Wireless IP Camera
HD 720p

NBC-265-W

BOSCH

Table of Contents

1 Safety

1.1 Safety precautions

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 could result in minor or moderate bodily injury.

CAUTION!
Low risk: Indicates a potentially hazardous situation.
If not avoided, this could result in property damage or risk of damage to the device.

1.2   Important safety instructions

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.

1. **Cleaning -** Generally, using a dry cloth for cleaning is sufficient but a moist, fluff-free cloth or leather shammy may also be used. Do not use liquid cleaners or aerosol cleaners.
2. **Heat Sources -** Do not install the unit near any heat sources such as radiators, heaters, stoves, or other equipment (including amplifiers) that produce heat.
3. **Water -** Never spill liquid of any kind on the unit.
4. **Lightning -** Take precautions to protect the unit from power and lightning surges.
5. **Controls adjustment -** Adjust only those controls specified in the operating instructions. Improper adjustment of other controls may cause damage to the unit.
6. **Power sources -** Operate the unit only from the type of power source indicated on the label.
7. **Servicing -** Unless qualified, do not attempt to service this unit yourself. Refer all servicing to qualified service personnel.
8. **Replacement parts -** Use only replacement parts specified by the manufacturer.
9. **Installation -** Install in accordance with the manufacturer's instructions and in accordance with applicable local codes.
10. **Attachments, changes or modifications -** Only use attachments/accessories specified by the manufacturer. 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.

1.3 FCC & ICES compliance

FCC & ICES Information

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.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

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.

FCC RF Radiation Exposure Statement
The equipment complies with RF exposure limits set forth for an uncontrolled environment.
The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

1.4   UL certification

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*. 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.

1.5 CE certification

C€0700①

This indicates compliance with the R&TTE Directive 1999/5/EC
and meets the relevant parts of following technical
specifications:
ETSI EN 300 328 V1.7.1:2006
ETSI EN301489-17 V2.1.1:2009
ETSI EN301489-1 V1.8.1:2008
IEC60950-1:2005+A1:2009
EN60950-1:2006+A11:2009
EN 62311:2008
This equipment complies with CE RF radiation exposure limits
set forth for an uncontrolled environment.
This equipment should be installed and operated with a
minimum distance of 20 centimeters between the radiator and
your body.

1.6 Bosch notices

Disposal - Your Bosch product was developed and
manufactured with high-quality material and components that
can be recycled and reused. This symbol means that
electronic and electrical appliances, which have reached the
end of their working life, must be collected and disposed of
separately from household waste material. Separate collecting
systems are usually in place for disused electronic and
electrical products. Please dispose of these devices at an
environmentally compatible recycling facility, per *European
Directive 2002/96/EC*

More information

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

1.7   Copyrights

The firmware 4.1 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.

2   Introduction

2.1   Features

This WLAN HD 720p IP camera is a ready-to-use, complete network video surveillance system inside a compact camera. The camera offers a cost-effective solution for a broad range of applications. It uses H.264 compression technology to give clear images reducing bandwidth and storage.The camera can be used as a stand-alone video surveillance system with no additional equipment or it can easily integrate with the Bosch DVR 700 Series recorders.

Features include:

–   Removable SD/SDHC card offers days of storage inside camera
–   Tri-streaming: Two H.264 streams and one M-JPEG stream
–   HD 720p Progressive scan for sharp images of moving objects
–   Two-way audio and audio alarm
–   Tamper and motion detection
–   Conforms to the ONVIF standard for wide compatibility
–   Wireless LAN connection

2.2 Unpacking

Unpack carefully and handle the equipment with care.

The packaging contains:

– IP camera with lens
– Universal power supply with US, EU and UK plug
– SD card
– Camera mount kit
– Quick installation guide
– CD ROM
    – Bosch Video Client
    – Documentation
    – Tools
– Wireless antenna

If equipment has been damaged during shipment, repack it in the original packaging and notify the shipping agent or supplier.

WARNING!
Installation should only be performed by qualified service personnel in accordance with the National Electrical Code or applicable local codes.

CAUTION!
The camera module is a sensitive device and must be handled carefully.

3   Installation

3.1   Wireless antenna
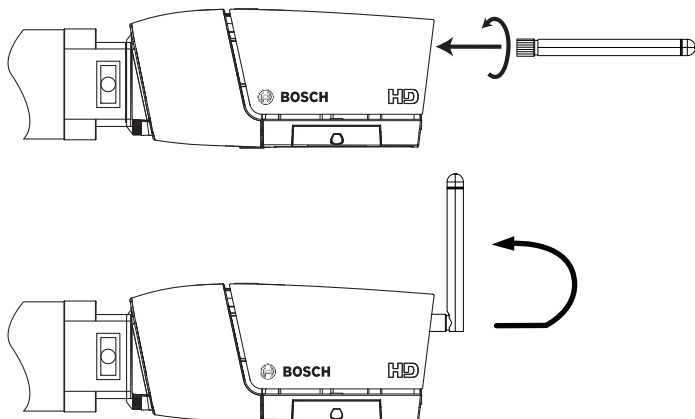
Figure 3.1   Wireless antenna

1.   Screw the antenna onto the screw connector on the rear of the camera.
2.   Straighten the antenna.

3.2   SD card
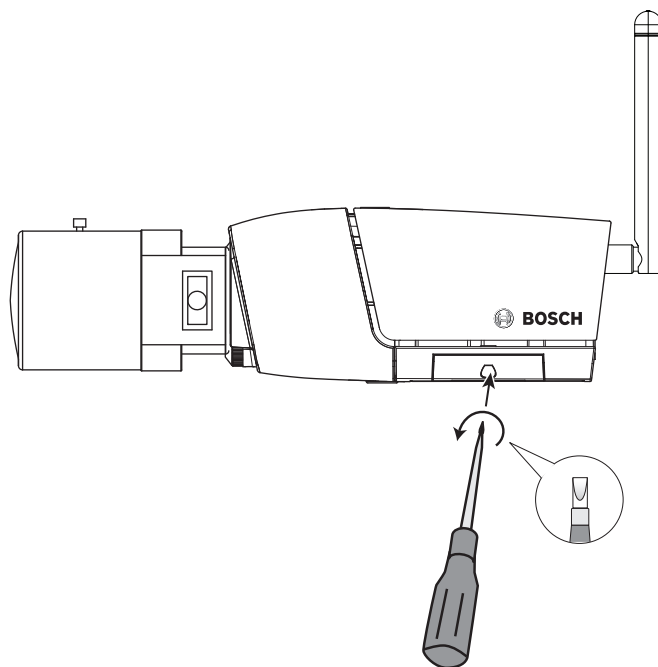
Figure 3.2   SD card

1.   Unscrew the cover on the right side of the camera.
2.   Slide the SD card into the slot.
3.   Close and secure the cover.

The camera supports most SD/SDHC cards.

Note:

Use high speed SD cards, class 4 or above (the higher read/
write speed the better).

3.3   Mounting the camera

The camera can be mounted either from the top or from the bottom (1/4"-20 UNC thread). The mounting socket is isolated from ground to prevent ground loops.

> ⚠ **CAUTION!**
> Do not point the camera/lens into direct sunlight as this may damage the sensors.
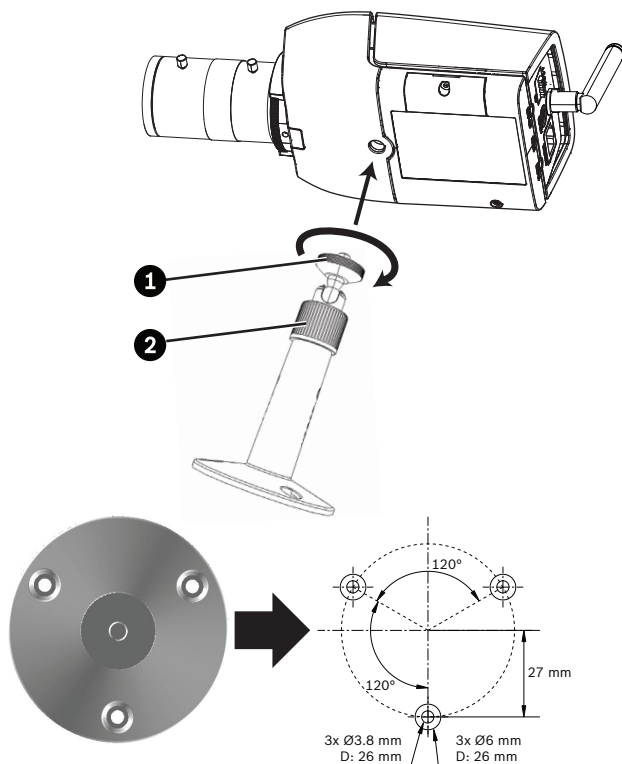
Figure 3.3   Mounting a camera

1.   Use three screws to secure the base of the mounting unit to a wood (Ø3.8 mm, 26 mm deep) or concrete (Ø6 mm, 26 mm deep) surface.
2.   On the mounting unit, loosen the ball-socket adjustment ring (2).

3. Adjust the ball-socket so that camera mount is correcrly aligned for the required angle.
4. Screw camera onto mount and, when in position, tighten the locking ring (1) securely.
5. Tighten the ball-socket adjustment ring (2) securely.

3.4   Network connector
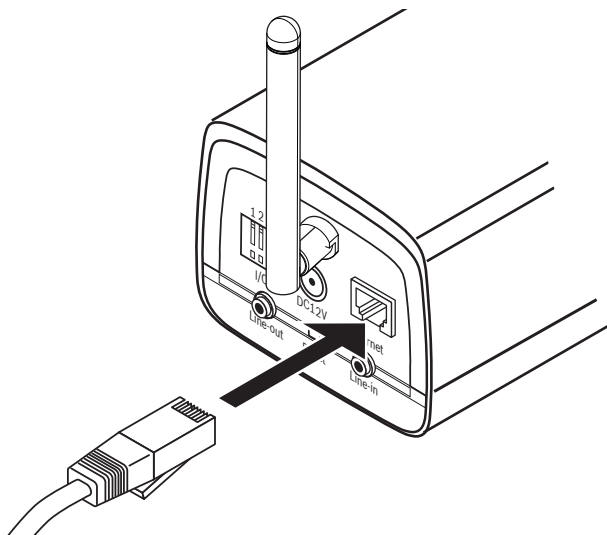
Figure 3.4   Network connection

–   Connect the camera to a 10/100 Base-T network.
–   Use a shielded UTP Category 5e cable with RJ45
     connectors.

3.5 Power connection

3.5.1 DC power connection
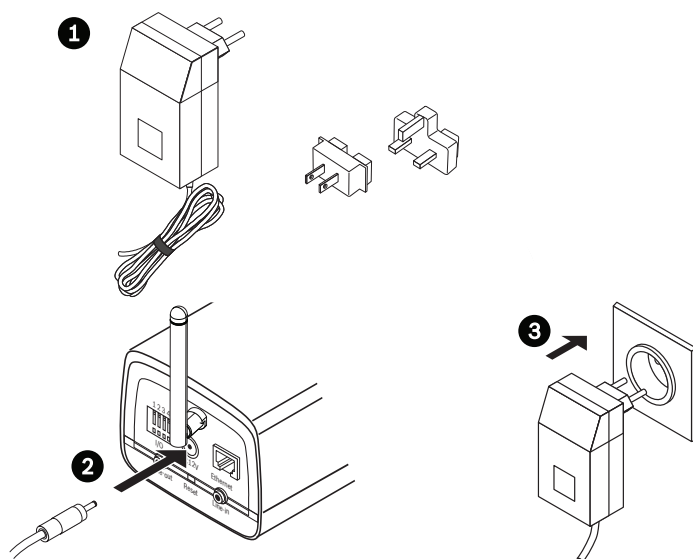
Figure 3.5 DC power connection

1. Slide the plug adapter that matches your outlet socket onto the supplied power supply.
2. Insert the power connector jack from the power supply into the DC12V socket of the camera.
3. Connect the power supply to either a 230 VAC or a 120 VAC power supply outlet.

When power is supplied to the camera the LED on the bottom-front of the camera lights. (This LED can be disabled in the Installer menu.)

Note:

The date/time must be synchronized each time after power on. It is important to ensure that the date/time is correct for recording. An incorrect date/time setting could prevent correct recording.

3.6   I/O connector
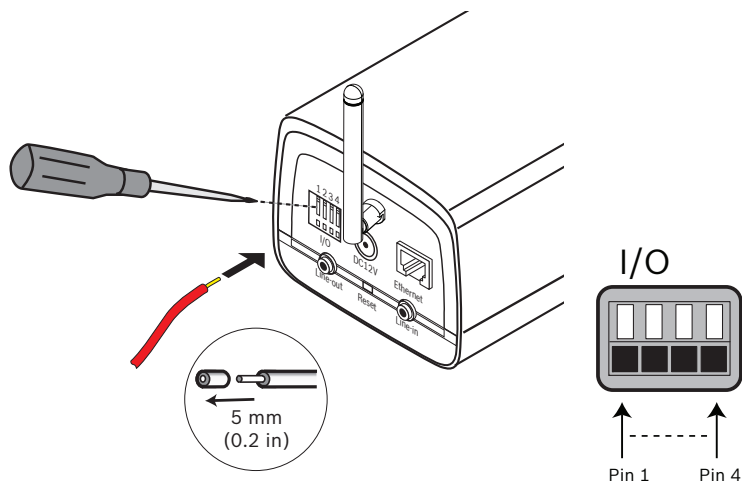
Figure 3.6   I/O connector pins

Function	Pin	I/O socket
Relay	1	Relay out contact 1
	2	Relay out contact 2
Alarm input	3	Relay in Positive
	4	Relay in Negative

– Max. wire diameter AWG 22-28 for both stranded and solid; cut back 5 mm (0.2 in) of insulation.
– Relay output switching capability: Max. voltage 24 VAC or 24 VDC. Max. 1 A continuous, 12 VA.
– Trigger in: +9 VDC minimum; +30 VDC maximum. Reverse polarity connection will be inactive.
– Alarm input configurable as active low or active high.

3.7   Audio connectors

Line in: 9 kOhm typ., 200 mVrms
Line out: 16 Ohm min. 200 mVrms
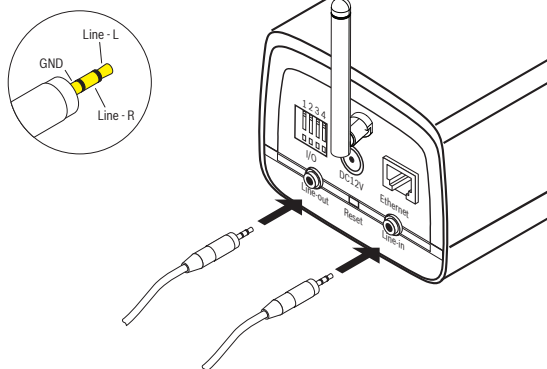
Figure 3.7   Audio connectors

Connect audio devices to the **Line In** and **Line Out** connectors.

3.8   Resetting the camera

If the camera cannot be connected because the IP address has changed, press and hold the reset button (7 seconds approximately) until the LED flashes (red) to recall the factory default values. The factory default IP address is 192.168.0.1
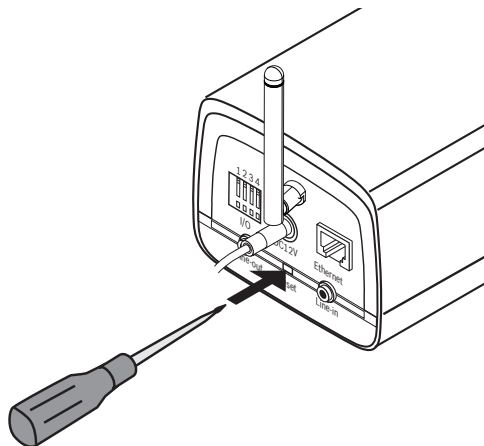
Figure 3.8   Reset button

4 Browser connection

A computer with Microsoft Internet Explorer can be used to receive live images from the camera, control cameras, and replay stored sequences. The camera is configured over the network using a browser or via the Bosch Video Client (supplied with the product).

4.1 System requirements

– Microsoft Internet Explorer version 7.0 or higher
– Monitor: resolution at least 1024 × 768 pixels, 16 or 32 bit color depth
– Intranet or Internet network access

The Web browser must be configured to enable Cookies to be set from the IP address of the unit.
In Windows Vista, deactivate protected mode on the **Security** tab under **Internet Options**.

To play back live video images, an appropriate ActiveX must be installed on the computer. If necessary, the required software and controls can be installed from the product CD provided.

a. Insert the CD into the CD-ROM drive of the computer. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double click `BVC-installer.exe`
b. Follow the on-screen instructions.

To get full support for recordings and snapshots, install the `MPEG_ActiveX` from the product disk to your computer.

4.2 Establishing the connection

The camera must be assigned a valid IP address to operate on your network. The default address pre-set at the factory is
`192.168.0.1`
1. Start the Web browser.
2. Enter the IP address of the camera as the URL.

Note:

If the connection is not established, the maximum number of possible connections may already have been reached. Depending on the device and network configuration, up to 25 web browsers, or 50 Bosch VMS connections are supported.

4.2.1 Password protection in camera

A camera offers the option of limiting access across various authorization levels. If the camera is password-protected, a message to enter the password appears.
1. Enter the user name and the associated password in the appropriate fields.
2. Click **OK**. If the password is correct, the desired page is displayed.

4.3 Protected network

If a RADIUS server is used for network access control (802.1x authentication), the camera must be configured first. To configure the camera for a Radius network, connect it directly to a PC via a crossed network cable and configure the two parameters, **Identity** and **Password**. Only after these have been configured can communication with the camera via the network occur.

4.4   Connection established

When a connection is established, the **LIVEPAGE** is initially
displayed. The application title bar displays the type number of
the connected camera and three items: **LIVEPAGE**,
RECORDINGS, **SETTINGS**.

Note:
The **RECORDINGS** link is only visible if a storage medium is
available. (Ensure that MPEG_ActiveX is installed.)
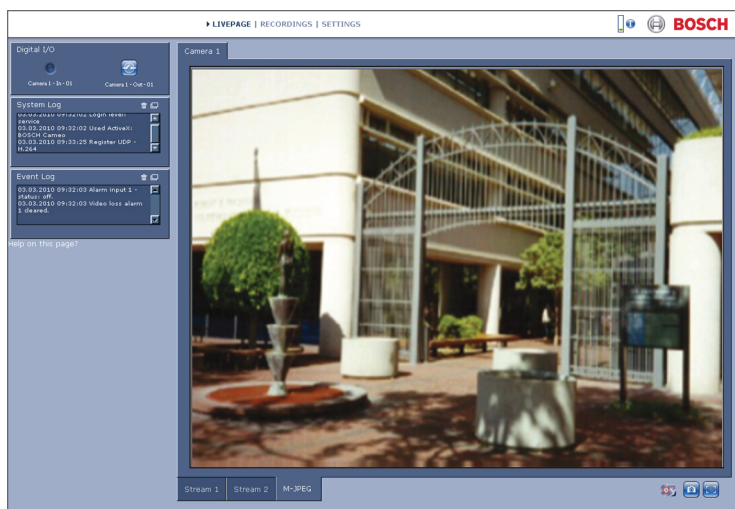
Figure 4.1   Livepage

4.4.1   LIVEPAGE

The **LIVEPAGE** is used to display and control the video stream.
Refer to *Section 7.1 Livepage, page 131* for more information.

4.4.2   RECORDINGS

Click **RECORDINGS** in the application title bar to open the
playback page. Refer to *Section 7.2 Recordings page, page 136*
for more information.

4.4.3   SETTINGS

Click **SETTINGS** in the application title bar to configure the
camera and the application interface. A new page containing

the configuration menu is opened. All settings (except date/
time) are stored in the camera memory so that they are
retained, even if the power is interrupted.
Changes that influence the fundamental functioning of the unit
(for example, firmware updates) can only be made using the
configuration menu.
The configuration menu tree allows all parameters of the unit to
be configured. The configuration menu is divided into **Basic
Mode** and **Advanced Mode**.
Refer to *Section 5 **Basic Mode**, page 63* for more information on
basic settings; refer to *Section 6 Advanced Mode, page 68* for
more information on advanced settings.

Note:
It is recommended that only expert users or system
administrators use the **Advanced Mode**.

5   Basic Mode

5.1   Basic Mode menu tree

The basic mode configuration menu allows a set of basic camera parameters to be configured.

Basic Mode	
>	**Device Access**
>	**Date/Time**
>	**Network**
>	**Encoder**
>	**Audio**
>	**Recording**
>	**System Overview**

To view the current settings:

1.   If necessary, click the Basic Mode menu to expand it. The sub-menus are displayed.
2.   Click a sub-menu. The corresponding page is opened.

The settings are changed by entering new values or by selecting a pre-defined value in a list field.

Saving changes

After making changes in a window, click **Set** to send the new settings to the device and save them there.

Clicking **Set** saves only the settings in the current window. Changes in any other windows are ignored.

Click **SETTINGS** in the applications title bar to close the window without saving the changes.

Note:

When entering names do not use any special characters, for example **&**. Special characters are not supported by the internal recording management system.

5.2 Device Access

5.2.1 Camera name

The camera can be assigned a name to assist in identifying it. The name simplifies the management of multiple devices in more extensive systems.

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

5.2.2 Password

A password prevents unauthorized access to the device. The device recognizes three authorization levels: **service**, **user**, and **live**.

– **service** is the highest authorization level. Entering the correct password gives access to all the functions of the camera and allows all configuration settings to be changed.

– **user** is the middle authorization level. This user can operate the device, play back recordings, and also control a camera but cannot change the configuration.

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

Use the various authorization levels to limit access. Proper password protection is only guaranteed if all higher authorization levels are also protected with a password. For example, if a **live** password is assigned, a **service** and a **user** password should also be set. When assigning passwords, always start from the highest authorization level, **service**, and use different passwords.

Password

Define and change a separate password for each level while logged in as **service** or if the device is not protected by a password. Enter the password (19 characters maximum) for the selected level.

Confirm password

Re-enter the new password to ensure that there are no typing mistakes.

The new password is only saved after clicking **Set**. Therefore, click **Set** immediately after entering and confirming the password, even if you plan to assign a password at another level.

5.3   Date/Time

Device date, time and zone

If there are multiple devices operating in the 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 devices are operating on the same time.

As the device time is controlled by the internal clock, it is not necessary to enter the day or date of the week. These are set automatically. The time zone in which the system is located is also set automatically.

▶   Click **Sync to PC** to apply the system time from your computer to the device.

Note:

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

5.4   Network

Use the settings on this page to integrate the device into a network. Some changes only take effect after a reboot. In this case, the **Set** button 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. If the IP address, subnet mask, or gateway address is changed, then the device is only available under the new addresses after the reboot.

DHCP
If the network has a DHCP server for dynamic IP address allocation, set this parameter to **On** to activate the automatic acceptance of DHCP-assigned IP addresses.

Note:
Certain applications (for example, Bosch Video Management System) use the IP address for the unique assignment of the device. If using 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 camera. The IP address must be valid for the network.

Subnet mask
Enter the appropriate subnet mask for the set IP address.

Gateway address
Enter the IP address of the gateway to establish a connection to a remote location in a different subnet. Otherwise, this field can remain empty (0.0.0.0).

5.5   Encoder

Select a profile for encoding the video signal. Pre-programmed profiles are available that give priority to different parameters. When a profile is selected, its details are displayed.

Main frequency and Operation environment
Select **50 Hz** or **60 Hz** as the main frequency, and **Indoor** or **Outdoor** for the operation environment.

5.6   Audio

Switch the camera microphone **On** or **Off**.

5.7   Recording

Record the images from the camera to a storage medium. For long-term authoritative images, it is essential to use an NVR or an appropriately sized iSCSI system.

5.7.1   Storage medium

1.   Select the required storage medium from the list.
2.   Click **Start** to start recording or **Stop** to end recording.

5.8   System Overview

This page provides general information on the hardware and firmware system, including version numbers. No items can be changed on this page but they can be copied for information purposes when troubleshooting.

6   Advanced Mode

6.1   Advanced Mode menu tree

The advanced mode configuration menu contains all camera
parameters that can be configured.

Advanced Mode	
>	General
>	Web Interface
>	Camera
>	Recording
>	Alarm
>	Interfaces
>	Network
>	Service

To view the current settings:

1.   Click the **Advanced Mode** menu to expand it. The
     associated menu sub-headings are displayed.
2.   Click a menu sub-heading to expand it.
3.   Click a sub-menu. The corresponding page is opened.

The settings are changed by entering new values or by selecting
a pre-defined value in a list field.

Saving changes

After making changes in a window, click **Set** to send the new
settings to the device and save them there.

Clicking **Set** saves only the settings in the current window.
Changes in any other windows are ignored.

Click **SETTINGS** in the applications title bar to close the
window without saving the changes made.

Note:

When entering names do not use any special characters, for
example **&**. Special characters are not supported by the internal
recording management system.

6.2   General

General	
>	**Identification**
>	**Password**
>	**Date/Time**
>	**Display Stamping**

6.2.1   Identification

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

Camera name
Assign a camera name to assist in identifying it. The name simplifies the management of multiple devices in more extensive systems, for example the VIDOS or Bosch VMS software. The camera name is used for remote identification, for example, in the event of an alarm. Enter a name that makes it as easy as possible to identify the location unambiguously.

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.

6.2.2   Password
A password prevents unauthorized access to the device. The device recognizes three authorization levels: **service**, **user**, and **live**.

- **service** is the highest authorization level. Entering the correct password gives access to all the functions of the camera and allows all configuration settings to be changed.
- **user** is the middle authorization level. This user can operate the device, play back recordings, and also control a camera but cannot change the configuration.

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

Use the various authorization levels to limit access. Proper password protection is only guaranteed if all higher authorization levels are also protected with a password. For example, if a **live** password is assigned, a **service** and a **user** password should also be set. When assigning passwords, always start from the highest authorization level, **service**, and use different passwords.

Password
Define and change a separate password for each level while logged in as **service** or if the device is not protected by a password. Enter the password (19 characters maximum) for the selected level.

Confirm password
Re-enter the new password to ensure that there are no typing mistakes.
The new password is only saved after clicking **Set**. Therefore, click **Set** immediately after entering and confirming the password, even if assigning a password at another level.

6.2.3   Date/Time

Date format
Select the 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 devices are operating on the
same time.
1.   Enter the current date. Since the device time is controlled
      by the internal clock, it is not necessary to enter the day of
      the week – it is added automatically.
2.   Enter the current time or click **Sync to PC** to apply the
      system time from your computer to the device.

Note:
It is important to ensure 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 the system is located.

Daylight saving time
The internal clock can switch automatically between normal
and daylight saving time (DST). The device already contains the
data for DST switch-overs up to the year 2015. Use this data or
create alternative time saving data, if required.
First, check the time zone setting. If it is not correct, select the
appropriate time zone for the system:
1.   Click **Set**.
2.   Click **Details**. A new window opens showing an empty
      table.
3.   Click **Generate** to fill the table with the preset values from
      the camera.
4.   Select the region or the city which is closest to the
      system's location from the list box below the table.