BOSCH

Videojet connect 7000

VJC-7000-90

en Installation Manual

Table of contents

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 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.

1.3 Safety Precautions

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

⚡

Danger!
High risk: 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!
Medium risk: Indicates a potentially hazardous situation. If not avoided, this may result in minor or moderate injury.

⚠

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

ℹ

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

1.4 Important Safety Instructions

Damage requiring service – Unplug the devices from the main AC power source and refer servicing to qualified service personnel whenever any damage to the device has occurred, such as:
- the power supply cable is damaged;
- an object has fallen on the device;
- the device has been dropped, or its enclosure has been damaged;
- the device does not operate normally when the user follows the operating instructions correctly.

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

Grounding:
- Connect outdoor equipment to the unit's inputs only after this unit has had its ground terminal connected properly to a ground source.
- Disconnect the unit's input connectors from outdoor equipment before disconnecting the 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, size of grounding conductors, location of discharge unit, connection to grounding electrodes, and requirements for the grounding electrode.

Installation location - The unit is intended only for installation in a Restricted Access Location.

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)*.

Overvoltage – Installation category (also called Overvoltage Category) specifies the level of mains voltage surges that the equipment will be subjected to. The category depends upon the location of the equipment, and on any external surge protection provided. Equipment in an industrial environment, directly connected to major feeders/short branch circuits, is subjected to Installation Category III. If this is the case, a reduction to Installation Category II is required. This can be achieved by use of an isolating transformer with an earthed screen between primary and secondary, or by fitting listed Surge Protective Devices (SPDs) from live to neutral and from neutral to earth. Listed SPDs shall be designed for repeated limiting of transient voltage surges, suitable rated for operating voltage and designated as follows:
- Type 2 (Permanently connected SPDs intended for installation on the load side of the service equipment overcurrent device)
- Nominal Discharge Current (In) 20 kA min.

For example: FERRAZ SHAWMUT, STT2240SPG-CN, STT2BL240SPG-CN rated 120/240 VAC, (In=20 kA)

Power disconnect - An appropriate disconnect device shall be provided external to the equipment.

Surge suppression - Use proper surge suppression on your network video, power, audio, and alarm cables.

Warning!
Short-circuit (overcurrent) protection device required
This product relies on the building's installation for short-circuit (overcurrent) protection.
Ensure that the protective device is Listed rated not greater than: 20 A.

1.5 Important Notices

Notice!
This device is intended for use in public areas only.
U.S. federal law strictly prohibits surreptitious recording of oral communications.

Notice!
This is a **class A** 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 device complies with part 15 of the FCC Rules. Operation is subject to the following conditions:

- this device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to Part 15 of the FCC Rules and ICES-003 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a **commercial environment**. This equipment generates, uses, and radiates radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his expense.
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.

1.6 Customer Support and Service

If this unit needs service, contact the nearest Bosch Security Systems Service Center for authorization to return and shipping instructions.

Service Centers

USA

Telephone: 800-366-2283 or 585-340-4162
Fax: 800-366-1329
Email: cctv.repair@us.bosch.com

Customer Service

Telephone: 888-289-0096
Fax: 585-223-9180
Email: security.sales@us.bosch.com

Technical Support

Telephone: 800-326-1450
Fax: 585-223-3508 or 717-735-6560
Email: technical.support@us.bosch.com

Repair Center

Telephone: 585-421-4220
Fax: 585-223-9180 or 717-735-6561
Email: security.repair@us.bosch.com

Canada

Telephone: 514-738-2434
Fax: 514-738-8480

Europe, Middle East & Africa Region

Please contact your local distributor or Bosch sales office. Use this link:
http://www.boschsecurity.com/startpage/html/europe.htm

Asia Pacific Region

Please contact your local distributor or Bosch sales office. Use this link:
http://www.boschsecurity.com/startpage/html/asia_pacific.htm

More Information

For more information please contact the nearest Bosch Security Systems location or visit www.boschsecurity.com

2 Unpacking

- This equipment should be unpacked and handled with care. Check the exterior of the packaging for visible damage. If an item appears to have been damaged in shipment, notify the shipper immediately.
- Verify that all the parts listed in the Parts List below are included. If any items are missing, notify your Bosch Security Systems Sales or Customer Service Representative.
- Do not use this product if any component appears to be damaged. Please contact Bosch Security Systems in the event of damaged goods.
- The original packing carton is the safest container in which to transport the unit and must be used if returning the unit for service. Save it for possible future use.

2.1 Parts List

Each device ships with the following parts:

- One (1) VIDEOJET connect 7000 enclosure with three (3) M16 plugs, three (3) ¾” blanking plugs, and five (5) M16 gland locknuts installed
- Parts bag with:
  - one (1) terminal plug connector, 2-pin [for connections to optional washer]
  - one (1) terminal plug connector, 3-pin [for AC mains power input]
  - one (1) terminal plug connector, 6-pin [for alarm inputs]
  - one (1) terminal plug connector, 7-pin [for alarm outputs and for the supervised alarm input]
  - three (3) watertight M16 cable glands with O-rings
- Installation Manual

2.2 Additional Tools Required

Installers must provide the following items to complete installation of VIDEOJET connect 7000.

- Phillips-head screwdriver, M6, for the four (4) captive lid screws (M6 x 35), and for the M6 mounting screws (if mounting is desired)
- Ring crimp tool (Davico type DHCR15 or equivalent)

2.3 Additional Hardware Required

- Four (4) M6 mounting screws and washers (if mounting is desired)
- Power cable
- Ethernet cable (Cat5e/Cat6e rated to 350 MHz)
- Metal conduit suitable for containing cables external to the enclosure
- One (1) 2.2K ohm (Ω) end-of-line terminating resistor [for the supervised alarm input, if desired]

2.4 Optional Accessories

- SFP-based fiber optic modules (1GB only) such as:
  - Agilent, SFP-GE-SX-MM850-A HFBR5710LP 7
  - Cisco, GLC-LH-SM 1300nm
  - Cisco, GLC-SX-MM 850nm 8
  - Finisar, FTLF8519P2BTL 850nm

3 Product Overview

The device VIDEOJET connect 7000 (VJC-7000-90) is a full-featured network power supply unit that can operate a variety of Bosch PTZ cameras such as MIC7000. The device includes one (1) HPoE network connection, two (2) standard network interfaces for connections to additional IP devices, one (1) slot for an optional CompactFlash (CF) memory card, two (2) slots for use with SFP-based fiber optic modules, alarm/washer control interfaces*, and audio in.

Specification	**Value**
Power requirements	100 VAC - 240 VAC (90 VAC - 264 VAC with tolerance considered), 50/60 Hz; 56V output
Alarm inputs *	Four (4) normal dry contacts (selectable N.O./N.C.) Monitored supervised alarm input (Alarm 1), 2.2K ohm (Ω) end-of-line terminating resistor
Alarm outputs *	Three (3) open collector outputs, 32 VDC, 150 mA
Audio *	One (1) mono line in; one (1) mono line out
connector	3.5 mm stereo jack
signal line in	9 kohm typical, 5.5 Vpp max. 25

signal line out	3.0 Vpp at 10 kohm typical;
	2.3 Vpp at 32 ohm typical;
	1.7 Vpp at 16 ohm typical

Washer driver output *	Dry contact relay, 250 V, 5 A
Washer switch *	Push button to activate/test the washer relay momentarily
Communication	Three (3) 10BASE-T/100BASE-TX/1000Base-TX. If SFP fiber optic modules installed: two (2) 1000 BASE-FX
Local storage	One (1) slot for an optional CompactFlash (CF) memory card, Type I / Type II, True IDE Mode, 1 TB max (user-supplied)
SFP (small form-factor pluggable)	Two (2) slots for use with SFP-based fiber optic modules (1 GB only) as recommended in the section *Optional Accessories, page 10*

The device provides the following features:

- HD-Base T PoH dedicated for one RJ45 Ethernet connection between the device and a Bosch IP camera powered by PoE/High PoE
- a push button on the PBCA to allow users to activate/test a connected washer pump accessory * (optional, user-supplied)
- ability to control connected cameras using the built-in web browser of the device
- support for daisy chaining a maximum of 50 units (based on specific conditions)

*** Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

Notice!
A MIC7000 camera connected to VIDEOJET connect 7000 requires firmware version 5.93 or later. Download the firmware from https://downloadstore.boschsecurity.com.

Notice!
If a MIC7000 camera is assigned to Camera 1 in the Transcoder Setup, it becomes “bound” to the alarm inputs/outputs, the audio input/output, and the washer output provided by the VIDEOJET connect 7000 device.

Note: To achieve a distance of 100 m (328 ft) using Cat5e/Cat6e cable, Bosch recommends using cable with a minimum rating of 350 MHz.

3.1 Typical Configuration - Basic

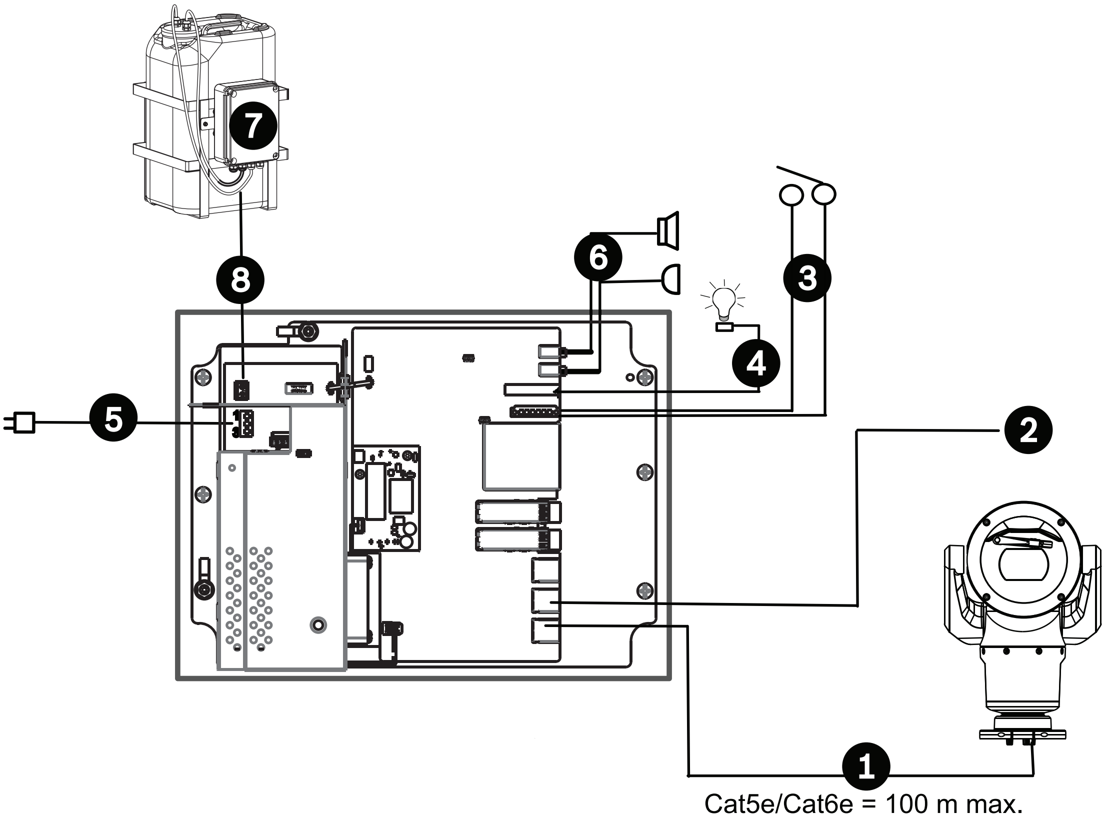


Figure 3.1: Basic configuration with VIDEOJET connect 7000

1	Ethernet (network) cable (Cat5e/Cat6e) (user-supplied) between a Bosch camera and the port labeled *PoE* on VIDEOJET connect 7000
2	Data-only IP cable (Cat5e/Cat6e) to the head-end network **Note:** The cable to the head-end also can be fiber optic cable from one of the two SFP slots.
3	Alarm input / output interface cables (user-supplied)
4	Alarm output cables (user-supplied)
5	120 / 230 VAC, 50/60 Hz
6	Audio input / output interface cables (user-supplied)

7	External washer pump (user-supplied)
8	Washer output, 2-conductor (user-supplied)

3.2 Typical Configuration - Daisy Chain

The VIDEOJET connect 7000 is able to operate in a ‘daisy chain’ type network configuration as shown in the figure below. The number of units that can be connected to a single network link depends upon many factors. For example, a maximum of 50 units can be connected when a single MIC7000 camera is attached to each VIDEOJET connect 7000 that is set to stream a single live video at 15 fps and a single recording stream at 15 fps, and encoding bit rates to 7 Mbs maximum.
Attaching multiple cameras and increasing bit rate significantly impacts the maximum number of units that can be connected in a daisy chain network configuration. Regardless of individual device settings, it is important to keep the overall network bandwidth to less than 700 Mhz.
Reliability of the network communication can be increased by connecting both ends of the daisy chain network to the head-end switch. Because sophisticated programming (such as RSTP) must be set up in the head-end switch, this configuration is recommended for advanced network users only. By default, flow control of the VIDEOJET connect 7000 is enabled. Only advanced users should consider disabling flow control.

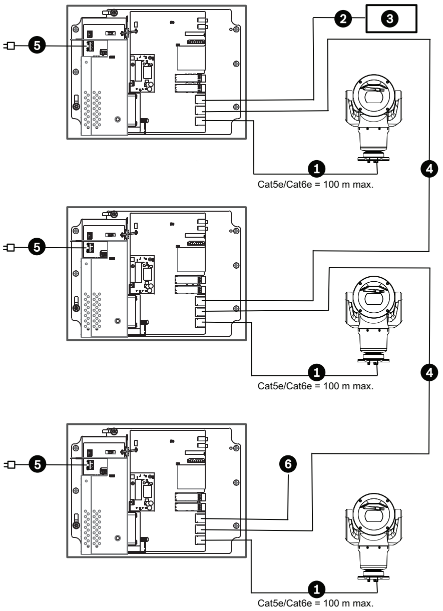


Figure 3.2: Typical daisy chain configuration for VIDEOJET connect 7000

1	Ethernet (network) cable (Cat5e/Cat6e) (user-supplied) between a Bosch camera and the port labeled *PoE* on VIDEOJET connect 7000
2	Data-only IP cable (Cat5e/Cat6e) to the head-end network **Note:** The cable to the head-end also can be fiber optic cable from one of the two SFP slots.
3	Head-end network
4	“Daisy chain” Data-only IP cable **Note:** The cable to the head-end also can be fiber optic cable from one of the two SFP slots.
5	120 / 230 VAC, 50/60 Hz

6	“Daisy chain” Data-only IP cable to the next VIDEOJET connect 7000 unit (*not shown*)

3.3 Typical Configuration - Multiple Cameras to Head-end Network

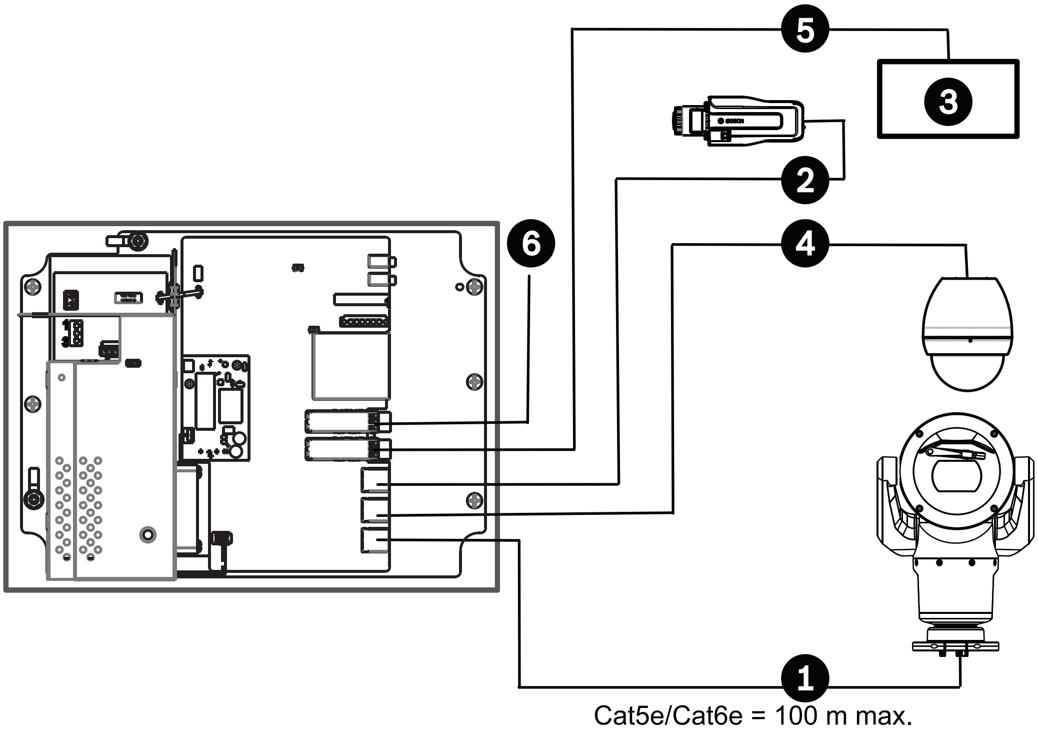


Figure 3.3: Multiple cameras to VIDEOJET connect 7000

1	Ethernet (network) cable (Cat5e/Cat6e) (user-supplied) between a Bosch camera and the port labeled *PoE* on VIDEOJET connect 7000
2	Data-only IP cable (Cat5e/Cat6e) between a Bosch IP camera and the port labeled *ETH 2* on VIDEOJET connect 7000
3	Head-end network
4	Data-only IP cable (Cat5e/Cat6e) between a Bosch camera and the port labeled *ETH 1* on VIDEOJET connect 7000
5	Fiber optic cable to the head-end network
6	Fiber optic cable to the next VIDEOJET connect 7000 unit (*if applicable*)

3.4 Typical Configuration - Mobile Viewing

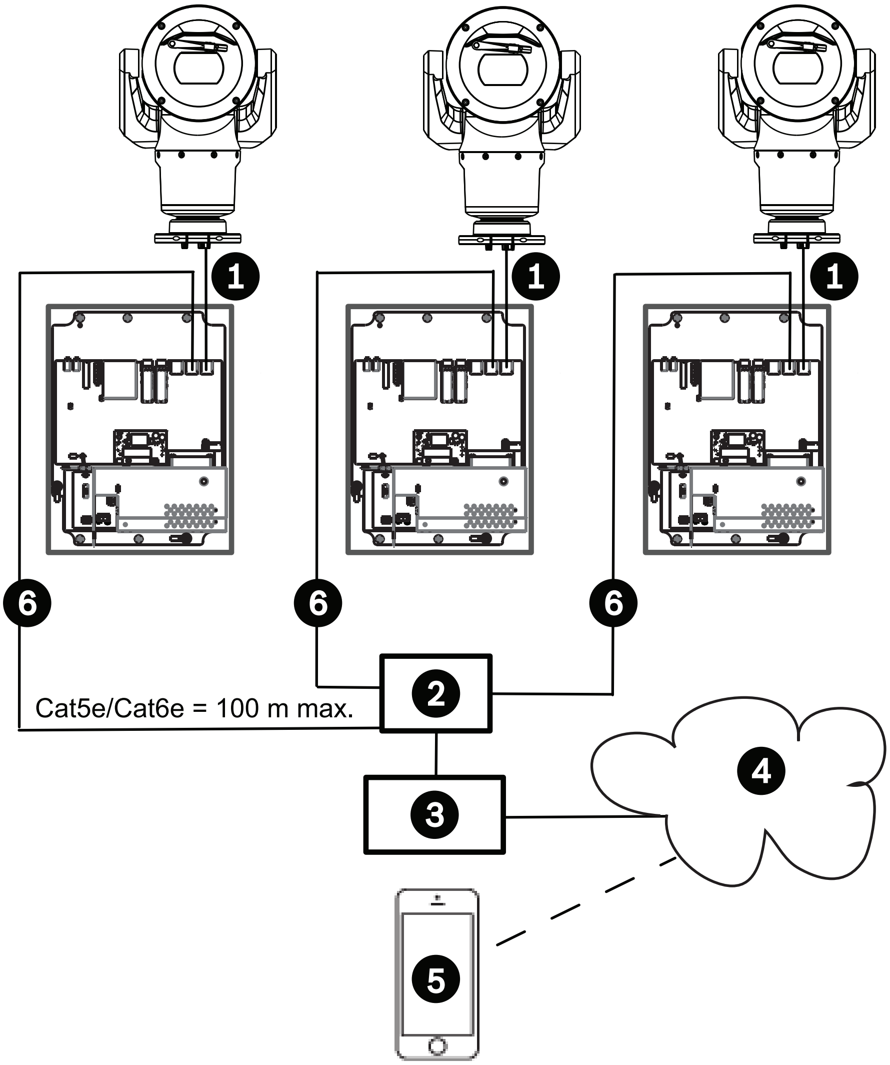


Figure 3.4: Mobile Viewing using the integrated Transcoder of VIDEOJET connect 7000

1	Ethernet (network) cable (Cat5e/Cat6e) (user-supplied) between a Bosch camera and the port labeled *PoE* on VIDEOJET connect 7000
2	Network switch (user-supplied)
3	Head-end network
4	Internet (“the cloud”)
5	Mobile device with Bosch video security app
6	Data-only IP cable to the next VIDEOJET connect 7000 unit **Note:** The cable also can be fiber optic cable from one of the two SFP slots.

4 Technical Data

4.1 Specifications

Specification	Value
Power requirements	100 VAC - 240 VAC (90 VAC - 264 VAC with tolerance considered), 50/60 Hz; 56V output
Alarm inputs *	Four (4) normal dry contacts (selectable N.O./N.C.) Monitored supervised alarm input (Alarm 1), 2.2K ohm (Ω) end-of-line terminating resistor
Alarm outputs *	Three (3) open collector outputs, 32 VDC, 150 mA
Audio *	One (1) mono line in; one (1) mono line out
connector	3.5 mm stereo jack
signal line in	9 kohm typical, 5.5 Vpp max. 25

signal line out	3.0 Vpp at 10 kohm typical;
	2.3 Vpp at 32 ohm typical;
	1.7 Vpp at 16 ohm typical

Washer driver output *	Dry contact relay, 250 V, 5 A
Washer switch *	Push button to activate/test the washer relay momentarily
Communication	Three (3) 10BASE-T/100BASE-TX/1000Base-TX. If SFP fiber optic modules installed: two (2) 1000 BASE-FX
Local storage	One (1) slot for an optional CompactFlash (CF) memory card, Type I / Type II, True IDE Mode, 1 TB max (user-supplied)
SFP (small form-factor pluggable)	Two (2) slots for use with SFP-based fiber optic modules (1 GB only) as recommended in the section *Optional Accessories, page 10*

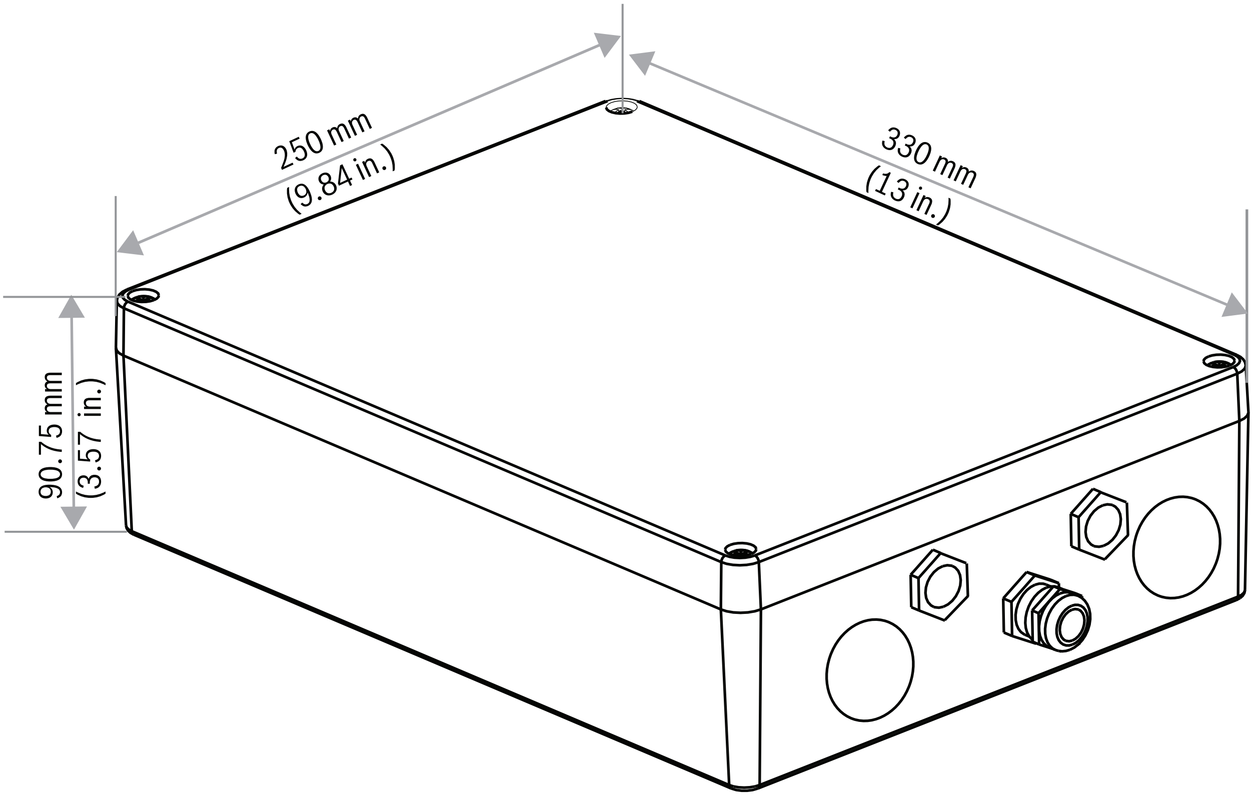
Ingress Protection Rating/ Standard	IP66, IP67, NEMA Type 4

*** Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

Notice!

If a MIC7000 camera is assigned to Camera 1 in the Transcoder Setup, it becomes “bound” to the alarm inputs/outputs, the audio input/output, and the washer output provided by the VIDEOJET connect 7000 device.

4.2 Dimensional Drawing



5 Installation

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 accepts no liability for any damages or losses caused by incorrect or improper installation.

Warning!
Overvoltage hazard
This product requires a surge protector device (SPD) or surge arrester as part of the installation to address overvoltages exceeding Overvoltage Category II, 2500 Vpk.

Note: In these steps, the item numbers in parentheses refer to the numbers in the figure in *PCBA Connections, page 21*.
Bosch recommends installing the device in a shaded location away from direct sunlight.
2. Remove the lid. Loosen the four (4) screws and remove the lid of the enclosure.

5.1 Mounting

3. Mount the device to a stable surface, if desired.

- Locate the four (4) mounting holes.
- If applicable, drill four (4) holes in the mounting surface for the mounting anchors appropriate for M6 screws, using the figure below as reference.
- Secure the enclosure to the mounting surface using four (4) M6 stainless steel screws and washers (not supplied), which fit through the large holes in the enclosure.

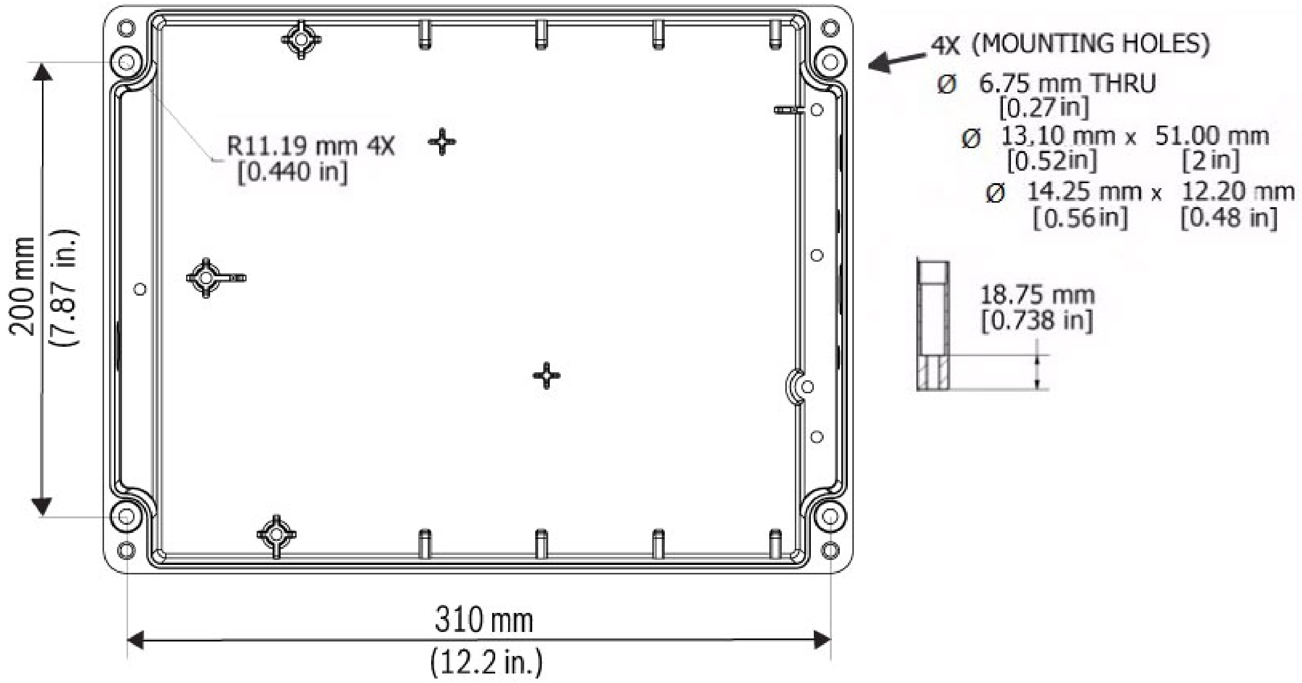


Figure 5.1: Dimensions, mounting holes, VIDEOJET connect 7000

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

5.2 Conduit Installation

4. Install cable feed-throughs.

– Based on your installation requirements, install conduit (not supplied), cable glands with O-rings, and/or plugs into the enclosure holes as needed, using the recommendations in the graphic below.

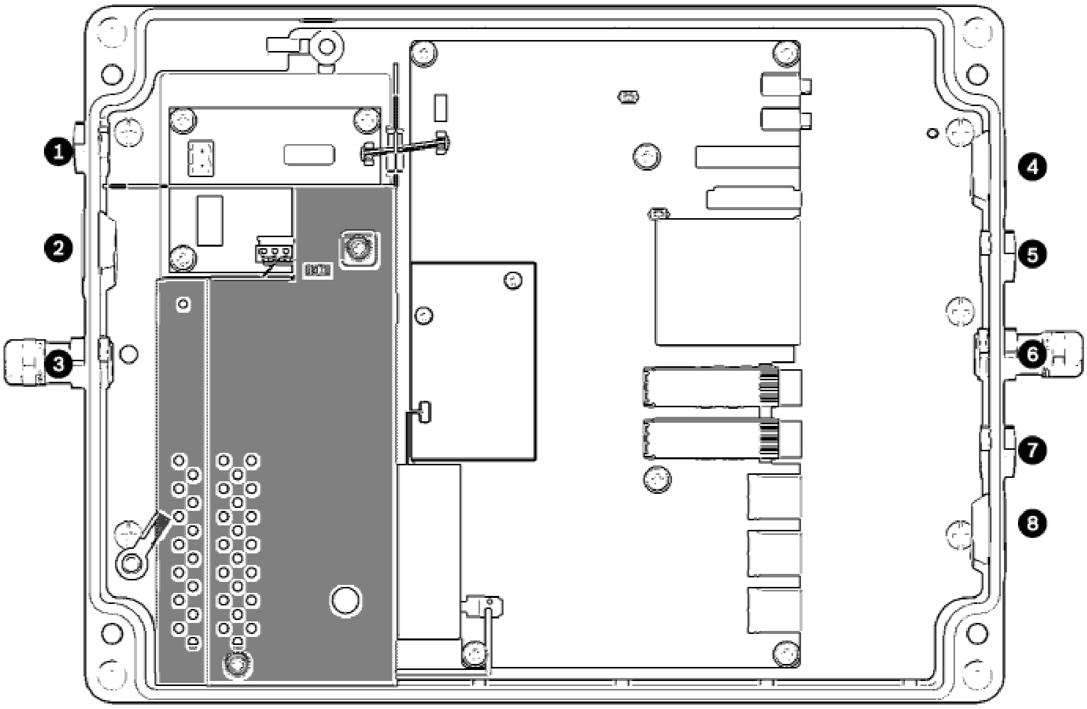


Figure 5.2: Layout of VIDEOJET connect 7000 enclosure

1	Optional hole (size M16 / ½), plugged, for cable gland intended for connections to washer*
2	Optional hole (size M25 / ¾”), plugged, for conduit (user-supplied) to AC mains power
3	Cable gland, size M16 / ½, for cable (user-supplied) to AC mains power
4	Optional hole (size M25 / ¾”), plugged, for conduit (user-supplied) for audio* and/or for alarm inputs/ outputs*, or for fiber optic cable (user-supplied)
5	Optional hole (size M16 / ½), plugged, for conduit (user-supplied) for audio* and/or for alarm inputs/ outputs*, or for fiber optic cable (user-supplied)
6	Cable gland, size M16 / ½, for data-only IP cable (Cat5e/Cat6e, user-supplied) or for fiber optic cable (user-supplied)
7	Optional hole (size M16 / ½), plugged, for conduit (user-supplied) for data-only IP cable (Cat5e/Cat6e, user-supplied) or fiber optic cable (user-supplied)
8	Optional hole (size M25 / ¾”), plugged, for conduit (user-supplied) for HPoE Ethernet (network) cable (Cat5e/Cat6e, user-supplied) to IP camera

*** Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

– Secure the conduit as recommended by the conduit manufacturer.

Note: Use the figure of the layout of the Printed Circuit Board Assembly (PCBA) on the next page as reference when completing steps 5 – 13.

5.3 PCBA Connections

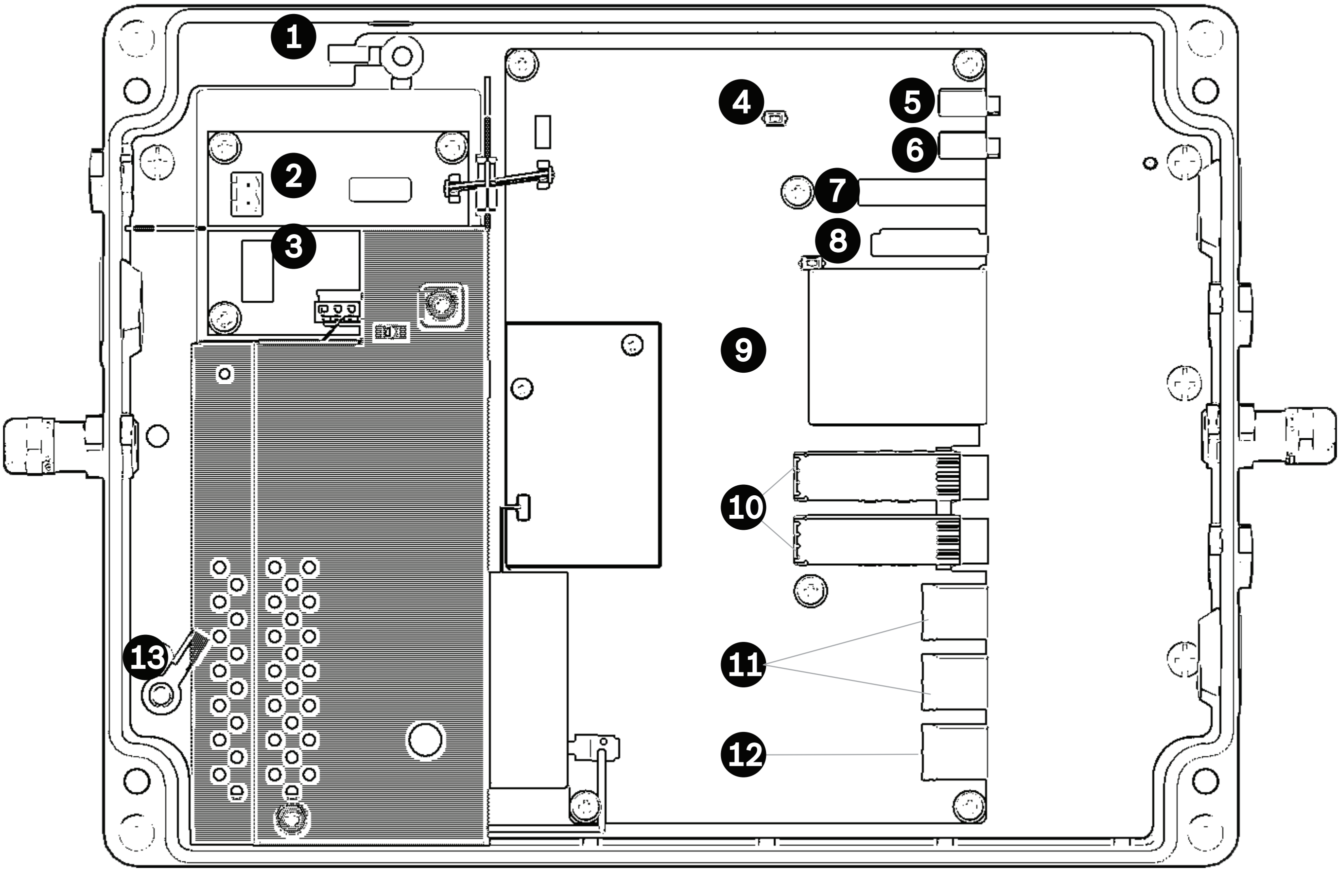


Figure 5.3: Layout of VIDEOJET connect 7000 PCBA

1	Ground lug, washer output (optional)
2	Terminal block, 2-pin [for connections to optional washer]
3	Terminal plug connector, 3-pin [for AC mains power input]
4	Push button to activate/test the washer relay momentarily
5	Audio OUT
6	Audio IN
7	Terminal plug connector, 7-pin [for alarm outputs and for the supervised alarm input]
8	Terminal plug connector, 6-pin [for alarm inputs]
9	One (1) slot for optional CompactFlash (CF) memory card, Type I / Type II, True IDE Mode, 1 TB max (user-supplied)
10	Two (2) slots for use with SFP-based fiber optic modules (1 GB only) (user-supplied)
11	Two (2) RJ45 Ethernet (female) ports (labeled *ETH1*, *ETH2*)
12	One (1) RJ45 HPoE Ethernet (female) port (labeled *PoE*)
13	Ground lug, AC mains (**required**)

5.4 Power Cable Installation

5. Connect the power cable.

- Prepare the cable as needed.
- Feed the cable through an appropriate cable gland or conduit hole near where the 3-pin terminal plug connector for the mains power cable will be installed on the PCBA (item 3).
- Connect the cable wires to the connector according to the table below.

Pin	Description / Function
1	Neutral voltage
2	*No connection*
3	Line voltage

- Check that the connections are secure.
- Carefully press the connector to the appropriate location on the PCBA.
- Ground the chassis.
  - Remove the brass nut and the top copper washer from the earth termination post (item 1 closest to item 2); set these aside.
  - Remove the ring terminal (supplied).
  - Insert the earth core from the mains cord into the ring terminal and crimp it in place.
  - Place the ring terminal onto the earth termination post on the bottom copper washer. (The ring terminal will be between the two (2) copper washers.)
  - Replace the top copper washer. Secure with the brass nut.

5.5 Ethernet Cables Installation

6. Connect the HPoE Ethernet cable.

- Feed an Ethernet cable from the IP camera through an appropriate cable gland or conduit hole near the port labeled *PoE* on the PCBA (item 12).
- Connect the cable to the port on the PCBA.

7. Connect network Ethernet cable(s), if applicable.

- Feed an Ethernet cable (Cat5e/Cat6e rated to 350 MHz) from the head-end network through an appropriate cable gland or conduit hole near the RJ45 ports labeled *ETH1* and *ETH2* (item 11).
- Connect the cable to one of the ports.
- If connecting to another network device (such as a second VIDEOJET connect 7000 unit), feed an Ethernet cable through an appropriate cable gland or conduit hole and connect it to the RJ45 port labeled *ETH2* (item 11).

5.6 Fiber Installation

8. Install SFP modules, if applicable.

- Install SFP module(s) into the SFP socket(s) (item 10). Refer to the installation instructions of the manufacturer of your chosen SFP module. Refer to the section *Optional Accessories, page 10* for recommendations.
- Feed fiber optic cable from the external device through an appropriate cable gland or conduit hole near the SFP socket(s).
- Terminate the cable.
- Connect the cable to the appropriate SFP socket(s).

5.7 Alarm Inputs

*** Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

9. Connect Alarm inputs, if applicable.

- Prepare the cable as needed.
- Feed the cable through an appropriate cable gland or conduit hole near where the 6-pin terminal plug connector for alarm inputs will be installed on the PCBA (item 8).
- Make the connections for alarm inputs (for external devices such as door contacts or sensors) to the connector according to the table below.

Pin	Description / Function		Pin	Description / Function
1	Alarm 2		4	Alarm 4
2	Ground		5	Ground
3	Alarm 3		6	Alarm 5

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.

- Make the connection for the supervised alarm input (Alarm 1), if applicable, to pin 7 of the 7-pin terminal plug connector for alarm outputs (item 7 on the PCBA).
- Attach a 2.2K ohm (Ω) end-of-line terminating resistor (user-supplied).
- Check that the connections are secure.
- Carefully press the connector to the appropriate location on the PCBA.

5.8 Alarm Outputs

* **Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

10. Connect Alarm outputs, if applicable.

- Prepare the cable as needed.
- Feed the cable through an appropriate cable gland or conduit hole near where the 7-pin terminal plug connector for alarm outputs will be installed on the PCBA (item 7).
- Make the connections for relay outputs (for switching external units such as lamps or alarm sirens) to the connector according to the table below.

Pin	Description / Function		Pin	Description / Function
1	Ground		4	Alarm Output 2
2	Alarm Output 1		5	Alarm Output 3
3	Ground		6	Ground

- Check that the connections are secure.
- Carefully press the connector to the appropriate location on the PCBA.

5.9 Washer Pump

* **Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.

11. Connect the washer pump drive, if applicable.

- Prepare the cable as needed.
- Feed the cable through the cable gland or conduit hole near where the 2-pin terminal plug connector for the washer pump connections will be installed on the PCBA (item 2).
- Make the connections to the connector according to the table below.

Pin	Description / Function
1	Relay Normally Open
2	Relay Common

- Check that the connections are secure.

- Carefully press the connector to the appropriate location on the PCBA.

5.10 Audio In and Out

*** Note**: This feature is valid only for a MIC7000 camera "bound" to Camera 1.
Note: Audio OUT is not available in initial production units. A firmware update, expected in mid-2015, is required.

12. Connect Audio IN and OUT, if applicable.

- Prepare the cable as needed.
- Feed the cable through an appropriate cable gland or conduit hole near the connectors for Audio IN and Audio OUT.
- Connect the cable for Audio IN (9 kohm typical, 5.5 Vpp max. 25) to the second audio connector (item 6).
- Connect the cable for Audio OUT (3.0 Vpp at 10 kohm typical; 2.3 Vpp at 32 ohm typical; 1.7 Vpp at 16 ohm typical) to the outermost connector (item 5).
- Check that the connections are secure.

5.11 Local Storage Media (CF Card)

13. Install a CF card to save recordings locally, if applicable.

Caution!
Bosch recommends disconnecting power to the unit whenever inserting or removing a CF card.

Carefully slide a Type I / Type II, True IDE Mode, 1 TB max CF card into the card slot (item 9) as far as it will go until it locks into place.

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

(To remove a CF card, push carefully in the direction **opposite** of insertion until the mechanical catch releases, and then remove the card.)

5.12 Final Steps

14. Verify power to the device.

- Connect the device to the power source.
- If desired, test the washer by pushing the button on the PCBA (item 4) to activate the washer pump. Note that for MIC7000, the software in the camera prevents the washer from running more than 10 seconds continuously to prevent emptying the washer bottle.

15. Complete the installation.

- Re-attach the enclosure lid.
- Tighten the four (4) lid screws to 1.5 – 3 N m (13 – 26.5 in. lb) to ensure that the enclosure is watertight.

6 Control of Connected Devices

The embedded software gives users the ability to control connected cameras using a web browser. This chapter provides details about the web browser.

6.1 System Requirements

The camera requires specific software and hardware to allow a user to view live images and to configure camera settings over a TCP/IP network. These requirements are:

- A computer with the Microsoft Windows XP, Vista, or Windows 7 operating system, network access, and the Microsoft Internet Explorer Web browser version 8.0 or later, or
- A computer with Microsoft Windows XP, Vista, or Windows 7 operating system, network access, and reception software such as the Bosch Video Management System or the Video Client, or other third party head-end video management software, or
- A compatible hardware decoder from Bosch Security Systems connected to a video monitor.

Notice!
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. In Windows Vista, deactivate protected mode on the Security tab under Internet Options.
You can find notes on using Microsoft Internet Explorer in the online Help in Internet Explorer.

If you choose to use a computer running Microsoft Internet Explorer or any of the Bosch software, the computer must conform to the following minimum requirements:

- Operating System: Windows XP (Service Pack 3) or Windows 7 (32 or 64 bits)
- Processor: Intel Pentium Quad Core, 3.0 GHz or comparable
- RAM: 2048 MB
- Free Hard Disk Space: 10 GB
- Video system: NVIDIA GeForce 8600 or higher display with a minimum of 16-bit color
- Network interface: 100/1000-BaseT
- Software:
  - Microsoft Internet Explorer, version 8.0 or higher
  - Video Client
  - DirectX 9.0c
  - Oracle Java Virtual Machine 1.6.0_26 or newer

The camera includes the means to decode the video via a web browser; however, for more advanced features such as local recording to PC, snapshot, and full screen display, you must obtain MPEG-ActiveX.
For the latest versions of the Video Client, DirectX, Oracle Java Virtual Machine, and MPEG-ActiveX software, go to *www.boschsecurity.com*, navigate to the product page for your camera, and then download the software from the Software tab.

Notice!
Ensure that the graphics card is set to 16-bit or 32-bit color. If you need further assistance, contact your PC system administrator.

6.2 Configuration Overview

When a connection is established, the **LIVE** page is initially displayed. The application title bar displays three items: **LIVE**, **PLAYBACK**, **SETTINGS**.

Note:
The **PLAYBACK** link is only visible if a storage medium has been configured for recording. (With VRM recording this option is not active.)
The **LIVE** page is used to display the live video stream and control the unit.
The **PLAYBACK** page is used for playing back recorded sequences.
The **SETTINGS** page is used to configure the unit and the application interface.

6.3 About the SETTINGS Page

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.
Not every page has a Set button. Changes to pages without a Set button are set immediately. If a page does show a Set button, you must click the Set button for a change to take effect.

⚠ **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.

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 camera reboots and the changed settings are activated.

7 General settings

7.1 Identification

7.1.1 Naming

Assign a unique name to assist in identification. This name simplifies the management of multiple devices in more extensive systems.
The name is used for remote identification, for example, in the event of an alarm. Choose a name that makes it as easy as possible to identify the location unambiguously.
You can use additional lines to enter kanji characters.

1. Click the + sign to add a new line
2. Click the icon next to the new line. A window with a character map opens.
3. Click the required character. The character is inserted into the **Result** field.
4. 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.
5. Click the < icon to the right of the **Result** field to delete the last character, or click the X icon to delete all characters.
6. Click the **OK** button to apply the selected characters to the new line of the name. The window closes.

7.1.2 ID

Each device should be assigned a unique identifier that can be entered here as an additional means of identification.

7.1.3 iSCSI Initiator extension

Add text to an initiator name to make identification easier 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 page.)

7.2 Password

The camera 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 camera 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 camera and change all configuration settings.
With the **user** authorization level, you can operate the unit and also control cameras, for example, but you cannot change the configuration.
The lowest authorization level is **live**. It can only be used to view the live video image and switch between the different live image displays.
You can define and change a password for each authorization level if you are logged in as **service** or if the unit is not password protected.
Enter the password for the appropriate authorization level here.

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

Notice!
A new password is only saved when you click the **Set** button. You should therefore click the **Set** button immediately after entering and confirming a password.

7.3 Date/Time

Date format
Select your required date format.

Device date/Device time

Notice!
Ensure that recording is stopped before synching to the PC.

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 camera.

Note: It is important that the date/time is correct for recording. An incorrect date/time setting could prevent correct recording.

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 from the database in the unit 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 save and activate the table.

Time server IP address

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

Time server type

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

8 Web Interface

8.1 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 camera.

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.

Show VCA metadata
When video content analysis (VCA) is activated, additional information is displayed in the live video stream. For example, in Motion+ mode, the sensor areas for motion detection are marked.

Show VCA trajectories
When video content analysis (VCA) is activated, check this item to show additional information that traces the path of objects.

Show overlay icons
Select this checkbox to show overlay icons on the live video image.

Video player
Select the desired video player from the list in the drop-down box. Options are “Auto detect” (default), Bosch Video SDK, Bosch Autoload Decoder, JPEG

JPEG size
You can specify the size of the JPEG image on the **LIVE** page. Options are Small, Medium, Large, 720p, 1080p, and “Best possible” (default).

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

JPEG quality
You can specify the quality at which the JPEG images appear on the **LIVE** page.

8.2 LIVE Functions

On this page you can adapt the functions on the **LIVE** page 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 **LIVE** page. The selected items are indicated by a check mark.
2. Check whether the required functions are available on the **LIVE** page.

Transmit audio

You can only select this option if audio transmission is actually switched on (see Audio).The audio signals are sent in a separate data stream parallel to the video data, and so increase the network load. The audio data are encoded according to G.711 and require an additional bandwidth of approx. 80 kbps per connection in each direction.

Show alarm inputs

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

Show alarm outputs

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

Show event log

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

Show system log

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

Show ‘Intelligent Tracking’

Show ‘Special Functions’

8.3 Logging

Save event log

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

File for event log

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

Save system log

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

File for system log

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

9 Transcoder

9.1 Transcoder Setup

Select a maximum of four cameras for which you want to offer transcoded video. Transcoding is only available for cameras configured for Recording. Ensure that these cameras will have recordings, either by configuring the cameras accordingly or by having the transcoder manage recording.

9.1.1 Device [number]

- Click the drop-down box directly below the Camera number (1, 2, 3 or 4). The system scans your network for available devices and displays the list. This list includes MIC7000 cameras, MIC IP PSU devices, and analog cameras integrated into your system through a single-channel encoder (in which case the corresponding encoder is listed for the selection).
- Select the desired device from the list. The parameters **Type**, **MAC**, and **Name** are displayed, if available.

Notice!
If a MIC7000 camera is assigned to Camera 1 in the Transcoder Setup, it becomes “bound” to the alarm inputs/outputs, the audio input/output, and the washer output provided by the VIDEOJET connect 7000 device.

9.1.2 Name

- Change the name if desired.

Do not use any special characters, for example **&**, in the name. Special characters are not supported by the system's internal management.
Note that the name here is only used for the transcoder operation. Changes here will not overwrite the name assigned to the camera or to the encoder on the corresponding **SETTINGS** page of the respective unit. The name that you enter here will be displayed in the title bar of the transcoder Web pages and in the list of available cameras on the **PLAYBACK** page. If you leave the field empty, the IP address of the unit is displayed.

9.1.3 Password

- In the field **Password**, enter the service password of the selected camera.
- Click **Set** to save the settings. For each connected camera a link is added in the title bar next to the **SETTINGS** link stating the camera number 1 to 4 and its name or IP address.

9.1.4 Http port, Https port

By default, the numbers **HTTP port** and **HTTPS port** for the camera are set automatically for each camera as an offset to the transcoder ports. The corresponding fields are marked by the white outline and the highlighted connection line. You may change the numbers, if necessary, on the page **Network Access**.

9.1.5 Configure Router

- If your router has UPnP enabled, click **Configure Router** to save the settings to the router. Otherwise, configure your router manually.

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

9.2 Transcoder Profile

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

Profile	Profile name	Maximum bit rate	Transcoding interval	Base resolution	Deblocking/ CABAC
1	High resolution 1	4000 kbps	1	Large	ON
2	High resolution 2	3000 kbps	1	Large	ON
3	Low bandwidth	1500 kbps	1	Large	ON
4	DSL	500 kbps	1	Large	ON
5	ISDN (2B)	100 kbps	1	Small	OFF
6	ISDN (1B)	50 kbps	1	Small	OFF
7	Modem	22 kbps	2	Small	OFF
8	GSM	8 kbps	4	Small	OFF

To change a profile, select it by clicking its tab and then change the parameters within that profile.
If a setting outside the permitted range for a parameter is entered, the nearest valid value is substituted when the settings are saved.

9.2.1 Profile Name

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

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

9.2.2 Maximum bit rate

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 be adjusted automatically.

9.2.3 Transcoding interval

Transcoding interval
This parameter determines the interval at which images are **encoded** and transmitted. For example, entering or selecting 4 means that only every fourth image is **encoded**, while the following there are skipped, which can be particularly advantageous for networks with low bandwidths. The image rate in (images per second (ips) appears next to the text field or slider.

9.2.4 Base resolution

Base resolution

Select the desired resolution for the video image.
The size of the video image depends on the settings of the connected device.

9.2.5 I-frame distance

I-frame distance

This parameter allows you to set the intervals in which the I-frames will be coded. 0 means auto mode, whereby the video server inserts I-frames as necessary. An entry of 3 indicates that only every third image is an I-frame. Note that the values supported depend on the **GOP structure** setting. For example, only even values are supported with IBP; if you have selected IBBP, only 3 or multiples of 3 are supported.

9.2.6 Min. P-frame QP

Min. P-frame QP

This parameter allows you to adjust the image quality of the P-frame and to define the lower limit for the quantization of the P-frames, and thus the maximum achievable quality of the P-frames. In the H.264-protocol, the Quantization Parameter (QP) specifies the degree of compression and thus the image quality for every frame. The lower the quantization of the P-frame (QP value), the higher the encoding quality (and thus the best image quality) and the lower the frame refresh rate depending on the settings for the maximum data rate under network settings. A higher quantization value results in low image quality and lower network load. Typical QP values are between 18 and 30.
The basic setting Auto automatically adjusts the quality to the settings for the P-frame video quality.

9.2.7 I/P-frame delta QP

I/P-frame delta QP

This parameter sets the ratio of the I-frame quantization (QP) to the P-frame quantization (QP). For example, you can set a lower value for I-frames by moving the slide control to a negative value. Thus, the quality of the I-frames relative to the P-frames is improved. The total data load will increase, but only by the portion of I-frames. The basic setting Auto automatically adjusts to the optimum combination of movement and image definition (focus).
To obtain the highest quality at the lowest bandwidth, even in the case of increased movement in the picture, configure the quality settings as follows:

1. Observe the coverage area during normal movement in the preview images.
2. Set the value for **Min. P-frame QP** to the highest value at which the image quality still meets your needs.
3. Set the value for **I/P-frame delta QP** to the lowest possible value. This is how to save bandwidth and memory in normal scenes. The image quality is retained even in the case of increased movement since the bandwidth is then filled up to the value that is entered under **Maximum bit rate**.

9.2.8 Deblocking filter

Deblocking filter

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

9.2.9 CABAC

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

9.3 Audio

This is the volume control for the Audio Input and Output.

Line In 1
You can set the input volume with the slider (from 0 to 31, with 0 as the default).

Line In 2
Ignore this parameter.
Note: The current GUI shows 2 Line Inputs, but only 1 is supported.
Note: Audio OUT is not available in initial production units. A firmware update, expected in mid-2015, is required.

10 Recording

10.1 Introduction to Recording

Images can be recorded to an appropriately-configured iSCSI system or, for devices with the appropriate storage slot, to a local media card such as a CompactFlash (CF) card.
CF 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 recordings when accessing an iSCSI system. This is an external program for configuring recording tasks for video servers. For further information please contact your local customer service at Bosch Security Systems.

10.2 Storage Management

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

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

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

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

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

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

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

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

Caution!
Each storage medium can only be associated with one user. If a storage medium is already being used by another user, you can decouple the user and connect the drive with the camera. 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** to specify which data stream should be recorded on the storage media selected. **Rec. 1** stores Stream 1, **Rec. 2** stores Stream 2. This means that you can record the standard data stream on a hard drive and record alarm images on the mobile CF card, for example.
5. Check the boxes for the **Overwrite older recordings** option to specify which older recordings can be overwritten once the available memory capacity has been used. **Recording 1** corresponds to Stream 1, **Recording 2** corresponds to Stream 2.

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

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

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

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

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

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

10.3 Remote Video Device

This page provides information on the current recording status of the cameras connected to VIDEOJET connect 7000. For easy identification, the IP address of the connected camera is the heading for each corresponding information block.

The data in the fields in this window may be followed by an icon. Move the cursor over the icon to show more details about each field.

10.3.1 Status

This field provides the status of the remote video device. Status descriptions include “Offline,” “Recording,” and “Running.”

10.3.2 Last error

This field identifies when the last error occurred on the remote video device.

10.3.3 Recording target

This field identifies the recording target for the respective camera. This target is also the source for the recordings available on the PLAYBACK page.

10.3.4 Bit rate

This field identifies the bit rate of the recording for the remote video device.

10.3.5 Initialize Recording

Note: This is only required if the Transcoder is going to Manage the recordings. Otherwise, the recording settings of the connected device will apply.
To configure VIDEOJET connect 7000 to manage recordings, you must initialize the recordings.

- Click **Initialize Recording** for the respective device. The **Configuration** window appears. (To initialize recording for all connected devices at once, click **Initialize All**.)
- In the Configuration window, mark the **SETTINGS** page of the remote video device that you want to configure with the recording defaults of VIDEOJET connect 7000. Generally, this means that a simple basic configuration is set which grants you most effective recording that also supports forensic search:

Recording Profiles
Select the desired Recording Profiles. Recording mode as it affects the defaults to be set. Note that only the Day tab on the Recording Profiles page is overwritten, that is the tab marked green.
- **Pre-alarm**
The best stream profile and the maximum pre-alarm time for RAM recording together with a minimum post-alarm time are selected, all available alarm triggers are activated, and metadata is included in recording.
- Continuous
The best stream profile is selected for recording, pre- and post-alarm times are deleted, all available alarm triggers are deactivated, and metadata is included in recording.

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

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

- Click Set to save the settings. The recording target is the one defined in the transcoder. Only recordings to this target will now be available on the PLAYBACK page.

10.3.6 Start/Stop Recording

- Click the respective button to start or stop the recording for a camera.

11 Alarm

11.1 Alarm Task Editor

Caution!
Editing scripts on this page overwrites all settings and entries on the other alarm pages. This procedure cannot be reversed.
In order to edit this page, you must have programming knowledge and be familiar with the information in the Alarm Task Script Language document.

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.

12 Network

The settings on these pages are used to integrate the device into a network. Some changes only take effect after a reboot. In this case **Set** changes to **Set and Reboot**.

1. Make the desired changes.
2. Click **Set and Reboot**.

The device is rebooted and the changed settings are activated.

12.1 Network Access

The settings on this page are used to integrate the camera 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 camera reboots and the changed settings are activated.

If the IP address, subnet mask, or gateway address is changed, then the device 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 camera.
Certain applications (Bosch Video Management System, Archive Player, Configuration Manager) use the IP address for the unique assignment of the unit. If you use these applications, the DHCP server must support the fixed assignment between IP address and MAC address, and must be appropriately set up so that, once an IP address is assigned, it is retained each time the system is rebooted.

IPv4
Fill in the 3 fields in this section of the screen.

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

IPv6
Consult with the network administrator before making changes to this section.

IP address
Enter the desired IP address for the camera in this field. The IP address must be valid for the network. A typical IPv6 address may resemble the following example:
2001:db8: :52:1:1
Consult the network administrator for valid IPv6 address construction.

Prefix length
A typical IPv6 node address consists of a prefix and an interface identifier (total 128 bits). The prefix is the part of the address where the bits have fixed values or are the bits that define a subnet.

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 1 / DNS server address 2

The camera is easier to access if the unit is listed on a DNS server. If you wish, for example, to establish an Internet connection to the camera, it is sufficient to enter the name given to the unit on the DNS server as a URL in the browser. Enter the IP address of the DNS server here. Servers are supported for secure and dynamic DNS.

Video transmission

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

Caution!

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

HTTP browser port

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

HTTPS browser port

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

Notice!

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

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

RCP+ port 1756

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

Telnet support

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

Interface mode ETH

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

Select the type of Ethernet link for the interface for the camera connected to the port labeled *PoE* on the PCBA of VIDEOJET connect 7000.
Depending on the device connected, it may be necessary to select a special operation type.
Options are:

- Auto
- 10 Mbps HD (half duplex)
- 10 Mbps FD (full duplex)
- 100 Mbps HD (half duplex)
- 100 Mbps FD (full duplex)

If necessary, select the type of Ethernet link for the interface for the device connected to the port labeled ETH 1 on the PCBA of VIDEOJET connect 7000.
Depending on the device connected, it may be necessary to select a special operation type.
Options are:

- Auto
- 10 Mbps HD (half duplex)
- 10 Mbps FD (full duplex)
- 100 Mbps HD (half duplex)
- 100 Mbps FD (full duplex)

Note: Do not select a baud rate for this port unless a device is connected to this port on VIDEOJET connect 7000.
If necessary, select the type of Ethernet link for the interface for the device connected to the port labeled ETH 2 on the PCBA of VIDEOJET connect 7000.
Depending on the device connected, it may be necessary to select a special operation type.
Options are:

- Auto
- 10 Mbps HD (half duplex)
- 10 Mbps FD (full duplex)
- 100 Mbps HD (half duplex)
- 100 Mbps FD (full duplex)

Note: Do not select a baud rate for this port unless a device is connected to this port on VIDEOJET connect 7000.

Network MSS (Byte)

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

iSCSI MSS (Byte)

You can specify a higher MSS value for a connection to the iSCSI system than for the other data traffic via the network. The potential value depends on the network structure. A higher value is only useful if the iSCSI system is located in the same subnet as the camera.

Network MTU (Byte)

The value in the field defaults to 1514.

12.2 DynDNS

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 camera 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.

Provider
The value in this field defaults to dyndns.org. Select another option as necessary.

Host name
Enter the host name registered on DynDNS.org for the camera 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 camera, click the **Register** button.

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

12.3 Advanced

12.3.1 Cloud-based Services

The operation mode determines how the camera communicates with Bosch Cloud-based Security and Services. For more information about these services and their availability, visit: http://cloud.boschsecurity.com

- Select **Auto** to allow the camera to poll the server a few times; if no contact is made, it stops polling.
- Select **On** to constantly poll the server.
- Select **Off** to block polling.

12.3.2 RTSP port

12.3.3 Authentication (802.1x)

To configure Radius server authentication, connect the unit directly to a computer using a network cable. If a Radius server controls access rights over the network, select **On** to activate authentication to communicate with the unit.

1. Enter the user name that the Radius server uses for the unit in the **Identity** field.
2. Enter the **Password** that the Radius server expects from the unit.

12.4 Network Management

12.4.1 SNMP

The camera supports the SNMP V1 (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages (traps) to IP addresses. It supports SNMP MIB II in the unified code.

If **On** is selected for the SNMP parameter and a SNMP host address is not entered, the device does not send the traps automatically and will only reply to SNMP requests. If one or two SNMP host addresses are entered, SNMP traps are sent automatically. Select **Off** to deactivate the SNMP function.

SNMP host addresses

To send SNMP traps automatically, enter the IP address of one or two target devices here.

SNMP traps

To choose which traps are sent:

1. Click **Select**. A dialog box appears.
2. Click the check boxes of the appropriate traps.
3. Click **Set** to close the window and send all of the checked traps.

12.4.2 UPnP

Select **On** to activate UPnP communication. Select **Off** to deactivate it.

When the Universal Plug-and-Play (UPnP) function is activated, the unit responds to requests from the network and is automatically registered on the requesting computers as a new network device. This function should not be used in large installations due to the large number of registration notifications.

Note:

To use the UPnP function on a Windows computer, both the Universal Plug-and-Play Device Host and the SSDP Discovery Service must be activated.

12.4.3 Quality of Service

The priority of the different data channels can be set by defining the DiffServ Code Point (DSCP). Enter a number between 0 and 252 as a multiple of four. For alarm video you can set a higher priority than for regular video and you can define a Post Alarm Time over which this priority is maintained.

12.5 Switch Configuration

Ethernet flow control is a mechanism for temporarily stopping the transmission of data using the PAUSE frame in order to clear the existing buffers.

By default, flow control is enabled. Bosch recommends to use it for the daisy chain configuration, but to disable it if the VIDEOJET connect 7000 unit is connected as a single unit.

To enable flow control for any or all of the RJ45 ports (POE, ETH1, ETH2) or either or both of the SFP ports (Fiber 1, Fiber 2) on the VIDEOJET connect 7000 unit, check the box under the appropriate column.

Note: Lower bandwidth links may delay the overall network

12.6 Accounts

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

Type

Select either FTP or Dropbox for the account type.

Before using a Dropbox account ensure that the time settings of the device have been correctly synchronized.

Account name

Enter an account name to be shown as the target name.

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

FTP server login
Enter your login name for the account server.

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

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

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

12.7 IPv4 Filter

To restrict the range of IP addresses within which you can actively connect to the device, fill-in an IP address and mask. Two ranges can be defined.

- Click **Set** and confirm to restrict access.

If either of these ranges are set, no IP V6 addresses are allowed to actively connect to the device.

The device itself may initiate a connection (for example, to send an alarm) outside the defined ranges if it is configured to do so.

12.8 Encryption

If an encryption license is installed, this submenu gives access to the encryption parameters.

13 Service

13.1 Installer Menu

Click **Reboot** to restart the camera.

Factory defaults
Click the **Defaults** button to restore the configuration settings defined in the camera’s web server to their default values. A confirmation screen appears. Allow 5 seconds for the camera to optimize the picture after a mode reset.

13.2 Maintenance

Upgrading your camera
The camera allows an operator to update the camera firmware via the TCP/IP network. The Maintenance page allows updates of the firmware.
For the latest firmware, go to www.boschsecurity.com, navigate to the product page for your camera, and then download the software from the Software tab.
The preferred method to update your camera is through a direct connection between the camera and a PC. This method entails connecting the Ethernet cable from the camera directly to the Ethernet port of a PC.
If the direct-connect method is not practical, you can also update the camera through a Local Area Network (LAN). You cannot, however, update the camera through a Wide Area Network (WAN) or via the Internet.

Update server
Enter the path of the server on which to perform the update. Click **Check** to verify the path.

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

⚠ **Caution!**
Before launching the firmware upload make sure that you have selected the correct upload file. Uploading the wrong files can result in the unit no longer being addressable, in which case you must replace the unit.
You should never interrupt the installation of firmware. An interruption can lead to the flash-EPROM being incorrectly programmed. This in turn can result in the unit no longer being addressable, in which case it will have to be replaced. Even changing to another page or closing the browser window leads to an interruption.

Upload

1. Enter the full path of the file to upload or click **Browse** to navigate to the required firmware file (*.fw).
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.

4. Click OK to the warning message to continue the firmware upload, or Cancel to stop the upload.
   The page displays a progress bar as the firmware is uploaded.
   Note: Once the progress bar reaches 100%, the system opens the reset page. Allow the reset page to complete its action.

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

Download

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

Configuration

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

Maintenance log

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

13.3 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.

13.4 System Overview

The data on this page are for information purposes only and cannot be changed. Keep a record of this information 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.

14 Operation via the browser

14.1 Live page

After the connection is established, the **LIVE** page is initially displayed. 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.

Other information may also be shown next to the live video image. The items shown depend on the settings on the **LIVE Functions** page.

14.1.1 LIVE page overview

There are views for video from Camera 1, Camera 2, Camera 3, Camera 4, and a Multi view that displays up to 4 connected devices.
The device VIDEOJET connect 7000 displays only M-JPEG video, not streaming live video.

14.1.2 Digital I/O

Depending on the configuration of the unit, the alarm input and the output are displayed next to the image.
The alarm symbol is for information and indicates the status of an alarm input:

- Active 1 = Symbol lights
- Active 0 = Symbol not lit.

The camera alarm output allows the operation of an external device (for example, a light or a door opener).

- To operate, click the relay symbol.

The symbol is red when the output is activated.

14.1.3 System Log / Event Log

The **System Log** field contains information about the operating status of the camera and the connection.
Events such as the triggering or the end of alarms are shown in the **Event Log** field.

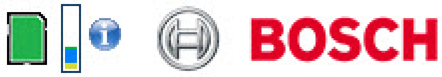
1. To view, filter and save these messages to a file, click ⧉ in the top right-hand corner.
2. To clear the log, click 🗑 in the top right-hand corner of the relevant field.

14.1.4 Recording status

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

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

14.1.5 Storage, CPU and network status



When accessing the unit with a browser, the local storage, processor and network status icons are shown in the upper right of the window next to the Bosch logo.
When a local storage card is available, the memory card icon changes color (green, orange or red) to indicate the local storage activity. If you hover over this icon with the mouse the storage activity is shown as a percentage.
If you hover over the middle icon, the CPU load is shown.
If you hover over the right-hand icon, the network load is shown.

This information can help with problem solving or when fine tuning the unit. For example:
- if the storage activity is too high, change the recording profile,
- if the CPU load is too big, change the IVA settings,
- if the network load is too big, change the encoder profile to reduce bitrate.

14.1.6 Status icons

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

Decoding error

The frame might show artifacts due to decoding errors.

Alarm flag

Indicates that an alarm has occurred.

Communication error

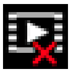
A communication error, such as a connection failure to the storage medium, a protocol violation or a timeout, is indicated by this icon.

Gap

Indicates a gap in the recorded video.

Watermark valid

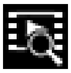
The watermark set on the media item is valid. The color of the check mark changes according to the video authentication method that has been selected.


Watermark invalid

Indicates that the watermark is not valid.

Motion alarm

Indicates that a motion alarm has occurred.


Storage discovery

Indicates that recorded video is being retrieved.

14.1.7 IP Address of Connected Devices

To the left of the status icons in the upper right corner of the window, the browser displays the IP address of each camera connected to VIDEOJET connect 7000.

14.2 Playback

Click **PLAYBACK** in the application title bar to view, search or export recordings. This link is only visible if a direct iSCSI or memory card has been configured for recording. (With VRM recording this option is not active.)

A collapsible panel on the left of the display has four tabs:
- **Track list**
- **Export**

- **Search**
- **Search results**

Select the recording number to be shown in the **Recording** drop-down menu at the top of the window.

14.2.1 Selecting recordings for playback

To see all saved sequences:

1. Click the track list tab .
2. A list of tracks with a number assigned is displayed. Start time and stop time, recording duration, number of alarms and recording type are shown for each track.
3. At the bottom of the window, select the maximum number of tracks to be displayed in the list.
4. Use the arrow buttons at the bottom to browse the list.
5. To view tracks beginning from a particular time, enter the time code and click **Get Tracks**.
6. Click a track. The playback for the selected track starts.

14.2.2 Exporting tracks

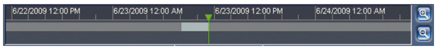
1. Select a track in the track list.
2. Click the export tab .
3. The start and stop time are filled-in for the selected track. If required, change the times.
4. Select a target.
5. Select the original or a condensed speed.
6. Click the save icon .

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

14.2.3 Searching for tracks

1. Click the search tab .
2. Click one of the **Search mode** options to define the search parameters.
3. To limit the search to a particular time range, enter the start and stop times.
4. Click **Start Search**.
5. The results are shown in the search results tab .
6. Click a result to play it back.
7. Click the search tab again to define a new search.

14.2.4 Controlling playback



The time bar below the video image allows quick orientation. The time interval associated with the sequence is displayed in the bar in gray. A green arrow above the bar indicates the position of the image currently being played back within the sequence.
The time bar offers various options for navigation in and between sequences.

- Change the time interval displayed by clicking the plus or minus icons. The display can span a range from two months to a few seconds.
- If required, click in the bar at the point in time at which the playback should begin.
- Red bars indicate the points in time where alarms were triggered.

To view the current live image, click **Now**.

Controls

Control playback by means of the buttons below the video image.

Use the jog dial to quickly scan the sequences. The time code is displayed above it.

The buttons have the following functions:

⏯ Start/Pause playback

Select the playback speed using the speed regulator: 100%

⏮ Jump to start of active sequence or to previous sequence

⏭ Jump to start of the next video sequence in the list

Bookmarks

You can set markers in a sequence and jump to these directly. 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

Bookmarks are only valid while in the **Recordings** page; they are not saved with the sequences. All bookmarks are deleted when you leave the page.

15 Configure VIDEOJET connect 7000 to Operate with a MIC7000 Camera

To configure alarm inputs and outputs, audio, and video playback for a MIC7000 camera, that camera must be “bound” to Camera 1 in the Transcoder Setup in the **SETTINGS** page of VIDEOJET connect 7000.

15.1 Configure Alarm Inputs and Outputs

To configure alarm inputs and outputs for a camera “bound” to Camera 1, follow these steps:

- On the camera, verify that the value in the field **Application variant** is set to “[camera name] – VJC-7000.” (Access the field from **Camera** > **Installer Menu** in the web browser of the camera.) This variant will align the appropriate parameters of the camera with the parameters of VIDEOJET connect 7000.
- In the device VIDEOJET connect 7000, verify that the parameters “Show alarm inputs” and “Show alarm outputs” are selected in the menu **Web Interface** > **LIVE Functions**.

Note: The **Interfaces** menu, which displays alarm inputs and outputs (alarm I/O), appears only in the configuration menu of the camera “bound” to VIDEOJET connect 7000 (the camera for which the value in the field **Application variant** is set to “[camera name] – VJC-7000”).

15.2 Configure Audio

To configure audio for a camera “bound” to Camera 1, follow these steps:

- On the camera, verify that the value in the field **Application variant** is set to “[camera name] – VJC-7000.” (Access the field from **Camera** > **Installer Menu** in the web browser of the camera.) This variant will align the appropriate parameters of the camera with the parameters of VIDEOJET connect 7000.
- In the device VIDEOJET connect 7000, select the **Transmit audio** check box in the menu **Web Interface** > **LIVE Functions**.
- In the device VIDEOJET connect 7000, set the Input volume in the menu **Transcoder** > **Audio**.

Note: The page **Camera** > **Audio** (in the configuration menu between **Miscellaneous** and **Pixel Counter**) appears only in the configuration menu of the camera “bound” to VIDEOJET connect 7000.

15.3 Configure Video Playback

To configure video playback with VIDEOJET connect 7000, first you must map the device to record. See Recording for details.

16 Troubleshooting and Maintenance

16.1 Troubleshooting

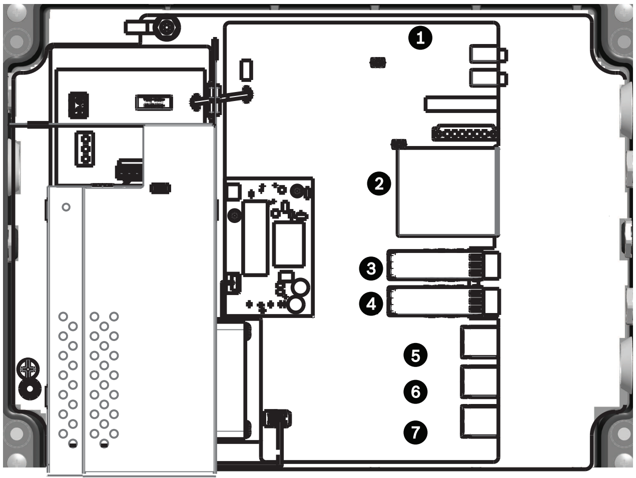


Figure 16.1: LEDs in VIDEOJET connect 7000

The table below identifies the behavior of the LEDs on the PCBA.

LED	Symbol	Function	Color/Behavior
1	D100	Power	Off: Power not applied Red: Startup in progress Green: Power/Unit is active Red flashing: System fault (for example, FW upload failed)
2	P3V3	Reserved	Factory use only. Orange: Power is applied
3	D1301	CF Recording	Off: CF not installed or not recording Orange: Recording active
4/5	D403/ D404	SFP1/ SFP2	Off: SFP not installed or not connected to a network Green: SFP installed and connected to a network Green flashing: Network traffic
6-8	D400/ D402/ D405	ETH1/ ETH2/ POE	Off: Not connected to a network / faulty cable Green: Connected to a network Green flashing: Network traffic

16.2 Maintenance

Damage requiring service – Unplug the devices from the main AC power source and refer servicing to qualified service personnel whenever any damage to the device has occurred, such as:
- the power supply cable is damaged;
- an object has fallen on the device;
- the device has been dropped, or its enclosure has been damaged;
- the device does not operate normally when the user follows the operating instructions correctly.

Servicing - Do not attempt to service this device yourself. Refer all servicing to qualified service personnel.

17 Technical data

For more specific product details, see the VIDEOJET connect 7000 datasheet.

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

Bosch Security Systems, Inc
1706 Hempstead Road
Lancaster, PA, 17601
USA