DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD | DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD
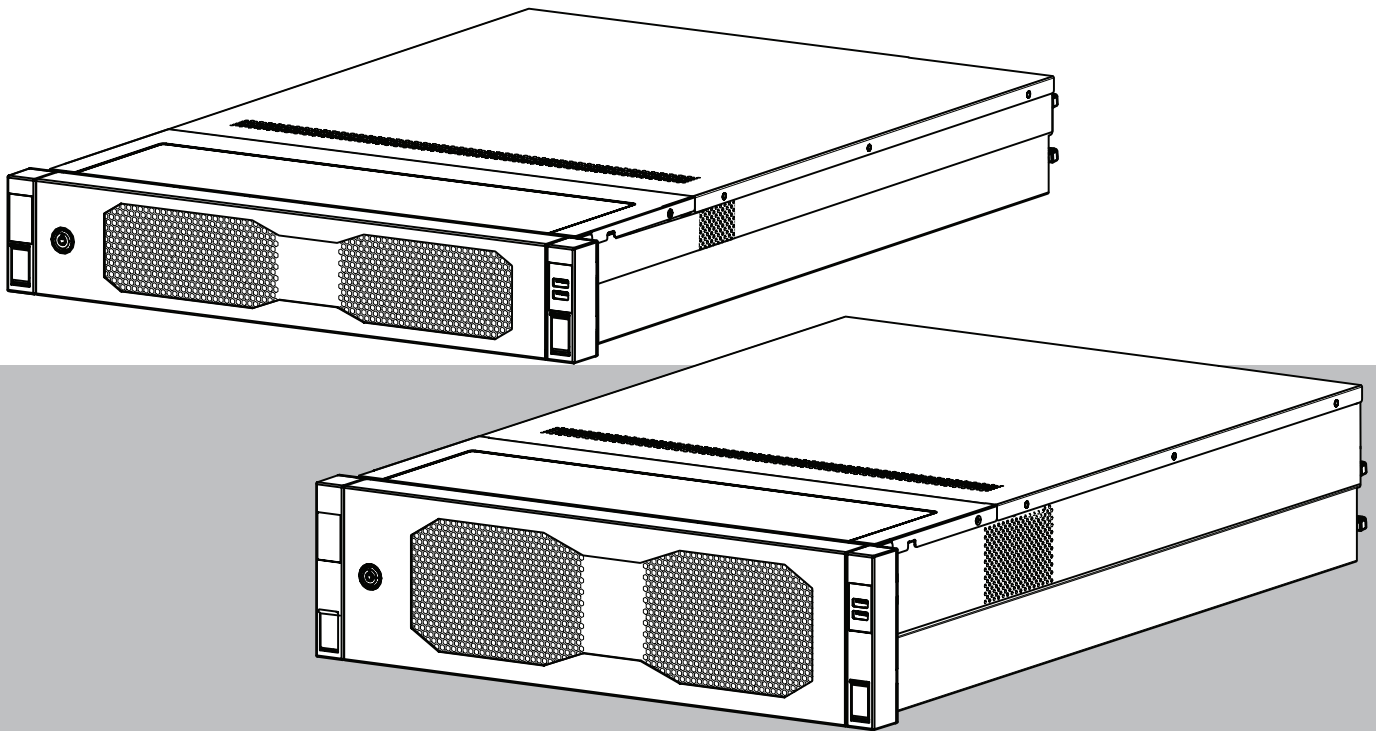
en   Installation manual

DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one
7000 3U
Table of contents | en   3

Table of contents

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!**
> This is a **class A** product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

> **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.

	Notice! This product cannot be directly connected to the internet (including public wireless LAN) of a telecom carrier (mobile network companies, landline network companies, Internet providers, etc.). When connecting this product to the Internet, make sure to connect it through a router or switch.

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!
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.

1.6.1   Cleaning

Notice!
Unplug the device from the power source before cleaning. Follow the instructions provided
with the device.

Notice!
Do not use liquid cleaners or aerosol cleaners. Clean only with a dry cloth.

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 prevent unauthorized removal of the hard drives. Always remove
the key from the lock and store the key in a secure place.

- Use the Chassis Intrusion Sensor feature to detect any unauthorized physical access into the interior of 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.
- To ensure that the web browser is secure and working properly, always keep it up to date.
- Do not switch off Windows Defender and Windows firewall, and always keep it up to date. Do not install additional anti-virus software, which can disrupt the security configurations.
- 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.
- Do not change the BIOS UEFI settings. Changing the BIOS UEFI settings can compromise or even result in malfunctioning of the system.
- The BMC system must not be connected to the public network.

1.8   Compliance

Canada

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

European Union

Notice!

This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to **EN 55032**. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

United States of America

FCC Supplier's Declaration of Conformity

F.01U.417.248	DIP-74C0-00N	Management appliance, 2U w/o HDD
F.01U.417.249	DIP-74C4-8HD	Management appliance, 2U 8X4TB
F.01U.417.250	DIP-74C8-8HD	Management appliance, 2U 8X8TB
F.01U.417.251	DIP-74CI-8HD	Management appliance, 2U 8X18TB
F.01U.417.252	DIP-74CI-12HD	Management appliance, 2U 12X18TB
F.01U.417.253	DIP-74G0-00N	Management appliance, 3U w/o HDD
F.01U.417.254	DIP-74GI-16HD	Management appliance, 3U 16X18TB

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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
− Security information, which covers potential effects caused by third-party vulnerabilities: https://www.boschsecurity.com/us/en/support/product-security/security-information.html

To receive updates on new security advisories, you can subscribe to the RSS feeds on the Bosch Security and Safety Systems Security Advisories page at: 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.

Quantity	Component
1	DIVAR IP all-in-one 7000
Accessory box	
1	Registration leaflet
1	Installation manual (English)
1	Labels for storage device trays (numbered 0-16)
2	Power supply clamp (for locking power cord)
2	EU Power cords
2	US Power cords
Front bezel box	
1	Front bezel
2	Keys
Rail kit box	
2	Rail modules
1	Screw pack

2.2 Product registration

Register your product under:
https://www.boschsecurity.com/product-registration/

3   System overview

DIVAR IP all-in-one 7000 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 7000 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 7000 is based on the operating system Microsoft Windows Server IoT OS
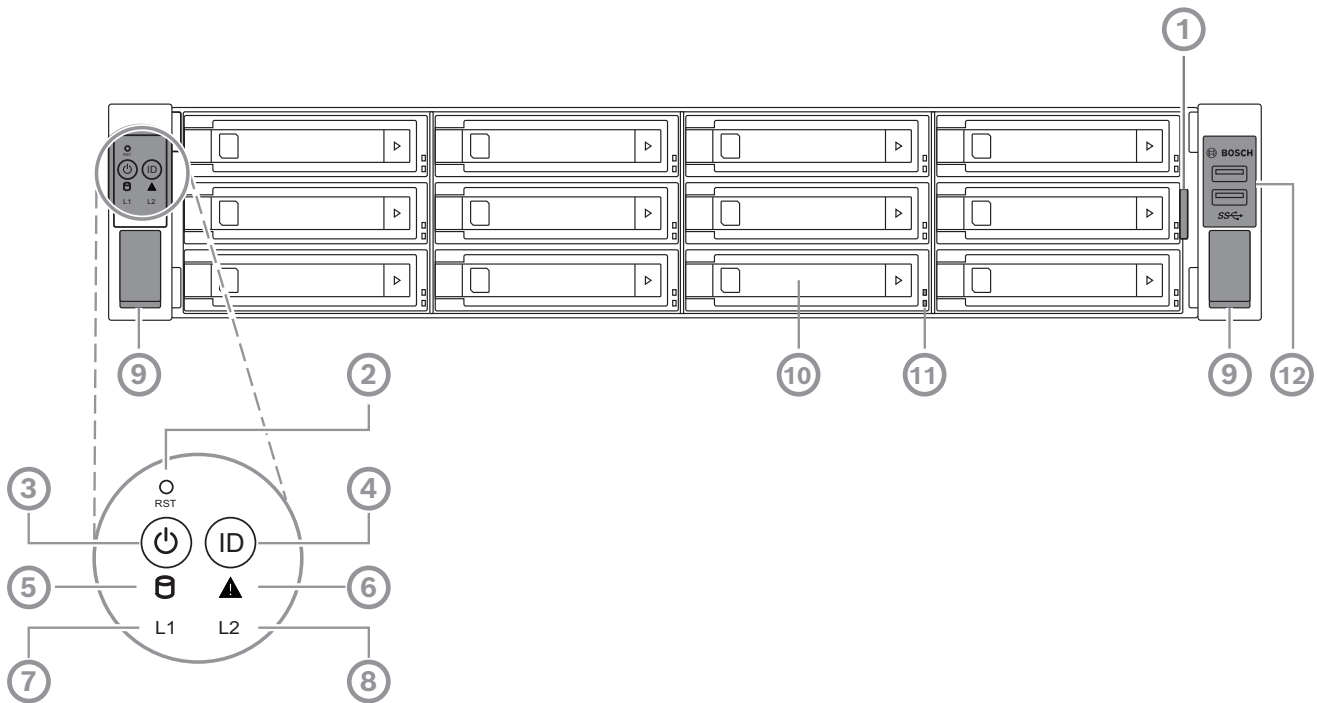2022 Standard.

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

Device components

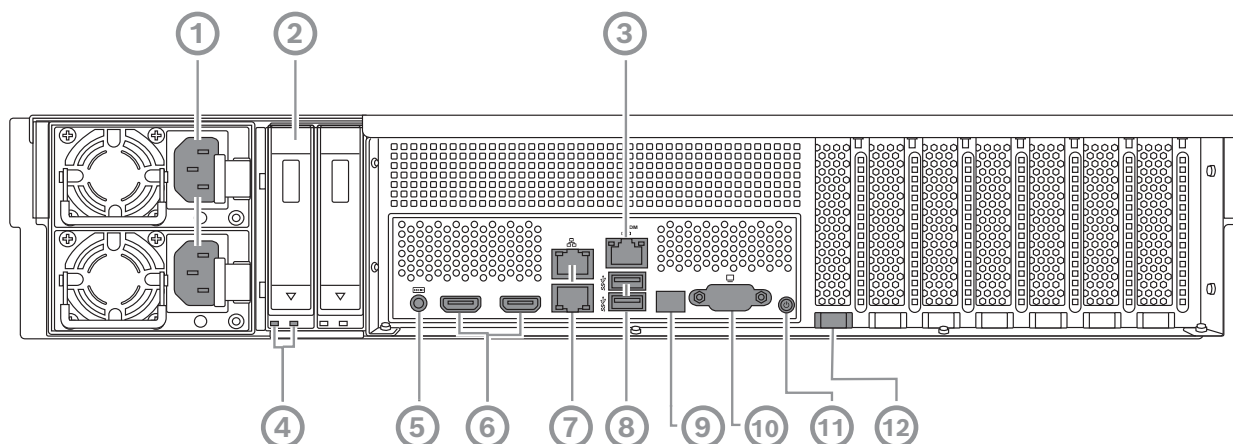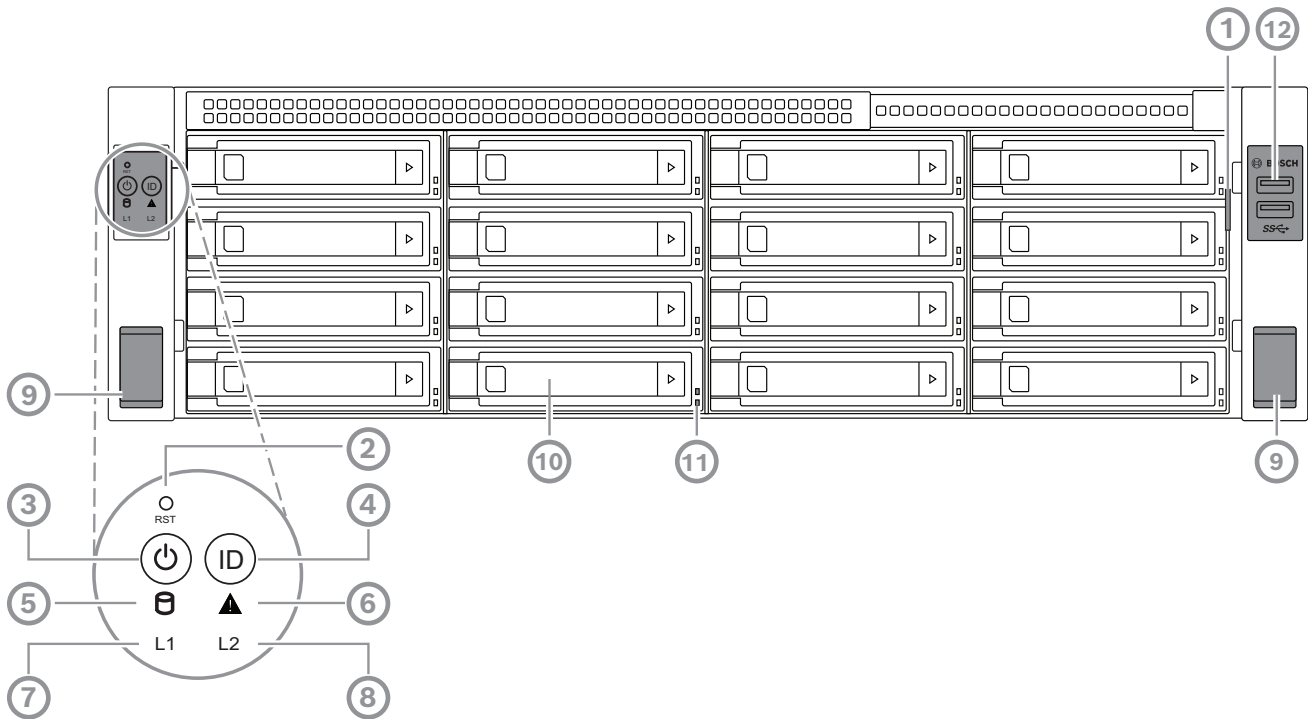| Component	Description
Hard drives	2U: The device has up to 12 storage device bays for SATA storage devices. 3U: The device has up to 16 storage device bays for SATA storage devices. The storage devices are hot swappable. Once setup correctly, the storage devices can be removed without turning off the system. **Note**: For empty units, the storage devices must be purchased separately. For the latest shipping lists, see the datasheet in the online product catalog.
Power supply	The device has two 800 W power supplies.
Control panel	The control panel is located on the front and has power buttons and status monitoring LEDs.
I/O ports	On the rear, there are various I/O ports to connect the device to the network and to other devices.

3.1   Device views

Front view 2U

1	Information tag with device identification data	**2**	Reset button
3	Power button with LED	**4**	Location button with LED
5	HDD LED	**6**	BMC message LED
7	LAN1 LED	**8**	LAN2 LED
9	Handles (for pulling the system out from the rack, also houses a screw to secure the system to the rack)	**10**	Hard drive tray
11	Hard drive tray LEDs	**12**	2 USB 3.2 Gen 1 ports (Type-A)

Rear view 2U

1	Mains connection	**2**	Solid state drive tray
3	BMC port	**4**	Solid state drive tray LEDs
5	BMC debug console (do not use)	**6**	2 HDMI™ ports
7	2 LAN ports (RJ45), teamed (LAN2: top LAN port, LAN1: bottom LAN port) **Note:** Do not change the teaming mode.	**8**	2 USB 3.2 Gen 1 ports (Type-A)
9	Port 80 LED	**10**	VGA port (covered, not used for local operation)
11	Power button	**12**	Location LED (onboard)

Front view 3U

1	Information tag with device identification data	**2**	Reset button
3	Power button with LED	**4**	Location button with LED
5	HDD LED	**6**	BMC message LED
7	LAN1 LED	**8**	LAN2 LED
9	Handles (for pulling the system out from the rack, also houses a screw to secure the system to the rack)	**10**	Hard drive tray
11	Hard drive tray LEDs	**12**	2 USB 3.2 Gen 1 ports (Type-A)

Rear view 3U

1	Mains connection	2	Solid state drive tray
3	BMC port	4	Solid state drive tray LEDs
5	BMC debug console (do not use)	6	2 HDMI™ ports
7	2 LAN ports (RJ45), teamed (LAN2: top LAN port, LAN1: bottom LAN port) **Note:** Do not change the teaming mode.	8	2 USB 3.2 Gen 1 ports (Type-A)
9	Port 80 LED	10	VGA port (covered, not used for local operation)
11	Power button	12	Location LED (onboard)

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	Button LED color	Description
Power	Green	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.

Button	Button LED color	Description
(ID) **Location**	Blue	The location button is used to turn on/off the LED both on this location button and on the location LED on the rear of the system. You can turn on both the LED on this location button and the location LED on the rear of the system either by pressing this location button, or remotely through BMC. This function allows you to quickly locate the system in a rack from both the rear and the front of the rack, for example for servicing purposes. Once the system has been serviced, press this location button again, to turn off the LED on this location button and the location LED on the rear of the system.

Control panel LEDs

LED	LED color	LED state	Description
HDD	-	Off	No activity
	Amber	Blinking	Read/write data into the storage device
BMC message LED	Green	On	System is normal; no incoming event
	Amber	On	A hardware monitor event is indicated
L1 LAN1 LED	-	Off	No link between system and network
	Green	On	Link between system and network
		Blinking	Network transmission or receiving activity
L2 LAN2 LED	-	Off	No link between system and network
	Green	On	Link between system and network
		Blinking	Network transmission or receiving activity

3.3 Hard drive tray LEDs

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

LED state		Description
Lower hard drive tray LED (green color)	**Upper hard drive tray LED (red color)**	
Off	Off	Indicates that a hard drive is not installed.

LED state		Description
Lower hard drive tray LED (green color)	**Upper hard drive tray LED (red color)**	
On	Off	Indicates that a hard drive is installed, but there is no activity.
Blinking	Off	Indicates hard drive read/write activity.
Off	On	Indicates that a hard drive under RAID is removed.
Blinking (4 Hz)	Blinking (4 Hz)	Identifies the HDD from a remote location through BMC.
Blinking (4 Hz)	Blinking (1 Hz)	Indicates that a hard drive rebuild is in progress, or hot spare.
Blinking (4 Hz)	Off	Indicates activity when other hard drives are in RAID rebuild.
On	On	Indicates that a hard drive under RAID is abnormal. Either the hard drive has failed, or it has been detected that a new hard drive was plugged in.
On	Blinking (1 Hz)	(For RAID 6) Indicates that this hard drive is the second hard drive to be rebuilt for RAID6, and is waiting for the first hard drive to complete the rebuild.

3.4   Solid state drive tray LEDs

The device supports hot-swappable SATA solid state drives in solid state drive trays. Each solid state drive tray has two LEDs on the front of the tray.

LED state		Description
Right solid state drive tray LED (green color)	**Left solid state drive tray LED (red color)**	
Off	Off	Indicates that a solid state drive is not installed.
On	Off	Indicates that a solid state drive is installed, but there is no activity.
Blinking	Off	Indicates solid state drive read/write activity.

3.5   LAN and BMC LEDs

On the rear of the device, there are two LAN ports and one BMC port. Each LAN port as well as the BMC port has two LEDs.

LED	LED color	LED state	Description
LAN 1/LAN 2 LED on the right	Green	On	Indicates a bandwidth of 1 Gbps
	Amber	On	Indicates a bandwidth of 100 Mbps
	-	Off	Indicates a bandwidth of 10 Mbps

LED	LED color	LED state	Description
LAN 1/LAN 2 LED on the left	Green	On	Connected
		Blinking	Data is being accessed
	-	Off	No connection
BMC LED on the right	Green	On	Indicates a bandwidth of 1 Gbps
	Amber	On	Indicates a bandwidth of 100 Mbps
	-	Off	Indicates a bandwidth of 10 Mbps
BMC LED on the left	Green	On	Connected
		Blinking	Data is being accessed
	-	Off	No connection

4   Preparing for installation

Read this section in its entirety before you begin the installation.
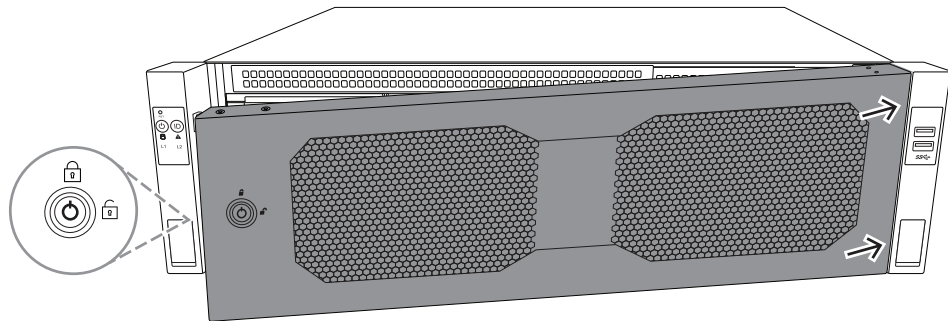
4.1   Installing the front bezel

For extra security, a front bezel can be installed to prevent unauthorized physical access to the storage devices.

To install the front bezel

1.   Make sure that the bezel lock is set to locked (🔒) (if necessary, use the bundled bezel key).
2.   Push the right side of the bezel into the notches on the right of the device.
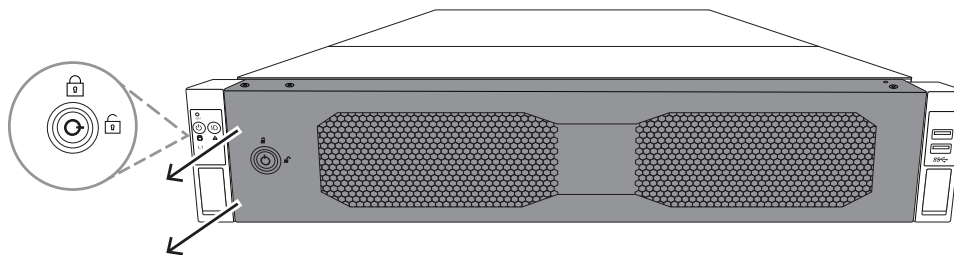2U:
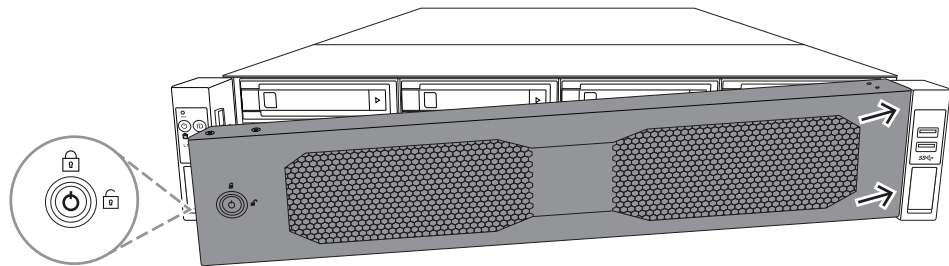
3U:

3.   Keep pushing the bezel towards the right and push the left side of the bezel down onto the system until it clicks into place.
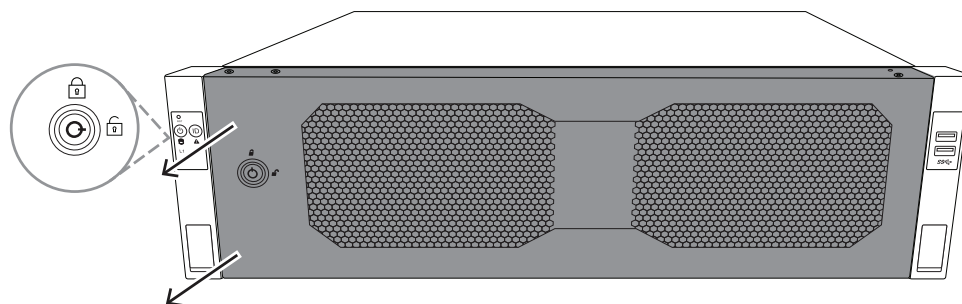The bezel is securely installed onto the system.

To remove the front bezel

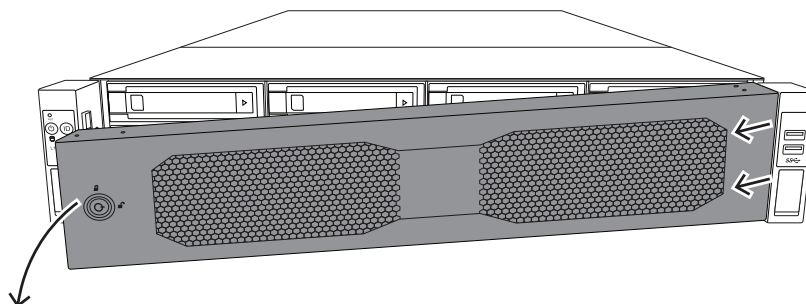1.   Set the bezel lock to unlocked (🔓) using the bundled bezel key.

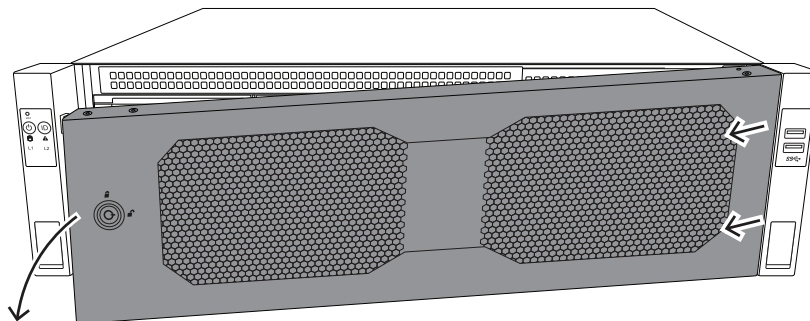2. Pull the bezel outwards from the side with the bezel lock.
   2U:

3U:

3. Pull the bezel towards the left to remove the bezel completely from the system.
   2U:

3U:

4.2   Choosing the installation location

– Place the system near at least one grounded power outlet.

- Place the system in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise, and electromagnetic fields are generated.
- Leave approximately 25 in (63.5 cm) clearance in front of the rack to be able to open the front door completely.
- Leave approximately 30 in (76.2 cm) of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.

> **Notice!**
> This equipment is intended for installation in Restricted Access Location or equivalent.

> **Notice!**
> This product is not suitable for use with visual display work place devices according to §2 of the German Ordinance for Work with Visual Display Units.

4.3 Rack precautions

> **Warning!**
> To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- In single rack installations, attach stabilizers to the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.
- In multiple rack installations, couple the racks together.
- Always make sure the rack is stable before extending a component from the rack.
- Extend only one component at a time - extending two or more simultaneously may cause the rack to become unstable.
- We strongly recommend that at least two able-bodied persons perform the rack and rail installation.

4.4 General system precautions

- Review the electrical and general safety precautions that came with the components you are adding to your chassis.
- Determine the placement of each component in the rack before installing the rails.
- Install the heaviest components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the system from power surges and voltage spikes if you want to keep your system operating in case of a power failure.
- Allow the hard drives and power supply modules to cool before touching them.
- Always keep the rack's front door and all panels and components on the system closed when not servicing to maintain proper cooling.

4.5 Installation considerations

Ambient operating temperature

If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum operating temperature.

Reduced airflow

Equipment should be mounted into a rack so that the amount of airflow required for safe operation is not compromised.

Mechanical loading

Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit overloading

Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable ground

A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of power strips, etc.).

5   Rack installation

This chapter describes the installation of DIVAR IP all-in-one 7000 in a rack.

You can also watch a video showing the rack installation. To get to the video, scan the following QR code:

Applicable racks

There is a variety of racks on the market, so that the installation procedure slightly differs depending on the rack type.

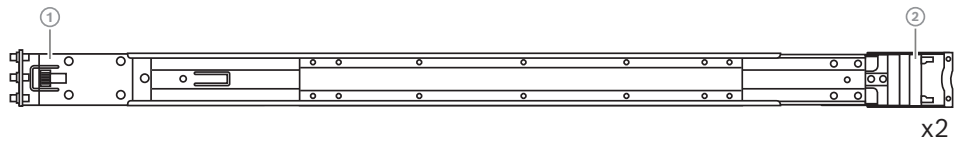The rack mount kit is adaptable for installation in following rack types:

–   Square-hole rack
–   Round-hole rack
–   10-32 threaded rack

The delivered rails fit a rack with a depth of 21.3 in (54.16 cm) to 36.2 in (92.08cm).

Prerequisites

To install DIVAR IP all-in-one 7000 in a rack, you need:

–   The rack mount kit delivered with the device. The rack mount kit includes:
    –   Two rail modules

x2

1 - Front end
2 - Rear end

    –   A bag of bundled screws (4 screw sets)

x2   x2   x8   x8

Procedure

To install DIVAR IP all-in-one 7000 in a rack, you must do the following:

1.   *Installing the inner rails to the chassis, page 27*
2.   *Installing the outer rails to the rack, page 29*
3.   *Installing the chassis in the rack, page 34*

## 5.1   Installing the inner rails to the chassis

Caution!

Do not pick up the chassis with the front handles. They are designed to pull the system from a rack only.

Each rail consists of an outer rail, intermediate rail, and inner rail. The inner rail can be removed from the outer and intermediate rail and be installed to the chassis.

5.1.1   Preparing the inner rails for installation

To prepare the inner rails for installation to the chassis:

1.   Slide the intermediate rail (1) out of the outer rail (2) until it clicks to a stop.
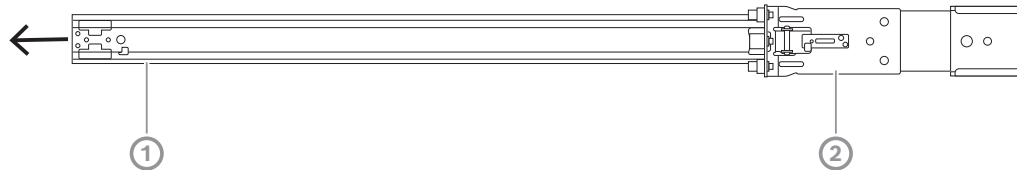
2.   Slide the inner rail (1) out of the intermediate rail (3) until it clicks to a stop. Slide the white release tab (2) outwards and remove the inner rail (1) completely from the intermediate rail (3).
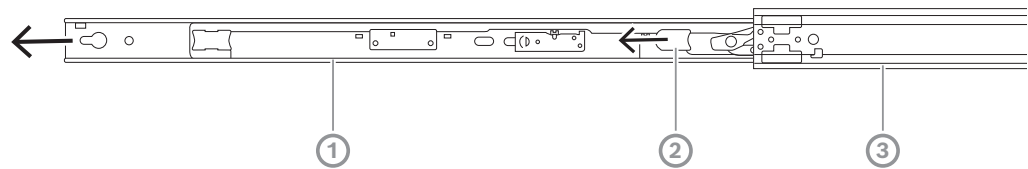

3.   Push the tab (1) on the inside of the intermediate rail to slide the intermediate rail back into the outer rail.
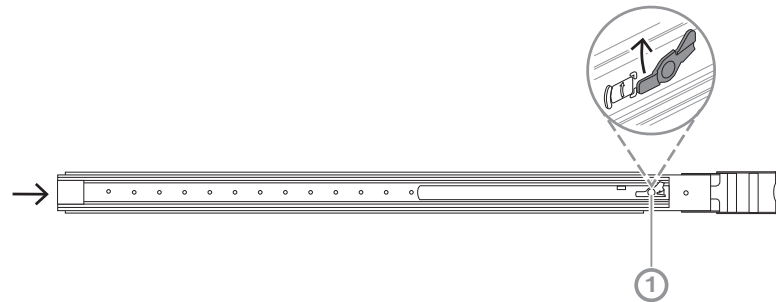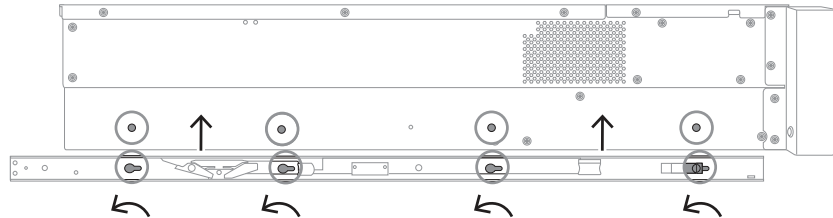

5.1.2   Installing the inner rails

To install the inner rail:

1.   Align the inner rail to the notches on both sides of the chassis.
2.   Push the inner rail backwards towards the rear of the chassis so that the inner rail extensions click and are latched onto the chassis.
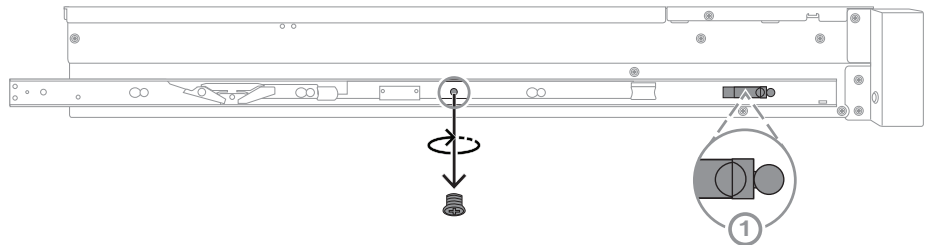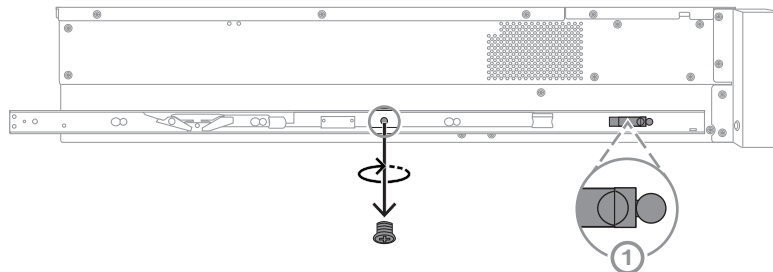   2U:
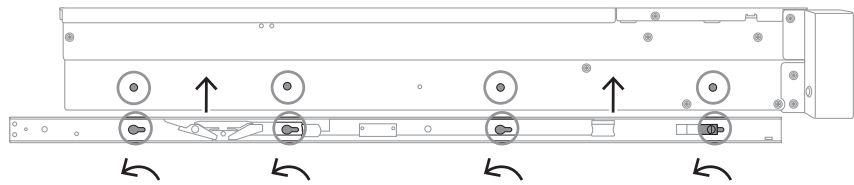
3U:

3. Make sure the spring latch (1) is completely latched onto the notch near the front of
the chassis.
4. Secure the inner rail to the chassis using the bundled screw.
2U:

3U:

5.2   Installing the outer rails to the rack

Each outer rail consists of a front clamp and a rear clamp. You can adjust the distance
between the front and the rear clamp by sliding the rail on the rear clamp, so that the outer
rail fits into different sizes of racks.
The outer rails come with mounting screws pre-installed on the front of the outer rail. The
pre-installed mounting screws allow for installation in square-hole racks without using any
tools.

For installation to round-hole racks or to 10-32 threaded racks, make sure to swap the mounting screws to the bundled set of mounting screws designed for the respective type of racks.

Depending on the type of the rack, the installation procedure slightly differs.
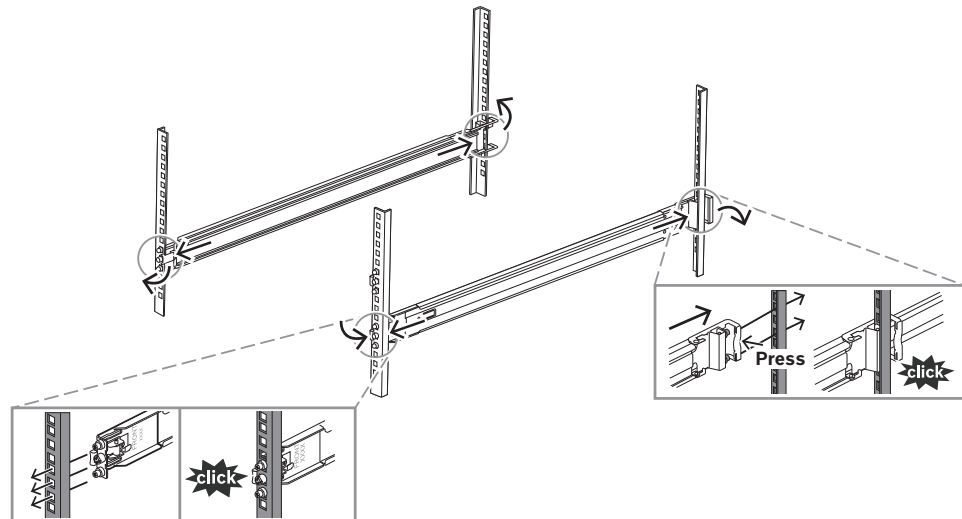
Refer to:

– *Installing the outer rails in a square-hole rack, page 30*
– *Installing the outer rails in a round-hole rack, page 30*
– *Installing the outer rails in a 10-32 threaded rack, page 32*

5.2.1 Installing the outer rails in a square-hole rack

To install the outer rails in a square-hole rack:

1. Determine the position in the rack where you want to install the chassis.
2. Place the outer rails at the desired position inside the rack posts with the front clamps towards the front rack posts and the rear clamps towards the rear rack posts.
3. Push the mounting bracket pins at the front end of the outer rails into the holes in the rack posts. Make sure that the clamps on the front of the outer rails click into place.
4. Align the mounting bracket pins at the rear end of the outer rails with the holes in the rack posts. Then press down the clamps and push the mounting bracket pins into the holes in the rack posts while pushing down the clamps.
5. Release the rear clamps and make sure that they click into place and clamp onto the rack posts.
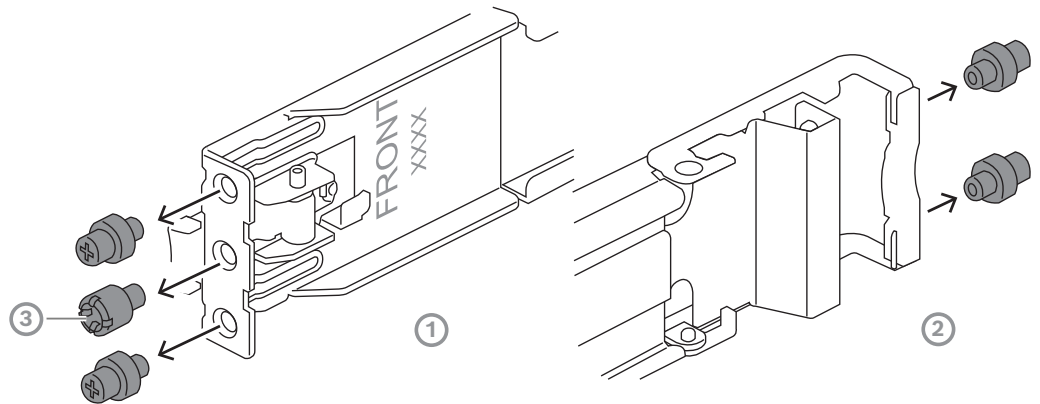

5.2.2 Installing the outer rails in a round-hole rack

To install the outer rails in a round-hole threaded rack:

1. Remove the pre-installed rack mounting screws for the square-hole rack from both, the front end (1) and the rear end (2) of the outer rail. Remove also the middle M5-bracket screw (3) on the front end of the outer rail.

2. Install the bundled mounting screws for the round-hole rack to both, the front end (1) and the rear end (2) of the outer rail.
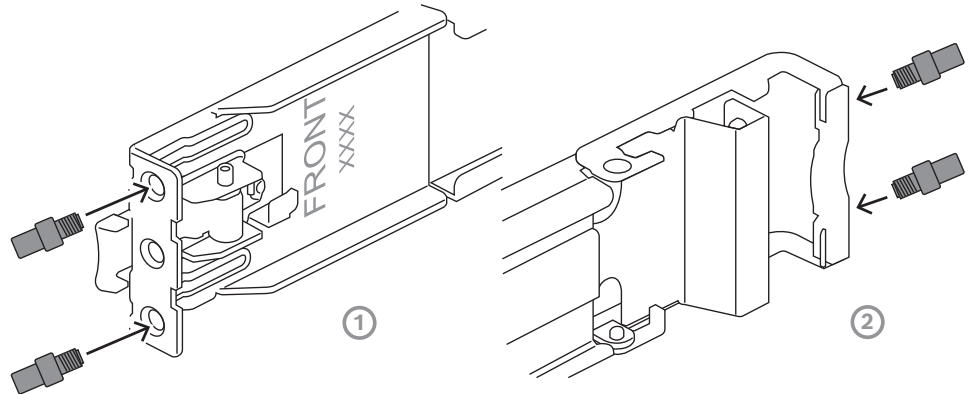
3. Determine the position in the rack where you want to install the chassis.
4. Place the outer rails at the desired position inside the rack posts with the front clamps towards the front rack posts and the rear clamps towards the rear rack posts.
5. Push the mounting bracket pins at the front end of the outer rails into the holes in the rack posts. Make sure that the clamps on the front of the outer rails click into place.
6. Reinstall the previously removed M5-bracket screw (3) to the front end of the outer rail.
7. Align the mounting bracket pins at the rear end of the outer rails with the holes in the rack posts. Then press down the clamps and push the mounting bracket pins into the holes in the rack posts while pushing down the clamps.

8.   Release the rear clamps and make sure that they click into place and clamp onto the rack posts.

5.2.3   Installing the outer rails in a 10-32 threaded rack

To install the outer rails in a 10-32 threaded rack:

1.   Remove the pre-installed rack mounting screws for the square-hole rack from both, the front end (1) and the rear end (2) of the outer rail. Remove also the middle M5-bracket screw (3) on the front end of the outer rail.
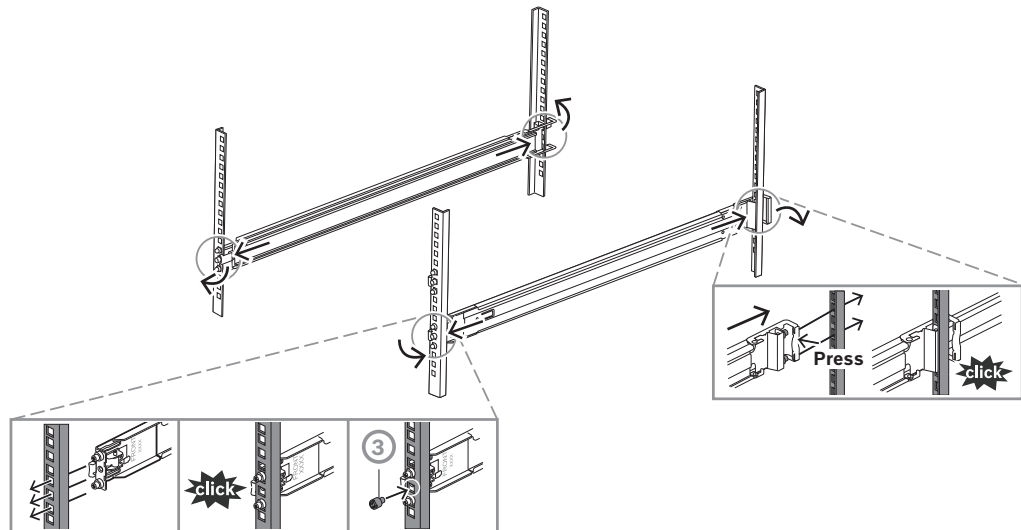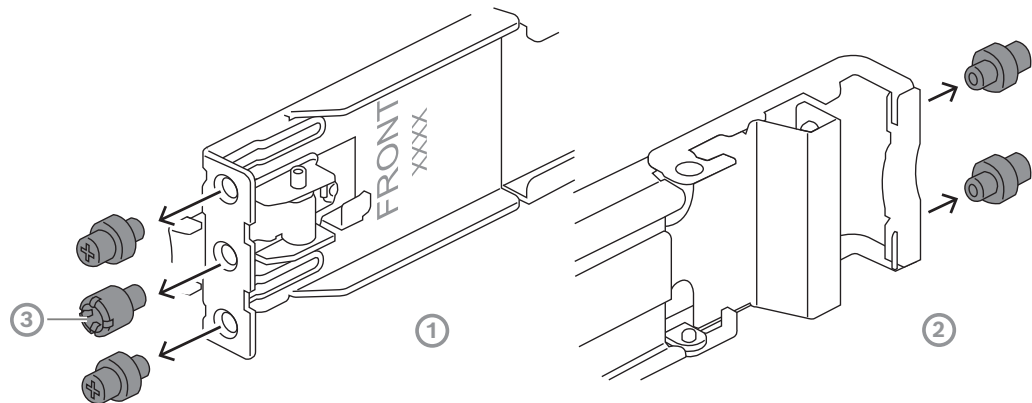
2. Install the bundled 10-32 pins to both, the front and the rear ends of the outer rail. Then, tighten the pins to secure them.

3. Determine the position in the rack where you want to install the chassis.
4. Place the outer rails at the desired position inside the rack posts with the front clamps towards the front rack posts and the rear clamps towards the rear rack posts.
5. Push the 10-32 pins at the front end of the outer rails into the holes in the rack posts. Make sure that the clamps on the front of the outer rails click into place.
6. Align the 10-32 pins at the rear end of the outer rails with the holes in the rack posts. Then press down the clamps and push the 10-32 pins into the holes in the rack posts while the clamps are pushed down.
7. Release the rear clamps and make sure that they click into place and clamp onto the rack posts.
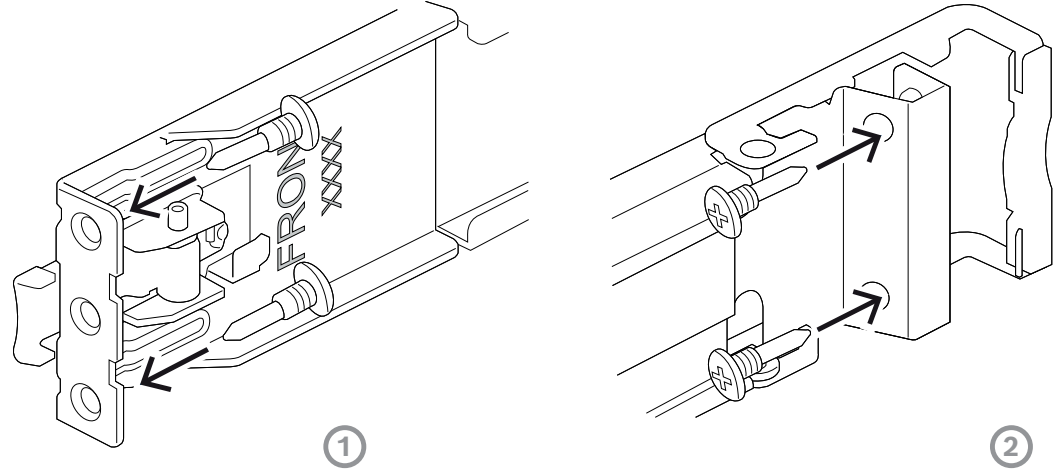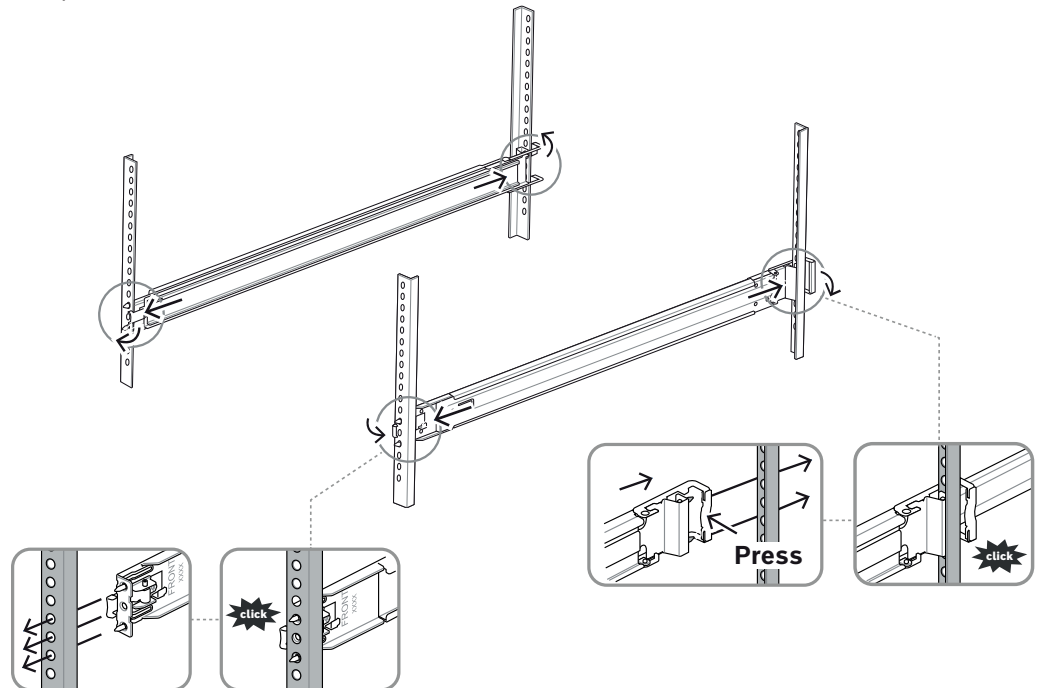
5.3 Installing the chassis in the rack

> **Warning!**
> Stability hazard
> Before sliding the unit out for servicing make sure that the rack stabilizing mechanism is in place, or the rack is bolted to the floor. Failure to stabilize the rack can cause the rack to tip over.

> **Warning!**
> Do not pick up the unit with the front handles. The handles are designed to pull the system from a rack only.

> **Notice!**
> Mounting the chassis into the rack requires at least two people to support the chassis during installation. Please follow safety recommendations printed on the rails.

> **Notice!**
> Always install chassis into racks from the bottom up.

To install the chassis in the rack:
1. Fully extend the intermediate rail (1) until it clicks to a stop.
2. Align the inner rails of the chassis with the intermediate rails.
3. Slide the inner rails into the intermediate rails, keeping the pressure even on both sides.
   2U:

click

3U:
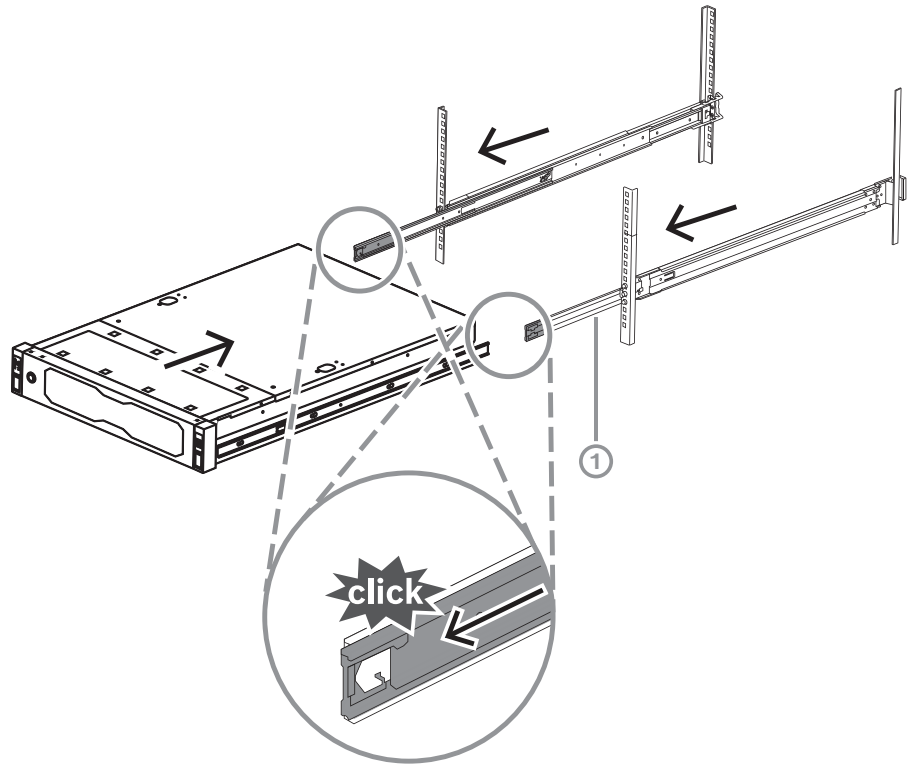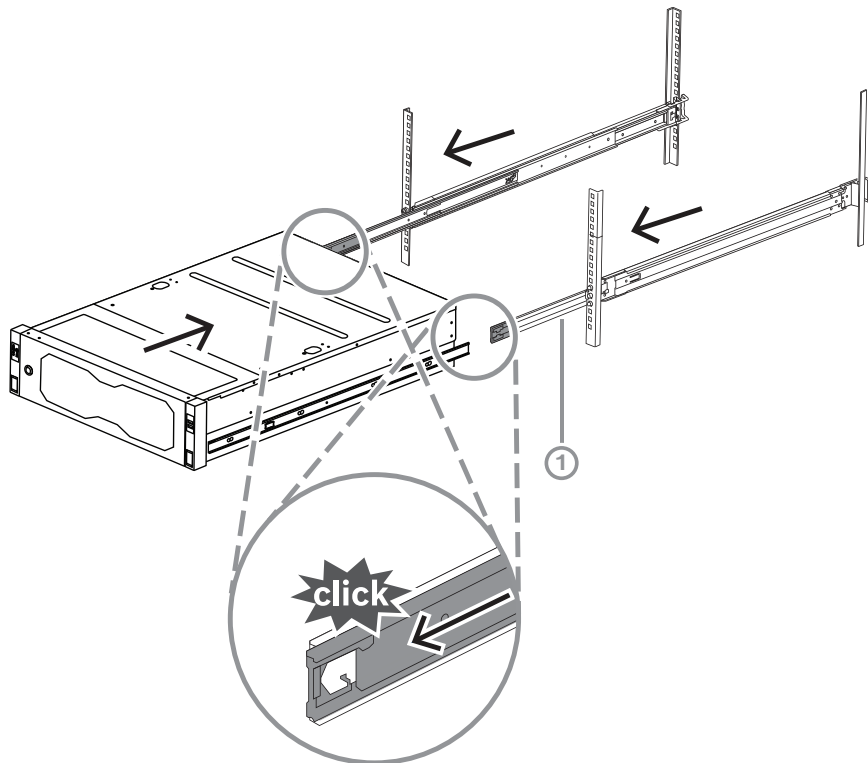
click

4. Once the chassis reaches a stop, push the blue release tab (1) on the inner rail (2).
2U:
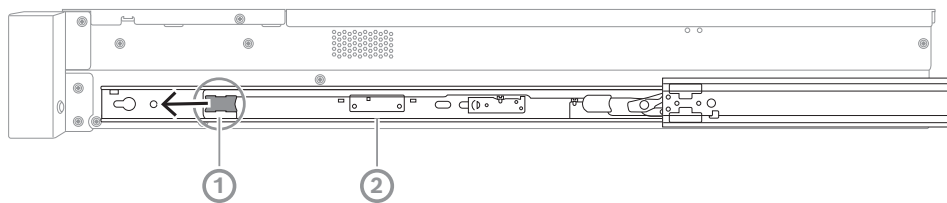
3U:
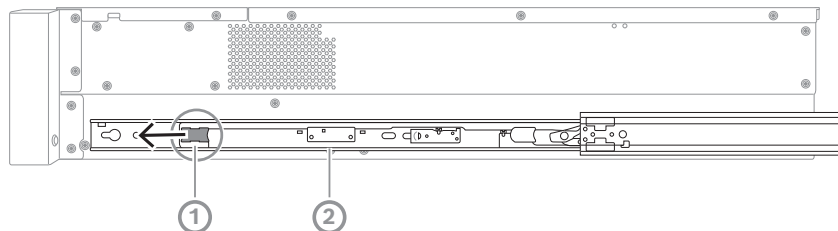
5. Push the chassis completely into the rack and make sure that it clicks into the locked position, then pull the handles down (1) and secure the chassis using the pre-installed screw.

6.   Secure the rear end of the chassis using the bundled screw (2).
     2U:
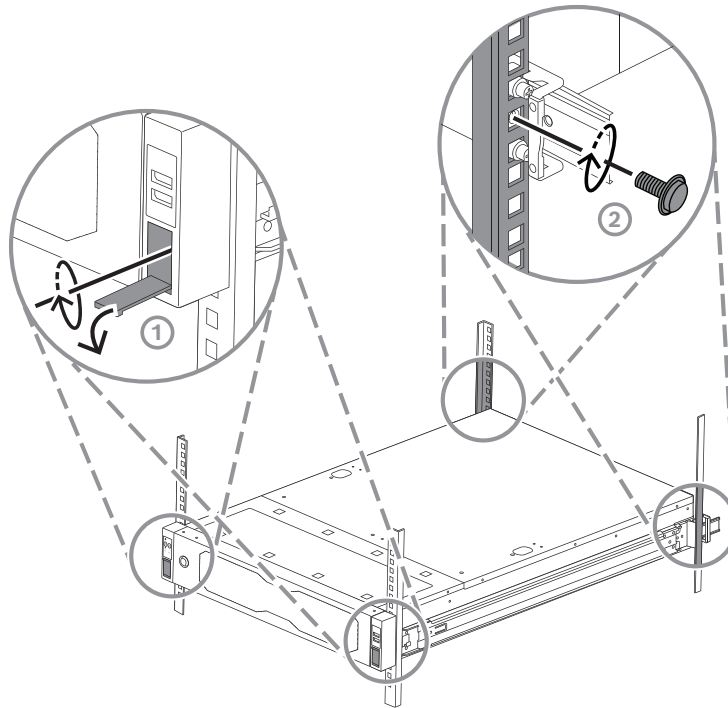
3U:
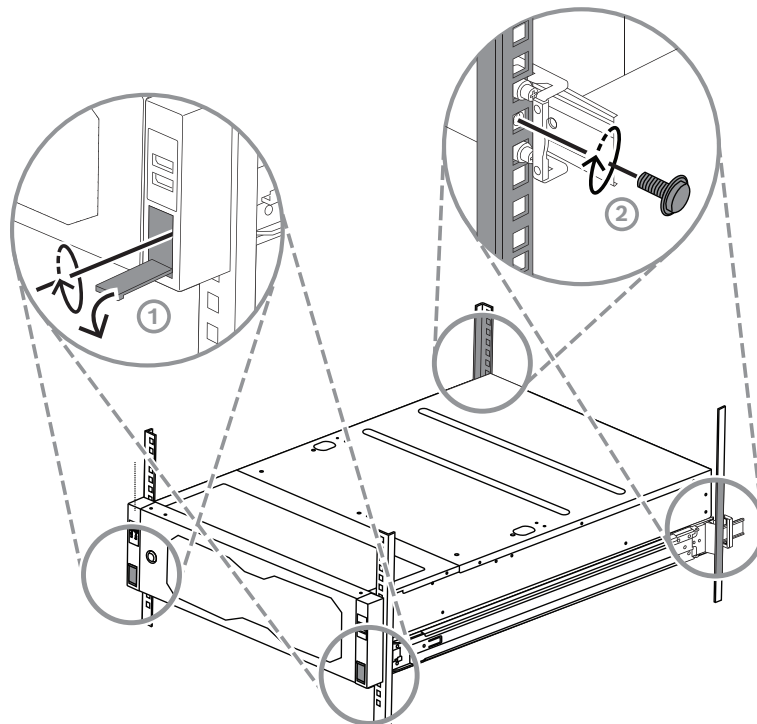
6   Installing a SATA hard drive

DIVAR IP all-in-one 7000 2U has up to 12 hot-swappable SATA hard drives and DIVAR IP all-in-one 7000 3U has up to 16 hot-swappable SATA hard drives on the front of the system, which can be removed without turning off the system.

The hard drives are mounted in trays to simplify their installation and removal from the chassis. The trays also help promote proper airflow for the storage device bays.

(i)

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

(i)

Notice!

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

(i)

Notice!

Spare hard drives supplied by Bosch for the DIVAR IP all-in-one 7000 devices, are not pre-installed in hard drive trays. Use the hard drive trays delivered with the devices.

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

1. *Removing a hard drive tray from a hard drive bay, page 38*
2. *Installing a hard drive into a hard drive tray, page 39*
3. *Installing a hard drive tray into a hard drive bay, page 40*

6.1   Removing a hard drive tray from a hard drive bay

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

1. Press the release button (1) to the right of the hard drive tray.
    The hard drive tray handle (2) extends.

2. Use the hard drive tray handle (2) to pull the hard drive tray out of the chassis.
    2U:
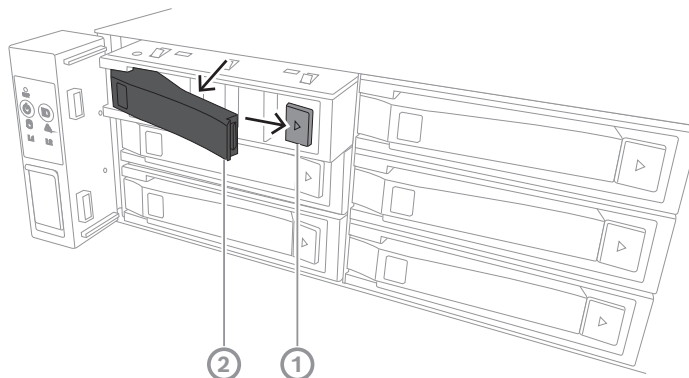
3U:
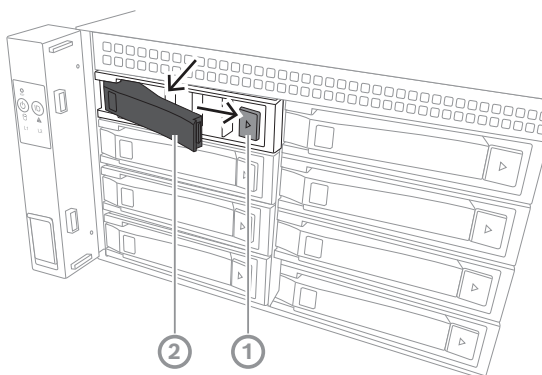
6.2   Installing a hard drive into a hard drive tray

Notice!
This component is an electrostatic sensitive device. Take caution when handling an
electrostatic sensitive device.
You can take the following precautions when working with electrostatic sensitive devices:
- Operate the device in a static-free environment or area.
- Avoid touching the pins, leads, or circuitry without being properly grounded.
- Wear anti-static gloves or an ESD wrist strap connected by a ground cord to a properly
grounded device or surface.

To install a hard drive into a hard drive tray:

▸ Press the hard drive into the hard drive tray until it clicks into place and is seated securely in the hard drive tray.
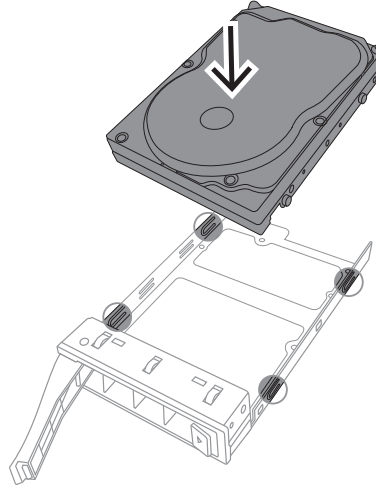
	Notice!
i	Except for short periods of time (swapping hard drives), do not operate the unit with the hard drives removed from the bays.

6.3 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 hard drive bay until the handle retracts and the hard drive tray clicks into the locked position.
   2U:
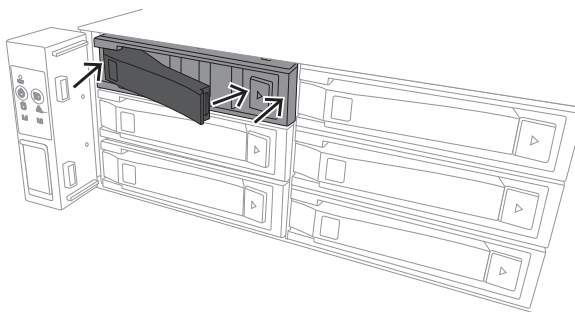
3U:
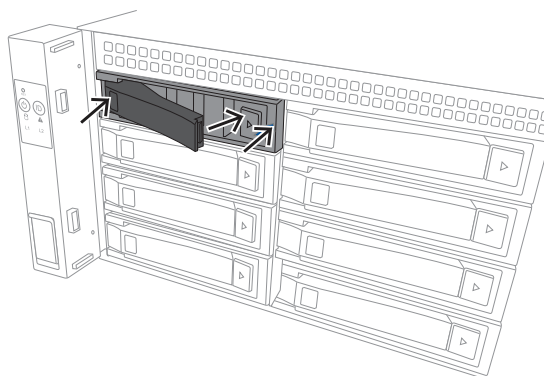
7 Turning on the unit

ℹ️ **Notice!**
Enclosure openings
Before you turn on the unit, remove the protective film from the top of the unit so that it does not block any enclosure openings.

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 cords from the power supply units 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.

8   System setup

The Microsoft Windows Server IoT 2022 for Storage Standard 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 Standard 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.

8.1   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
     –   The password must contain characters from three of the following four categories:
          At least one uppercase letter.
          At least one lowercase letter.
          At least one digit.
          At least one special character.

8.2   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.

8.3   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.

> **(i) 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.

8.4 First sign-in and initial system setup

> **(i) Notice!**
> Do not change any operating system settings. Changing operating system settings can result in malfunctioning of the system.

> **(i) Notice!**
> To perform administrative tasks, you must sign in to the administrator account.

> **(i) 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.

> **(i) Notice!**
> For security reasons, User Account Control (UAC) dialog boxes are displayed asking for your confirmation to make the intended changes to your system. You can only proceed with the installation after confirming that you want to make the appropriate changes.

To setup the system:
1. Connect the DIVAR IP all-in-one unit and the cameras to the network.
2. Turn on the unit.
   Wait until the BIOS screen is displayed and setup routines for Microsoft Windows Server IoT 2022 for Storage Standard 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
– The password must contain characters from three of the following four categories:
   – At least one uppercase letter.
   – At least one lowercase letter.

–   At least one digit.
–   At least one special character.
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.   In the following User Account Control dialog boxes, click **Yes** to continue. The installation starts.

11.   After the installation is complete, the system restarts and you are directed to the Windows sign-in page. Sign in to the administrator account.

12.   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.

8.4.1   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 **Install operation mode**.
     The BVMS license agreement is displayed.
2.   Read and accept the license agreement, then click **Yes, 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/

8.4.2   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 **Install operation mode**.
     The VRM license agreement is displayed.
2.   Read and accept the license agreement, then click **Yes, 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.

8.4.3 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 **Install operation mode**.
   The installation dialog box is displayed.
2. In the installation dialog box, click **Yes, 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.

> **(i)** **Notice!**
> For further details, refer to the BVMS or Configuration Manager documentation.

8.5 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.

8.6 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, you must do the following:

1. *Configuring RAID5, page 48*.
2. *Recovering the unit, page 49*.

8.6.1 Configuring RAID5

> **Notice!**
> The initial RAID configuration is not necessary for units with pre-installed hard drives. Units with preinstalled drives are delivered with a default configuration.

To configure RAID5:
1. Install all hard drives.
2. Turn on the unit and press Del to enter the BIOS setup.

> **Notice!**
> BIOS password
> The initial BIOS password is unique for each unit. You can find it on the label at the rear of the unit. Bosch strongly recommends to change this initial password. Make sure to store the new password in a secure location.
> Observe the following password requirements:
> - Passwords must have a minimum length of 14 characters.
> - Passwords must contain at least one uppercase letter.
> - Passwords must contain at least one lowercase letter.
> - Passwords must contain at least one special character.
> - Passwords must contain at least one number.

3. In the BIOS setup, navigate to the tab **Advanced**.
4. Select the option **BROADCOM <MegaRAID 9560-16i 8GB> Configuration utility**, then press Enter.
5. In the next dialog box, select the option **Main menu**, then press Enter.
6. In the next dialog box, select the option **Configuration Management**, then press Enter.
7. In the next dialog box, select the option **Create Virtual Drive**, then press Enter.
8. In the next dialog box, select the option **Select RAID Level**, then press Enter.
   The **Select RAID Level** dialog box is displayed.
9. In the **Select RAID Level** dialog box, select **RAID5**, then press Enter.
10. In the next dialog box, select the option **Select Drives**, then press Enter.
11. In the next dialog box, navigate to the option **Check All** to check if all hard drives are enabled. Then press Enter.
12. In the next dialog box, navigate to the option **Apply Changes**, then press Enter.
13. In the next dialog box, the message **The operation has been performed successfully** is displayed.
    Select **OK**, then press Enter.
14. In the next dialog box, in the **CONFIGURE VIRTUAL DRIVE PARAMETERS:** section, apply following settings:
    Strip Size: **64 KB**.
    Read Policy: Read Ahead
    Write Policy: **Always Write Back**.
    Default Initialization: Fast
    Leave the other settings unchanged.
    To save the configuration, select the option **Save Configuration**, then press Enter.
15. In the next dialog box, select the option **Confirm**, press Enter, then set the status to **Enabled**, then press Enter again.
16. In the next dialog box, select **Yes**, then press Enter.

17. In the next dialog box, the message **The operation has been performed successfully** is displayed.
    Select **OK**, then press Enter.
    The virtual RAID5 drive has been created and you receive the confirmation that the operation was successful.
18. To save and exit, press F4.
    The **Save & Exit Setup** dialog box is displayed.
19. Select **Yes** and press Enter.
    The system starts.

Checking RAID5 virtual drive settings
To check the RAID5 virtual drive settings:
1. Turn on the unit and press Del to enter the BIOS setup.
2. In the BIOS setup, navigate to the tab **Advanced**.
3. Select the option **BROADCOM <MegaRAID 9560-16i 8GB> Configuration utility**, then press Enter, then press Enter.
4. In the next dialog box, select the option **Main menu**, then press Enter.
5. In the next dialog box, select the option **Virtual Drive Management**, then press Enter.
   The RAID 5 virtual drive settings are displayed.
6. Press F4 to exit the BIOS setup.

8.6.2   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 will take several 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.
     Note: This process might take several days.
   – **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 will take several 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.

8.7 Configuring BMC settings

DIVAR IP all-in-one 7000 has a dedicated BMC port on the rear side.

Each DIVAR IP all-in-one 7000 unit is delivered with the default BMC user name **admin** and with an initial BMC password. The initial BMC password is unique for each unit. You can find it on the label at the rear of the unit, below the BMC port.

After the first logon to the BMC web interface, you will be requested to change this initial password. Make sure to store the new password in a secure location.

Observe the following password requirements:

–   Passwords must have a minimum length of 14 characters.
–   Passwords must contain at least one uppercase letter.
–   Passwords must contain at least one lowercase letter.
–   Passwords must contain at least one special character.
–   Passwords must contain at least one number.

i	**Notice!** For security reasons, do not connect the device to a public network through the BMC port.

Configuring the BMC settings

To configure the BMC settings:

1. Turn on the unit and press Del to enter the BIOS setup.

i	**Notice!** BIOS password The initial BIOS password is unique for each unit. You can find it on the label at the rear of the unit. Bosch strongly recommends to change this initial password. Make sure to store the new password in a secure location. Observe the following password requirements: - Passwords must have a minimum length of 14 characters. - Passwords must contain at least one uppercase letter. - Passwords must contain at least one lowercase letter. - Passwords must contain at least one special character. - Passwords must contain at least one number.

2. In the BIOS setup, navigate to the tab **Server Mgmt**.
3. Select the option **BMC Network Configuration**, then press Enter.
4. In the next dialog box, select the option **Configuration Address source**, then press Enter.
    The **Configuration Address source** dialog box is displayed.
5. In the **Configuration Address source** dialog box, select the desired option how the BMC address should be configured, then press Enter.

6.   Set the desired network configuration parameters.
7.   Press F4 and Enter to save and exit.
     The DIVAR IP all-in-one 7000 unit restarts.

9   Troubleshooting

Unable to power up

Problem	Solution
The system does not power up when power button is pressed.	– Make sure that the power cord is properly connected. – Make sure that the PSU power cable is working by trying a different PSU power cable. – Check if the PSU LED lights up green or not. – Check if any LEDs light up in the rear panel.

Unable to boot into OS

Problem	Solution
The system is stuck on a certain screen when booting before entering OS.	– Check the Port 80 LED located on the rear of the device (refer to *Port 80 LED, page 52*).

9.1   Port 80 LED

The device features a port 80 LED that allows you to identify the system status and errors during POST (Power On Self Test).

LED	LED state	Description
Port 80 LED	On	Displays a 2-digit error code that indicates the system status

These POST codes appear at the bottom right of the BIOS screen as a two-digit string that is the same as the two-digit output from the primary I/O port 80.

0	1	2	3	4	5	6	7	8	9
0	1	2	3	4	5	6	7	8	9

A	b	C	d	E	F				
A	b	C	d	E	F				

The POST code may be requested by Bosch Technical support in case of troubleshooting.

10   Service and maintenance

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 14*).
    or

–   Go to the following webpage: https://www.boschsecurity.com/product-registration/

11 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
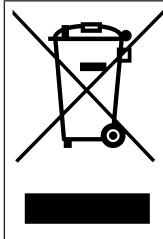
	This product and/or battery must be disposed of separately from household waste. Dispose such equipment according to local laws and regulations, to allow their reuse and/or recycling. This will help in conserving resources, and in protecting human health and the environment.

12   Additional information

12.1   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/

12.2   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/

Building solutions for a better life

202408131758