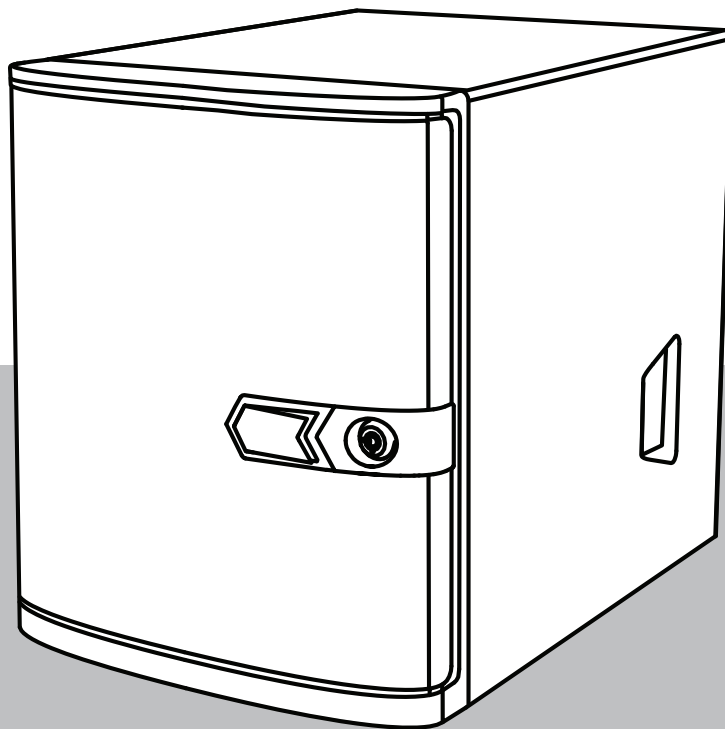




BOSCH

DIVAR IP all-in-one 4000

DIP-4420IG-00N | DIP-4424IG-2HD | DIP-4428IG-2HD |
DIP-442IIG-2HD



en

Installation manual

Table of contents

1	Safety	4
1.1	Safety message explanation	4
1.2	Installation precautions	4
1.3	Electrical safety precautions	5
1.4	ESD precautions	7
1.5	Operating precautions	7
1.6	Service and maintenance precautions	8
1.7	Cybersecurity precautions	9
1.8	Compliance	10
1.9	Software precautions	11
1.9.1	Use latest software	11
1.9.2	OSS information	11
2	Introduction	12
2.1	Parts included	12
2.2	Product registration	12
3	System overview	13
3.1	Device views	13
3.2	Control panel elements	15
3.3	Hard drive tray LEDs	16
3.4	LAN LEDs	17
4	Installing a SATA hard drive	18
4.1	Installing a Bosch-supplied hard drive	18
4.2	Installing a non-Bosch-supplied hard drive	20
5	Turning on the unit	24
6	System setup	25
6.1	Default settings	25
6.2	Prerequisites	25
6.3	Operation modes	25
6.4	First sign-in and initial system setup	26
6.4.1	Choosing operation mode BVMS	28
6.4.2	Choosing operation mode VRM	28
6.4.3	Choosing operation mode iSCSI storage	28
6.5	Signing in to the administrator account	29
6.6	Configuring new hard drives	29
6.7	Recovering the unit	30
7	Troubleshooting	32
8	Service and repair	33
9	Decommissioning and disposal	34
10	Additional information	35
10.1	Additional documentation and client software	35
10.2	Support services and Bosch Academy	35

1 Safety

Read, follow, and retain for future reference all of the following safety instructions.

1.1 Safety message explanation

**Warning!**

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

**Caution!**

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

**Notice!**

Indicates a situation which, if not avoided, could result in damage to the equipment, to the environment, or to data loss.

1.2 Installation precautions

**Notice!**

Installation must only be carried out by authorized specialist personnel.

**Notice!**

The installation of this product must comply with all requirements of the applicable local code.

**Notice!**

Install this product only in a dry, weather-protected location.

**Notice!**

Do not install the device near any heat sources, such as radiators, heaters, stoves, or other equipment which produces heat.

**Notice!**

Install this product according to the instructions of the manufacturer.

**Notice!**

Accessories

Use only accessories recommended by the manufacturer. Do not use accessories that are not recommended by the manufacturer, as they may cause hazards.

**Notice!**

If you install this device in an enclosure, make sure that the enclosure is adequately ventilated according to the manufacturer's instructions.

**Caution!**

Installation precaution

Do not place this device on an unstable stand, tripod, bracket, or mount. The device may fall, causing serious injury to persons and damage to the device. Mount the device according to the instructions of the manufacturer.

1.3**Electrical safety precautions****Warning!**

Fire or electrical shock

Do not expose this device to rain or moisture to reduce the risk of fire or electrical shock.

**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!**

This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that the protective device is rated not greater than: 250 V, 20 A.

**Notice!**

Safety Extra Low Voltage (SELV) circuits

All the input/output ports are SELV circuits. Connect SELV circuits only to other SELV circuits.

**Notice!**

Power supplies

Operate the product only from the type of power source indicated on the label. Use only the provided power supply or UL approved power supplies. Use a power supply according to LPS or NEC Class 2.

**Warning!**

Make sure that the power supply cord includes a grounding plug and is plugged into a grounded electrical outlet.

**Notice!**

Protect connection cables

Protect all connection cables from possible damage, especially at connection points.

**Notice!**

Permanently connected devices must have an external, readily operable mains plug or all-pole mains switch in accordance with installation rules.

**Notice!**

Pluggable devices must have an easily accessible electrical outlet installed near the equipment.

**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!**

Do not put any objects in the openings of this product. The objects may touch dangerous voltage points or short-circuit components, which could result in a fire or electrical shock.

**Caution!**

Power supply cords

Make sure to route the power supply cords in a way so that they are protected from any possible damage.

**Warning!**

To prevent electrical shock hazard, disconnect all power cables from the electrical outlet before relocating the system.

**Caution!**

Disconnect power cables before installing or removing any components from the device.

**Notice!**

When disconnecting power, first turn off the system and then unplug the power cord from the power supply module in the system.

**Notice!**

Be aware of the locations of the power on/off switch on the device 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.

**Warning!**

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.

1.4 ESD precautions

**Notice!**

Electrostatically sensitive device

Electrostatic Discharge (ESD) can damage electronic components. To avoid electrostatic discharges, use proper CMOS/MOSFET protection measures.

- 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.

1.5 Operating precautions

**Notice!**

Intended use

This product is for professional use only. It is not intended to be installed in a public area that is accessible to the general population.

**Notice!**

Do not use this product in any humid or wet location.

**Notice!**

Take precautions to protect the device from power and lightning surges.

**Notice!**

Keep the area around the device clean and free of clutter.

**Notice!**

Enclosure openings

Do not block or cover the openings. Any openings in the enclosure are provided for ventilation purposes. These openings will prevent overheating and ensure a reliable operation.

**Notice!**

Do not open or remove the device cover. Opening or removing the cover may cause damage to the system and will void the warranty.

**Notice!**

Do not spill any liquid on the device.

**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.

**Notice!**

Disconnect the power before moving the product. Move the product with care. Excessive force or shock may damage the product and the hard disk drives.

**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!**

Video loss is inherent to digital video recording; therefore, Bosch Security Systems cannot be held liable for any damage that results from missing video information.

To minimize the risk of losing information, we recommend multiple, redundant recording systems, and a procedure to back up all analog and digital information.

1.6

Service and maintenance precautions

**Notice!**

Do not attempt to service this product. Refer all servicing to qualified service personnel.

**Notice!**

Damaged device

Whenever your device is damaged, disconnect the power supply, and contact your qualified service personnel.

- If safe operation of the device cannot be ensured, remove it from service and secure it to prevent unauthorized operation. In such cases, contact the Bosch technical support.
- Disconnect power supply and arrange for the device to be serviced by qualified personnel in the following cases, because safe operation is no longer possible:
 - The power cable/plug is damaged.
 - Liquids or foreign bodies have entered the device.
 - The device has been exposed to water or extreme environmental conditions.
 - The device is faulty despite correct installation/operation.
 - The device has fallen from a height, or the housing has been damaged.
 - The device was stored over a long period under adverse conditions.
 - The device performance is noticeably changed.

**Warning!****Battery replacement - For qualified service personnel only**

A lithium battery is located inside the unit enclosure. To avoid danger of explosion, replace the battery as per instructions. Replace only with the same or equivalent 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 the replaced battery in an environmentally friendly way and not with other solid waste. Follow the local directives.

**Warning!****Hot swap fan replacement - For qualified service personnel only**

Hazardous moving parts. Keep away from moving fan blades. The fan blades might still be turning when you remove the fan assembly from the chassis. Keep fingers, screwdrivers, and other objects away from the openings in the fan assembly's housing.

**Warning!**

Replacement parts specified by the manufacturer

Use replacement parts specified by the manufacturer. Unauthorized replacements could void the warranty and cause fire, electrical shock, or other hazards.

**Notice!**

Perform safety inspections after service or repairs to the device to make sure the device operates properly.

1.7

Cybersecurity precautions

For cybersecurity reasons, observe the following:

- Make sure that the physical access to the system is restricted to authorized personnel only. Place the system in an access control protected area, in order to avoid physical manipulation.
- Lock the front bezel to protect against unauthorized removal of the hard drives. Always remove the key from the lock and store the key in a secure place.
- Use the rear chassis hasp or the Kensington slot to additionally secure the device.
- The operating system includes the latest Windows security patches available at the time the software image was created. Use the Windows online update functionality or the corresponding monthly roll-up patches for offline installation to regularly install OS security updates.
- Do not switch off Windows Defender and Windows firewall, and always keep it up to date.
- Do not install additional anti-virus software.
- Do not provide system information and sensitive data to persons you do not know unless you are certain of a person's authority.
- Do not send sensitive information over the internet before checking a website's security.
- Limit local network access to trusted devices only. Details are described in the following documents which are available in the online product catalog:
 - *Network Authentication 802.1X*
 - *Cybersecurity guidebook for Bosch IP video products*
- For access through public networks use only the secure (encrypted) communication channels.

- The administrator account provides full administrative privileges and unrestricted access to the system. Administrative rights enable users to install, update, or remove software, and to change configuration settings. Furthermore, administrative rights enable users to directly access and change registry keys and with this to bypass central management and security settings. Users signed in to the administrator account can traverse firewalls and remove anti-virus software, which will expose the system to viruses and cyber-attacks. This can pose a serious risk to the system and data security.
To minimize cybersecurity risks, observe the following:
 - Make sure that the administrator account is protected with a complex password according to the password policy.
 - Make sure that only limited number of trusted users has access to the administrator account.
- Due to operation requirements, the system drive must not be encrypted. Without encryption, the data stored on this drive can be easily accessed and removed. To avoid data theft or accidental loss of data, make sure that only authorized persons have access to the system and to the administrator account.
- For installation and update of software as well as for system recovery, it might be necessary to use USB devices. Therefore, the USB ports of your system must not be disabled. However, connecting USB devices to the system poses a risk of malware infection. To avoid malware attacks, make sure that no infected USB devices are connected to the system.

1.8

Compliance

Canada

CAN ICES-003(B) / NMB-003(B)

United States of America

FCC Supplier's Declaration of Conformity

F.01U.404.040	DIP-4420IG-00N	Management Appliance w/o HDD
F.01U.404.041	DIP-4424IG-2HD	Management Appliance 2x4TB
F.01U.404.042	DIP-4428IG-2HD	Management Appliance 2x8TB
F.01U.404.043	DIP-442IIG-2HD	Management Appliance 2x18TB

Compliance statement

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.

Responsible party

Bosch Security Systems, LLC
130 Perinton Parkway
14450 Fairport, NY, USA
www.boschsecurity.us

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: 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.

1.9 Software precautions

1.9.1 Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:

- General information: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.

You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under:

<https://downloadstore.boschsecurity.com/>

1.9.2 OSS information

Bosch uses Open Source Software in the DIVAR IP all-in-one products.

You can find the licenses of the used Open Source Software components on the system drive under:

```
C:\license txt\
```

The licenses of Open Source Software components used in any further software installed on your system, are stored in the installation folder of the respective software, for example under:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-commander\[version]\License
```

or under:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Introduction

2.1 Parts included

Make sure that all parts are included and not damaged. If the packaging or any parts are damaged, contact your shipper. If any parts are missing, contact your Sales or Customer Service Representative.

DIP-4420IG-00N

Quantity	Component
1	DIVAR IP all-in-one 4000
1	Installation manual
1	Registration leaflet
1	Power cord EU
1	Power cord US
2	Keys
3	Labels for hard drive trays (numbered 0-2)
18	Hard drive screws

DIP-4424IG-2HD, DIP-4428IG-2HD, DIP-442IIG-2HD

Quantity	Component
1	DIVAR IP all-in-one 4000
1	Installation manual
1	Registration leaflet
1	Power cord EU
1	Power cord US
2	Keys
3	Labels for hard drive trays (numbered 0-2)

2.2 Product registration

Register your product under:

<https://www.boschsecurity.com/product-registration/>



3 System overview

DIVAR IP all-in-one 4000 is a mini tower unit with two front-swappable SATA hard drives. It is an easy to use all-in-one recording, viewing, and management solution for network surveillance systems.

Running the full 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 4000 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 4000 is based on the operating system Microsoft Windows Server IoT 2022 for Storage Workgroup.

DIVAR IP System Manager is the central user interface that offers an easy system setup, configuration and software upgrade.

3.1 Device views

DIVAR IP all-in-one 4000 has a compact mini-tower chassis. It has a hinged front cover that hides the hard drives and the control panel.

The control panel is located on the front of the device and has power buttons and status monitoring LEDs.

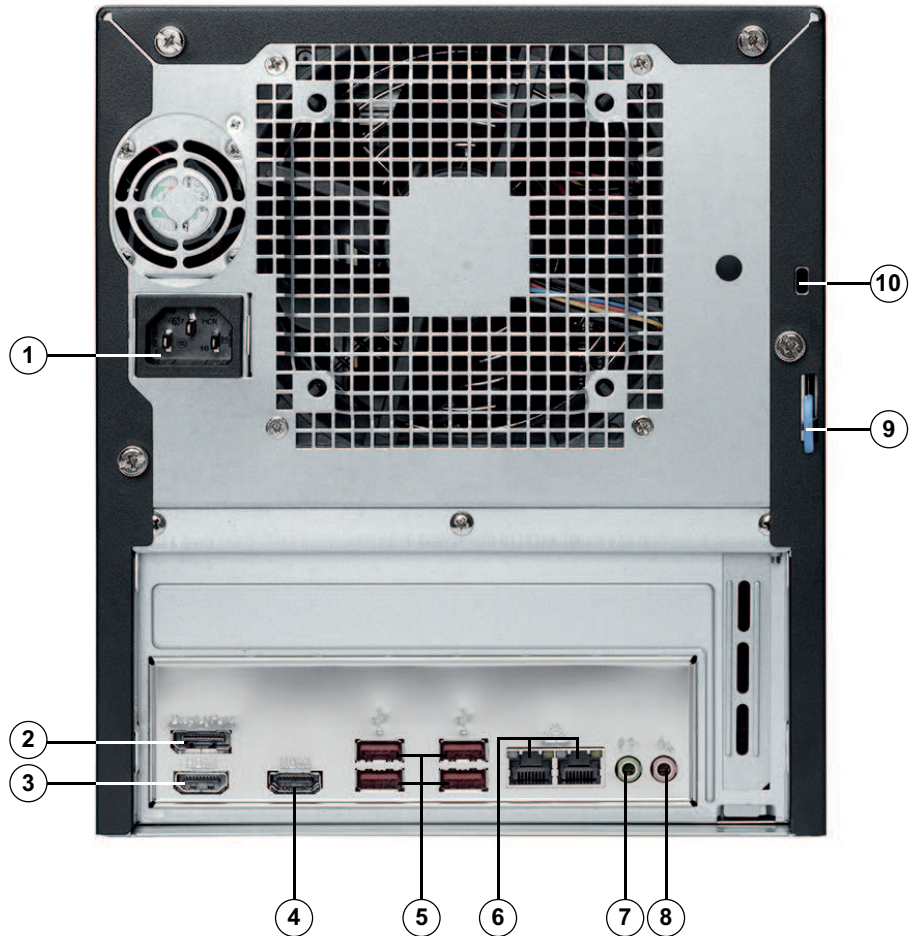
On the rear of the device, there are various I/O ports.

Front view



1	Front cover	2	Lock for front cover
3	2 hard drive bays (for 3.5" hard drives)	4	Air intake filter
5	2 slot covers Note: Do not remove!	6	Power LED
7	HDD LED	8	Network LED
9	Information LED	10	Reset button
11	2 USB 2.0 ports (Type A)	12	Power on/off button

Rear view





1	Mains connection	2	DisplayPort port
3	HDMI 2.0 port	4	HDMI 1.4 port
5	4 USB 3.2 ports (Type A)	6	2 LAN ports (RJ45), teamed Note: Do not change the teaming mode!
7	Audio output: Line-out	8	Audio input: Mic-level input
9	Rear chassis hasp (compatible with a variety of commonly available locks). Note: Locks are not included.	10	Kensington security slot (for a standard Kensington lock). Note: Kensington lock is not included.





3.2 Control panel elements

The control panel located on the front of the device has 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.
 Reset	The reset button is used to reboot the system.

Control panel LEDs

LED	LED state	Description
 Power	Solid green	This LED indicates that power is supplied to the system's power supply unit. This LED is illuminated when the system is operating.
 HDD	Amber flashing	This LED indicates activity on the HDDs or on peripheral drives when flashing.
 Network	Green flashing	This LED indicates network activity when flashing.
 Information	This LED indicates the system status.	
	Solid red	An overheat condition has occurred. (This might be caused by cable congestion.)
	Blinking red (1 Hz)	Fan failure: check for an inoperative fan.

3.3

Hard drive tray LEDs

The device supports swappable SATA hard drives in hard drive trays. Each hard drive tray has two LEDs on the front of the tray.

Note: For non-RAID configurations, some LED indications are not supported, for example hot spare.

LED	LED state	Description
Upper hard drive tray LED	Green flashing	Indicates HDD activity.

LED	LED state	Description
Lower hard drive tray LED	Not used	

3.4

LAN LEDs

On the rear of the device, there are two LAN ports. Each LAN port has two LEDs.

LED	LED state	Description
LAN 1/LAN 2 LED on the right	Amber flashing	Indicates LAN activity.
LAN 1/LAN 2 LED on the left	Solid green	Indicates a bandwidth of 100 Mbps.
	Solid amber	Indicates a bandwidth of 1 Gbps.
	Off	Indicates a bandwidth of 10 Mbps.

4 Installing a SATA hard drive

DIVAR IP all-in-one 4000 has two front-swappable SATA hard drives. The hard drives are mounted in hard drive trays to simplify their installation and removal from the chassis. The hard drive trays also help promote proper airflow for the hard drive bays.

Notice!

Bosch strongly recommends to use hard drives approved and supplied by Bosch. The hard drives as one of the critical component are carefully selected by Bosch based on available failure rates.

Bosch is not liable for any data loss or damages, or system failures of units equipped with hard drives that are not supplied by Bosch.

Bosch cannot provide support if non-Bosch-supplied hard drives are considered to be the cause of the problem. To troubleshoot potential hardware issues, Bosch will require Bosch-supplied hard drives to be installed.

For more information about Bosch-supplied hard drives, see the datasheet in the Bosch online product catalog under:

www.boschsecurity.com



Notice!

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



Procedure

The installation procedure for Bosch-supplied hard drives and non-Bosch-supplied hard drives differs.

Refer to

- *Installing a Bosch-supplied hard drive, page 18*
- *Installing a non-Bosch-supplied hard drive, page 20*

4.1 Installing a Bosch-supplied hard drive

Notice!

Hard drives supplied by Bosch come already pre-installed in a hard drive tray.



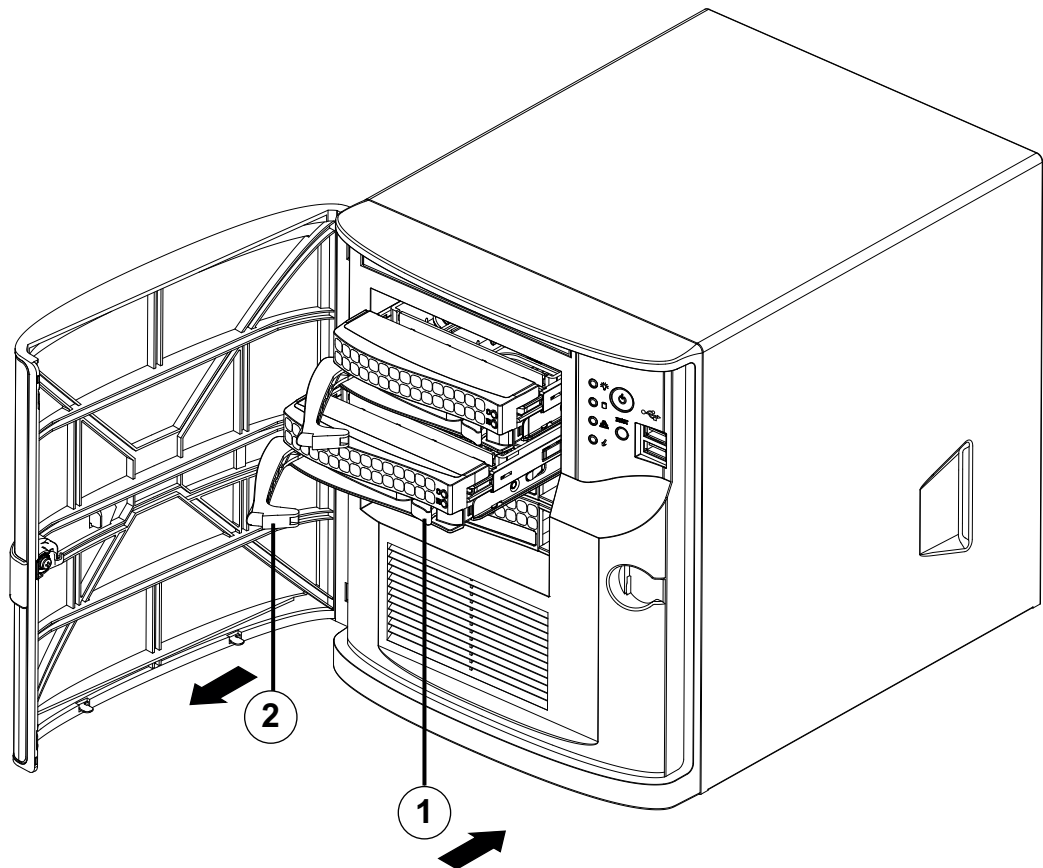
To install a Bosch-supplied hard drive, you must do the following:

1. *Removing a hard drive tray from a hard drive bay, page 18.*
2. *Installing a hard drive tray into a hard drive bay, page 19.*

Removing a hard drive tray from a hard drive bay

To remove a hard drive tray 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 tray. This extends the hard drive tray handle.
3. Use the handle to pull the hard drive tray out of the chassis.



1	Release button
2	Hard drive tray handle

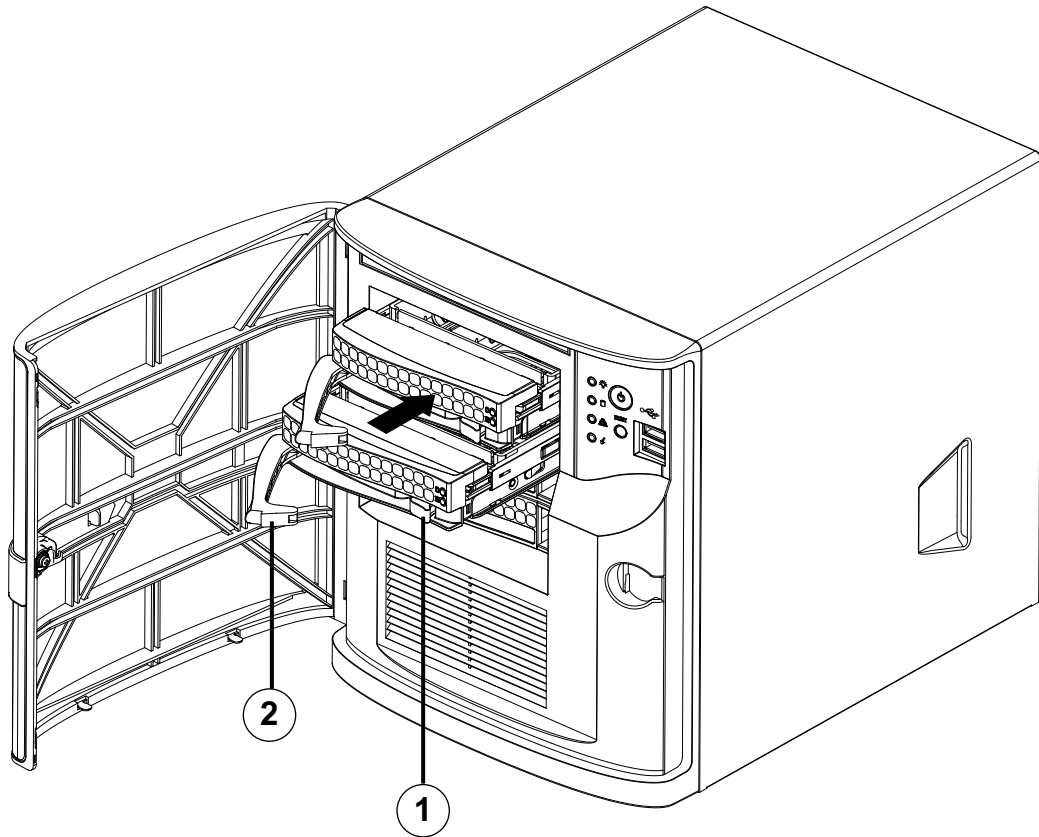
**Notice!**

Do not operate the device with the hard drive trays removed from the bays.

Installing a hard drive tray into a hard drive bay

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

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



1	Release button	2	Hard drive tray handle
---	----------------	---	------------------------

4.2 Installing a non-Bosch-supplied hard drive

Notice!

Bosch strongly recommends to use hard drives approved and supplied by Bosch. The hard drives as one of the critical component are carefully selected by Bosch based on available failure rates.

Bosch is not liable for any data loss or damages, or system failures of units equipped with hard drives that are not supplied by Bosch.

Bosch cannot provide support if non-Bosch-supplied hard drives are considered to be the cause of the problem. To troubleshoot potential hardware issues, Bosch will require Bosch-supplied hard drives to be installed.

For more information about Bosch-supplied hard drives, see the datasheet in the Bosch online product catalog under:

www.boschsecurity.com



To install a non-Bosch-supplied hard drive, you must do the following:

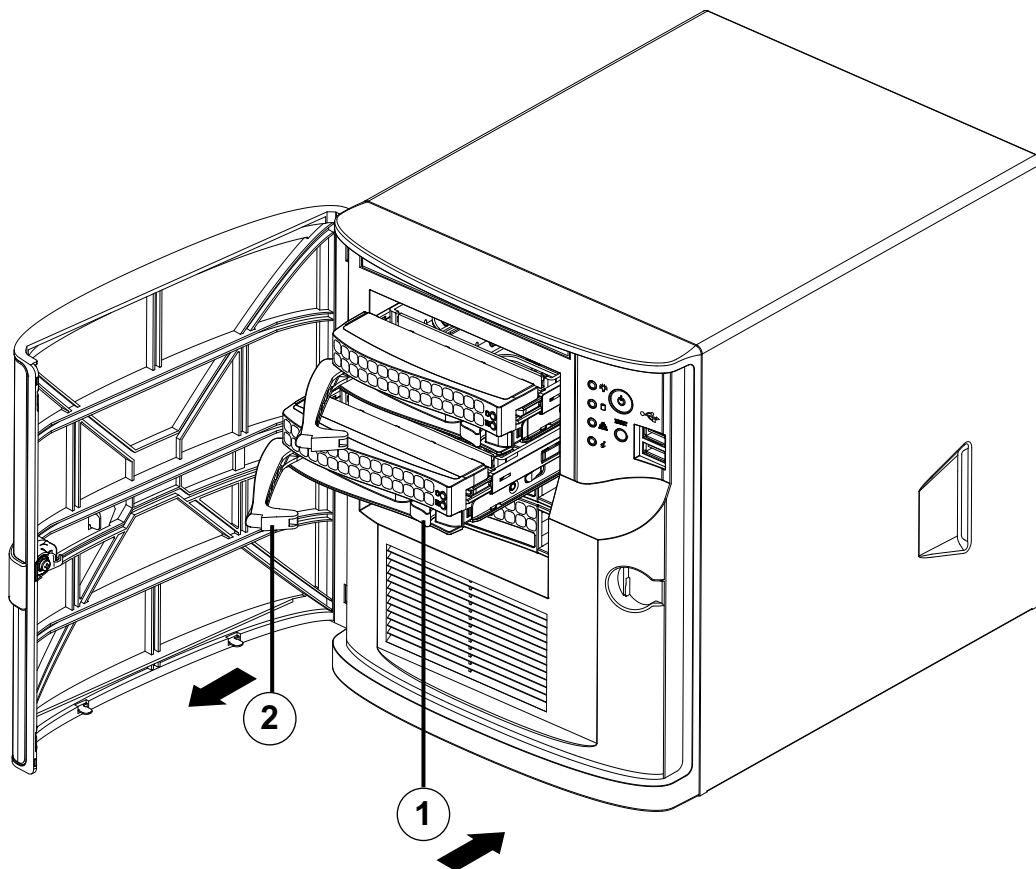
1. *Removing a hard drive tray from a hard drive bay, page 18.*
2. *Installing a hard drive into a hard drive tray, page 21.*
3. *Installing a hard drive tray into a hard drive bay, page 19.*

Removing a hard drive tray from a hard drive bay

To remove a hard drive tray 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 tray. This extends the hard drive tray handle.

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



1	Release button	2	Hard drive tray handle
---	----------------	---	------------------------



Notice!

Do not operate the device with the hard drive trays removed from the bays.

Installing a hard drive into a hard drive tray

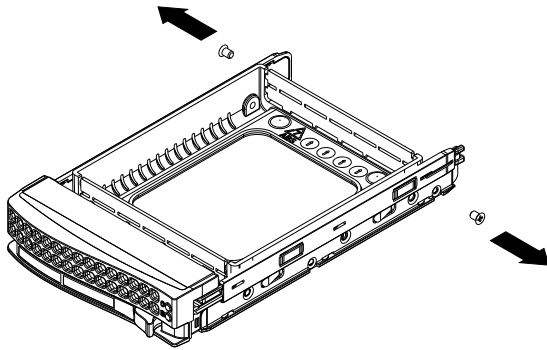


Notice!

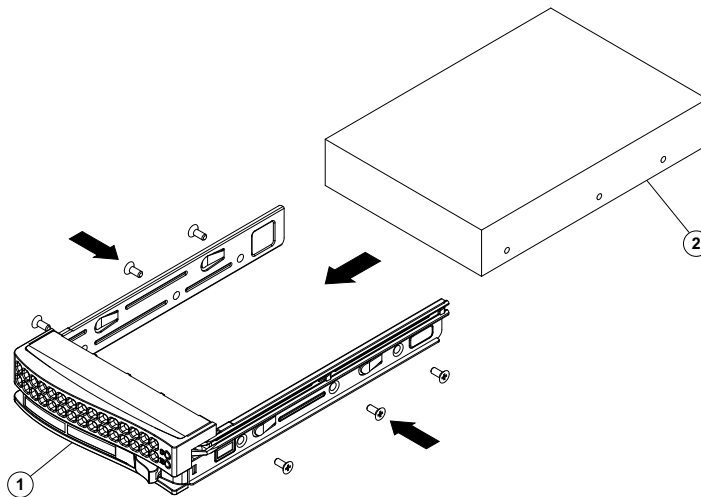
This description applies only to DIP-4420IG-00N units.

To install a hard drive into a hard drive tray:

1. Remove the screws, which secure the plastic bracket to the hard drive tray.



2. Remove the plastic bracket from the hard drive tray and place the hard drive tray on a flat surface.
3. Slide a new hard drive into the hard drive tray with the printed circuit board side facing down.
4. Align the mounting holes in both, the hard drive tray and the hard drive.
5. Secure the hard drive to the hard drive tray with six screws (additional screws are delivered with the unit).

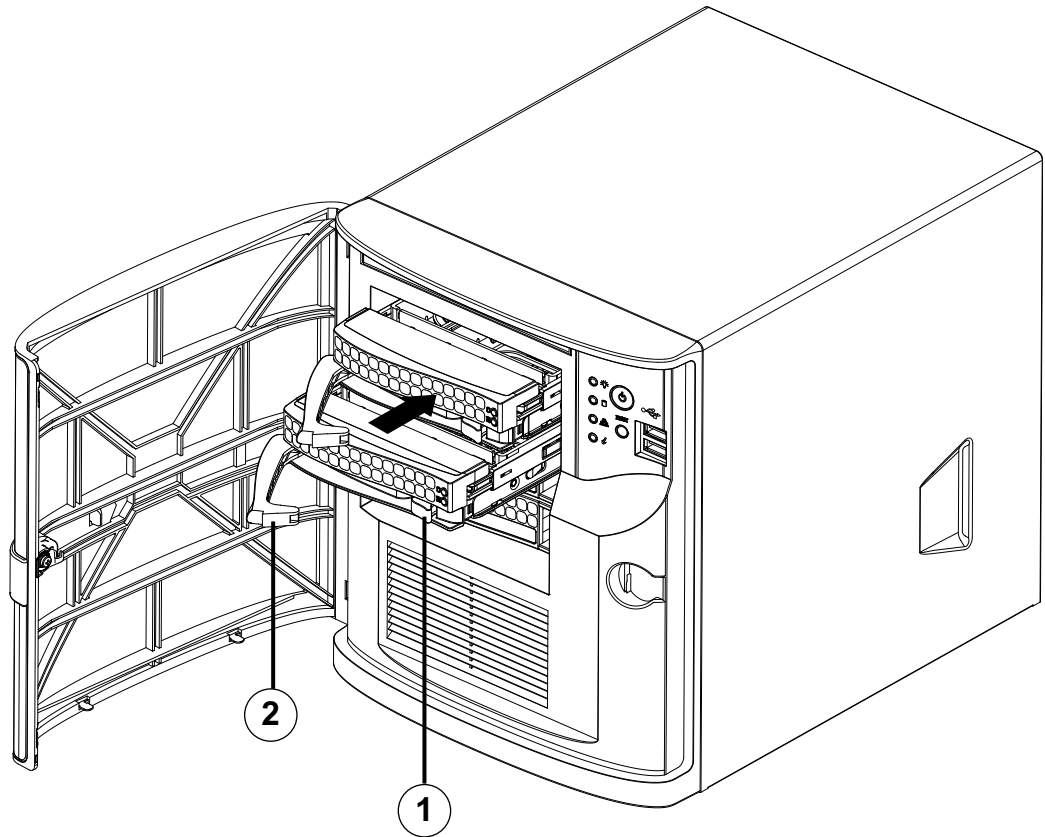


1	Hard drive tray	2	SATA hard drive
---	-----------------	---	-----------------

Installing a hard drive tray into a hard drive bay

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

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



1 Release button	2 Hard drive tray handle
------------------	--------------------------

5 Turning on the unit

Prerequisite

DIVAR IP needs to have an active network link during installation. Make sure that the network switch you are connecting to is powered on.

To turn on the unit:

1. Plug the power cord from the power supply unit into a high-quality power strip that offers protection from electrical noise and power surges.
Bosch recommends to use an uninterruptible power supply (UPS).
2. Push the power button on the control panel to turn on the unit.

To turn off the unit:

1. Sign in to the administrator account BVRAdmin. For more information, refer to Signing in to the administrator account.
2. Shut down the unit normally via the Windows **Start** menu.

6 System setup

The Microsoft Windows Server IoT 2022 for Storage Workgroup operating system provides a user interface for initial server configuration, unified storage appliance management, simplified setup and storage management, and support for Microsoft iSCSI Software Target. It is specially tuned to provide optimal performance for network-attached storage. The Microsoft Windows Server IoT 2022 for Storage Workgroup operating system provides significant enhancements in storage management scenarios, as well as integration of storage appliance management components and functionality.

DIVAR IP System Manager application is the central user interface that offers an easy system setup, configuration and software upgrade.



Notice!

The following description is valid for DIVAR IP all-in-one units that come with pre-installed hard drives.

If you have installed hard drives to an empty unit, you first must configure them before performing the initial setup.

Refer to

- *Configuring new hard drives, page 29*

6.1 Default settings

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 name: **BVRAdmin**
- Password: to be set at first sign-in.
Password requirements:
 - Minimum 14 characters.
 - At least one upper case letter.
 - At least one lower case letter.
 - At least one digit.

6.2 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.

6.3 Operation modes

DIVAR IP all-in-one systems 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.
- Advanced video recording solution for BVMS 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.

6.4 First sign-in and initial system setup

**Notice!**

Do not change any operating system settings. Changing operating system settings can result in malfunctioning of the system.

**Notice!**



To perform administrative tasks, you must sign in to the administrator account.

**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.

To setup the system:

1. Connect the DIVAR IP all-in-one unit and the cameras to the network.
2. Turn on the unit.
Setup routines for Microsoft Windows Server IoT 2022 for Storage Workgroup are performed. This process can take several minutes. Do not turn off the system.
After the process is completed, the Windows language selection screen is displayed.
3. Select your country/region, the desired operating system language and the keyboard layout from the list, then click **Next**.
The Microsoft software license terms are displayed.
4. Click **Accept** to accept the license terms and wait until Windows restarts. This can take several minutes. Do not turn off the system.
After restart, the Windows sign-in page is displayed.
5. Set a new password for the administrator account **BVRAdmin** and confirm it.
Password requirements:
 - Minimum 14 characters.
 - At least one upper case letter.
 - At least one lower case letter.
 - At least one digit.Then press Enter.
The **Software Selection** page is displayed.
6. The system automatically scans the local drive and any connected external storage media for the DIVAR IP System Manager installation file **SystemManager_x64_[software version].exe**, which is located in a folder with the following structure: `Drive root\BoschAppliance\`.
The scan might take some time. Wait for it to complete.

7. Once the system has detected the installation file, it is displayed on the **Software Selection** page. Click the bar that displays the installation file to start the installation.
Notice: Make sure that the latest version of DIVAR IP System Manager is installed. You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under: <https://downloadstore.boschsecurity.com/>.
 8. If the installation file is not found during the scan process, proceed as follows:
 - Go to <https://downloadstore.boschsecurity.com/>.
 - Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**. A list of all available software packages is displayed.
 - Locate the ZIP file **SystemManager_[software version].zip** and save it to a storage medium such as a USB stick.
 - Unzip the file on the storage medium by making sure that the folder **BoschAppliance** is placed in the root of the storage medium.
 - Connect the storage medium to your DIVAR IP all-in-one system. The system will automatically scan the storage medium for the installation file. The scan might take some time. Wait for it to complete.
 - Once the installation file is detected, it will be displayed on the **Software Selection** page. Click the bar that displays the installation file to start the installation.
Note: To be automatically detected, the installation file must be located in a folder with the following structure: Drive root\BoschAppliance\ (for example F:\BoschAppliance\).
If the installation file is located at another location that does not match the pre-
- 
- defined folder structure, click  to navigate to the respective location. Then click the installation file to start the installation.
9. Before the installation starts, the **End User License Agreement (EULA)** dialog box is displayed. Read the license terms, then click **Accept** to continue. The installation starts.
 10. After the installation is complete, the system restarts and you are directed to the Windows sign-in page. Sign in to the administrator account.
 11. The Microsoft Edge browser opens and the **DIVAR IP - System setup** page is displayed. The page shows the device type and the device serial number, as well as the three operation modes and the available software versions for each operation mode. You must choose the desired operation mode and the desired software version to configure your DIVAR IP all-in-one system.
Note: If the desired software version for the respective operation mode is not available on a local drive, proceed as follows:
 - Go to <https://downloadstore.boschsecurity.com/>.
 - Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**. A list of all available software packages is displayed.
 - Locate the ZIP files of the desired software packages, for example **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, and save them to a storage medium such as a USB stick.
 - Unzip the files on the storage medium. Do not change the folder structure of the unzipped files.
 - Connect the storage medium to your DIVAR IP all-in-one system.

**Notice!**

Changing the operation mode after installation requires a full factory reset.

**Notice!**

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under: <https://downloadstore.boschsecurity.com/>.

6.4.1**Choosing operation mode BVMS**

To operate the DIVAR IP all-in-one system as a full video recording and management system:

1. On the **DIVAR IP - System setup** page, select the operation mode **BVMS** and the desired BVMS version that you want to install, then click **Next**.
The BVMS license agreement is displayed.
2. Read and accept the license agreement, then click **Install** to continue.
The installation starts and the installation dialog box shows the installation progress. Do not turn off the system and do not remove the storage media during the installation process.
3. After all software packages have been installed successfully, the system restarts. After restart, you are directed to the BVMS desktop.
4. On the BVMS desktop, click the desired application to configure your system.

**Notice!**

For further details, refer to the respective DIVAR IP all-in-one web-based training and to the BVMS documentation.

You can find the training under: www.boschsecurity.com/xc/en/support/training/

6.4.2**Choosing operation mode VRM**

To operate the DIVAR IP all-in-one system as a pure video recording system:

1. On the **DIVAR IP - System setup** page, select the operation mode **VRM** and the desired VRM version that you want to install, then click **Next**.
The VRM license agreement is displayed.
2. Read and accept the license agreement, then click **Install** to continue.
The installation starts and the installation dialog box shows the installation progress. Do not turn off the system and do not remove the storage media during the installation process.
3. After all software packages have been installed successfully, the system restarts. After restart, you are directed to the Windows sign-in screen.

**Notice!**

For further details, refer to the VRM documentation.

6.4.3**Choosing operation mode iSCSI storage**

To operate the DIVAR IP all-in-one system as an iSCSI storage expansion:

1. On the **DIVAR IP - System setup** page, select the operation mode **iSCSI storage** and the desired iSCSI storage version that you want to install, then click **Next**.
The installation dialog box is displayed.
2. In the installation dialog box, click **Install** to continue.
The installation starts and the installation dialog box shows the installation progress. Do not turn off the system and do not remove the storage medium during the installation process.

3. After all software packages have been installed successfully, the system restarts. After restart, you are directed to the Windows sign-in screen.
4. Add the system as an iSCSI storage expansion to an external BVMS or VRM server using BVMS Configuration Client or Configuration Manager.



Notice!

For further details, refer to the BVMS or Configuration Manager documentation.

6.5 Signing in to the administrator account

Signing in to the administrator account in BVMS operation mode

To sign in to the administrator account in BVMS operation mode:

1. On the BVMS desktop, press Ctrl+Alt+Del.
2. Press and hold the left Shift key immediately after clicking **Switch User**.
3. Press Ctrl+Alt+Del again.
4. Select the **BVRAdmin** user and enter the password that was set during the system setup. Then press Enter.

Note: To go back to the BVMS desktop, press Ctrl+Alt+Del and click **Switch user** or **Sign out**. The system will automatically go back to BVMS desktop without a system restart.

Signing in to the administrator account in VRM or iSCSI operation mode

To sign in to the administrator account in VRM or iSCSI operation mode:

- ▶ On the Windows sign-in screen, press Ctrl+Alt+Del and enter the **BVRAdmin** password.

6.6 Configuring new hard drives

DIVAR IP all-in-one units 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 unit need to be configured before using them for video recording.

To configure new hard drives for video recording:

1. Install all hard drives before turning on the unit for the first time.
2. Turn on the unit.
Setup routines for Microsoft Windows Server IoT 2022 for Storage Workgroup are performed. This process can take several minutes. Do not turn off the system.
After the process is completed, the Windows language selection screen is displayed.
3. Press Shift and F10 to open the Windows **Command Prompt** box.
4. In the **Command Prompt** dialog box, enter **diskmgmt.msc**, then press Enter.
The **Disk Management** dialog box is displayed, showing all available disk drives with their volumes. The new drives that are not yet configured, are displayed as **Offline** and their volumes as **Unallocated**.
5. In the **Disk Management** dialog box, right-click the disk that you want to configure, then click **Online**.
The status of the disk changes to **Online**.
6. Right-click in the volume field, then select **New Simple Volume...**
The **New Simple Volume Wizard** dialog box is displayed.
7. Click **Next** to continue.
The **Specify Volume Size** dialog box is displayed.

8. In the **Simple volume size in MB:** field, enter the desired volume size that you want to use. If you want to use the maximum volume size, leave the pre-selected value unchanged.
9. Click **Next** to continue.
The **Assign Drive Letter or Path** dialog box is displayed.
10. In the **Assign the following drive letter:** list, select the desired drive letter.
11. Click **Next** to continue.
The **Format partition** dialog box is displayed.
12. Under **Format this volume with the following settings:**, apply following settings:
 - **File system: NTFS**
 - **Allocation unit size: Default**
 - **Volume label: Data** (Note: If you have two physical disks to be used as data partitions, name the first one **Data** and the second one **Data2**).
 - Select the **Perform a quick format** check box.
13. Click **Next** to continue.
The **Completing the New Simple Volume Wizard** dialog box is displayed, showing all selected settings.
14. Click **Finish** to close the dialog box.
The new volume is created, and displayed in the **Disk Management** dialog box.
15. Repeat these steps for the next disk drive.
16. When all disk drives have been configured successfully, close the **Disk Management** dialog box and the **Command Prompt** dialog box and proceed with the DIVAR IP all-in-one system setup.

Refer to

- *First sign-in and initial system setup, page 26*

6.7

Recovering the unit

To recover the unit:

1. Turn on the unit and press F7 during the BIOS power-on-self-test to enter Windows PE.
The **System Management Utility** dialog box is displayed.
2. Select one of the following options:
 - **System factory default:** This option will format video data partitions and restore the OS partition with the factory default image.
This process might take up to 5 minutes.
 - **Full data overwrite and system factory default:** This option will format video data partitions, completely overwriting existing data, and restore the OS partition with factory default image.
This process might take up to 48 hours.
 - **OS system recovery only:** This option will restore the OS partition with the factory default image and import existing virtual hard drives from existing video data partitions.
This process might take up to 5 minutes.

Note:

The **OS system recovery only** option does not delete video footage that is stored on the data HDDs. However, it replaces the complete operating system partition (including the video management system settings) with a default configuration. To access existing video footage after recovery, the video management system configuration needs to be exported before the system recovery and re-imported afterwards.

**Notice!**

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


3. Confirm the selected option.
The system starts the formatting and image recovery process.
4. After the recovery process is complete, confirm the system restart.
The system restarts and setup routines are performed.
5. After the process is complete, the Windows language selection screen is displayed.
6. Proceed with the initial system setup.

Refer to

- *First sign-in and initial system setup, page 26*

7 Troubleshooting

Overheating

Problem	Solution
<p>An overheating condition has occurred.</p> <p>The system status LED  is solid red.</p>	<ul style="list-style-type: none">- Make sure that no cables obstruct the airflow in the system.- Make sure that the fan is present and operating normally.- Make sure that the chassis cover is installed properly.- Make sure that the ambient room temperature is not too high.

8 Service and repair

The storage system is backed by a 5-year service level agreement. Issues will be handled according to Bosch service and support guidelines.

The storage equipment is shipped with an original manufacturer service and support agreement for hardware.

The Bosch technical support is the single point of contact in case of failure but the service and support obligations are fulfilled by the hardware manufacturer or a partner.

To enable the manufacturer's service and support organization to fulfill the defined service levels, the system must be registered. Otherwise, the defined service level cannot be provided but only best effort.

To register your product:

- Scan the QR code that you find on the device itself, in the delivered registration leaflet, or in this manual (refer to *Product registration, page 12*).
- or
- Go to the following webpage: <https://www.boschsecurity.com/product-registration/>

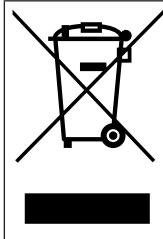
Refer to

- *Product registration, page 12*

9 Decommissioning and disposal

At a certain point in the life cycle of your product, it might be necessary to replace or to take out of order the device itself or a component. As the device or the component may hold sensitive data, like credentials or certificates, use the proper tools and methods to make sure that your relevant data is securely deleted during decommissioning or before disposal.

Old electrical and electronic equipment



This product and/or battery must be disposed of separately from household waste. Dispose such equipment according to local laws and regulations, to allow their reuse and/or recycling. This will help in conserving resources, and in protecting human health and the environment.

10 Additional information

10.1 Additional documentation and client software

For more information, software downloads, and documentation, go to the respective product page in the product catalog:

<http://www.boschsecurity.com>

You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under:

<https://downloadstore.boschsecurity.com/>

10.2 Support services and Bosch Academy



Support

Access our **support services** at www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Visit the Bosch Building Technologies Academy website and have access to **training courses**, **video tutorials** and **documents**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309021302