Release Notes
DIVAR IP all-in-one 7000 Gen 4 (DIP-74xx)

Date: 18-Jun-2024

Table of Contents

1 Document History

Date	Version	Changes
18.06.2024	1.0	Initial Release

2 DIVAR IP all-in-one 7000 Gen 4, production package DIP-74xxAIO_v01.00.01

DIVAR IP all-in-one 7000 Gen 4 is an affordable and easy to use all-in-one recording, viewing, and management solution for network surveillance systems of up to 256 channels (with 8 channels pre-licensed). DIVAR IP all-in-one 7000 Gen 4 comes as 2U or 3U rack mount units that combine advanced Bosch Video Management System capabilities and state-of-the-art recording management into a single cost-effective, convenient to install and operate 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 7000 Gen 4.

2.1 Sub-component software versions

- OS: Microsoft Server IoT 2022 Storage Standard
- BIOS/UEFI: 5.0.1 - Bosch specific
- RAID FW: 5.250.02-3847
- BMC FW: 1.1.6 - Bosch specific
- OS Image: 1.1.30.0410 (including Inband Tool 1.19.01)
- DIVAR IP System Manager: 2.3.0
- System Manager Package: BVMS_12.1.0_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 7000 Gen 4 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.
- In case of initial DIVAR IP System Manager installation from a USB device, the installation file will first be copied from USB. It will take few minutes and during this time the EULA is still displayed.
- The BMC port shall not be connected to a public network permanently. The systems are shipped with a sticker showing the dedicated BMC password. The sticker shall be either stored at a secure location or password shall be changed.
- 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.

- The systems are shipped with a sticker showing the dedicated BIOS password. The sticker shall be either stored at a secure location or password shall be changed.
- 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	Bosch CTN	Original manufacturer description	Original manufacturer PN
4TB	DIP-AIO-4HDD-T	Toshiba 3.5" SATA 6G/S HDD 4TB 7200RPM	MG08ADA400E
8TB	DIP-AIO-8HDD-T	Toshiba 3.5" SATA 6G/S HDD 8TB 7200RPM	MG08ADA800E
18TB	DIP-AIO-18HDD-T	Toshiba 3.5" SATA 6G/S HDD 18TB 7200RPM	MG09ACA18TE

- 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. Recording bandwidth was tested with min. 8 drives installed in the unit. It is not recommended to use lower number of drives, as it will affect recording performance.
- 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).
- If the unit is configured in BVMS Operation Mode and BVMS 12.1 is installed, it is strongly recommended to install BVMS 12.1 Cumulative patch 3, available on E-drive, or higher version Cumulative patch.

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.
- BMC network interface is visible from Windows operating system. This does not affect operation of the system, however, it shall not be re-configured from its default configuration.
- BMC graphics adapter device is visible from Windows operating system and is disabled in Windows in case a local HDMI monitor is connected to the system. It shall not be manually re-enabled in Windows in this use-case.
- 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.
- The Inband Tool version 1.19.01, provided in the factory OS image, does not support an API to provide system health information to Bosch Remote Portal, as well as does not support sending SNMP traps. In order to utilize these functionalities, the Inband Tool application should be updated to later versions.