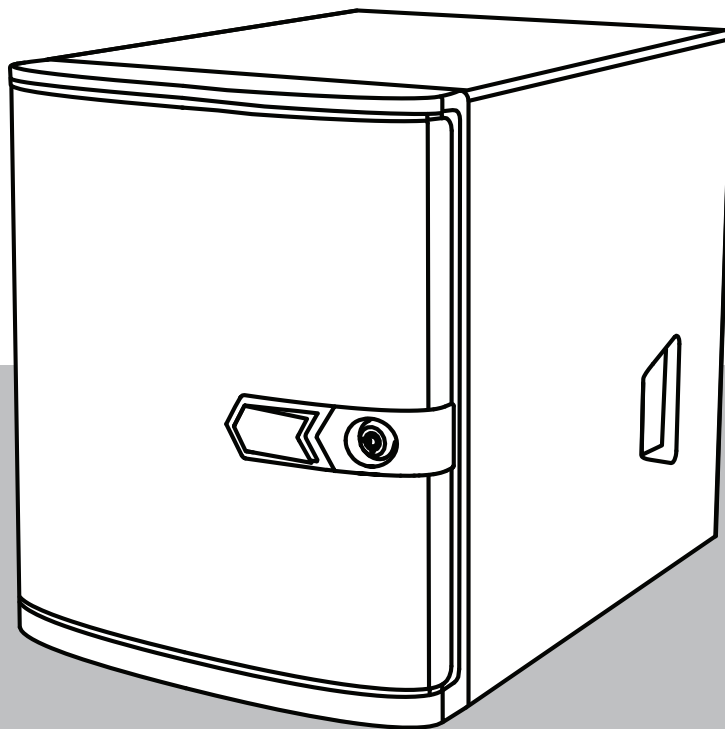




BOSCH

DIVAR IP all-in-one 4000

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



en

User manual

Table of contents

1	Safety	4
1.1	Operating precautions	4
1.2	Cybersecurity precautions	5
1.3	Software precautions	6
1.3.1	Use latest software	6
1.3.2	OSS information	6
2	Introduction	7
3	System overview	8
4	System setup	9
4.1	Default settings	9
4.2	Prerequisites	9
4.3	First sign-in and initial system setup	9
4.3.1	Choosing operation mode BVMS	11
4.3.2	Choosing operation mode VRM	11
4.3.3	Choosing operation mode iSCSI storage	12
5	Upgrading software	13
5.1	Upgrading DIVAR IP System Manager	13
5.2	Upgrading software using DIVAR IP System Manager	13
6	Remote connection to the system	16
6.1	Protecting the system from unauthorized access	16
6.2	Setting up port forwarding	16
6.3	Choosing an appropriate client	16
6.3.1	Remote connection with BVMS Operator Client	16
6.3.2	Remote connection with Video Security App	17
6.4	Connecting to an Enterprise Management Server	17
6.5	Connecting to the Remote Portal	17
6.5.1	Creating a Remote Portal account	17
6.5.2	Registering DIVAR IP all-in-one devices to Remote Portal	18
6.5.3	Unregistering DIVAR IP all-in-one devices from Remote Portal	18
7	Maintenance	19
7.1	Signing in to the administrator account	19
7.2	Monitoring the system	19
7.3	Replacing a faulty hard drive and configuring a new hard drive	19
7.3.1	Replacing a faulty hard drive	20
7.3.2	Configuring a new hard drive	20
7.4	Collecting DIVAR IP System Manager log files	22
7.5	Recovering the unit	22
8	Additional information	24
8.1	Additional documentation and client software	24
8.2	Support services and Bosch Academy	24

1 Safety

Observe the safety precautions in this chapter.

1.1 Operating precautions

**Notice!**

Intended use

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

**Notice!**

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

**Notice!**

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

**Notice!**

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

**Notice!**

Enclosure openings

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

**Notice!**

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

**Notice!**

Do not spill any liquid on the device.

**Warning!**

Use caution when servicing and working around the backplane. Hazardous voltage or energy is present on the backplane when the system is operating. Do not touch the backplane with any metal objects and make sure no ribbon cables touch the backplane.

**Notice!**

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

**Warning!**

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

**Notice!**

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

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

1.2

Cybersecurity precautions

For cybersecurity reasons, observe the following:

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

To minimize cybersecurity risks, observe the following:

 - Make sure that the administrator account is protected with a complex password according to the password policy.
 - Make sure that only limited number of trusted users has access to the administrator account.

- Due to operation requirements, the system drive must not be encrypted. Without encryption, the data stored on this drive can be easily accessed and removed. To avoid data theft or accidental loss of data, make sure that only authorized persons have access to the system and to the administrator account.
- For installation and update of software as well as for system recovery, it might be necessary to use USB devices. Therefore, the USB ports of your system must not be disabled. However, connecting USB devices to the system poses a risk of malware infection. To avoid malware attacks, make sure that no infected USB devices are connected to the system.

1.3 Software precautions

1.3.1 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/>

1.3.2 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

DIVAR IP all-in-one 4000 is an affordable and easy to use all-in-one recording, viewing, and management solution for network surveillance systems of up to 32 channels (with 8 channels pre-licensed).

DIVAR IP all-in-one 4000 is a 2-bay mini tower unit that combines advanced Bosch Video Management System capabilities and state-of-the-art recording management into a single cost-effective, convenient to install and operate IP recording device for IT-minded customers.

DIVAR IP all-in-one 4000 devices utilize embedded design and core components, and are based on the operating system Microsoft Windows Server IoT 2022 for Storage Workgroup.

DIVAR IP all-in-one 4000 devices feature “enterprise-rated” front-swappable SATA hard drives, providing up to 36 TB of gross storage capacity.

3 System overview

Operating system

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

DIVAR IP System Manager

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

Operation modes

DIVAR IP all-in-one 4000 devices can operate in three different modes:

- Full video recording and management system, utilizing the BVMS and Video Recording Manager core components and services.
This mode provides an advanced IP video security solution that delivers seamless management of digital video, audio and data across an IP network. It seamlessly combines IP cameras and encoders, provides system-wide event and alarm management, system health monitoring, user and priority management. This mode provides the best video management system to go with Bosch video surveillance devices, leveraging the unique capabilities of Bosch cameras and recording solutions. It includes Video Streaming Gateway components to integrate third-party cameras.
- Advanced video recording solution for a BVMS system, utilizing the Video Recording Manager core components and services, leveraging the unique capabilities of Bosch cameras and recording solutions. Up to two Video Recording Manager servers can be added to a BVMS system running on a DIVAR IP all-in-one device.
- iSCSI storage expansion for a BVMS system, which runs on a different hardware. Up to two of these iSCSI storage expansions can be added to a BVMS system running on a DIVAR IP all-in-one 4000 device.

When setting up the system, in the DIVAR IP System Manager application, you must choose the desired operation mode to configure your system.

With the DIVAR IP System Manager application you can also upgrade the installed software. You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under:

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



Notice!

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

4 System setup

4.1 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.

4.2 Prerequisites

Observe the following:

- DIVAR IP needs to have an active network link during installation. Make sure that the network switch you are connecting to is powered on.
- The default IP address must not be occupied by any other device in the network. Make sure that the default IP addresses of existing DIVAR IP systems in the network are changed before adding another DIVAR IP.

4.3 First sign-in and initial system setup



Notice!

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



Notice!

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




Notice!

In case of password loss a system recovery must be performed as described in the installation manual. The configuration must be done from scratch or must be imported.

To setup the system:

1. Connect the DIVAR IP all-in-one unit and the cameras to the network.
2. Turn on the unit.
Setup routines for Microsoft Windows Server IoT 2022 for Storage Workgroup are performed. This process can take several minutes. Do not turn off the system.
After the process is completed, the Windows language selection screen is displayed.
3. Select your country/region, the desired operating system language and the keyboard layout from the list, then click **Next**.
The Microsoft software license terms are displayed.

4. Click **Accept** to accept the license terms and wait until Windows restarts. This can take several minutes. Do not turn off the system.
After restart, the Windows sign-in page is displayed.
5. Set a new password for the administrator account **BVRAdmin** and confirm it.
Password requirements:
 - Minimum 14 characters.
 - At least one upper case letter.
 - At least one lower case letter.
 - At least one digit.
 Then press Enter.
The **Software Selection** page is displayed.
6. The system automatically scans the local drive and any connected external storage media for the DIVAR IP System Manager installation file **SystemManager_x64_[software version].exe**, which is located in a folder with the following structure: `Drive root\BoschAppliance\`.
The scan might take some time. Wait for it to complete.
7. Once the system has detected the installation file, it is displayed on the **Software Selection** page. Click the bar that displays the installation file to start the installation.
Notice: Make sure that the latest version of DIVAR IP System Manager is installed. You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under: <https://downloadstore.boschsecurity.com/>.
8. If the installation file is not found during the scan process, proceed as follows:
 - Go to <https://downloadstore.boschsecurity.com/>.
 - Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**.
A list of all available software packages is displayed.
 - Locate the ZIP file **SystemManager_[software version].zip** and save it to a storage medium such as a USB stick.
 - Unzip the file on the storage medium by making sure that the folder **BoschAppliance** is placed in the root of the storage medium.
 - Connect the storage medium to your DIVAR IP all-in-one system.
The system will automatically scan the storage medium for the installation file.
The scan might take some time. Wait for it to complete.
 - Once the installation file is detected, it will be displayed on the **Software Selection** page. Click the bar that displays the installation file to start the installation.
Note: To be automatically detected, the installation file must be located in a folder with the following structure: `Drive root\BoschAppliance\` (for example `F:\BoschAppliance\`).
If the installation file is located at another location that does not match the pre-defined folder structure, click  to navigate to the respective location. Then click the installation file to start the installation.
9. Before the installation starts, the **End User License Agreement (EULA)** dialog box is displayed. Read the license terms, then click **Accept** to continue. The installation starts.
10. After the installation is complete, the system restarts and you are directed to the Windows sign-in page. Sign in to the administrator account.
11. The Microsoft Edge browser opens and the **DIVAR IP - System setup** page is displayed. The page shows the device type and the device serial number, as well as the three operation modes and the available software versions for each operation mode. You must choose the desired operation mode and the desired software version to

configure your DIVAR IP all-in-one system.

Note: If the desired software version for the respective operation mode is not available on a local drive, proceed as follows:

- Go to <https://downloadstore.boschsecurity.com/>.
- Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**. A list of all available software packages is displayed.
- Locate the ZIP files of the desired software packages, for example **BVMS_[BVMS version]_SystemManager_package_[package version].zip**, and save them to a storage medium such as a USB stick.
- Unzip the files on the storage medium. Do not change the folder structure of the unzipped files.
- Connect the storage medium to your DIVAR IP all-in-one system.



Notice!

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

4.3.1

Choosing operation mode BVMS

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

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



Notice!

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

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

4.3.2

Choosing operation mode VRM

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

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

**Notice!**

For further details, refer to the VRM documentation.

4.3.3**Choosing operation mode iSCSI storage**

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

1. On the **DIVAR IP - System setup** page, select the operation mode **iSCSI storage** and the desired iSCSI storage version that you want to install, then click **Next**.
The installation dialog box is displayed.
 2. In the installation dialog box, click **Install** to continue.
The installation starts and the installation dialog box shows the installation progress. Do not turn off the system and do not remove the storage medium during the installation process.
 3. After all software packages have been installed successfully, the system restarts. After restart, you are directed to the Windows sign-in screen.
 4. Add the system as an iSCSI storage expansion to an external BVMS or VRM server using BVMS Configuration Client or Configuration Manager.
-

**Notice!**

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

5 Upgrading software

Make sure that you upgrade DIVAR IP System Manager to the latest version.

5.1 Upgrading DIVAR IP System Manager

1. Go to <https://downloadstore.boschsecurity.com/>.
2. Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**.
A list of all available software packages is displayed.
3. 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.
4. Unzip the file on the storage medium.
5. Connect the storage medium to your DIVAR IP all-in-one device.
6. Start DIVAR IP System Manager:
 - If you are signed in to Windows with the **BVRAdmin** administrator account, double-click the DIVAR IP System Manager icon on the Windows desktop.
DIVAR IP System Manager starts.
 - If your system is running in BVMS operation mode, click the DIVAR IP System Manager icon on the BVMS desktop and sign in to the BVRAdmin administrator account. DIVAR IP System Manager opens in a full screen dialog box (You can exit the dialog box by pressing Alt+ F4).
7. The **Software packages** page is displayed. Select the software package **DIVAR IP System Manager Commander**, and then click **Next** to continue.
The installation dialog box is displayed.
8. In the installation dialog box, click **Install** to continue.
The installation starts and the user interface is being updated. This process may take a few minutes. Do not turn off the system and do not remove the storage medium.
Observe the notifications that are displayed at the top of the page. If reconnecting fails, reload the page.
9. After the installation has been successfully completed, on the **Software packages** page, select the software package **DIVAR IP System Manager Executor**, and then click **Next** to continue.
The installation dialog box is displayed.
10. In the installation dialog box, click **Install** to continue.
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.
Observe the notifications that are displayed at the top of the page.

5.2 Upgrading software using DIVAR IP System Manager

With the DIVAR IP System Manager application you can upgrade the installed software on your system.

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



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




Notice!

Downgrade of the installed software to an earlier version is not supported.

To upgrade the installed software:

1. Go to <https://downloadstore.boschsecurity.com/>.
2. Under the **Software** tab, select **BVMS Appliances** from the list, then click **Select**. A list of all available software packages is displayed.
3. 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.
4. Unzip the files on the storage medium. Do not change the folder structure of the unzipped files.
5. Start DIVAR IP System Manager:
 - If you are signed in to Windows with the **BVRAdmin** administrator account, double-click the DIVAR IP System Manager icon on the Windows desktop. DIVAR IP System Manager starts.
 - If your system is running in BVMS operation mode, click the DIVAR IP System Manager icon on the BVMS desktop and sign in to the BVRAdmin administrator account. DIVAR IP System Manager opens in a full screen dialog box (You can exit the dialog box by pressing Alt+ F4).
6. The **Software packages** page is displayed, showing the device type and the device serial number on the top of the page.
 - In the column **Name**, you see all DIVAR IP System Manager software applications that are already installed on your system as well as all further DIVAR IP System Manager software applications that were detected by the system on the **Images** drive or on a storage medium.
 - In the column **Installed version**, you see the software application version that is currently installed on your system.
 - In the column **Status**, you see the status of the respective software application:
 - The  icon indicates that no later versions of the installed software application were detected by the system on the **Images** drive or on a storage medium.
Note: To make sure that you use the latest software version, double-check the available software versions in the Bosch Security and Safety Systems download store under:
<https://downloadstore.boschsecurity.com/>
 - The  icon indicates that the system has detected later versions of the installed software application on the **Images** drive or on a storage medium. The icon is also displayed if the system has detected a software application that is not yet installed on your system.
 - In the column **Available version**, you see the later versions of the installed software applications. These versions were detected by the system on the **Images** drive or on a storage medium. The column also displays the available versions of the detected software applications that are not yet installed on your system.
Note: Only later versions of the installed software applications are displayed. The downgrade of a software application to an earlier version is not supported.
7. In the column **Name**, click the respective option button to select the software application that you want to upgrade or to install.
8. In the column **Available version**, select the desired version to which you want to upgrade your software application, or which you want to install, and then click **Next**. If applicable, a license agreement dialog box is displayed.

9. 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.
10. After all software packages are installed successfully, you will receive the message **Installation finished successfully.** at the top of the page.
11. If the installation was not successful, you will receive the message **Installation failed.** and the  icon will be displayed. In this case, press F5 to go back to the **Software packages** page. Download the respective software packages again and retry. If the issue persists, contact technical support.

6 Remote connection to the system

You can make a remote connection to your DIVAR IP all-in-one system and access it from the internet.

To create a remote connection, you must do the following:

1. *Protecting the system from unauthorized access, page 16.*
2. *Setting up port forwarding, page 16.*
3. *Choosing an appropriate client, page 16.*

You can also connect to your DIVAR IP all-in-one via Bosch Remote Portal and utilize current and future functionality available via Remote Portal. For more information, refer to Connecting to the Remote Portal.

6.1 Protecting the system from unauthorized access

To protect the system from unauthorized access, make sure to follow strong password rules before you connect the system to the internet. The stronger your password, the more protected your system will be from unauthorized persons and malware.

6.2 Setting up port forwarding

To access a DIVAR IP all-in-one system from the internet through a NAT/PAT capable router, you must configure port forwarding on your DIVAR IP all-in-one system and on the router.

To set up port forwarding:

- ▶ Enter following port rules in the port forwarding settings of your internet router:
 - port 5322 for SSH tunnel access using BVMS Operator Client.
Note: This connection is only applicable for BVMS operation mode.
 - port 443 for HTTPS access to VRM using Video Security Client or Video Security App.
Note: This connection is only applicable for BVMS or VRM operation mode.

Your DIVAR IP all-in-one is now accessible from the Internet.

6.3 Choosing an appropriate client

There are two options to make a remote connection to your DIVAR IP all-in-one system:

- *Remote connection with BVMS Operator Client, page 16.*
- *Remote connection with Video Security App, page 17.*



Notice!

The compatibility of the versions of BVMS Operator Client or Video Security App is determined by the versions of the BVMS or VRM software installed in DIVAR IP. For detailed information refer to the respective software documentation and training material.

6.3.1 Remote connection with BVMS Operator Client



Notice!

This connection is only applicable for BVMS operation mode.

To make a remote connection with BVMS Operator Client:

1. Install BVMS Operator Client on the client workstation.
2. After finishing the installation successfully, start Operator Client using the desktop

shortcut .

3. Enter the following, then click **OK**.
User name: admin (or other user in case one is configured)
Password: user password
Connection: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Remote connection with Video Security App

**Notice!**

This connection is only applicable for BVMS or VRM operation mode.

To make a remote connection with Video Security App:

1. In Apple's App Store search for Bosch Video Security.
2. Install the Video Security app on your iOS device.
3. Start the Video Security app.
4. Select **Add**.
5. Enter the public IP address or dynDNS name.
6. Make sure Secure Connection (SSL) is switched on.
7. Select **Add**.
8. Enter the following:
User name: admin (or other user in case one is configured)
Password: user password

6.4 Connecting to an Enterprise Management Server

For a central management of multiple DIVAR IP all-in-one systems in BVMS operation mode, you can use a BVMS Enterprise Management Server installed on a separate server.

For detailed information about BVMS Enterprise System configuration and operation, refer to the BVMS documentation and training material.

6.5 Connecting to the Remote Portal

Prerequisites**Remote Portal connection**

To connect DIVAR IP all-in-one devices to the Remote Portal make sure that the following prerequisites apply:

- DIVAR IP System Manager 2.0 (or higher) must be installed on the device.
- A Remote Portal account must be created.

Remote Portal communication

Connectivity requirements for the Remote Portal communication.

Notice: All connections are outgoing.

HTTPS (Port 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTs (Port 8883)

- [mqtt://mqtt.bosch-iot-hub.com:8883](https://mqtt.bosch-iot-hub.com:8883)

6.5.1 Creating a Remote Portal account

To create a Remote Portal account:

1. Go to <https://remote.boschsecurity.com/login>.
2. Click **Sign up**.

3. Enter your company name and your email.
4. Select your company region.
5. Read the terms and conditions and the data protection notice, and then select the checkboxes to accept them.
6. Click **Sign up** to create an account.

6.5.2 Registering DIVAR IP all-in-one devices to Remote Portal

To register a DIVAR IP all-in-one device to Remote Portal:

1. Start DIVAR IP System Manager.
2. Click the **Remote Portal connection** tab.
3. If you have an existing Remote Portal account, enter your email and password, and then click **Register** to register your DIVAR IP all-in-one device to Remote Portal.

Notice!



SingleKey ID

Bosch has introduced SingleKey ID as an identity provider (IdP) to allow a central sign-in to all Bosch applications, services and platforms.

To connect the device to Remote Portal by using SingleKey ID, follow the instructions on the screen.

Notice!

Default commissioning company setting



If your email is assigned to multiple company accounts, make sure that you register your DIVAR IP all-in-one device to the correct company account.

- Sign in to your Remote Portal account.

- Go to **User settings > My companies**, select the desired account, and then select the option

Default commissioning company.

Note: The **Default commissioning company** setting automatically expires after 12 hours.

-
4. If you do not have a Remote Portal account yet, click **Create account** to create a Remote Portal account first. Refer to Creating a Remote Portal account.

6.5.3 Unregistering DIVAR IP all-in-one devices from Remote Portal

To unregister a DIVAR IP all-in-one device from Remote Portal:

1. Start DIVAR IP System Manager.
2. Click the **Remote Portal connection** tab.
3. Click **Unregister** to unregister your DIVAR IP all-in-one device from Remote Portal.

Note: Unregistering the device from Remote Portal does not delete the device configuration in Remote Portal. To delete the device configuration, sign in to the corresponding Remote Portal company account.

7 Maintenance

7.1 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.

7.2 Monitoring the system

The DIVAR IP all-in-one systems come with the pre-installed application **SuperDoctor**, which you can use to monitor your system.

Activating the monitoring functionality

To activate the monitoring functionality:

1. Sign in to the administrator account (refer to *Signing in to the administrator account, page 19*).
2. On the desktop, in the **Tools** folder, right-click the **startSD5Service** script, and then click **Run with PowerShell**.
3. Double-click the **SuperDoctor 5 Web** icon on the desktop.
4. Sign in to the web interface using the following default credentials:
 - User name: **admin**
 - Password: **DivaripSD5**
5. Click the **Configuration** tab, and then click **Account Setting** and change the default password.

Note: Bosch strongly recommends to change the default password immediately after the first sign-in to the **SuperDoctor** application.
6. Under the **Configuration** tab, click **Alert Configuration**.
7. Activate the **SNMP Trap** feature and specify the IP address of the receiver for SNMP traps.

Deactivating the monitoring functionality

To deactivate the monitoring functionality:

1. Sign in to the administrator account (refer to *Signing in to the administrator account, page 19*).
2. On the desktop, in the **Tools** folder, right-click the **stopSD5Service** script, and then click **Run with PowerShell**.

7.3 Replacing a faulty hard drive and configuring a new hard drive

If a hard drive that is installed on your DIVAR IP all-in-one system is faulty and cannot be used any longer, you must do the following steps:

1. *Replacing a faulty hard drive, page 20.*
2. *Configuring a new hard drive, page 20.*

**Notice!**

Bosch is not liable for any data loss, damages, or system failures of units equipped with hard drives that are not supplied by Bosch. Bosch cannot provide support if non-Bosch-supplied hard drives are considered to be the cause of the problem. To troubleshoot potential hardware issues, Bosch will require Bosch-supplied hard drives to be installed.

7.3.1**Replacing a faulty hard drive**

To replace a faulty hard drive:

1. Turn off the DIVAR IP all-in-one unit.
2. Remove the faulty hard drive from the unit and install the new hard drive.
Refer to chapter *Installing a SATA hard drive* in the Installation manual.

7.3.2**Configuring a new hard drive**

To configure a new hard drive, you must do the following:

1. *Creating new partition and volume, page 20*
2. *Enabling the Server service, page 21.*
3. *Creating LUNs (iSCSI virtual disks), page 21.*
4. *Disabling the Server service, page 21.*
5. *Formatting LUNs, page 22.*

Creating new partition and volume

To create new partition and volume:

1. On the Windows **Start** menu, select **Server Manager**, and then select **File and Storage Services > Volumes > Disks**.
All disk drives that are installed on your system are displayed.
2. Right-click the new disk drive that you installed, and then click **New Volume...**
The **New Volume Wizard** dialog box is displayed.
3. Click **Next** to continue.
The **Server and Disk** dialog box is displayed.
4. Select the respective server and disk and click **Next** to continue.
The **Size** dialog box is displayed.
5. In the **Volume size:** field, enter the desired volume size that you want to use. If you want to use the maximum volume size, leave the pre-selected value unchanged. Then click **Next** to continue.
The **Drive Letter or Folder** dialog box is displayed.
6. In the **Drive letter:** list, select the drive letter that should be assigned to the volume, and then click **Next** to continue.
The **File System Settings** dialog box is displayed.
7. Apply the following:
 - **File system:** NTFS
 - **Allocation unit size:** Default
 - **Volume label:** enter the same volume label as the one of the replaced faulty disk (**Data** or **Data2**).
8. Click **Next** to continue.
The **Confirmation** dialog box is displayed.
9. Check if all settings are correct, and then click **Create**.
The system starts the creation of the new partition and volume.
After the creation is completed, the **Results** dialog box is displayed.
10. Click **Next** to continue.
The new partition and volume are created successfully and all storage space is allocated.

Enabling the Server service

1. On the Windows **Start** menu, select **Services**.
The **Services** dialog box is displayed.
2. Locate the **Server** service in the list and double-click it.
The **Server Properties** dialog box is displayed.
3. Under the tab **General**, in the **Startup type:** list, select **Manual**, and then click **Apply**.
4. Under **Service status:**, click **Start** to start the service, and then click **OK** to apply the changes. Then close the **Services** dialog box.

Creating LUNs (iSCSI virtual disks)

1. On the Windows **Start** menu, select **Server Manager**, and then select **File and Storage Services > iSCSI**.
All iSCSI virtual disks on your system are displayed.
2. Right-click the LUN (the iSCSI virtual disk) of the replaced hard drive, which has the status **Error**, and then click **Remove iSCSI Virtual Disk**.
The **Remove iSCSI Virtual Disk** dialog box is displayed.
3. Click **OK** to confirm the removal of the LUN.
4. Repeat these steps for all LUNs that have the status **Error**.
5. In the **iSCSI VIRTUAL DISKS** dialog box, right-click on a blank space, and then click **New iSCSI Virtual Disk...**
The **iSCSI Virtual Disk Location** dialog box is displayed.
6. Under **Server**, select the respective server, under **Storage location:**, select **Type a custom path** and enter the letter that you assigned to the new hard drive (refer to *Creating new partition and volume, page 20*). Then click **Next** to continue.
The **iSCSI Virtual Disk Name** dialog box is displayed.
7. In the **Name:** field, enter the name of the LUN. Then click **Next** to continue.
The **iSCSI Virtual Disk Size** dialog box is displayed.
8. In the **Size** field, enter 2000 and change the size unit to **GB**.
If less than 2000 GB are available, configure the size of the LUN to the available GB space minus 50 MB.
9. Under **Fixed size:**, clear the checkbox **Clear the virtual disk on allocation**. Then click **Next** to continue.
The **iSCSI Target** dialog box is displayed.
10. Under **Existing iSCSI target:**, select **TG0**. Then click **Next** to continue.
The **Confirmation** dialog box is displayed.
11. Check if all settings are correct, and then click **Create**.
The system starts the creation of the new iSCSI virtual disk.
After the creation is completed, the **Results** dialog box is displayed.
12. Click **Close** to close the dialog box.
13. Repeat these steps to create further LUNs using all available space.
14. After creating all LUNs, they will be listed in the **iSCSI VIRTUAL DISKS** list.

Disabling the Server service

1. On the Windows **Start** menu, select **Services**.
The **Services** dialog box is displayed.
2. Locate the **Server** service in the list and double-click it.
The **Server Properties** dialog box is displayed.
3. Under the tab **General**, under **Service status:**, click **Stop** to stop the service.

4. In the **Startup type:** list, select **Disabled**, and then click **Apply**.
5. Click **OK** to apply the changes, and then close the **Services** dialog box.

Formatting LUNs

1. Start BVMS Configuration Client.
2. In the **Device Tree**, navigate to the pool that includes the faulty hard drive, right-click the **TGO** iSCSI target, and then click **Scan Target** to update the list of LUNs that are available on this iSCSI target.
This will remove the LUNs associated with the faulty hard drive and add the LUNs created on the new hard drive.
3. The **LUNs** dialog box lists all available LUNs and shows their state (formatted or unformatted).
4. Select the unformatted LUNs and click **Format LUN**. Then click **OK** to continue.
5. After the formatting is finished, a confirmation dialog box is displayed. Click **OK** to finalize the process.

7.4 Collecting DIVAR IP System Manager log files

The DIVAR IP System Manager application includes a dedicated script that simplifies the log file collection.

To collect DIVAR IP System Manager log files:

1. Sign in to the administrator account (refer to *Signing in to the administrator account, page 19*).
2. On the Windows **Start** menu, click **Export System Manager Logs**.
The script exports the log files to the folder `Documents\Bosch` and creates a ZIP file with following name structure `SysMgrLogs-[date]_[time]`.
You can use this ZIP file to attach it to the detailed error description.

7.5 Recovering the unit

To recover the unit:

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

Note:

The **OS system recovery only** option does not delete video footage that is stored on the data HDDs. However, it replaces the complete operating system partition (including the

video management system settings) with a default configuration. To access existing video footage after recovery, the video management system configuration needs to be exported before the system recovery and re-imported afterwards.

**Notice!**

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

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

Refer to

- *First sign-in and initial system setup, page 9*

8 Additional information

8.1 Additional documentation and client software

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

<http://www.boschsecurity.com>

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

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

8.2 Support services and Bosch Academy



Support

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



Bosch Building Technologies Academy

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

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2023

Building solutions for a better life.

202309021034