Table of contents

1 Introduction

This training focuses on essential troubleshooting topics for the DIVAR IP all-in-one 7000 4th generation (DIP-74xx). We deliberately concentrate on this device to maintain a manageable scope. In some instances, we provide background on previous editions.

The topics are organized into chapters based on similar themes for easy navigation.

2 Timeline of DIVAR IP all-in-one releases

Below is an overview of the DIVAR IP All-in-One recorders released by Bosch over the years. To enhance usability, the devices have been categorized into two groups based on form factor: Mini Tower or 19" Rack mount.

2.1 Mini Tower form factor

	DIP-52xx	DIP-44xx
Release date	Aug 2019	Jan 2023
Installation	Pre-installed	Package for System Manager
BVMS upgrade	BVMS setup + patch	Package for System Manager
BVMS version	9.0 - tbd	11.1.1 - tbd
Operating System	Microsoft Windows Storage Server 2016, 64-bit	Microsoft Windows Server IoT 2022 for Storage Workgroup
Storage options	JBOD	JBOD
Max. Storage	48 TB	36 TB
Channels	8 - 42	8 - 32
Max. Bandwidth	170 Mbit/s	250 Mbit/s
Number of Disks	4	2
Size	Mini-tower	Mini-tower
Processor	Intel i3-8100 processor	Intel® Core™ i3-10100E
Memory	8 GB SO-DIMM	8GB DDR4-2666 1RX8 LP SODIMM
Graphics	Intel UHD 630: 1 x DVI, 1 x DisplayPort, 1 x HDMI GPU version: Nvidia Quadro P620 or successor; 4 x Mini-DisplayPort	Intel® UHD Graphics 630 (three digital outputs : 1 DisplayPort port, 2 HDMI ports)
License Scheme	DIP-52 specific Lite scheme with specific 32base for BVMS>=11	Lite scheme with specific 32base for BVMS>=11

2.2 19" Rack form factor

	71xx	72xx	73xx	64xx	74xx
Release date	April 2016	April 2020	April 2021	Jan 2023	June 2024
Installation	Appliance-Finder/ Installer	Pre-installed	Software Center	Package for System Manager	Package for System Manager
BVMS upgrade	Appliance-Installer/ BVMS setup + patch	BVMS setup + patch	BVMS package for SW Centre	Package for System Manager	Package for System Manager
BVMS version	6.0 - 12.0.1	9.0 - tbd	10.1.1 – tbd	11.1.1 - tbd	12.1 – tbd
Operating System	Windows Storage Server 2012 R2, 64-bit	Windows Storage Server 2016, 64-bit	Microsoft Windows Server IoT 2019 for Storage Standard	Microsoft Windows Server IoT 2022 for Storage Workgroup	Microsoft Windows Server IoT 2022 for Storage Standard
Storage options	RAID5/6 + HS	RAID5/6 + HS	RAID5/6 + HS	RAID5 (+HS)/ RAID6	RAID5 (+HS)/ RAID6
Max. Storage	64TB/192TB	96TB/192TB	96TB/192TB	72 TB	216/288 TB
Channels	32 - 128	8 - 256	8 - 256	8 - 64	8 - 256
Max. Bandwidth	475 Mbit/s	550 Mbit/s	550 Mbit/s	400 Mbit/s	550 Mbit/s
Number of Disks	8 / 16	8 / 16	8 / 16	4	12 / 16
Size	2U / 3U	2U / 3U	2U / 3U	1U	2U / 3U
Processor	Intel Xeon Processor E3-1275 V3	Intel Xeon Processor E3-1275 V3	Intel® Xeon® E-2226GE	Intel® Core™ i3-10100E	Intel® Core™ i7-12700E
Memory	8 GB, DDR3-1666 ECC UNB	8 GB, DDR3-1666 ECC UNB	16GB DDR4-2666 2Rx8 ECC UDIMM	16GB DDR4-2933 2Rx8 ECC UDIMM	16 GB DDR5-4800 1Rx16 ECC UDIMM

Graphics	4 x Mini Display Port	Optional Nvidia Quadro P620 or successor	Intel HD onboard graphics: 1 DVI-I port, 2 DisplayPort ports	Intel® UHD Graphics 630: 1 DVI - D port, 2 DP+ +(Dual-Mode DisplayPort) ports	Intel® UHD Graphics 770: 2x HDMI 2.0
License Scheme	DIP-70/71 specific. Plus scheme with specific 32base for BVMS>=11	DIP-72/73 specific. Plus scheme with specific 32base for BVMS>=11	DIP-72/73 specific. Plus scheme with specific 32base for BVMS>=11	Plus scheme with specific 32base for BVMS>=11	Plus scheme with specific 32base for BVMS>=11

3 DIP hard and soft limits

The DIP-74xx has specific limits, some of them hard limits, some are soft limits. What do we mean by this?

Hard limits are limits imposed by hardware and software; you cannot go over them, or the system will malfunction in some way.

Soft limits have been put in place based on tests; above these limits, operation of the system cannot be guaranteed and cannot be supported.

The way the soft limits have been determined is by running extensive tests on how the systems behave under specific conditions and stresses. Based on the outcomes of these tests, soft limits are determined.

3.1 Bandwidth

- DIP-74xx: 550 Mbit/s

The maximum bandwidth a DIP has available is determined by testing and is limited by many factors. This means that to a certain point, this is a soft limit, but it is the limit that is tested to be sustainable in the system “whatever happens”. Going over this maximum bandwidth may give adverse outcomes if the system gets taxed.

As a DIP needs to always be able to perform its functions at the same level, also while repairing a degraded system, the maximum bandwidth that is determined to be sustainable is lower than the theoretical maximum.

The main limiting factor for the bandwidth in the system is the VRM-managed iSCSI recording. To determine the limits, several benchmarking tests are done, all based on a system that is full and overwriting existing video data, as this is a trickier situation than writing on empty drives:

- Healthy system with RAID5 storage
- Degraded and repairing system with RAID5 storage
- All connected cameras running through VSG
- Healthy system with RAID6 storage
- Degraded and repairing system with RAID6 storage

On DIP-74xx, additionally tests are done with a failing PSU and switchover to the failover PSU as well.

Further tests done are based on network interruptions; how does the system cope when all iSCSI connections reconnect at the same time?

3.2 iSCSI sessions

iSCSI sessions are the connections from a device to the iSCSI target. There is a limit to the number of sessions that can be made to an iSCSI target, the limitation is determined by the Microsoft iSCSI target of the operating system, and the hardware which is used for that device (CPU and memory load), as well as the limitations of the software running on the system; VSG, VRM-based recording, BVMS decoding.

Each device recording to an iSCSI target uses one iSCSI session. When a Workstation plays back one or more streams, whether through VRM or direct iSCSI connection, it also consumes one iSCSI session per connected Workstation. If direct iSCSI playback is configured instead of VRM playback, each Workstation connecting to the iSCSI target will use one iSCSI session each during playback.

Available details for recent DIP AIOs:

Device	Bandwidth	Max iSCSI recording sessions	Maximum channel licenses (BVMS)
DIP-74xx	550 Mbit/s	256	256
DIP-64xx	400 Mbit/s	128	64
DIP-44xx	250 Mbit/s	64	32
DIP-73xx	550 Mbit/s	256	256
DIP-52xx	170 Mbit/s	42	42

3.3 Number of channels

The maximum number of BVMS channels is determined by the maximum number of licenses for a given system in BVMS operating mode. This is a soft limit in the sense that we sell the DIPs with a maximum amount of BVMS channels (see tables above). Currently, there is no hard stop on the number of channels that a customer could buy for a device, other than the hard limit for each BVMS edition. The channel licenses soft limit may be changed into a hard limit in the future.

BVMS edition channel limits:

- 42 channels for BVMS Lite
- 256 channels for BVMS Plus

3.4 Multi-imager

Multi-imager cameras (FLEXIDOME multi 7000i), require specific attention. Adding just one of them introduces 4 camera streams, each with a high bandwidth requirement if left on default settings. Some CPP13 and CPP14 cameras may have default settings that result in individual camera-module streams exceeding 20 Mbps. Consequently, one multi-imager camera could output up to 80 Mbps if left on default settings in certain environments.

It's important to closely examine any installations involving multi-imagers, and to a lesser extent, other CPP13 and CPP14 cameras. Even minor mistakes or leaving settings on default can significantly impact the entire recording system.

3.5 Storage capacity

The maximum storage capacity serves as a hard limit. ASUS conducts tests on specific HDDs for our systems, including each new HDD intended to be supported in our DIP-74xx models. Our DIP-74xx systems do not support any other drives. Currently, the maximum supported capacity for drives is 18 TB.

We do not support hard drives that are bought through other channels than our own; even the exact same drive but bought from a 3rd party is officially not supported.

3.6 DIP testing

In addition to the tests conducted to ascertain the maximum recording load on the system, we also perform thorough testing on decoding performance. You can find detailed outcomes of these tests in the technical certification training and on the knowledge base.

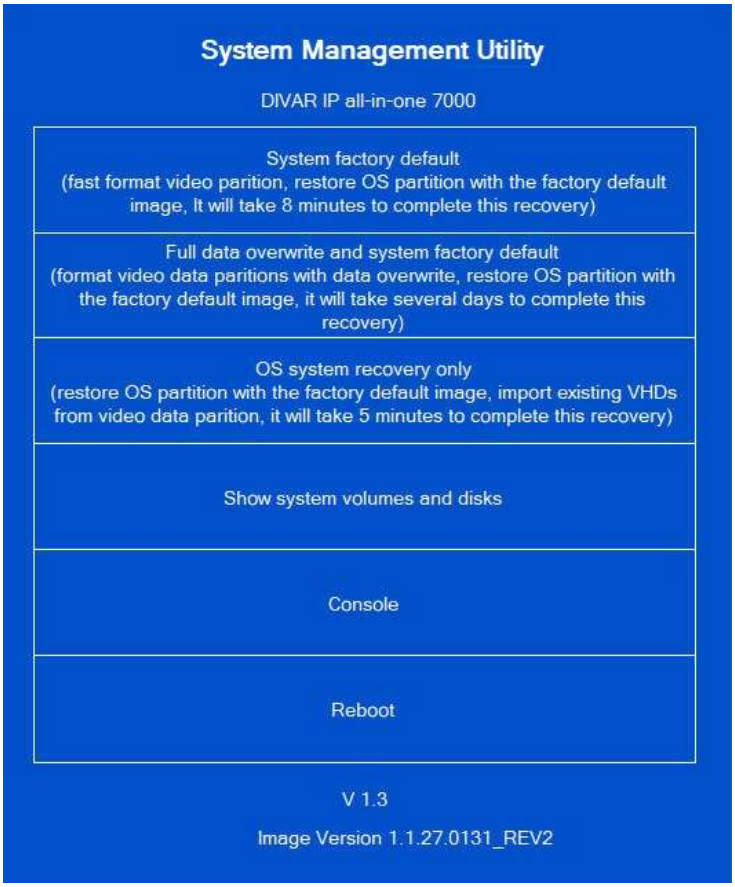
Furthermore, we assess transcoding limitations, determining the number of streams that can be transcoded simultaneously and at which resolutions.

Additional testing encompasses smoke testing, package testing, and evaluation of software behaviour.

4 System configuration

4.1 Recovery menu explained

The recovery menu in the DIP-74xx is quite similar to that of the DIP-44xx and DIP-64xx. To initiate the unit's recovery process, press F7 during the BIOS power-on self-test, and the System Management Utility will be displayed.



The first option is **System factory default**. This is a relatively quick procedure where the OS partition is overwritten with the factory default image and the video data partitions are quickly formatted. This takes approximately 8 minutes to go through and after that the system is back to the 'out-of-the-box'-state (pre-installation of any software).

Full data overwrite and system factory default is a very time-intensive procedure. It will overwrite the OS partition with the factory default image. The data partitions will be overwritten with 1's and 0's to completely erase the information that was there on the drives. Due to the latter part of this operation, the procedure will take several days to complete.

The last option: **OS system recovery only**, will overwrite the OS partition with the factory default image, but will leave the data partitions intact and will import existing VHDs on these partitions into the system. This makes it possible to access pre-recovery video data with a clean system, but only if the BVMS configuration files are exported before recovery and imported after recovery. This is a quick procedure, taking approximately 5 minutes to complete for a completely clean system, before installation of any software.

Note that none of these 3 options will impact the BVMS licenses at all. Once the system is licensed correctly, a recovery will not impact the licensing status whatsoever, this the same as on the DIP-44xx and DIP-64xx.

Other options in the System Management Utility include:

- **Show System Volumes and Disks** – show the various hard drives, RAID arrays and partitions in the system
- **Console** – open the command prompt
- **Reboot** – exit the utility and reboot the system

4.2 BIOS

The BIOS in a DIP-74xx is custom-made for Bosch, rendering standard ASUS BIOS versions incompatible. Attempting to use a regular ASUS BIOS will trigger rejection by the DIVAR IP all-in-one system by design. However, if the BIOS resets to its default settings, those defaults are already optimized for seamless operation. Therefore, no additional adjustments are required to ensure correct system functionality.

The DIP-74xx is the first DIP model featuring a pre-set BIOS password, noted on the rear of the unit. If the sticker on the unit's rear is removed or unreadable, an additional sticker can be found inside the unit, placed on the motherboard, providing default passwords for both BIOS and BMC.

Upon logging in to the BIOS using the default password, immediate password alteration is strongly recommended. This changed BIOS must be stored in a secure location.

NOTE: ASUS does not maintain a database of default passwords per unit for data security purposes. If the default password is irretrievably lost, there is no way to access the BIOS.

4.2.1 Recovering the system to the default BIOS password

If the modified BIOS password is lost, system recovery to the default BIOS password is necessary to regain access to the BIOS. To do this, the BIOS needs to be updated, which will reset the password back to the default. The following section explains how to update the BIOS.

4.2.2 Updating the BIOS

During the lifespan of the DIP-74xx, there may arise a need to update the BIOS, but this will only be necessary if mandated by development. In such cases, a BIOS update file will be provided through development/product management channels.

For the BIOS update procedure, follow the steps outlined below. These instructions are derived from internal documentation provided by the Engineering team on 09-Feb-2024 (V19):

4.2.2.1 Scope

This section describes the step-by-step process of updating the BIOS on the DIVAR IP all-in-one 7000 4th gen (DIP-74xx).

Note: Updating the BIOS will reset the BIOS password to the default version.

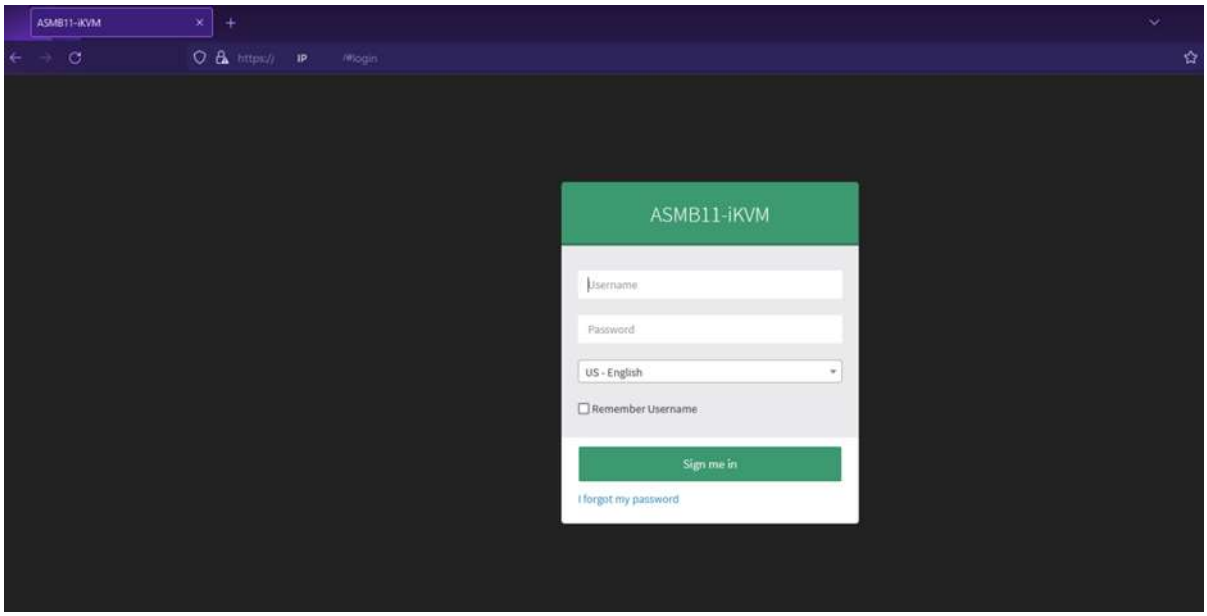
WARNING: Do not turn off or restart the DIVAR IP all-in-one during the BIOS update. An incomplete or incorrect BIOS update can severally affect the functionality of device or permanently damage it.

4.2.2.2 Requirements

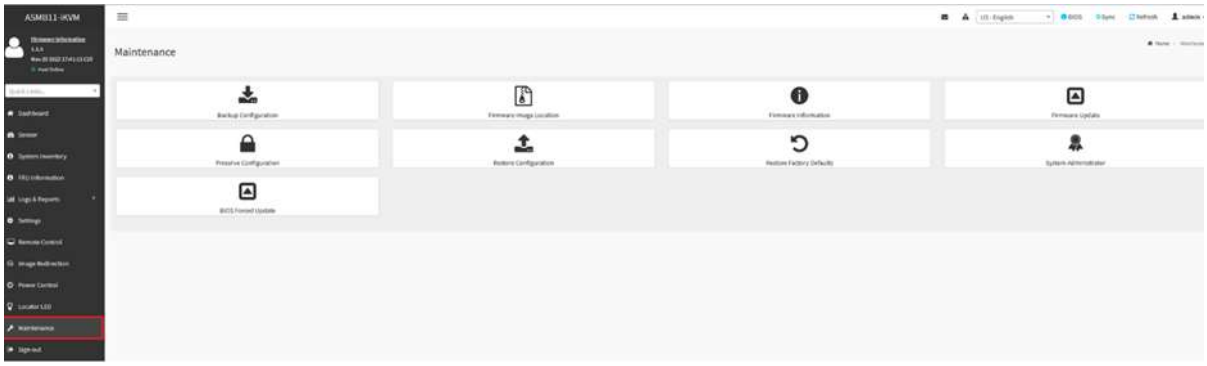
- A Bosch DIVAR IP all-in-one 7000 4th gen system in place but powered off for this update.
- BMC already configured on BIOS settings.

4.2.2.3 Procedure steps

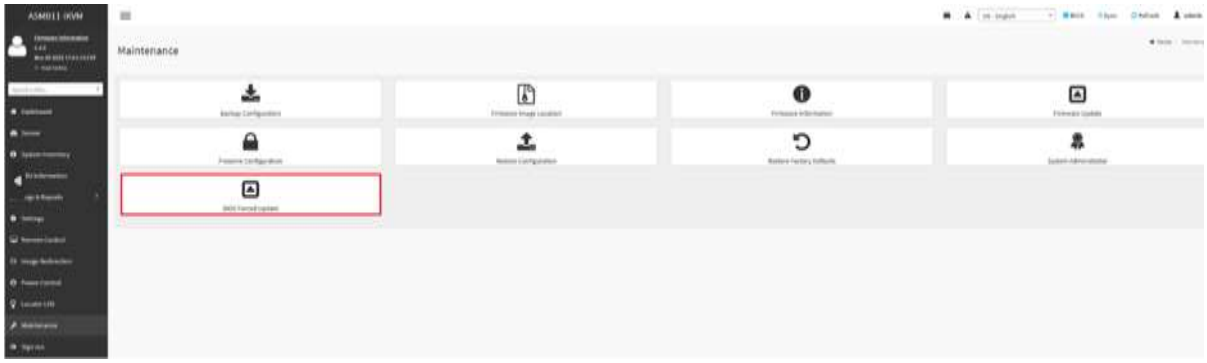
1. Open a web browser and enter the IP address of the DIVAR IP BMC. This will display the login page where you can enter your login credentials.



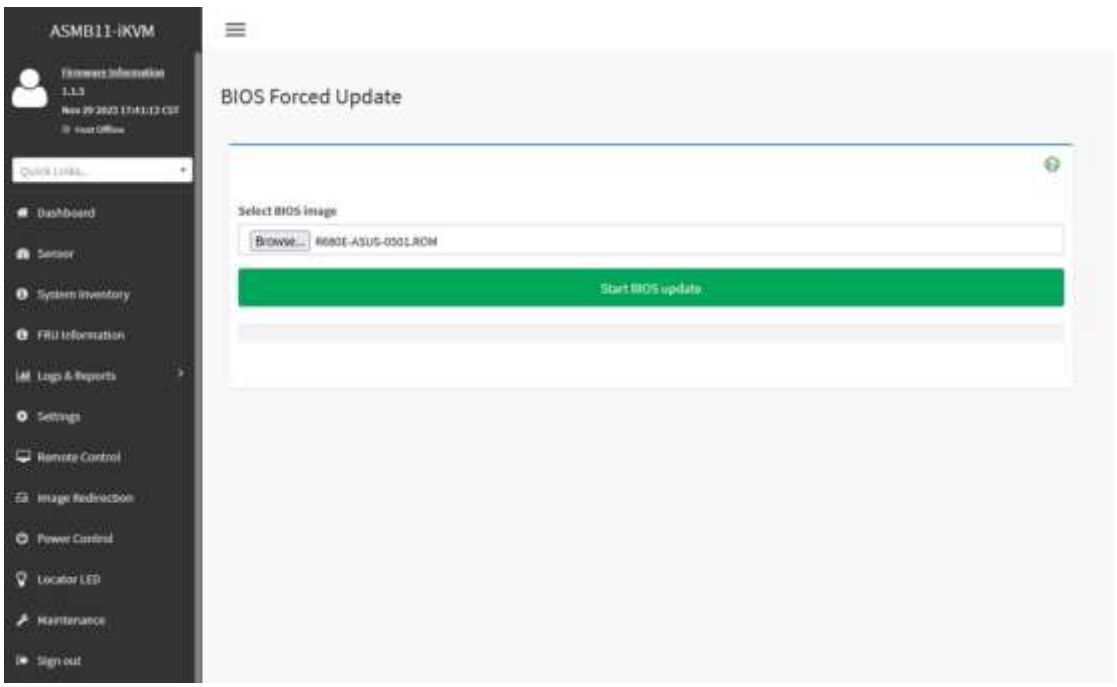
2. Select the "**Maintenance**" option from the left-hand menu:



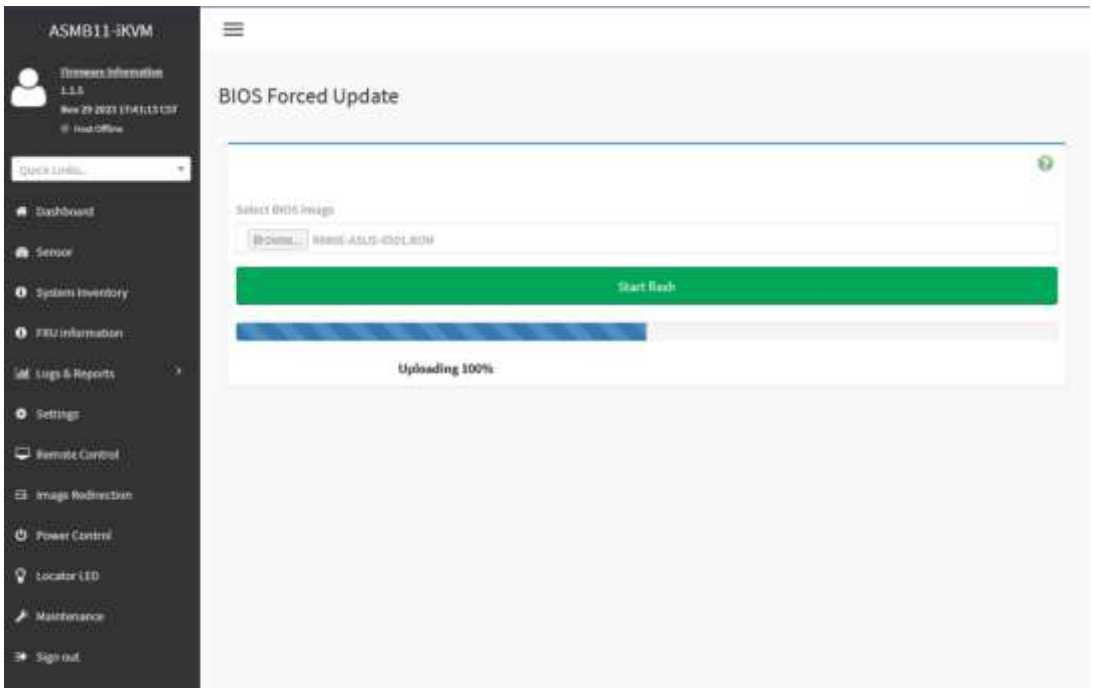
3. Choose the "**BIOS Forced Update**" option.



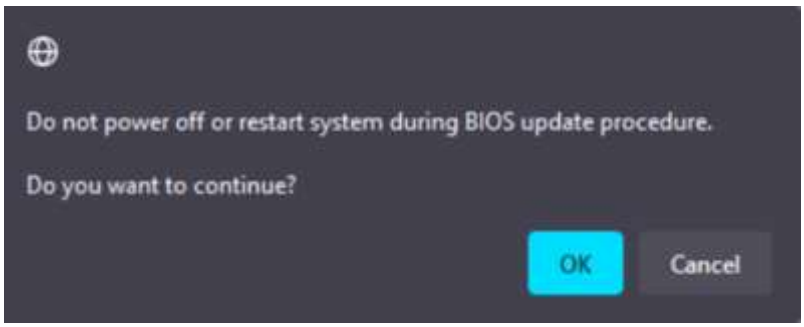
4. Click on "**Browse**" to search for and select the BIOS ROM file:



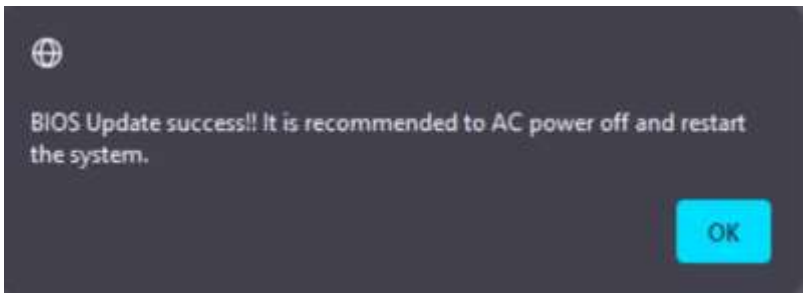
5. Click on the "**Start BIOS update**" button and wait for the upload to reach 100%. Then, click on the "**Start flash**" button:



6. Click on "**OK**" to confirm the flash procedure:



7. If the update process completes successfully, the following pop-up will be displayed:



With the update completed, it's time to power on the DIVAR IP. Procedure finished!

4.3 Operation modes

How to select the Operation mode for a DIP has undergone significant changes compared to DIVAR IP all-in-one models predating the DIP-44xx and DIP-64xx. The DIP-74xx maintains a similar structure to these newer models regarding Operation modes.
Unlike the DIP-73xx, you cannot use scripts to transition between Operation modes.

To change the Operation mode:

1. Begin by recovering the system through the System Management Utility.
2. Next, install DIVAR IP System Manager from the Software Selection.
3. Finally, use System Manager to select the desired operation mode, and it will automatically install any required software.

The differences between Operation modes encompass services as well as firewall settings. Especially because of the latter, simply turning services off or on will not be enough to run in one of the other operation modes (for example, when starting out in BVMS mode). For comprehensive troubleshooting, it's important to set up the system from scratch in the appropriate operation mode.

Probably the most-used operation mode is **BVMS mode**; in which the system is used as a full recording and management system, including VRM and iSCSI storage.

VRM mode can be used if there is already a device running BVMS in the system, but a distributed VRM configuration is desired. A DIP can then be configured solely for VRM functionality and added to the BVMS server on the other device.

VRM mode is still supported, but individual licensing for this mode has been discontinued with BVMS 12. With the DIP-74xx, there's no need to worry about VRM licensing, as an adequate number of licenses are already included in the DIP system for maximum operation.

VRM support is tied to the management system. If there is an SMA for the main system, VRM installation is also supported. However, systems with fully standalone VRM are not supported on the new DIPs.

For additional information, please refer to the **End of Life Announcement for Video Recording Manager – standalone**, dated 16-09-2022.

iSCSI Storage mode can also be used in a BVMS system. If you already have a DIP configured for BVMS, but require additional storage, simply configure an additional DIP in iSCSI Storage mode and integrate it as storage into the DIP's configuration. This can be done using either the DIP Configuration Wizard or BVMS Configuration Client.

For further information on the operation modes, please refer to the DIVAR IP all-in-one technical certification training.

4.4 DIVAR IP System Manager

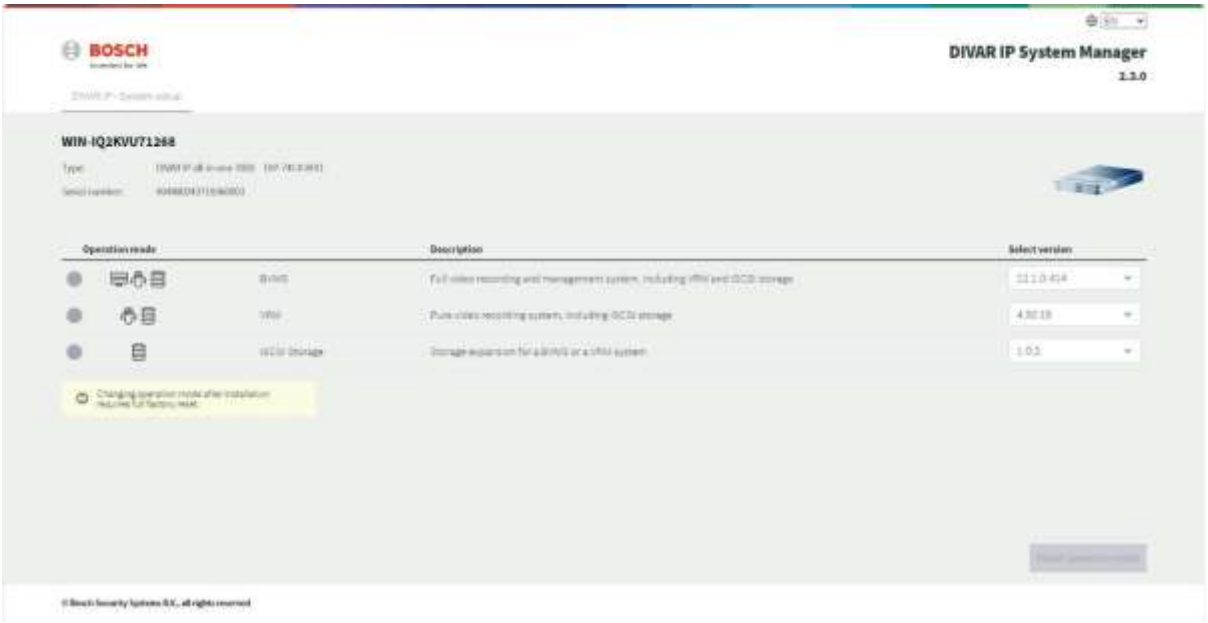
System Manager has been utilized for installing and managing DIP software installations since the introduction of DIP-44xx and DIP-64xx. Starting from System Manager version 2.1, a licensable feature called Remote System Management (RSM) has been added. This feature enables a connection to the Bosch Remote Portal, facilitating remote monitoring and administration of the DIP and its connected cameras.

RSM is an optional addition and not mandatory for the operation of the DIP. The System Manager primarily operates in two main states:

1. System setup: Selecting and installing an operation mode.
2. Software packages: Updating already installed software.

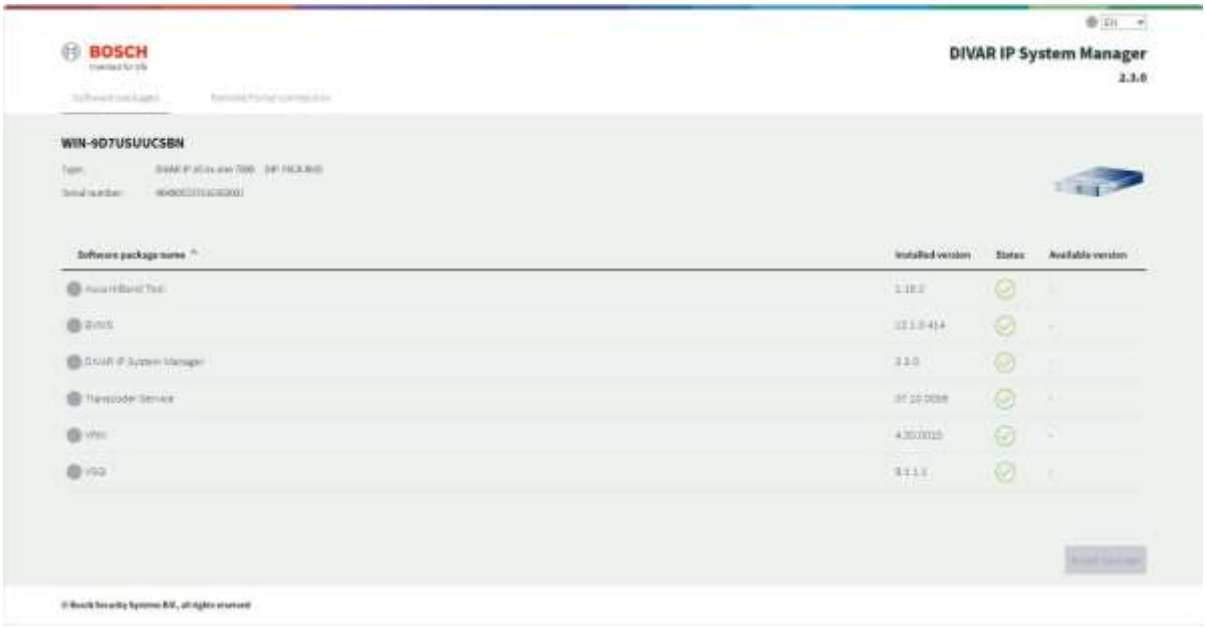
Once the first state is completed, System Manager will transition to the second state. There is no direct method to return to state 1, except through system recovery and reinstalling System Manager.

4.4.1 State 1: System setup



In this state, System Manager searches for software in both the Images partition > BoschAppliance and any files located in a BoschAppliance folder on a connected USB device. Additional details regarding this aspect of the installation process can be found in the Installation Manual, the technical certification training materials, as well as in the video "DIVAR IP all-in-one: First-time installation" available on YouTube.

4.4.2 State 2: Software packages



New software can be downloaded from the Bosch Download Store and saved either in the BoschAppliance folder on the Images partition or on an attached USB device. System Manager will then detect these software updates and display them as update options once it transitions to state 2 after the installation of an operation mode.

If any listed packages are removed using **Windows Add or Remove Programs**, the change may not be immediately reflected in the list since the software is not continuously monitored. To ensure the correct listing, it's recommended to restart the **Bosch.SysMgm.Commander** service.

4.4.3 Folders

System Manager installation folder is here: C:\Program Files\Bosch\SysMgmService
System Manager data folder is here: C:\ProgramData\Bosch\SysMgmService

In the chapter about gathering information, comprehensive details will be provided regarding the logging capabilities of System Manager.

4.4.4 Remote System Management

In the previous DIVAR IP all-in-one Troubleshooting Guide, a significant chapter was dedicated to the Remote System Management Service. As the focus of this guide is primarily on the core processes of the DIP, this chapter is now a stand-alone Troubleshooting Guide, which is also available on our Bosch-internal Training Academy.

5 Information gathering

5.1 ASUS Inband Tool

With the release of the DIP-74xx, a new tool is available for health monitoring and log gathering, it essentially replaces SuperMicro's SuperDoctor5; the ASUS Inband Tool. This tool operates as a service on the DIP and provides a webpage with hardware health monitoring options, hardware status details, and hardware information, as well as an option to export logs and run reports. There are other tools that can be used to gather logs from the DIP (LSA and BMC), but the ASUS Inband Tool is the main and most elaborate tool for this purpose. Besides this purpose, the Inband tool also provides the service to Remote System Management to remotely read out the health status of the system's components.
Detailed troubleshooting guidance is found in **ASUS's troubleshooting guide**.

5.1.1 Report option

A detailed overview of the Inband tool is provided in the how-to video titled "**DIVAR IP all-in-one 7000 4th gen – Monitoring the system**". The tool has a "Report" menu option that allows creating CSV or JSON-formatted reports on the system. The CSV format is preferred for support purposes. The following information can be exported:

System:

- CPU Information
- CPU Utilization
- Memory Information
- Memory Utilization
- DISK Utilization
- Disk Information
- NIC Information

System Log:

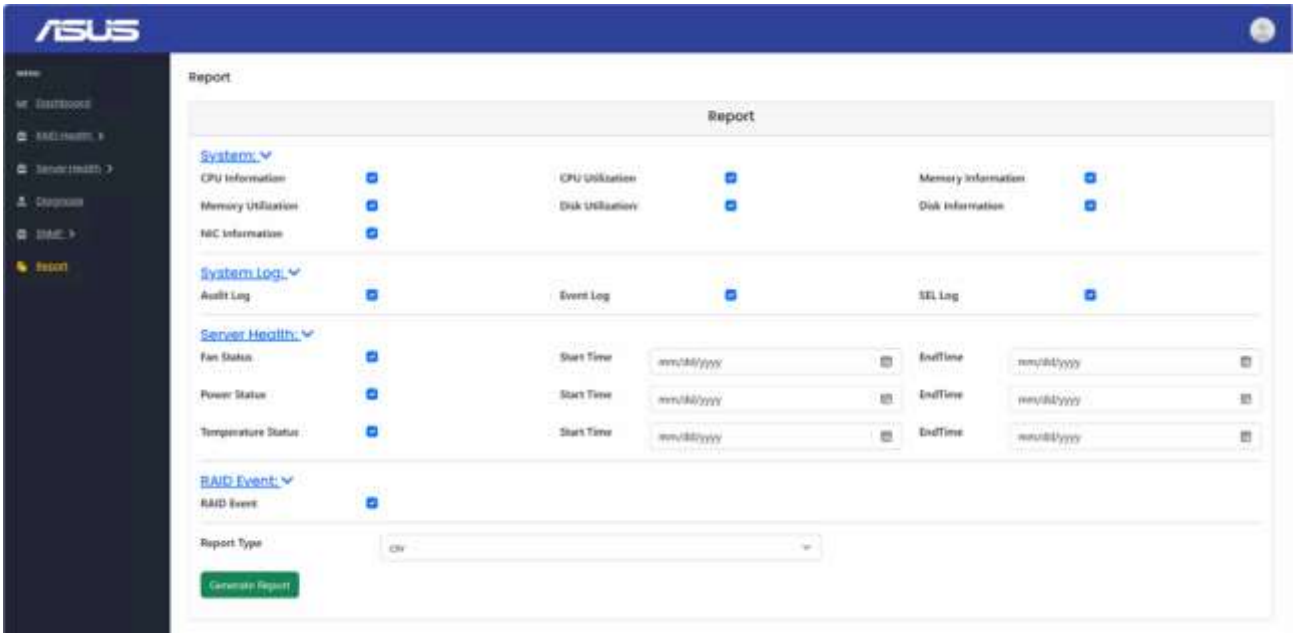
- Audit Log
- Event Log
- System Event Log (SEL)

Server Health:

- Fan Status (over time)
- Power Status (over time)
- Temperature Status (over time)

RAID Events

As the server health statuses are recorded over time, the gathered logging can be defined with a start and end date to narrow down the troubleshooting information.



Besides the exported logs from the ASUS Inband Tool, ASUS Technical Support recommends adding the following to reports to them:

- Microsoft Windows System Information Export
- Screenshots of any error messages on-screen or symptoms on-screen
- Photographs of any physical issues

5.2 DIVAR IP System Manager

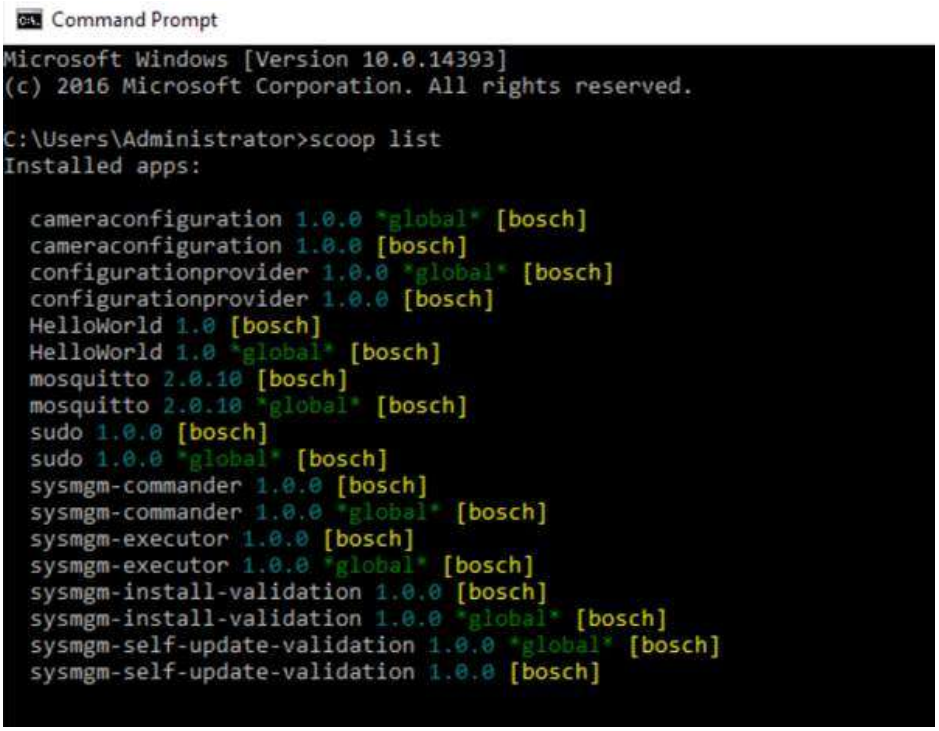
Please note that any known issues at the release of a version of System Manager, as well as any additional specifics or noteworthy information, can be found in the Release Notes of the software. These Release Notes are distinct from DIP or BVMS releases, as System Manager is its own software entity.

If an installation package is corrupted in any way (for instance, if the signature is not valid or if the manifest file is corrupted), it will not appear on the System Manager page to begin with. In such

cases, it is usually easiest to re-download the package before initiating a full troubleshooting session.

5.2.1 Using Scoop commands to troubleshoot

Troubleshooting using Scoop commands, requires Command Line access with Admin privileges. The command "scoop list" displays installed software and versions for installed apps:



Note that Scoop only lists what has been installed through **DIVAR IP System Manager**. Windows-level software shows in "**Add/remove programs**." For the UI: Control Panel is filtered for Bosch software (contains “Bosch” in the name” and merged with scoop list.

Command	Explanation
scoop	Lists all available commands
scoop help <command>	Explains usage of a particular command
scoop uninstall <app>	Uninstalls an app
scoop reset <app>@<version>	Rolls back an app to a specific version, e.g., restore previously installed version. This just resets the internal housekeeping of scoop; the app still needs to be deleted manually.

Caution is advised due to potential unwanted behavior or untested combinations of different components.

Steps for cautious uninstalling/resetting are:

1. Execute **scoop list** to find the exact AppName for the package
2. Execute **scoop uninstall *AppName***
3. After the uninstall check if the App folder has really been deleted by scoop, otherwise delete it manually. The App folder should no longer be present under **C:\ProgramFiles\Bosch\SysMgmService\Apps**
4. Open Windows Services and stop **Bosch.SysMgm.Commander**, wait ~20s for it to stop properly, then start it again. This will then propagate the changes to the Back-end/Local UI

5.2.2 In case of failed Scoop installations

Buckets\Bosch:

- Examine manifest content of the application to be installed.
- Compare with the source (e.g., USB-stick) to ensure consistency.

File Cache:

- Check if the installer file is found in the cache folder.
  - The cache contains essential installer files that Scoop utilizes.
- Open the installer zip-file and inspect its contents.
  - Validating the contents ensures the files are complete and usable.

Apps Folder:

- Inspect sub-folders within the Apps folder.
- Verify versions of the sub-folders against the expected versions.
- Monitor the app's sub-folder during installation; some files might be temporary and are deleted upon failure.

Update/Install from Command Line:

- Execute the command specified in the manifest from the command line.
  - This allows you to observe the process directly.
- Observe the command line output generated by Scoop.
  - The command line output may offer insights into any errors or issues.

Installer log files:

Check for a log-file generated by the installer being executed, this can uncover issues, errors, or any specific reasons for installation failures. Note that not all installers create log-files.

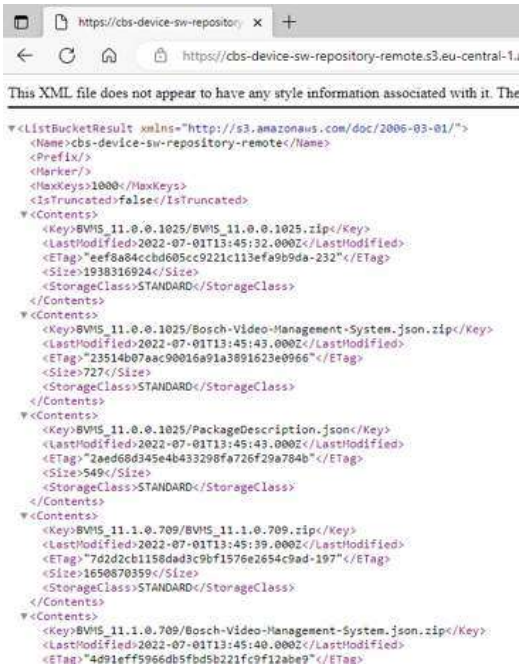
5.2.3 Remote Software Repository troubleshooting

The Software Repository serves as the centralized hub for all manifests and installers. The repository is publicly available through a secure HTTPS connection. On the back-end, the repository is hosted on an S3 bucket. As the repository address will change occasionally, the best way is to use what is referenced in the install command in the **sysmgm-commander.log**:

```
[2024-02-14 06:51:35.078 INF] SysMgmCommand { CorrelationId = 1e837741-efb1-4360-80ff-a204a4fcc05f, OperationCorrelationId = -87d7fea4-5879-46bb-ba61-66363eb804eb, Command = install, ComponentName = healthmonitor, ComponentVersion = 1.1.0, MetadataRepository = https://sw-repo-remote.s3.eu-central-1.amazonaws.com/healthmonitor_1.1.0/healthmonitor.json.zip, SourceMetadataRepository = , Timeout = 01:00:00, CurrentVersion = , Reboot = False, ComponentDisplayName = }

[2024-02-14 06:51:35.079 INF] ================================================================================
==== INSTALL OPERATION START

[2024-02-14 06:51:35.080 INF] [1e837741-efb1-4360-80ff-a204a4fcc05f] ["SysMgmCommandManager"] Received message "SysMgmCommand" from actor "BoschIOInstallationDomainMapper" > OperationCorrelationId : "-87d7fea4-5879-46bb-ba61-66363eb804eb" | CommandType: install
```



The key **MetadataRepository** contains the URL to the repository that can then be checked for the manifests. In the example above the address is **https://sw-repo-remote.s3.eu-central-1.amazonaws.com/**

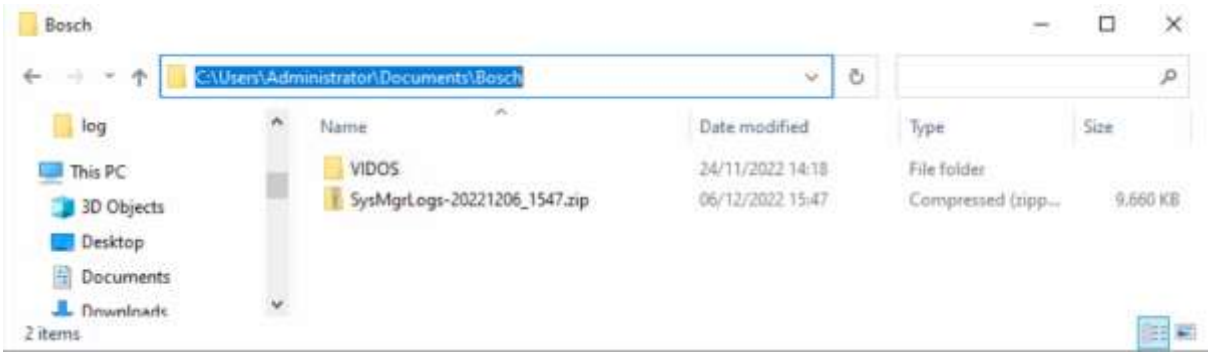
Opening that address in a web browser gives you an overview of the manifests of the software found in the repository, like in this example.

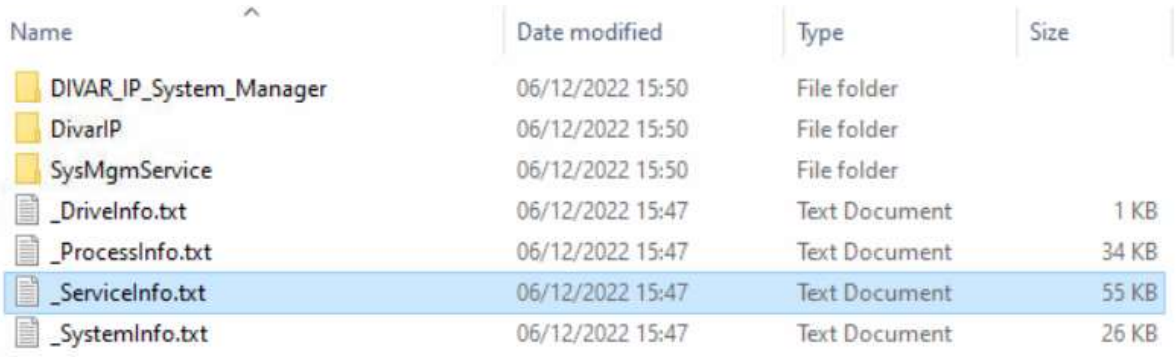
5.2.4 Collecting and reading System Manager logs

Collect all logs under **C:\ProgramData\Bosch\SysMgmService\log**

To facilitate the easy collection of System Manager logs, a script named "**Export System Manager Logs**" has been added to the Start Menu of the DIP-74xx:

Make sure to run the script as Administrator. After executing this script, the resulting ZIP file can be found in **C:\Users\Administrator\Documents\Bosch**:



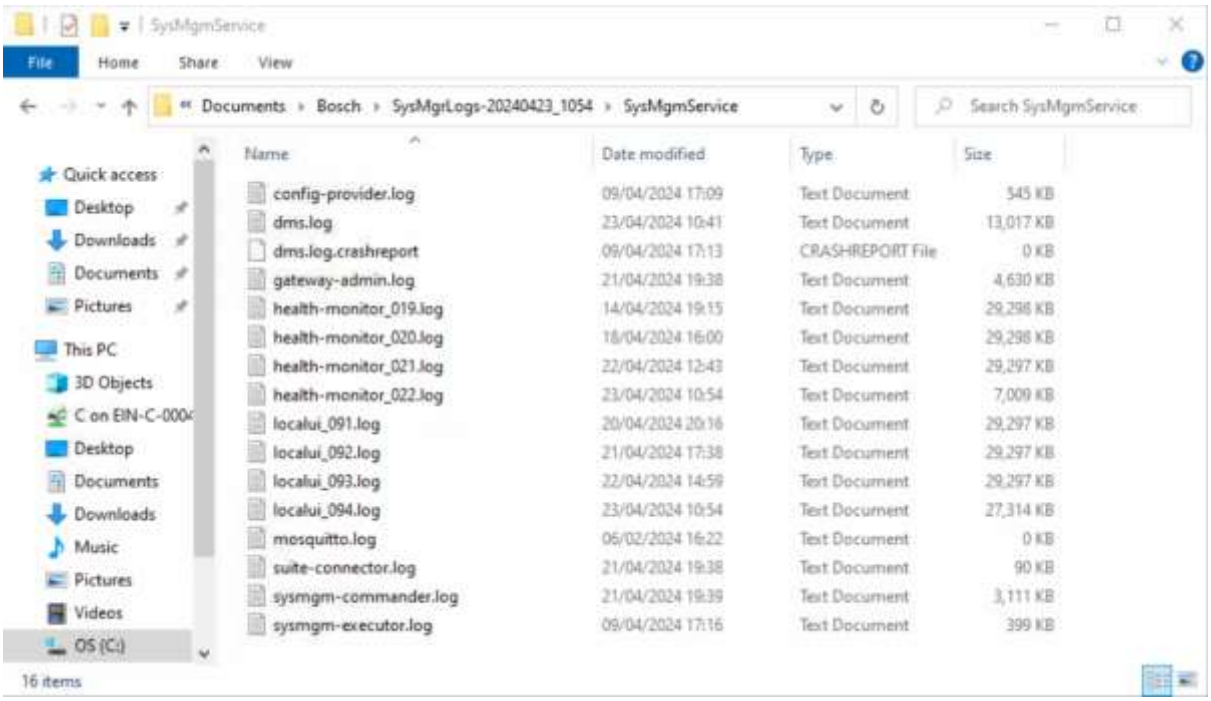


The logs gathered in the ZIP file include:

- **DIVAR_IP_System_Manager** – Installation logs for System Manager
- **DivarIP** – Installation logs for the DIVAR IP AIO's other software
- **SysMgmService** – Logs copied from C:\ProgramData\Bosch\SysMgmService\log
- **_DriveInfo.txt** – Details about the storage on the DIP
- **_ProcessInfo.txt** – Details on currently running processes
- **_ServiceInfo.txt** – Details on currently running services
- **_SystemInfo.txt** – Windows System Information

These files contain essential information for troubleshooting installation failures or other issues. The ZIP file is not encrypted, and all log files are in plain text format.

5.2.5 System Manager Log types



There are various System Manager logs that are available. Some of the logs are used for the System Manager on the DIP itself, others are mainly used for services that are required for Remote System Management. We will focus on the logs that are in use for the System Manager services.

Here's an overview of the available logs, the most used logs are **bold**:

- config-provider.log - Log for replication of camera configuration from BVMS to DMS
- dms.log – camera communication log
- gateway-admin.log - Provisioning log
- health-monitor.log – health monitoring log for remote reporting
- **localui.log** – any logs from the local UI itself
- mosquitto.log – MQTT communication log for RSM integration, normally MQTT logging is disabled
- suite-connector.log - remote connection to IoT core log
- **sysmgm-commander.log** – backend communication log
- **sysmgm-executor.log** – execution of installations log

5.2.6 Using System Manager logs to find installation issues

The complete installation process can be followed by checking the System Manager logs.

5.2.6.1 Localui.log

The start of the process always involves locating the installation files on the system. Any issues encountered here, will be documented in the localui.log files. Typically, these log files will contain lines stating:

```
INFO – PackageScannerActor: DrivesFound received => 2 Drives found
```

But when drives containing installation files are introduced into the system, this event is also recorded in the log file:

```
INFO – OperationModeValidatorActor: ValidateOperationMode received =>
F:\BVMS_11.1.1_SystemManager_package_1.0\VRM_4.03.0025_OpMode\OpModeDescr
iption.json
```

```
INFO – OperationModeValidatorActor: ValidateOperationMode received =>
F:\BVMS_11.1.1_SystemManager_package_1.0\ISCSi_1.0.0_OpMode\OpModeDescrip
tion.json
```

```
INFO – OperationModeValidatorActor: ValidateOperationMode received =>
F:\BVMS_11.1.1_SystemManager_package_1.0\BVMS_11.1.1.65_OpMode\OpModeDesc
ription.json
```

In this instance, three Operation Mode packages were discovered on a USB device inserted into the DIP.

Once an operation mode is selected and the package is ready to be installed, messages similar to the following will appear in the log:

```
SignalR is going to send available operation modes to 1 clients.
```

```
INFO – NotifyActor: OperationModeAvailable received => Operation Mode:
BVMS – Operation Mode Version: 11.1.1
```

```
INFO – NotifyActor: OperationModeAvailable received => Operation Mode:
BVMS – Operation Mode Version: 11.1.1.65
```

Then the process starts:

```
SignalR is going to notify 1 clients that a download is in progress
```

```
INFO – NotifyActor: DownloadProgress received => Progress:
DownloadProgress { Total = 15, Downloaded = 11 }
```

```
ModalProgress: DownloadOnGoing
```

And then:

```
ModalProgress: INSTALLATIONUPDATE: INSTALLING
```

Any issues encountered during file detection or initial file validation will be documented in this log.

5.2.6.2 sysmgm_commander.log

Typically, monitoring status changes within this log can provide insights into incidents occurring at various stages of the installation process. Keep an eye out for statuses such as "STARTED," "DOWNLOADING," "INSTALLING," etc., along with the corresponding package names.

Once the process commences, you can observe it in the commander log:

```
INFO - ServiceBusActor => ==…== OPERATION START
```

The download process is initiated, as evident from the entries in the localui log:

```
FileDownloadActor: DownloadRequest received => Guid: e0cb4e10-31b5-43b2-997d-3f3916b2749a - RepositoryUrl: C:\ProgramData\Bosch\SysMgmService\cache\BVMS_11.1.1.65_OpMode\bvms-opmode.json.zip - InstallationFolder: C:\ProgramData\Bosch\SysMgmService\temp\ - IsValid: True - Timeout: 00:05:00
```

Once the download is completed, the file undergoes validation. Additionally, within the log, you can locate the manifest file, which is crucial for installation, as it provides valuable information regarding the installation order and variables:

```
ComponentInfo: ValidateManifests received => Component: Bosch-Video-Management-System - Path: C:\ProgramData\Bosch\SysMgmService\temp\bvms-opmode.json
```

After this, signatures, and integrity for each of the components are validated and reported:

```
INFO - SignatureValidationActor: ValidateSignature received => RequesterId: 77915a47-a87c-4657-989c-74be2fa424a3 - Directory: C:\ProgramData\Bosch\SysMgmService\temp\bvms-opmode.json\Bosch-Video-Management-System.json
```

```
INFO - IntegrityActor: SignatureValidated received => RequesterId: 823af8e9-fc1c-4e05-a007-0f8248668cad - IsValidSignature: True
```

If any issues arise with the signatures or integrity of the files, they will be flagged at this point. If everything is in order, the installation execution is initiated:

```
INFO - ProcessActor => Executing a new Start Process command. FileName: powershell.exe - Arguments: sudo scoop cache rm Bosch-Video-Management-System
```

Once a package is installed successfully, the following log-line (or similar) is added:

```
Creating shim for 'config-dip'.Running post-install script...'config-dip' (1.0.0) was installed successfully!
```

If there are issues in the installation that are indicated in the Commander log, more information can be found in the following files.

5.2.6.3 Manifest files

During this phase of the process, manifest files in JSON format come into play. These files can be located at: C:\ProgramData\Bosch\SysMgmService\localscoopbucket. They contain comprehensive information about an installation package, including:

- Signature and hash
- Version
- Description
- URL (location of the package)
- Pre-install dependencies (files required to be installed before the main package)
- Pre-installation script for the dependencies
- Installation script for the main package
- Post-installation dependencies (files required to be installed after the main package)
- Post-installation script for the dependencies

In addition to this vital information, if the main package or its dependencies have their own logging during installation, it will be part of the variables in the installation script. For instance, for BVMS, the line would appear as follows:

```
"$arguments = @('/s
/debuglog\"c:\\ProgramData\\Bosch\\VMS\\Log\\bvms_setup_11.1.1.65.log\"
/v\" /qn /L*v+
\"c:\\ProgramData\\Bosch\\VMS\\Log\\bvms_msi_11.1.1.65.log\"
```

In this scenario, if any issues arise during the installation of the BVMS setup package, additional details can be found in the BVMS logs located at C:\ProgramData\Bosch\VMS\Log\bvms_msi_11.1.1.65.log\ (the log name will vary depending on the BVMS version), especially if the System Manager logs do not provide conclusive information.

5.2.6.4 sysmgm_executor.log

The execution of the installation, as per the scripting outlined in the Manifest file, is recorded in the sysmgm_executor.log.

Each package will be installed sequentially, and an installation process will resemble the following:

```
INFO - ProcessActor => Executing a new Start Process command. FileName:
powershell.exe - Arguments: sudo scoop install config-dip --global

INFO - ProcessActor => StartProcess, creating a start info.

INFO - ProcessActor => Executing Process.Start.

INFO - ProcessActor => Installing 'config-dip' (1.0.0) [64bit]Downloading
C:\ProgramData\Bosch\SysMgmService\cache\config-dip_1.0.0\config-
dip_1.0.0.zip (424 B)...

Checking hash of config-dip_1.0.0.zip ... ok.

Extracting config-dip_1.0.0.zip ... done.
```

```
Linking C:\Program Files\Bosch\SysMgmService\apps\config-dip\current =>
C:\Program Files\Bosch\SysMgmService\apps\config-dip\1.0.0

Creating shim for 'config-dip'.Running post-install script...'config-dip'
(1.0.0) was installed successfully!
```

Any errors that occur will be documented in this file. Further investigation into the logging for the package encountering the issue will be necessary, based on the information provided in this log file.

Within the log file, you may encounter several mentions of Scoop. Scoop is the package manager utilized for installing the packages.

5.2.6.5 Troubleshooting order

To begin troubleshooting if a package fails to install correctly:

1. **Refer to Manifest files**: Utilize Manifest files to understand the order of package installations and associated variables.
2. **Examine commander and executor logs**: Analyze both commander and executor logs to identify the nature of the issue. Determine if it's related to signature or integrity (commander) or if it's an issue during the installation process itself (executor).
3. **Utilize package-specific logging**: If available, refer to the package's own logs for additional troubleshooting details. Alternatively, consult executor logs or Windows logs for further insights.
4. **Consider manual installation**: Running the installation manually can sometimes pinpoint the issue or help circumvent problematic variables.

If the issue arises in the Commander logs, it's likely caused by a corrupt package, a broken or removed USB device, or potential tampering with the package.

If the issue surfaces in the Executor logs, it may indicate problems with the DIP itself, such as filesystem limitations, permission issues, or interference from running processes. Windows logs may also provide relevant information in such cases.

5.2.7 Troubleshooting examples

5.2.7.1 Logfile analysis

Sysmgm-commander: start of installation:

```
======== OPERATION START
```

Sysmgm-executor: Block where installation is executed:

```
======== SEQUENCE RECEIVED

…

======== SEQUENCE EXECUTED
```

LocalUI: New drive detected:

```
12/09/2022 19:57:14 INFO - PackageScannerActor: DrivesFound received => 3 Drives
found

…

12/09/2022 19:57:15 INFO - NotifyActor: DrivesFound received => Number of Drives
Found: 1

12/09/2022 19:57:15 INFO - PackageScannerActor: DrivesFound received => 4 Drives
found
```

5.2.7.2 Corrupted manifest – sysmgm-commander.log

Hacker manipulated the manifest to e.g., install another version:

```
12/09/2022 19:45:29 INFO - ServiceBusActor =>
================================================== OPERATION START
12/09/2022 19:45:29 INFO - ServiceBusInstallationDomainMapActor:
RequestInstallPackage received => RequesterId: 82e572be-15c9-430e-8a59-
d7cecc5908a0 - CorrelationID: Demo-65146b4d-4031-4aed-badc-c394bcbb47d3 - Package
Name: Demo - Package Version: 1.0.0 - Package Owner:  - Timeout: Demo-65146b4d-
4031-4aed-badc-c394bcbb47d3 - MetadataURL:
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\demo.json.zip
12/09/2022 19:45:29 INFO - SysMgmCommandManagerActor: SysMgmCommand received =>
RequesterId:82e572be-15c9-430e-8a59-d7cecc5908a0, ComponentName:Demo,
Command:install, Timeout: Timeout { Duration = 00:30:00, IsZero = False }
…
12/09/2022 19:45:29 INFO - BoschIOActor: OperationStatusChanged received =>
Status: STARTED
…
12/09/2022 19:45:29 INFO - BoschIOInstallationDomainMapActor:
InstallationStatusChanged received => RequestorId: 82e572be-15c9-430e-8a59-
d7cecc5908a0 - CorrelationId: Demo-65146b4d-4031-4aed-badc-c394bcbb47d3 - Status:
UPDATE_METADATA
…
12/09/2022 19:45:29 INFO - BoschIOActor: OperationStatusChanged received =>
Status: DOWNLOADING
…
12/09/2022 19:45:29 INFO - FileDownloadActor: DownloadRequest received => Guid:
82e572be-15c9-430e-8a59-d7cecc5908a0 - RepositoryUrl:
```

```
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\demo.json.zip -
InstallationFolder: C:\ProgramData\Bosch\SysMgmService\temp\ - IsValid: True -
Timeout: 00:05:00
12/09/2022 19:45:29 INFO - FileDownloadActor => Starting download for url:
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\demo.json.zip.
…
12/09/2022 19:45:29 INFO - CompressedFileActor => Metadata extraction command
executed: InstallationDomain.Akka.Messages.Commands.ExtractFile
…
12/09/2022 19:45:29 INFO - SignatureValidationActor: ValidateSignature received
=> RequesterId: 2244bf72-1b13-42c9-9b85-fde7dff0040a - Directory:
C:\ProgramData\Bosch\SysMgmService\temp\demo.json\demo.json
12/09/2022 19:45:29 INFO - IntegrityActor: SignatureValidated received =>
RequesterId: 2244bf72-1b13-42c9-9b85-fde7dff0040a - IsValidSignature: False
12/09/2022 19:45:29 Stopped
12/09/2022 19:45:29 ERROR - UpdateMetadataActor: ValidatedFilesIntegrity received
=> Package file validation failed: RequesterId: cdc77887-de73-4356-91de-
2c02f9651228
12/09/2022 19:45:29 ERROR - InstallationCoordinatorActor: UpdatedMetadata
received => Failed! Component: Demo - File:
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\demo.json.zip
12/09/2022 19:45:29 INFO - ServiceBusInstallationDomainMapActor:
InstallationStatusChanged received => RequesterId: 82e572be-15c9-430e-8a59-
d7cecc5908a0 - CorrelationID: Demo-65146b4d-4031-4aed-badc-c394bcbb47d3 - Status:
UPDATE_METADATA_ERROR_EXTRACTION_CONTENT
…
12/09/2022 19:45:29 INFO - ServiceBusActor: RequestedInstallPackageStatus
received => RequesterId: 82e572be-15c9-430e-8a59-d7cecc5908a0 - CorrelationId:
Demo-65146b4d-4031-4aed-badc-c394bcbb47d3 - Status: FINISHED_ERROR_METADATA -
SenderMessage: Metadata content corrupted.
```

5.2.7.3 Corrupted PackageDescription.json – localUI.log

Manipulated PackageDescription file, for example invalid json – package will not appear on the user interface:

```
12/09/2022 20:02:09 INFO - PackageDescriptionValidatorActor:
ValidatePackageDescription received => G:\demo_1.0.0\PackageDescription.json
12/09/2022 20:02:09 INFO - PackageDescriptionInfo: MapPackageDescription received
=> Requestor: 4af0af89-ba5a-4625-9644-db50de49cd98
12/09/2022 20:02:09 now supervising
akka://SystemManagementUI/user/PackageDescriptionInfo/$f
12/09/2022 20:02:09 DEBUG - PackageDescriptionMapActor => started.
12/09/2022 20:02:09 Started (SysMgm.UI.Akka.Actors.PackageDescriptionMapActor)
12/09/2022 20:02:09 After parsing a value an unexpected character was
encountered: S. Path 'PackageVersion', line 10, position 3.
Newtonsoft.Json.JsonReaderException:
…
12/09/2022 20:02:09 ERROR - PackageDescriptionValidatorActor:
PackageDescriptionMapped received => After parsing a value an unexpected
character was encountered: S. Path 'PackageVersion', line 10, position 3.
12/09/2022 20:02:09 DEBUG - PackageDescriptionMapActor => started.
12/09/2022 20:02:09 Restarted (SysMgm.UI.Akka.Actors.PackageDescriptionMapActor)
12/09/2022 20:02:09 ERROR - PackageScannerActor: PackageDescriptionValidated
received => Package Description Invalid: G:\demo_1.0.0\PackageDescription.json,
Cause: After parsing a value an unexpected character was encountered: S. Path
'PackageVersion', line 10, position 3.
```

```
Manipulated PackageDescription file, for example: changed content like version
number – package will not appear on the user interface:

12/09/2022 20:06:04 INFO – PackageDescriptionValidatorActor:
ValidatePackageDescription received => G:\demo_1.0.0\PackageDescription.json
…
12/09/2022 20:06:04 INFO – PackageDescriptionValidatorActor:
PackageDescriptionMapped received => PackageDescription: Demo
…
12/09/2022 20:06:04 INFO – SignatureValidationActor: ValidateSignature received
=> RequesterId: e6319218-be33-4cb0-8ef7-9d107ea5480d – Directory:
G:\demo_1.0.0\PackageDescription.json
12/09/2022 20:06:04 ERROR – PackageDescriptionValidatorActor: SignatureValidated
received => Signature invalid
```

5.2.7.4 Wrong hash– sysmgm-executor.log

Wrong hash can occur if installer file has got corrupted, e.g., download error, error on USB stick, virus etc.

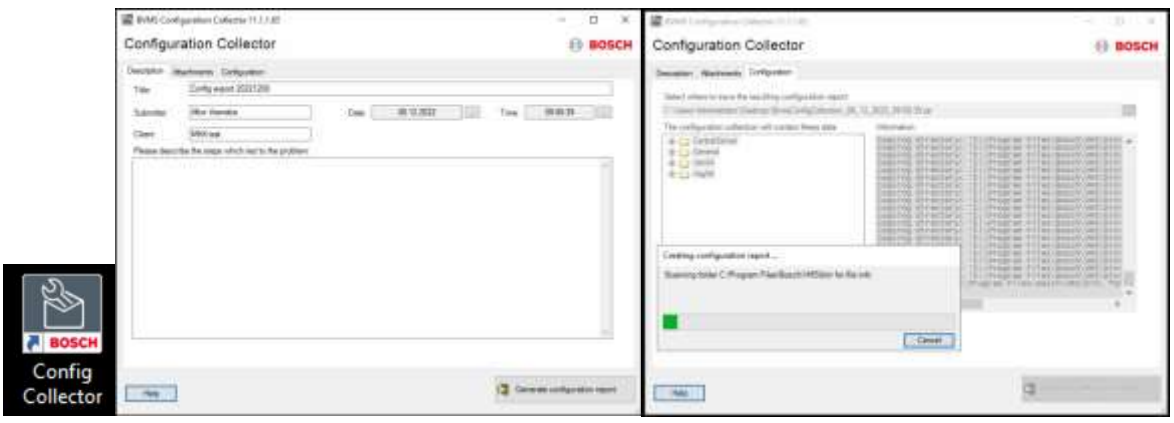
```
12/09/2022 09:33:17 INFO – ClusterProcessActor =>
================================================================================
==================== SEQUENCE RECEIVED
…
12/09/2022 09:33:20 INFO – ProcessActor => Executing a new Start Process command.
FileName: powershell.exe – Arguments: sudo scoop install Demo --global
12/09/2022 09:33:20 INFO – ProcessActor => StartProcess, creating a start info.
12/09/2022 09:33:20 INFO – ProcessActor => Executing Process.Start.
12/09/2022 09:33:23 INFO – ProcessActor => Installing 'Demo' (1.0.0)
[64bit]Downloading
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\Demo_1.0.0.msi (125.3 MB)...
Checking hash of Demo_1.0.0.msi ... ERROR Hash check failed!
App:         bosch/Demo
URL:         C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\Demo_1.0.0.msi
First bytes: D0 CF 12 E0 A1 B1 1A E1
Expected:    ba561121523247ff417ee1b1ffeb69d7ca4b4443ec2fc938d84668f398fd9ead
Actual:      4a48f018d7904da7f228341e173c274b30dd3d624c79425f526264cbd625dc9f
Please try again or create a new issue by using the following link and paste your
console output:
https:////
12/09/2022 09:33:23 INFO – ProcessActor => Executing a new Start Process command.
FileName: powershell.exe – Arguments: sysmgm-install-validation True Demo
12/09/2022 09:33:23 INFO – ProcessActor => StartProcess, creating a start info.
12/09/2022 09:33:23 INFO – ProcessActor => Executing Process.Start.
12/09/2022 09:33:25 INFO – ProcessActor => Installed apps matching 'Demo':
  Demo 1.0.0 *failed*
  Demo 1.0.0 *global* *failed*
 *Failed installation identified. Starting cleanup process...*
```

5.2.7.5 Successful installation – sysmgm-executor.log

```
12/09/2022 20:14:35 INFO - ClusterProcessActor =>
================================================================================
SEQUENCE RECEIVED
…
12/09/2022 20:14:35 INFO - ProcessActor => Executing a new Start Process command.
FileName: powershell.exe - Arguments: taskkill /IM DemoPackage.exe /F
…
12/09/2022 20:14:35 INFO - ProcessActor => Executing a new Start Process command.
FileName: powershell.exe - Arguments: sudo scoop cache rm Demo
…
12/09/2022 20:14:36 INFO - ProcessActor => Executing a new Start Process command.
FileName: powershell.exe - Arguments: sudo scoop update
…
Scoop was updated successfully!
…
12/09/2022 20:14:38 INFO - ProcessActor => Executing a new Start Process command.
FileName: powershell.exe - Arguments: sudo scoop install Demo --global
12/09/2022 20:14:38 INFO - ProcessActor => StartProcess, creating a start info.
12/09/2022 20:14:38 INFO - ProcessActor => Executing Process.Start.
12/09/2022 20:14:45 INFO - ProcessActor => Installing 'Demo' (1.0.0)
[64bit]Downloading
C:\ProgramData\Bosch\SysMgmService\cache\demo_1.0.0\Demo_1.0.0.msi (125.3 MB)...
Checking hash of Demo_1.0.0.msi ... ok.
Extracting Demo_1.0.0.msi ... done.
Linking C:\Program Files\Bosch\SysMgmService\apps\Demo\current => C:\Program
Files\Bosch\SysMgmService\apps\Demo\1.0.0
Creating shim for 'DemoPackage'.'Demo' (1.0.0) was installed successfully!
…
 Valid installation identified.
================================================================================
==================================== SEQUENCE EXECUTED
```

5.3 BVMS logs

To export BVMS logs, click on the Config Collector shortcut located on the Windows desktop.



The process of using these logs for troubleshooting BVMS installations falls outside the scope of this DIP troubleshooting guide. This aspect is covered comprehensively in BVMS troubleshooting documentation and training materials.

5.4 Locating DIP Serial and BMC Information

The DIP serial number can be located through various methods:

- Run DIVAR IP System Manager from the desktop, which displays device information:

- Use the command "`wmic bios get serialnumber`" in Command Prompt or PowerShell:

```
PS C:\Users\Administrator> wmic bios get serialnumber
SerialNumber
404800237614360001
```

BMC information cannot be retrieved within the software and is physically provided on the device itself. It can be located below the BMC port on the back of the device (the label will read “BMC” on the released product):

How to **configure** BMC, can be found in the **Installation Manual** in the **System setup** chapter; **Configuring BMC settings** as well as in this guide.

5.4.1 How to reset a lost BMC password

This procedure is taken from an Engineering document “DIP-74 Recover system to default IPMI password” from 31 May 2024, version 9.

5.4.1.1 Scope

This procedure instructs on how to recover the IPMI password and set a new password on the DIVAR IP all-in-one 7000 4th gen (DIP-74xx).

5.4.1.2 Requirements

- A Bosch DIVAR IP all-in-one 7000 4th gen system must be in place.
- Access should be available using the local user BVRAdmin.

5.4.1.3 Procedure steps

1. Log in to DIVAR IP with the BVRAdmin user.
2. Open the Command Prompt as Administrator.
3. Navigate to the path C:\Program Files\ASUSInbandAP\ipmitool.

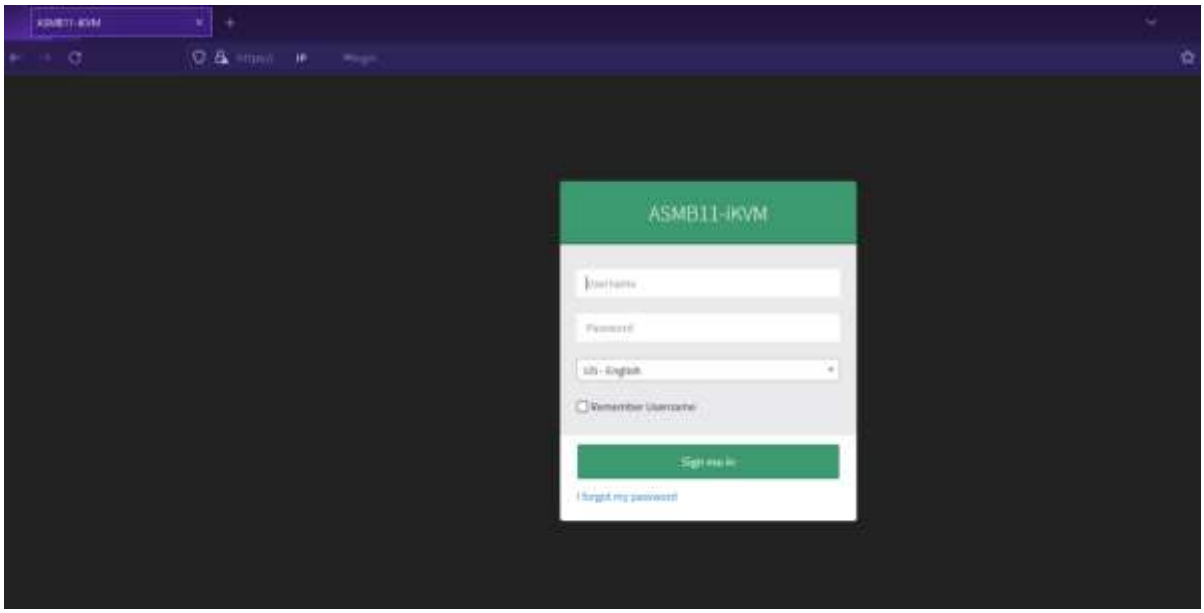
4. To display the current users, execute the command:
   `ipmitool.exe –I ms user list 1`

   VERY IMPORTANT: Only change the password for the **admin** user, do not change any of the other users’ passwords. **Administrator** and **ASUSInbandUser** are used for **internal** functions.
   Do not change these passwords, as doing so may cause some features to stop working.

5. To reset the password, execute the command:
   `ipmitool.exe –I ms user set password ID newpassword`

   Note: Confirm the ID of the desired user and create a new strong password.

6. Using a web browser, enter the IP address of the BMC interface, along with the username and new password as defined in the previous step.

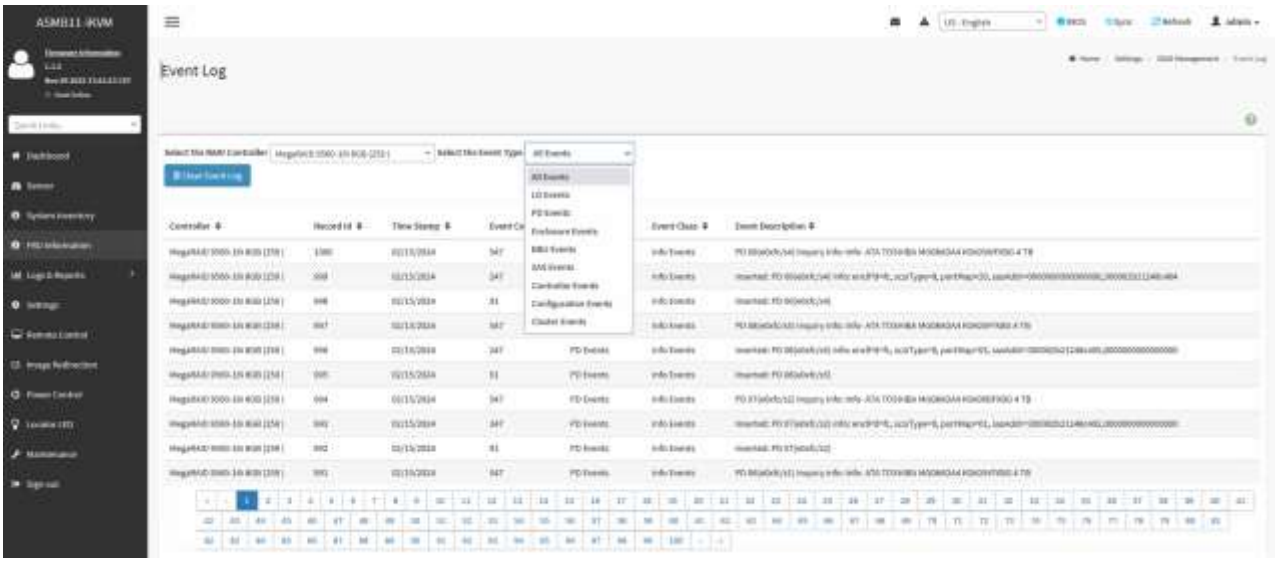


5.5 BMC logs

While it is possible to export some logging from the BMC interface, it is recommended by ASUS to use the ASUS Inband Tool for this purpose instead. If the Operating System is not responsive for any reason, it is a backup solution. In this event however, ASUS points to the startup codes seen on the LED display at the back of the unit, as well as on the boot-up screen's right hand side corner, for all needed troubleshooting information.

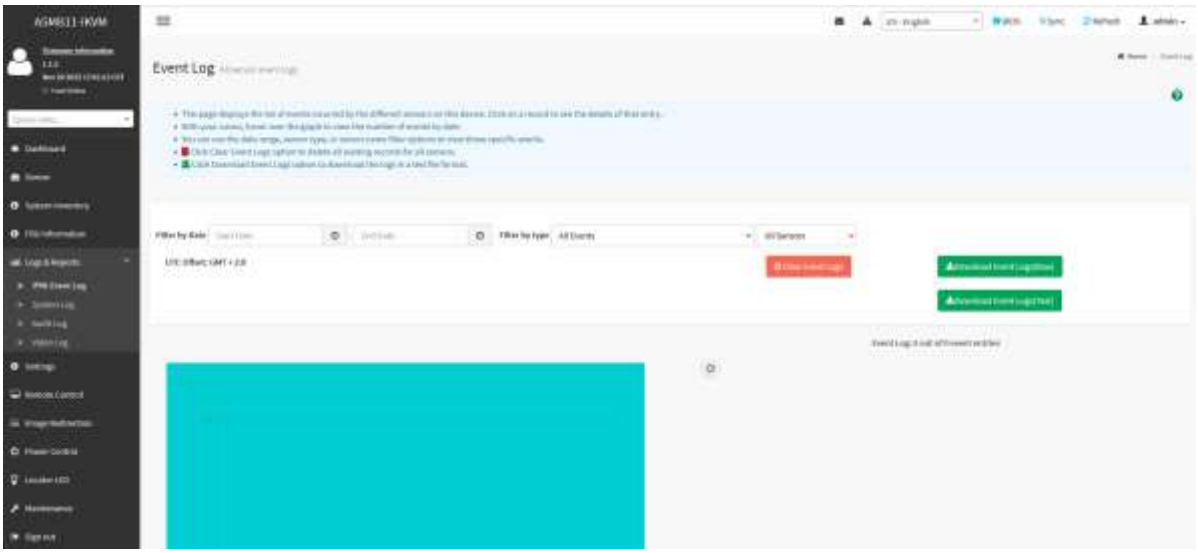
5.5.1 RAID Event Log

The events recorded for the RAID array can be viewed through BMC but cannot be exported. To access and view the logs, go to **Home > Settings > RAID Management > Event Log**. The events can be filtered by event type, but they can only be viewed and not exported. If access to the OS is impossible, creating a screenshot of the RAID events here would be the best solution.


ASMB11-iKVM
Event Log

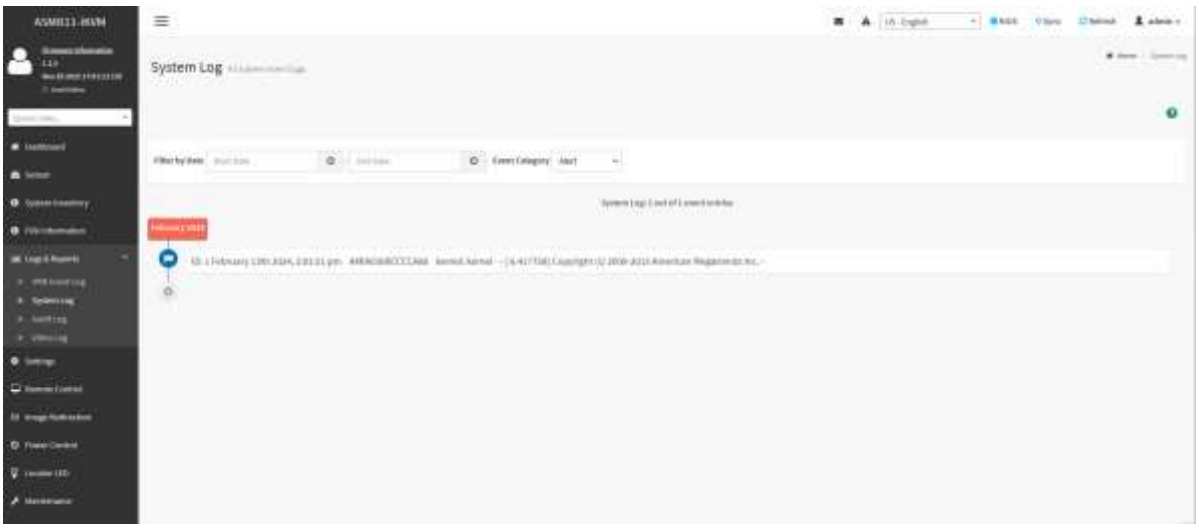
5.5.2 IPMI Event Log

The Logs & Reports > IPMI Event Log page displays the list of events incurred by the different sensors on the device. Click on a record to see the details of that entry. Hover over the graph to view the number of events by date, You can use date range, sensory type, or sensor name filter options to view specific events. Click the "**Clear Event Logs**" option to delete all existing records for all sensors. Click the "**Download Event Logs**" option to download the logs in a raw or text format.



5.5.3 System Log

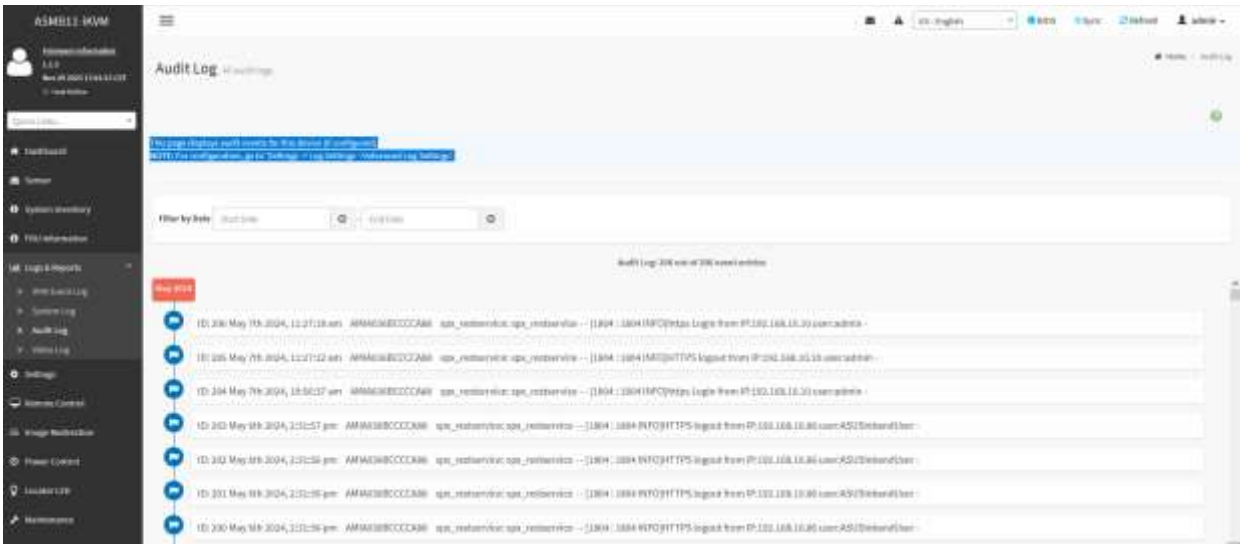
This page displays logs of system events for the device (if the options have been configured). **NOTE**: Logs must be configured under "**Settings > Log Settings >Advanced Log Settings**" to display any entries. Filtering options are also available for this and all logs in this section. It is not possible to download any logs from this page.



5.5.4 Audit Log

This page displays audit events for this device (if configured).
NOTE: For configuration, go to "**Settings > Log Settings >Advanced Log Settings**".

It is not possible to download any logs from this page.



5.5.5 Video Log

This page displays available recorded video files (if the options have been configured).

NOTE: For this configuration, go to "**Settings > Video Recording > Auto Video Settings > Video Trigger Settings**".

It is not possible to download any logs from this page.

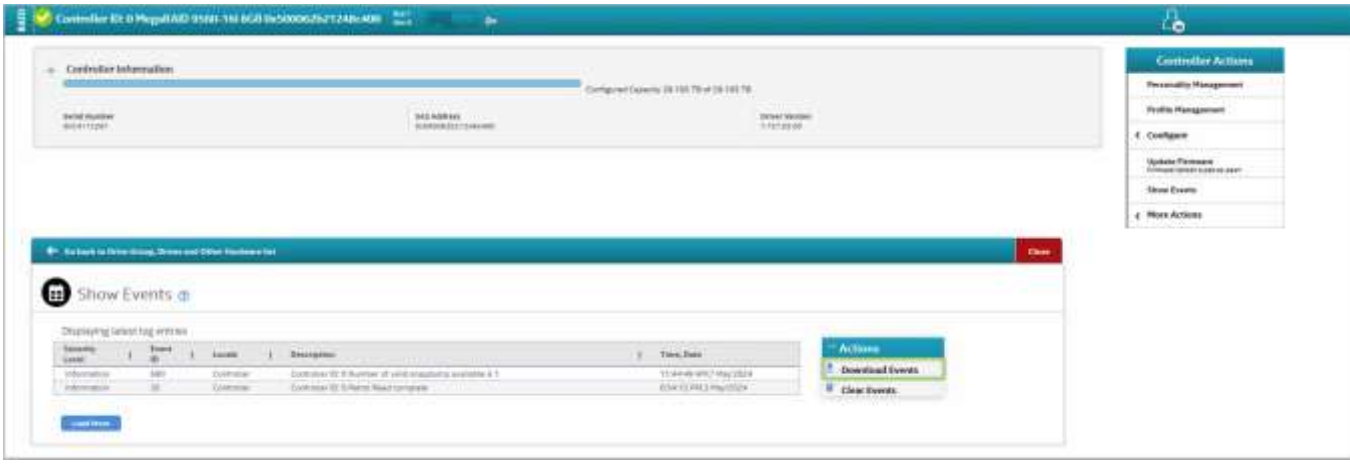
5.6 LSA Logs

As mentioned, the ASUS Inband Tool is the preferred log collection tool, all relevant logs can be gathered from there for ASUS Tech Support. However, LSA also has a log collection option, these logs only pertain to the RAID configuration on the device.

Once logged into the LSI Storage Authority service on the server (use the LSA shortcut on the Windows Desktop for ease of connection), there are two possible options for log collection. The

first is to “Download Server Report” on the upper right-hand side of the screen, this downloads an extensive log collection, which incorporates various files and logs pertaining to every aspect of the RAID hardware and configuration. If only an Event Log is required, a simpler option is available by clicking **Show Events** under the **Actions** header.

This provides an overview of the events on the RAID controller, note that the buffer for this log seems rather limited, so only recent events will show. Click the option “**Download Events**” to download a JSON-formatted log with a longer time frame than the web page listing.



5.7 POST codes

Also titled “**Boot up Q codes**” by ASUS, during boot, the system will display codes on the bottom right of the screen and on a small LED display on the back of the unit. Here are some useful codes to be aware of:

- 0x55: Memory not installed or error.
- 0x58: CPU self-test failed.
- 0x5A: CPU error.
- 0xdA: Boot option failed.

6 Monitoring

6.1 ASUS Inband Tool

A How-to video is available showing the options of the tool in detail; for DIP-74xx "**Monitoring the System**"

6.1.1 Overview

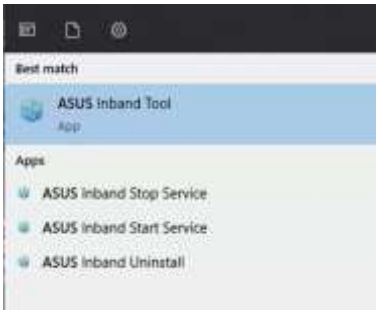
The ASUS Inband Tool covers the same role as SuperDoctor5 did on the DIP-73xx. It monitors the hardware health or availability in real-time and provide alerts to administrators, and it also provides health information to Remote System Management if it is used.

Its key features are:

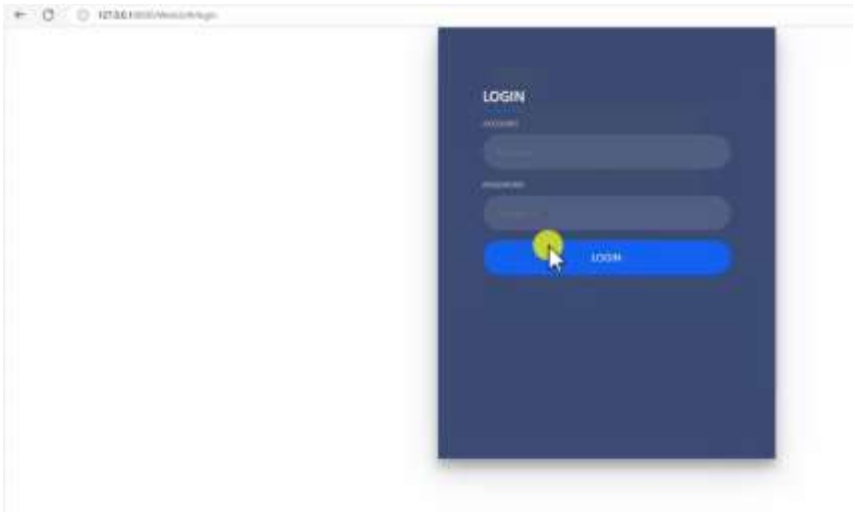
- **Supports monitoring, control, and management functions.**
  - RAID and disk health, both storage and OS,
  - Power status & health,
  - fan health and speed,
  - various hardware temperatures,
  - various hardware voltages,
  - chassis intrusion,
  - power consumption,
  - and memory health.
  - Information on the system and its parts;
    - computer summary information,
    - CPU and GPU information,
    - Memory information
    - Hard drive information
    - Network Interface Card information
    - Logs:
      - Audit Log
      - Event Log
      - SEL Log
- **Provides SNMP extensions for network management system.**
- **Easy to use Web-based interface.**

ASUS Inband Tool is specifically developed for the DIP-74xx, so is not available from ASUS directly.

Open ASUS Inband Tool from the Windows Start Menu, or by clicking the icon in the Tools folder:



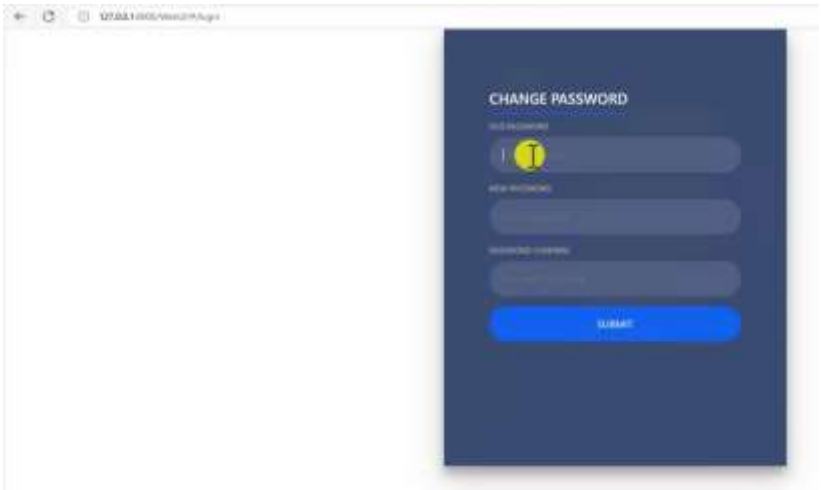
6.1.2 Logging in



To log in to the tool initially, use these credentials:

- username: admin
- password: admin

Then you need to immediately change the password to a secure one adhering to the usual rules, in order to proceed:

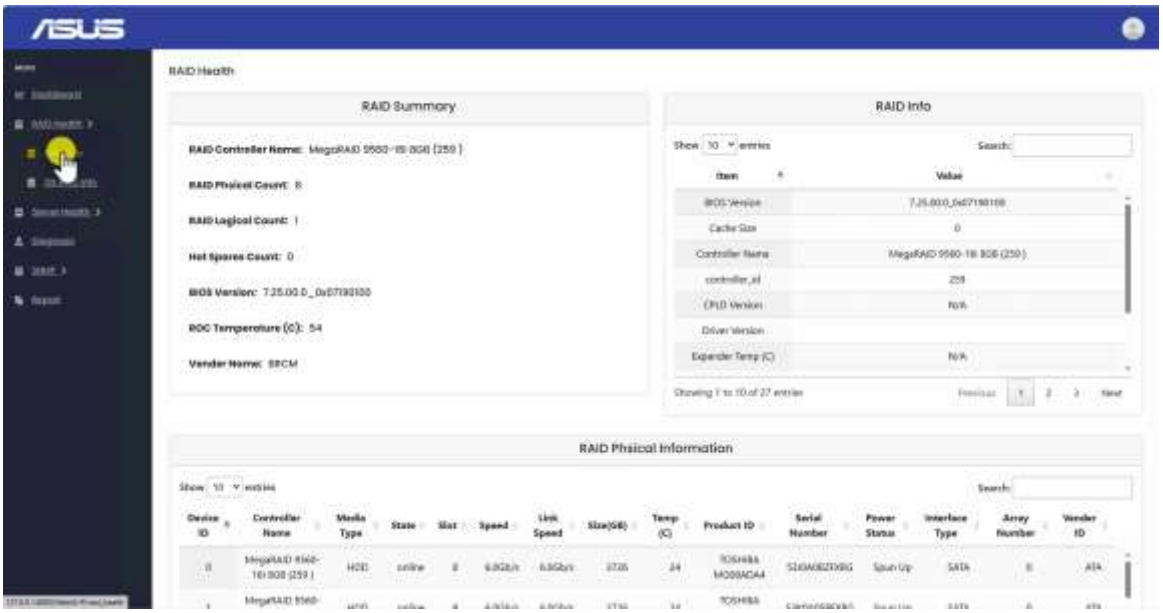


6.1.3 Dashboard

You will be presented with the dashboard which gives information on the health of various components in the system right away. The following chapters will describe the various menu items.

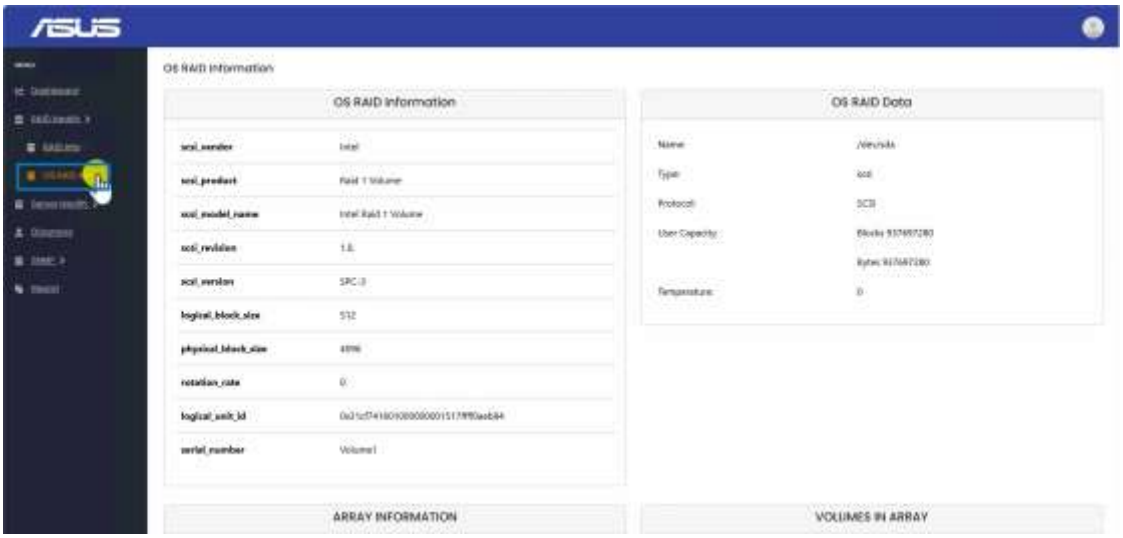
RAID Health

RAID Health is split into RAID Info – for the storage HDDs, and OS RAID Info – for the two Operating System HDDs:



In the RAID Info screen you will find details on the RAID card hardware as well as the HDD hardware details. The screen only shows RAID information, rebuilding etc. is done through LSA.

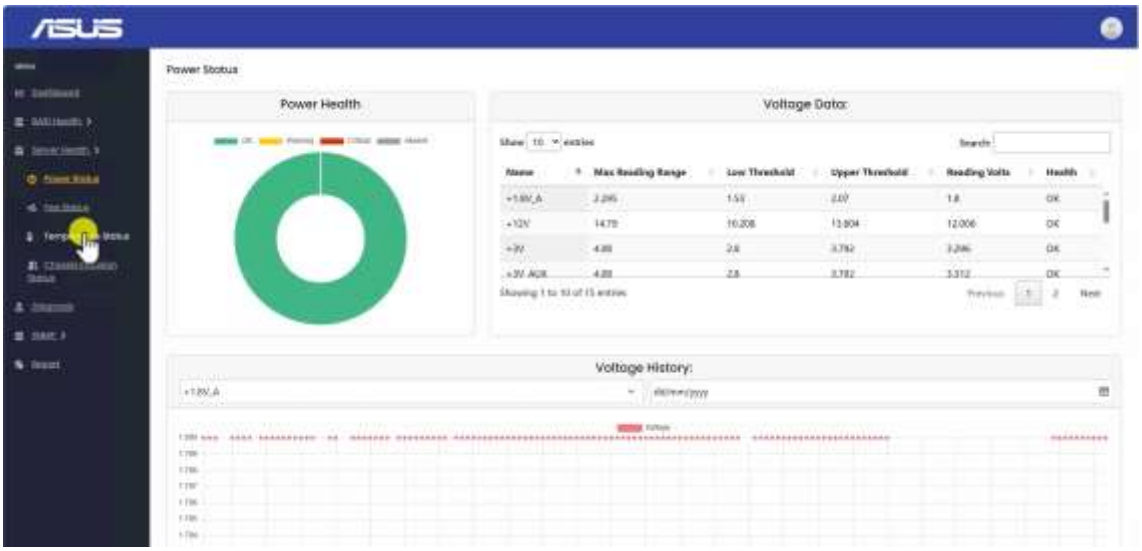
At the bottom of the screen you will find the RAID Event Log.



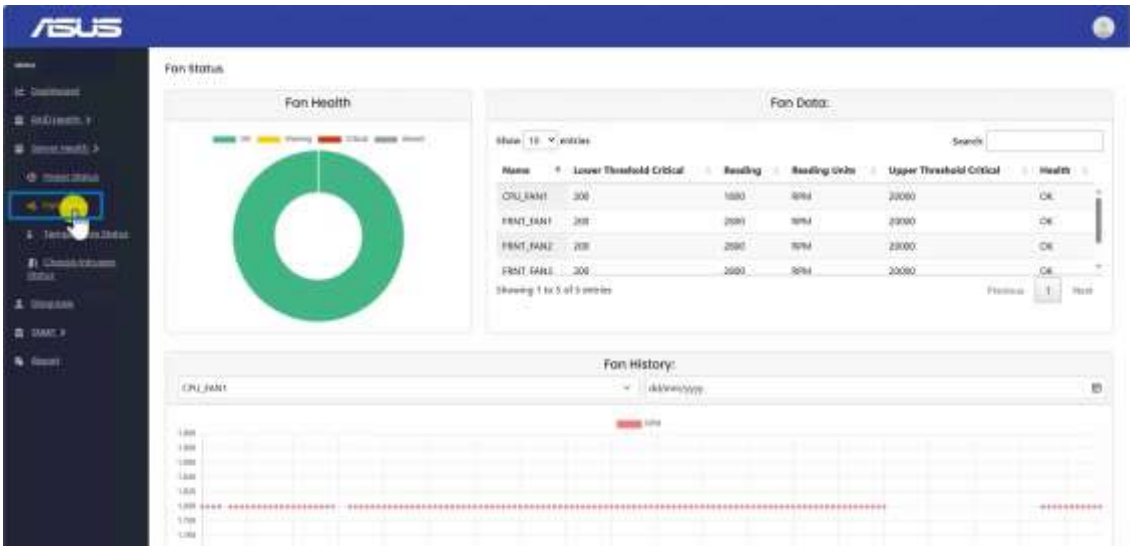
The OS RAID Info screen shows basic information, mount data, Intel array information, volumes in the array and details on the disks.

6.1.4 Server Health

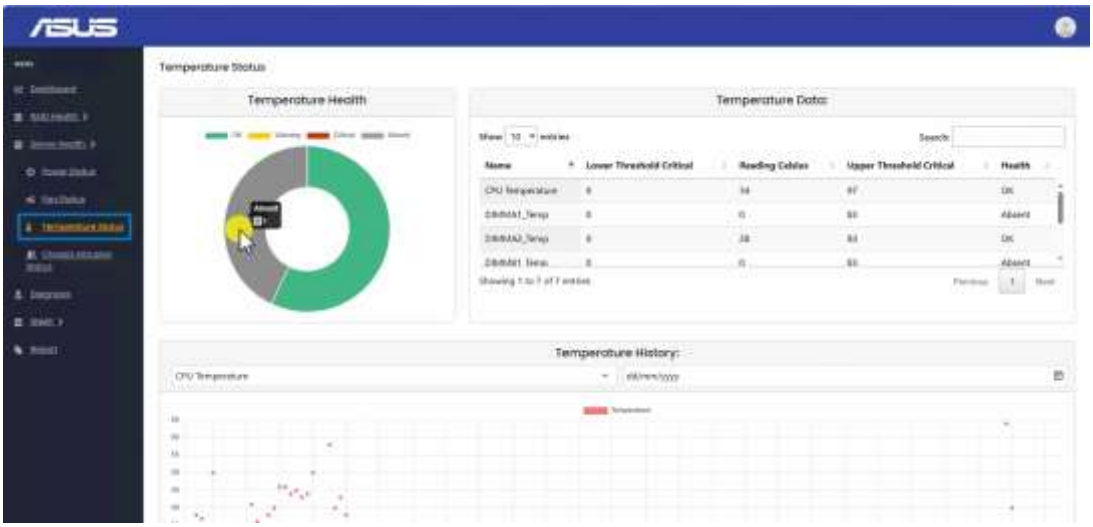
Server Health is split into Power Status, Fan Status, Temperature Status and Chassis Intrusion Status:



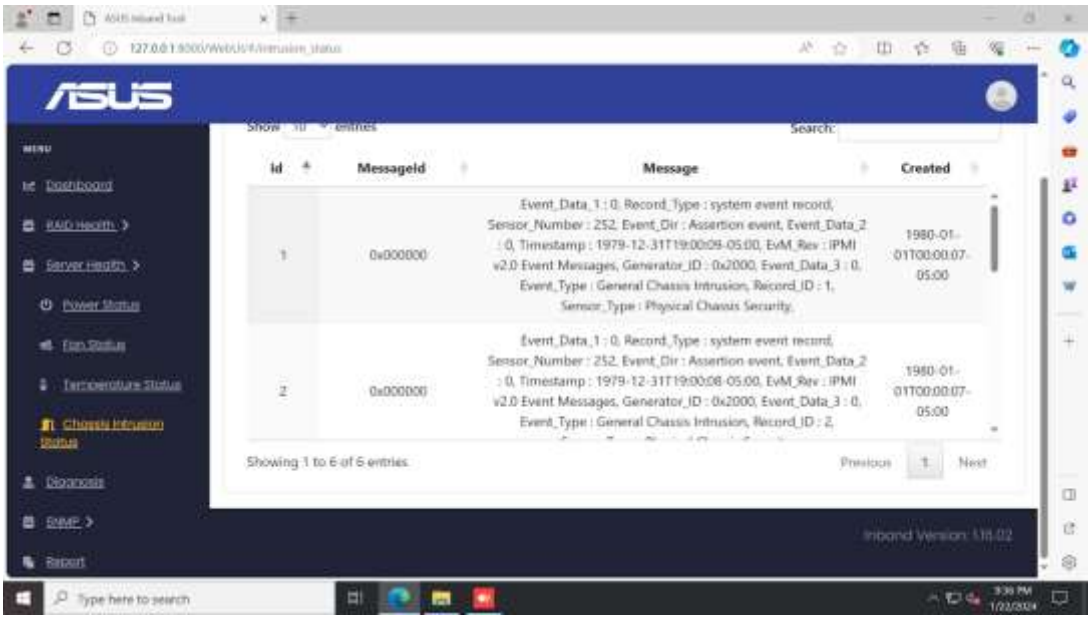
Power Status shows how the power supplies are doing and the voltage history as well. It doesn't include the PSU sensor, that is covered in the System Error Log (SEL) if an event occurs.



Fan Status shows health, data, and history for all fans in the unit.

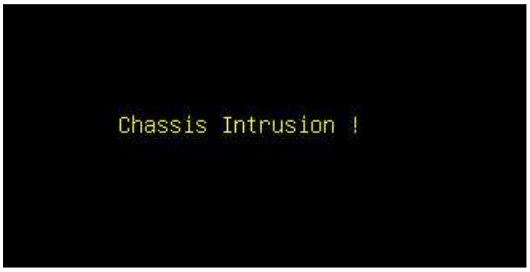


Temperature Status shows details on temperatures of various parts of the system, like CPU, memory, and RAID as well as their historical temperatures.



Chassis Intrusion Status is used to determine of the system was tampered with. If the chassis intrusion sensory is triggered, information will show here.

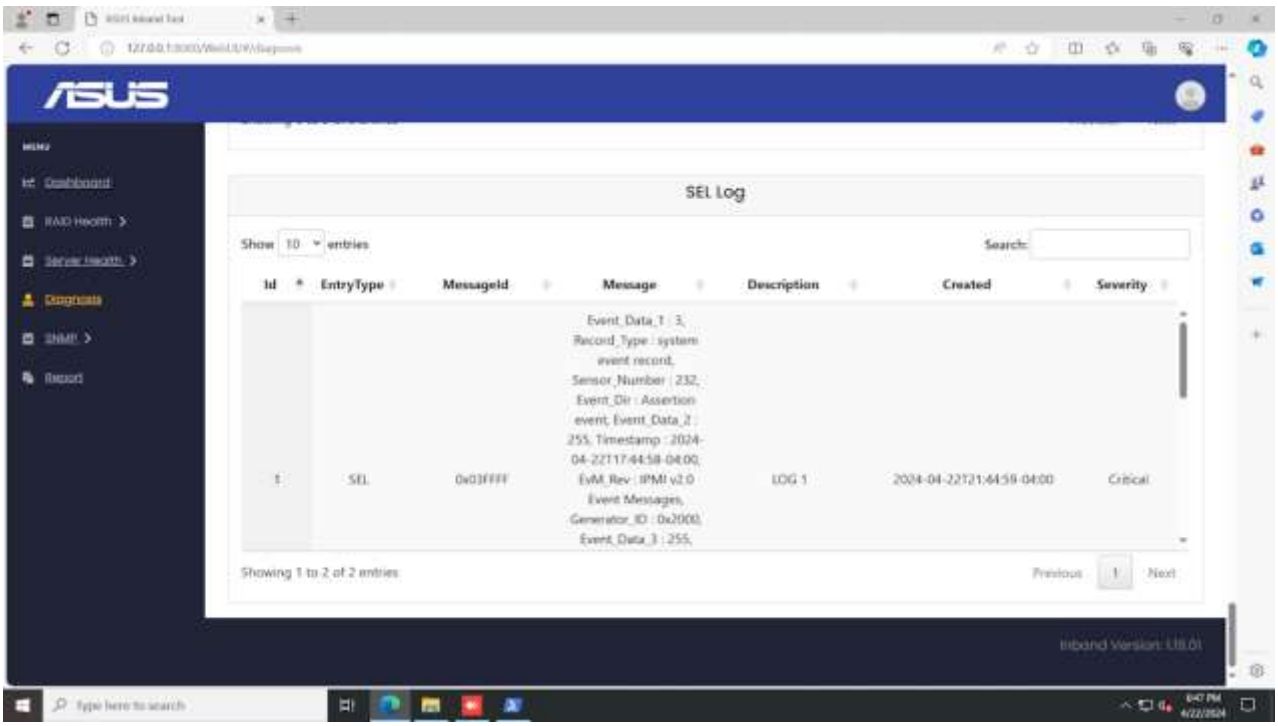
Chassis intrusion warnings will also show at boot-up when the system's top cover has been opened. It will show this warning during POST:



6.1.5 Diagnosis

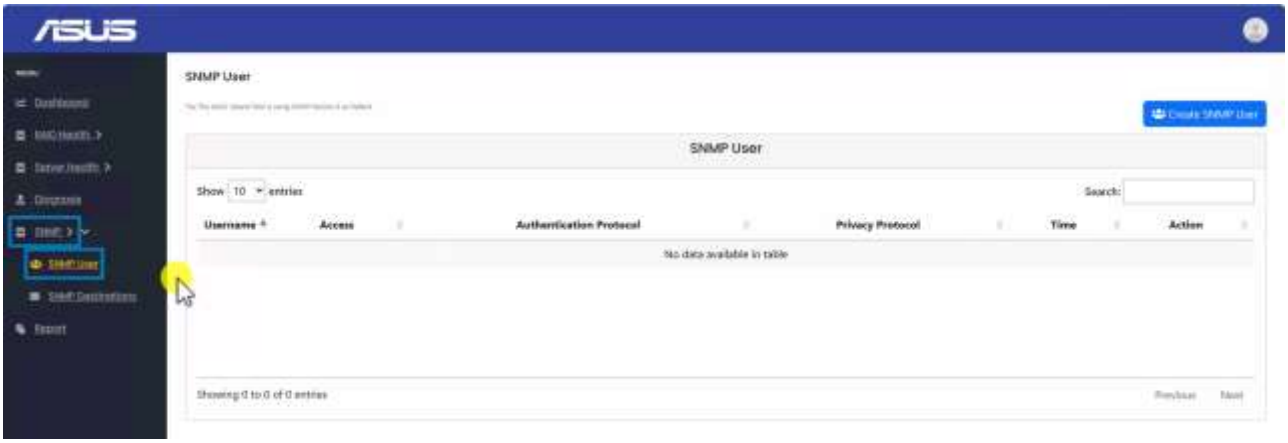
The Diagnosis screen shows details about Utilization of hardware components, contains Computer Summary Information, which gives details on the system itself, similar to Windows System Info. More details on the CPU, GPU, BMC hardware and software adapter, physical memory, local drives C, D and E, and services using the network interface under NIC Information.

The SEL (System Event Log) Log. This log indicated events that may impact system stability or issues:



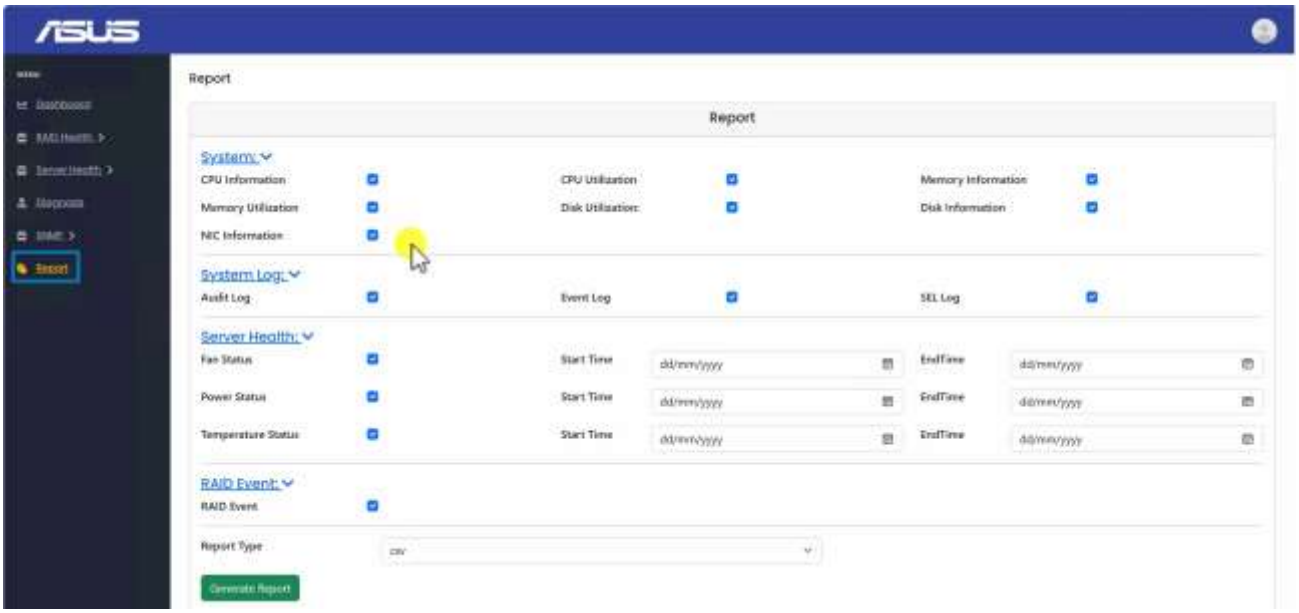
6.1.6 SNMP

In the SNMP screen you can set-up SNMP users and destinations to distribute the information from the ASUS Inband Tool through SNMP.



6.1.7 Report

On the Report screen all information shown on the other screens can be exported into a report, enabling to choose what information to store.

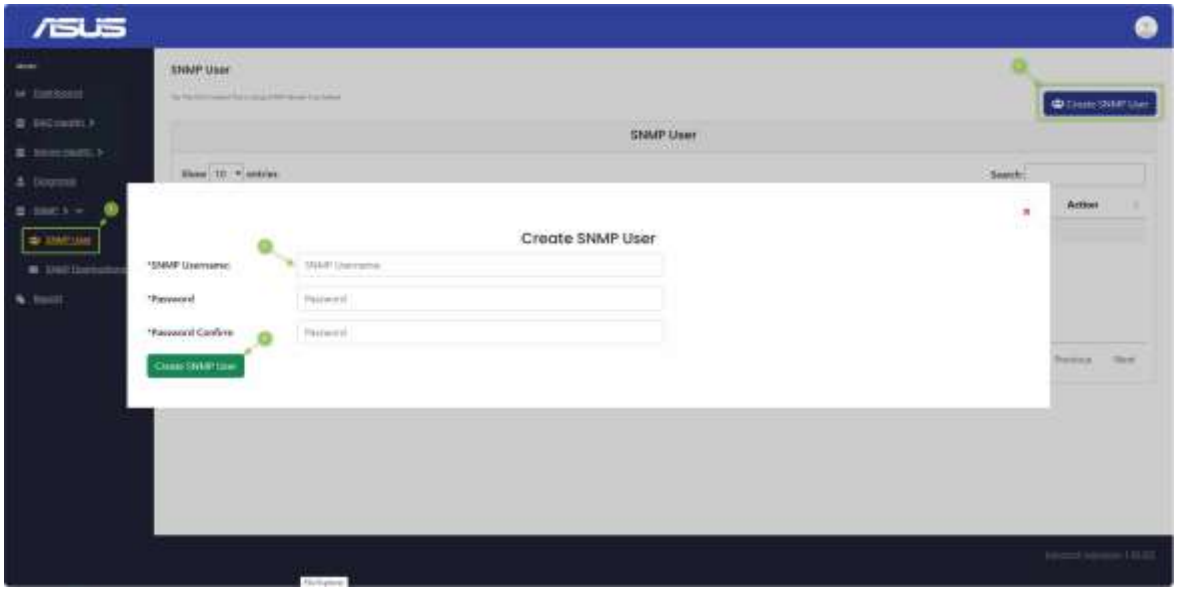


6.2 SNMP

6.2.1 Inband SNMP

The ASUS Inband Tool can be used to set up the SNMP system. Only SNMP v3 is supported for the DIP-74xx, as earlier versions pose security risks. To begin, a user must be defined to receive the SNMP information. Here are the steps to follow:

1. Select **SNMP** > **SNMP User** from the left-hand side menu
2. Click on the blue "**Create SNMP User**" button on the top right-hand side of the screen
3. Create a **username** and a **password** for the user
4. Select the green "**Create SNMP User**" button

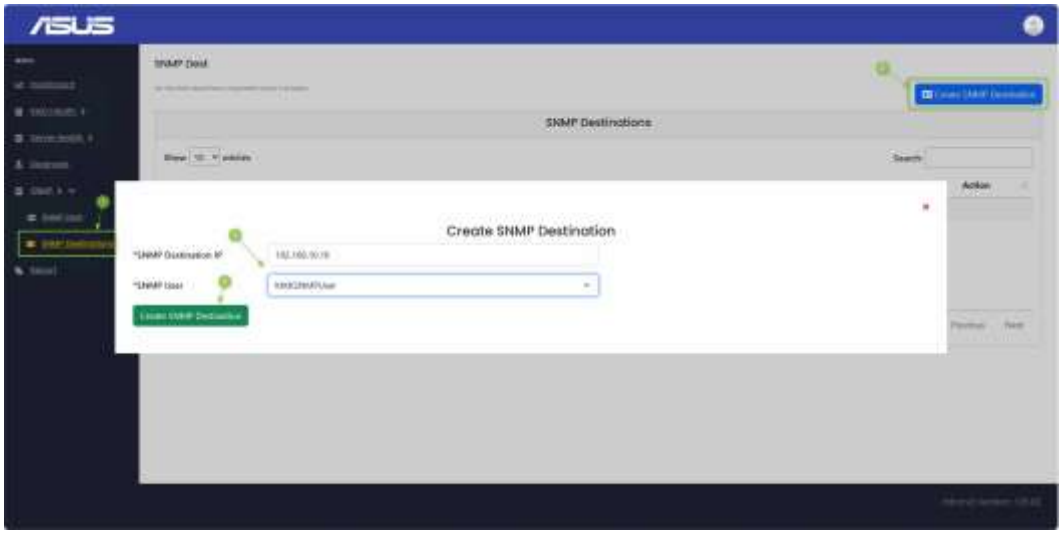


NOTE: Before proceeding, ensure that the destination has an SNMP Client set up with the configured username and password. Without a working SNMP destination, the next steps will fail with a 404 error.

Now, define the destination for the SNMP information to flow to. Here are the steps to follow:

1. Select **SNMP** > **SNMP Destinations**
2. Click on the blue "**Create SNMP Destination**" button on the top right-hand side of the screen
3. Enter the **destination IP** for the SNMP Client that you are running and fill in the **user** that was created in the previous step to receive SNMP information

4. Select the green “**Create SNMP Destination**” button



Once the server’s configuration is complete, ensure that the SNMP Client is configured correctly to receive SNMP information by sending test messages.

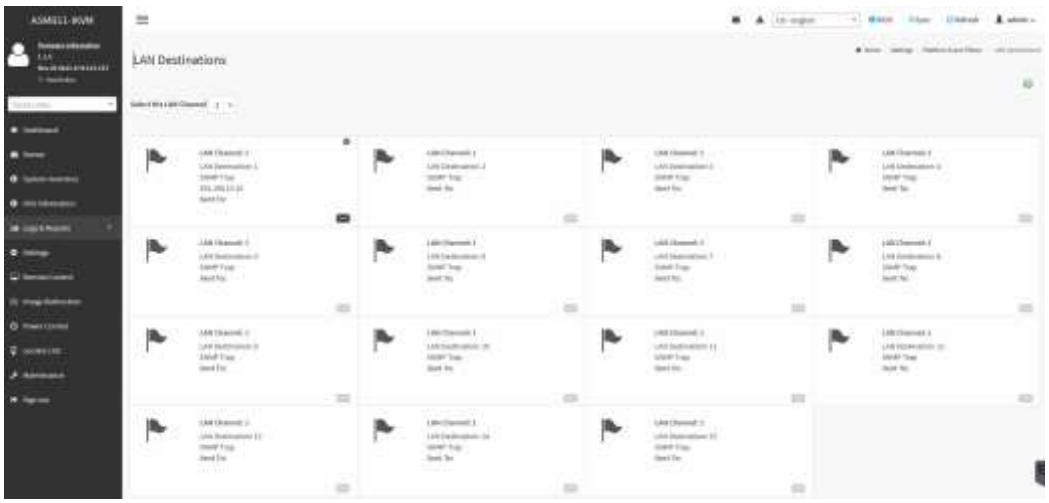
WARNING:

Currently, there is an **issue** with the Inband SNMP agent in version 1.19.1 of the ASUS Inband Tool, causing **Inband SNMP to not work, even when configured correctly**. An update package for the tool is planned to address this issue shortly.

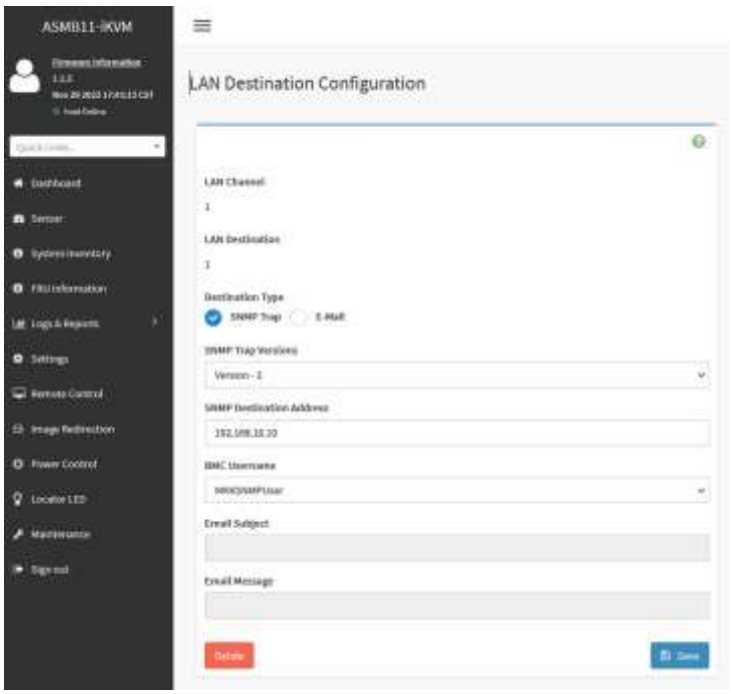
Workaround: with the SNMP settings correctly set up on the Inband Tool, SNMP will work correctly over the BMC connection instead. This may serve as a workaround for customers who want to use SNMP to gather system information on a central server..

6.2.2 Out of band SNMP using BMC

1. In a web browser, navigate to the BMC IP address and log in to the BMC environment using either the default or configured password.
2. Navigate to **Home > Settings > Platform Event Filter > LAN Destinations**. 15 SNMP destinations can be configured:

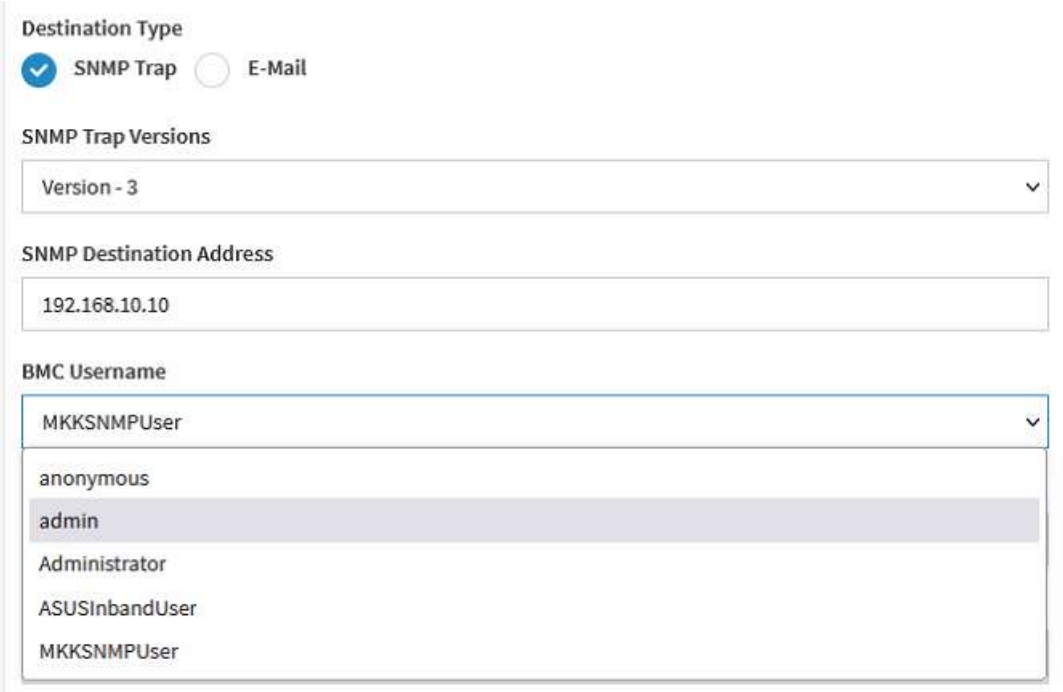


3. In this scenario, we previously configured a user and destination in the ASUS Inband Tool, and these settings can be found when opening "LAN Channel: 1".



4. Configure the “**Destination Type**” as **SNMP**, “**SNMP Trap Versions**” to “**Version-3**”

5. Configure the "**SNMP Destination Address**" to the SNMP client's IP address and username, of which several are pre-configured already.
   Note: it is not possible to configure a unique username here, if that is required, the user must be added through the ASUS Inband Tool.



6. After the configuration is complete, you can send a test alert to the destination address and check if it was received correctly.

6.3 BMC

The BMC and its interface provide a means to connect to the device remotely using an iKVM interface, which stands for virtual Keyboard-Video-Mouse interface. In previous systems, we referred to the hardware part as BMC and the software part as the IPMI protocol. However, due to security issues with IPMI, we no longer use it, and now simply refer to the entire interface as BMC.

In the DIP-74xx, the usage of the remote interface differs from that of the DIP-73xx as we now support the iKVM function, which was not supported on the DIP-73xx. Another change is that ASUS' BMC interface does not offer as many health monitoring options as SuperMicro's interface did. All of these functions can now be found in the ASUS Inband Tool.

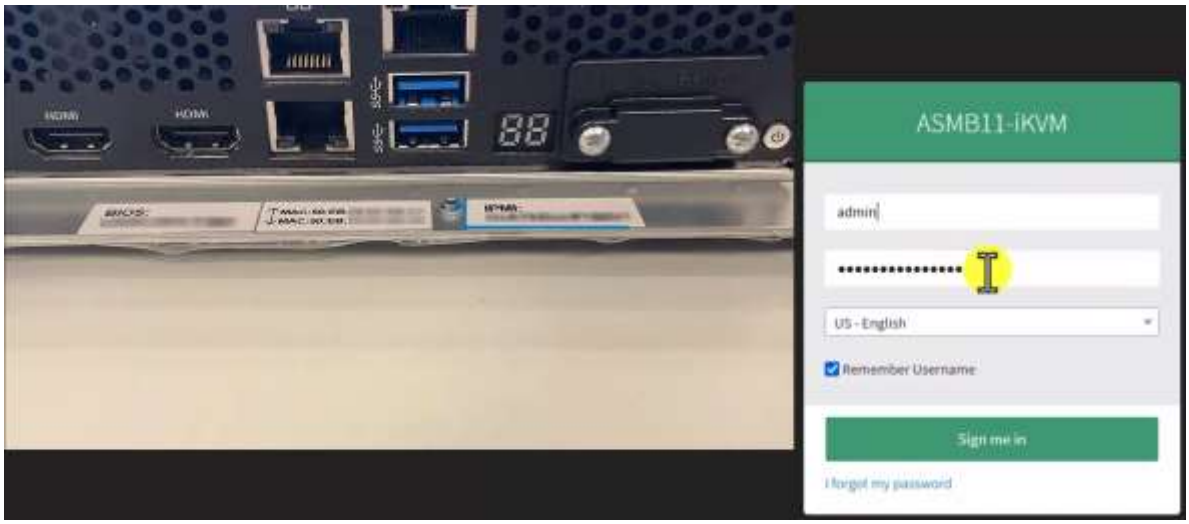
6.3.1 Configuring BMC settings

The Installation Manual includes a chapter on "**Configuring BMC settings**," which provides instructions on how to configure the BMC interface using the BIOS. Additionally, we have a **How-to video** available on this topic titled "**Configuring BMC Settings**" for the DIP-74xx.

6.3.2 Monitoring the system using the BMC interface

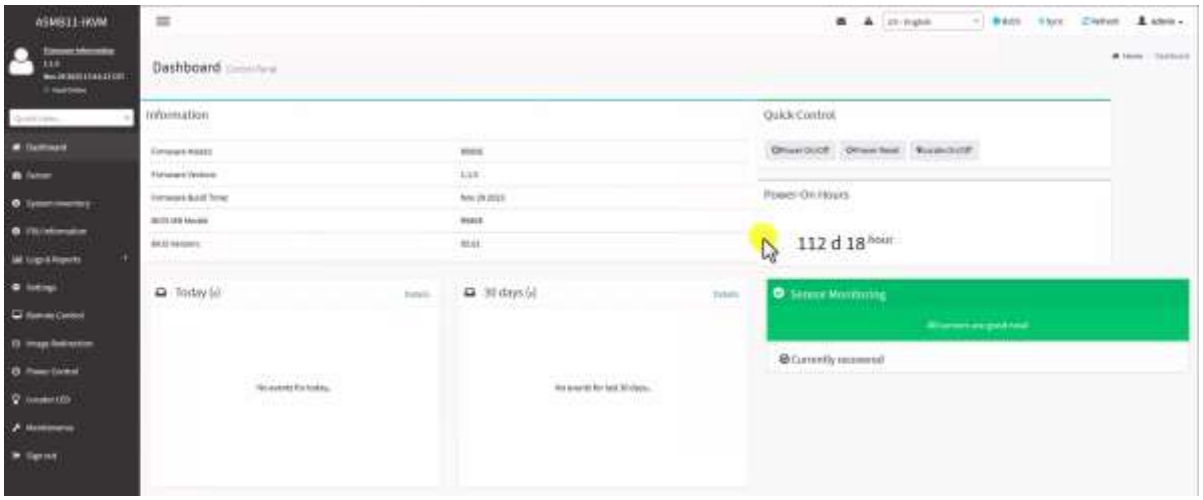
We have a How-to video available on this topic titled "**Remote operation with BMC iKVM interface**" for the DIP-74xx. In this video, we will demonstrate how to log in and control the DIP. It is important to ensure that no local monitor is connected when using iKVM, as it will interfere with the BMC connection. Here are the steps to follow:

1. In a browser, enter the DIP's BMC IP address, which is configured in the BIOS of the device. For details, refer to the Installation Manual or the previously mentioned How-to video.
2. Sign into the BMC interface using the password found on the rear of the unit:



Note that after the initial login, it is recommended to change the password. When creating the new password, please adhere to the default password rules.

3. The Dashboard shows basic information. For more details on the BMC interface, check the ASUS ASMB11-iKVM manual or https://www.asus.com/me-en/commercial-servers-workstations/asmb9-ikvm/helpdesk_manual/ .



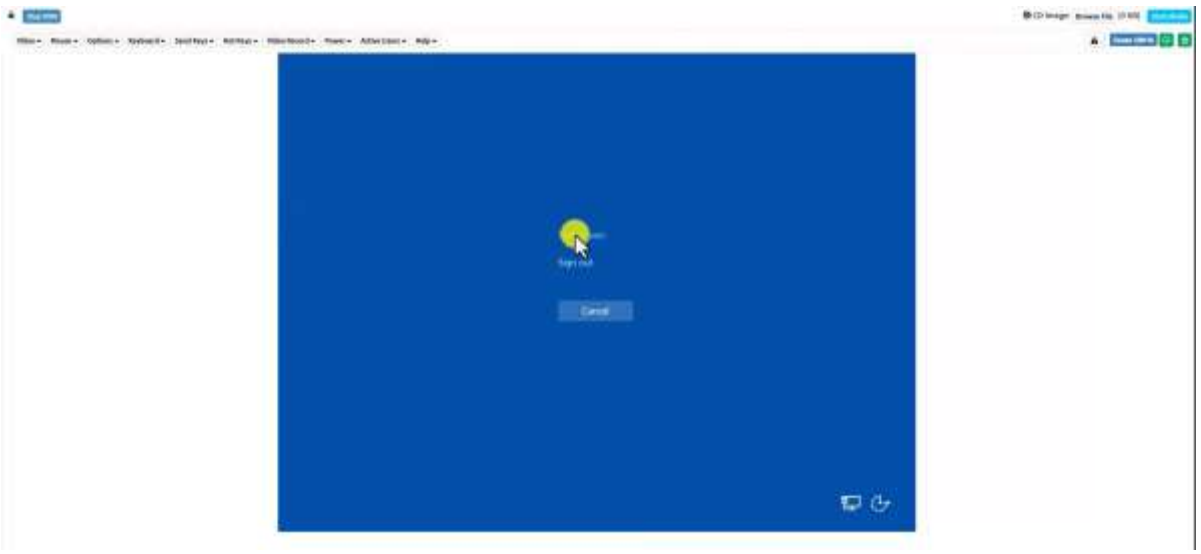
4. Select **Remote Control** in the left-hand side menu to open the iKVM page

5. Click the **Launch H5Viewer** button to launch the iKVM interface

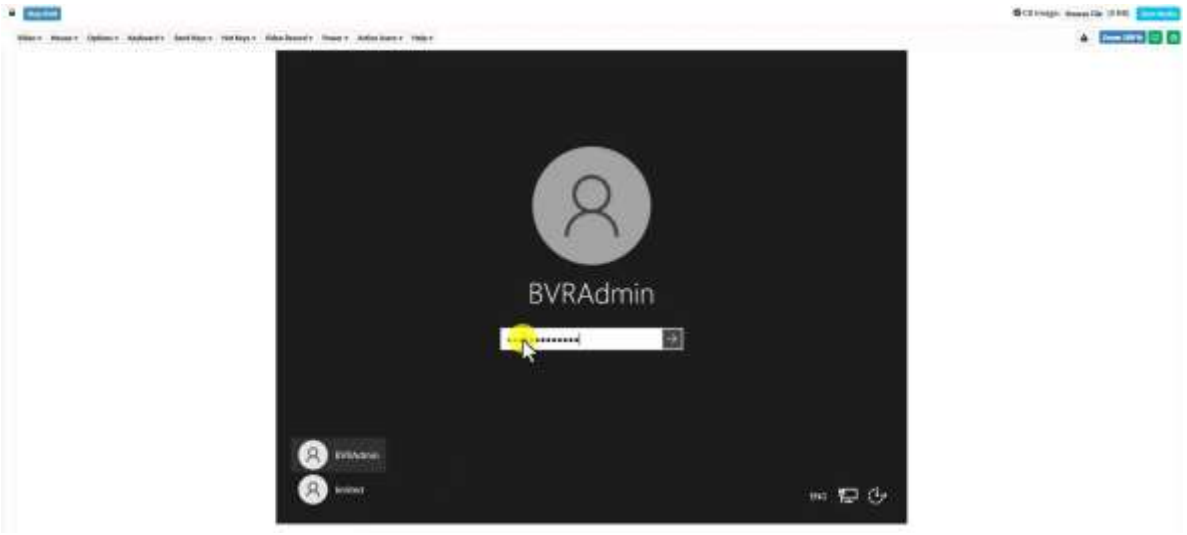
6. You will be connected to the DIP-74xx and will likely see the BVMS Desktop/kiosk mode screen.

7. To log into Windows, click on the **Send Keys** menu in the KVM menu bar at the top of the screen, and then select **CTRL+ALT+DEL** to open the Windows user menu.

8. Select "**Switch user**" and then immediately press and hold the **Shift** key to access the Windows lock screen.



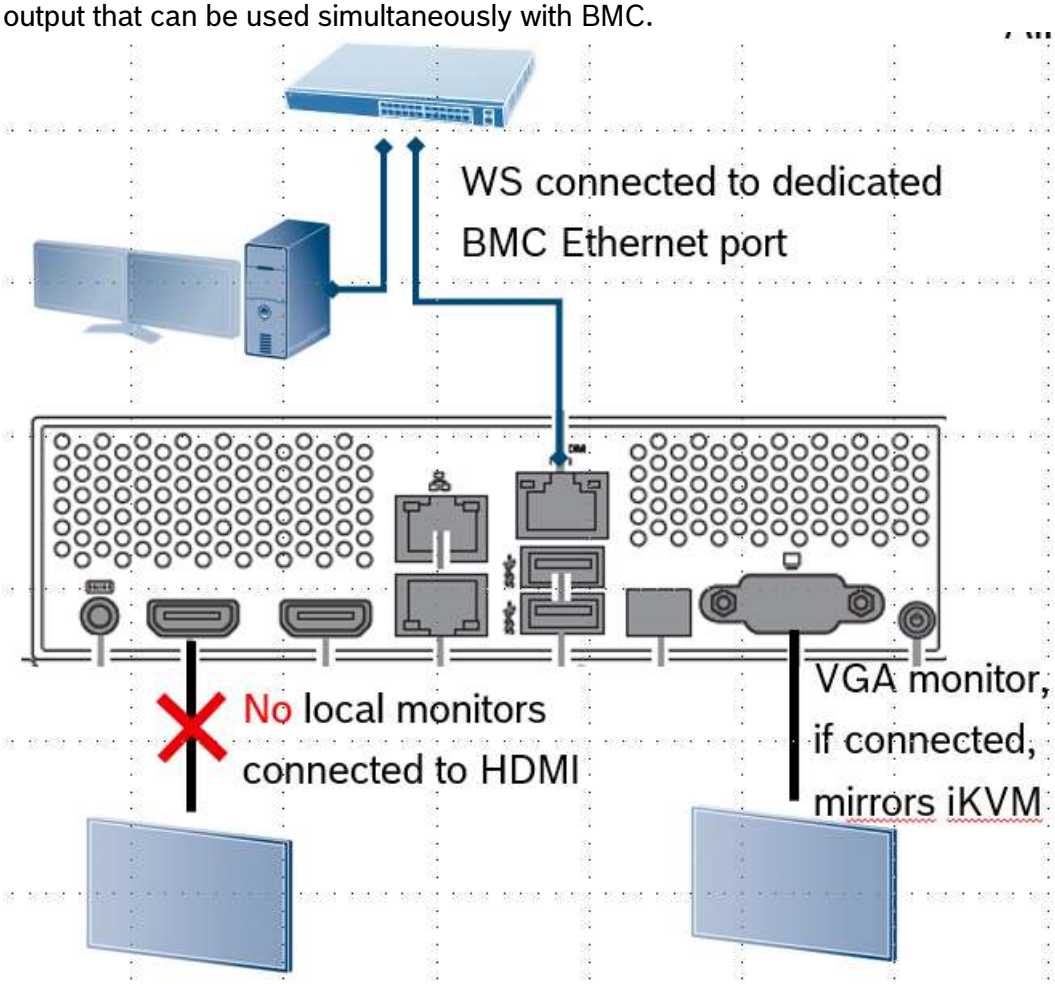
9. Use the **Send Keys** menu again to select **CTRL+ALT+DEL** and log in to Windows with the correct credentials.



10. You can now do anything on the machine remotely using the BMC interface, including restarting the unit without losing the connection.

6.3.3 Local monitor with BMC connected

The HDMI connections are disabled when the BMC connection is active, but the unit has a VGA output that can be used simultaneously with BMC.



To connect a VGA monitor, remove the cover and connect the monitor to the VGA port. The output will mirror the iKVM output, but the resolution is limited, and transcoding is not available. Both iKVM and VGA output are only used for administrative purposes, but all setup and operation steps are available via BMC iKVM:

- BIOS
- Recovery menu and operation
- OS initial setup
- Software Selection screen
- System Manager operation
- Kiosk screen (BVMS Desktop)
- Windows OS & applications

6.3.4 Updating BMC firmware

You may need to update the BMC firmware at some point. Only Bosch-approved BMC firmware versions are supported, and Bosch will provide the necessary firmware, not ASUS. The following steps outline the update process.

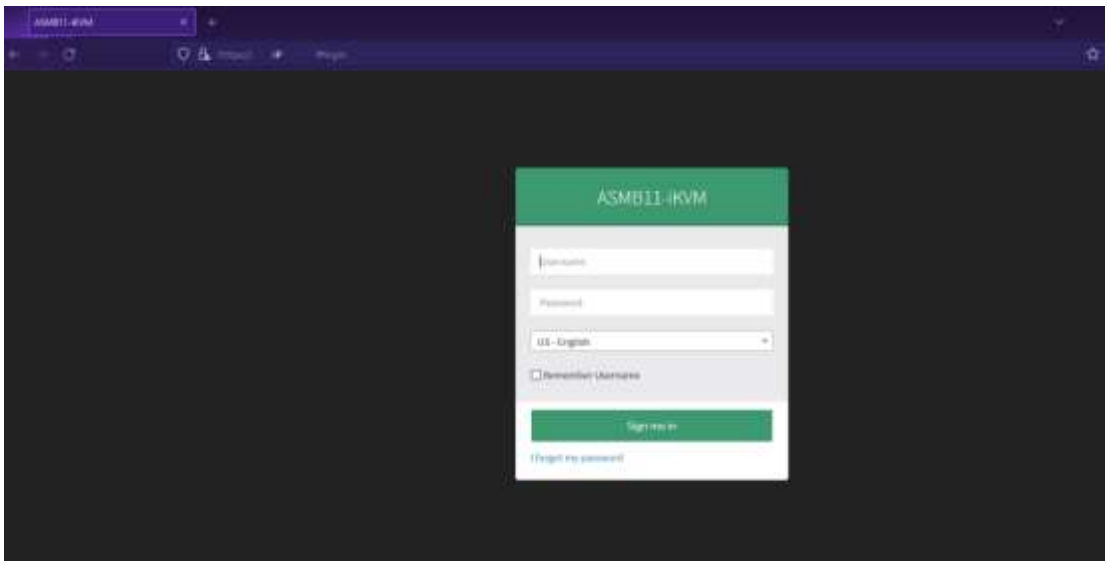
6.3.4.1 Requirements

You will need the following:

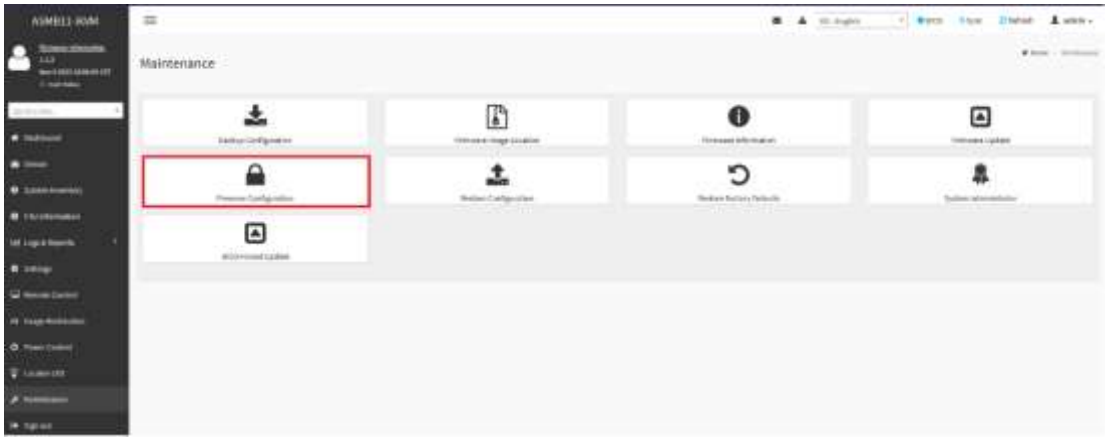
- An installed Bosch DIVAR IP all-in-one 7000 4th gen system
- BMC already configured in BIOS settings
- Updated BMC Firmware
  Note: Only Bosch-approved BMC Firmware versions are supported for updates.

6.3.4.2 Procedure steps

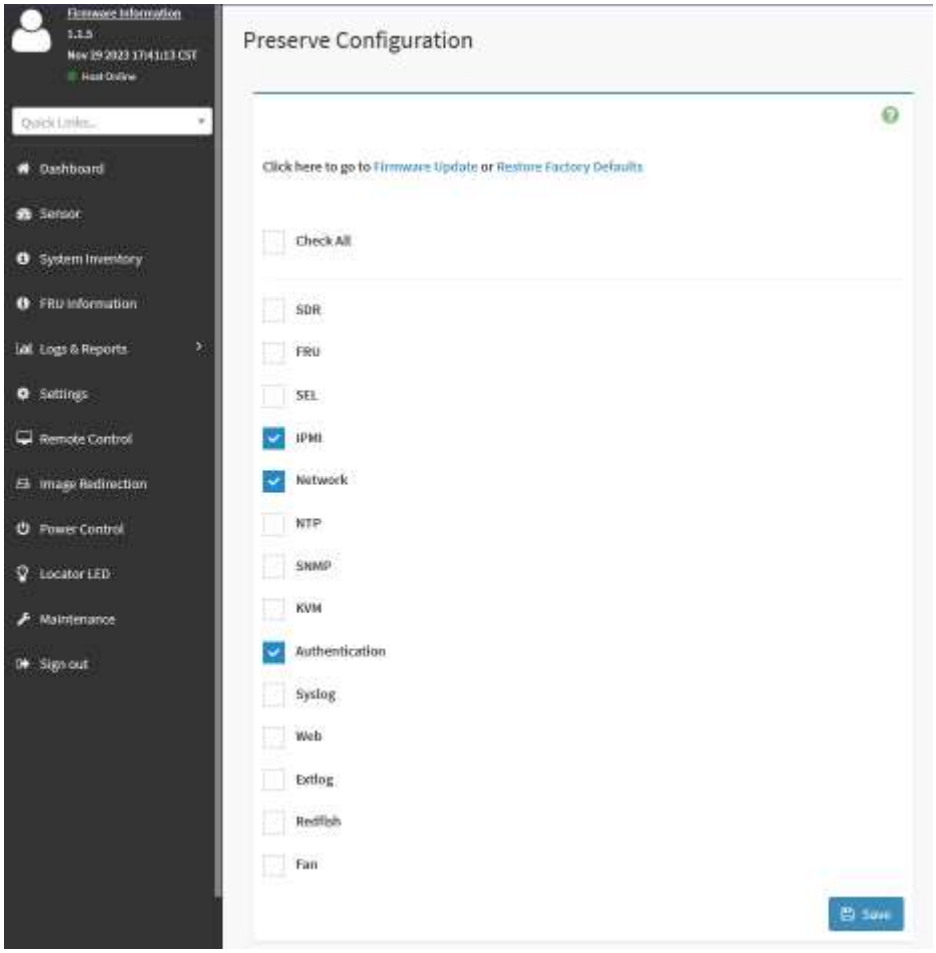
1. Open a web browser and enter the BMC IP address.
   Note: The address must include "**https://**" before the BMC IP address to work properly.



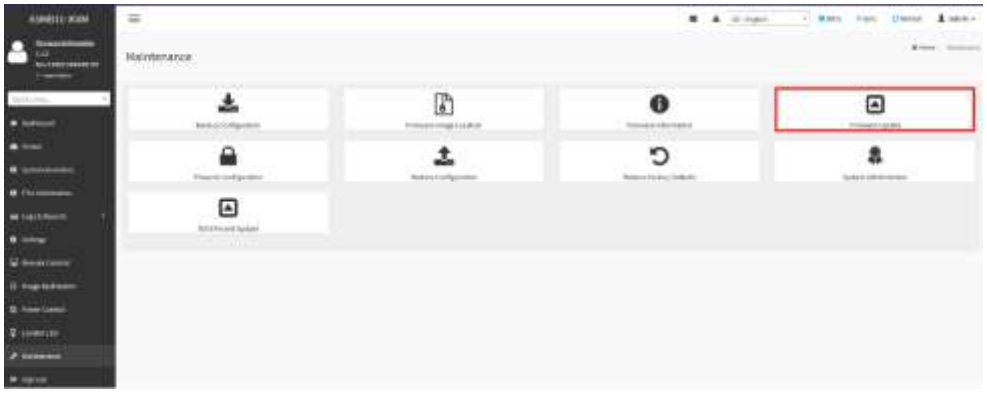
2. Before proceeding with the firmware upgrade, it is recommended to preserve the current main BMC configuration. On the left panel, select "**Maintenance**", then click on "**Preserve Configuration**".



3. Check the options for **IPMI**, **Network**, and **Authentication**, then click on the "**Save**" button.

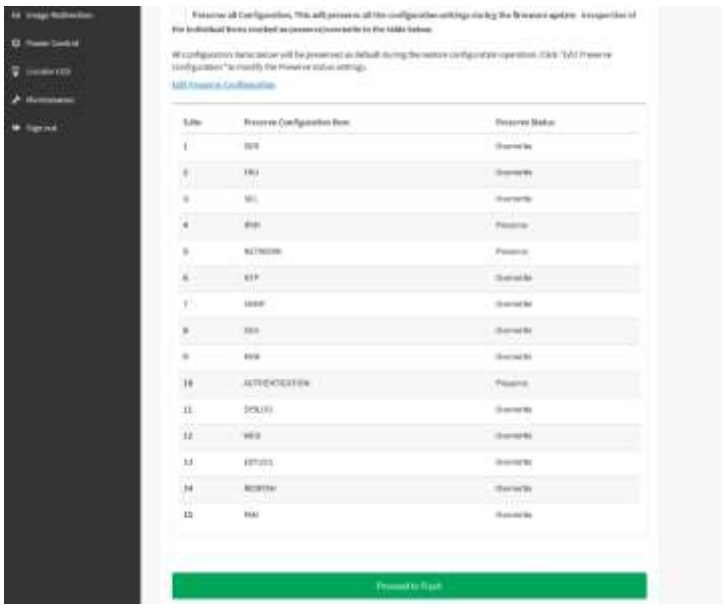


4. Return to the "**Maintenance**" option in the left pane, then click on "**Firmware update**".

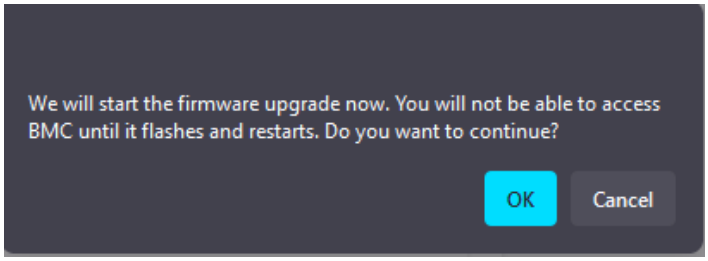


5. First, click on "**Browse**" to find and select the latest firmware file (*.ima), then click on the "**Start Firmware Update**" button.

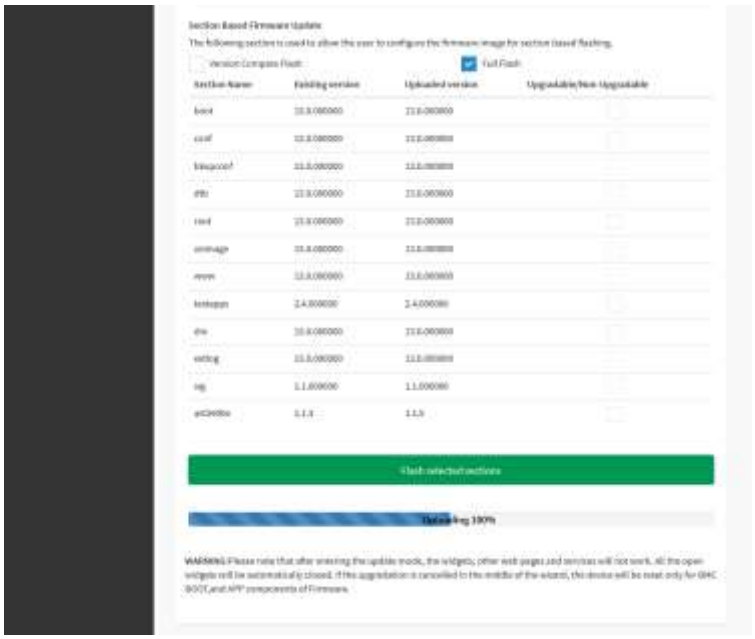
6. The preserved options will be displayed. Click on the "**Proceed to Flash**" button.



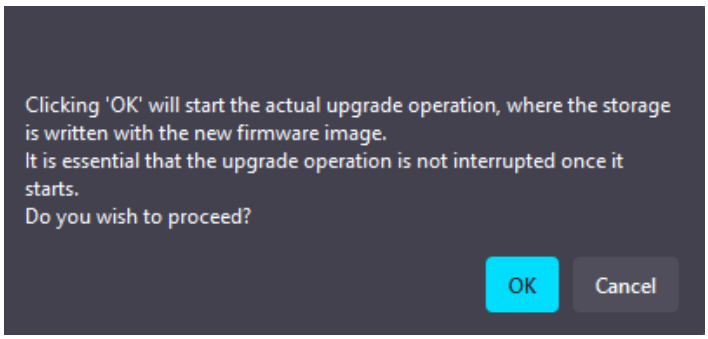
7. A pop-up window will be displayed. Click "**OK**" to continue.



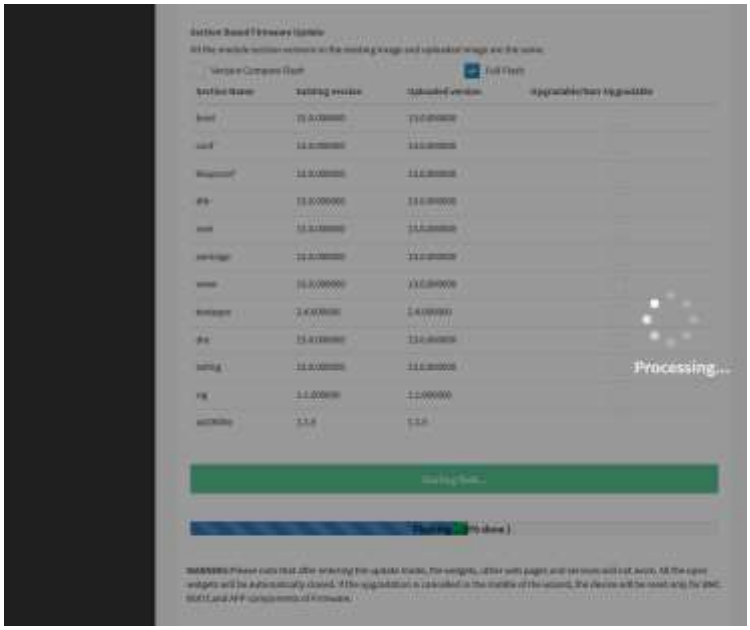
8. Wait for the firmware file to upload until it reaches 100%, then click on "**Flash selected option**" at the bottom.



9. A pop-up window will appear. Click "**OK**" to continue.
Note: This process cannot be interrupted.



10. During the update, a progress bar will be displayed. Please wait until it is finished.



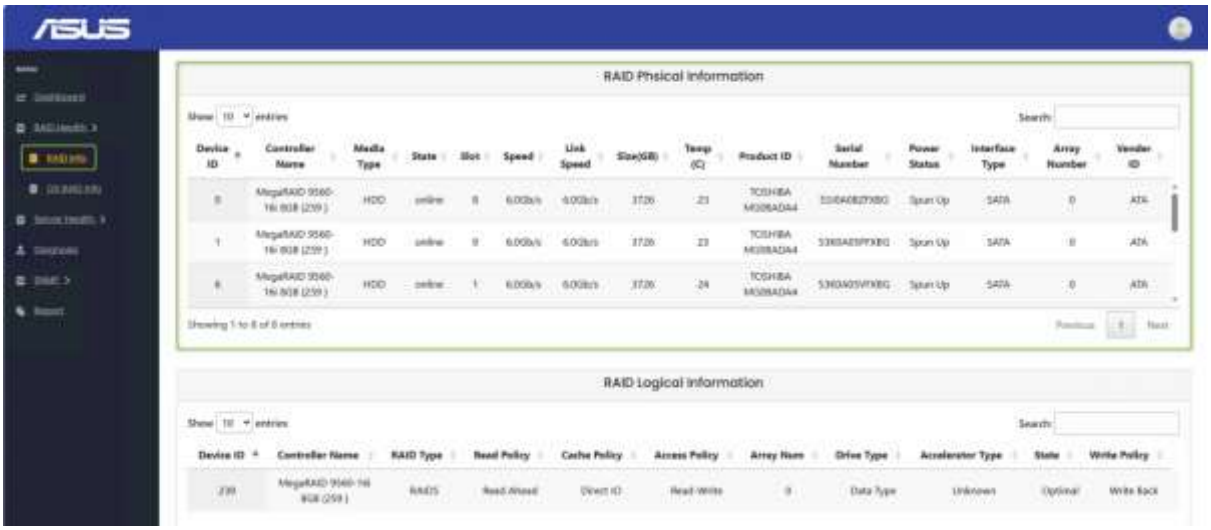
11. If the update process finishes successfully, the following pop-up will be displayed:

12. The firmware reset is now in progress. Please wait a few minutes before opening a new session to the BMC IP address. The firmware has been updated, and the procedure is now complete.

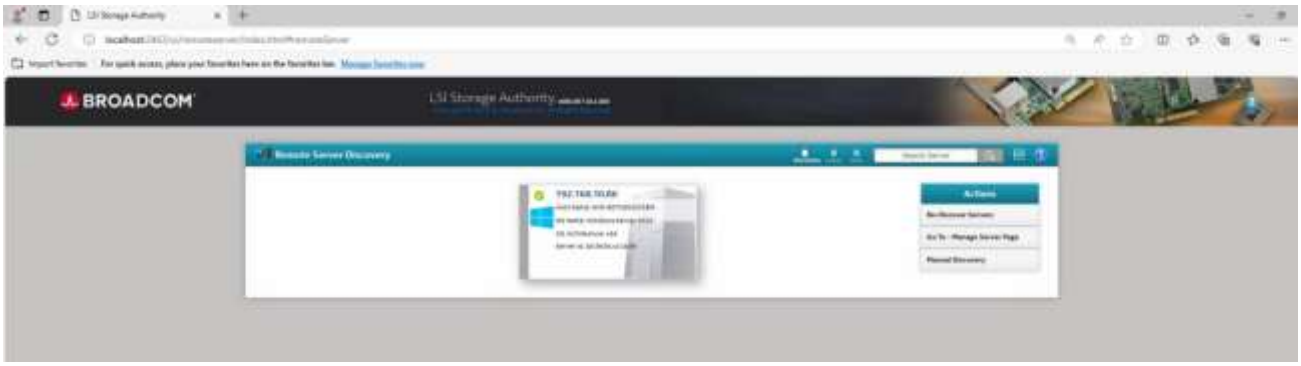
7 Storage: Configuration & Troubleshooting

7.1 Replacing a failed storage hard drive

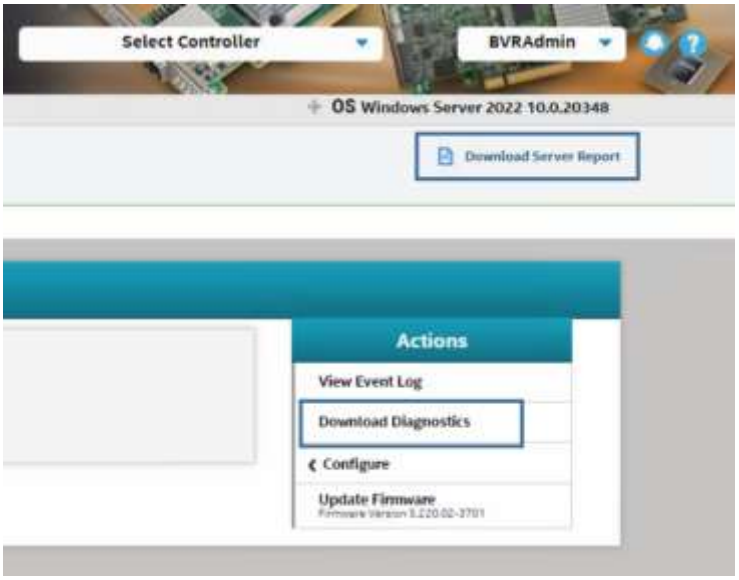
One option to quickly check all the hardware in the device, is the **ASUS Inband Tool**. the tool can be started from the Windows Start menu.
ASUS Inband Tool shows information on and **status** of the **RAID array**, as seen in the following screenshot:



While the ASUS Inband Tool can be used to find issues in the storage array, another tool is required to rebuild the drive; **LSI Storage Authority**. LSA for short, it can be found on the DIP-74xx's Windows desktop. This utility can be used to monitor the **status** of the **drives** in the device's **RAID array** specifically.



Another option for more in-depth troubleshooting, is to download a **Server Report** or "**Download Diagnostics**":



A **How-to video** is available on the DIVAR IP AIO playlist on YouTube and in the DIP AIO technical certification training; "**Installing a storage hard drive**", as well as a chapter in the **User Manual** titled "**Replacing a faulty hard drive and configuring a new hard drive**" exactly detailing these steps.

The following instruction describes how to proceed to rebuild the RAID 5 after replacing a damaged HDD on the RAID 5 pool of the DIVAR IP all-in-one 7000 4th generation, based on an internal document v9, 9 February 2024.

7.1.1 Requirements

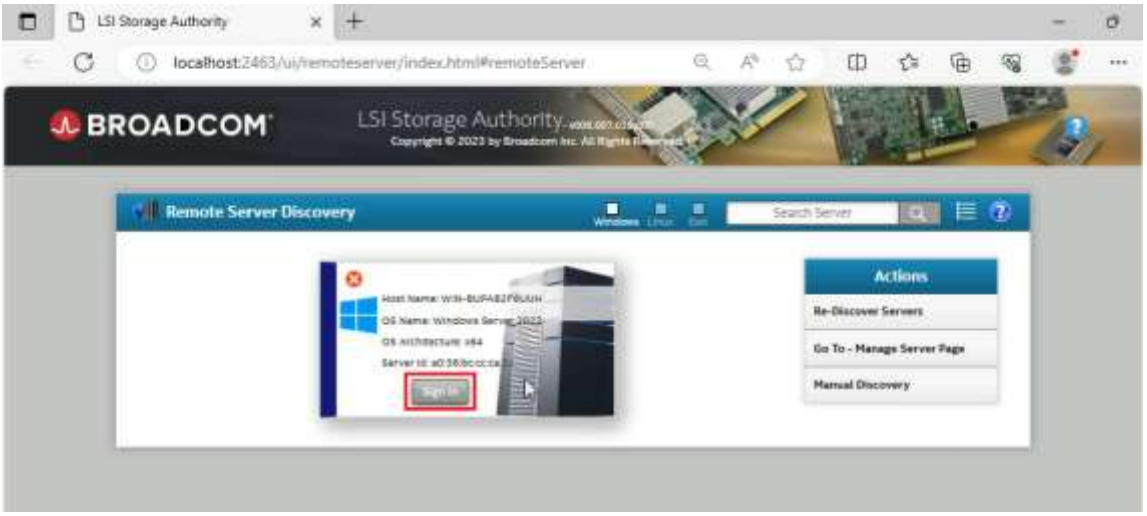
- A Bosch DIVAR IP all-in-one 7000 system is in place.
- A new compatible HDD was used to replace the damaged HDD in the RAID pool.

WARNING: A red LED will be displayed in front of the damaged HDD. On DIP-74xx with RAID5, with only one faulty HDD, there is no DATA LOSS.

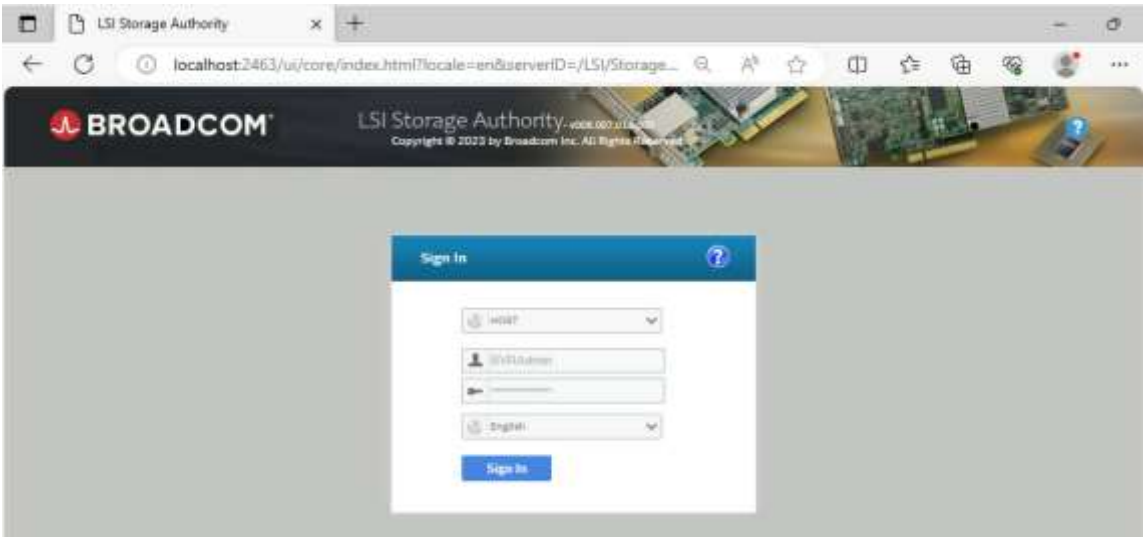
7.1.2 Replacing the damaged HDD

1. To open the RAID Manager in a browser, simply click the "Launch LSA" shortcut on the Windows desktop.

2. Navigate to the main page and click on "**Sign In**" under "**Remote Server Discovery**."

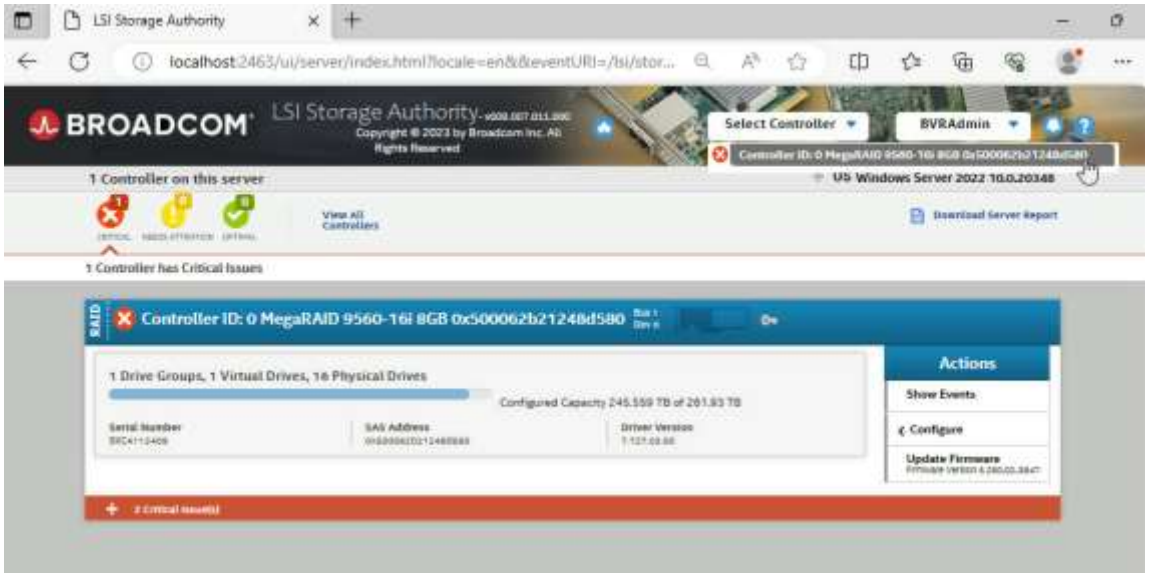


3. Enter the BVRAdmin username and password, and then click the "**Sign In**" button to proceed.

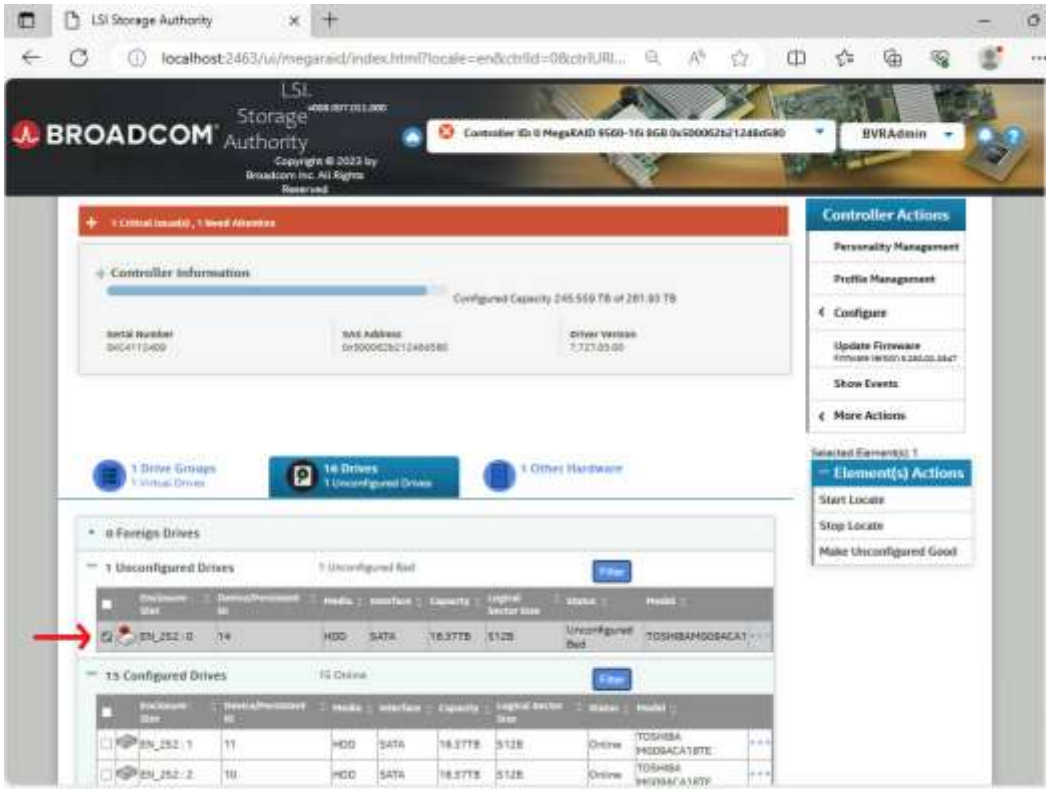


4. You can see that a drive has failed right away. From this screen you can check out the event log, check the diagnostics, silence the alarm of the degraded RAID array, and figure out which drive is broken.

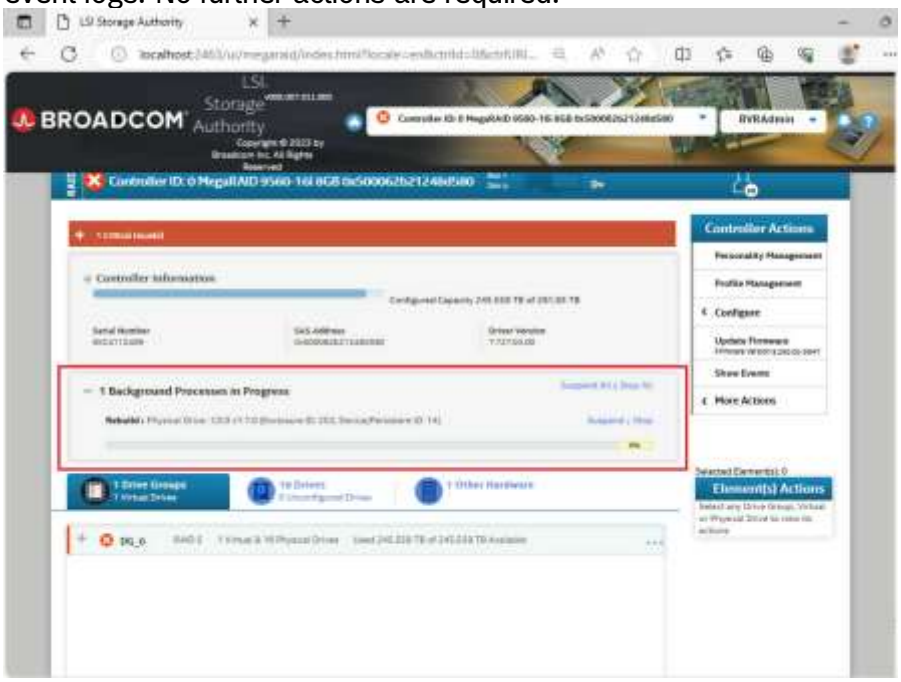
5. To proceed, click on the "**Select Controller**" option at the top, and then click on **MegaRAID 9560-16i** to access the configuration.



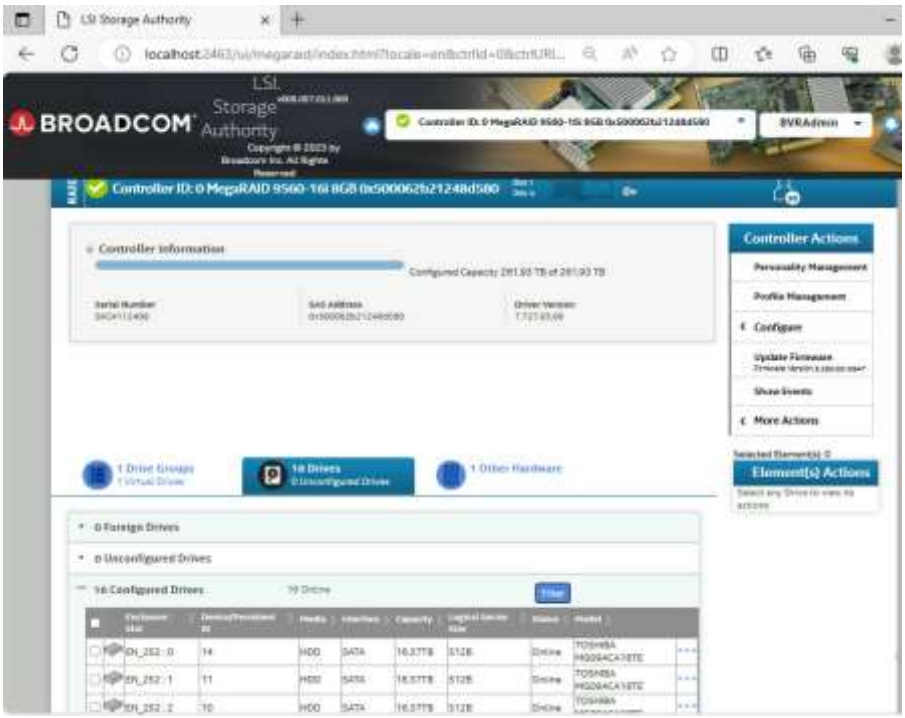
6. The faulty HDD will be displayed under "**Drives**" with a red LED indicator. You can remove the damaged HDD without shutting down, as the system supports hot swap.
Note: If you need to physically confirm the faulty HDD, you can select the "**Start Locate**" option to activate the red LED on the HDD.



7. After determining which drive is broken and replacing it with a suitable BOSCH-supplied replacement, the critical state doesn't go away right at that moment. First the array needs to be rebuilt. This can take a long time, but the start and end of the rebuild are found in the event logs. No further actions are required.



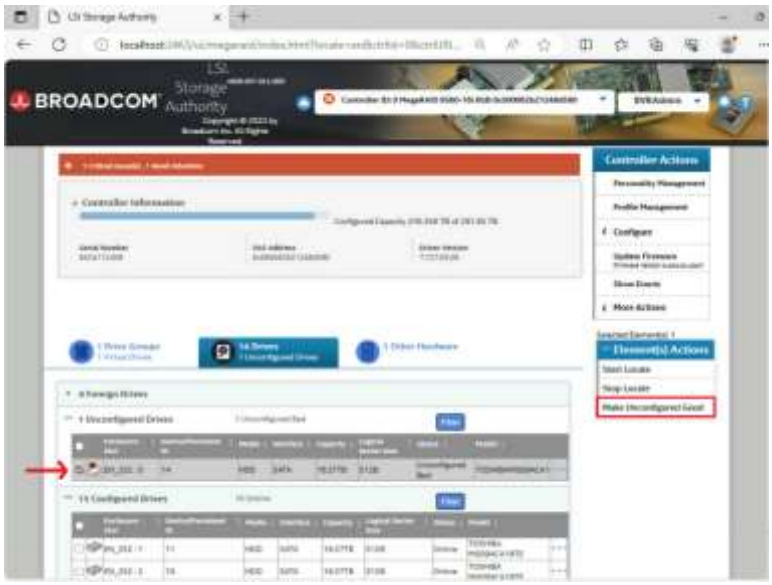
8. Once the rebuild process is complete, the alert will automatically disappear and the status will show no alerts, with a green check mark next to the RAID Controller's name.



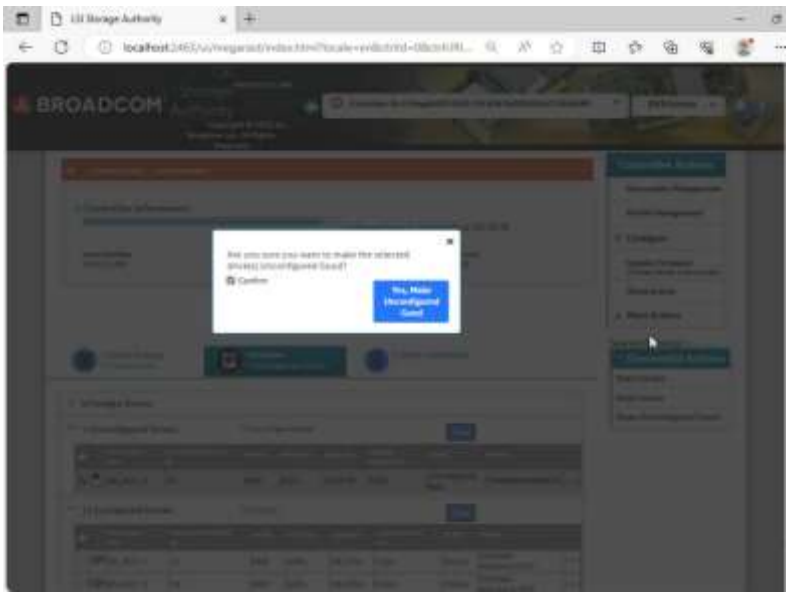
7.1.3 If adding the new HDD doesn't start the rebuild automatically

1. In some cases, a drive does not rebuild on its own and needs to be told to rebuild. To do this, select the RAID Controller **MegaRAID 9560-16i**, then choose "**Drives**" and "**Unconfigured Drives**." Click on the checkbox of the faulty HDD with the status "**Unconfigured Bad**," and then select the option "**Make Unconfigured Good**".

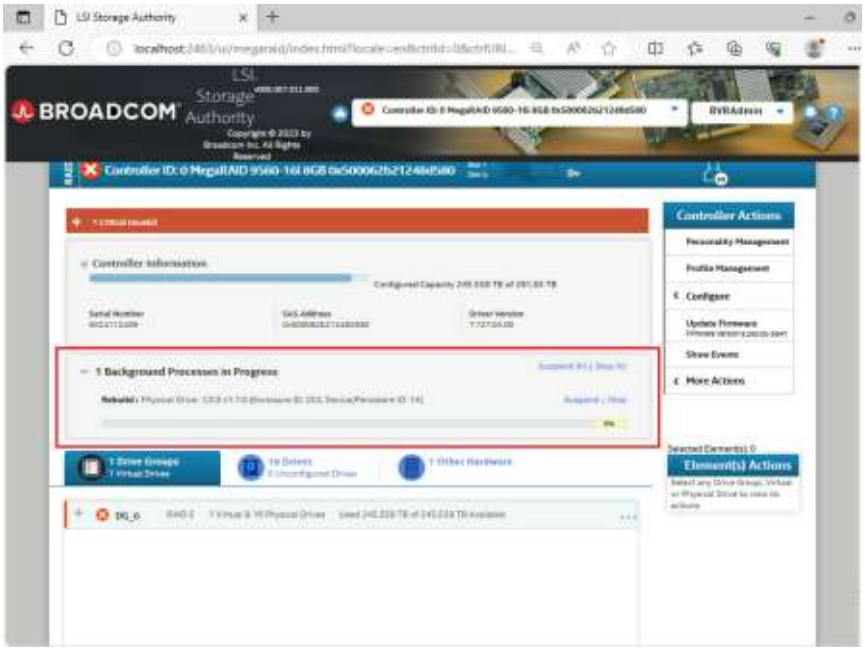
   Make sure to only do this after replacing with a known good drive, doing this with a broken drive will only postpone the inevitable!



2. Confirm the inserted drive is a new drive & can be used to rebuild:
   Select the "**Confirm**" checkbox and then click on "**Yes, Make Unconfigured Good**."

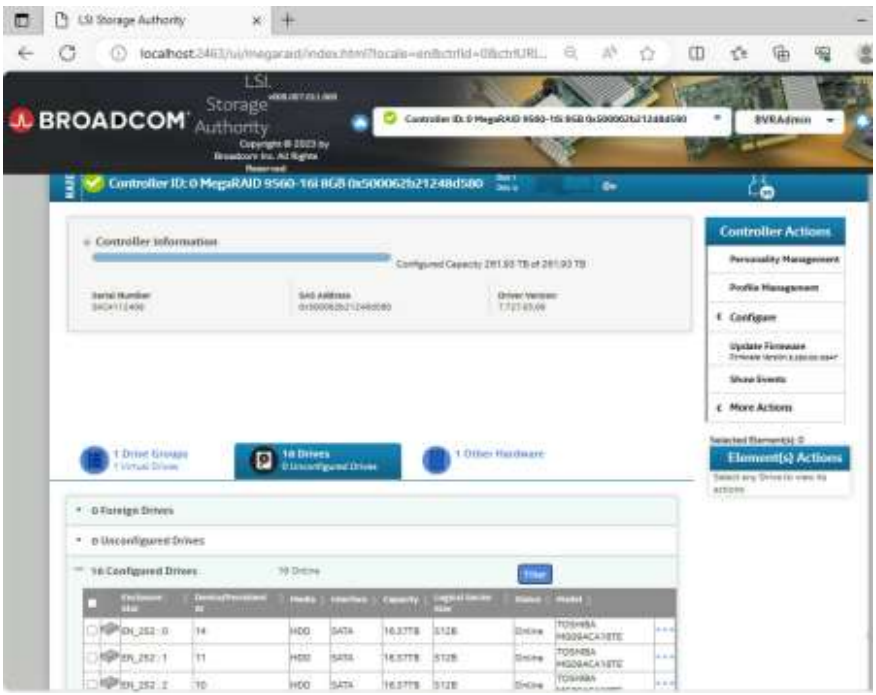


3. The system will automatically begin clearing the HDD and start the rebuilding process. No further actions are needed.



4. After the rebuild is complete, the alert will automatically disappear, and the status will be as in the screenshot.

   The RAID array is in perfect shape once more.



7.2 Replacing a failed OS hard drive

The unit has two accessible SSD drives at the rear of the machine. If one of the drives fails, it can be replaced. The following procedure outlines the steps to take. It was written by Engineering on 12 February 2024, version 22.

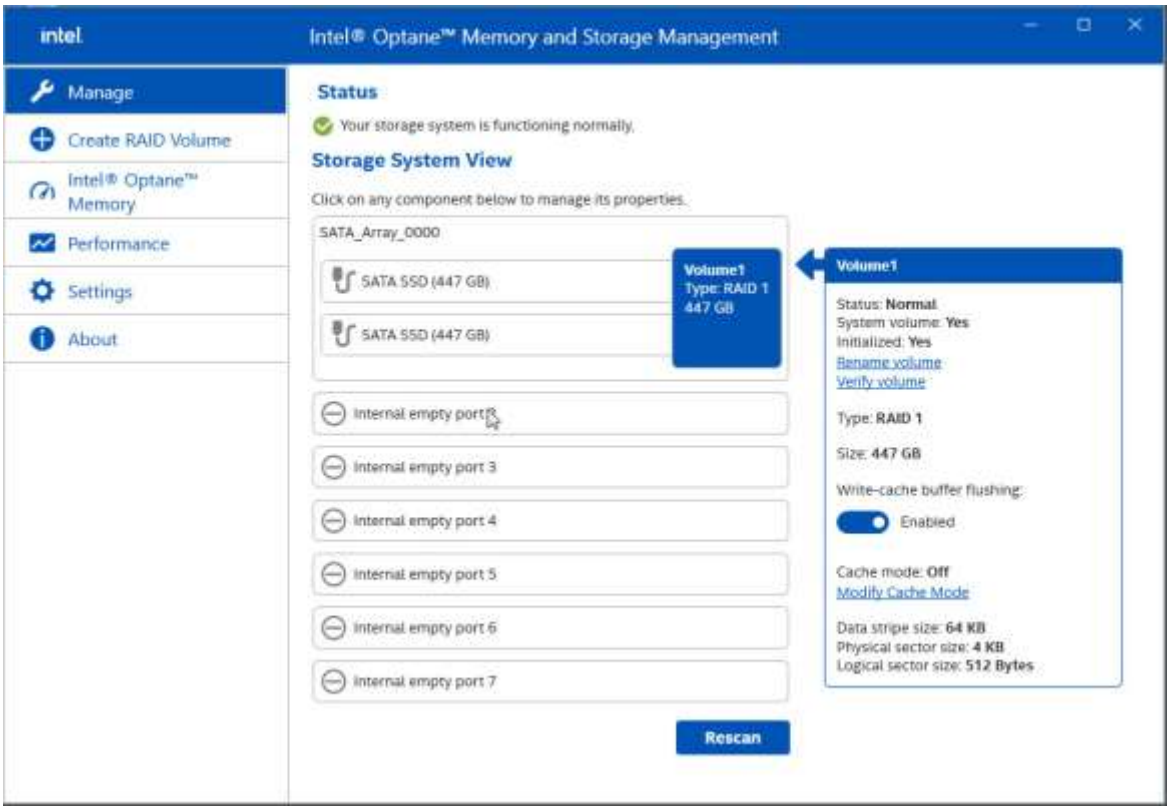
7.2.1 Requirements

The requirements are as follows:

- A Bosch DIVAR IP all-in-one 7000 system
- A new compatible SSD used to replace the damaged SSD in the RAID1 pool

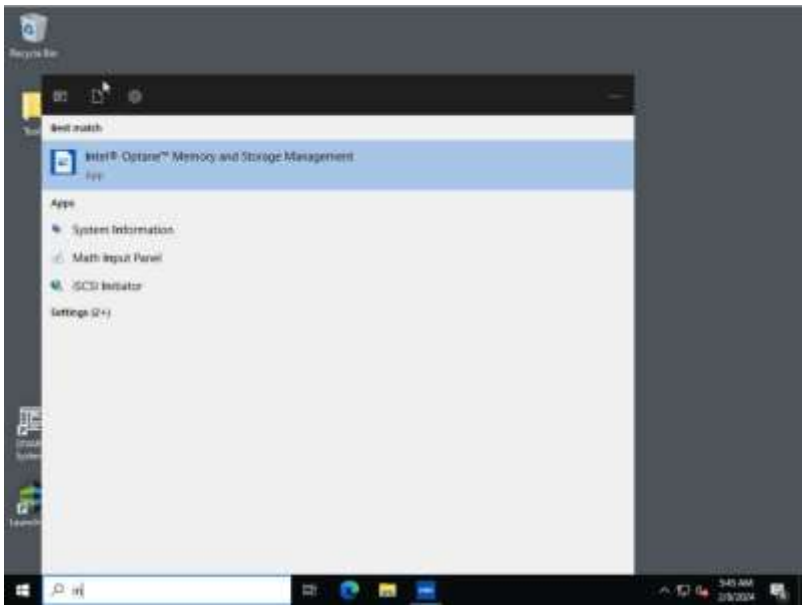
7.2.2 Healthy configuration

When the RAID volume and SSDs are healthy, the system will display the status below in **Intel Optane Memory and Storage Management** with a green check icon:

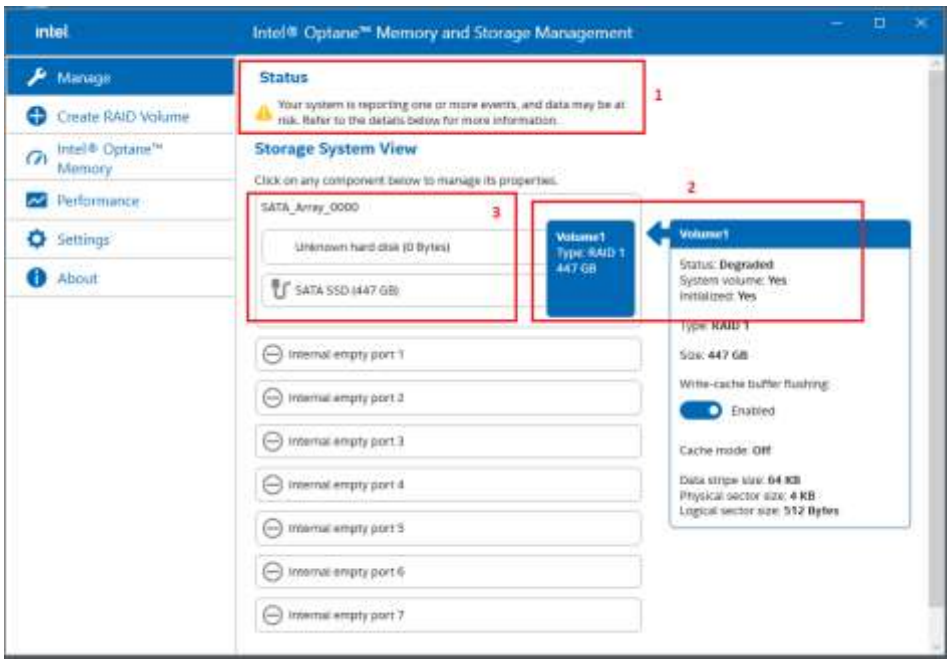


7.2.3 Replacing a damaged SSD

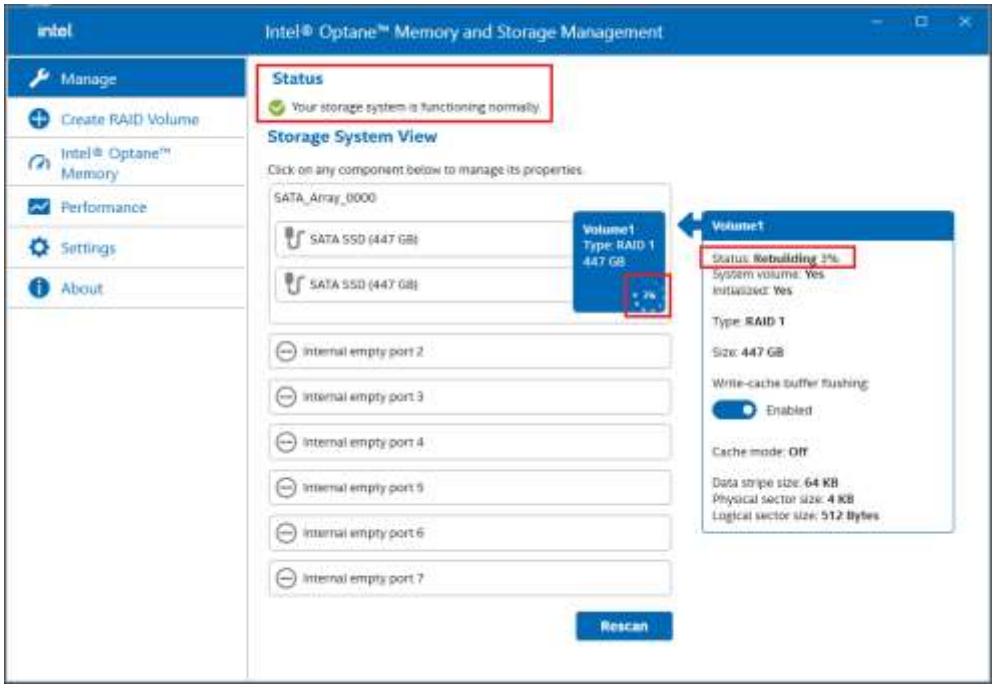
1. Open the **Intel Optane Memory and Storage Management** application using Windows Search.



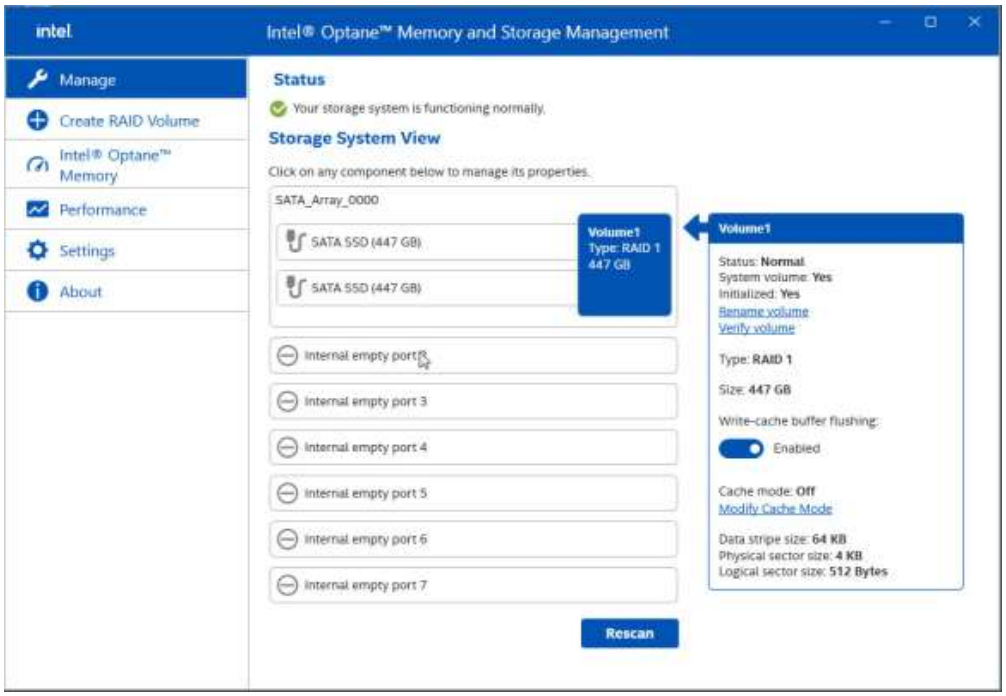
2. On the main page, the **RAID status (1)** will appear with a yellow alert icon and a message indicating that the data may be at risk. If you click on the volume, you can see that the status is **Degraded (2)**. In the **list of disks (3)**, check which SSD is damaged and remove it (a red light will be displayed in front of the damaged SSD).



3. After inserting the new SSD, you need to reboot the DIP for the rebuilding process to start. After the reboot, open **Intel Optane Memory and Storage Management** to verify that everything is functioning properly and that the rebuilding process is running.



4. Once the rebuilding process is complete, the alert will automatically disappear, and the status should return to normal. The procedure is now complete.



7.3 Configuring and checking RAID 5

This procedure is described in the DIP-74xx Installation Manual, as well as in a detailed How-to video titled “Configuring an empty unit with new hard drives”, but here in a detailed step-by-step guide, taken from the Engineering article version 33 from 4 March 2024:

7.3.1 Scope

The following instruction describes how to create a RAID5 logical volume on the DIVAR IP all-in-one 7000 4th gen.

WARNING: This procedure will wipe the current logical volume and therefore cause DATA LOSS.

7.3.2 Requirements

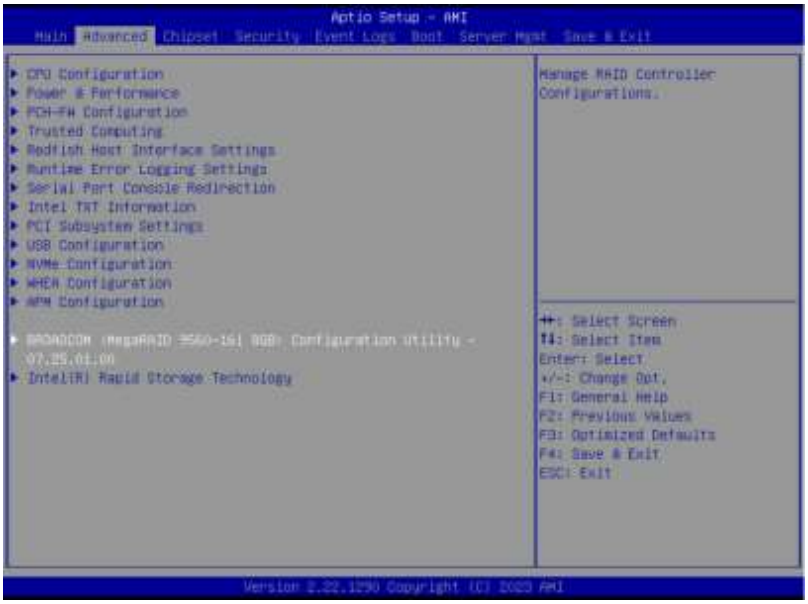
A Bosch DIVAR IP all-in-one 7000 4th gen system in place.

7.3.3 Procedure steps

1. On the startup screen, press DEL to enter the BIOS setup menu.

2. Enter the BIOS password;

3. Navigate to the right using the arrow key until you reach the second tab "**Advanced**". Then, press the down key until you highlight the option "**BROADCOM <MegaRAID 9560-16i 8GB> Configuration utility**" and press enter.

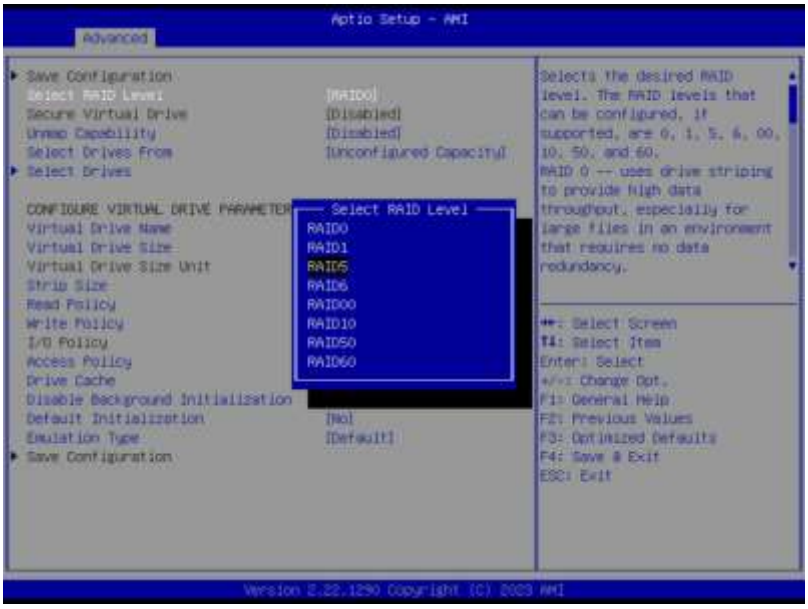


4. In the Configuration utility, select the first option "**Main Menu**" and press enter.

5. Select the first option "**Configuration Management**" and press enter.

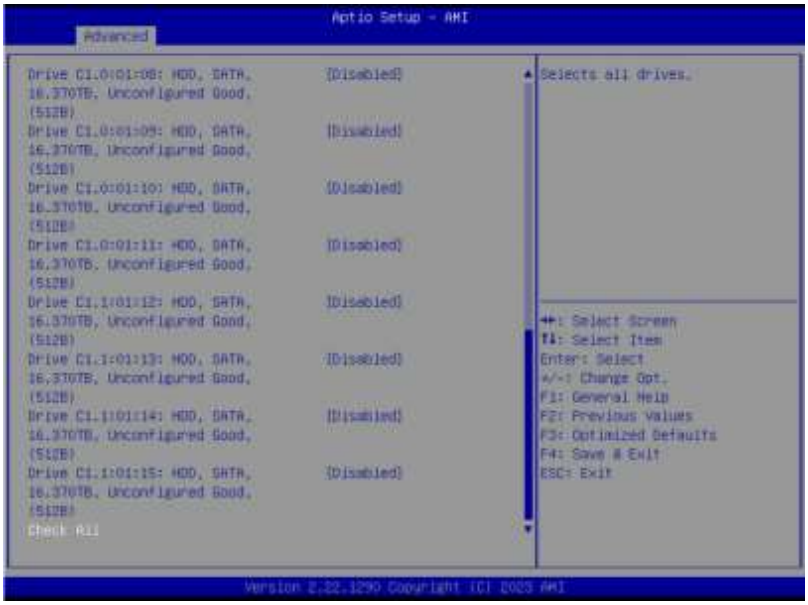
6. Choose the second option "**Create Virtual Drive**" and then press enter.

7. Select the "**Select RAID Level**" option and press enter. Then, use the down key to choose **RAID5** and press enter again.

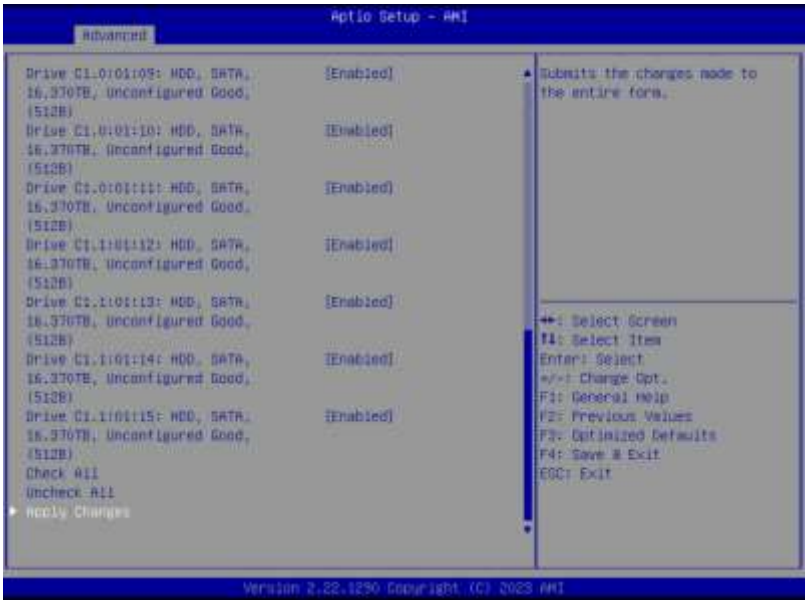


8. Press the down key until you reach the option "**Select Drives**" and then press enter.

9. Confirm the HDD drives by pressing the down key until you reach the option "Check All" at the bottom, then press enter.



10. Press the down key once to display more options, then select "**Apply Changes**" and press enter.



11. After the message "**The operation has been performed successfully**" is displayed, press enter under "**OK**".

12. Use the down key to change the parameters described below to apply the best configuration for the volume, then press enter to select each one:

- Strip Size: 64KB

- Read Policy: Read Ahead

- Write Policy: Always Write Back

- Default Initialization: Fast

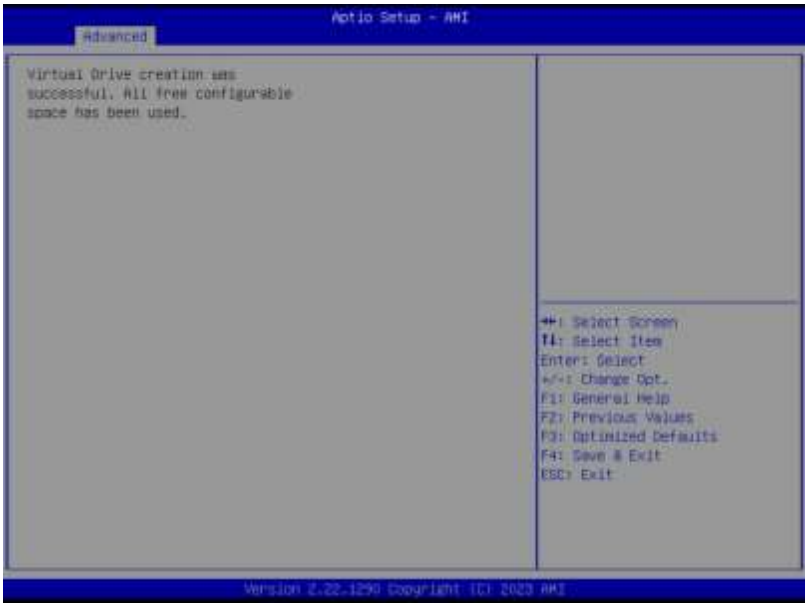
Leave the other options at their default values. To finish this step, press the down key until you reach the last option "Save Configuration" and then press enter.

13. Press enter under the option "**Confirm**" and then select "**Enabled**" by pressing enter again.

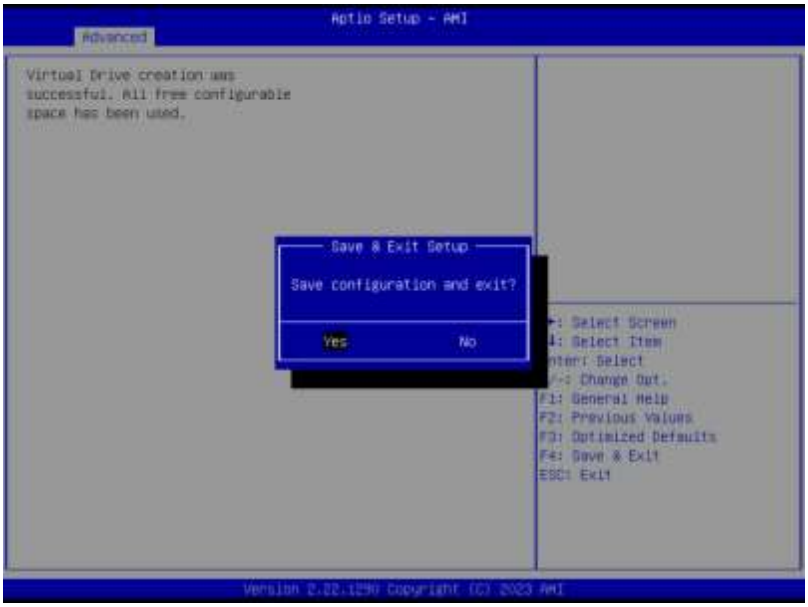
14. Press the down key to select "**Yes**" and then press enter.

15. After the message "The operation has been performed successfully" is displayed, press enter under "OK".

16. The virtual drive RAID5 has been created, and a message "Virtual Drive creation was successful. All free configurable space has been used" will be displayed.



17. The process is complete! You can now exit the BIOS setup by pressing **F4** to save and then selecting "**Yes**" by pressing enter. The system will start up normally.



7.3.4 Checking Virtual Drive Settings

If you want to check the new volume configuration, please follow steps 1 through 3 of this procedure. Then, in the **Advanced** Menu of the configuration utility, select the third option "**Virtual Drive Management**" and press enter.

The information about the logical volume RAID5 will be displayed. You can now exit the BIOS setup. The initialization of the Virtual Drive will be finished automatically, and no further intervention is needed.

7.4 Converting RAID5 to RAID6

The following description was copied from the Engineering Docupedia internal site. The version copied is version 16 of 4 March 2024.

The following instruction describes how to configure a data partition from RAID 5 to RAID 6 on the DIVAR IP all-in-one 7000 4th generation. It is not possible to directly migrate from RAID 5 to RAID 6, so the first step is to delete RAID 5 and then create RAID 6.

WARNING: This procedure will clean up the current logical volume in RAID5 and will therefore cause DATA LOSS.

7.4.1 Requirements

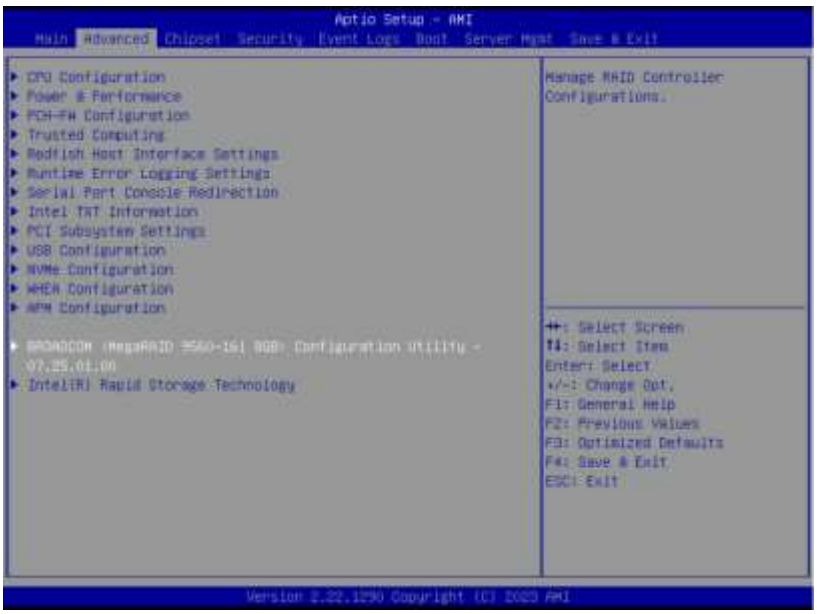
It is important to note that before proceeding with this process on a Bosch DIVAR IP all-in-one 7000 system, it is necessary to make a backup of the data on the disk.

7.4.2 Procedure steps

1. On the startup screen, press the DEL key to enter the BIOS setup menu.

2. To proceed, enter the BIOS password.

3. Use the arrow key to navigate to the right until the second tab "**Advanced**", then press the down key until you reach the option "**BROADCOM <MegaRAID 9560-16i 8GB> Configuration utility**", and press enter.

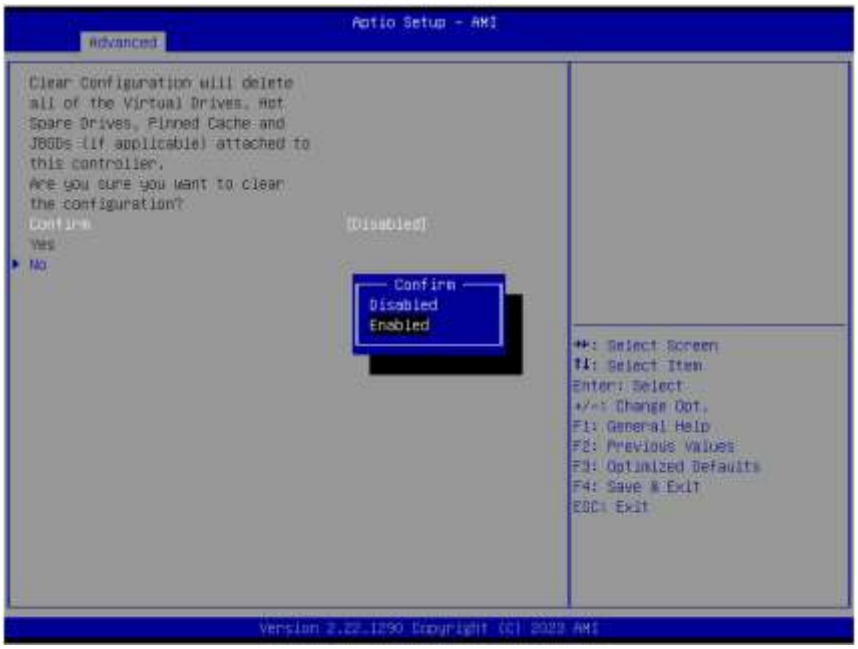


4. In the Configuration utility, select the first option "**Main Menu**" and press enter.

5. Select the first option "**Configuration Management**" and press enter.

6. Select the second option "**Clear Configuration**" and then press enter.

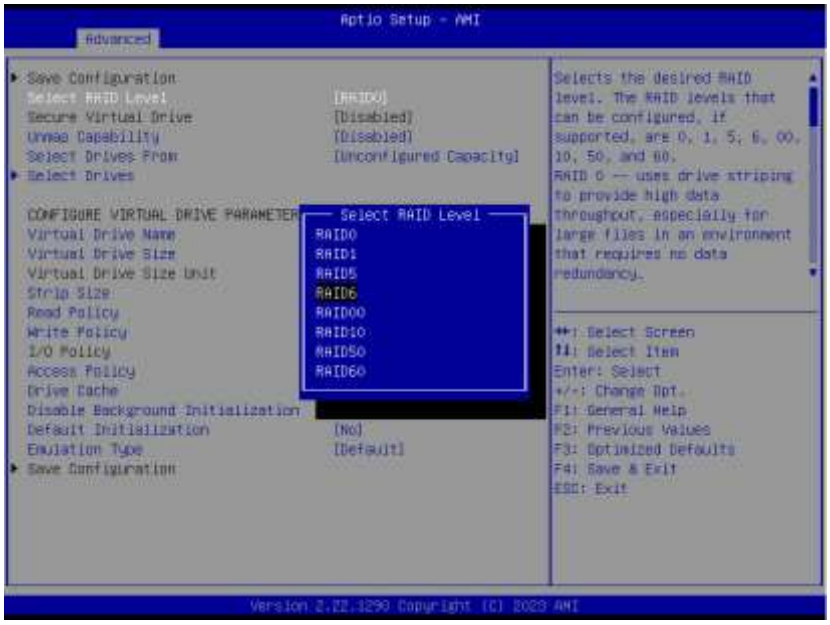
7. Press enter under the option "**Confirm**" and select "**Enabled**" by pressing enter again. Then, press the down key to select "**Yes**" and press enter.



8. After the message "**The operation has been performed successfully**" is displayed, press enter under "**OK**".

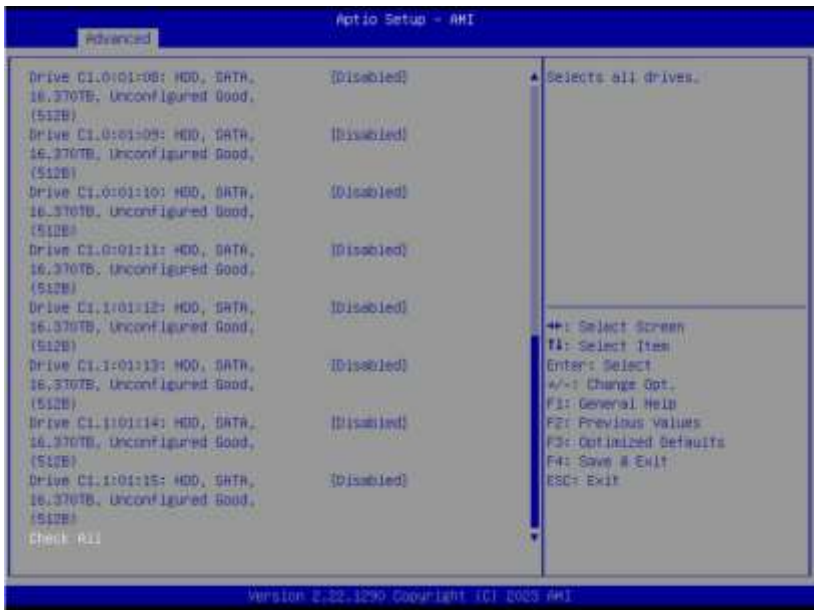
9. Select the second option "**Create Virtual Drive**" and then press enter.

10. Under the "**Select RAID Level**" option, press enter, then press the down key to select RAID6 and press enter again.

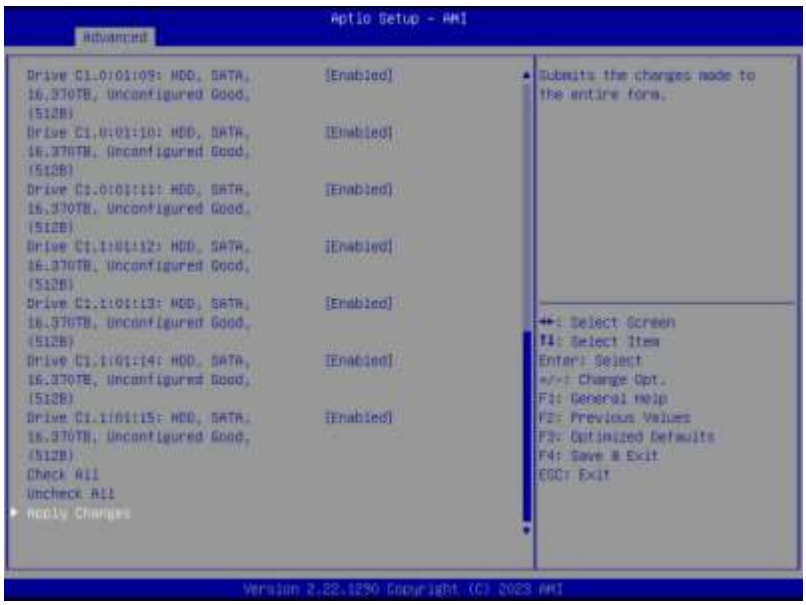


11. Press the down key until you reach the option "**Select Drives**" and then press enter.

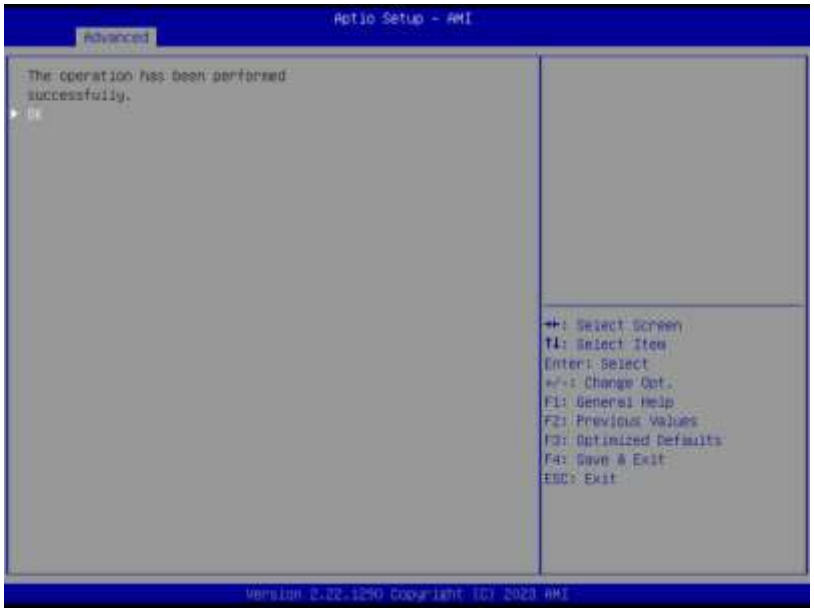
12. Confirm if the HDD drives are present by pressing the down key until you reach the option "**Check All**" at the bottom, then press enter.



13. Press the down key once to display more options, then select "**Apply Changes**" and press enter.



14. After the message "**The operation has been performed successfully**" is displayed, press enter under "**OK**".



15. Use the down key to change the parameters described below to apply the best configuration for the volume, then press enter to select each one:
    - Strip Size: 64KB
    - Read Policy: Read Ahead
    - Write Policy: Always Write Back
    - Default Initialization: Fast

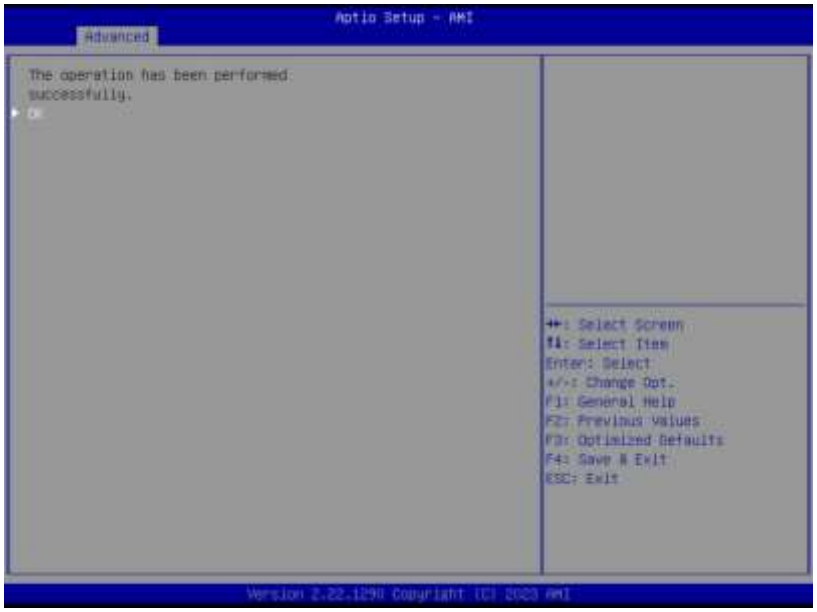
    Leave the other options at their default values.

    To finish this step, press the down key until you reach the last option "**Save Configuration**" and then press enter.

16. Press enter under the option "**Confirm**" and then select "**Enabled**" by pressing enter again.

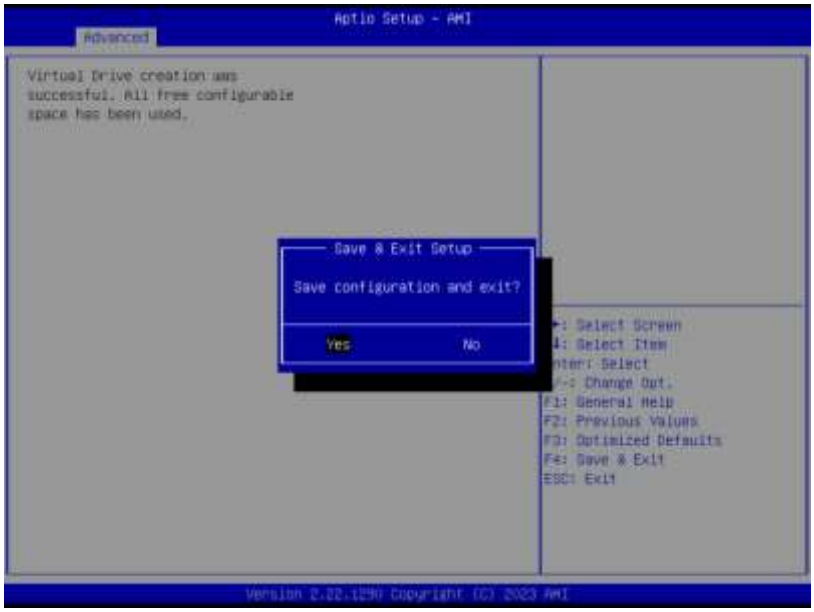
17. Press the down key to select "**Yes**" and then press enter.

18. After the message "**The operation has been performed successfully**" is displayed, press enter under "**OK**".



19. The virtual drive RAID6 has been created, and a message "**Virtual Drive creation was successful. All free configurable space has been used**" will be displayed.

20. It's done! You can now exit the BIOS setup by pressing F4 to save and then selecting "Yes" by pressing enter. The system will start up normally.



7.4.3 Checking Virtual Drive Settings

Additionally, if you want to check the new volume configuration, please follow steps 1 through 3 of this procedure. Then, in the **Advanced Menu** of the configuration utility, select the third option "**Virtual Drive Management**" and press enter.

The information about logical volume RAID6 will be displayed.

You can now exit the BIOS setup. The initialization of the Virtual Drive will be completed automatically, no intervention is necessary.

7.5 Further storage considerations

7.5.1 Can a RAID array be recovered when multiple drives fail?

The ability to rebuild drives depends on the RAID type. In RAID 5, if two or more drives fail, there may not be enough information to rebuild them. However, with RAID 6, it's possible to replace and rebuild 2 failed drives without data loss. Regardless of the RAID type, it's crucial to replace failed drives promptly to minimize the risk of data loss.

7.5.2 Hard drive recommendations

As stated in the data sheet, our policy on 3rd party hard drives (even if they are the same brand/model as provided by Bosch) is as follows:

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.

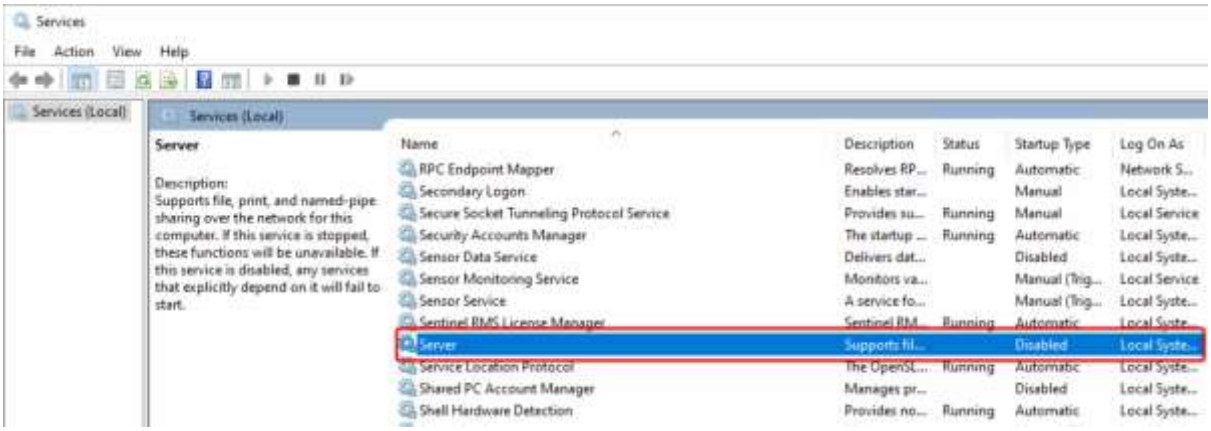
ASUS tracks the hard drives delivered with the system and those delivered by Bosch separately. Any exchanges are noted in their system and known issues with drives are also tracked through ASUS.

8 Various features + tips & tricks

8.1 Server service enabled/disabled

As can be seen in a number of procedures which are mentioned in this Troubleshooting Guide, the **Server** service is disabled by default on the DIPs. This is done on purpose, to provide extra security to our DIP systems. If this service is enabled, it can be used to access the system or its services.

In some cases, it is required to have the service temporarily enabled, to run certain processes. Therefore, it needs to be enabled only while running the procedure and needs to be disabled again when the procedure no longer requires it.



8.2 Remote connection; what about NAT?

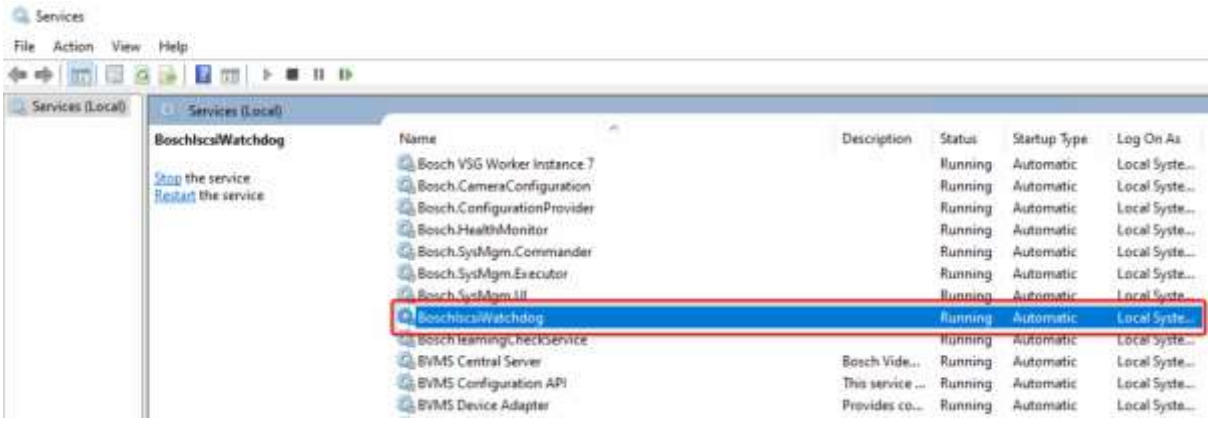
The option to make settings for Network Address Translation (NAT) in the Configuration Wizard (BVMS mode) was removed with version 11.0. It is however still possible to connect to the DIP from a remote PC, using either Operator Client or Video Security Client.

The way to connect remotely to a DIP, is to use an SSH tunnel. It required specific settings on the DIP as well as on the network's router.

For a full step-by-step explanation on how to make this setup, check the DIP's User Manual, chapter **Remote connection to the system**.

8.3 iSCSI watchdog

There is an issue with Microsoft Windows, which causes iSCSI configuration not to come back up after restarting, mainly in larger networks. For this reason, an iSCSI Watchdog service is added to the system. The watchdog detects when the iSCSI configuration takes too long to start and restarts the iSCSI service. This watchdog can be found on the DIP-44xx, DIP-64xx and DIP-74xx.



8.4 How to install anti-virus software

DIVAR IPs rely on Windows internal virus and threat detection software. The systems are tested only with this software, no other packages are therefore tested or supported by Bosch. It is therefore recommended that if a customer has 3rd party anti-virus software installed and it is suspected to be the cause for malfunction of the system, to remove it first before continuing to troubleshoot the system.

8.5 Useful paths, files, and folders

Keep these strictly internal only and make sure not to edit, as making changes here may cause the system to become inoperable & require a recovery. These files give insight for troubleshooting purposes in how the system is initially installed and where something may have gone wrong during installation.

Description	Path/Command
Location of Initial Configuration scripts **(deleted after first oobe config)**	C:\Windows\Panther\User *Can be accessed via Shift + F10 on Initial Setup screen
Unattend file to call the first script OOBE after first logon	C:\Windows\Panther\unattend.xml
OOBE main script to configure DIP	C:\Windows\System32\oem\oobe\OOBE_Model.cmd
Bootloader - Appliance Finder file	C:\Windows\System32\oem\oobe\ApplianceFinder\ApplianceFinder.exe
Windows Security Baseline - GPOs, scripts, and other files	C:\Windows\System32\oem\oobe\WindowsSecurityBaseline\
Windows Startup to show the ApplianceFinder /Bootloader	Registry Editor - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell (REG_SZ) Default value: C:\Windows\System32\oem\oobe\ApplianceFinder\ApplianceFinder.exe To don't show the ApplianceFinder: Value shall be changed to: explorer.exe *Can be changed with Shift + F10 during initial installation screen or F8 "Safe mode with command prompt" and open the notepad SMC_model.cmd to disable on script or run regedit on cmd to change the regkey
Limited User default credentials in registry	Registry Editor - Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultPassword (REG_SZ)

Get OS Image version provided by supplier	Registry Editor - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Bosch\DLA\Image Version (REG_SZ) Command to get value: Get-ItemProperty -Path HKLM:\SOFTWARE\Wow6432Node\Bosch\DLA\ -Name "ImageVersion"

8.6 DIP port list

While the DIPs have many different ports that are used for various applications running on them, only a handful of ports need to be configured in some cases on other network equipment. This list was copied from an Engineering document created 6 March 2024, version 47.

The most important ports to note:

Server	Protocol	Direction	Port	Remark
Bosch Open SSH Service	TCP	In	5322	same port as BVMS SSH service, BVMS SSH service is replaced by Bosch Open SSH service by System Management
Camera Configuration (DMS) DITTO API	TCP		5371	http restricted to localhost
HTTP download from S3 bucket	TCP		5372	S3 bucket that is provided by the backend is mapped to this port
Mosquitto MQTT Broker	TCP		**1883**	For MQTTs should be 8883 - will change with System Manager 2.0
SuperDoctor v5	TCP	In/Out	8181	DIP-44/52/64/72/73 specific
SuperDoctor v5	TCP	In/Out	8454	DIP-44/52/64/72/73 specific
SuperDoctor v5	TCP	In/Out	5333	DIP-44/52/64/72/73 specific
SuperDoctor v5	TCP	In/Out	5666	DIP-44/52/64/72/73 specific
SuperDoctor v5	TCP	In/Out	5999	DIP-44/52/64/72/73 specific
SuperDoctor v5	UDP	In/Out	161 (SNMP)	DIP-44/52/64/72/73 specific
SuperDoctor v5	UDP	In/Out	162 (SNMP)	DIP-44/52/64/72/73 specific
SysMgm-Reserved	TCP		5360-5380	Reserved for SysMgm use
SysMgm-Commander Service	TCP		5373	
SysMgm-Configuration Provider Service	TCP		5375	
SysMgm-Executor Service	TCP		5374	
SysMgm-Health Monitor Service	TCP		5376	
SysMgm-LocalUI Service	TCP		5377	
SysMgm-LocalUI Web Server	TCP		5378	via http (user always redirect to https)
SysMgm-LocalUI Web Server	TCP		5379	via https
Cloud Connector REST API	TCP		5380	via https

BVMS-Reserved	TCP		5381-5499	Reserved for BVMS use
BVMS - Management Server / Enterprise Management Server ports	UDP	In	123	TimeServer NTP
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5322	SSH connection
BVMS - Management Server / Enterprise Management Server ports	TCP		5323 (12.1.0) 5422 (12.2.0+)	Authorization Provider Service, **port changed** with BVMS version 12.2.0
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5387	not in use; Formerly used by ES SDK, Config. Pg. Sdk-Host, REST Https)
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5388	not in use; Formerly used by ES SDK, Config. Pg. Sdk-Host, REST Https)
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5389	OnvifProxy, Event notification
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5390	.NET Remoting
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5391	Remoting port for all NVR services
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5392	WCF, gateway.push.apple.com
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5393	Data-Access-Service
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5394	Remoting port for OpClient
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5395	User preferences, File transfer
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5396	Mex Entry point (normally switched off)
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5397	NoTouchDeployment port
BVMS - Management Server / Enterprise Management Server ports	TCP	In	5398	Internal communication between AKKA.Net component and CS.
BVMS - Management Server / Enterprise Management Server ports	TCP	In	162	

BVMS - Management Server / Enterprise Management Server ports	TCP	In	5389-5396	
BVMS - Management Server / Enterprise Management Server ports	TCP	In	135	BRS
BVMS - Management Server / Enterprise Management Server ports	UDP	In	135	BRS
BVMS - Management Server / Enterprise Management Server ports	TCP	In	808	Central Server connected to Dibos on this port when using WCF
BVMS - Management Server / Enterprise Management Server ports	TCP	In	1756	For primary VRM
BVMS - Management Server / Enterprise Management Server ports	TCP	In	1757	For secondaryVRM
BVMS - Configuration API	TCP	In	5399	HTTPS
BVMS - Management Server / Enterprise Management Server ports	UDP	In	12544	BVMS SNMP Get Port
BVMS - Video Recording Manager ports	TCP	In	554	Retrieve Primary RTSP Stream
BVMS - Video Recording Manager ports	TCP	In	555	Retrieve Secondary RTSP Stream
BVMS - Video Recording Manager ports	TCP	In	40023	Telnet (local host only since VRM 4.x)
BVMS - Video Recording Manager ports	TCP	In	40080	
BVMS - Video Recording Manager ports	TCP	In	40081	
BVMS - Video Recording Manager ports	TCP	In	41080	
BVMS - Video Recording Manager ports	TCP	In	41081	
BVMS - Video Recording Manager ports	TCP	In	1756	via RCP+ , (1757 for Sec. VMR RCP+ client)
BVMS - Video Recording Manager ports	TCP	In	1757	via RCP+ , (1757 for Sec. VMR RCP+ client)
BVMS - Video Recording Manager ports	UDP	In	1757	Scan Target Broadcast
BVMS - Video Recording Manager ports	UDP	In	1758	Scan Response
BVMS - Video Recording Manager ports	UDP	In	1759	Network discovery, Scan Target Multicast
BVMS - Video Recording Manager ports	UDP	In	1760	
BVMS - Video Recording Manager ports	UDP	In	1800	Network discovery, Scan Target Multicast

BVMS - Video Recording Manager ports	UDP	In	1900	Network discovery, Scan Target Multicast
BVMS - Video Recording Manager ports	TCP	In	80	Primary VRM playback via http
BVMS - Video Recording Manager ports	TCP	In	443	Primary VRM playback via https
BVMS - Video Recording Manager ports	TCP	In	81	Secondary VRM playback via http
BVMS - Video Recording Manager ports	TCP	In	444	Secondary VRM playback via https
BVMS - Mobile Video Service ports	TCP	In	80	Access via http
BVMS - Mobile Video Service ports	TCP	In	443	Access via https
BVMS - Mobile Video Service ports	TCP	In	2195	Mac iOS
BVMS - Mobile Video Service ports	UDP	In	1064-65535	Live Streaming
BVMS - Mobile Video Service ports	TCP	In	5382	Media stream
BVMS - Mobile Video Service ports	TCP	In	5383	Media stream
BVMS - Mobile Video Service ports	TCP	In	5384	Media stream
BVMS - Mobile Video Service ports	TCP	In	5385	Media stream
BVMS - iSCSI Storage System ports	TCP	In	3260	
BVMS - Bosch Video Streaming Gateway ports	TCP	In	8756-8762	RCP +
BVMS - Bosch Video Streaming Gateway ports	TCP	In	8080-8086	HTTP
BVMS - Bosch Video Streaming Gateway ports	TCP	In	8443-8449	HTTPS
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1757	Scan Target Broadcast
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1758	Scan Response
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1759	Scan Target Multicast
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1800	Scan Target Multicast
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1900	Scan Target Multicast
BVMS - Bosch Video Streaming Gateway ports	UDP	In	1064-65535	
BVMS - Operator Client / Cameo SDK ports	TCP	In	5394	WCF
BVMS - Operator Client / Cameo SDK ports	UDP	In	1024-65535	Live Streaming
BVMS - Operator Client / Cameo SDK ports	TCP	In	40082	
BVMS - Operator Client / Cameo SDK ports	TCP	In	41756	

BVMS - Encoder ports	TCP	In	1756	via RCP+
BVMS - Encoder ports	UDP	In	1757	Scan Target
BVMS - Encoder ports	UDP	In	1758	Scan Response
BVMS - Encoder ports	UDP	In	1800	Scan Target Multicast
BVMS - Encoder ports	TCP	In	80	Access via http
BVMS - Encoder ports	TCP	In	443	Access via https
BVMS - Encoder ports	UDP	In	123	SNTP
BVMS - Encoder ports	UDP	In	161	SNMP
BVMS - Encoder ports	TCP	In	554	RTSP Streaming
BVMS - Encoder ports	TCP	In	3260	iSCSI Recording
BVMS - Optional encoder ports: FTP	TCP	In	21	FTP (Optional encoder port)
BVMS - Optional encoder ports: SSDP	UDP	In	1900	SSDP (Optional encoder port)
BVMS - Optional encoder ports: UPNP	UDP	In	3702	UPNP (Optional encoder port)
BVMS - Optional encoder ports: SRTSP	UDP	In	9554	SRTSP (Optional encoder port)
BVMS - Optional encoder ports: RTSP send	UDP	In	15344	RTSP send (Optional encoder port)
BVMS - Optional encoder ports: RTSP send	UDP	In	15345	RTSP send (Optional encoder port)
BVMS - Decoder ports	TCP	In	1756	via RCP+
BVMS - Decoder ports	UDP	In	1757	Scan Target Broadcast
BVMS - Decoder ports	UDP	In	1758	Scan Response
BVMS - Decoder ports	UDP	In	1800	Scan Target Multicast
BVMS - Decoder ports	TCP	In	80	Access via http
BVMS - Decoder ports	TCP	In	443	Access via https
BVMS - Decoder ports	UDP	In	1024-65535	Streaming ports
BVMS - Decoder ports	UDP	In	123	SNTP
BVMS - Decoder ports	UDP	In	161	SNMP
BVMS - DVR ports	TCP	In	80	Access via http
BVMS - DVR ports	TCP	In	443	Access via https
BVMS - Config Client	TCP	In	1024-65535	Video Streaming
BVMS - PID, Person Identification ports	TCP	In	8443	Access via https
BVMS - Workstation Monitoring	TCP	In	5410	
BVMS - Workstation Monitoring	TCP	In	5411	
BVMS - LPR, BVMS Device Adapter ports	TCP	In	31000	VRC
BVMS - AMS, Access Management System ports	TCP	In	62904	Access via https

For just the BVMS ports list, check **BVMS Configuration Manual > Troubleshooting > Used Ports**.

8.7 Ports and domains for connectivity

In order for the DIVAR IP to be able to communicate with Remote Portal, the following table shows details on settings that must be made so that these ports and domains are reachable from the device:

Port	Protocol	Clients	Purpose	Hostname/port	IP
443	HTTPS	User Workstation	Web Access Remote Portal UI	https://remote.boschsecurity.com:443	52.29.189.224
443	HTTPS	Device	REST API for device provisioning	https://api.remote.boschsecurity.com/rest/iot/devices:443	52.29.189.224
8883	MQTTS	Device	Device communication for telemetry, events, commands	tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883	
443	HTTPS	Device	Download of software artefacts Upload of log files	https://sw-repo-remote.s3.eu-central-1.amazonaws.com:443	

The ports described in the table must be open, the protocols must be allowed on the network and the domains need to be reachable using DNS.

8.8 Software Package information

The software packages for the DIPs are categorized into various types. To provide insights into the naming and numbering scheme, Engineering has compiled an internal document. Below is a copy of the information contained in version 7, dated January 30, 2023".

8.8.1 Software Package ID Convention

The System Manager installer and Operation mode package are stored in separate ZIP files for distinct reasons:

1. We anticipate different release schedules between BVMS and System Manager, necessitating separate updates. This streamlines the process for users, ensuring they only download the necessary System Manager files.
    a. However, this may require users to manage two ZIP files, deviating from the single-file experience in Software Center.
    b. We need to guarantee that any version of System Manager accepts any version of package files (backward and forward compatibility) or implement intelligent handling of forward incompatibilities.
2. The **System Manager ZIP file** exclusively contains the installer in the "BoschAppliance" folder, following a naming convention like "`SystemManager_[software version].zip`". Internal discussions confirm that System Manager updates will be exclusively through new releases, maintaining a clear correspondence between ZIP file and version.
3. The **Operation mode package ZIP file** encompasses all necessary files and installers for Operating mode installation or application SW package updates:
    a. Follows the convention "`BVMS_[BVMS softwareversion]SystemManager_package[package version].zip`"
    b. There could be different package versions released for the same BVMS version, for example including mandatory security related BVMS patches, or any other changes that we would not want to release as separate (update) packages.
4. **BVMS updates**, including VRM, VSG, and other BVMS components, will have their own separate packages.
    a. Zip-file naming convention: "`BVMS_[BVMS softwareversion]Updates_SystemManager_package[package version].zip`"
5. Future iterations may introduce **additional ZIP file families** for specific applications, including updates for ASUS Inband Tool, SD5 for earlier DIPs, KBD-Digital Adapter driver, etc. ZIP file contains all patches released at the time of the release of the ZIP file. If one or more patches need to be added, package version is increased, and ZIP file is replaced.
    a. SD5 ZIP file naming convention: `SD5_[SD5 software version]_SystemManager_package_[package version].zip`

8.9 Closing System Manager when opened through BVMS Desktop

When DIVAR IP System Manager is opened through the BVMS Desktop (aka Kiosk Mode), it is opened using the Limited user. It will require logging in using the BVRAdmin user's credentials. Once logged in, there is no close button on the interface due to the way the webpage is called up. The way to again close the System Manager, is to use ALT+F4.

8.10 Power outage & restore

When a power outage occurs and later the power network restores itself, a DIP system will automatically boot back up to the state it was in prior to the power outage. Please note that in some cases, this can cause issues if there are many DIPs (or other electrical equipment), which start up at the same time. Typically, devices will pull more current during initial boot, which can trigger a fuse to be switched due to excessive current demand, causing another power outage.

If this is the case on a site, it is advisable to only switch on power one-by-one on the devices in the same group, so a power surge does not re-occur.

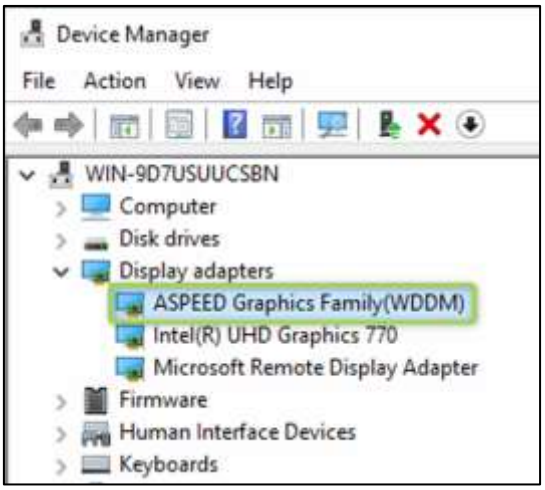
8.11 Power button operation

The front power button on a DIP will not do anything if only pressed shortly, this in order to make sure that an accidental bump does not shutdown the system. In order to force a shutdown, hold the power button for 4-5 seconds. There is no way to gracefully shut down the DIP through hardware buttons, this can be done from software only (through Windows or BMC).

The reset button on the system is slightly recessed and because of this operates as expected. Pressing the reset button will shut down and restart the device immediately.

8.12 Disabled monitor in Windows

In Windows and in Device Manager, a second monitor can be seen, listed as ASPEED Graphics Family(WDDM). This monitor is the iKVM monitor, which cannot be used as another monitor in Windows:



The system has a script running on a schedule which will automatically turn this monitor on and off.

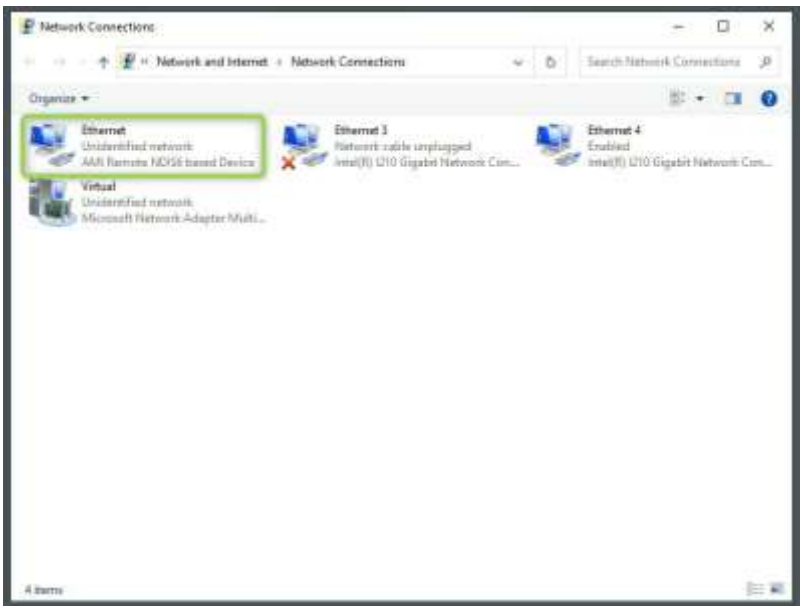
- When no HDMI monitor is connected, this monitor will be enabled.
- When an HDMI monitor is connected, this monitor will be disabled.

This is why, for a remote BMC connection to work, no HDMI monitor should be connected.

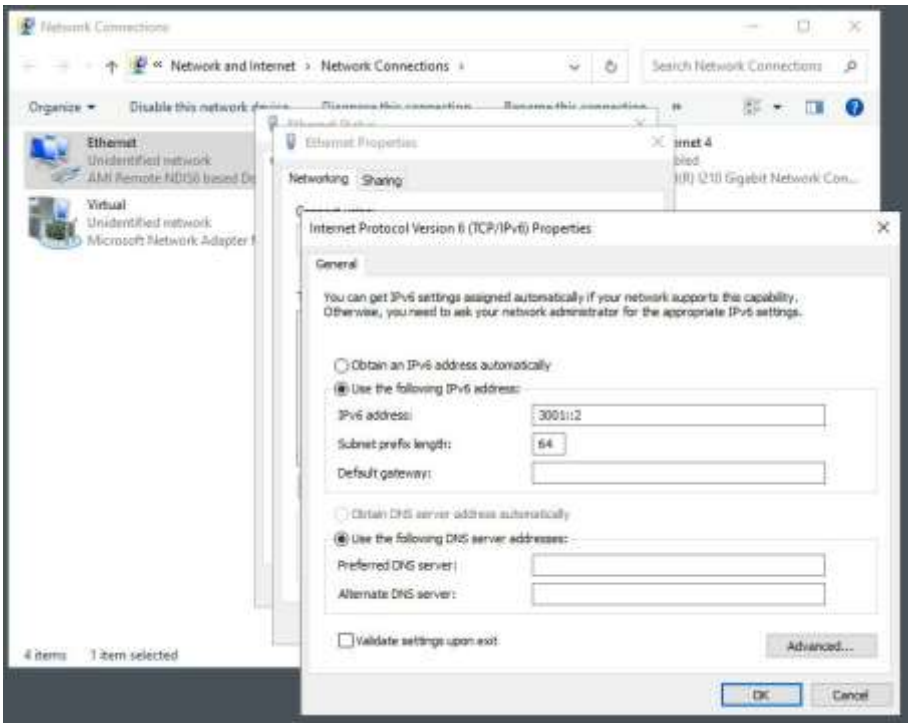
Note that when the Aspeed monitor is enabled, this also enables the (covered up) VGA monitor, which provides the video output to the remote BMC connection. So, it is possible to connect a VGA monitor and have a BMC connection at the same time. This is not really advertised, but it is supported for customer use as well for exactly the described use-case; when no HDMI monitor is connected. In that scenario, it needs to be clear that both iKVM and the VGA output are only used for management purposes. The resolution is limited, and no transcoding is possible, so this set-up is not meant for Operator Client usage. More details on this usage can be found in the chapter on BMC.

8.13 Additional network interface card

In addition to the two teamed NICs and the virtual teamed connection for the normal LAN connection, there is a 4th network interface visible in the Windows Network Connections overview: the "AMI Remote NDIS6 based device" adapter.



The adapter is active and serves as the internal connection from the ASUS InBand Tool to the Baseboard Management Controller (BMC). This adapter does not interfere with teaming, and it does not appear in the BVMS Wizard and scans because the IPv4 protocol is disabled on this adapter.



Instead, it is configured to use the IPv6 protocol for communication. This configuration ensures that the adapter is dedicated to its specific purpose and does not disrupt other network operations.

8.14 LSI Storage Authority Error Code 49 Invalid Credentials

Described in this chapter is an issue which was found externally with the LSI Storage Authority application that we use to monitor the RAID array.

Note that this issue should **not** occur on the DIP-74xx (it occurs on the DIP-64xx), as it was fixed in DIP-specific Windows settings, except for Russian and perhaps some other untested language. For those languages, please check the procedure below to fix this issue.

The problem is caused by the fact that the credentials check is based on the English language, so when the Operating System is set to another language than English, the program has an issue with starting up and throws out the **error code 49 Invalid Credentials**.

8.14.1 Solution

To be able to use the LSA app in a non-English OS, the LSA configuration file needs to be edited.

Follow these steps:

1. Stop the **LSAService** in Windows Services
2. Edit the LSA config file (**LSA.conf**)
   `C:\Program Files(x86)\LSI\LSIStroageAuthority\conf\LSA.conf`
3. Check the following command: full_access_groups = Administrators

Depending on the language, this must be adjusted here (these are examples):

- French = full_access_groups = Administrators
- German = full_access_groups = Administrators
- Spanish = full_access_groups = Administrators
- Russian = full_access_groups = Администраторы or Administratory

As soon as you have carried out point 3 and saved it, you must restart the **LSAService**. After following these steps, you should be able to log back in without any problems.

This information was taken from this website: https://www.thomas-krenn.com/de/wiki/LSI_Storage_Authority_Error_Code_49_Invalid_Credentials

9 Revision history

Issue	Date	Editor	Description of amendment
V1.0	June 2024	Afke Veenstra	Creation of the troubleshooting guide