Options: Momentary (default), On, Off.

Camera OSD

Controls how the OSD displays camera response information, such as Digital Zoom, Iris open/close, and Focus near/far.. Options: On, Off.

Language

Select the language in which to display the text in the configuration settings.

Display Position

Select the number that corresponds with the desired display position. Default: 0.

OSD Brightness

Set the brightness of the on-screen display (OSD).

Settings Group 2 has the following settings:

Scene #

The number of the scene.

Title

The title of the scene.

In Tour

Options: Yes, No

Sector#

The number of the sector

Title

The title of the sector

Blanking

Select On to activate sector blanking. Select Off to deactivate sector blanking.

Settings Group 3 has the following settings:

Custom Tour Period

Select the amount of time that the custom tour should run. Options are: 3s, 4s, 5s (default), 10s, 15s, 20s, 25s, 30s, 40s, 50s, 1 min, 2 min, 3 min, 4 min, 5 min, 10 min.

Added Scenes

This column displays the list of added scenes. To reorder the sequence of scenes, click the up or down arrows below this column.

Available Scenes

Click Download to populate the list in this column. From this list, select any or all of the scenes to add, and then click the left arrow button between the Added Scenes column and the Available Scenes column to add the scene(s) to the Added Scenes column.

4.28 Alarm

4.28.1 Input Options

Input 1

Type
Alarm input 1

Alarm Input
N.O.

AUX
1

Type

Select the name of the alarm input.

Alarm input

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

4.28.2 Output Options

Output 1

Type
OSD

Alarm Output
N.O.

Shot
1

Name

Type

Select the name of the alarm output.

Alarm Output

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

4.28.3

Alarm Rules

Alarm Rule 1

Enabled Yes No

Name

Input Options

Input # 1

Input option

Output Options

Output # 1

Output option

Output period

The encoder features an alarm rule engine. In its simplest form, an alarm rule can define which input(s) activate which output(s). An alarm rule allows you to customize the encoder to respond automatically to different alarm inputs.








To configure an alarm rule, specify one input from either a physical connection, a motion detection trigger, or from a connection to the camera's Livepage. The physical input connection can be activated by dry contact devices such as pressure pads, door contacts and similar devices. Next, specify up to two (2) rule outputs, or the camera's response to the input. Outputs include a physical alarm relay, an AUX command, or a preposition scene.

1. Click the Enabled check box to activate the alarm.
2. Enter the Name of the alarm rule.
3. Choose one of the following alarm inputs:
 - Alarm Input 1: a physical alarm connection.
 - Alarm Input 2: a physical alarm connection.
 - IVA/MOTION+: an alarm when IVA or motion detection is activated.
 - Connection: an alarm when an attempt is made to access the camera's IP address.

4. Select the output option:
 - None: no defined command.
 - Alarm Relay: defines a physical connection from the open collector alarm output.
 - Aux On: defines a standard or custom keyboard ON command.
Note: Only commands 1, 8, 18, 20, 43, 60, 80, 86 are supported. Support for the remaining commands is scheduled for a future release.
 - Aux Off: defines a standard or custom keyboard OFF command.
Note: Only commands 1, 8, 18, 20, 43, 60, 80, 86 are supported. Support for the remaining commands is scheduled for a future release.
 - Shot: defines a preset scene from shot 1-99.
 - Transmit: Transmits a message back to the head end (available with RS-232 serial and Bilinx connections).
5. Select the Output period, which controls the length of time the output relay is activated:
 - Follow: Alarm output will remain activated for the same amount of time the alarm input is activated
 - Latched: Alarm stays on until the operator clears it.

4.28.4

Alarm States

Alarm States		
Alarm 1		Off
Alarm 2		Off
Alarm 3		Off
Alarm 4		Off
Alarm 5		Off
Alarm 6		Off
Alarm 7		Off

This page identifies the status of each alarm set in the system.

4.29

Miscellaneous

Password

Enter a password for the encoder.

Address

Allows the appropriate camera to be operated via the numerical address in the control system. Type a number between 0000 and 9999, inclusive, to identify the camera.

Reset to Factory Defaults

Click Reset to reset the password and address to factory defaults. Click Reboot to reboot the encoder.

4.30 Logs

To save the log file information:

1. Click Download to obtain the log information. The log information populates the Logs window.
2. Click Save.
3. Navigate to the directory in which you want to store the log information.
4. Type a name for the log file and click Save.

4.31 Advanced Mode: Recording

4.32 Storage Management

Storage Management

Device manager

Managed by VRM

Recording media

iSCSI Media

iSCSI IP address: 192.168.0.123

Password:

Read

Storage overview

192.168.0.123

- [-] 192.168.0.123
 - [-] IDX 0 - iqn.2007-01.com.bosch.de:fwm.iscsi.disk1
 - [-] LUN 0 - Size 10000 MB - Locked by iqn.2005-12.com.bosch:uvrm00075f71ca30
 - [-] LUN 1 - Size 40000 MB - Owner
 - [-] LUN 2 - Size 30000 MB - Locked by iqn.2005-12.com.bosch:uvrm00075f76a975
 - [-] IDX 1 - iqn.2007-01.com.bosch.de:fwm.iscsi.disk0
 - [-] LUN 0 - Size 10000 MB - Owner
 - [-] LUN 1 - Size 10000 MB - Locked by iqn.2005-12.com.bosch:uvrm00075f71dc99

Managed storage media

Target	Media Type	Size [MB]	Status	Rec. 1	Rec. 2
192.168.0.123 / 0 / 1	iSCSI system	39936	Online	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Overwrite older recordings Recording 1 Recording 2

Add Remove Edit Set

You can record the images from the camera connected to the encoder on the local SD card or on an appropriately configured iSCSI system.

SD cards are the ideal solution for shorter storage times and temporary recordings, for example alarm recordings or local buffering in the event of network interruptions.

For long-term, authoritative images, it is essential that you use an appropriately sized iSCSI system.

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

Device manager

If you have added the device to a VRM system, the VRM Video Recording Manager will manage all recording. In this case the Managed by VRM box is checked and you will not be able to configure any further settings here.

Recording media

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

iSCSI Media

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



NOTICE!

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

1. Enter the IP address of the required iSCSI target in the iSCSI IP address field.
2. If the iSCSI target is password protected, enter this into the Password field.
3. Click the Read button. The connection to the IP address will be established. In the Storage overview field, you can see the corresponding logical drives.

Local Media

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

Activating and configuring storage media

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



CAUTION!

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

1. In the Recording media section, click the iSCSI Media and Local Media tabs to display the applicable storage media in the overview.
2. In the Storage overview section, double-click the required storage medium, an iSCSI LUN or one of the other available drives. The medium is then added to the Managed storage media list. In the Status column, newly added media are indicated by the status Not active.
3. Click the Set button to activate all media in the Managed storage media list. In the Status column, these are indicated by the status Online.
4. Check the box in the Rec. 1 or Rec. 2 column to specify which recording should be recorded on the storage media selected.

5. Check the boxes for the Overwrite older recordings option to specify which older recordings can be overwritten once all the available memory capacity has been used.

**CAUTION!**

If older recordings are not allowed to be overwritten when the available memory capacity has been used, the recording in question will be stopped. You can specify limitations for overwriting old recordings by configuring the retention time (see *Section 4.34 Retention Time*, page 62).

Formatting storage media

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

**CAUTION!**

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

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

Deactivating storage media

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

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

4.33 Recording Profiles

Recording Profiles

Day Night Weekend

Stream profile settings

Stream 1 Low bandwidth

Stream 2 Low bandwidth

Settings for selected recordings

Camera	Recording	Standard recording	Alarm recording
Camera 1	1	Stream 1	Stream 1
Camera 1	2	Stream 1	Stream 1

Recording includes Metadata

Standard recording Continuous Stream Stream 1

Alarm recording

Pre-alarm time 0 s

Post-alarm time 0 s

Alarm stream Stream 1

encoding interval and bit rates from profile: High resolution 1

Alarm triggers

Alarm input 1 2 3 4

Analysis alarm 1

Video loss alarm 1

Virtual alarm 1 2 3 4

Export to FTP Configure FTP server

Copy Settings Default Set

You can define up to ten different recording profiles. You will then use these recording profiles in the recording scheduler, where they are linked with the individual days and times (see *Section 4.35 Recording Scheduler, page 63*).



NOTICE!

You can change or add to the recording profile description on the tabs on the Recording Scheduler page (see *Section Time periods, page 64*).

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

Stream profile settings

You can select the profile setting that is to be used for each data stream in the event of recordings. This selection is independent of the selection for live data stream transmission (see *Section 4.21 Encoder Streams, page 47*).

The properties of the profiles are defined on the Encoder Profile page (see *Section 4.20 Encoder Profile, page 44*).

Settings for selected recordings

The settings in this settings group only refer to the recordings selected in the list field. You can select both recordings.

Recording includes

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

**CAUTION!**

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

Standard recording

Here you can select the mode for standard recordings.

If you select Continuous, the recording proceeds continuously. If the maximum memory capacity is reached, older recordings will automatically be overwritten. If you select the Pre-alarm option, the unit uses a special recording mode for optimal usage of storage capacity: As soon as a time window for alarm recording begins, recording takes place continuously on one segment that corresponds in size to a complete alarm sequence (pre- and post-alarm time). This segment functions in a similar manner to a ring buffer and is overwritten until an alarm is actually triggered. Then, recording occurs on the segment only for the duration of the preset post-alarm time and a new segment is subsequently used in the same manner.

If you select Off, no automatic recording takes place.

**CAUTION!**

You can specify limitations for overwriting older recordings in Continuous mode by configuring the retention time (see *Section 4.34 Retention Time, page 62*).

Stream

Here you can select the data stream that is to be used for standard recordings. You can select the data stream for alarm recordings separately and independently of this (see *Section Alarm stream, page 61*).

Pre-alarm time

You can select the required pre-alarm time from the list field. This parameter is only accessible if you have selected the Pre-alarm option under Standard recording.

Post-alarm time

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

Alarm stream

Here you can select the data stream that is to be used for alarm recordings. You can select the data stream for standard recordings separately and independently of this (see *Section Stream, page 61*).

encoding interval and bit rates from profile:

You can select an alternative encoding interval for the data stream for alarm recordings. Otherwise the encoding interval of the selected encoder profile is used (see *Section 4.20 Encoder Profile, page 44*).

Export to FTP

Select this parameter if you want all alarm recordings to be exported to an FTP server automatically. Make sure to have inserted all relevant data for FTP posting (see *Section 4.46 FTP Posting, page 79*).

Alarm input / Analysis alarm / Video loss alarm

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

**NOTICE!**

The alarm inputs are configured and activated on the Alarm Inputs page (see *Section 4.28.1 Input Options, page 54*).

The numbering of the checkboxes for the alarm inputs corresponds to the labeling of the alarm inputs on the encoder.

Virtual alarm

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

**NOTICE!**

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

4.34**Retention Time**

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

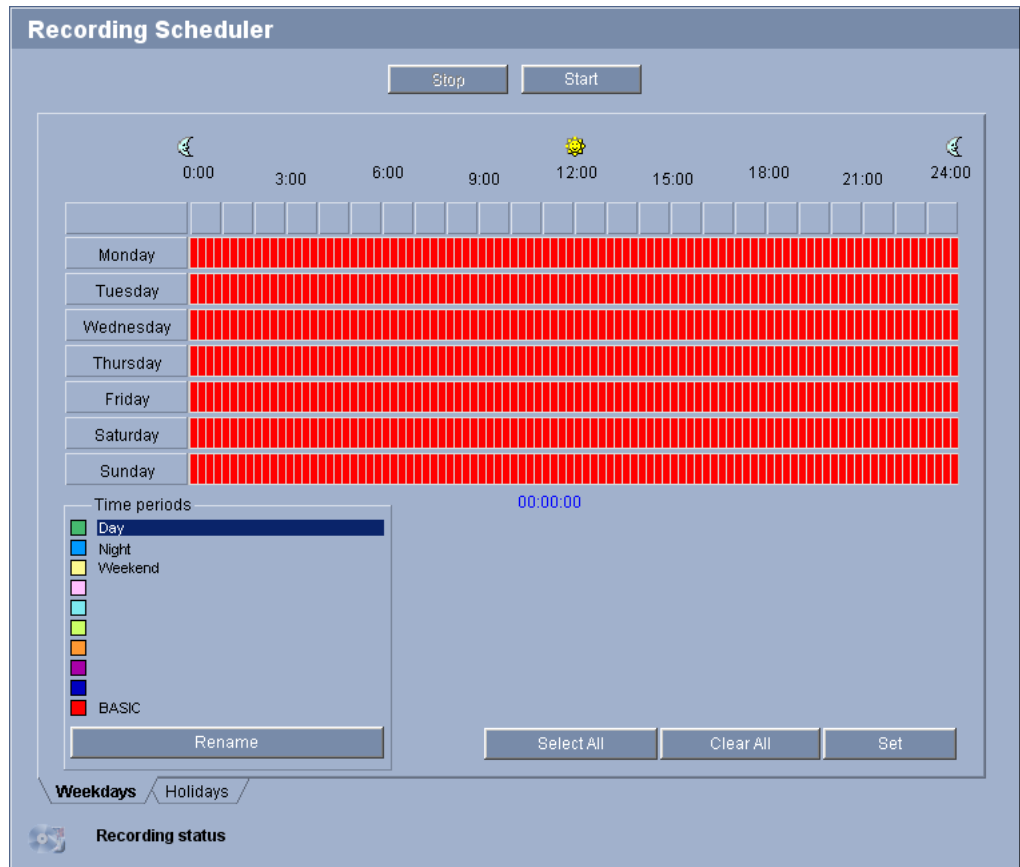
**NOTICE!**

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

Recording 1 / Recording 2

Enter the required retention time in hours or days for each recording.

4.35 Recording Scheduler



The recording scheduler allows you to link the created recording profiles with the days and times at which the camera's images are to be recorded in the event of an alarm. You can link any number of 15-minute intervals with the recording profiles for each day of the week. Moving the mouse cursor over the table displays the time below it. This aids orientation.

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

1. Click the profile you want to link in the Time periods field.
2. Click in a field in the table, hold down the mouse button and drag the cursor over all the periods to be assigned to the selected profile.
3. Use the right mouse button to deselect any of the intervals.
4. Click the Select All button to link all time intervals to the selected profile.
5. Click the Clear All button to deselect all of the intervals.
6. When you are finished, click the Set button to save the settings in the unit.

Holidays

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

1. Click the Holidays tab. Any days that have already been selected will be shown in the table.
2. Click the Add button. A new window will open.

3. Select the desired date from the calendar. You can select several consecutive calendar days by holding down the mouse button. These will later be displayed as a single entry in the table.
4. Click OK to accept the selection. The window will close.
5. Assign the individual holidays to the recording profiles, as described above.

Deleting holidays

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

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

Time periods

You can change the names of the recording profiles.

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

Activating the recording

After completing configuration you must activate the recording scheduler and start the recording. The configuration can be changed at any time.

1. Click Start to activate the recording scheduler.
2. Click Stop to deactivate the recording scheduler. Running recordings are interrupted.

Recording status

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

4.36

Recording Status

Recording Status		
	Recording 1	Recording 2
Status	Offline	Offline
Last error	None	None
Recording target	0.0.0.0	0.0.0.0
Media		
Bit rate	0 kbps	0 kbps

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

4.37 Advanced Mode: Alarm

4.38 Alarm Connections

Alarm Connections

Connect on alarm	<input type="text" value="Off"/>	▼
Number of destination IP address	<input type="text" value="1"/>	▼
Destination IP address	<input type="text" value="0.0.0.0"/>	
Destination password	<input type="text"/>	
Video transmission	<input type="text" value="UDP"/>	▼
Stream	<input type="text" value="1"/>	▼
Remote port	<input type="text" value="80"/>	▼
Video output	<input type="text" value="First available"/>	▼
Decoder	<input type="text" value="First available"/>	▼
SSL encryption	<input type="text" value="Off"/>	▼
Auto-connect	<input type="text" value="Off"/>	▼

You can select how the encoder 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 encoder will connect in sequence in the event of an alarm, until a connection is made.

Connect on alarm

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

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



NOTICE!

In the default setting, Stream 1 is transmitted for alarm connections. Bear this fact in mind when assigning the profile (see *Section 4.20 Encoder Profile, page 44*).

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 Bosch Video Management System, you can store a general password here. The encoder can use this general password to connect to all remote stations protected with the same password. In this case, proceed as follows:

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

**NOTICE!**

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

Video transmission

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

**CAUTION!**

Please note that in some circumstances, a larger bandwidth must be available on the network for additional video images in the event of an alarm, in case multicast operation is not possible. To enable multicast operation, select the UDP option for the Video transmission parameter here (see *Section 4.45 Multicast, page 77*).

Stream

Select the stream for transmission in case of an alarm.

Remote port

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

Video output

If you know which unit is being used as the receiver, you can select the analog video output to which the signal should be switched. If the destination unit is unknown, it is advisable to select the First available option. In this case, the image is placed on the first free video output. This is an output on which there is no signal. The connected monitor only displays images when an alarm is triggered. If you select a particular video output and a split image is set for this output on the receiver, you can also select from Decoder the decoder in the receiver that is to be used to display the alarm image.

**NOTICE!**

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

Decoder

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

SSL encryption

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



NOTICE!

Please note that the SSL encryption must be activated and configured at both ends of a connection. This requires the appropriate certificates to be uploaded onto the encoder (see *Section SSL certificate, page 82*).

You can activate and configure encryption of the media data (video, audio, and metadata) on the Encryption page (see *Section 4.48 Encryption, page 80*).

Auto-connect

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



NOTICE!

In the default setting, Stream 1 is transmitted for automatic connections. Bear this fact in mind when assigning the profile (see *Section 4.20 Encoder Profile, page 44*).

Audio

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

4.39

VCA

The screenshot displays the VCA configuration interface. On the left, the 'Video 1' tab is active, showing various settings: 'VCA configuration' set to 'Profile #1', 'Preset' set to 'Off', 'Alarm status' set to 'Off', 'Aggregation time [s]' set to 0, and 'Analysis type' set to 'MOTION+'. Under the 'Motion detector' section, 'Sensitivity' is at 100, 'Minimum object size' is at 4, and 'Debounce time 1 s' is unchecked. The 'Tamper detection' section has 'Global change' set to 50, with checkboxes for 'Global change', 'Scene too bright', 'Scene too dark', and 'Scene too noisy', all of which are checked. At the bottom are 'Load...', 'Save...', 'Default', and 'Set' buttons. On the right, a live video feed shows a room with several cameras on tripods.

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

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

1. Select a VCA profile and enter the required settings.
2. If necessary, click the Default button to return all settings to their default values.
3. Click the Save... button to save the profile settings to a file. A new window is opened, in which you can specify where you want to save the file and what name you want to save it under.
4. Click the Load... button to load a saved profile. A new window opens in which you can select the profile file and specify where to save the file.

You can switch off the video content analysis completely if the device's full power is to be made available for the encoder.

VCA configuration

Select one of the profiles here to activate it or edit it. The **Silent MOTION+** configuration is active by default. In this configuration, metadata is created to facilitate searches of recordings; however, no alarm is triggered. You can rename the profile.

1. To rename the file, click the icon to the right of the list field and enter the new profile name in the field.
2. Click the icon again. The new profile name is saved.



CAUTION!

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

Preset

Options are: Off, or any of the presets that have already been saved

Alarm status

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

Aggregation time [s]

You can set an aggregation time of between 0 and 20 seconds if necessary. The aggregation time always starts when an alarm event occurs. It extends the alarm event by the value set. This prevents alarm events that occur in quick succession from triggering several alarms and successive events in a rapid sequence. No further alarm is triggered during the aggregation time.

Note that the value for the pre-alarm time must be greater than the value for the aggregation time, so that also the alarm event is recorded. The post-alarm time set for alarm recordings only starts once the aggregation time has expired (see *Section 4.33 Recording Profiles*, page 60).

Analysis type

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

**NOTICE!**

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

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

Metadata is always created for a video content analysis, unless this was explicitly excluded. Depending on the analysis type selected and the relevant configuration, additional information overlays the video image in the preview window next to the parameter settings. With the **MOTION+** analysis type, for example, the sensor fields in which motion is recorded will be marked with rectangles.

**NOTICE!**

On the LIVEPAGE Functions page, you can also enable additional information overlays for the LIVEPAGE (see *Section 4.15 LIVEPAGE Functions, page 41*).

Motion detector (MOTION+ only)

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

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

**CAUTION!**

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

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

Sensitivity (MOTION+ only)

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

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

Minimum object size (MOTION+ only)

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

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

Debounce time 1 s (MOTION+ only)

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

Select Area (MOTION+ only)

The areas of the image to be monitored by the motion detector can be selected. The video image is subdivided into square sensor fields. Each of these fields can be activated or deactivated individually. If you wish to exclude particular regions of the camera's field of view

from monitoring due to continuous movement (by a tree in the wind, etc.), the relevant fields can be deactivated.

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

Global change

You can set how large the global change in the video image must be for an alarm to be triggered. This setting is independent of the sensor fields selected under Select Area. Set a high value if fewer sensor fields need to change to trigger an alarm. With a low value, it is necessary for changes to occur simultaneously in a large number of sensor fields to trigger an alarm.

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

Global change

Activate this function if the global change, as set with the Global change slide control, should trigger an alarm.

Scene too bright

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

Scene too dark

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

Scene too noisy

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

4.40 Alarm E-Mail

Alarm E-Mail

Send alarm e-mail	Off ▼
Mail server IP address	<input style="width: 90%;" type="text"/>
SMTP user name	<input style="width: 90%;" type="text"/>
SMTP password	<input style="width: 90%;" type="text"/>
Format	Standard (with JPEG) ▼
Image size	Small ▼
Attach JPEG from camera	<input type="checkbox"/>
Destination address	<input style="width: 90%;" type="text"/>
Sender name	<input style="width: 90%;" type="text"/>
Test e-mail	<input style="margin-right: 20px;" type="button" value="Send Now"/> <input type="button" value="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 encoder automatically sends an e-mail to a previously defined e-mail address.

Send alarm e-mail

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

Mail server IP address

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

SMTP user name

Enter a registered user name for the chosen mailserver here.

SMTP password

Enter the required password for the registered user name here.

Format

You can select the data format of the alarm message.

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



CAUTION!

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

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

Image size

The size of the image. Options are: Small, Medium, Large.

Attach JPEG from camera

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

Destination address

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

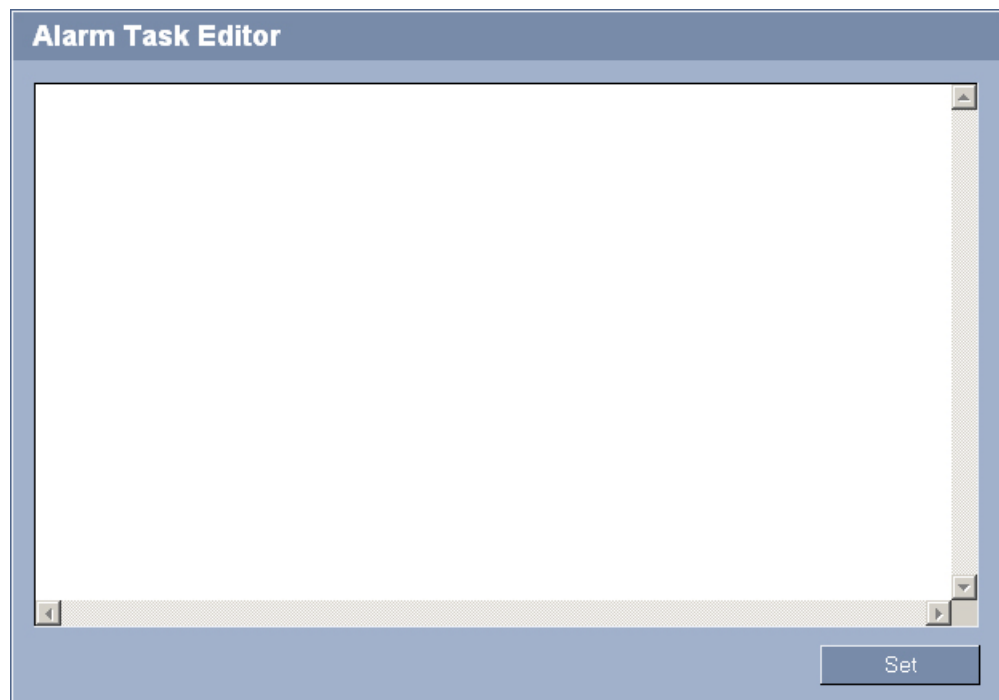
Sender name

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

Test e-mail

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

4.41 Alarm Task Editor



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.

4.42 Advanced Mode: Network

4.43 Network Access

Network

DHCP

Automatic IP assignment

Ethernet

IPv4

IP address

Subnet mask

Gateway address

IPv6

IP address

Prefix length

Gateway address

DNS server address

[Details >>](#)

DynDNS

Enable DynDNS

Host name

User name

Password

Force registration now

Status DynDNS function switched off

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

1. Make the desired changes.
2. Click the Set and Reboot button. The encoder is rebooted and the changed settings are activated.



CAUTION!

If you change the IP address, subnet mask or gateway address, the encoder 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 encoder. Certain applications (for example, Bosch Video Management System) use the IP address for the unique assignment of the unit. If you use these applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be

appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

Ethernet

Fill in the fields for the appropriate IP version: IPv4 or IPv6.

IP address

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

Subnet mask

For IPv4 only, enter the appropriate subnet mask for the selected IP address here.

Prefix length

For IPv6 only, enter the number of characters in the prefix.

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 resolve a mail or FTP server address specified as a name. Enter the IP address of the DNS server here.

**NOTICE!**

Click the Details button to reveal the rest of the fields in this page.

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 encoder 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 encoder 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 encoder, click the Register button.

Status

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

4.44**Advanced**

Advanced

SNMP
SNMP
1. SNMP host address
2. SNMP host address
SNMP traps

802.1x
Authentication
Identity
Password

RTSP
RTSP port

UPnP
UPnP

TCP metadata input
TCP port
Sender IP address

Quality of service
Video
Control
Alarm video
Post-alarm time

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 encoder is rebooted and the changed settings are activated.

SNMP

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

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

1. SNMP host address / 2. SNMP host address

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

SNMP traps

You can select which traps are to be sent.

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

Authentication

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

To configure the unit, you must connect the encoder directly to a computer. This is because communication via the network is not enabled until the Identity and Password parameters have been set and successfully authenticated.

Identity

Enter the name that the RADIUS server is to use for identifying the encoder.

Password

Enter the password that is stored in the RADIUS server.

RTSP port

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

UPnP

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



NOTICE!

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

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

TCP port

The device can receive data from an external TCP sender, for example an ATM or POS device, and store it as metadata. Select the port for TCP communication. Select Off to deactivate the TCP metadata function.

Sender IP address

Enter the IP address of the TCP metadata sender here.

Quality of Service

The encoder offers Quality of Service (QoS) configuration options to ensure fast network response to PTZ data and images. Quality of Service (QoS) is the set of techniques to manage network resources. QoS manages the delay, delay variation (jitter), bandwidth, and packet loss parameters to guarantee the ability of a network to deliver predictable results. QoS identifies the type of data in a data packet and divides the packets into traffic classes that can be prioritized for forwarding.

Consult with your network administrator for assistance configuring the **Video**, **Control**, and the **Alarm Video** settings.

Post-alarm time

The length of time post-alarm. Options range from 0s to 3h.

4.45**Multicast**

	Enable	Multicast Address	Port	Streaming
Video 1	<input type="checkbox"/>	0.0.0.0	60001	<input type="checkbox"/>

Stream 1 | Stream 2

Multicast packet TTL: 64 Set

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

**NOTICE!**

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

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

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

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

**NOTICE!**

The settings must be made individually for each stream.

Enable

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

Multicast Address

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

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

**NOTICE!**

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

Port

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

Enter the port address of the required stream here.

Streaming

Click the checkbox to activate multicast streaming mode for the relevant stream. An enabled stream is indicated by a check mark. The device even streams multicast data if there is no active connection.

Streaming is typically not required for standard multicast operation.

Multicast packet TTL

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

4.46 FTP Posting

FTP Posting

JPEG posting

Image size: Small

File name: Overwrite

Posting interval: 0 s (0 = Off)

FTP server

FTP server IP address: 0.0.0.0

FTP server login: [text input]

FTP server password: [text input] Check

Path on FTP server: [text input] Browse

Max. bit rate: 10000 kbps

Set

You can save individual JPEG images on an FTP server at specific intervals. You can then retrieve these images at a later date to reconstruct alarm events if required. The resolution corresponds to the highest setting from the two data streams. Furthermore, you can export selected recordings manually from the RECORDINGS page or activate the automatic export of alarm recordings on the Recording Profiles settings page.

Image size

The size of the image. Options are: Small, Medium, Large.

File name

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

- Overwrite
The same file name is always used and any existing file will be overwritten with the current file.
- Increment
A number from 000 to 255 is added to the file name and automatically incremented by 1. When it reaches 255 it starts again from 000.
- Date/time suffix
The date and time are automatically added to the file name. When setting this parameter, ensure that the unit's date and time are always correctly set. Example: the file snap011005_114530.jpg was stored on October 1, 2005 at 11:45 and 30 seconds.

Posting interval

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

FTP server IP address

Enter the IP address of the FTP server.

FTP server login

Enter your login name for the FTP server.

FTP server password

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

Path on FTP server

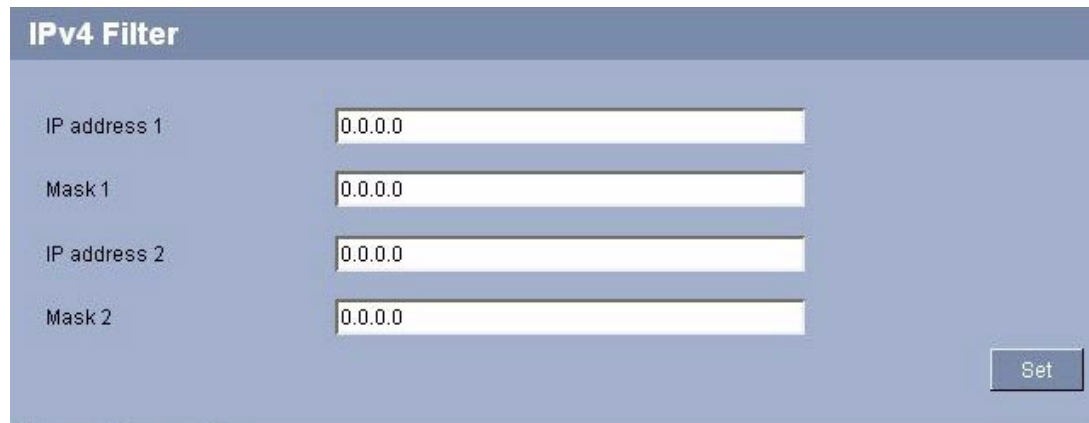
Enter the exact path on the FTP server.

Max. bit rate

You can limit the bit rate for FTP posting.

4.47

IPv4 Filter



IP address 1	<input type="text" value="0.0.0.0"/>
Mask 1	<input type="text" value="0.0.0.0"/>
IP address 2	<input type="text" value="0.0.0.0"/>
Mask 2	<input type="text" value="0.0.0.0"/>

This page allows configuration of an IPv4 filter that allows or blocks network traffic that matches a specific IP address and subnet mask.

IP address 1

The IP address of the network from which the network traffic is coming.

Mask 1

The subnet mask that corresponds to IP address 1.

IP address 3

The IP address of the network to which the network traffic is going.

Mask 2

The subnet mask that corresponds to IP address 2.

4.48

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 4.51 Licenses, page 83*).

4.49 Advanced Mode: Service

4.50 Maintenance

Maintenance			
Firmware	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Upload"/>
Progress	<input type="text" value="0%"/>		
Configuration	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Upload"/>
			<input type="button" value="Download"/>
SSL certificate	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Upload"/>
Download logfile			<input type="button" value="Download"/>
Upload history			<input type="button" value="Show"/>

Firmware

The encoder 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 encoder can be serviced and updated remotely without a technician having to change the installation on site.

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



CAUTION!

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

You should never interrupt the installation of firmware. An interruption can lead to the flash-EEPROM 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 Search to locate and select the file.
3. Next, click Upload to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

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

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

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

Configuration

You can save configuration data for the encoder 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 Search to select the required file.
2. Make certain that the file to be loaded comes from the same unit type as the unit you want to configure.
3. Next, click Upload to begin transferring the file to the unit. The progress bar allows you to monitor the transfer.

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

Download

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

SSL certificate

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

If you wish to upload multiple files onto the encoder, 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 Search 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 encoder (for example **192.168.0.10/reset**).

The new SSL certificate is valid.

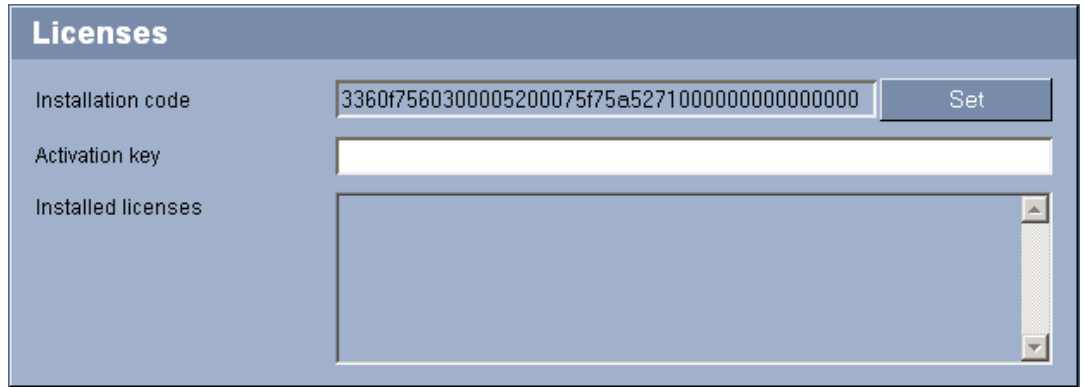
Download logfile

You can download an internal maintenance log from the unit to send it to Customer Service for support purposes. When doing this, ensure that HTTPS browser port is not set to Off and TLS 1.0-support is activated for your browser. Click Download and select a storage location for the file.

Upload history

Click Show to display the upload history.

4.51 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.

4.52 System Overview



System Overview	
Hardware version	F0004C40
Firmware version	45500551
Device type	MIC VIP
IP address	192.168.0.20
Audio option	No
Storage medium attached	No
Initiator name	iqn.2005-12.com.bosch.unit00075f79d395
MAC address	00-07-5F-79-D3-95
Major version number	5.51
Build number	45
Stream 1	High resolution 1
Stream 2	Low bandwidth
Temperature	100°F / 37.5°C (max 114°F / 45.5°C)
Serial number	044000120105010018

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.

4.53 Function test

The encoder 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 encoder operates as expected in the event of an alarm.

Your check should include the following functions:

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

5 Operation

5.1 Function test

The encoder 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 encoder operates as expected in the event of an alarm. Your check should include the following functions, some of which are detailed in this chapter:

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

5.2 The LIVEPAGE

Once the connection is established, the Web browser displays the LIVEPAGE. It shows the live video image on the right of the browser window. Depending on the configuration, various text overlays may be visible on the live video image (see *Section 4.12 Display Stamping, page 39*). Other information may be shown next to the live video image on the LIVEPAGE. The display depends on the settings on the LIVEPAGE Functions page (see *Section 4.15 LIVEPAGE Functions, page 41*).

Display stamping

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



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



Alarm flag set on media item



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



Gap; no video recorded



Watermarking not valid



Watermarking flag set on media item



Motion flag set on media item



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

Image selection

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

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

View Control

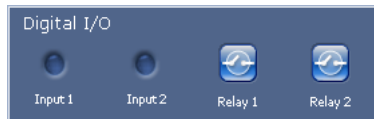
Control options for peripherals (for example a pan/tilt head or dome camera) depend on the type of unit installed and on the configuration of the encoder.

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



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

Digital I/O

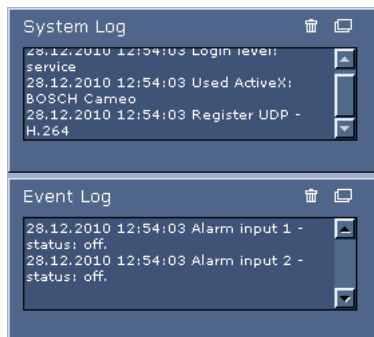


The alarm icons **Input 1** and **Input 2** are for information purposes and indicate the status of an alarm input: When an alarm is triggered, the corresponding icon lights up blue. The unit's configuration determines whether the alarm is displayed, as well as additional details (see *Section 4.15 LIVEPAGE Functions, page 41*).

Triggering relay

You can switch connected units using the relays in the encoder (for example lights or door openers). To activate this, click the icon for the corresponding relay next to the video image. The icon will be red when the relay is activated.

System Log / Event Log



The System Log field contains information about the operating status of the encoder and the connection. You can save these messages automatically in a file (see *Section 4.15 LIVEPAGE Functions, page 41*).

Events such as the triggering or end of alarms are shown in the Event Log field. You can save these messages automatically in a file (see *Section 4.15 LIVEPAGE Functions, page 41*).

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

5.3 Saving snapshots

You can save individual images from the video sequence currently shown on the LIVEPAGE in JPEG format on your computer's hard drive. The icon for recording single images is only visible if the unit is configured to enable this process (see *Section Allow snapshots, page 42*).

- ▶ Click the icon. The image is saved at a resolution of 704 × 576 pixels (4CIF). The storage location depends on the configuration of the encoder (see *Section Path for JPEG and video files, page 42*).



5.4 Recording video sequences

You can save sections of the video sequence currently shown on the LIVEPAGE on your computer's hard drive. The icon for recording video sequences is only visible if the unit is configured to enable this process (see *Section Allow local recording, page 42*).

1. Click the icon to start recording. The storage location depends on the configuration of the encoder (see *Section Path for JPEG and video files, page 42*). A red dot in the icon indicates that recording is in progress.



2. Click the icon again to stop recording.

Image resolution

Sequences are saved at the resolution that has been preset in the configuration for the encoder (see *Section 4.20 Encoder Profile, page 44*).

5.5 Running recording program

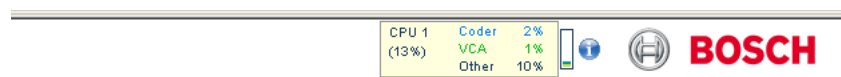
The hard drive icon below the camera image on the LIVEPAGE changes during an automatic recording.



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

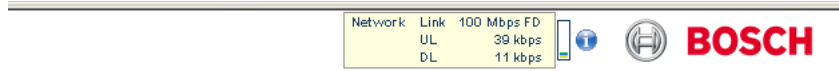
5.6 Processor load

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



You can obtain additional information to help you when troubleshooting or fine tuning the unit. The values indicate the proportions of the individual functions on the encoder load, shown as percentages. Move the cursor over the graphic indicator. Some additional numerical values are also displayed.

5.7 Network connection



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

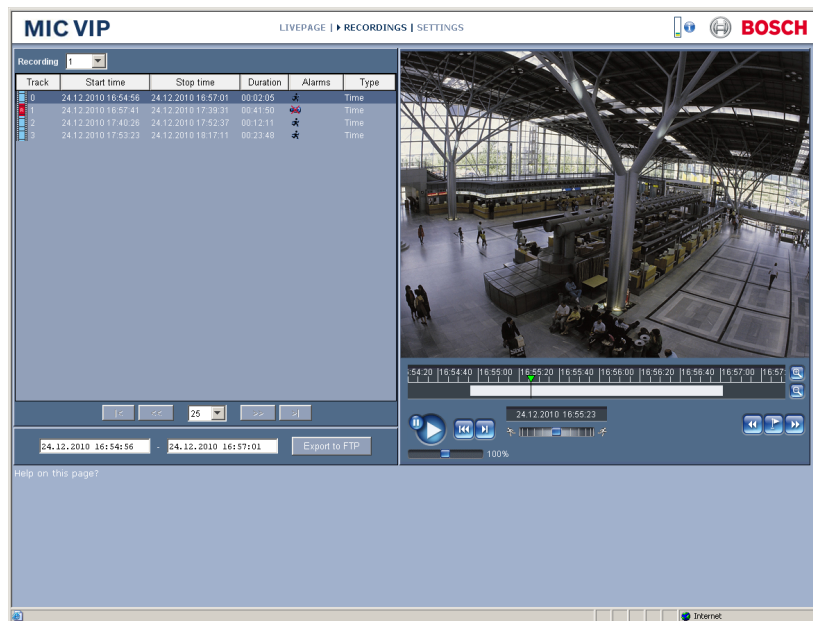
Link	Ethernet link type
UL	Uplink, speed of the outgoing data traffic
DL	Downlink, speed of the incoming data traffic

5.8 The RECORDINGS page

The RECORDINGS page for playing back recorded video sequences can be accessed from the LIVEPAGE and from the SETTINGS menu.

The RECORDINGS link is only visible if a storage medium has been selected (see *Section 4.32 Storage Management, page 57*).

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



Selecting recordings

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

1. Select **1** or **2** from the Recording list. (The contents for 1 and 2 are identical, only the quality and location may be different.)
2. Use the arrow buttons below the list to browse the list.

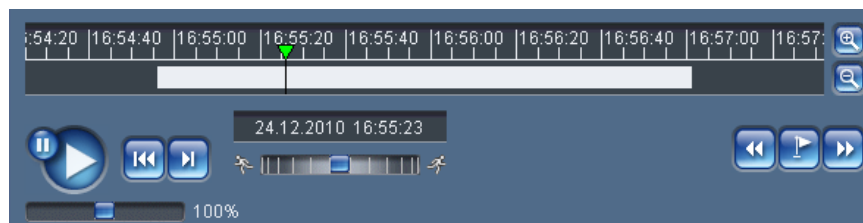
3. Select the number of entries that are displayed simultaneously.
4. Click a list entry. The playback for the selected track starts immediately in the video window.

Exporting recordings

You can export tracks or sequences to an FTP server. The FTP server is defined on the FTP Posting settings page.

1. In the list, select the tracks you want to export.
2. If required, change the times within the selected range. To do so, drag the mouse over the time bar or enter the values in the text fields next to the Export to FTP button.
3. Click Export to FTP to send the selected recordings to the FTP server. The information below the button allows you to monitor the export.

Controlling a playback



You will see a time bar below the video image for quick orientation. A green arrow above the bar indicates the position of the image currently being played back within the sequence.

The time bar offers various options for navigation.

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

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

Buttons

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



Start or pause playback



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



Leap to the start of the next video sequence

Slide controls

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



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



Bookmarks

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



Jump to the previous bookmark



Set bookmark



Jump to the following bookmark



NOTICE!

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

5.9

Operation using software decoders

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

The video server is also designed for use with the DiBos 8 digital recorder.

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

6 Maintenance and upgrades

6.1 Testing the network connection

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

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

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

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

6.2 Unit reset

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



CAUTION!

All configured settings will be discarded during a reset.

If necessary, back up the current configuration using the Download button on the Maintenance configuration page (see *Section 4.50 Maintenance, page 81*).



NOTICE!

After a reset, the unit can only be addressed via the factory default IP address. The IP address can be changed as described in the **Installation** chapter (see *Section 3.10 Assign an IP Address, page 26*).

1. If necessary, back up the current configuration using the Download button on the Maintenance configuration page (see *Section 4.50 Maintenance, page 81*).
2. Using a pointed object, press the Factory Reset button located below the SD slot until the **POWER** LED flashes red (see *Figure 3.8*). All settings will revert to their defaults.
3. Change the IP address of the encoder if necessary.
4. Configure the unit to meet your requirements.

6.3 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 4.52 System Overview, page 83*). 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 Download logfile, page 82*).

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

6.4 General malfunctions

Malfunction	Possible causes	Recommended solution
No connection between the unit and terminal program.	Incorrect cable connections.	Check all cables, plugs, contacts, terminals and connections.
	The computer's serial interface is not connected.	Check the other serial interface.
	Interface parameters do not match.	If necessary select a different interface and make sure that the computer's interface parameters match those of the unit. Try the following standard parameters: 19,200 baud, 8 data bits, no parity, 1 stop bit. Next, disconnect the unit from the power supply and reconnect it again after a few seconds.
No image transmission to remote station.	Camera error.	Connect local monitor to the camera and check the camera function.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
	Incorrect encoder stream property set for connection to hardware decoder.	Select the H.264 BP+ bit-rate-limited option on the Encoder Streams configuration page.
No connection established, no image transmission.	The unit's configuration.	Check all configuration parameters.
	Faulty installation.	Check all cables, plugs, contacts and connections.
	Wrong IP address.	Check the IP addresses (terminal program).
	Faulty data transmission within the LAN.	Check the data transmission with ping .
	The maximum number of connections has been reached.	Wait until there is a free connection and then call the sender again.
The unit does not report an alarm.	Alarm source is not selected.	Select possible alarm sources on the Alarm Inputs configuration page.
	No alarm response specified.	Specify the desired alarm response on the Alarm Connections configuration page, change the IP address if necessary.
Control of cameras or other units is not possible.	The cable connection between the serial interface and the connected unit is not correct.	Check all cable connections and ensure all plugs are properly fitted.
	The interface parameters do not match those of the other unit connected.	Make sure that the settings of all units involved are compatible.

Malfunction	Possible causes	Recommended solution
The unit is not operational after a firmware upload.	Power failure during programming by firmware file.	Have the unit checked by Customer Service and replace if necessary.
	Incorrect firmware file.	Enter the IP address of the unit followed by /main.htm in your Web browser and repeat the upload.
Placeholder with a red cross instead of the ActiveX components.	JVM not installed on your computer or not activated.	Install Sun JVM from the product CD.
Web browser contains empty fields.	Active proxy server in network.	Create a rule in the local computer's proxy settings to exclude local IP addresses.
The POWER LED flashes red.	Firmware upload failed.	Repeat firmware upload.

6.5 Fiber Optic Module

Issue	Symptom	Resolution
No data present	No Power	Check power to the module: <ul style="list-style-type: none"> – If Green LED is present, then Check power to CNFE2MC: <ul style="list-style-type: none"> – If Power LED is Green, then check data link
	Invalid Fiber Link	Check fiber connection to the module: <ul style="list-style-type: none"> – If Red LED is present, then the fiber link is missing. If the LED is Flashing Red, then Check the fiber connection to the CNFE2MC: <ul style="list-style-type: none"> – If the Link/Act LED is not lit, then the fiber link is missing.
No Video present	RJ-45 Connection	Check the PWR/Link on the module: <ul style="list-style-type: none"> – If the LED is slowly Flashing Red, then Check all video connections from the camera. <ul style="list-style-type: none"> – If the LED is rapidly Flashing Red, then Check the RJ-45 connector on the module: <ul style="list-style-type: none"> – If the right LED (Green) is not lit, then no data is present at this RJ-45 connection. – If no LED lit on the RJ-45 connector, then there is a fault with this connector, the RJ-45 cable, or the cable is not connected to the CNFE2MC. Check the RJ-45 connector on the CNFE2MC: <ul style="list-style-type: none"> – If the right LED (Green) is not lit, then no data is present at this RJ-45 connection. – If no LED lit on the RJ-45 connector, then there is a fault with this connector, the RJ-45 cable, or the cable is not connected to the module.

6.6 Malfunctions with iSCSI connections

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

6.7 LEDs

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

POWER LED

Does not light up: Encoder is switched off.

Lights up green: Encoder is switched on.

Lights up red: Startup in progress.

Flashes green: Video connection established.

Flashes red: Encoder is faulty, for example following failed firmware upload.

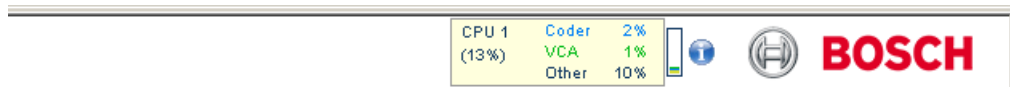
10/100 Base-T RJ45 socket

Green LED lights up: Network connection established.

Orange LED lights up: Data transmission via network connection.

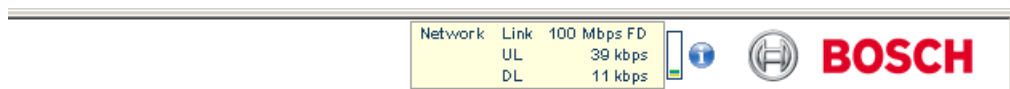
6.8 Processor load

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



You can obtain additional information to help you when troubleshooting or fine tuning the unit. The values indicate the proportions of the individual functions on the encoder load, shown as percentages. Move the cursor over the graphic indicator. Some additional numerical values are also displayed.

6.9 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

6.10 Terminal block

The terminal block has several contacts for:

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

Pin assignment serial interface

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

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

Pin assignment I/O

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

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

6.11 Communication with terminal program

Data terminal

If the encoder cannot be found in the network or the connection to the network is interrupted, you can connect a data terminal to the encoder 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 encoder (see *Section Pin assignment serial interface, page 95*).

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



NOTICE!

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

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

Configuring the terminal

Before the terminal program can communicate with the encoder, 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 encoder to access the main menu. Other submenus and functions can be accessed using the on-screen commands.

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

Assigning an IP address

Before you can operate the encoder in your network you must first assign it an IP address that is valid for your network.

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

1. Start a terminal program such as HyperTerminal.
2. Enter the user name **service**. The terminal program displays the main menu.
3. Enter command **1** to open the **IP** menu.
4. Enter **1** again. The terminal program displays the current IP address and prompts you to enter a new IP address.
5. Enter the desired IP address and press Enter. The terminal program displays the new IP address.
6. Use the displayed commands for any additional settings you require.



NOTICE!

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

Reboot

Briefly interrupt the power supply to the encoder 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.

6.12 Transfer and disposal

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.

6.13 Repairs

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.

6.14 Copyrights

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

Copyright 1984-1989, 1994 Adobe Systems Incorporated.

Copyright 1988, 1994 Digital Equipment Corporation.

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

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

Bosch Security Systems, Inc.

850 Greenfield Road
Lancaster, PA 17601
U.S.A.

www.boschsecurity.com

© Bosch Security Systems, Inc., 2012