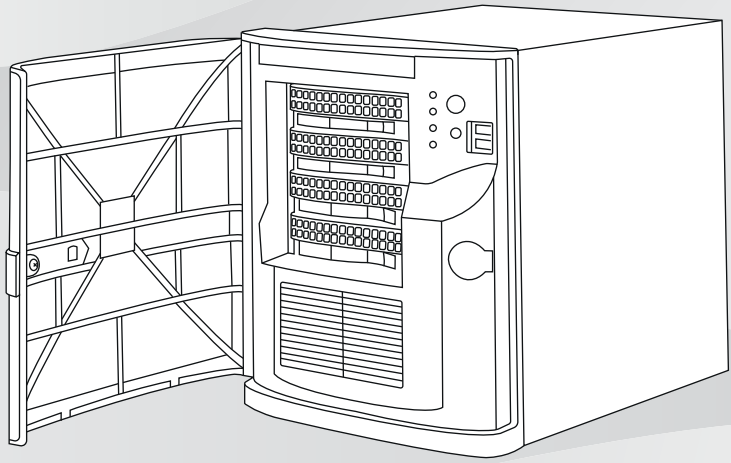
DIVAR IP all-in-one 5000

DIP-5240IG-00N | DIP-5244IG-4HD | DIP-5248IG-4HD | DIP-524CIG-4HD | DIP-5240GP-00N | DIP-5244GP-4HD | DIP-5248GP-4HD | DIP-524CGP-4HD



en Installation manual

Table of contents

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.
- Do not wear loose clothing such as neckties and unbuttoned shirt sleeves while working on the system. Loose clothing 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, or local directives.

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.

Notice!
The operating system includes the latest Windows security patches available at the time the software image was created. We recommend that you regularly install the latest security patches using the Windows Update function.

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.
- Disconnect the power cables before installing or removing any components from the computer, including the backplane.
- 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 circuits 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

Notice!
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.

Notice!
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.

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.

1.5 Data security precautions

For data security reasons observe the following:

– Physical access to the system shall be restricted to authorized personnel only. It is strongly suggested to place the system in an access control protected area, in order to avoid physical manipulation of the system.
– Windows online update functionality or the corresponding monthly roll-up patches for offline installation can be used to install OS security updates.

– Limiting local network access to trusted devices is strongly suggested. Details are described in the Technical note *Network Authentication 802.1X* and in the *Bosch IP Video and Data Security Guidebook*, available in the online product catalog.
– For access via public networks only use the secure (encrypted) communication channels.

See also
– *Remote connection to the system, page 28*

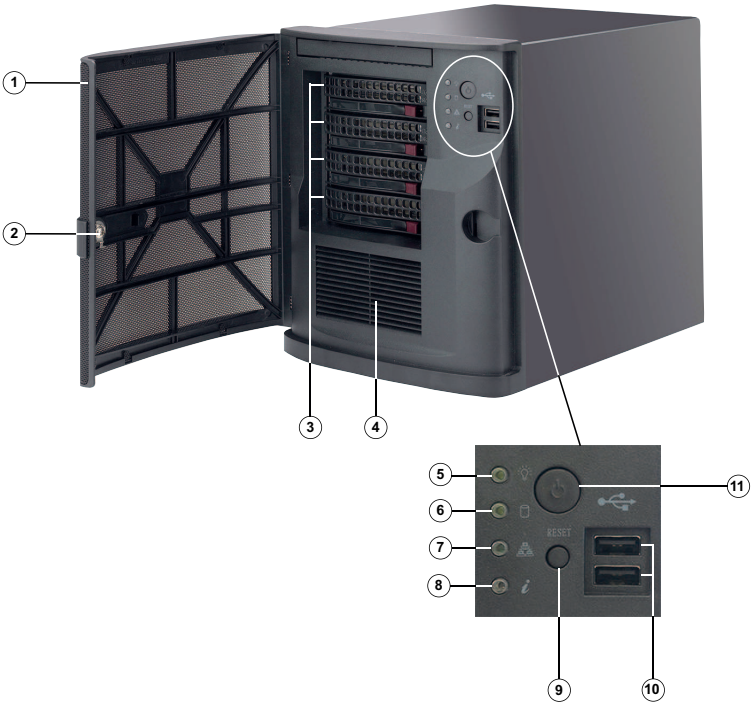
2 System overview

The DIVAR IP all-in-one 5000 system is an easy to use all-in-one recording, viewing, and management solution for network surveillance systems.
Running the full BVMS (BVMS solution and powered by Bosch Video Recording Manager (VRM) including the Bosch Video Streaming Gateway (VSG) to integrate 3rd party cameras, DIVAR IP all-in-one 5000 is an intelligent IP storage device that eliminates the need for separate Network Video Recorder (NVR) server and storage hardware.
BVMS 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 all-in-one 5000 is a 4-bay mini tower unit that features front-swappable SATA hard drives.
It is easy to install and operate. All system software is pre-installed — creating an out-of-the-box ready-to-use video management appliance.
DIVAR IP all-in-one 5000 utilizes Windows Storage Server 2016 operating system.

2.1 Device views

The DIVAR IP all-in-one 5000 system has a compact mini-tower chassis. It has a hinged front cover that hides the hard drives and the control panel.
The control panel located on the front features power buttons and status monitoring LEDs.
On the rear there are various I/O ports.

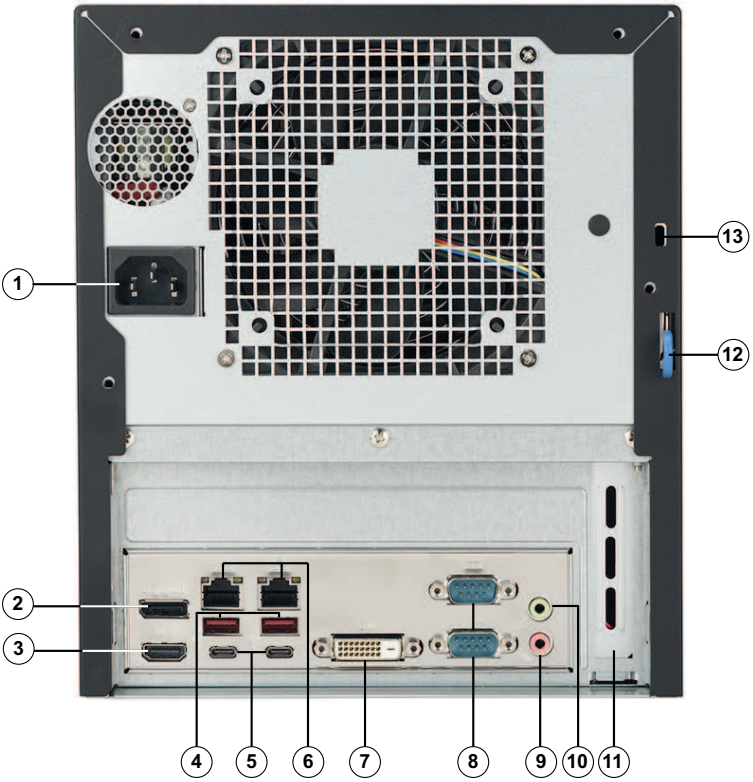
Front view



1	Front cover	2	Lock for front cover
3	4 x hot-swap hard drive ports (for 3.5" hard drives)	4	Air intake filter
5	Power LED	6	HDD LED (not used)

7	Network LED	8	Information LED
9	Reset button	10	2 x USB 2.0
11	Power on/off button		

Rear view



1	Mains connection	2	Display port
3	HDMI 2.0	4	2 x USB 3.1 (Type A)
5	2 x USB 3.1 (Type C)	6	2 x LAN ports (RJ45), teamed **Note:** Do not change the teaming mode!

7	DVI-D port	8	2 x COM ports
9	Audio Mic in	10	Audio Line out
11	Additional GPU card with 4x mini-display ports (in this case the mini-display ports should be used for monitor connection). **Note:** Only available for DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD and DIP-524CGP-4HD.	12	Rear chassis hasp (compatible with a variety of commonly available locks). **Note:** Locks are not included.
13	Kensington security slot (for a standard Kensington lock). **Note:** Kensington lock is not included.		

2.2 Control panel elements

The control panel located on the front of the chassis features power buttons and status monitoring LEDs.

Control panel buttons

Button	Description
 **Power**	The power button is used to apply or remove power from the power supply to the system. **Note:** Turning off system power with this button removes the main power, but keeps standby power supplied to the system. **To remove all power, unplug the system before performing maintenance tasks.**

Button	Description
 **Reset**	The reset button is used to reboot the system.

Control panel LEDs

LED	Description	
 **Power**	This LED indicates that power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is operating.	
 **HDD**	This LED is not used.	
 **Network**	This LED indicates network activity when flashing.	
 **Information**	This LED indicates the system status.	
	System status	**Description**
	Continuously on and red	An overheat condition has occurred. (This may be caused by cable congestion.)
	Blinking red (1 Hz)	Fan failure: check for an inoperative fan.
	Blinking red (0.25 Hz)	Power failure: check for an inoperative power supply.

LED	Description	
	Solid blue	Local UID has been activated. Use this function to locate the unit in a rack environment.
	Blinking blue (300 msec)	Remote UID has been activated. Use this function to locate the unit from a remote location.

3 Installing a hard drive

The DIVAR IP all-in-one 5000 system features four front-swappable hard drives. The hard drives are mounted in hard drive carriers to simplify their installation and removal from the chassis. These hard drives carriers also help promote proper airflow for the hard drive bays.

Procedure

To install a hard drive, you have to perform following steps:

1. *Removing a hard drive carrier from a hard drive bay, page 16*
2. *Installing a hard drive into a hard drive carrier, page 17*
3. *Installing a hard drive carrier into a hard drive bay, page 19*

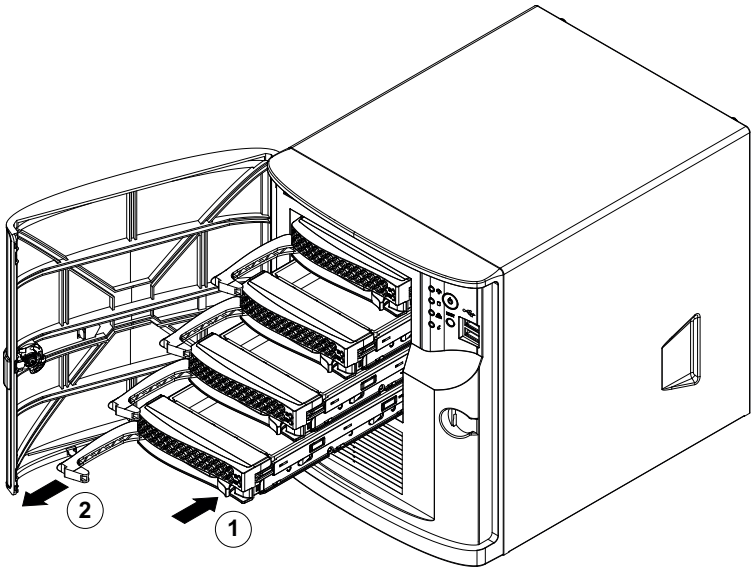
Notice!
Review the warnings and precautions listed in this manual before performing works on the chassis.

3.1 Removing a hard drive carrier from a hard drive bay

To remove a hard drive carrier from a hard drive bay:

1. Unlock the front cover and swing it open.
2. Press the release button to the right of the hard drive carrier. This extends the hard drive carrier handle.

3. Use the handle to pull the hard drive carrier out of the chassis.



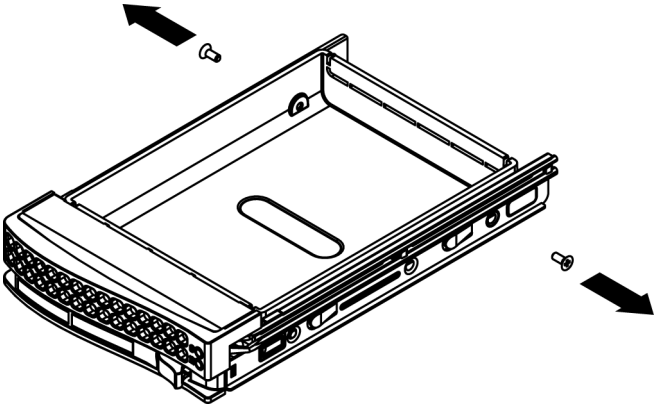
1	Release button	2	Hard drive carrier handle

Notice!
Do not operate the unit with the hard drive carriers removed from the bays.

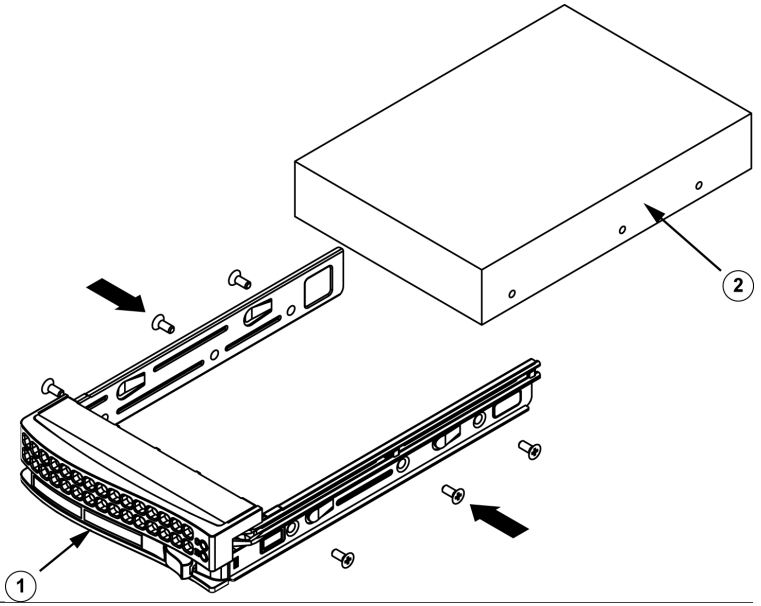
3.2 Installing a hard drive into a hard drive carrier

To install a hard drive into a hard drive carrier:

1. Remove the screws which secure the dummy drive to the hard drive carrier.



2. Remove the dummy drive from the hard drive carrier and place the hard drive carrier on a flat surface.
3. Slide a new hard drive into the hard drive carrier with the printed circuit board side facing down.
4. Align the mounting holes in both, the hard drive carrier and the hard drive.
5. Secure the hard drive to the hard drive carrier with the six screws.



1	Hard drive carrier	2	SATA hard drive

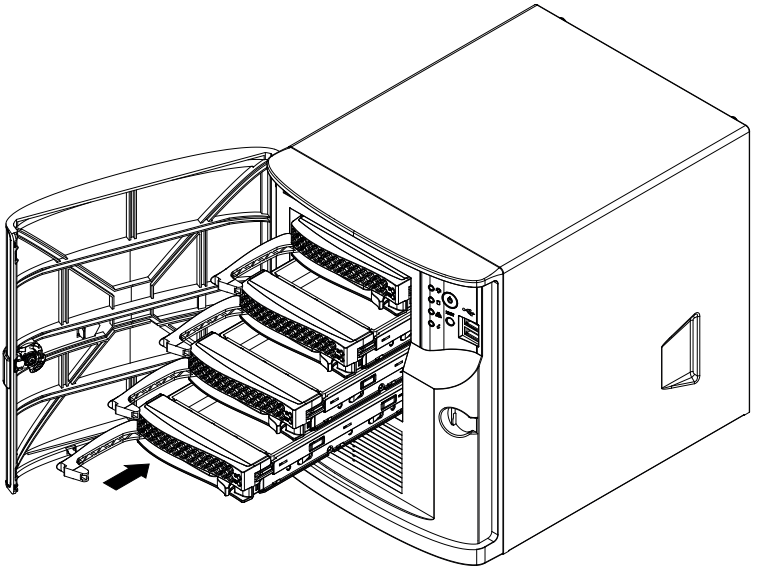
Notice!

Bosch recommends 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. Hard disk drives not delivered from Bosch are not supported. For more information about supported hard disk drives, see the datasheet in the Bosch Online Product Catalog at: www.boschsecurity.com

3.3 Installing a hard drive carrier into a hard drive bay

To install a hard drive carrier into a hard drive bay:

1. Insert the hard drive carrier horizontally into the hard drive bay, orienting the hard drive carrier so that the release button is on the right.
2. Push the hard drive carrier into the bay until the handle retracts and the hard drive carrier clicks into the locked position.
3. Close and lock the front cover.



4 System setup

4.1 Default settings

DIVAR IP systems are shipped with a pre-installed Configuration Wizard from factory.
All DIVAR IP systems are preconfigured with a default IP address and with default iSCSI settings:

– IP Address: automatically assigned by DHCP (fallback IP address: 192.168.0.200).
– Subnet mask: automatically assigned by DHCP (fallback subnet mask: 255.255.255.0).

Default user settings for administrator account

– User: BVRAdmin
– Password: WSS4Bosch

4.2 Prerequisites

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.

4.3 Operating modes

The DIVAR IP system can operate in three different modes:

- Full video recording and management system, utilizing the BVMS and VRM core components and services: This mode allows for advanced video management features such as event and alarm handling.
- Pure video recording system, utilizing the VRM core components and services.
- iSCSI storage expansion for a BVMS or VRM system, which runs on a different hardware.

Notice!
Recorded video streams need to be configured in a way that the maximum bandwidth of the system (BVMS/VRM base system plus iSCSI storage expansions) is not exceeded.

4.4 Preparing hard drives for video recording

Systems that come pre-equipped with hard drives from factory are ready to record out-of-the-box.
Hard drives that have been added to an empty system need to be prepared (formatted) before using them for video recording.

To format a hard drive you have following options:

– Performing the initial factory setup: see *Recovering the unit, page 30*.
– Executing the formatting script.

Executing the formatting script

To execute the formatting script, you have to logon to the administrator account (BVRAdmin).

1. Boot the system.
2. On the BVMS default screen, press CTRL+ALT+DEL.
3. Hold SHIFT, click **Switch User** and keep SHIFT pressed for about five seconds.
4. Enter administrator user name and password.
5. On the Desktop, in the **Tools** folder, right-click the **Format_data_hard_drives** script, and then click **Run as administrator**.
6. Follow the instructions.
7. After formatting you can add the storage to the video management configuration.

Notice!
Formatting a hard drive deletes all existing data on the hard drive.

4.5 Starting the application

The application provides a simple to install and intuitive to use solution for network surveillance systems.

To start the application:

1. Connect the unit and the cameras to the network.
2. Turn on the unit.
   The Windows Storage Server 2016 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.
6. After restart is finished, press CTR+ALT+DELETE. The Windows logon page is displayed.
7. Enter the default password **WSS4Bosch**.
8. After entering the password, a message is displayed that you must change the password before logging on the first time. To confirm, click **OK**.
9. Change the password.
   A series of scripts perform important setup tasks. This can take several minutes. Do not turn off the computer.
   The BVMS default screen is displayed.
   You can now decide in which mode you want to operate the system:
   - *Operating as full video recording and management system, page 24*
   - *Operating as pure video recording system, page 24*
   - *Operating as iSCSI storage expansion, page 24*

Notice!
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.

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

Notice!
To perform administrative tasks, you have to log on to the administrator account.

4.5.1 Operating as full video recording and management system

To operate the DIVAR IP system as full video recording and management system:

1. On the BVMS default screen, double-click the BVMS Config Wizard icon  to start the Config Wizard.
   The **Welcome** page is displayed.
2. Configure the system using the Config Wizard.

See also

– *Using BVMS Config Wizard, page 25*

4.5.2 Operating as pure video recording system

To operate the DIVAR IP system as pure video recording system, you have to logon to the administrator account (BVRAdmin) in order to perform the necessary configuration steps.

1. On the BVMS default screen, press CTRL+ALT+DEL.
2. Hold SHIFT, click **Switch User** and keep SHIFT pressed for about five seconds.
3. Enter administrator user name and password.
4. On the Desktop, in the **Tools** folder, right-click the **Disable_BVMS** script, and then click **Run as administrator**.
5. Configure the Video Recording Manager (VRM) from an external system using BVMS Configuration Client or Configuration Manager.

4.5.3 Operating as iSCSI storage expansion

To operate the DIVAR IP system as an iSCSI storage expansion, you have to logon to the administrator account (BVRAdmin) in order to perform the necessary configuration steps.

1. On the BVMS default screen, press CTRL+ALT+DEL.
2. Hold SHIFT, click **Switch User** and keep SHIFT pressed for about five seconds.
3. Enter administrator user name and password.
4. On the Desktop, in the **Tools** folder, right-click the **Disable_BVMS_and_VRM** script, and then click **Run as administrator**.
5. Add the system as an iSCSI storage expansion to an external BVMS or VRM server using BVMS Configuration Client or Configuration Manager.

4.6 Using BVMS 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 Config Wizard. Use BVMS Configuration Client instead.

– adjusting schedules
– configuring systems with no or multiple Video Recording Manager
– 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 Config Wizard:

1. On the BVMS default screen, double-click the Config 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 Config Wizard, and for detailed information concerning Config Wizard itself, refer to the BVMS manual available in the online product catalog.

See also

– *Additional documentation and client software, page 32*

4.7 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 BVMS 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.

4.8 Using BVMS Operator Client

Use BVMS 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 BVMS 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 camera is viewed in playback mode.

To perform further functionalities refer to the BVMS manual available in the online product catalog.

5 Remote connection to the system

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:

- ▸ Enter following port rules in the port forwarding settings of your internet router:
  - – port 5322 for SSH tunnel access using BVMS Operator Client.
  - – port 443 for HTTPS access to VRM using Video Security Client or Video Security App.

The DIVAR IP system is now accessible from the Internet.

5.3 Choosing an appropriate client

This chapter describes the ways that allow remote connection to a DIVAR IP system through the internet.

There are 2 ways to make a remote connection:

- – *Remote connection with Operator Client, page 29*.
- – *Remote connection with Video Security App, page 29*.

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

5.3.1 Remote connection with Operator Client

To make a remote connection with BVMS Operator Client:

1. Install BVMS Operator Client on the client workstation.
2. After finishing the installation successfully, start Operator Client using the desktop shortcut  .
3. Enter the following, then click **OK**.
   User name: admin (or other user in case one is configured)
   Password: enter user password
   Connection: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

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.
6. Make sure Secure Connection (SSL) is switched on.
7. Select **Add**.
8. Enter the following:
   User name: admin (or other user in case one is configured)
   Password: enter user password

6 Maintenance

6.1 Monitoring the system

The system provides tools for health monitoring.
To activate the monitoring functionality, you have to logon to the administrator account (BVRAdmin).

1. On the BVMS default screen, press CTRL+ALT+DEL.
2. Hold SHIFT, click **Switch User** and keep SHIFT pressed for about five seconds.
3. Enter user name and password.
4. On the Desktop, in the **Tools** folder, right-click the **Enable_SuperDoctor_5_Service** script, and then click **Run as administrator**.
5. Double-click the **SuperDoctor 5 Web** icon in the same folder.
6. Log on to the web interface using the following default credentials:
   User Name: ADMIN
   Password: ADMIN
7. Click the **Configuration** tab, and then click **Password Settings** and change the default password.
8. Click the **Configuration** tab, and then click **Alert Configuration**.
9. Activate the **SNMP Trap** feature and specify the IP address of the receiver for SNMP traps.

6.2 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.
2. Select one of the following:
   - **Initial factory setup:** restores to factory default image and deletes all data on the HDDs.
     or
   - **System Recovery (back to Factory Defaults):** restores to factory default image; data on the HDDs will not be deleted.

Note:
While the **System Recovery** option doesn't delete video footage stored on the data HDDs, it still replaces the complete OS partition (including VMS settings) with a default configuration. In order to access existing video footage after recovery, the VMS configuration needs to be exported before System Recovery and re-imported afterwards.

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.

6.3 Service and repair

The storage system is backed by a 3-year warranty. Issues will be handled according to Bosch Service and Support guidelines. The storage equipment is shipped with an original manufacturer Service and Support agreement.
The Bosch Technical Support is the Single Point of Contact in case of failure but the Service and Support obligations are fulfilled by the manufacturer or a partner.
In order to enable the manufacturer's Service and Support organization to fulfill the defined Service Levels, the system must be re-registered. Otherwise, the defined service level cannot be provided but only best effort.
A description what information is required and where to send is included in each shipment as paper work. The description is also electronically available in the Bosch online product catalog.

7 Additional documentation and client software

For more information, software downloads, and documentation, visit www.boschsecurity.com and go to the respective product page.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com