

DIVAR IP 3000

DIP-3040-00N, DIP-3042-2HD, DIP-3042-4HD



BOSCH

en Installation Manual

Table of Contents

1	Safety precautions	4
1.1	General safety precautions	4
1.2	Electrical safety precautions	5
1.3	ESD precautions	6
1.4	Operating precautions	6
2	System overview	7
2.1	Chassis features	7
2.2	Chassis components	7
2.2.1	Chassis	7
2.2.2	Backplane	7
2.2.3	Power supply	7
2.3	Device views	8
2.3.1	LED description - front panel	9
2.3.2	LAN port LED description - rear panel	10
3	Chassis setup and maintenance	11
3.1	Removing hard drive trays	11
3.2	Installing a hard drive	11
4	System setup - first steps	12
4.1	Introduction	12
4.2	Setup instruction	12
4.3	Starting the application	12
4.4	Using Bosch VMS Config Wizard	13
4.5	Adding additional licenses	14
4.6	Using Bosch VMS Operator Client	14
5	Connecting to the internet	16
5.1	Protecting the system from unauthorized access	16
5.2	Setting up port forwarding	16
5.3	Choosing an appropriate client	16
5.3.1	Remote connection with Operator Client	16
5.3.2	Remote connection with Video Security App	16
5.4	Installing an Enterprise Management Server	17
6	Recovering the unit	18
7	Additional Documentation and client software	19

1 Safety precautions

Observe the safety precautions in this chapter.

1.1 General safety precautions

Follow these rules to ensure general safety:

- Keep the area around the system clean and free of clutter.
- Place the chassis top cover and any system components that have been removed away from the system or on a table so that they won't accidentally be stepped on.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.



Warning!

Interruption of mains supply:

Voltage is applied as soon as the mains plug is inserted into the mains socket.

However, for devices with a mains switch, the device is only ready for operation when the mains switch (ON/OFF) is in the ON position. When the mains plug is pulled out of the socket, the supply of power to the device is completely interrupted.



Warning!

Removing the housing:

To avoid electric shock, the housing must only be removed by qualified service personnel.

Before removing the housing, the plug must always be removed from the mains socket and remain disconnected while the housing is removed. Servicing must only be carried out by qualified service personnel. The user must not carry out any repairs.



Warning!

Power cable and AC adapter:

When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire.

Electrical Appliance and Material Safety Law prohibits the use of UL or CSA-certified cables (that have UL/CSA shown on the code) for any other electrical devices.



Warning!

Lithium battery:

Batteries that have been inserted wrongly can cause an explosion. Always replace empty batteries with batteries of the same type or a similar type recommended by the manufacturer. Handle used batteries carefully. Do not damage the battery in any way. A damaged battery may release hazardous materials into the environment.

Dispose of empty batteries according to the manufacturer's instructions.



Warning!

Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

**Notice!**

Electrostatically sensitive device:

To avoid electrostatic discharges, the CMOS/MOSFET protection measures must be carried out correctly.

When handling electrostatically sensitive printed circuits, grounded anti-static wrist bands must be worn and the ESD safety precautions observed.

**Notice!**

Installation should only be carried out by qualified customer service personnel in accordance with the applicable electrical regulations.

**Disposal**

Your Bosch product has been developed and manufactured using high-quality materials and components that can be reused.

This symbol means that electronic and electrical devices that have reached the end of their working life must be disposed of separately from household waste.

In the EU, separate collecting systems are already in place for used electrical and electronic products. Please dispose of these devices at your local communal waste collection point or at a recycling center.

1.2 Electrical safety precautions

Basic electrical safety precautions should be followed to protect you from harm and the system from damage:

- Be aware of the locations of the power on/off switch on the chassis as well as the room's emergency power-off switch, disconnection switch or electrical outlet. If an electrical accident occurs, you can then quickly remove power from the system.
- Do not work alone when working with high voltage components.
- Power should always be disconnected from the system when removing or installing main system components, such as the motherboard or memory modules. When disconnecting power, you should first turn off the system and then unplug the power cords from all the power supply modules in the system.
- When working around exposed electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off the power if necessary.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage any electrical components or circuit boards they come into contact with.
- The power supply power cords must include a grounding plug and must be plugged into grounded electrical outlets. The unit has more than one power supply cord. Disconnect both power supply cords before servicing to avoid electrical shock.
- Mainboard replaceable soldered-in fuses: Self-resetting PTC (Positive Temperature Coefficient) fuses on the mainboard must be replaced by trained service technicians only. The new fuse must be the same or equivalent as the one replaced. Contact technical support for details and support.

**Caution!**

Mainboard Battery: There is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities. This battery must be replaced only with the same or an equivalent type recommended by the manufacturer (CR2032). Dispose of used batteries according to the manufacturer's instructions.

1.3

ESD precautions

Electrostatic Discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. The following measures are generally sufficient to neutralize this difference before contact is made to protect your equipment from ESD:

- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- Use a grounded wrist strap designed to prevent static discharge.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Do not let components or printed circuit boards come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only. Do not touch its components, peripheral chips, memory modules or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the mainboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure your computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the mainboard.

1.4

Operating precautions

The chassis cover must be in place when the system is operating to assure proper cooling. Out of warranty damage to the system can occur if this practice is not strictly followed.

Note:

Please handle used batteries carefully. Do not damage the battery in any way. A damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

2 System overview

The DIVAR IP 3000 system is an affordable and easy to use all-in-one recording, viewing, and management solution for network surveillance systems of up to 32 channels. All channels are pre-licensed. Running the full Bosch VMS solution and powered by Bosch VRM (Video Recording Manager) including the Video Streaming Gateway to integrate 3rd party cameras, DIVAR IP 3000 is an intelligent IP storage device that eliminates the need for separate NVR (Network Video Recorder) server and storage hardware.

DIVAR IP 3000 is a 4-bay mini tower unit that combines advanced management and state-of-the-art recording management into a single cost-effective, plug and play IP recording appliance for IT-minded customers which are seeking for a state-of-the-art “second generation” DVR and NVR recording solution.

Easy to install and operate, DIVAR IP 3000 features wizard-based set-up and centralized configuration to reduce installation times. All components are pre-installed and pre-configured. Simply connect to the network and turn on the unit – DIVAR IP 3000 is ready to begin recording straight out of the box.

Bosch Video Management System manages all IP and digital video and audio, plus all the security data being transmitted across your IP network. It seamlessly combines IP cameras and encoders, provides system-wide event and alarm management, system health monitoring, user and priority management.

DIVAR IP 3000 features front-swappable SATA-II hard drives. All system software is pre-installed and pre-activated – creating an out-of-the-box ready-to-use video management appliance. DIVAR IP 3000 utilizes Windows Storage Server 2008 R2 operating system.

2.1 Chassis features

The chassis includes the following features:

- CPU (Intel i3 processor)
- 4 slots for SATA drives (front replaceable)
- 1x VGA output (onboard)
- 1x DVI graphics output
- 4x USB 2.0, 1x USB 3.0
- 1x internal USB Transcoder device
- 1x Gigabit Ethernet LAN port

2.2 Chassis components

This chapter describes the most common components included with your chassis.

2.2.1 Chassis

The chassis includes 4 slots for hard drives.

2.2.2 Backplane

The backplane accepts front-swappable SATA-II hard drives.



Warning!

Use caution when servicing and working around the backplane. Hazardous voltage or energy is present on the backplane when the system is operating. Do not touch the backplane with any metal objects and make sure no ribbon cables touch the backplane.

2.2.3 Power supply

The chassis features a highly energy-efficient power supplies.

2.3 Device views

There are several LEDs on the front and rear of the chassis. The LEDs show the over-all status of the system and the activity and health of specific components.

Front view:



1	Lock for front cover	4	LAN activity LED
2	Power on/off LED	5	System status LED
3	Hard disk access LED	6	Individual hard disk LED

Rear view:

1	1x VGA (monitor)	5	Mains connection 100 - 240 VAC
2	1x Ethernet (RJ45)	6	1x USB 3.0 Note: Do not use this port for keyboard and mouse.
3	4x USB 2.0 Note: Use these ports for keyboard and mouse connection.	7	1x DVI (monitor), for local viewing Note: If the system is only connected to the DVI port, no video signal is displayed until the system has started completely. This can take 1 – 2 minutes. A video signal is always displayed when the monitor is connected to the VGA port.
4	1x eSATA for data export Note: Do not connect hard disk drives for recording.		

2.3.1**LED description - front panel**

This chapter describes the LED displays on the front of the chassis.

LED indicator	LED color	LED state	Description
Power LED	N/A	Off	Power off
	Blue	On (default)	Working (S0 state)

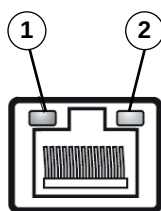
LED indicator	LED color	LED state	Description
HDD LED	N/A	Off	No disk access
	Blue	Blinking	Disk access
LAN LED	N/A	Off	Network disconnected
	Blue	On	Network connected
	Blue	Blinking	Network activity
System LED	N/A	Off	Power off
	Blue	On (default)	System has booted in normal operation.
	Blue	Blinking	System is booting or shutting down
	Red	On	Critical event occurred, such as degraded RAID volume. Bosch also provides the API and then application program is able to control this status.
Individual hard disk LED	N/A	Off (default)	Hard drive not present.
	Blue	On	Hard drive present.
	Red	On	Bosch provides the API to let application program to control this status.

2.3.2

LAN port LED description - rear panel

This chapter describes the LAN port LED on the rear of the chassis.

LAN connector:



Nr.	LED indicator	LED color	LED state	NIC state
1	RJ45 LED (left)	N/A	Off	No connection or 10 Mb/s
		Green	On	100 Mb/s
		Yellow	On	1000 Mb/s
2	RJ45 LED (right)	Yellow	On	Active connection
		Yellow	Blinking	Transmit or receive activity

3 Chassis setup and maintenance

This chapter covers the steps required to install components and perform maintenance on the chassis.

**Caution!**

Review the warnings and precautions listed in the manual before setting up or servicing this chassis.

See also:

Safety precautions, page 4

3.1 Removing hard drive trays

The drives are mounted in drive carriers to simplify their installation and removal from the chassis. These carriers also help promote proper airflow for the drive bays.

To remove hard drive trays from the chassis:

1. Turn off the system.
2. Press the release button on the drive carrier. This extends the drive carrier handle.
3. Use the handle to pull the drive carrier with the drive out of the chassis.
4. Insert the drive carrier with the new drive into the chassis bay, making sure that the drive carrier handle is completely closed.

**Notice!**

Except for short periods of time, do not operate the unit with the hard drives removed from the bays.

3.2 Installing a hard drive

The drives are mounted in drive carriers.

To install a hard drive to the hard drive carrier:

1. Remove the drive from the carrier.
2. Install a new drive into the carrier with the printed circuit board side facing down so that the mounting holes align with those in the carrier.
3. Replace the drive carrier into the chassis bay, making sure that the drive carrier handle is completely closed.

**Notice!**

We recommend using the respective Bosch hard disk drives. The hard disk drives as one of the critical component are carefully selected by Bosch based on available failure rates. HDD – not delivered from Bosch – are not supported. Information on supported HDDs can be found in the datasheet in the Bosch Online Product Catalog.

4 System setup - first steps

The following installation directive provides information on Installation and Configuration. This chapter is valid for DIVAR IP models that come with pre-installed hard drives. Empty units start into the DOM recovery menu on first start.

See also:

- *Recovering the unit, page 18*

4.1 Introduction

DIVAR IP systems are shipped with a pre-installed Configuration Wizard from factory.

4.2 Setup instruction

All DIVAR IP systems are preconfigured with a default IP address and with default iSCSI settings.

- IP Address: 192.168.0.200
- Subnet mask: 255.255.255.0

Observe the following:

- DIVAR IP needs to have an active network link during installation. Make sure that the network switch you are connecting to is powered on.
- The default IP address must not be occupied by any other device in the network. Make sure that the default IP addresses of existing DIVAR IP systems in the network are changed before adding another DIVAR IP.
- Determine whether the initial installation is on a DHCP network. If not then you must assign valid IP addresses to the video devices. Consult the local IT administrator to obtain a valid IP address range to be used with DIVAR IP and associated devices.
- The default iSCSI settings are optimized for use with VRM.

User with administrator rights:

- User: BVRAdmin
- Password: WSS4Bosch



Notice!

We strongly recommend not changing the user settings. Changing the user settings can result in malfunctioning of the system.

4.3 Starting the application

DIVAR IP system is ready to go out of the box. The application provides a simple to install and intuitive to use solution for network surveillance systems.



Notice!

In order to start the application for the first time you must use the VGA port. If the system is only connected to the DVI port, no video signal is displayed until the system has started completely. This can take 1 – 2 minutes. A video signal is always displayed when the monitor is connected to the VGA port.

To start the application:

1. Connect the unit and the cameras to the network.
2. Turn on the unit.
The Windows Storage Server 2008 R2 setup process starts.
3. Select the appropriate language for the installation, then click **Next**.

4. In the **Country or region**, **Time and currency** and **Keyboard layout** lists, click the appropriate item, then click **Next**.
The Microsoft Software License Terms and the EULA (End User License Agreement) are displayed.
5. Accept the license terms, then click **Start**. Windows restarts.
After restart is finished, different Bosch VMS versions are displayed on the screen.
6. Double-click the Bosch VMS version you want to install.
Note. We recommend that you install the latest version.
The installation can take several minutes. Do not turn off the computer. If necessary, restart the system.
7. After restart is finished, press CTR+ALT+DELETE. The Windows logon page is displayed.
8. Enter the default password **WSS4Bosch**.
9. After entering the password, a message is displayed that you must change the password before logging on the first time. To confirm, click **OK**.
10. Change the password.
A series of scripts perform important setup tasks. This can take several minutes. Do not turn off the computer.
The Bosch VMS default screen is displayed.
Note: In case of password loss a system recovery must be performed as described in the installation manual. The configuration must be done from scratch or must be imported.
11. On the Bosch VMS default screen, double-click the **Bosch VMS Wizard** icon  to start the Configuration Wizard.
The **Welcome** page is displayed.
12. Configure the system using the Configuration Wizard.

**Notice!**

To perform administrative tasks, the BVRAdmin account can be entered when Bosch VMS default screen is displayed. To do so, press CTRL+ALT+DEL, then hold down SHIFT while clicking the **Switch User** option and keep SHIFT pressed for about five seconds.

**Notice!**

We strongly recommend not changing any operating system settings. Changing operating system settings can result in malfunctioning of the system.

See also:

- *Using Bosch VMS Config Wizard, page 13*
- *Adding additional licenses, page 14*
- *Recovering the unit, page 18*

4.4 Using Bosch VMS Config Wizard

Intended use for Config Wizard is the quick and easy configuration of a smaller system. Config Wizard helps you to achieve a configured system including VRM, iSCSI system, cameras, recording profiles and user groups.

User groups and their permissions are configured automatically. You can add or remove users and set passwords.

Config Wizard can access Management Server only on the local computer.

You can save an activated configuration for backup purposes and import this configuration later. You can change this imported configuration after import.

Config Wizard adds the local VRM automatically.

Restrictions:

The following tasks cannot be done with the Configuration Wizard. Use Bosch VMS Configuration Client instead.

- adding additional license packages
- adjusting schedules
- configuring systems with no or multiple VRM
- configuring external storage devices
- adding Video Streaming Gateway
- all advanced configurations beyond a basic setup (maps or alarms, for example)

To achieve a quick configuration using the Configuration Wizard:

1. On the Bosch VMS default screen, double-click the **Bosch VMS Wizard** icon. The **Welcome** page is displayed.
2. Follow the wizard and observe the instructions on the screen.

**Notice!**

For the tasks that cannot be done with Configuration Wizard, and for detailed information concerning Configuration Wizard itself, refer to the Bosch VMS manual (see *Additional Documentation and client software*, page 19).

4.5**Adding additional licenses**

You can add additional licenses using Configuration Client.

To activate the software:

1. Start Configuration Client.
2. On the **Tools** menu, click **License Manager....**
The **License Manager** dialog box is displayed.
3. Click to check the boxes for the software package, the features, and the expansions that you want to activate. For the expansions, enter the number of licenses.
If you have received a Bundle Information file, click **Import Bundle Info** to import it.
4. Click **Activate**.
The **License Activation** dialog box is displayed.
5. Write down the computer signature or copy and paste it into a text file.
6. On a computer with Internet access, enter the following URL into your browser:
<https://activation.boschsecurity.com>
If you do not have an account to access the Bosch License Activation Center, either create a new account (recommended) or click the link to activate a new license without logging on. If you create an account and log on before activating, the License Manager keeps track of your activations. You can then review this at any time.
Follow the instructions to obtain the License Activation Key.
7. Return to the Bosch VMS software. In the **License Activation** dialog box, type the License Activation Key obtained from the License Manager and click **Activate**.
The software package is activated.

4.6**Using Bosch VMS Operator Client**

Use Bosch VMS Operator Client to verify the live, recording and playback functionality of DIVAR IP.

To verify live image functionality in the Operator Client

1. On the Bosch VMS default screen, double-click the Operator Client icon . The application starts.

2. Enter the following and click **OK**.
User name: admin
Password: no password required (if not set with the wizard)
Connection: 127.0.0.1
3. Click the live image icon. The Logical Tree with the cameras is displayed.
4. Select a camera and drag it to an image window. The image of the camera is displayed if the camera is assigned correctly.

Note:

Cameras in the image window with a red dot in the camera's icon are viewed live.

To verify recording functionality in the Operator Client

- ▶ Cameras in the Logical Tree with a red dot in the camera's icon are recording.

To verify playback functionality in the Operator Client

- ▶ The time line moves if the a camera is viewed in playback mode.

Performance overview live:

	4CIF		
	2.5 Mbit	5 Mbit	10 Mbit
Number of software monitors	17	13	8

	720p		
	2.5 Mbit	5 Mbit	10 Mbit
Number of software monitors	12	10	5

	1080p		
	2.5 Mbit	5 Mbit	10 Mbit
Number of software monitors	6	5	3

To perform further functionalities refer to the Bosch VMS manual. References to the manual are described in *Additional Documentation and client software*, page 19.

5 Connecting to the internet

This section describes the steps that are required to access the DIVAR IP system from the internet.

5.1 Protecting the system from unauthorized access

In order to protect the system from unauthorized access, we recommend that you follow strong password rules before connecting the system to the internet. The stronger your password, the more protected your system will be from unauthorized persons and malware.

5.2 Setting up port forwarding

In order to access a DIVAR IP system from the internet through a NAT/PAT capable router, port forwarding must be configured on the DIVAR IP system and on the router.

To set up port forwarding:

1. Make sure the system is fully configured with all devices.
2. On the Bosch VMS default screen, double-click the **Bosch VMS Wizard** icon. The **Welcome** page is displayed.
3. Follow the wizard until the **Basic** page is displayed.
4. Under **Port Mapping**, select the **Enable Port Mapping** check box.
5. Specify the public IP address or the DNS name of your internet connection.
6. Follow the wizard until the **Finish** page is displayed, then click **Details**.
7. Note the port rules displayed in the **Port Mapping Table** or export the table to a USB drive.
8. Enter these port rules in the port forwarding settings of your internet router.
The DIVAR IP system is now accessible from the Internet.

5.3 Choosing an appropriate client

There are two supported clients that allow remote connections to a DIVAR IP system through the internet.

5.3.1 Remote connection with Operator Client

To make a remote connection with Bosch VMS Operator Client

1. Download the resource folder of the Bosch VMS installer using the following network share:
`\\<IP address of DIVAR IP>\sources`
2. Copy the **Setup** directory to the remote workstation that will be used for remote viewing.
3. In the **Setup** directory, right-click `setup.exe`, then click **Run as administrator** and accept the security message.
4. In the **Welcome** dialog box clear all check boxes except Operator Client.
5. Follow the installation process.
6. After finishing the installer successfully, start Operator Client using the desktop shortcut.
7. Enter the following, then click **OK**.
User name: admin
Password: enter user password
Connection: enter public IP address or dynDNS name

5.3.2 Remote connection with Video Security App

To make a remote connection with Video Security App:

1. In Apple's App Store search for **Bosch Video Security**.
2. Install the Video Security app on your iOS device.

3. Start the Video Security app.
4. Select **Add**.
5. Enter the public IP address or dynDNS name (see Setting up port forwarding).
6. Make sure Secure Connection (SSL) is switched on.
7. Select **Add**.
8. Enter the following:
User name: admin
Password: enter user password

**Notice!**

Only use Bosch VMS Operator Client Video Security App in the version that matches DIVAR IP. Other clients or application software may work but are not supported.

5.4

Installing an Enterprise Management Server

For a central management of multiple systems you can install Bosch VMS Enterprise Management Server on a separate server.

To install Bosch VMS Enterprise Management Server on a separate server:

1. Download the resource folder of the Bosch VMS installer using the following network share:
\\<IP address of DIVAR IP>\sources
2. Copy the **Setup** directory to the server that should act as an Enterprise Management Server.
3. In the **Setup** directory, right-click `setup.exe`, then click **Run as administrator** and accept the security message.
4. In the **Welcome** dialog box, clear all check boxes except **Enterprise Management Server** and **Configuration Client**.
5. Follow the installation instructions.
6. After finishing the installer successfully, start Configuration Client using the desktop shortcut.

**Notice!**

For Enterprise Management Server configuration refer to the Bosch VMS documentation.

6 Recovering the unit

Following procedure describes how to restore the factory default image.

To restore the unit to factory default image

1. Start the unit and press **F7** during the BIOS power-on-self-test.
The Recovery menu is displayed.



Notice!

Make sure that a VGA monitor, a keyboard and a mouse are connected to the unit.

2. Select one of the following:
 - **Initial to factory image (all data will be deleted)**
(restores to factory default image and deletes all data on the HDDs)
or
 - **Restore to Factory image (all data will not be deleted)**
(restores to factory default image; data on the HDDs will not be deleted)

Note:

Windows performs the setup. The screen displays the percentage of the process.



Notice!

Do not turn off the unit during the process. This will damage the Recovery media.

3. The unit starts from the Recovery media. If the setup is successful, press **Yes** to restart the system.
4. Windows performs the initial setup of the operating system. The unit restarts after Windows has completed the setup.
5. After the restart of the unit, the factory settings are installed.

7 Additional Documentation and client software

Documentation for Bosch Security Systems products can be found as follows:

- ▶ Open any browser > enter www.boschsecurity.com > select your region and your country > start a search for your product > select the product in the search results to show the existing documents.

And on the following network share:

- ▶ \\<IP address of DIVAR IP>\sources

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2014