Table of contents

1 Safety

Observe the safety precautions in this chapter.

1.1 Operating precautions

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

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

Notice!
Video loss is inherent to digital video recording; therefore, Bosch Security Systems cannot be held liable for any damage that results from missing video information.
To minimize the risk of losing information, we recommend multiple, redundant recording systems, and a procedure to back up all analog and digital information.

1.2 Data security precautions

For data security reasons observe the following:

- Physical access to the system shall be restricted to authorized personnel only. It is strongly suggested to place the system in an access control protected area, in order to avoid physical manipulation of the system.
- Windows online update functionality or the corresponding monthly roll-up patches for offline installation can be used to install OS security updates.
- Limiting local network access to trusted devices is strongly suggested. Details are described in the Technical note Network Authentication 802.1X and in the Bosch IP Video and Data Security Guidebook, available in the online product catalog.
- For access via public networks only use the secure (encrypted) communication channels.

2 Introduction

Operating modes

The DIVAR IP all-in-one systems can operate in three different modes:

– Full video recording and management system, utilizing the BVMS and VRM core components and services: This mode allows for advanced video management features such as event and alarm handling.
– Pure video recording system, utilizing the VRM core components and services.
– iSCSI storage expansion for a BVMS or VRM system, which runs on a different hardware.

Notice!

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

DIVAR IP Software Center

DIVAR IP Software Center is the central user interface for software setup, upgrade and operation mode selection.

After installation of DIVAR IP Software Center you must choose the desired operation mode to configure your system.

With DIVAR IP Software Center you can also update and upgrade the installed software.

You can find the latest software and available upgrade packages in the **Download Area** of Bosch Security and Safety Systems under:

https://downloadstore.boschsecurity.com/

3 System overview

The DIVAR IP all-in-one 7000 systems are based on the operating system Microsoft Windows Server IoT 2019 for Storage Standard. The operating system provides an user interface for initial server configuration, unified storage appliance management, simplified setup and storage management, and support for Microsoft iSCSI Software Target.
It is specially tuned to provide optimal performance for network-attached storage. The Microsoft Windows Server IoT 2019 for Storage Standard operating system provides significant enhancements in storage management scenarios, as well as integration of storage appliance management components and functionality.

Notice!
This chapter is valid for DIVAR IP all-in-one 7000 models that come with pre-installed hard drives.
The operating system of empty units loaded with third party hard drives will start normally, but the added hard drives must be configured with the RAID utility prior to initial software setup.
For further details, refer to the Installation manual.

DIVAR IP systems are shipped with a pre-installed Configuration Wizard from factory.
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: BVRAdmin
- Password: to be set at first logon.

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 First logon and system setup

Notice!
We strongly recommend not changing any operating system settings. Changing operating system settings can result in malfunctioning of the system.

Notice!
To perform administrative tasks, you have to log on 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.

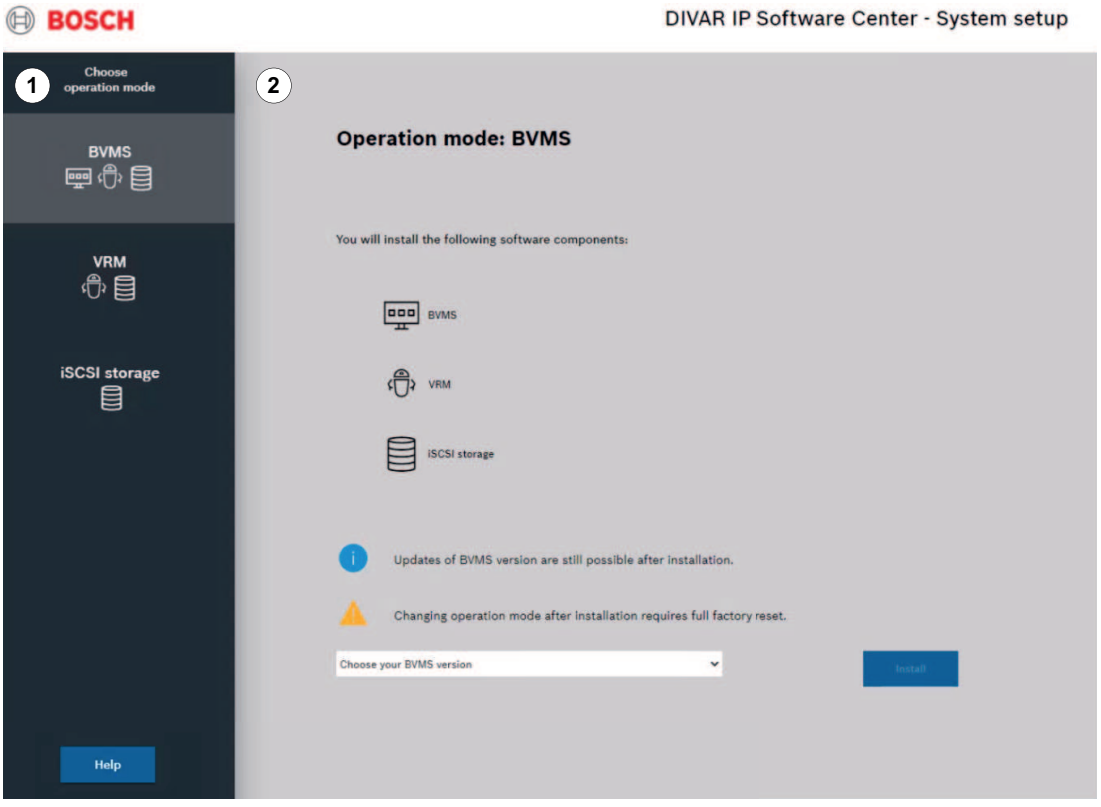
To setup the system:

1. Connect the DIVAR IP all-in-one 7000 unit and the cameras to the network.
2. Turn on the unit.
   Setup routines for Microsoft Windows Server IoT 2019 for Storage Standard are performed. This 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 and the EULA (End User License Agreement) 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 the restart, the Windows logon page is displayed.
5. Set a new password for the administrator account **BVRAdmin** and confirm it (Note: The minimum password length is 14 characters). Then press ENTER**.**
   The **Software Selection** page is displayed.
6. Click the DIVAR IP Software Center installation file.
   The DIVAR IP Software Center installation starts. After the installation is completed, Windows restarts and you are directed to the Windows logon page.
   Note: If you do not have the DIVAR IP Software Center installation file stored on a local drive, insert a storage media (USB flash drive, DVD-ROM) with the installation file.
   The storage media is automatically scanned for the DIVAR IP Software Center installation file and the installation file is displayed on the **Software Selection** page.
7. Log on to the administrator account.
   The Microsoft Edge browser starts automatically.
8. Enter the admin user name and password and click **Sign in**.
   DIVAR IP Software Center starts and the software packages are loaded.
   Note: If the respective software packages for the desired operation mode are not available on a local drive, insert a storage media with the software packages to proceed with the system setup.
   You can find the latest software and available upgrade packages in the **Download Area** of Bosch Security and Safety Systems under:
   https://downloadstore.boschsecurity.com/

4.1 Choosing operation mode

In the DIVAR IP Software Center application you must choose the desired operation mode to configure your DIVAR IP all-in-one 7000 system.

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



1	Selection window
2	Main window

Refer to
– *Operating modes, page 5*

4.1.1 Operating as full video recording and management system

To operate the DIVAR IP system as full video recording and management system:

1. In the selection window, click **BVMS**.
   The software components, which will be installed, are displayed in the main window.
2. Select the desired BVMS version from the list, then click **Install**.
   The **BVMS installation** dialog box is displayed showing the software packages, which will be installed.
3. Click **Install** to continue.
   The installation of the software packages starts. This can take several minutes. Do not turn off the system and do not remove the storage media.
   Note: If an error occurs during installation, click **Finish**. This restarts the system. After restart, update the respective software packages and proceed with setup.

4. After all packages have been installed successfully, click **Finish**.
   The system restarts. After restart, you are directed to the BVMS desktop.
5. On the BVMS desktop, click the desired application to configure your system.

Notice!
For further details, refer to the BVMS documentation.

4.1.2 Operating as pure video recording system

To operate the DIVAR IP system as pure video recording system:

1. In the selection window, click **VRM**.
   The software components, which will be installed, are displayed in the main window.
2. Select the desired VRM version from the list, then click **Install**.
   The **VRM installation** dialog box is displayed showing the software packages, which will be installed.
3. Click **Install** to continue.
   The installation of the software packages starts. This can take several minutes. Do not turn off the system and do not remove the storage media.
   Note: If an error occurs during installation, click **Finish**. This restarts the system. After restart, update the respective software packages and proceed with setup.
4. After all packages have been installed successfully, click **Finish**.
   The system restarts. After restart, you are directed to the Windows logon screen.

Notice!
For further details, refer to the VRM documentation.

4.1.3 Operating as iSCSI storage expansion

To operate the DIVAR IP system as an iSCSI storage expansion:

1. In the selection window, click **iSCSI storage**.
   The software components, which will be installed, are displayed in the main window.
2. Select the desired components from the list, then click **Install**.
   The **iSCSI storage installation** dialog box is displayed showing the software packages, which will be installed.
3. Click **Install** to continue.
   The installation of the software packages starts. This can take several minutes. Do not turn off the system and do not remove the storage media.
   Note: If an error occurs during installation, click **Finish**. This restarts the system. After restart, update the respective software packages and proceed with setup.
4. After all packages have been installed successfully, click **Finish**.
   The system restarts. After restart, you are directed to the Windows logon screen.
5. 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 and updating software

With DIVAR IP Software Center you can update and upgrade the installed software.
You can find the latest software and available upgrade packages in the **Download Area** of Bosch Security and Safety Systems under:
https://downloadstore.boschsecurity.com/

Upgrading software

To upgrade the installed software:

1. Download the desired software packages from the **Download area** and save them either on a local drive or on a storage media. Then connect the storage media to your system.
2. Start DIVAR IP Software Center.
   The **Installed software** page is displayed.
3. In the **Upgrades** section, the available upgrades are displayed. Click **Upgrade** to upgrade the desired software.
   The **Upgrade** dialog box is displayed showing the software packages included in the upgrade.
   Note: The upgrade will save all your settings, update the software and restart the system.
4. Click **Install** to continue.
   The installation of the software packages starts. This can take several minutes. Do not turn off the system and do not remove the storage media.
   After the installation is completed, the system restarts.

Updating software

To update the installed software:

1. Download the desired software packages from the **Download area** and save them either on a local drive or on a storage media. Then connect the storage media to your system.
2. Start DIVAR IP Software Center.
   The **Installed software** page is displayed.
3. In the **Updates** section, the available updates are displayed. Click **Update all** to update all software packages to the new version.
   The **Update** dialog box is displayed showing the software packages, which will be updated.
   Note: The update will save all your settings, update the software and restart the system.
4. Click **Install** to continue.
   The installation of the software packages starts. This can take several minutes. Do not turn off the system and do not remove the storage media.
   After the installation is completed, the system restarts.

6 Remote connection to the system

This section describes the steps that are required to access the DIVAR IP system from the internet.

6.1 Protecting the system from unauthorized access

In order to protect the system from unauthorized access, we recommend that you follow strong password rules before connecting 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

In order to access a DIVAR IP system from the internet through a NAT/PAT capable router, port forwarding must be configured on the DIVAR IP 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.
- port 443 for HTTPS access to VRM using Video Security Client or Video Security App.

The DIVAR IP system is now accessible from the Internet.

6.3 Choosing an appropriate client

This chapter describes the ways that allow remote connection to a DIVAR IP system through the internet.

There are 2 ways to make a remote connection:

- *Remote connection with Operator Client, page 11*.
- *Remote connection with Video Security App, page 11*.

Notice!
Only use BVMS Operator Client or Video Security App in the version that matches DIVAR IP. Other clients or application software may work but are not supported.

6.3.1 Remote connection with Operator Client

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: enter user password
   Connection: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Remote connection with Video Security App

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: enter user password

6.4 Installing an Enterprise Management Server

For a central management of multiple systems you can install Bosch VMS Enterprise Management Server on a separate server.

To install Bosch VMS Enterprise Management Server on a separate server:

1. Download the BVMS installer from the product page.
2. Copy the BVMS installer to the server that should act as an Enterprise Management Server.
3. Double-click the installer program, then accept the security message.
4. In the **Welcome** dialog box, clear all check boxes except **Enterprise Management Server** and **Configuration Client**.
5. Follow the installation instructions.
6. After finishing the installer successfully, start Configuration Client using the desktop shortcut.

Notice!
For Enterprise Management Server configuration refer to the BVMS documentation.

7 Maintenance

7.1 Monitoring the system

The system provides tools for health monitoring.
To activate the monitoring functionality, you have to logon to the administrator account (BVRAdmin).

1. On the system screen (depending on the chosen operation mode, it is either the BVMS desktop or the Windows logon screen), press CTRL+ALT+DEL.
2. Hold SHIFT, click **Switch User** and keep SHIFT pressed for about five seconds.
3. Enter user name and password.
4. On the desktop, in the **Tools** folder, right-click the **Enable_SuperDoctor_5_Service** script, and then click **Run as administrator**.
5. Double-click the **SuperDoctor 5 Web** icon in the same folder.
6. Log on to the web interface using the following default credentials:
   User name: admin
   Password: DivaripSD5
7. Click the **Configuration** tab, and then click **Password Settings** and change the default password.
8. Click the **Configuration** tab, and then click **Alert Configuration**.
9. Activate the **SNMP Trap** feature and specify the IP address of the receiver for SNMP traps.

7.2 Recovering the unit

Following procedure describes how to restore the factory default image.

To restore the unit to factory default image:

1. Start the unit and press **F7** during the BIOS power-on-self-test.
   The Recovery menu is displayed.
2. Select one of the following:
   - **Initial factory setup:** restores to factory default image and deletes all data on the HDDs.
     or
   - **System Recovery (back to Factory Defaults):** restores to factory default image; data on the HDDs will not be deleted.

   Note:
   While the **System Recovery** option doesn't delete video footage stored on the data HDDs, it still replaces the complete OS partition (including VMS settings) with a default configuration. In order to access existing video footage after recovery, the VMS configuration needs to be exported before System Recovery and re-imported afterwards.

Notice!
Do not turn off the unit during the process. This will damage the Recovery media.

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

8 Additional information

8.1 Additional documentation and client software

For more information, software downloads, and documentation, visit http://www.boschsecurity.com and go to the respective product page in the product catalog.
You can find the latest software and available upgrade packages in the **Download Area** of Bosch Security and Safety Systems 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 Security and Safety Systems offers support in these areas:

- Apps & Tools
- Building Information Modeling
- Commissioning
- Warranty
- Troubleshooting
- Repair & Exchange
- Product Security

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

202010151745