BOSCH
Invented for life

Release Notes
DIVAR IP all-in-one 4000 (DIP-44xx)

Date: 26-Mar-2024

Table of Contents

1 Document History

Date	Version	Changes
20.01.2023	1.0	Initial Release
05.03.2024	1.1	Added issue 413074 and its fix
26.03.2024	1.2	Time Zone change issue for MS Windows Server IoT 2022 for Storage explained

2 DIVAR IP all-in-one 4000, production package DIP-44xxAIO_v01.00.01

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 System Manager application provides a central user interface for operation mode selection and for software setup and upgrades on the DIVAR IP all-in-one 4000.

2.1 Sub-component software versions

- OS: Microsoft Server IoT 2022 Storage Workgroup
- BIOS/UEFI: 2.1 V3 - Bosch specific
- OS Image: 1.0.4.001 (including SuperDoctor 5.14.0.1039)
- DIVAR IP System Manager: 1.5.0.6124
- System Manager Package: BVMS_11.1.1_SystemManager_package_1.0

2.2 Installation and operation notes

- For details on installation and operation procedures refer to the DIVAR IP all-in-one 4000 Installation and User manuals, and DIVAR IP System Manager Release notes.
- The operating system includes the latest Windows security patches available at the time the software image was created. Use the Windows update functionality or the corresponding monthly roll-up patches for offline installation to regularly install OS security updates.
- 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. You can find the latest software and available upgrade packages in the Bosch Security and Safety Systems download store under https://downloadstore.boschsecurity.com/
- For installation and update of software it might be necessary to use USB devices. To avoid malware attacks, make sure that no infected USB devices are connected to the system.
- Remote access to the system is possible via defined ports (e.g. with Bosch Video Security Client / App.), as described in the product documentation. Apart from this, Bosch strongly recommends to run the DIVAR IP all-in-one in a perimeterized network, and operated by trusted personnel only.
- Even though Bosch is selling DIVAR IP based on standard IT Hardware, BIOS, UEFI, firmware and software versions installed on these systems are Bosch specific. Upgrading or updating the systems with non-Bosch certified and approved versions is strictly not recommended as it might impact proper system functionality and the Service & Support coverage, which then can be provided by Bosch in case of technical issues. BIOS, UEFI, firmware and software versions of included system components shall only be upgraded with non-Bosch BIOS, UEFI, firmware and software versions if suggested and approved by Bosch. Support can only be provided on the latest approved versions.
- To prevent local manipulation on the system, it is advised to define a secure BIOS password.
- 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. HDDs listed below are or have been used in populated models (subject to change):

Size	System manufacturer PN	Description	Original manufacturer PN
4TB	HDD-T4000-ST4000NM024B	Seagate3.5"4TB,SATA6Gb/s.7.2KRPM,512e/ 4Kn	ST4000NM024B
8TB	HDD-T8000-ST8000NM017B	Seagate3.5"8TB,SATA6Gb/s,7.2KRPM,512e/ 4Kn	ST8000NM017B
18TB	HDD-T18T-ST18000NM000J	Seagate3.5",18TB,7.2kRPM,SATA3 6Gb/s,512e/ 4Kn	ST18000NM000J

- Recording bandwidth limits listed in the data sheet were measured with additional playback load at the level of 20% of recording bandwidth. Proper system operation can only be ensured, if playback load doesn’t exceed 20% of the defined maximum recording bandwidth.
- The "System factory default" recovery option only initiates a quick format of the hard drives. For secure disposal of sensitive data the hard drives need to be physically destroyed or overwritten with randomized data ("Full data overwrite and system factory default" recovery option).

2.3 Fixed issues

N/A - initial release.

2.4 Known limitations and issues

- DIVAR IP needs to have an active network link during installation. Make sure that the network switch you are connecting to is powered on and fully booted up.
- 395014 System Manager HTTPS Certificate may become invalid after changing timezone to the past shortly after its installation. Please define desired location/timezone at OS installation.
- BVMS Mobile Video Service (MVS) is not and shall not be installed locally, and is not required. The local MVS may be anyhow displayed in the BVMS system configuration, but can be manually removed from the BVMS configuration. The Video Security Client software, for example, can login to the system without requiring the MVS service.
- iSCSI CHAP shall be configured on the storage target, to prevent unauthorized access.
- Changes of the host IP address in the BVMS configuration client may not be transferred into the device certificate
- When attempting to perform dewarping via the transcoder, only circular view will be shown.
- Microsoft Remote Desktop functionality may be used for configuration or occasional monitoring of the system but shall not stay connected permanently.
- The system was not tested in domain joined configuration. Changes of Windows policies, imposed by domain, may affect system operation and security, and are not in Bosch control and responsibility.
- 413074 In rare cases of specific high-security network configurations, the device may experince extremely high CPU load due to ActiveProbing behavior of Windows Server 2022, which will eventually lead to failure to install operation mode of the device. To fix the issue, run Windows Update and install the 2024-02-Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems (KB5034770) (February 2024 Cumulative Update) or newer.

- Installation of the BVMS 12.1.0 System Manager package 1.0 (and higher BVMS versions) enables Windows User Account Control (UAC) feature to improve data security of the DIVAR IP all-in-one portfolio. However, enabling this feature in MS Windows Server IoT 2022 for Storage (used in DIVAR IP all-in-one 4000) disables the Time Zone selection in the Date&Time Settings Windows dialogue. To change the Time Zone, please open the Server Manager application, go to main Dashboard > Local Server on the left panel, then select the time zone on the right side. If the DIVAR IP is installed in BVMS operation mode, Time Zone can be also changed from the BVMS Wizard application.