DIVAR IP 5000

DIP-5042EZ-0HD | DIP-5042EZ-1HD | DIP-5042EZ-2HD | DIP-5042EZ-4HD | DIP-5044EZ-1HD | DIP-5044EZ-2HD | DIP-5044EZ-4HD

en Installation manual

Table of contents

1	**Safety**	**4**
1.1	Safety message explanation	4
1.2	Safety precautions	4
1.3	Important safety instructions	4
1.4	Notices	7
1.5	FCC and UL	9
2	**Available documentation**	**11**
3	**System overview**	**12**
3.1	Device views	12
3.2	LED description - front panel	15
3.3	LAN port LED description - rear panel	16
4	**Chassis setup**	**17**
4.1	Removing hard drive trays	17
4.2	Installing a hard drive	18
5	**Installation - first steps**	**19**
5.1	Setup notes	19
5.2	Connecting the unit	19
6	**Obtaining a basic configuration**	**20**
7	**Advanced setup - dual network**	**21**
8	**Advanced configuration**	**23**
9	**Maintaining the system**	**25**
9.1	Monitoring the system	25
9.2	Recovering the unit	26
9.3	Backing up the configuration	27
9.4	Adding/replacing hard disks	27
9.4.1	Extending a 2-disk unit	27
9.4.2	Extending an empty unit	28
9.4.3	Replacing hard disks	29
9.5	Updating the system	29
9.6	Using the IP Helper tool	30
10	**End-user license agreement**	**32**

1 Safety

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 Safety precautions

Caution!
Installation should only be performed by qualified service personnel in accordance with the National Electrical Code (NEC 800 CEC Section 60) or applicable local codes.

1.3 Important safety instructions

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.

- Operate the device only from the type of power source indicated on the label.
- 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.
- Leave approximately 5 cm (2 inches) clearance to the next object.
- Do not place the unit in an enclosure unless proper ventilation is provided, or the manufacturer's instructions have been adhered to.
- 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.

- For added protection during a lightning storm, or when leaving this unit unattended and unused for long periods, unplug the unit from the wall outlet and disconnect the cable system. This will prevent damage to the unit from lightning and power line surges.
- 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.
- 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 Bosch Service Center.
- Observe the relevant electrical engineering regulations.
- Use proper CMOS/MOS-FET handling precautions to avoid electrostatic discharge when adding or changing hard disks.
- Install the unit only in a dry, weather-protected location.
- 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.
- 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)*.
- All the input/output ports are Safety Extra Low Voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.
- 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.
- 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.

1.4 Notices

Notice!
The operating system includes the latest Windows security patches available at the time the software image was created. We recommend that you keep your device updated using the online update functionality.

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.

	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 intended for industrial, commercial, personal or household use. There are no restrictions to use the device in commercial and industrial areas, except those mentioned in the Safety information.

1.5 FCC and UL

FCC & ICES Information

(U.S.A. and Canadian Models Only)

This equipment has been tested and found to comply with the limits for a **Class B** digital device, pursuant to Part 15 of the FCC Rules and ICES-003 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a **residential installation**. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Intentional or unintentional modifications, not expressly approved by the party responsible for compliance, shall not be made. Any such modifications could void the user's authority to operate the equipment. If necessary, the user should consult the dealer or an experienced radio/television technician for corrective action.

The user may find the following booklet, prepared by the Federal Communications Commission, helpful: How to Identify and Resolve Radio-TV Interference Problems. This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

UL Disclaimer

Underwriter Laboratories Inc. ("UL") has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested fire, shock and/or casualty hazards as outlined in Standard(s) for Safety for Information Technology Equipment, UL 60950-1 . UL Certification does not cover the performance or reliability of the security or signaling aspects of this product.

UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY SECURITY OR SIGNALING-RELATED FUNCTIONS OF THIS PRODUCT.

2 Available documentation

This manual is available in different languages. You can find all manuals in the online product catalog.

More information

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

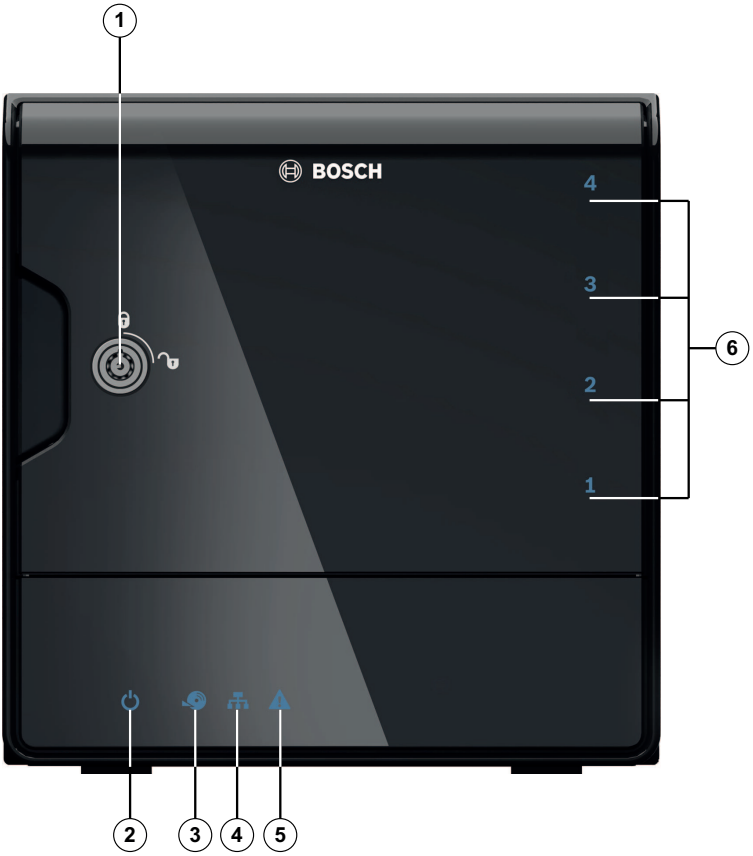
3 System overview

The DIVAR IP 5000 system is an affordable, easy to use all-in-one recording solution for network surveillance systems of up to 32 channels. All channels are pre-licensed. Running the full Bosch recording solution, DIVAR IP 5000 is an intelligent IP storage device that provides both, a professional video recording solution and ease of operation.
DIVAR IP 5000 is a 4-bay mini tower unit that combines advanced management and state-of-the-art recording management into a single, cost-effective, plug and play IP recording appliance for IT-minded customers.
DIVAR IP 5000 utilizes a highly energy efficient, embedded design at a very affordable price which nevertheless boasts Bosch quality through-and-through.
Easy to install and operate, DIVAR IP 5000 features wizard-based set-up and centralized configuration to reduce installation times. All components are pre-installed and pre-configured. Simply connect to the network and turn on the unit — DIVAR IP 5000 is ready to begin recording straight out-of-the-box.
DIVAR IP 5000 features front-swappable SATA-II hard drives. All system software is pre-installed and pre-activated — creating a ready-to-use video recording appliance.

3.1 Device views

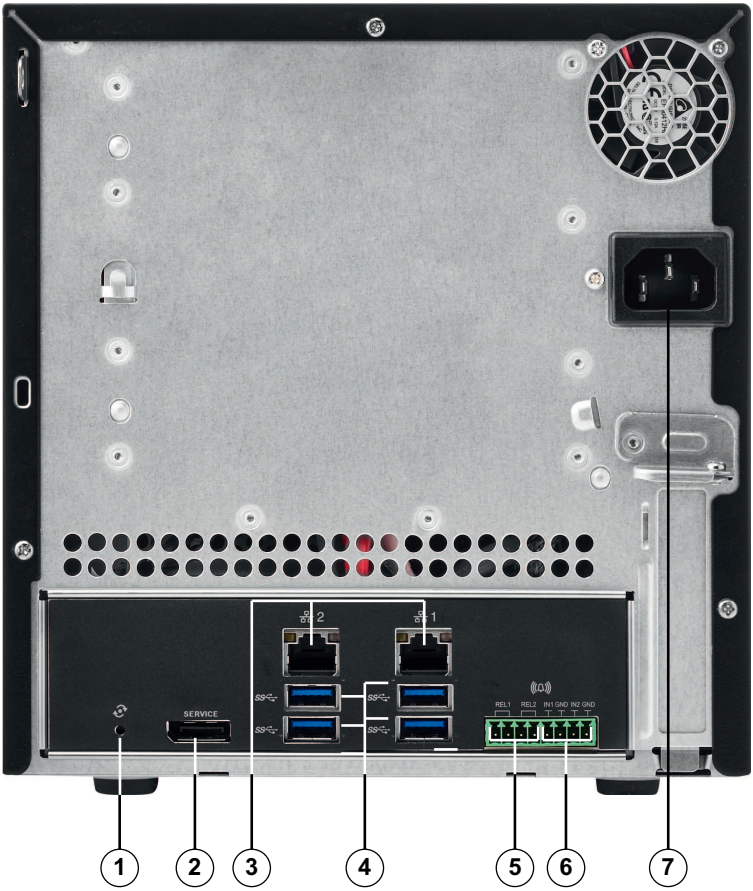
There are several LEDs on the front and rear of the chassis. The LEDs show the over-all status of the system and the activity and health of specific components.

Front view:



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

DIVAR IP rear view:



1	Factory reset button	**5**	2x Alarm Out
2	1x Display port **Note:** Only for troubleshooting.	**6**	2x Alarm In
3	2x Ethernet (RJ45)	**7**	Mains connection 100 - 240 VAC

4	4x USB 3.0 **Note:** Only for troubleshooting.		

3.2 LED description - front panel

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

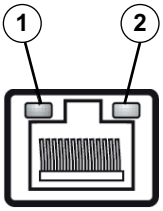
LED indicator	LED color	LED state	Description
Power LED	N/A	Off	Power off
	Blue	On (default)	Working
HDD LED	N/A	Off	No disk access
	Blue	Blinking	Disk access
LAN LED	N/A	Off	Network disconnected
	Blue	On	Network connected
	Blue	Blinking	Network activity
System LED	N/A	Off	System has booted in normal operation.
	Blue	Blinking	System is booting or a software update is being applied.
	Red	On	Undefined software error. Contact technical support.
Individual hard disk LED	N/A	Off (default)	No hard drive configured for this bay.
	Blue	On	Hard drive present and working.

LED indicator	LED color	LED state	Description
	Blue	Blinking	Hard drive health not optimal — needs attention.
	Red	On	Hard drive is configured for this bay, but is not working.

3.3 LAN port LED description - rear panel

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

LAN connector:



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

4 Chassis setup

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

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

Observe the following prerequisites when adding or replacing hard disks.

Prerequisites:

– For RAID configuration, all hard disks of the unit must have the same capacity

Notice!
Insert the hard disks before initial system start.

See also

– *Safety, page 4*
– *Installing a hard drive, page 18*

4.1 Removing hard drive trays

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.

To remove hard drive trays from the chassis:

1. Turn off the system.
2. Press the release button on the drive carrier. This extends the drive carrier handle.
3. Use the handle to pull the drive carrier with the drive out of the chassis.

4. Insert the drive carrier with the new drive into the chassis bay, making sure that the drive carrier handle is completely closed.

4.2 Installing a hard drive

The hard drives are mounted in hard drive carriers.

To install a hard drive to the hard drive carrier:

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

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

See also

– *Available documentation, page 11*

5 Installation - first steps

DIVAR IP systems are shipped with a pre-installed browser-based configuration wizard.

5.1 Setup notes

By default all DIVAR IP systems are configured to obtain a valid network address from DHCP server in the local network. In small networks this task is usually performed by an internet router. If there is no DHCP server in the network, DIVAR IP will use the following network settings:

– IP Address: 192.168.0.200
– Subnet mask: 255.255.255.0

Notice!
We strongly recommend that you do not change any operating system settings. Operating system access should only be used for troubleshooting. Changes can result in malfunctioning of the system.

5.2 Connecting the unit

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

Connecting the unit:

1. Connect the unit and the cameras to the network.
2. Connect the unit to the power supply.
3. Turn on the unit.

   Note: During this initial setup the system LED is blinking. After the system is ready for operation, the system LED stops blinking. The web based wizard pages of the DIVAR IP can be accessed from any browser within the network. Use these web page wizard pages to obtain a basic system configuration.

6 Obtaining a basic configuration

DIVAR IP 5000 offers an easy-to-use configuration wizard to achieve a basic configuration of a smaller system easily.
To achieve a basic configuration using the Configuration Wizard:

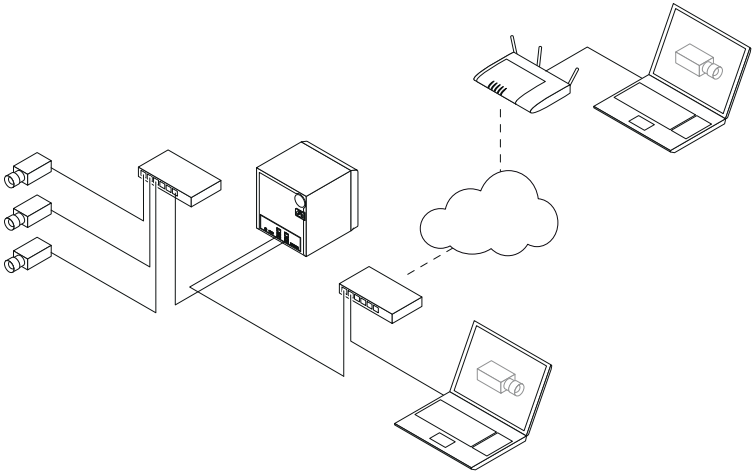
1. Open a web browser from any PC in the network, enter the IP address of DIVAR IP in the address bar, then press Enter. The **Welcome** page of the Configuration Wizard is displayed.
   Note:
   If you do not know the IP address, proceed as follows:
   – Only one DIVAR IP 5000 is in the network:
     Enter `http://mydivar` or `https://mydivar`, then press Enter. The **Welcome** page of the Configuration Wizard is displayed.
     Note: Use `mydivar` only if there is one DIVAR IP in the same network, not if there are multiple DIVAR IP.
   – Multiple DIVAR IP 5000 are in the same network:
     Use the IP Helper tool to display all devices with their IP addresses. The tool is available in the online catalog on the DIVAR IP 5000 product page.
2. On the **Welcome** page select your preferred language, then click **Start configuration**.
3. Run-through the wizard and follow the instructions. Each page provides you with information how to use it.
4. After finishing the Configuration Wizard your system has a basic configuration available. If the basic configuration needs to be extended, use the advanced configuration.

See also

– *Using the IP Helper tool, page 30*
– *Advanced configuration, page 23*

7 Advanced setup - dual network

DIVAR IP systems support the separation of networks. Users can connect both network interfaces to two different switches and configure the TCP/IP settings. This allows the separation of devices and public network.



By default both network interfaces are combined to one single network interface.

To separate the network interfaces:

1. Open a web browser from any PC in the network.
2. In the address bar of the web browser, enter `http://mydivar/configurationsite` or `http://<IP address of DIVAR IP>/configurationsite`, then press Enter. The DIVAR IP configuration window is displayed.
3. In the **Configuration** window, expand **Network**, then click **Network access**.
4. Click to clear the **Enable teaming of network interfaces** check box, then configure the network interfaces.
5. Enter your changes and save the configuration.

Notice!
If teaming mode is deactivated:
To connect the camera network, use the network connection on the backplane that is labeled with 1. That means all cameras for live and recording must be accessible over this network.
The second network connection on the backplane can be used for uplink, for example.

Notice!
Due to performance issues, do not use the DIVAR IP system as network bridge between both networks.

8 Advanced configuration

The advanced configuration allows you to configure the system to your needs.

To use the advanced configuration:

1. Open a web browser from any PC in the network.
2. In the address bar of the web browser, enter `http://mydivar/configurationsite` or `http://<IP address of DIVAR IP>/configurationsite`, then press Enter.
   The DIVAR IP configuration window is displayed.
   Note: If the DIVAR IP user interface is already open, click the **Configuration** tab.
3. Select the desired page in the tree structure to make the changes.
   - **Video devices page**
     Adding and removing devices
     Replacing devices
     Configuring cameras and video images
     Adjusting the video quality
     Adding non-listed devices via RTSP
     Defining the motion detection settings
   - **Recording page**
     Defining phases and assigning properties to phases
     Defining the recording mode
     Editing the video quality
   - **Alarms page**
     Adding and deleting actions
     Configuring alarm inputs and outputs
     Configuring e-mail properties
     Configuring alarm scenarios
     Configuring notifications
   - **Network page**
   - Identifying DIVAR IP devices
     Configuring the network interface
     Selecting a dynamic DNS provider

Testing the connections to DIVAR IP 5000 systems
Adding accounts
System page
Selecting the language
Setting the password
Setting the time zone, date, and time
Defining the storage mode
Maintaining the system
Managing certificates

4. Make the changes and save the configuration.

Notice!
Use the help that is available for each page.

See also

- *Obtaining a basic configuration, page 20*
- *Monitoring the system, page 25*
- *Using the IP Helper tool, page 30*

9 Maintaining the system

9.1 Monitoring the system

DIVAR IP Dashboard is used to monitor the status of a DIVAR IP system from any PC in the network.
DIVAR IP Dashboard provides information on the DIVAR IP system.

Notice!
To configure the system, use the Configuration Wizard first to obtain a basic configuration, then (if necessary) open the Configuration menu for advanced configuration.

To use DIVAR IP 5000 Dashboard:

1. Open a web browser from any PC in the network.
2. In the address bar of the web browser, enter `http://mydivar/dlacockpit` or `http://<IP address of DIVAR IP>/dlacockpit`, then press Enter. The DIVAR IP 5000 Dashboard window is displayed.
   Note: If the DIVAR IP user interface is already open, click the **Dashboard** tab.
3. Select the desired page in the tree structure to obtain system information.
   - **System information page**
     Displays the system status, hard drive information, and event logs, for example.
   - **Logbook page**
     Displays logbook information.
   - **Device monitor page**
     Displays all connected devices with device name, device type, firmware version, status, recording encryption and bandwidth..
     Offers an **Update manually...** and **Update from Internet** button to update the system software.

Notice!
Use the help that is available for each page.

See also
- *Obtaining a basic configuration, page 20*
- *Advanced configuration, page 23*

9.2 Recovering the unit

Following procedures describe how to restore the software default configuration and the factory default image.

Notice!
Before recovering DIVAR IP we recommend backing up the configuration.

Option 1: The unit is in operation

- Press the factory reset button on the back of the unit for 10 seconds. The software default configuration will be restored. Data on the hard disks will not be deleted.

Option 2: The unit is switched off

- Hold down the factory reset button on the back of the unit and press the power button on the front. The factory default image will be restored. Data on the hard disks will not be deleted.

Notice!
For both options, you can access the unit's website after 30 minutes.

See also
- *Backing up the configuration, page 27*

9.3 Backing up the configuration

Following procedure describes how to back up the configuration.

Notice!
We recommend backing up the configuration frequently so that recent backups are always available if required.

To back up the configuration:

1. In the DIVAR IP configuration, expand **System**, then click **Service**.
2. To back up the configuration, click ▶ to expand the **Backup** group, then click **Back up**. A dialog box is displayed.
3. Click **Save**. Where the configuration is saved depends on the browser settings.
   Note: If you want to select a specific target directory for the backup file, click the arrow to the right of the **Save** button, then click **Save as**.
4. To find the backup, click the Windows **Start** button, enter `downloads` in the search box, then press Enter.
   A dialog box containing the backup file is displayed.

9.4 Adding/replacing hard disks

Observe the following prerequisites when adding or replacing hard disks.

Prerequisites:

– For RAID configuration, all hard disks of the unit must have the same capacity

9.4.1 Extending a 2-disk unit

You can extend a unit with additional hard disks.

To add hard disks to a 2-disk unit:

1. Turn off the unit by pressing the power button.
2. Insert the new hard disks into the chassis bay, making sure that the drive carrier handle is completely closed.

3. Turn on the unit by pressing the power button.
4. Open DIVAR IP Dashboard with any browser. To do this, in the address bar of the web browser, enter `http://mydivar/dlacockpit` or `http://<IP address of DIVAR IP>/dlacockpit`, then press Enter. DIVAR IP 5000 Dashboard displays the message that you must open **Configuration** > **Disk management** for configuration.
5. Click **Configuration** to open the configuration.
6. Expand **System**, then click **Disk management**.
7. To add the storage capacity of the hard disks to the system, follow the instructions that are displayed.
8. After finishing the hard disk setup the individual disk status LED to the right of the disk carrier will turn blue.

See also

– *Chassis setup, page 17*

9.4.2 Extending an empty unit

You can extend an empty unit with additional hard disks.

To add hard disks to an empty unit:

1. Insert the new hard disks into the chassis bay, making sure that the drive carrier handle is completely closed.
2. Turn on the unit by pressing the power button.
3. The unit identifies the hard disks as new and starts the recovery menu automatically.
   After finishing the recovery process the DIVAR IP software is installed. The individual disk status LED to the right of the disk carrier will turn blue.
4. Perform a basic configuration using the configuration wizard.

See also

– *Chassis setup, page 17*
– *Obtaining a basic configuration, page 20*

9.4.3 Replacing hard disks

If a hard disk fails, the individual disk status LED to the right of the disk carrier will turn red.

To replace hard disks:

1. Remove the defective hard disk. Use the handle to pull the disk carrier out of the chassis.
   Note: You can remove the hard disk during operation.
2. Turn off the unit by pressing the power button.
3. Insert the new hard disks into the chassis bay, making sure that the drive carrier handle is completely closed.
4. Turn on the unit by pressing the power button.
5. Open DIVAR IP Dashboard with any browser. To do this, in the address bar of the web browser, enter `http://mydivar/dlacockpit` or `http://<IP address of DIVAR IP>/dlacockpit`, then press Enter. DIVAR IP 5000 Dashboard displays the message that you must open **Configuration** > **Disk management** for configuration.
6. Click **Configuration** to open the configuration.
7. Expand **System**, then click **Disk management**.
8. To add the storage capacity of the hard disks to the system, follow the instructions that are displayed.
9. After finishing the hard disk setup the individual disk status LED to the right of the disk carrier will turn blue.

See also

– *Chassis setup, page 17*

9.5 Updating the system

Following procedure describes how to update the system manually.

To update DIVAR IP manually:

1. In DIVAR IP Dashboard, click **Device monitor** in the tree structure.

2. Click **Update manually**.
   A dialog box is displayed where you can browse for the update file.

To update DIVAR IP using the internet:

1. In DIVAR IP Dashboard, click **Device monitor** in the tree structure.
2. Click **Update from Internet** .

Notice!
If your system is connected to the internet, the system is automatically checking for updates. If an update is available, you can download and install it directly. If your system is not connected to the internet, you can manually download the latest update package from the product pages. Updating your system includes all components as well as camera devices. Updating will take about 5 - 10 minutes and recodings are stopped during the update process.

9.6 Using the IP Helper tool

The IP Helper from Bosch is a small windows tool that allows users to view all IP devices with their IP addresses located in a network. With this tool user can find IP addresses of IP devices or configure the network settings of the IP devices in a quick and easy way without having expert knowledge. The IP Helper is a directly executable program, no installation is necessary. You can use any PC in the network to open IP Helper. Opening IP Helper directly from a USB stick is possible.
The IP Helper tool is available for download as follows:

– in the online catalog on the DIVAR IP 5000 product page
– under http://mydivar.com
– under http://downloadstore.boschsecurity.com/

To find DIVAR IP systems:

1. Double-click the IP Helper tool (`iphelper.exe`).

2. A dialog box opens that displays all IP devices with their IP addresses located in the network. Search for the DIVAR IP system you want to configure and note the IP address.
Note: To identify a DIVAR IP system, press **Blink LED**.

10 End-user license agreement

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS STORAGE SERVER 2012 R2 ESSENTIALS

These license terms are an agreement between you and:

- the server manufacturer that distributes the software with the server; or
- the software installer that distributes the software with the server.

Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply. If you obtain updates or supplements directly from Microsoft, Microsoft, and not the manufacturer or installer, licenses those to you. Printed paper license terms, which may come with the software, take the place of any on-screen license terms.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, contact the manufacturer or installer to determine its return policy for a refund or credit.

As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.

If you comply with these license terms, you have the rights below for each software license you acquire.

1. OVERVIEW.

a. Software. The software includes:

- server software; and
- additional software that may only be used with the server software.

b. License Model. The software is licensed based on:

- the number of instances of server software that you run; and
- the number of user accounts that access instances of server software.

c. Licensing Terminology.

- **Instance.** You create an "instance" of software by executing the software's setup or install procedure. You also create an instance of software by duplicating an existing instance. References to software in this agreement include "instances" of the software.
- **Run an Instance.** You "run an instance" of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.
- **Operating System Environment.** An "operating system environment" is:

  (i) all or part of an operating system instance, or all or part of a virtual (or otherwise emulated) operating system instance that enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and

  (ii) instances of applications, if any, configured to run on the operating system instance or parts identified above.

  There are two types of operating system environments: physical and virtual. A physical operating system environment is configured to run directly on a physical hardware system. The operating system instance used to run hardware virtualization software (e.g., Microsoft Virtual Server or similar technologies) or to provide hardware virtualization services (e.g., Microsoft virtualization technologies or similar technologies) is considered part of the physical operating system environment. A virtual operating system environment is configured to run on a virtual (or otherwise emulated) hardware system.

  A physical hardware system can have either or both of the following:

  (i) one physical operating system environment, and

  (ii) one or more virtual operating system environments.
- **Server.** A server is a physical hardware system or device capable of running server software. A hardware partition or blade is considered to be a separate physical hardware system.
- **Assigning a License.** To assign a license means simply to designate that license to one device or user.

USE RIGHTS.

a. Assignment of the License to the Server. The software license is permanently assigned to the server with which you acquired the software. That server is the

licensed server for that particular license. A hardware partition or blade is considered to be a separate server. You may not assign the same license to more than one server.

b. **Running Instances of the Server Software.** You may run, at any one time, one instance of the server software in one physical operating system environment on the licensed server.

c. **Using the Server Software**. You may install and use one copy of the server software on one licensed server. Up to 50 users can access and use the server software on that server as long as:

- each such user has an assigned user account with unique user id and password, and
- the user accesses the server software through that account.

You may reassign a user account from one user to another provided that the reassignment does not occur within 90 days of the last assignment.

d. **Creating and Storing Instances on Your Servers or Storage Media.** For each software license you acquire you may create and store any number of instances of the software on any of your servers or storage media. This may be done solely to exercise your right to run instances of the software under any of your licenses as described in the applicable use rights (e.g., you may not distribute instances to third parties).

e. **Included Microsoft Programs.** The software contains other Microsoft programs. These license terms apply to your use of those programs.

3. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. **Specific Use**. The manufacturer or installer designed this server for a specific use. You may only use the software for that use. You may not use the software to support additional software programs or functions, other than utilities or similar software used solely for administration, performance enhancement, preventative maintenance, or to provide complimentary data storage functionality for this server.

b. **Limitation on Functions Supported by the Software**. The manufacturer or installer licenses you to use the server software to support only the base functions as provided and installed on this server. You are not licensed to use the server to run or support:

- enterprise database software (such as Microsoft SQL Server), except non-enterprise engines such as Microsoft SQL Server Express Edition. The server software also may run or support enterprise database engines (including Microsoft SQL Server) that are integrated in and used only to support the server

software as part of the specific use for which the manufacturer or installer designed this server,

- enterprise resource planning (ERP) software,
- messaging or enterprise mail,
- Microsoft Exchange or Microsoft SharePoint Portal Server,
- team collaboration software,
- web-based time management applications that address appointment, meeting and other calendar items,
- more than 8 disk drives,
- NVMe-enabled hardware, and/or
- the external Serial Attached SCSI (SAS) interconnect.

These limitations do not restrict use of the server for data management (such as providing storage and backup functions) for the software identified above.

c. **No Windows Server CALs Required**. Servers that access or use functions of Windows Storage Server software licensed under these license terms do not require a client access license (CAL) for Windows Server. Obtaining a CAL for any Microsoft product does not grant you rights to use functions of the server software not licensed under these license terms.

d. **Multiplexing.** Hardware or software you use to:

- pool connections,
- reroute information,
- reduce the number of devices or users that directly access or use the software,
- reduce the number of devices or users the software directly manages,

(sometimes referred to as “multiplexing” or “pooling”), does not reduce the number of licenses of any type that you need.

e. **Font Components.** While the software is running, you may use its fonts to display and print content. You may only:

- embed fonts in content as permitted by the embedding restrictions in the fonts; and
- temporarily download them to a printer or other output device to print content.

f. **Icons, images, and sounds.** While the software is running, you may use but not share its icons, images, sounds, and media. The sample images, sounds, and media provided with the software are for your non-commercial use only.

g. **No Separation of Server Software.** You may not separate the server software for use in more than one operating system environment under a single license, unless expressly permitted. This applies even if the operating system environments are on the same physical hardware system.

h. **Additional Functionality.** Microsoft may provide additional functionality for the software. Other license terms and fees may apply.

i. **Maximum Instances**. The software or your hardware may limit the number of instances of the server software that can run in physical or virtual operating system environments on the server.

4. **MANDATORY ACTIVATION.** Activation associates the use of the software with a specific device. During activation, the software may send information about the software and the device to Microsoft. This information includes the version, language, and product key of the software, the Internet protocol address of the device, and information derived from the hardware configuration of the device. For more information, see microsoft.com/piracy/. **By using the software, you consent to the transmission of this information.** If properly licensed, you have the right to use the version of the software installed during the installation process up to the time permitted for activation. **Unless the software is activated, you have no right to use the software after the time permitted for activation.** This is to prevent its unlicensed use. **You are not permitted to bypass or circumvent activation.** If the device is connected to the Internet, the software may automatically connect to Microsoft for activation. You can also activate the software manually by Internet or telephone. If you do so, Internet and telephone service charges may apply. Some changes to your computer components or the software may require you to reactivate the software. **The software may remind you to activate it until you do.**

5. **VALIDATION.**

a. If the manufacturer or installer activated the software for you, you may not be asked to activate the software when you first use it. The software will from time to time validate the software and update or require download of the validation feature of the software. Validation verifies that the software has been activated and is properly licensed. Validation also permits you to use certain features of the software or to obtain additional benefits. For more information, see go.microsoft.com/fwlink/?linkid=39157.

b. During a validation check, the software will send information about the software and the device to Microsoft. This information includes the version and product key of the software, and the Internet protocol address of the device. Microsoft does not use the information to identify or contact you. By using the software, you consent to the

transmission of this information. For more information about validation and what is sent during a validation check, see go.microsoft.com/fwlink/?linkid=69500.

c. If, after a validation check, the software is found not to be properly licensed, the functionality of the software may be affected. For example, you may:

- need to reactivate the software, or
- receive reminders to obtain a properly licensed copy of the software,

or you may not be able to:

- use or continue to use some of the features of the software, or
- obtain certain updates or upgrades from Microsoft.

d. You may only obtain updates or upgrades for the software from Microsoft or authorized sources. For more information on obtaining updates from authorized sources, see go.microsoft.com/fwlink/?linkid=69502.

6. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time.

a. Consent for Internet-Based Services. The software features described below and in the Windows Storage Server Privacy Highlights connect to Microsoft or service provider computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. You may switch off these features or not use them. For more information about these features, visit go.microsoft.com/fwlink/?LinkID=280262. **By using these features, you consent to the transmission of this information.** Microsoft does not use the information to identify or contact you.

Computer Information. The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser, the name and version of the software you are using, and the language code of the device where you run the software. Microsoft uses this information to make the Internet-based services available to you.

- Windows (or Microsoft) Update Feature. You may connect new hardware to the device where the software is installed. Your device may not have the drivers needed to communicate with that hardware. If so, the update feature of the software can obtain the correct driver from Microsoft and install it on your device. You can switch off this update feature.
- Web Content Features. Features in the software can retrieve related content from Microsoft and provide it to you. Examples of these features are clip art, templates, online training, online assistance, and Appshelp. You may choose not to use these web content features.

Digital Certificates. The software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. They also can be used to digitally sign files and macros, to verify the integrity and origin of the file contents. The software retrieves certificates and updates certificate revocation lists using the Internet, when available.

Auto Root Update. The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.

Windows Media Digital Rights Management. Content owners use Windows Media Digital Rights Management Technology (WMDRM) to protect their intellectual property, including copyrights. This software and third-party software use WMDRM to play and copy WMDRM-protected content. If the software fails to protect the content, content owners may ask Microsoft to revoke the software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

Windows Media Player. When you use Windows Media Player, it checks with Microsoft for:

- compatible online music services in your region;
- new versions of the player; and
- codecs if your device does not have the correct ones for playing content.

You can switch off this last feature. For more information, visit www.microsoft.com/windows/windowsmedia/player/12/privacy.aspx.

Network Awareness. This feature determines whether a system is connected to a network by either passive monitoring of network traffic or active DNS or HTTP queries. The query only transfers standard TCP/IP or DNS information for routing purposes. You can switch off the active query feature through a registry setting.

Windows Time Service. This service synchronizes with time.windows.com once a week to provide your computer with the correct time. You can turn this feature off or choose your preferred time source within the Date and Time Control Panel applet. The connection uses standard NTP protocol.

- IPv6 Network Address Translation (NAT) Traversal service (Teredo). This feature helps existing home Internet gateway devices transition to IPv6. IPv6 is a next-generation Internet protocol. It helps enable end-to-end connectivity often needed by peer-to-peer applications. To do so, each time you start up the software, the Teredo client service will attempt to locate a public Teredo Internet service. It does so by sending a query over the Internet. This query only transfers standard Domain Name Service information to determine if your computer is connected to the Internet and can locate a public Teredo service. If you:

  - use an application that needs IPv6 connectivity, or
  - configure your firewall to always enable IPv6 connectivity

  by default, standard Internet Protocol information will be sent to the Teredo service at Microsoft at regular intervals. No other information is sent to Microsoft. You can change this default to use non-Microsoft servers. You can also switch off this feature using a command line utility named "netsh".

7. **DATA STORAGE TECHNOLOGY.** The server software may include data storage technology called Windows Internal Database. Components of the server software use this technology to store data. You may not otherwise use or access this technology under this agreement.

8. **MICROSOFT .NET BENCHMARK TESTING.** The software includes one or more components of the .NET Framework (".NET Components"). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at go.microsoft.com/fwlink/?LinkID=66406.

9. **SCOPE OF LICENSE.** The software is licensed, not sold. This agreement only gives you some rights to use the software. The manufacturer or installer, and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. For more information, see the software documentation or contact the manufacturer or installer. You may not:

   - work around any technical limitations in the software;
   - reverse engineer, decompile, or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;

- use the software's files and components within another operating system or application running on another operating system;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

Rights to access the software on any device do not give you any right to implement Microsoft patents or other Microsoft intellectual property in software or devices that access that device.

10. **BACKUP COPY.** You may make one backup copy of the software media. You may only restore the backup image to the same server from which the backup was created. You may use it only to create instances of the software.

11. **DOCUMENTATION.** Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

12. **PROOF OF LICENSE.** If you acquired the software on the server, a disc, or other media, your proof of license is the genuine Certificate of Authenticity label that comes with the server. To be valid, this label must be affixed to the server or appear on the manufacturer's or installer's software packaging. If you receive the label separately, it is invalid. You should keep the label on the server or packaging to prove that you are licensed to use the software. To identify genuine Microsoft software, see www.howtotell.com.

13. **TRANSFER TO A THIRD PARTY.** You may transfer the software only with the licensed server, the Certificate of Authenticity label, and this agreement, directly to a third party. Before any permitted transfer, the other party must agree that this agreement applies to the transfer and use of the software. You may not retain any instances of the software unless you also retain another license for the software.

14. **NOTICE ABOUT THE H.264/AVC VIDEO STANDARD AND THE VC-1 VIDEO STANDARD**. This software includes H.264/ AVC and VC-1 visual compression technology. MPEG LA, L.L.C. requires this notice:

    THIS PRODUCT IS LICENSED UNDER THE H.264/AVC AND THE VC-1 VIDEO PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (ii) DECODE H.264/AVC AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.

If you have questions about the Video Standards, further information may be obtained from MPEG LA, LLC; see www.mpegla.com.

15. **EXPORT RESTRICTIONS.** The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users, and end use. For additional information, see www.microsoft.com/exporting.

16. **SUPPORT SERVICES.** Contact the manufacturer or installer for support options. Refer to the support number provided with the software. For updates and supplements obtained directly from Microsoft, Microsoft provides support as described at www.support.microsoft.com/common/international.aspx.

17. **ENTIRE AGREEMENT.** This agreement (including the warranty below), and the terms for supplements, updates, and Internet-based services and support services that you use, are the entire agreement for the software and support services.

18. **APPLICABLE LAW.**

    - **United States.** If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

    - **Outside the United States.** If you acquired the software in any other country, the laws of that country apply.

19. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

20. **SECONDARY BOOT AND RECOVERY COPIES OF THE SOFTWARE**

    - **Secondary Boot Copy.** If a secondary boot copy of the server software is installed on the device, you may access, boot from, display, and run it solely in the event of a failure, malfunction, or corruption of the primary operating copy of the server software, and only until the primary operating copy has been repaired or reinstalled. You are not licensed to boot from and use both the primary operating copy and the secondary boot copy of the server software at the same time.

    - **Recovery Copy**. You may use any recovery copy of the server software provided solely to repair or reinstall the server software on the device.

21. **LEASED HARDWARE**. If you lease the device from the manufacturer or installer, the

following additional terms shall apply: (i) you may not transfer the software to another user as part of the transfer of the device, whether or not a permanent transfer of the software with the device is otherwise allowed in these license terms; (ii) your rights to any software upgrades shall be determined by the lease you signed for the device; and (iii) you may not use the software after your lease terminates, unless you purchase the device from the manufacturer or installer.

22. **NOT FAULT TOLERANT**. **The software is not fault tolerant. The manufacturer or installer installed the software on the device and is responsible for how it operates on the device.**

23. **RESTRICTED USE**. The Microsoft software was designed for systems that do not require fail-safe performance. You may not use the Microsoft software in any device or system in which a malfunction of the software would result in foreseeable risk of injury or death to any person.

24. **LIMITATION ON AND EXCLUSION OF DAMAGES. Except for any refund the manufacturer or installer may provide, you cannot recover any damages, including consequential, lost profits, special, indirect, or incidental damages.**

    This limitation applies to:

    - anything related to the software, services, content (including code) on third-party Internet sites, or third-party programs; and
    - claims for breach of contract, breach of warranty, guarantee, or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if:

    - repair, replacement, or a refund for the software does not fully compensate you for any losses; or
    - the manufacturer or installer, or Microsoft knew or should have known about the possibility of the damages.

    Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. They also may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential, or other damages.

LIMITED WARRANTY

A. LIMITED WARRANTY. If you follow the instructions, the software will perform substantially as described in the Microsoft materials that you receive in or with the software.

References to "limited warranty" are references to the express warranty provided by the manufacturer or installer. This warranty is given in addition to other rights and remedies you may have under law, including your rights and remedies in accordance with the statutory guarantees under local Consumer Law.

B. TERM OF WARRANTY; WARRANTY RECIPIENT; LENGTH OF ANY IMPLIED WARRANTIES. The limited warranty covers the software for 90 days after acquired by the first user. If you receive supplements, updates, or replacement software during those 90 days, they will be covered for the remainder of the warranty or 30 days, whichever is longer. If you transfer the software, the remainder of the warranty will apply to the recipient**.**

To the extent permitted by law, any implied warranties, guarantees, or conditions last only during the term of the limited warranty. Some states do not allow limitations on how long an implied warranty lasts, so these limitations may not apply to you. They also might not apply to you because some countries may not allow limitations on how long an implied warranty, guarantee, or condition lasts.

C. EXCLUSIONS FROM WARRANTY. This warranty does not cover problems caused by your acts (or failures to act), the acts of others, or events beyond the reasonable control of the manufacturer or installer, or Microsoft.

D. REMEDY FOR BREACH OF WARRANTY. The manufacturer or installer will, at its election, either (i) repair or replace the software at no charge, or (ii) accept return of the software together with the server for a refund of the amount paid, if any. The manufacturer or installer may also repair or replace supplements, updates, and replacement software or provide a refund of the amount you paid for them, if any. Contact the manufacturer or installer about its policy. These are your only remedies for breach of the limited warranty.

E. CONSUMER RIGHTS NOT AFFECTED. You may have additional consumer rights under your local laws, which this agreement cannot change.

F. WARRANTY PROCEDURES. Contact the manufacturer or installer to find out how to obtain warranty service for the software. For a refund, you must comply with the manufacturer's or installer's return policies.

G. NO OTHER WARRANTIES. The limited warranty is the only direct warranty from the manufacturer or installer. The manufacturer or installer, and Microsoft give no other

express warranties, guarantees, or conditions. Where allowed by your local laws, the manufacturer or installer, and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose, and non-infringement. If your local laws give you any implied warranties, guarantees, or conditions, despite this exclusion, your remedies are described in the Remedy for Breach of Warranty clause above, to the extent permitted by your local laws.

FOR AUSTRALIA ONLY. References to "Limited Warranty" are references to the warranty provided by the manufacturer or installer. This warranty is given in addition to other rights and remedies you may have under law, including your rights and remedies in accordance with the statutory guarantees under the Australian Consumer Law. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Goods presented for repair may be replaced by refurbished goods of the same type rather than being replaced. Refurbished parts may be used to repair the goods.

For further information regarding this warranty and to claim expenses in relation to the warranty (if applicable), please contact the manufacturer or installer; see the contact information provided in the system packaging.

H. LIMITATION ON AND EXCLUSION OF DAMAGES FOR BREACH OF WARRANTY. The Limitation on and Exclusion of Damages clause above applies to breaches of this limited warranty.

This warranty gives you specific legal rights, and you may also have other rights that vary from state to state. You may also have other rights that vary from country to country.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com
© Bosch Sicherheitssysteme GmbH, 2019