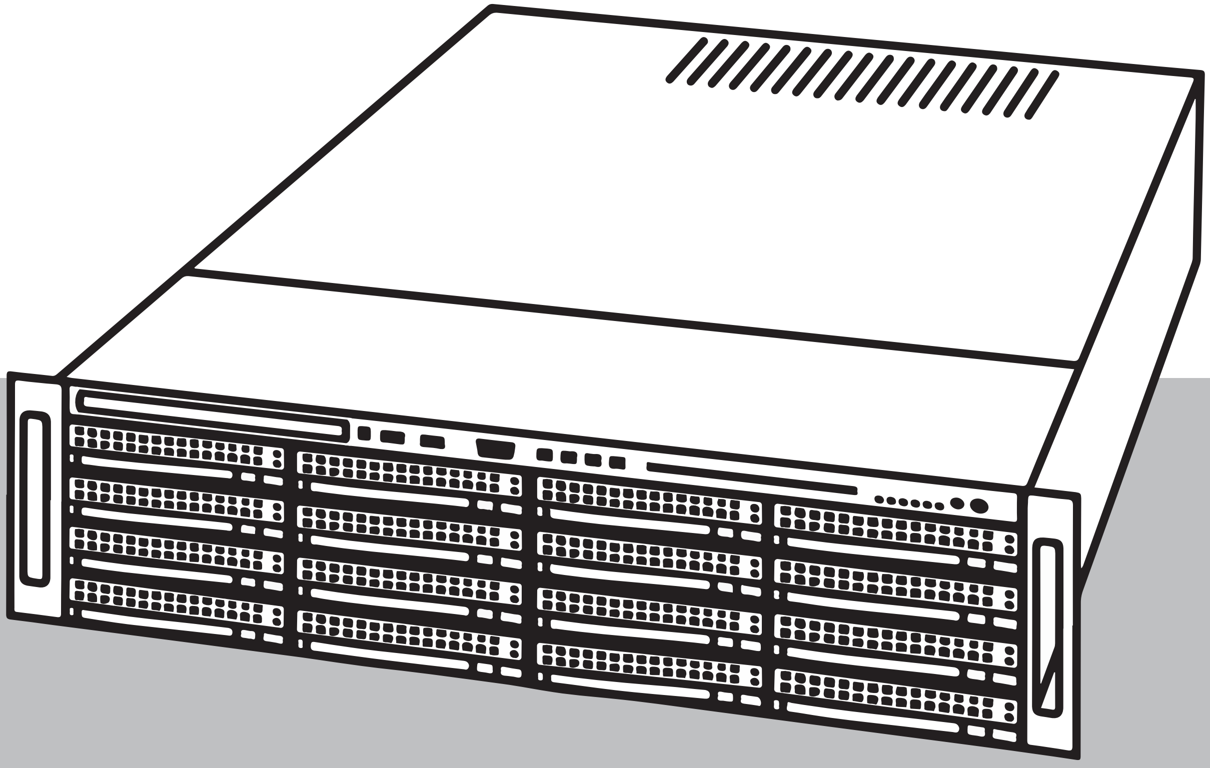
DIVAR IP all-in-one 7000 3U

DIP-73G0-00N | DIP-73G8-16HD | DIP-73GC-16HD



en Quick installation guide

Table of contents

1	**Safety**	**4**
1.1	Safety message explanation	**4**
1.2	General safety precautions	**4**
1.3	Electrical safety precautions	**7**
1.4	ESD precautions	**8**
1.5	Operating precautions	**8**
1.6	Notices	**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**	**13**
2.1	Parts included	**13**
2.2	Product registration	**13**
3	**System overview**	**14**
4	**Preparing for installation**	**18**
4.1	Choosing the installation location	**18**
4.2	Rack precautions	**18**
4.3	General system precautions	**18**
4.4	Installation considerations	**19**
5	**Rack installation**	**20**
5.1	Identifying the sections of the rack rails	**20**
5.2	Separating the sections of the rack rails	**20**
5.3	Installing the inner rails on the chassis	**21**
5.4	Installing the outer rails to the rack	**22**
5.5	Installing the chassis in the rack	**22**
6	**Installing a SATA hard drive**	**24**
6.1	Removing a hard drive carrier from a hard drive bay	**24**
6.2	Installing a hard drive into a hard drive carrier	**25**
6.3	Installing a hard drive carrier into a front drive bay	**25**
7	**Turning on the system**	**27**
8	**System setup**	**28**
8.1	Default settings	**28**
8.2	Prerequisites	**28**
8.3	Operating modes	**28**
8.4	First sign-in and initial system setup	**29**
8.5	Preparing hard drives for video recording	**32**
8.5.1	Configuring hard drives using the MegaRAID Storage Manager application	**32**
8.5.2	Recovering the unit	**33**
8.6	Signing in to the administrator account	**34**
8.7	Configuring IPMI settings	**34**
9	**Additional documentation and client software**	**35**

1 Safety

Observe the safety precautions in this chapter.

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 or environment, or data loss.

1.2 General safety precautions

Follow these rules to ensure general safety:

- Keep the area around the system clean and free of clutter.
- Place the chassis top cover and any system components that have been removed away from the system on a table so that they won't accidentally be stepped on.
- While working on the system, do not wear loose clothing such as neckties and unbuttoned shirt sleeves, which can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.
- After accessing the inside of the system, close the system back up and secure it to the rack unit after ensuring that all connections have been made.
- The system is heavy when fully loaded. When lifting the system, two people at either end should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.

Caution!
Installation should only be performed by qualified service personnel in accordance with applicable local codes.

Caution!
The Low Voltage power supply unit must comply with EN/UL 60950. The power supply must be a SELV-LPS unit or a SELV - Class 2 unit (Safety Extra Low Voltage - Limited Power Source).

Warning!
Interruption of mains supply:
Voltage is applied as soon as the mains plug is inserted into the mains socket.
However, for devices with a mains switch, the device is only ready for operation when the mains switch (ON/OFF) is in the ON position. When the mains plug is pulled out of the socket, the supply of power to the device is completely interrupted.

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

Warning!
Power cable and AC adapter:
When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL or CSA-certified cables (that have UL/CSA shown on the code) for any other electrical devices.

Warning!
Lithium battery:
Batteries that have been inserted wrongly can cause an explosion. Always replace empty batteries with batteries of the same type or a similar type recommended by the manufacturer. Handle used batteries carefully. Do not damage the battery in any way. A damaged battery may release hazardous materials into the environment.
Dispose of empty batteries according to the manufacturer's instructions, or local directives.

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

Notice!
Electrostatically sensitive device:
To avoid electrostatic discharges, the CMOS/MOSFET protection measures must be carried out correctly.
When handling electrostatically sensitive printed circuits, grounded anti-static wrist bands must be worn and the ESD safety precautions observed.

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

Read, follow, and retain for future reference all of the following safety instructions. Follow all warnings before operating the device.

- Clean only with a dry cloth. Do not use liquid cleaners or aerosol cleaners.
- Do not install device near any heat sources such as radiators, heaters, stoves, or other equipment (including amplifiers) that produce heat.

- Never spill liquid of any kind on the device.
- Take precautions to protect the device from power and lightning surges.
- Unless qualified, do not attempt to service a damaged device yourself. Refer all servicing to qualified service personnel.
- Install in accordance with the manufacturer's instructions in accordance with applicable local codes.
- Use only attachments/accessories specified by the manufacturer.
- Protect all connection cables from possible damage, particularly at connection points.
- Do not defeat the safety purpose of a polarized or ground-type plug.
- Permanently connected devices must have an external, readily operable mains plug or all-pole mains switch in accordance with installation rules.
- Pluggable devices must have an easily accessible socket-outlet installed near the equipment.
- Unplug the unit from the outlet before cleaning. Follow any instructions provided with the unit.
- Any openings in the unit enclosure are provided for ventilation to prevent overheating and ensure reliable operation. Do not block or cover these openings.
- If you install this device in an enclosure, make sure the enclosure is properly ventilated according to the manufacturer’s instructions.
- Install the unit only in a dry, weather-protected location.
- Do not use this unit near water, for example near a bathtub, washbowl, sink, laundry basket, in a damp or wet basement, near a swimming pool, in an outdoor installation, or in any area classified as a wet location.
- To reduce the risk of fire or electrical shock, do not expose this unit to rain or moisture.
- Never push objects of any kind into this unit through openings as they may touch dangerous voltage points or short-out parts that could result in a fire or electrical shock.
- Power supply cords should be routed so that they are not likely to be walked on or pinched by items placed upon or against them, playing particular attention to cords and plugs, convenience receptacles, and the point where they exit from the appliance.
- Operate the unit only from the type of power source indicated on the label. Use only the power supply provided or power supply units with UL approval and a power output according to LPS or NEC Class 2.
- Do not open or remove the cover to service this unit yourself. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.
- Be sure the service technician uses replacement parts specified by the manufacturer. Unauthorized substitutions could void the warranty and cause fire, electrical shock, or other hazards.
- Do safety inspections after service or repairs to the device to make sure the device operates properly.
- Observe the relevant electrical engineering regulations.
- When installing in a switch cabinet, ensure that the unit and the power supply units have sufficient grounding.
- Connect the unit to an earthed mains socket.
- Use proper CMOS/MOS-FET handling precautions to avoid electrostatic discharge (ESD).
- For protection of the device, the branch circuit protection must be secured with a maximum fuse rating of 16 A. This must be in accordance with *NEC800 (CEC Section 60)*.
- Disconnect the power before moving the unit. Move the unit with care. Excessive force or shock may damage the unit and the hard disk drives.

- All the input/output ports are Safety Extra Low Voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.
- If safe operation of the unit cannot be ensured, remove it from service and secure it to prevent unauthorized operation. In such cases, have the unit checked by Bosch Security Systems.
- 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.

1.3 Electrical safety precautions

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

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

⚠ **Caution!**
Replaceable batteries
Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

⚠ **Caution!**
DVD-ROM Laser: To prevent direct exposure to the laser beam and hazardous radiation exposure, do not open the enclosure or use the unit in any unconventional way.

1.4 ESD precautions

ⓘ **Notice!**
Electrostatic Discharge (ESD) can damage electronic components. To prevent damage to your system, it is important to handle the electronic components very carefully.

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

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

1.5 Operating precautions

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

1.6 Notices

ⓘ **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!**
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.

Disposal

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

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

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

Notice!

Do not dispose batteries in household waste. Dispose of batteries only at suitable collection points and, in the case of lithium batteries, mask the poles.

Caution!

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. Dispose of the replaced battery in an environmentally friendly way and not with other solid waste. Refer all servicing to qualified service personnel.

	Do not place this unit on an unstable stand, tripod, bracket, or mount. The unit may fall, causing serious injury and/or serious damage to the unit.

Information on sales, delivery, storage, and working life period

No restrictions or conditions apply for the sale or delivery of this product.

If stored under the specified conditions, the storage period is not restricted.

If used for the specified purpose in compliance with the safety instructions and technical specifications, the working life period of the product is in accordance with normal expectations for this type of product.

Information on equipment use

Device is for professional installation only. Operation of the devices is not intended for personal or household use. There are no restrictions to use the device in commercial and industrial areas, except those mentioned in the Safety information.

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.
- 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(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.385.543	DIP-73G0-00N	Management appliance, 3U w/o HD 3rd gen
F.01U.385.544	DIP-73G8-16HD	Management appliance, 3U 16X8TB 3rd gen
F.01U.385.545	DIP-73GC-16HD	Management appliance, 3U 16X12TB 3rd gen

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

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

This manual is written for professional system integrators and PC technicians. It provides information for the installation of the chassis. The installation should be done by experienced and qualified technicians only.
Before you start the installation, read and follow the safety instructions.

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 3U
1	Rack mount kit
1	Quick installation guide (English)
1	Registration leaflet
2	Power cord EU
2	Power cord US
1	QUERTY USB keyboard
1	USB mouse

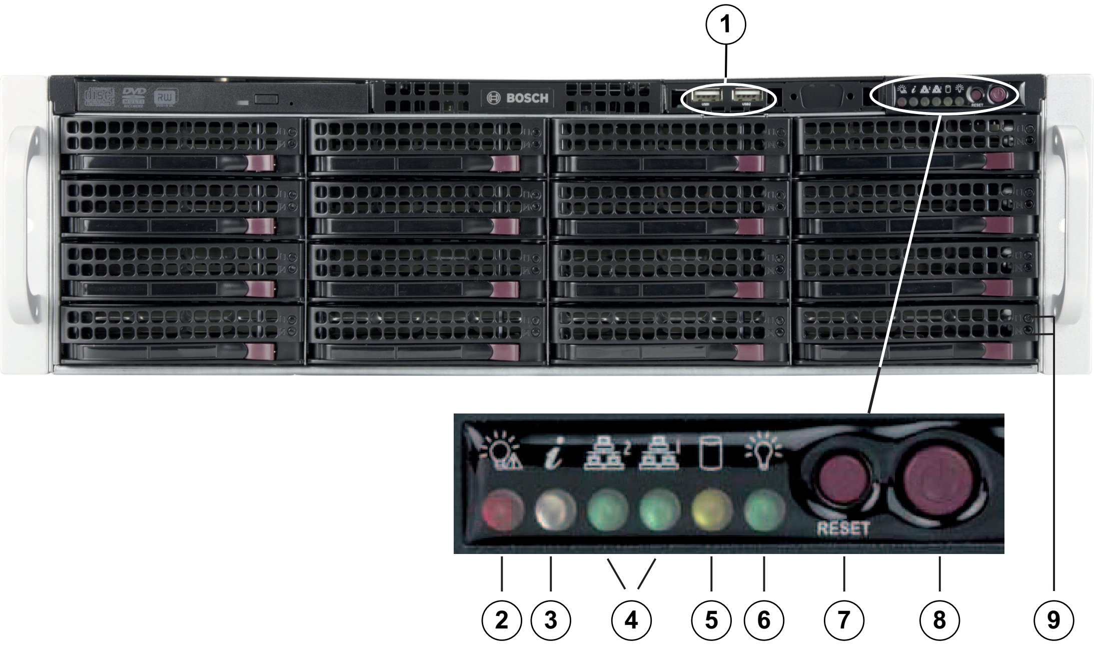
2.2 Product registration

Please register your product:
https://www.boschsecurity.com/product-registration/

3 System overview

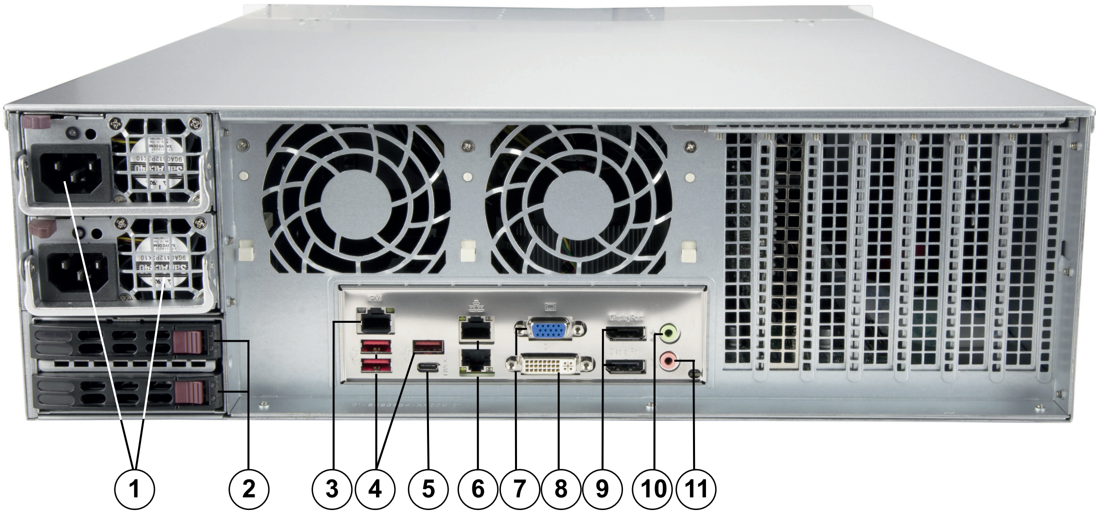
The chassis includes a control panel on the front that features power buttons and status monitoring LEDs. On the rear there are various I/O ports as well as power supply modules.

Front view:



1	2 USB 2.0 ports	**2**	Power failure LED
3	Information LED	**4**	NIC1 and NIC2 LEDs
5	HDD (drive activity) LED	**6**	Power LED
7	Reset button	**8**	Power button
9	Hard drive carrier LEDs		

Rear view:



1	2 power supply modules	**2**	2 redundant SSD drives for operating system (RAID1 mirror)

3	IPMI LAN	**4**	3 USB ports 3.1 Gen 2 (Type A)
5	USB port 3.1 Gen 2 (Type C)	**6**	2 LAN ports (teamed) **Note**: Do not change the teaming mode!
7	VGA display output (disabled)	**8**	DVI-I port
9	2 Display ports	**10**	Audio Line out
11	Audio MIC in		

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

The control panel LEDs provide status information about the system.

<table>
<tr><th>LED</th><th colspan="2">Description</th></tr>
<tr><td><b>Power failure</b></td><td colspan="2">This LED indicates that a power supply module has failed.</td></tr>
<tr><td rowspan="7"><b>Information</b></td><td colspan="2">This LED indicates the system status.</td></tr>
<tr><td><b>System status</b></td><td><b>Description</b></td></tr>
<tr><td>Continuously on and red</td><td>An overheat condition has occurred. (This may be caused by cable congestion.)</td></tr>
<tr><td>Blinking red (1 Hz)</td><td>Fan failure: check for an inoperative fan.</td></tr>
<tr><td>Blinking red (0.25 Hz)</td><td>Power failure: check for an inoperative power supply.</td></tr>
<tr><td>Solid blue</td><td>Local UID has been activated. Use this function to locate the unit in a rack environment.</td></tr>
<tr><td>Blinking blue (300 msec)</td><td>Remote UID has been activated. Use this function to locate the unit from a remote location.</td></tr>
</table>

LED	Description
NIC2	This LED indicates network activity on GLAN2 when flashing.
NIC1	This LED indicates network activity on GLAN1 when flashing.
HDD	This LED indicates activity on the HDDs or peripheral drives when flashing.
Power	This LED indicates that power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is operating.

Hard drive carrier LEDs

The chassis supports hot-swappable SAS/SATA hard drives in hard drive carriers. Each hard drive carrier has two LEDs on the front of the carrier: one activity LED and one status LED. Note: For non-RAID configurations, some LED indications are not supported, for example hot spare.

	LED color	LED state	Description
Activity LED	Blue	Solid On	Hard drive is installed.
	Blue	Blinking	I/O activity.
Status LED	Red	Solid On	Failed hard drive with RSTe support.
	Red	Blinking at 1 Hz	Rebuild hard drive with RSTe support.
	Red	Blinking with two blinks and one stop at 1 Hz	Hot spare for hard drive with RSTe support.
	Red	On for five seconds, then off	Power on for hard drive with RSTe support.
	Red	Blinking at 4 Hz	Identify hard drive with RSTe support.

Power supply LEDs

On the rear of the power supply module, an LED displays the status.

LED color	LED state	Description
Green	Solid On	Power supply is on.
Amber	Solid On	The power supply is plugged in and turned off or The system is off but in an abnormal state.

LED color	LED state	Description
	Blinking	The system power supply temperature has reached 63 °C. The system will automatically turn off when the power supply temperature reaches 70 °C and restart when the power supply temperature goes below 60 °C.

4 Preparing for installation

Read this section in its entirety before you begin the installation.

4.1 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 inches clearance in front of the rack to be able to open the front door completely.
- Leave approximately 30 inches 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.

4.2 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.

4.3 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.

4.4 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 manufacturer’s maximum rated ambient temperature (Tmra).

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.).

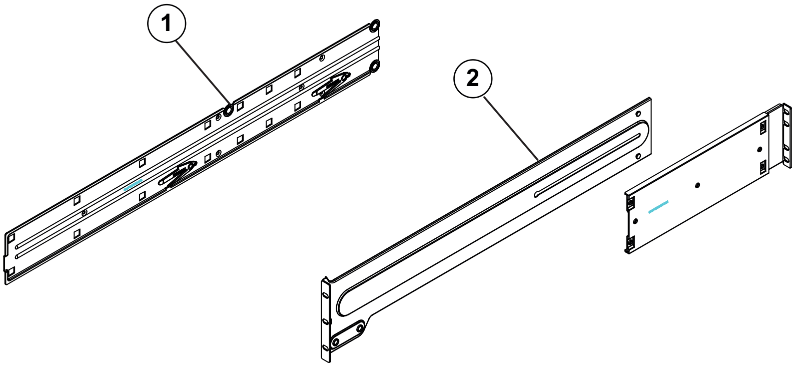
5 Rack installation

This section provides information on installing the chassis into a rack unit. There are a variety of rack units on the market, which may mean the assembly procedure will differ slightly. Also refer to the installation instructions that came with the rack unit you are using.

Notice!
The delivered rails fit a rack with a depth of 26.9 in (68.33 cm) to 36.4 in (92.46 cm) between the mounting posts.

5.1 Identifying the sections of the rack rails

The chassis package includes two rail assemblies, one designed and labeled for each side of the chassis. Each assembly consists of an inner rail that secures directly to the chassis, and an outer rail that secures to the rack. The outer rail has two sections that can slide and adjust to fit your rack depth.



1	Right side inner rail	2	Right side outer rail

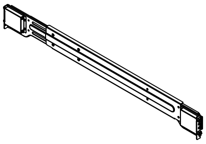
5.2 Separating the sections of the rack rails

The chassis package includes two rail assemblies in the rack mounting kit. Each assembly consists of two sections:

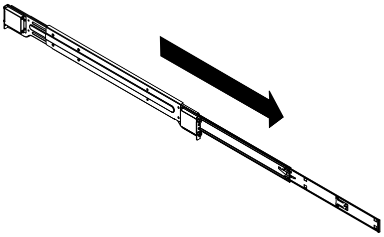
- an inner fixed chassis rail that secures directly to the chassis
- an outer fixed rack rail that secures directly to the rack itself.

To separate the inner and outer rails:

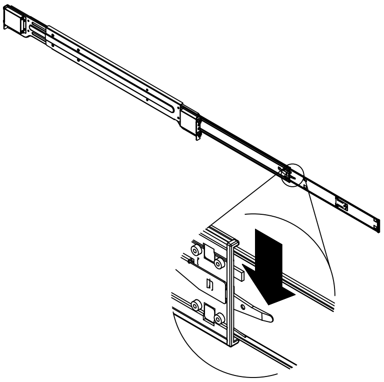
1. Locate the rail assembly in the chassis packaging.



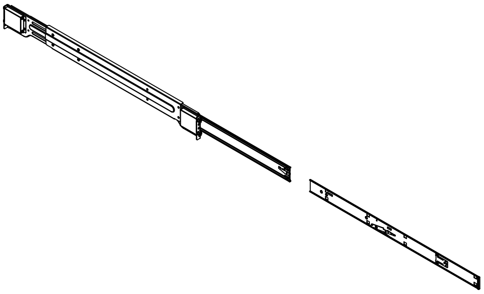
2. Extend the rail assembly by pulling it outward.



3. Press the quick-release tab.



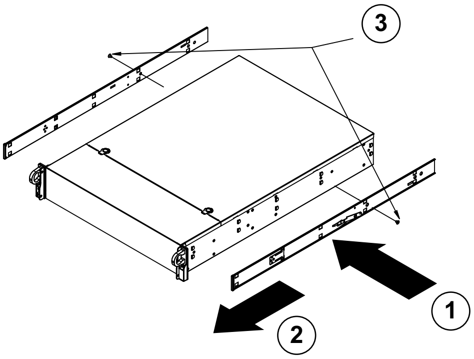
4. Separate the inner rail extension from the outer rail assembly.



5.3 Installing the inner rails on the chassis

The chassis includes a set of inner rails in two sections: inner rails and inner rail extensions. The inner rails are pre-attached to the chassis, and do not interfere with normal use of the chassis if you decide not to use a server rack. The inner rail extension is attached to the inner rail to mount the chassis in the rack.

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

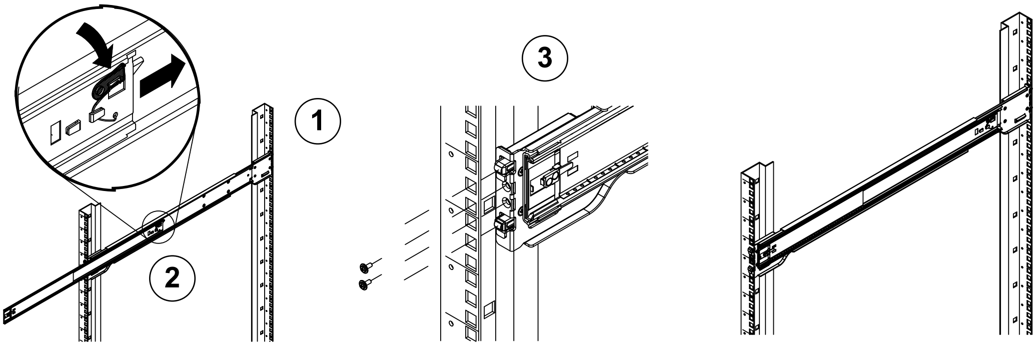


To install the inner rails:

1. Place the inner rail extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with 2 screws as illustrated.
4. Repeat steps 1-3 for the other inner rail extension.

5.4 Installing the outer rails to the rack

Outer rails attach to the rack and hold the chassis in place. The outer rails for the chassis extend between 30 inches and 33 inches.



To install the outer rails to the rack:

1. Secure the back end of the outer rail to the rack, using the screws provided.
2. Press the button where the two outer rails are joined to retract the smaller outer rail.
3. Hang the hooks of the rails onto the rack holes and if desired, use screws to secure the front of the outer rail onto the rack.
4. Repeat steps 1-3 for the remaining outer rail.

Locking Tabs

Both chassis rails have a locking tab, which serves two functions. The first is to lock the system into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the system in place when fully extended from the rack. This prevents the system from coming completely out of the rack when you pull it out for servicing.

5.5 Installing the chassis in the rack

You can install the chassis in a standard rack or in a Telco type 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.

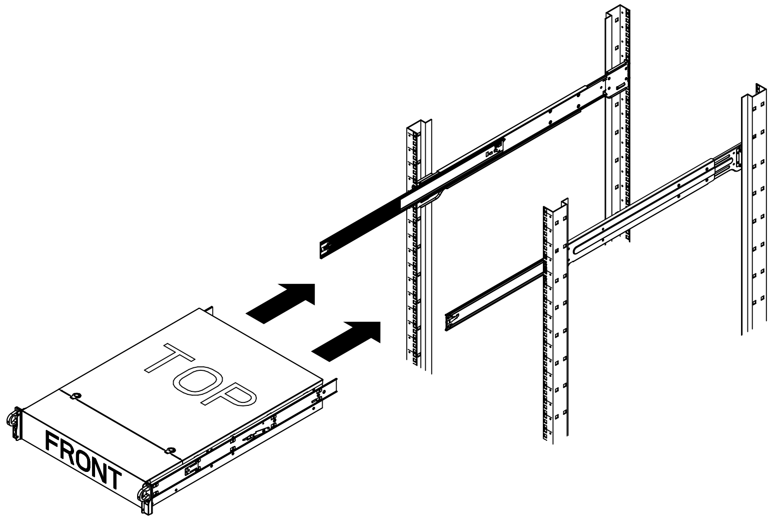
ⓘ **Notice!**
Mounting the chassis into the rack requires at least two people to support the chassis during installation. Please follow safety recommendations printed on the rails.

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

Installing the chassis in a standard rack

To install the chassis in a standard rack:

1. Extend the outer rails.
2. Align the inner rails of the chassis with the outer rails on the rack.
3. Slide the inner rails into the outer rails, keeping the pressure even on both sides.
4. Push the chassis completely into the rack and make sure that it clicks into the locked position.
5. Optionally, use screws to secure the front of the chassis to the rack.



Installing the chassis in a Telco type rack

Notice!
Do not use a two post "Telco" type rack.

To install the chassis in a Telco type rack:

1. Determine how far the chassis will extend out the front of the rack.
   Put larger chassis so that the weight between front and back is balanced.
   If a bezel is included on the chassis, remove it.
2. Attach one L-shaped bracket to each side of the chassis front and one L-shaped bracket to each side of the chassis rear.
3. Make sure that the brackets are positioned with just enough space to fit the width of the Telco rack.
4. Slide the chassis into the rack and tighten the brackets to the rack.

6 Installing a SATA hard drive

The unit has hot-swappable hard drives, which can be removed without turning off the system. The hard drives are mounted in hard drive carriers to simplify their installation and removal from the chassis. These hard drive carriers also help promote proper airflow for the hard drive bays.

Procedure

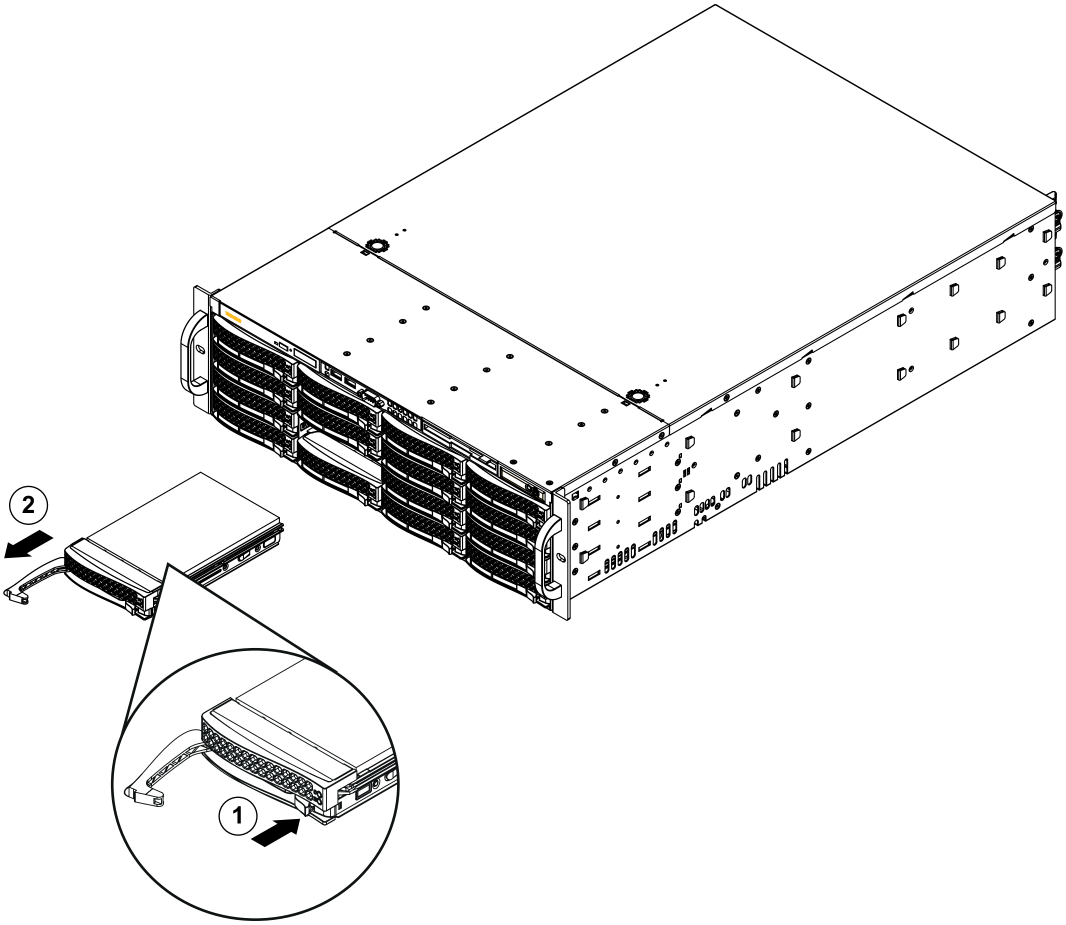
To install a hard drive, you have to perform following steps:

1. *Removing a hard drive carrier from a hard drive bay, page 24*.
2. *Installing a hard drive into a hard drive carrier, page 25*.
3. *Installing a hard drive carrier into a front drive bay, page 25*.

6.1 Removing a hard drive carrier from a hard drive bay

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

1. Press the release button to the right of the hard drive carrier. This extends the hard drive carrier handle.
2. Use the handle to pull the hard drive carrier out of the chassis.



1	Release button	2	Hard drive carrier handle

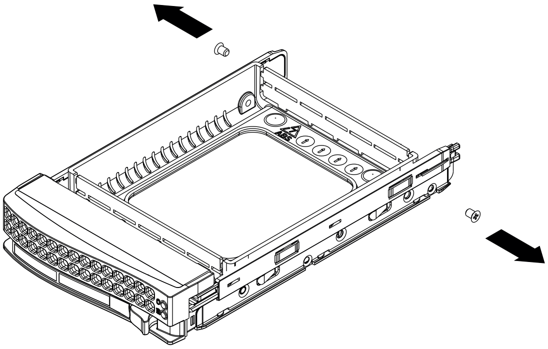
Notice!

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

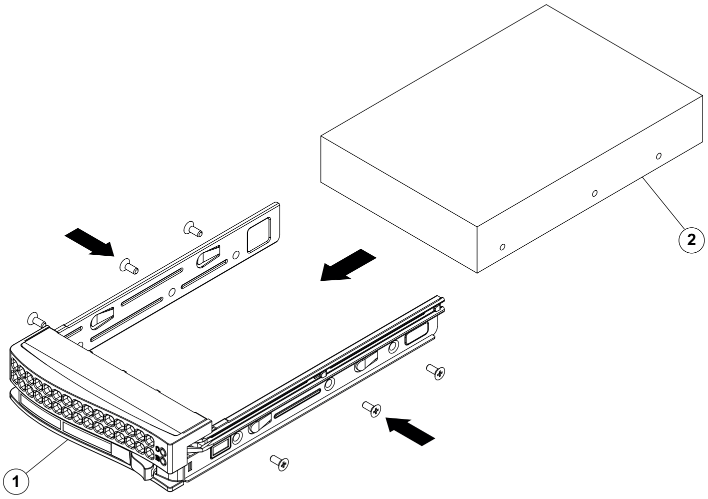
6.2 Installing a hard drive into a hard drive carrier

To install a hard drive into a hard drive carrier:

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



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



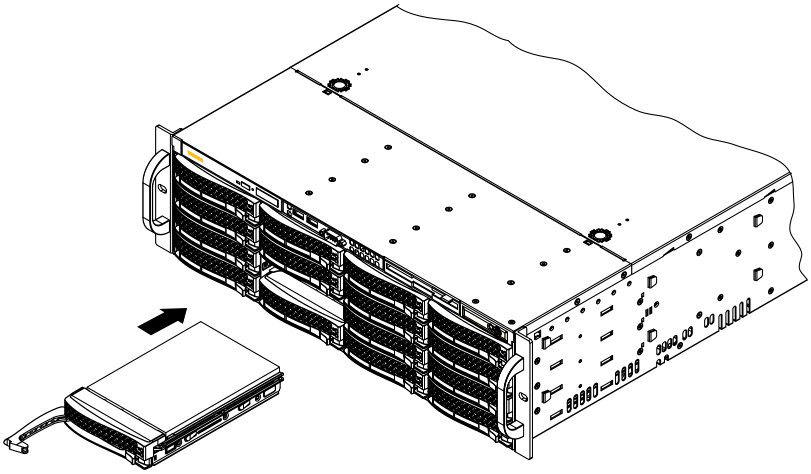
1	Hard drive carrier	2	SATA hard drive

Notice!
Bosch recommends using the respective Bosch hard disk drives. The hard disk drives as one of the critical component are carefully selected by Bosch based on available failure rates. Hard disk drives other then the delivered by Bosch are not supported.
For more information about supported hard disk drives, see the datasheet in the Bosch online product catalog at:
www.boschsecurity.com

6.3 Installing a hard drive carrier into a front drive bay

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

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



7 Turning on the system

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, page 34*.
2. Shut down the unit normally via the Windows **Start** menu.

8 System setup

The DIVAR IP all-in-one 7000 systems are based on the operating system Microsoft Windows Server IoT 2019 for Storage Standard. The operating system provides an 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 2019 for Storage Standard operating system provides significant enhancements in storage management scenarios, as well as integration of storage appliance management components and functionality.

Notice!
This chapter is valid for DIVAR IP all-in-one 7000 models that come with pre-installed hard drives.
If you want to install hard drives to an empty unit, configure them before performing the initial setup.

Refer to

- *Configuring hard drives using the MegaRAID Storage Manager application, page 32*

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.
  - At least one upper case letter.
  - At least one lower case letter.
  - At least one digit.

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 Operating modes

Operation modes

The 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 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.

Notice!
For further details, refer to the User manual.

8.4 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 2019 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.
   - 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 installation file **BoschAppliance_Setup_DSC_[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. In order to prepare the unit for installation of DIVAR IP System Manager, first the **BoschAppliance_Setup_DSC_10.01.0001.exe** needs to be installed.
   Once the system has detected this installation file, it is displayed on the Software Selection page. Click the bar that displays the installation file to start the installation and proceed to Step 14.
   In case this installation file is not detected:
8. Go to https://downloadstore.boschsecurity.com/.
9. Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**.
   A list of all available software packages is displayed.
10. Locate the ZIP file **SystemManager_[software version 2.0.0 or higher].zip** and save it to a storage medium such as a USB stick.
11. Unzip the file on the storage medium by making sure that the folder **BoschAppliance** is placed in the root of the storage medium.
12. Connect the storage medium to your DIVAR IP all-in-one device.
    The system will automatically scan the storage medium for the installation file **BoschAppliance_Setup_DSC_10.01.0001.exe**.
    The scan may take some time. Wait for it to complete.
13. 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.
    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.
14. The installation starts. The installation process may take a few minutes. Do not turn off the system and do not remove the storage medium during the installation process. After the installation has been successfully completed, the system will restart and you will be directed to the Windows sign-in page.
15. Sign in to the administrator account BVRAdmin.
    The **Software Selection** page is displayed, showing the DIVAR IP System Manager 2.x installation file **SystemManager_x64_[software version].exe**.
16. Click the bar that displays the installation file to start the installation.
17. 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.
    After the installation has been successfully completed, the system will restart and you will be directed to the Windows sign-in page.
18. Sign in to the administrator account BVRAdmin.
    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.

19. 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 device.

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/.

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/

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.

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.

8.5 Preparing hard drives for video recording

Systems that come pre-equipped with hard drives from factory are ready to record out-of-the-box.

Hard drives that have been added to an empty system need to be prepared before using them for video recording.

To prepare the hard drives for video recording, you have to do following steps:

1. *Configuring hard drives using the MegaRAID Storage Manager application, page 32*.
2. *Recovering the unit, page 33*.

8.5.1 Configuring hard drives using the MegaRAID Storage Manager application

If you have added third party hard drives to empty units, you must configure the hard drives using the **MegaRAID Storage Manager** application.

ⓘ **Notice!**
The setup process with the **MegaRAID Storage Manager** application is not necessary for units with pre-installed hard drives. These units are delivered with a default configuration.

To configure RAID5:

1. Install all hard drives.
2. Turn on the system.
3. Set up the operating system and install DIVAR IP System Manager as described in the user manual.
4. After the DIVAR IP System Manager window is displayed, minimize the window.
5. On the Windows desktop, double-click the **MegaRAID Storage Manager** icon to start the application.
   The **Enter User Name & Password** dialog box is displayed.

6. Enter user name and password, and then click **Login**.
   - User name: **BVRAdmin**
   - Password: as it was set during the initial operating system setup process
7. In the **MegaRAID Storage Manager** main window, click the tab **Physical**.
8. In the device tree, right-click the desired controller node, then click **Create Virtual Drive**.
   The **Create Virtual Drive - Choose mode** dialog box is displayed.
9. Click **Advanced**, then click **Next**.
   The **Create Drive Group - Drive Group Settings** dialog box is displayed.
10. In the **RAID Level** list, select RAID 5.
11. In the **Select unconfigured drives:** list, select the respective hard drives, then click **Add>**.
    The selected drives are displayed in the **Drive groups:** box.
12. Click **Next** to continue.
    The **Create Virtual Drive - Virtual drive settings** dialog box is displayed.
13. Apply the following settings:
    - **Initialization state**: Fast Initialization
    - **Strip Size:** 64 KB
    - **Write Policy:** Always Write Back

    NOTICE! Keep all other settings unchanged.
14. Click **Create Virtual Drive**.
    The virtual drive is created.
15. Click **Next** to continue.
    The **Create Virtual Drive - Summary** box is displayed.
16. Check the settings for the virtual drive configuration.
17. Click **Finish** to accept the settings and to complete the configuration.
    The virtual drive will be created and initialized.
18. Exit the **MegaRAID Storage Manager** application.
19. Perform a complete system recovery (Initial Factory Setup).

8.5.2 Recovering the unit

Following procedure describes how to restore the factory default image.

To restore the unit to factory default image:

1. Start the unit and press **F7** during the BIOS power-on-self-test to enter Windows PE.
   The Recovery menu is displayed.
2. Select one of the following options:
   - **Initial Factory Setup (all data on system will be lost):** This option deletes data on all HDD partitions and overwrites the operating system partition with the factory default image.
   - **Initial Factory Setup (overwriting existing data):** This option deletes and overwrites data on all HDD partitions. Furthermore, it overwrites the operating system partition with the factory default image.
     Note: This procedure might take very long.
   - **System Recovery (back to Factory Defaults):** This option overwrites the operating system partition with the factory default image and imports existing virtual hard drives from the HDDs during recovery.

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

8.6 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.

8.7 Configuring IPMI settings

DIVAR IP all-in-one 7000 has a dedicated IPMI port on the rear side.
Each DIVAR IP all-in-one 7000 unit is delivered with the default user name ADMIN and with an initial password. The initial password is unique for each unit. You can find it on the label at the rear of the unit, below the IPMI port.
Bosch strongly recommends to change the initial password during the IPMI configuration, and to store the new password at a secure location.

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

To configure the IPMI settings:

1. Turn on the unit and press Del to enter the BIOS setup.
2. In the BIOS setup, navigate to the tab **IPMI**.
3. Select the option **BMC Network Configuration**, then press Enter.
4. In the next dialog box, select the option **Update IPMI LAN Configuration**, then press Enter.
   The **Update IPMI LAN Configuration** dialog box is displayed.
5. In the **Update IPMI LAN Configuration** dialog box, select **Yes**, 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 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/

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

Building solutions for a better life.