GIGABYTE™

Gigabyte Server Management Console

Insyde Web GUI Interface for Firmware Version 23.08.xx

User's Guide

Rev. 1.0

Copyright

© 2026 Giga Computing Technology CO., LTD. All rights reserved.
The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of Giga Computing.
Changes to the specifications and features in this manual may be made by Giga Computing without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without Giga Computing's prior written permission.

Documentation Classifications

In order to assist in the use of this product, Giga Computing provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use of this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents.

For More Information

For related product specifications, the latest firmware and software, and other information please visit our website at http://www.gigabyte.com/Enterprise

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email:
marketing@gigacomputing.com

Table of Contents

Chapter 1 Getting Started....5
1-1 Software Requirement....5
1-2 Gigabyte Management Console Network Configuration....5
1-3 Log In Gigabyte Management Console....6
1-3-1 Required Browser Settings:....7
1-4 Quick Button and Logged-in User....7
1-5 Menu Bar....8
Chapter 2 Enter Gigabyte Management Console....10
2-1 Overview....10
2-2 Dashboard....11
2-3 Logs....13
2-3-1 System Event Log....13
2-3-2 Host Video Recorder....14
2-4 Hardware status....16
2-4-1 System Information....16
2-4-2 FRU Information....17
2-4-3 CPU Information....17
2-4-4 DDR Information....18
2-4-5 Inventory and LEDs....18
2-4-6 Sensors Readings....19
2-4-7 NIC Information (BIOS)....21
2-4-8 NIC Information (BMC)....21
2-4-9 NVMe/HDD Information (BIOS)....22
2-4-10 SMBIOS....23
2-5 Operations....24
2-5-1 Factory Reset....24
2-5-2 KVM....25
2-5-3 Firmware....35
2-5-4 Reboot BMC....36
2-5-5 SOL Console....36
2-5-6 Server power operations....37
2-5-7 Virtual front panel....38
2-5-8 Virtual Media....39
2-5-9 Boot Config....41
2-6 Settings....42
2-6-1 Alert....42
2-6-2 Alert Email....54
2-6-3 Alert Destination Configuration....55
2-6-4 Date and Time....57
2-6-5 Networks....58
2-6-6 VLAN....60
2-6-7 SOL....61
2-6-8 SNMP....63
2-6-9 iKVM and virtual media....64
2-6-10 Backup restore....65
2-6-11 Fan Profile....66
2-7 Security and access....67
2-7-1 Current users....67
2-7-2 LDAP....68
2-7-3 Users....79
2-7-4 Policies....80
2-7-5 Security settings....81
2-7-6 IP access control....82
2-8 Resource Management....85
2-8-1 Power....85
2-8-2 Power Schedule....85
2-9 BIOS (AMD BIOS joint feature)....87
2-9-1 Main....87

2-9-2 Advanced 88
2-9-3 AMD CBS 89
2-9-4 AMD PBS Option 90
2-9-5 Security 91
2-9-6 Power 92
2-9-7 Boot 93
2-10 Storage (will become visible when RAID Card is installed) 94
2-10-1 Storage System 94
2-10-2 Controllers 94
2-10-3 Event Log 96
Appendix 98
3-1 Appendix A - Assertion Condition (BIT EVENT) References 98
3-1-1 Sensor type: Temperature, Voltage, Current, Fan 98
3-1-2 Sensor type: Physical Security 98
3-1-3 Sensor type: Processor 98
3-1-4 Sensor type: Power supply 99
3-1-5 Sensor type: Other Units-based Sensor 99
3-1-6 Sensor type: Memory 99
3-1-7 Sensor type: Event Logging Disabled 99
3-1-8 Sensor type:Critical Interupt 100

Chapter 1 Getting Started

1-1 Software Requirement

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in video/keyboard/mouse functionality.

Supported Browsers

- Chrome latest version.
- Edge latest version
- Firefox (with limited support).

Note: It is advisable to use Chrome or IE for H5Viewer since Firefox has its own memory limitations.

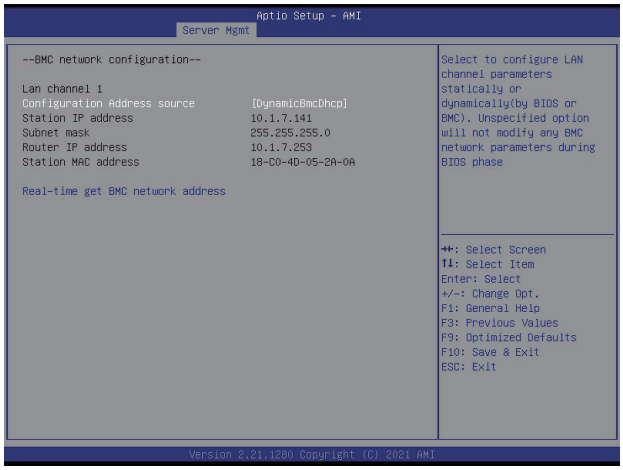
1-2 Gigabyte Management Console Network Configuration

Follow the instruction to enable the console redirection function.

1. You can gather the IP address on the POST screen.



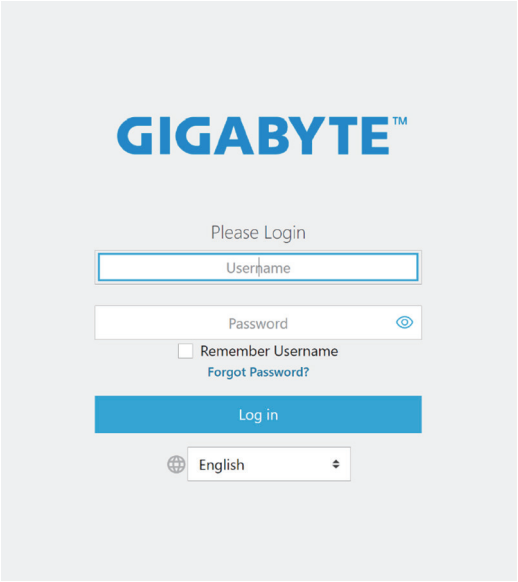
2. Or, Go to BIOS setup menu.
3. Select **Server Management**.
4. Select **BMC network Configuration**.
5. Define Configuration Address source to DynamicBmcDhcp or Static.
6. Save and Exit.
7. The **BMC IP Address** will appear on the **Station IP address** parameter.



8. Save the configuration and exit BIOS setup menu.

1-3 Log In Gigabyte Management Console

To access the Gigabyte Management Console, the MegaRAC utility will prompt you to enter the User Name and Password.

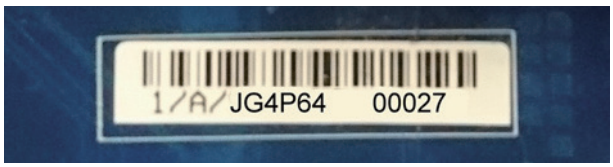


The fields are explained as follows:
For basic login to the MegaRAC UI, use the following login:

- **Username**: root
- **Password**: Refer to unique MB serial number.
- **US - English**: Changes the interface language.

NOTE!
If your motherboard / server version is older than G9 (upgrade version), then use the following login:
Username: root
Password: OpenBmc

This serial number can be found on the serial number sticker located on the motherboard of every GIGABYTE server motherboard and system. The unique pre-programmed password will be the last 11 characters of the serial number. For example, for the below serial number, the password will be “JG4P6400027

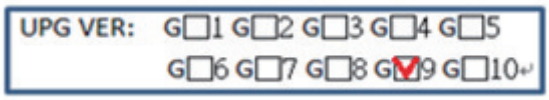


GIGABYTE will also affix new stickers that display the unique BMC password (example below) to both the product box (packaging) and to the CPU cover (for motherboards sold separately) or the server chassis.



Please see the reference guide below / attached for where to find locations of this sticker according to product / model type.

Products that have been implemented with this change will be indicated as version G9 on the “Upgrade Version” sticker located on the motherboard / motherboard anti-static packaging / server chassis / server packaging.



Remember Username: Check this option to remember your login credentials.
Forgot password: If you forget your password, you can generate a new one using this link.
Enter the user name, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

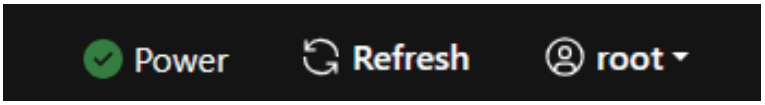
1-3-1 Required Browser Settings:

Allow file download from this site: For Internet Explorer, Choose **Tools** ->**Internet Options** ->**Security Tab**, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click **Custom level**
In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click **OK** to the entire dialog boxes.
For all Other Browsers, accept file download when prompted.
Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.
Enable cookies for this site: The icon indicates whether the cookies setting are enabled in browser.

Cookies must be enabled in order to access the website.

1-4 Quick Button and Logged-in User

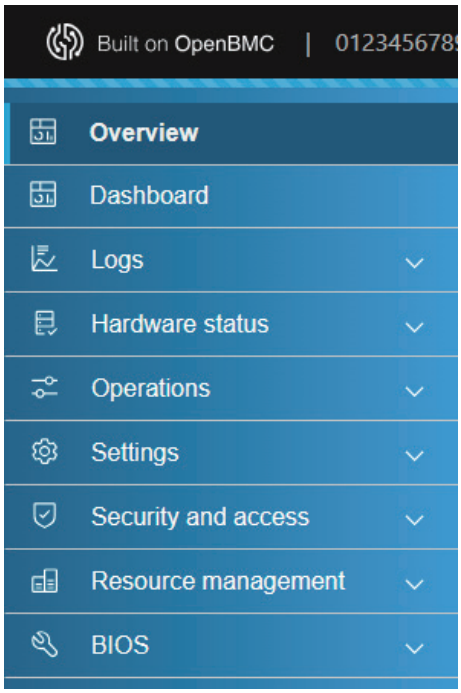
The user information and quick buttons are located at the top right of the Web GUI. A screenshot of the logged-in user information is shown below.



Power: This option shows Server power status and click the power icon to the Server power operations page.
Refresh: Click the icon to reload the current page.
root
The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions:
Profile setting: Click the root icon to change Profile settings.

1-5 Menu Bar

The menu bar displays the following:



Dashboard • Virtual Front Panel • Date & Time • Current Users • Virtual Media • Screen Preview • System Information • Network • Temperature • Voltage • Fan • Power information • CPU information • Event Log	**Settings** • Alerts • Alerts Policies • Alerts Email • Date & Time • Networks • VLAN • SNMP • Ikvm & Virtual Media • Syslog Settings • Fan Profile
Logs • System Event Log • Host Video Recorder	**Security and access** • Sessions • Current Users • LDAP • Users • Policies • Security Settings • IP Access Control
Hardware status • System information • FRU information • CPU Information • DIMM information • Inventory and LEDs • Sensor Readings • NIC information • NVMe information • System Component • SMBIOS	**BIOS** • Main • Advanced • AMD CBS • AMD PBS Option • Security • Power • Boot
Operations • Factory reset • KVM • Firmware • Unit Reset • SOL console • Server power operations • Virtual Front Panel • Virtual Media	**Storage** • Storage System • Controller • Physical Devices • Logical Devices • Event Log

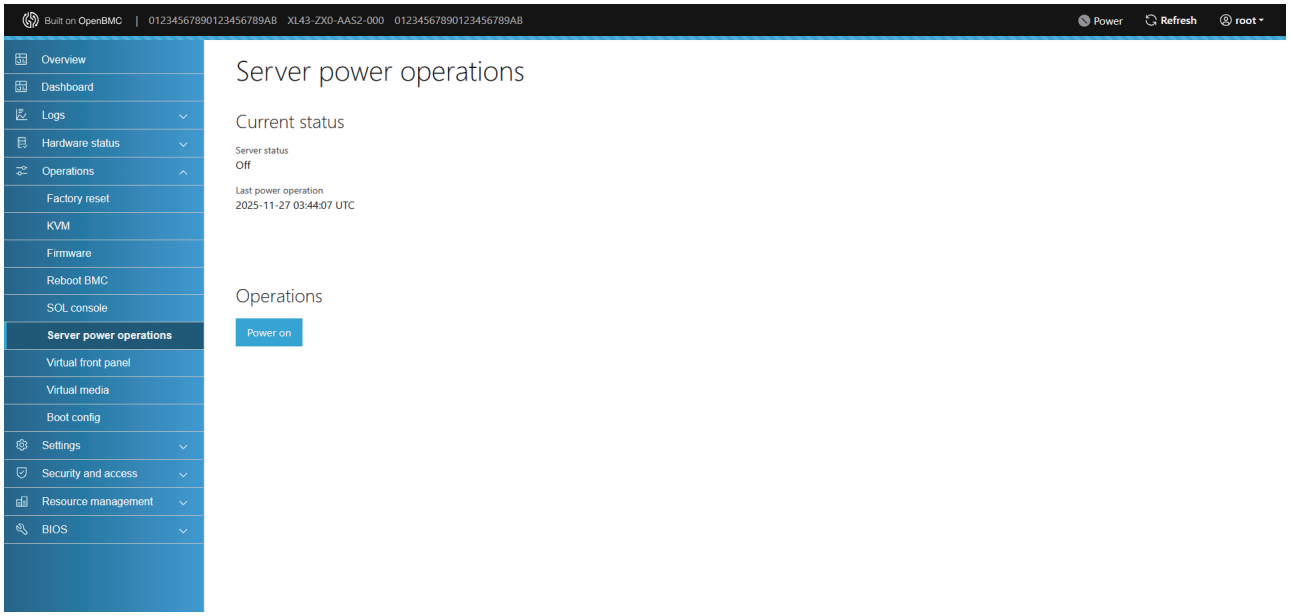
Chapter 2 Enter Gigabyte Management Console

2-1 Overview

Usage

Overview used to show the overall/important Host status in single page.

To open the Overview page, click **Overview** from the menu bar. It displays the following:



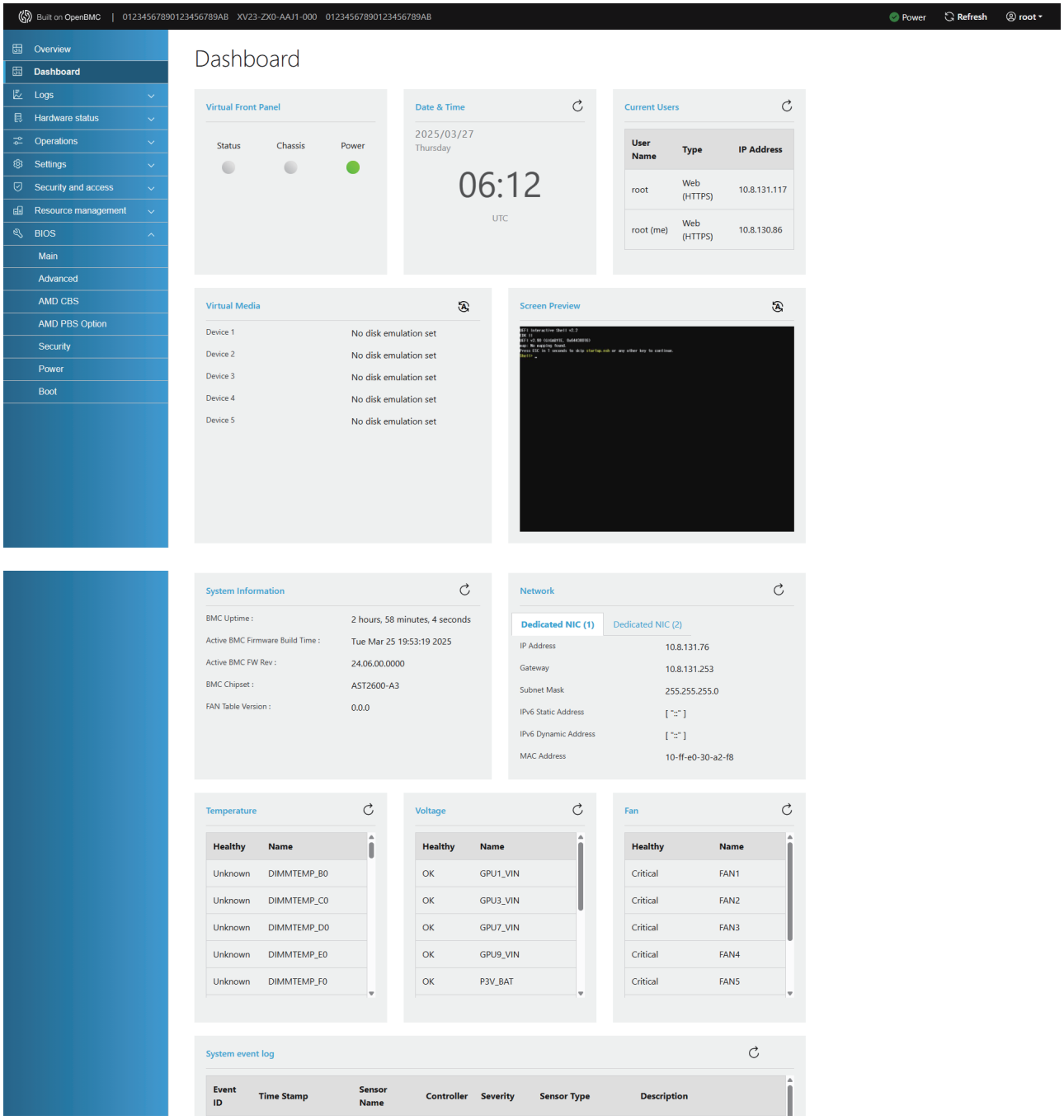
Overview includes the following information:

- System information
- Status information
- CPU information (AMD platform only)

Click the **"View more"** to display detailed information.

2-2 Dashboard

The Dashboard page gives the overall information about the status of a device.
To open the Dashboard page, click **Dashboard** from the menu bar. It displays the following:



Dashboard
A brief description of the Dashboard page is given below.

Virtual Front Panel
Displays Status LED, Chassis LED, and Power LED.

Date & Time
Displays BMC Date and Time.

Current Users
Displays connections status,included User Name, Connect Type, IP Address.

Screen Preview
Displays Virtual Media devices.

Virtual Media
Displays KVM screen.

System Information
Displays the technical information for the system.

Network
Displays Dedicated NIC and Shared NIC Network configurations (IP Address, Gateway, Subnet Mask, IPv6 Static Address, IPv6 Dynamic Address, MAC Address).

Temperature
Displays Host Temperature sensors Healthy and Name.

Voltage
Displays Power Voltage Healthy and Name.

Fan
Displays Host Fan Healthy and Name.

Power Information
Displays current power consumption reading and power cap enabled status.

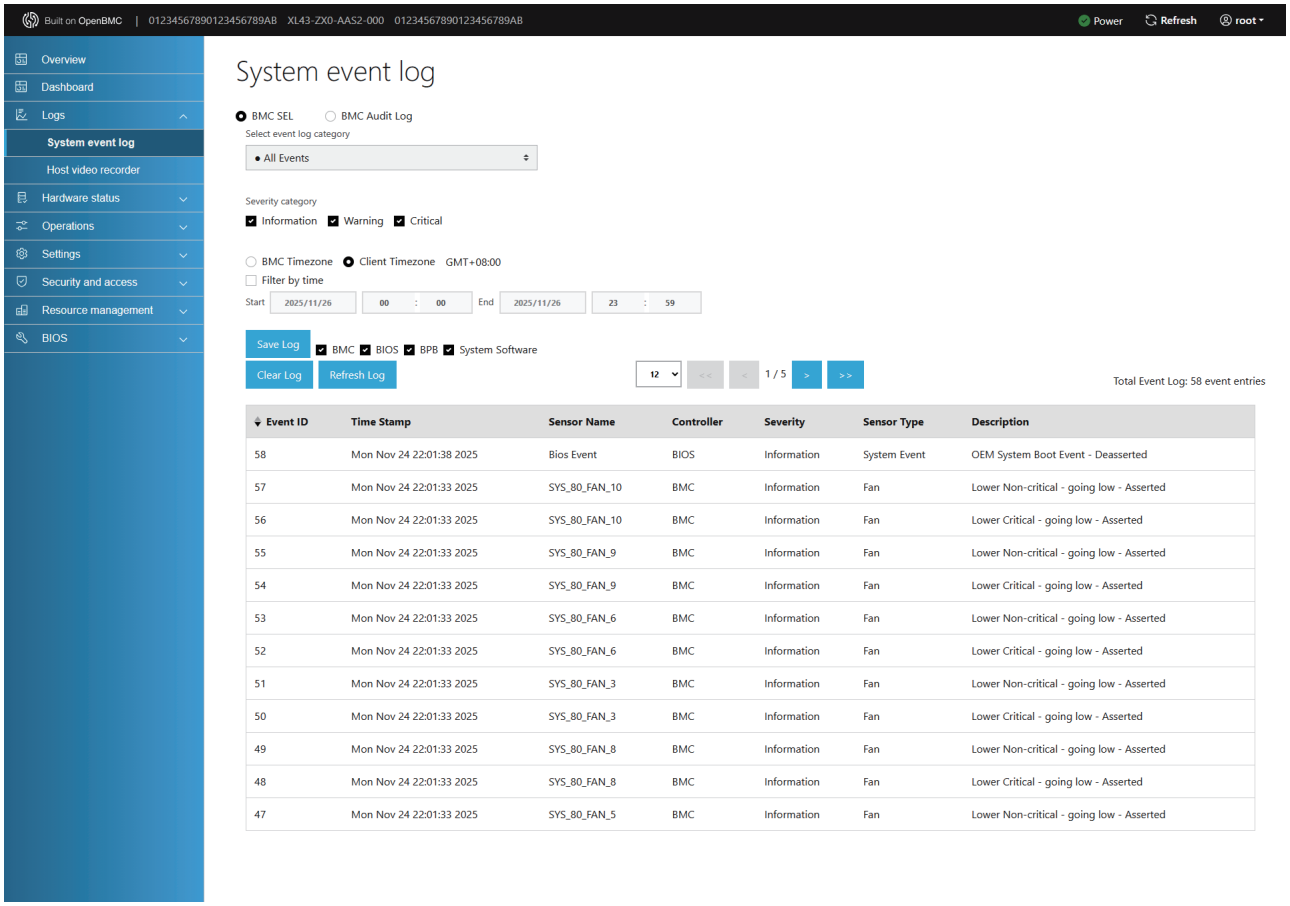
CPU Information
This section provides details about the CPU installed in each socket of the system. The following information is displayed for each socket: The various options of CPU information are given below:

- **Family ID:** This identifies the processor family.
- **Model ID:** This shows the specific model identifier for the processor.
- **Stepping ID:** This is an identifier for the processor's stepping.

Event Log
Displays the list of event logs occurred by the different sensors on this system.

2-3 Logs

2-3-1 System Event Log



Event ID	Time Stamp	Sensor Name	Controller	Severity	Sensor Type	Description
58	Mon Nov 24 22:01:38 2025	Bios Event	BIOS	Information	System Event	OEM System Boot Event - Deasserted
57	Mon Nov 24 22:01:33 2025	SYS_80_FAN_10	BMC	Information	Fan	Lower Non-critical - going low - Asserted
56	Mon Nov 24 22:01:33 2025	SYS_80_FAN_10	BMC	Information	Fan	Lower Critical - going low - Asserted
55	Mon Nov 24 22:01:33 2025	SYS_80_FAN_9	BMC	Information	Fan	Lower Non-critical - going low - Asserted
54	Mon Nov 24 22:01:33 2025	SYS_80_FAN_9	BMC	Information	Fan	Lower Critical - going low - Asserted
53	Mon Nov 24 22:01:33 2025	SYS_80_FAN_6	BMC	Information	Fan	Lower Non-critical - going low - Asserted
52	Mon Nov 24 22:01:33 2025	SYS_80_FAN_6	BMC	Information	Fan	Lower Critical - going low - Asserted
51	Mon Nov 24 22:01:33 2025	SYS_80_FAN_3	BMC	Information	Fan	Lower Non-critical - going low - Asserted
50	Mon Nov 24 22:01:33 2025	SYS_80_FAN_3	BMC	Information	Fan	Lower Critical - going low - Asserted
49	Mon Nov 24 22:01:33 2025	SYS_80_FAN_8	BMC	Information	Fan	Lower Non-critical - going low - Asserted
48	Mon Nov 24 22:01:33 2025	SYS_80_FAN_8	BMC	Information	Fan	Lower Critical - going low - Asserted
47	Mon Nov 24 22:01:33 2025	SYS_80_FAN_5	BMC	Information	Fan	Lower Non-critical - going low - Asserted

BMC SEL

This page displays the list of event logs occurred by the different sensors on this device.

Select event log category

The category could be either All Events, BMC Generated Events, BIOS Events, System Software Generated Events, SMI Handler Events, System Management Software Events, OEM Events, Remote Console Software Events, Terminal Mode Remote Console Software Event.

Severity category

- **Information:** This category includes non-critical events that provide general information about the system's operation.
- **Warning:** Events in the warning category indicate potential problems that may not require immediate attention.
- **Critical:** Critical logs represent serious problems that usually require immediate attention. These events may indicate system failure, hardware failure

Save Log

Click on the Save Log button to save all Log entries.

Clear Log

Click on the Save Log button to remove all Log entries.

Refresh Log

Click on the Refresh Log button to redisplay all of the current set of event records. The Log does not automatically refresh, in order to allow review of the entries.

NOTE!

Support circular mode only. The circular mode means older SELs will be automatically cleared when the SEL is almost full.

BMC Audit Log

Audit Log page will display all the system events occurred in this device that has been already configured.

Save Log

Click on the Save Log button to save all Log entries.

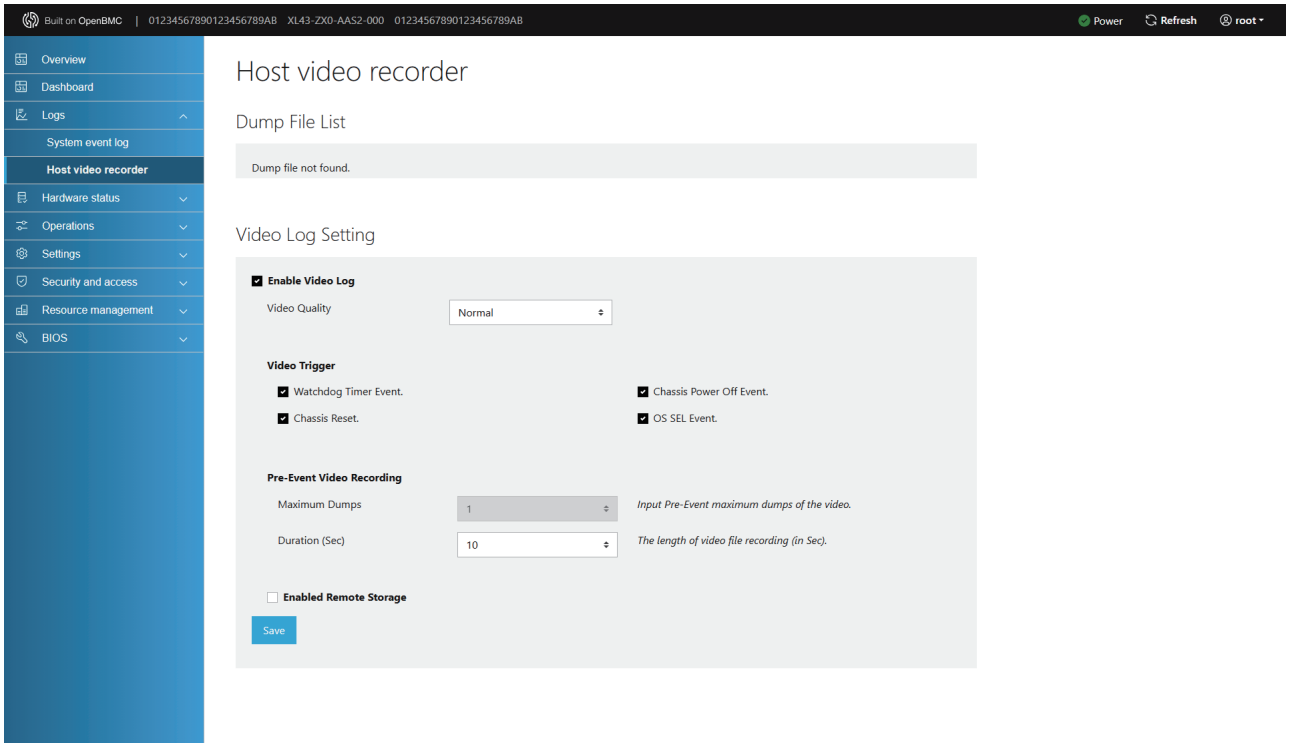
Clear Log

Click on the Save Log button to remove all Log entries.

Refresh Log

Click on the Refresh Log button to redisplay all of the current set of event records. The Log does not automatically refresh, in order to allow review of the entries.

2-3-2 Host Video Recorder



Dump File List

This page displays dump file list.

Video Log Setting

Enable Video Log

Toggle to enable/disabled host video recorder feature.

Video Quality

Select the video quality as Low, High, and Normal from the Video Quality drop-down list.

Video Trigger

Video Trigger Settings is used to configure the events that will trigger auto video recording function. Event List shows the list of available events to be configured. The events are:

- Watchdog Timer Event
- Chassis Power Off Event
- Chassis Reset
- Host Crash Event (CATERR/IERR for Intel, CPER for Nvidia, and RAS error for AMD ...etc)

Pre-Event Video Recording

Pre-Event Video Recording is to edit the Pre-Event video recording configurations.

- **Maximum Dumps:** Enter the pre-event maximum dumps of the video.
- **Duration (Sec):** Select the duration in seconds (10-60) from the drop-down list.

Enabled Remote Storage

Check to enable the Remote Video Support. NOTE: By default, video files will be stored in the local path of BMC. If remote video support is enabled, then the video files will be stored only in the remote path, not within BMC.

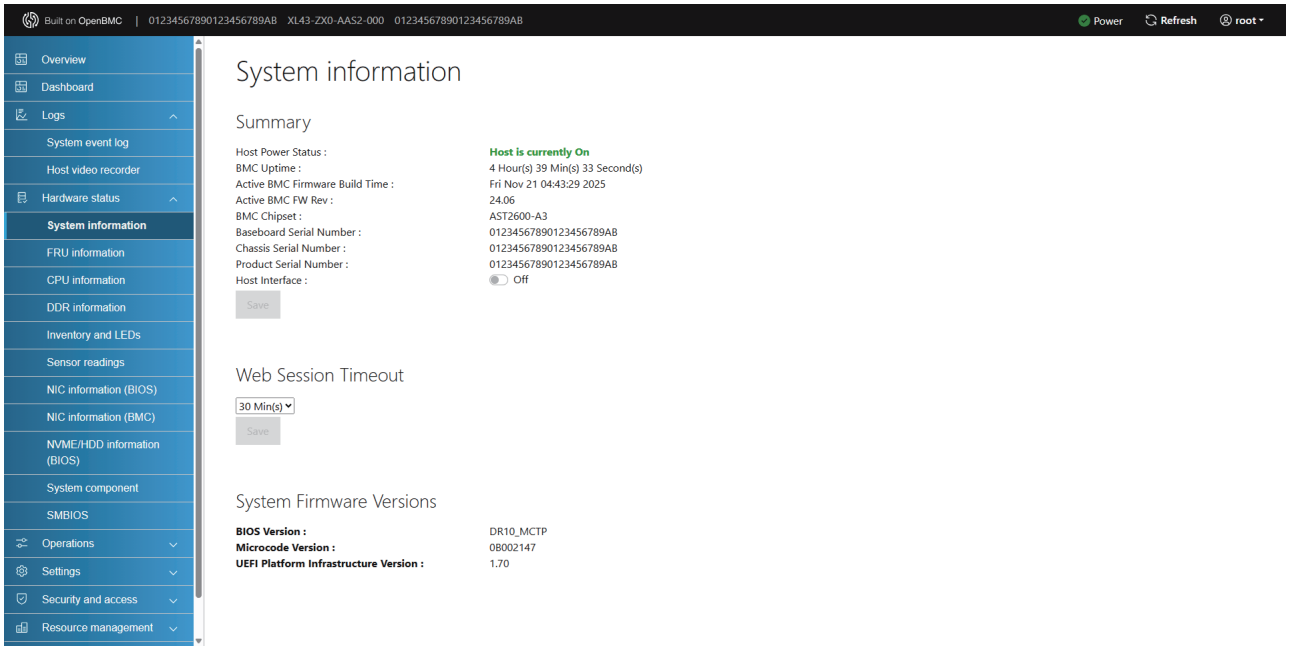
2-4 Hardware status

The Hardware Status page displays the following information:

- System Information
- FRU information
- CPU information
- DDR information
- Inventory and LEDs
- Sensor readings
- NIC Informatiion (BIOS)
- NIC Informatiion (BMC)
- NVMe/HDD information
- System Components
- SMBIOS

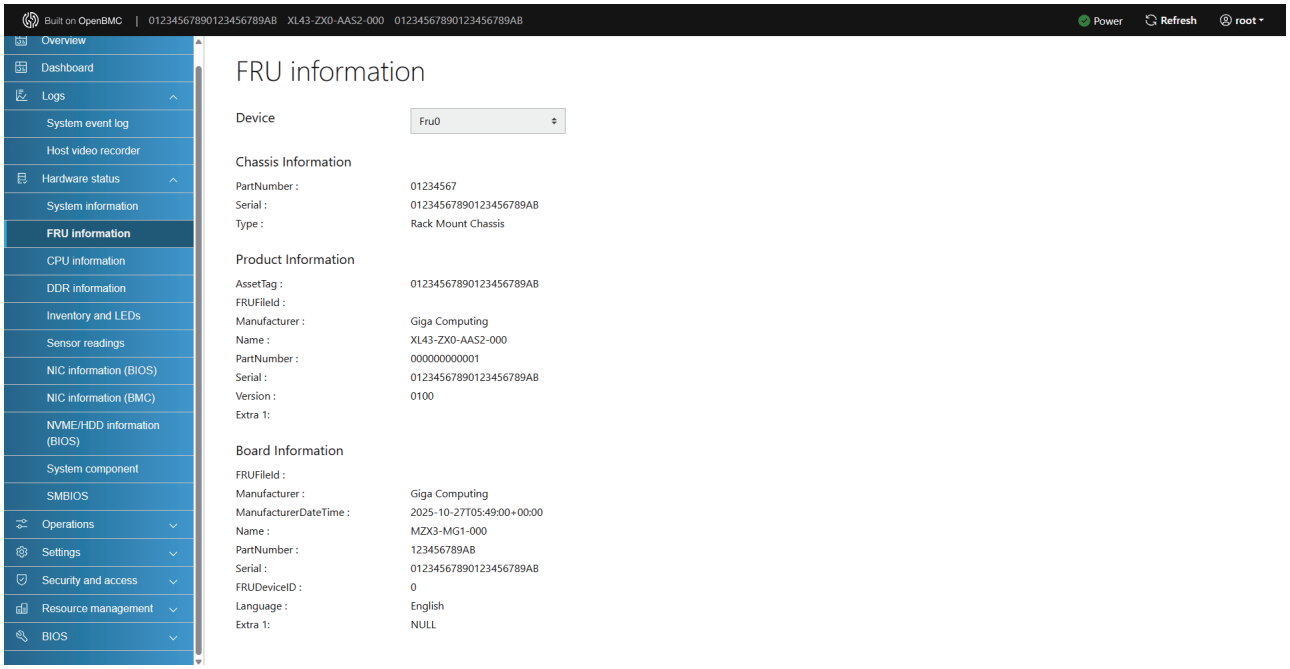
2-4-1 System Information

This page displays information about system information.
To open the System Information page, click **System Information** from the menu bar. It displays the following:



2-4-2 FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information.
To open the FRU Information page, click **FRU Information** from the menu bar. It displays the following:

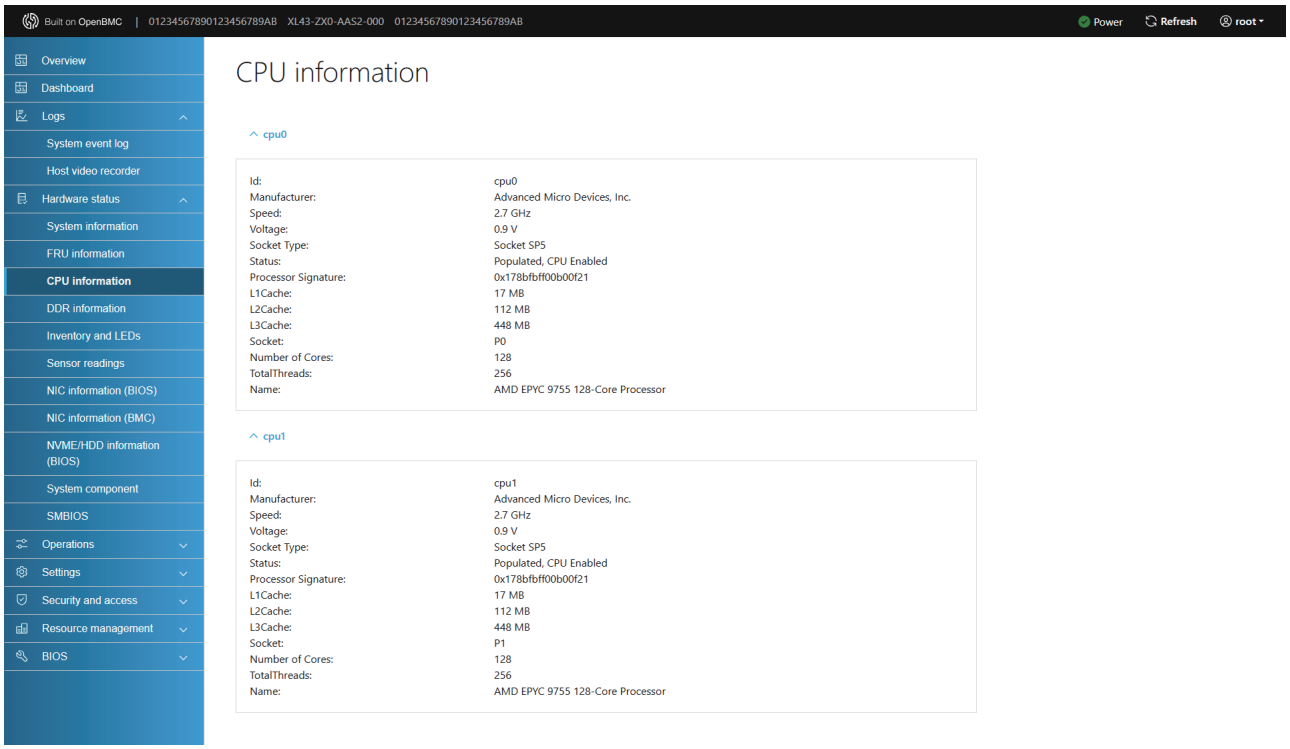


Device

Select to display FRU0 or FRU1 information.

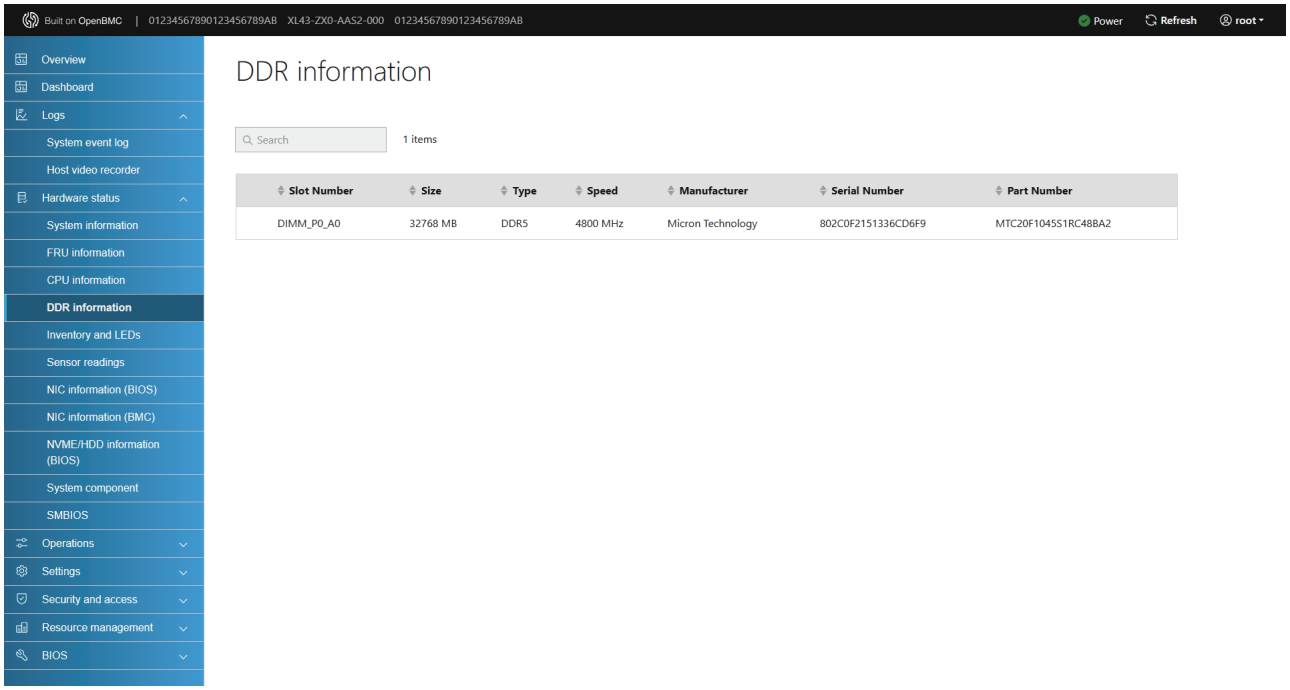
2-4-3 CPU Information

This page displays installed CPU information.
To open the CPU Information page, click **CPU Information** from the menu bar. It displays the following:



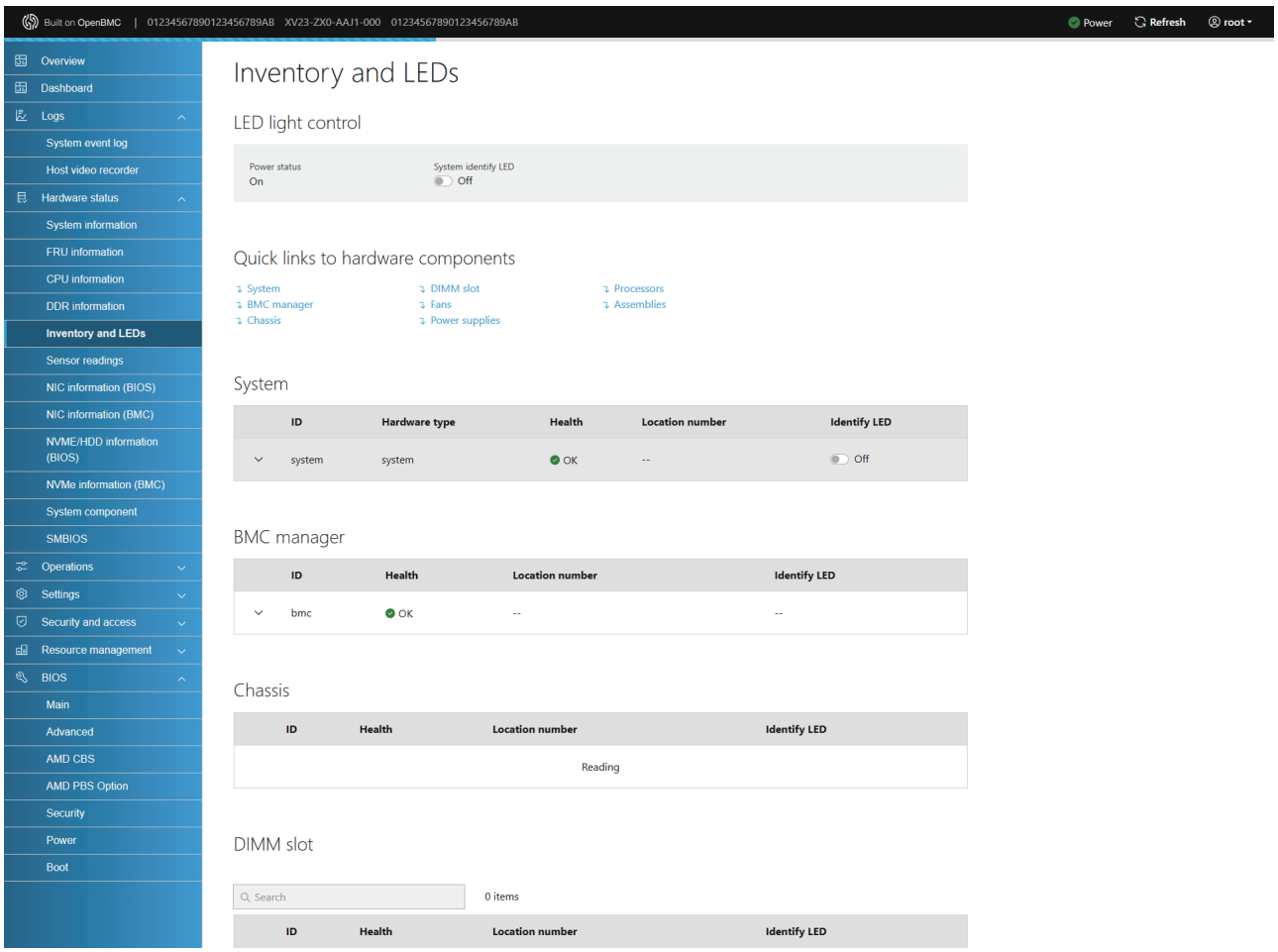
2-4-4 DDR Information

This page displays installed DDR information.
To open the DIMM Information page, click **DDR information** from the menu bar. It displays the following:



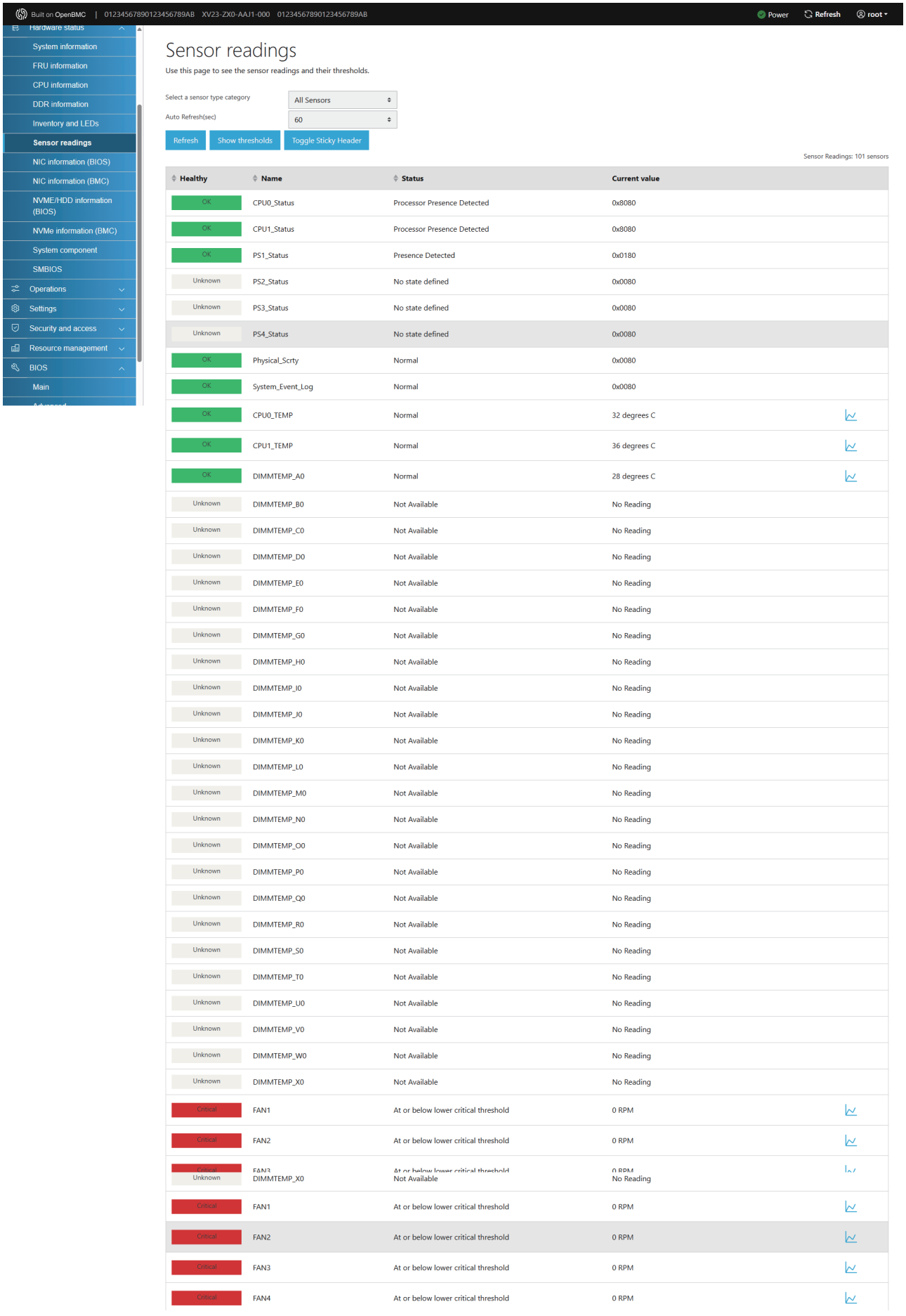
2-4-5 Inventory and LEDs

This page displays Inventory and LEDs information.
To open the this page, click **Inventory and LEDs** from the menu bar. It displays the following:



2-4-6 Sensors Readings

This page displays Sensor Readings information.
To open the this page, click **Sensor Readings** from the menu bar. It displays the following:



Sensor owner

Displays the Sensor Owner information.

Select a Sensor Type Category

- All Sensors
- Management Subsystem Health
- Button / Switch
- Processor
- Drive Slot
- Watchdog2
- Critical Interrupt
- Memory
- Power Supply
- Physical Security
- Power Unit
- System Event
- Event Logging Disabled
- Voltage Sensors
- All Sensors
- Fan Sensors
- Temperature Sensors
- OEM Sensors

Auto Refresh(sec)

Select the Auto Refresh time by drop-down list. Option available: 5/ 10/ 15/ 30/ 60/ 150/ 300/ Never

Refresh

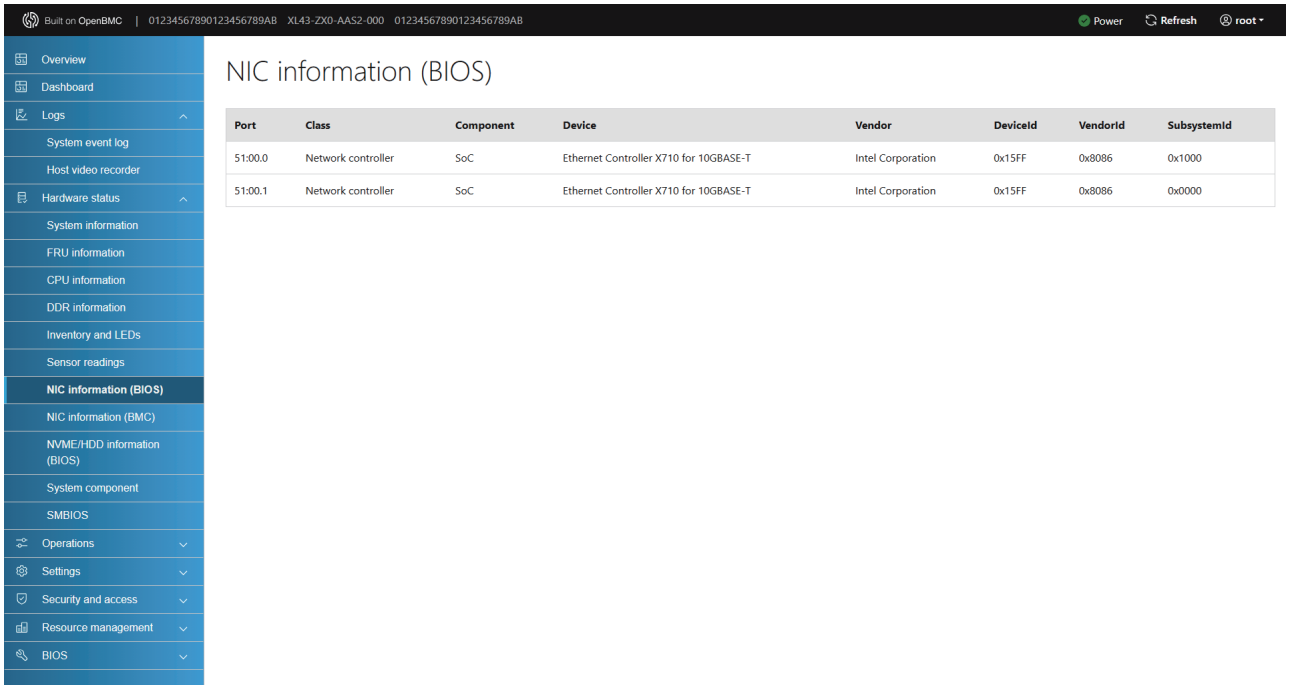
Click on the Refresh button to refresh the page.

Show Thresholds

Click on the Show Thresholds button to view non-critical, critical and non-recoverable thresholds.

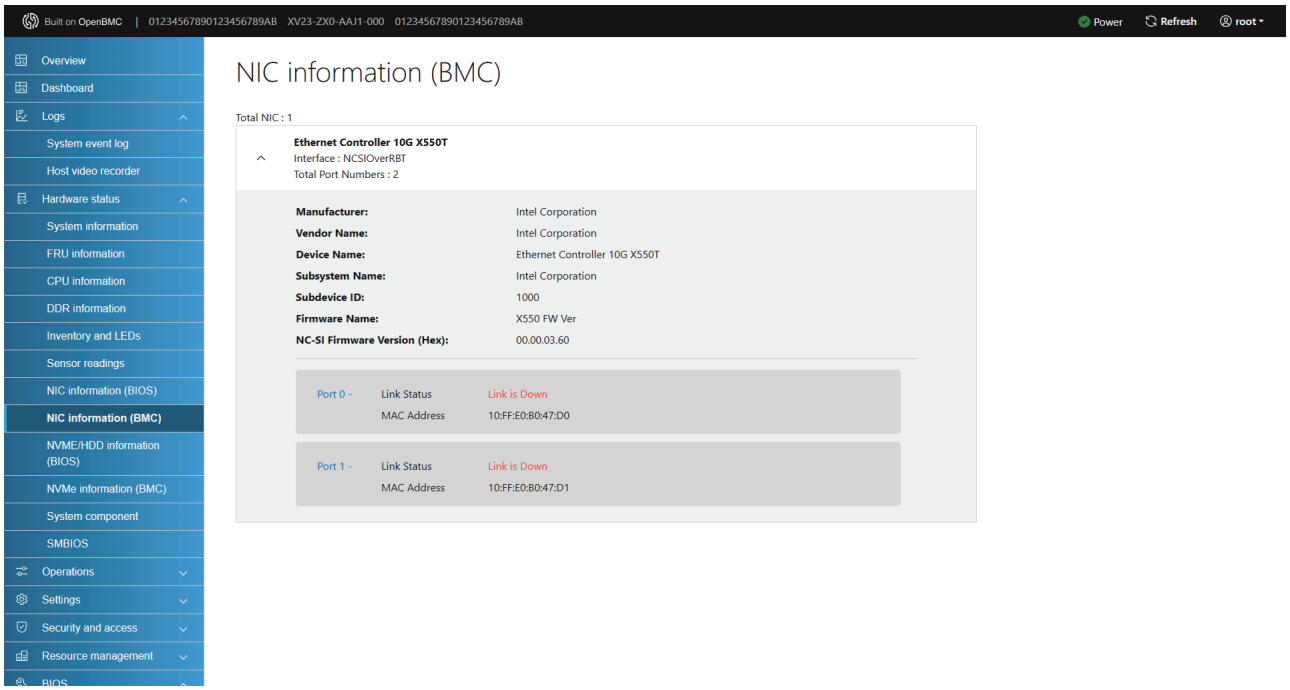
2-4-7 NIC Information (BIOS)

This page displays all detected NICs on this device. It allows you to on-board NICs, add-on NICs.
To open the this page, click **NIC Informatiion (BIOS)** from the menu bar. It displays the following:



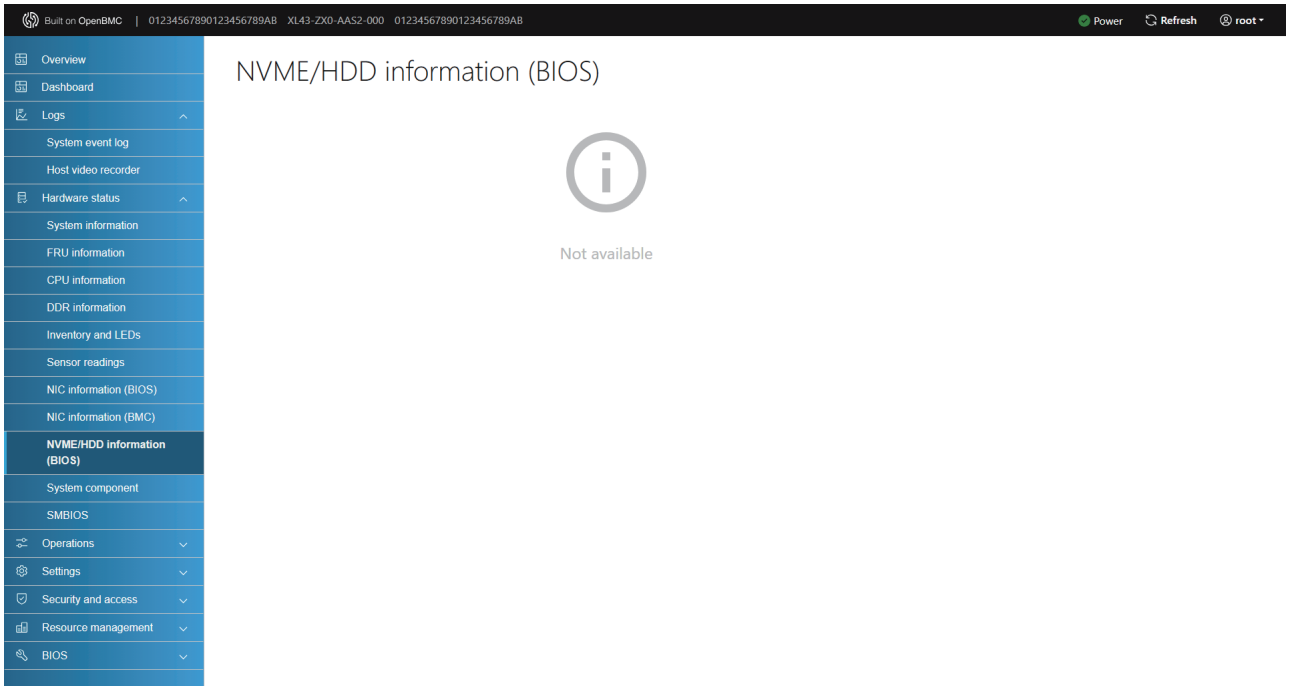
2-4-8 NIC Information (BMC)

This page displays all detected NICs on this device. It allows you to on-board NICs, add-on NICs.
To open the this page, click **NIC Informatiion (BMC)** from the menu bar. It displays the following:



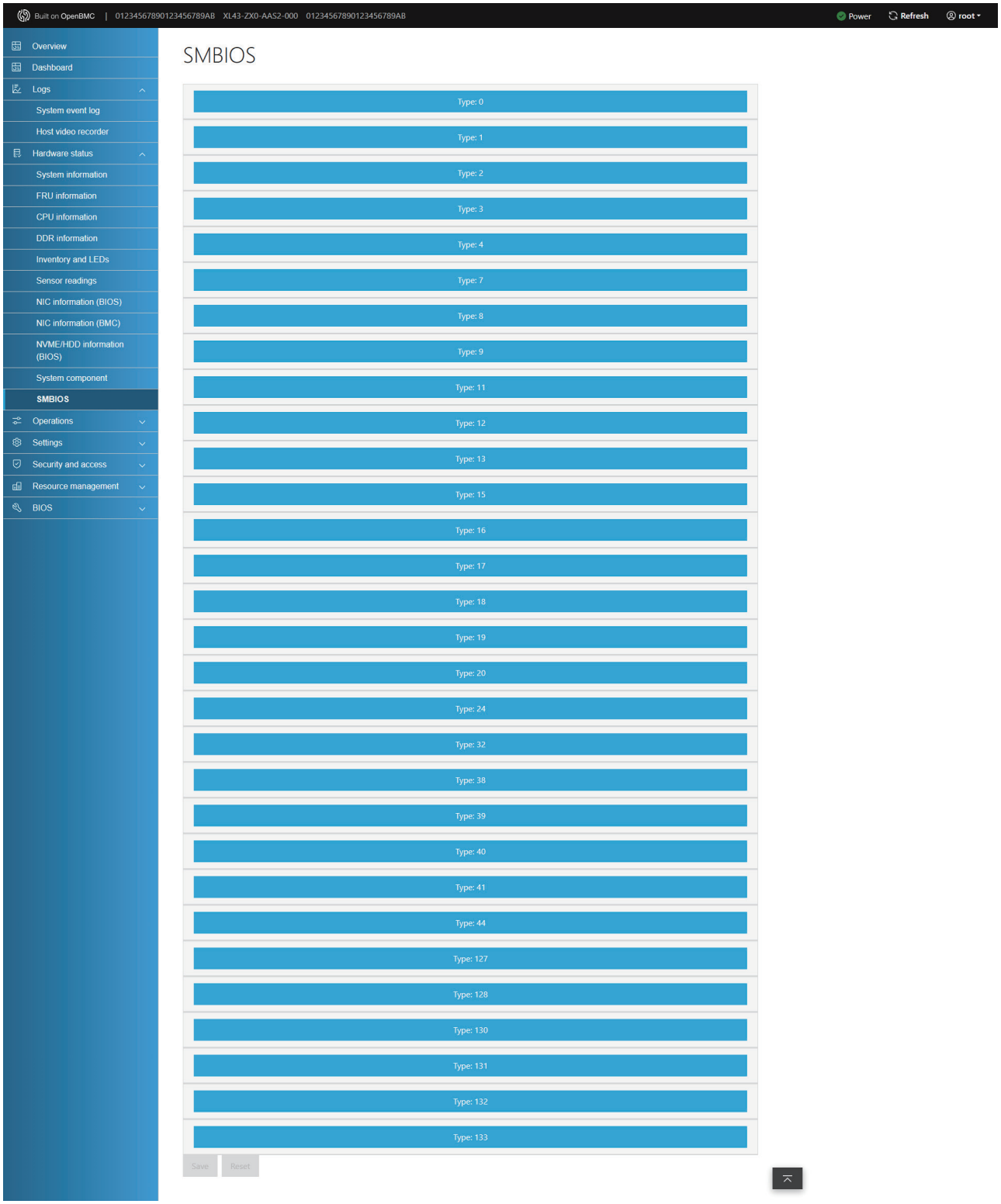
2-4-9 NVMe/HDD Information (BIOS)

This page displays all detected NVMe device and other hard drive devices in this system.
To open the this page, click **NVMe/HDD informatiion (BIOS)** from the menu bar. It displays the following:



2-4-10 SMBIOS

To enable this function, turn on the host and wait for the BIOS to upload the relevant data.
Display the SMBIOS.
Save: Click to save the settings.
Reset: Click to reset the changes.

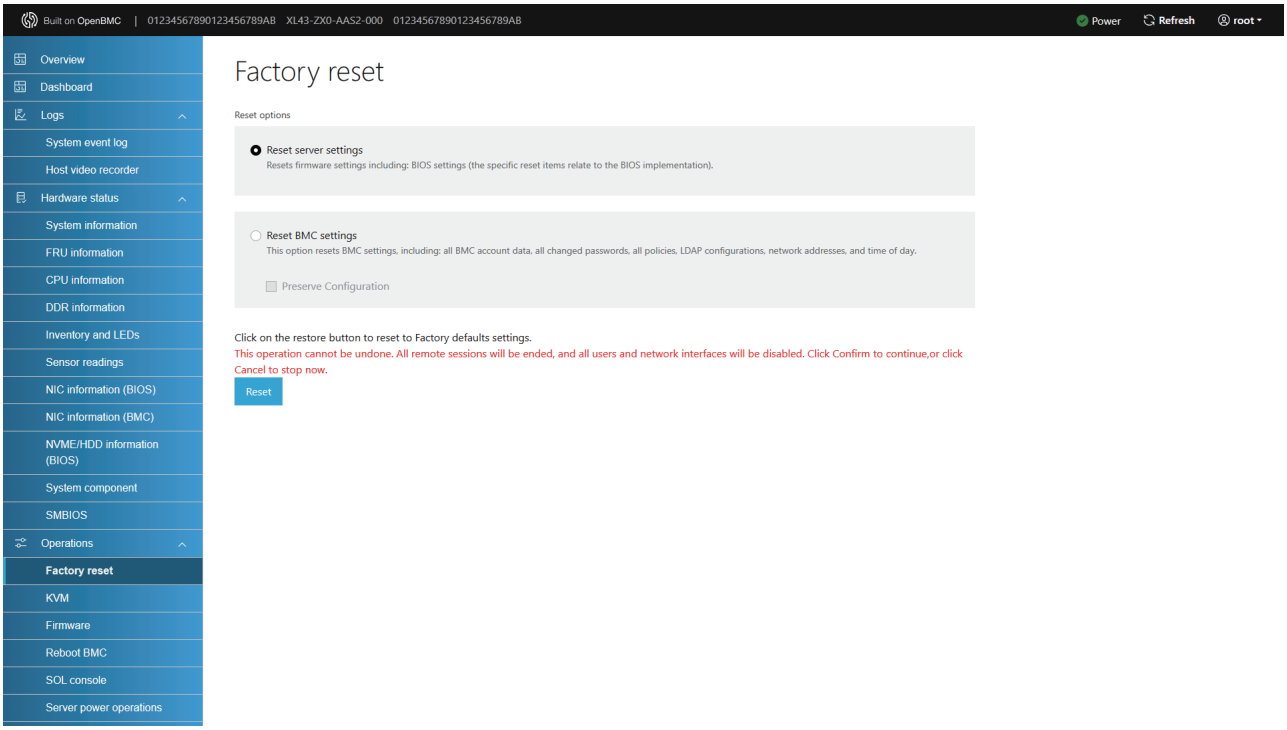


2-5 Operations

2-5-1 Factory Reset

In Web GUI, this option is used to reset the factory defaults of the device firmware, BIOS settings, BMC settings.
Warning: Please note that after entering reset factory widgets, other web pages and services will not work.
All open widgets will be closed automatically. The device will reset and reboot within a few minutes.

To open Factory Reset page, click Operations > Factory Reset from the menu bar. A sample screenshot of the Factory Reset Defaults Page is shown below.



Preserve Configuration: Select the settings to be preserved.

Reset: Click on the Reset button to reset factory settings.

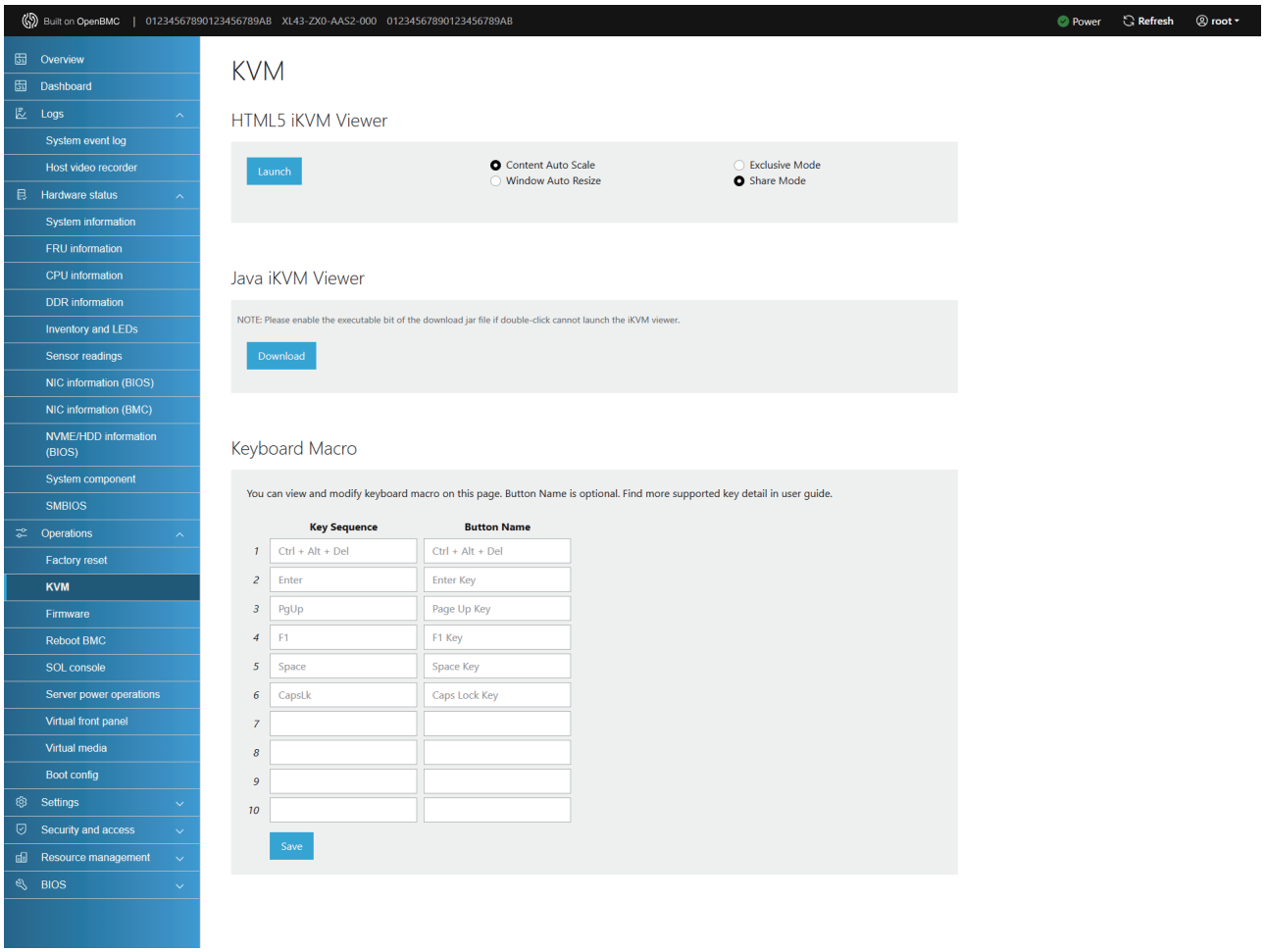
2-5-2 KVM

The system and browser requirements for Remote Control are given below.

System Requirements

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be a lag in the video/keyboard/mouse functionality.

To open KVM, click Operations > KVM from the menu bar. A sample screenshot of the KVM Page is shown below.



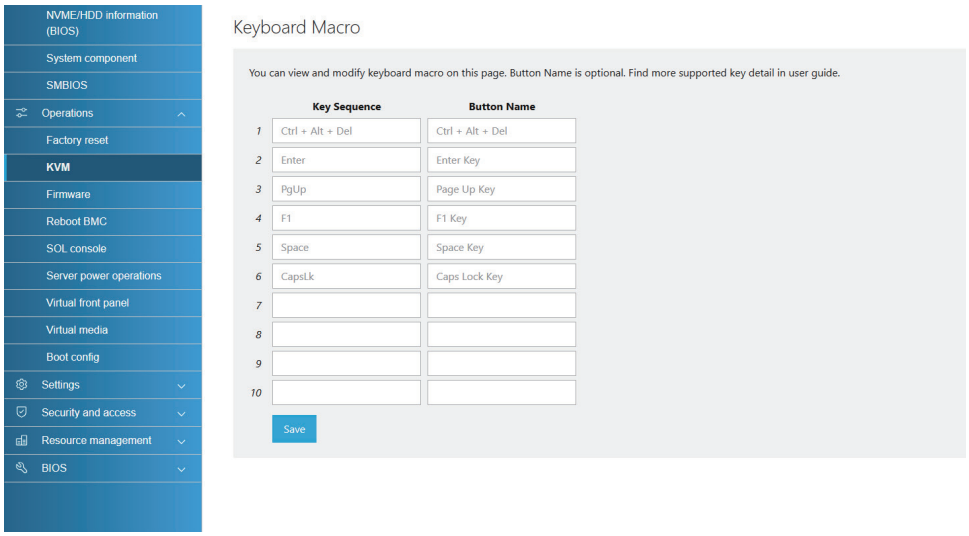
A detailed description of the menu items is given below.

HTML5 iKVM Viewer

Click the **Launch** button to launch the H5viewer window.

Keyboard Marco

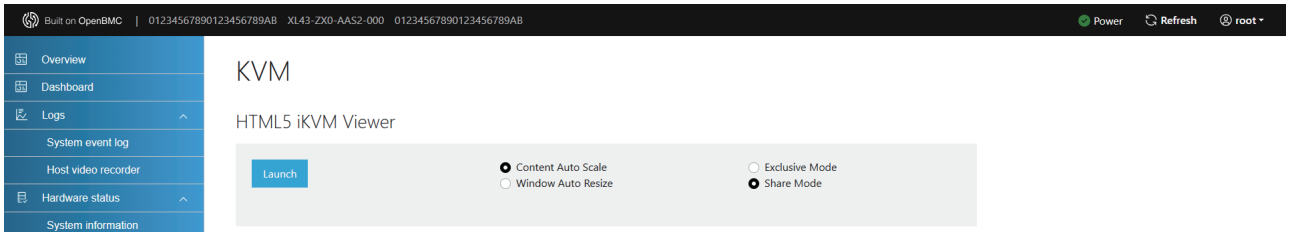
You can view and modify keyboard macro on this page. Button Name is optional.



Java iKVM Viewer

Click the **Download** button to download the Java iKVM Viewer jar file.

iKVM Setting Panel



Content Auto Scale

If this function is enabled, the iKVM display area will be scaled to fit the window automatically.

Window Auto Resize

If this function is enabled, the window size will be resized to the size of iKVM display area automatically.

Share Mode

If this function is enabled, the iKVM Server should try to share the desktop by leaving other clients connected.

Exclusive Mode

If this function is enabled, the iKVM Server should give exclusive access to this client by blocking all other clients.

Exclusive Mode rule:

1. Only the first connection can activate Exclusive mode.
2. If the second connection or other enable Exclusive mode, they can't eject other connection.
3. Some of client can not connect due to Exclusive mode, the viewer should show the reason.



1. Client Mode status (Share Mode or Exclusive Mode)
2. Host resolution
3. iKVM update frame per second
4. Current virtual keyboard layout

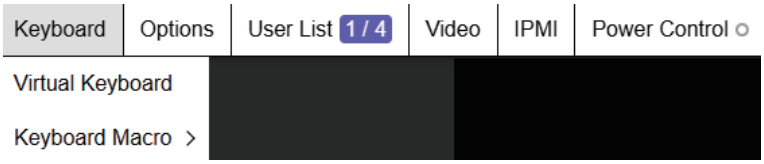
NOTE! If it shows **(View Only)** in front of the title indicator, which means the user can not control mouse, keyboard, power control menu, ipmi menu, keyboard menu and option menu.

Remote Mouse

- Control the host remotely via mouse.
- Supported mouse operations: left click, right click, middle click, move, drag and drop, mouse wheel.

Remote Keyboard

- Control the host remotely via a keyboard.
- Supported keys: all keys on a standard keyboard.



Virtual Keyboard

- Virtual Keyboard is an on-screen keyboard.
- Click the button **Keyboard** -> **Virtual Keyboard** to launch the virtual keyboard.

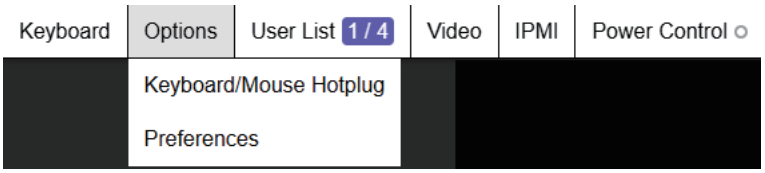
- The language layout of the virtual keyboard can be changed.
  1. Right click on the virtual keyboard to open the language layout menu.
  2. Select a language to change the keyboard layout.

- Winkey usage: It depends on host OS.
  1. WinKey + <other key>: WinKey Shortcuts
  2. Double-click WinKey: Open and close the Start Screen or Start Menu

Keyboard Macro

- This feature provides many hotkeys, shortcuts, and macros for use with a keyboard.
  Go to **Keyboard** -> **Keyboard Macro**
  1. Keyboard Macro list
     - Default Macro
     - Ctrl+Alt+Del
     - Alt+Tab
     - Alt+Esc
     - Ctrl+Esc
     - Alt+Space
     - Alt+Enter
     - Alt+Hypen
     - Alt+F4
     - Alt+PrntScn
     - PrntScn
     - F1
     - Alt+F1
     - Pause
  - Custom Macro: Users can define at web > Remote Control > Keyboard Macros page
  2. Hold key: When the hold key is enabled, it will emulate when the user presses a key.

Options

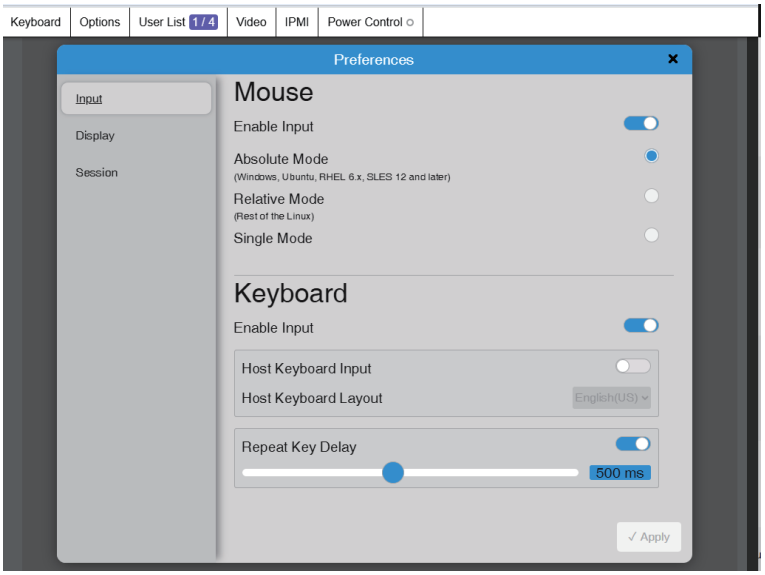


Keyboard Mouse Hotplug

Click to activate Keyboard Mouse Hotplug.

Preferences

Click to open preferences.



Input

Mouse

- Allow different modes of mouse to be set on the BMC, so that the client can use the mouse control correctly.
  - If enabling mouse input, it will send mouse events from client to host, and vice versa.

- Mouse mode (depends on the host OS).
  - **Absolute mode** - use the absolute location on srceen to address.
  - **Relative mode** - use the bias value to move Host cursor (Ex: X axis +1 means move to left a unit).
  - **Single mode** - behavior like Relative mode. But the client cursor is hidden to avoid user confusion with Host cursor image.

NOTE!

- Use **absolute mode** first. When **absolute mode** not work, use candidate **relative/single mode** to move the cursor. (eg: bios envirnment)
- **Single mode** can be regarded as enhanced **relative mode**. It provides a better user experience.
- Enter and Exit single mode
  - **Enter:** Click the viewer GUI to enter.
  - **Exit:** press **esc** or combo key **ctrl+6** to leave.

Keyboard

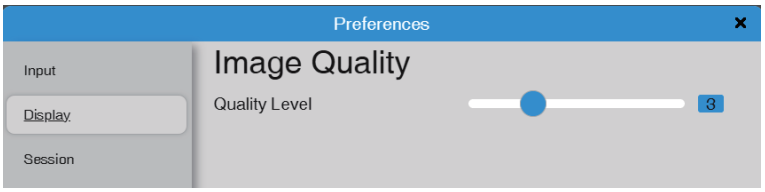
- Host keyboard input switch:
  - Host keyboard input switch is used to make client keyboard layout(Not virtual keyboard) mapping host keyboard layout.
  - For example, If client keyboard layout is JP and the host keyboard layout is US, and then you press "=" on the client keyboard, the host will display "^" character.

- Host keyboard Layout:
  - Set Host keyboard Layout's language.

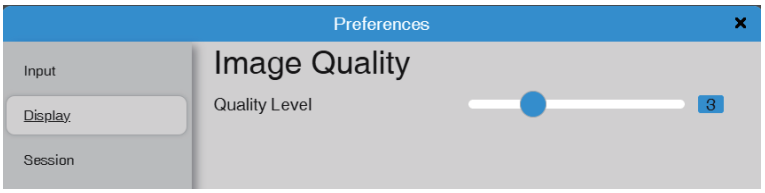
- Provide multi language keyboard layouts to be used, as well as setting the key press repeating timeout period.
  - If enabling keyboard input, it will send keyboard events from the client to host, and vice versa.
  - Change virtual keyboard layout.
  - Adjust key down repeat delay. Range is 0 - 1000 ms.

Display

Image Quality
Control the host screen Quality. The more, the sharper the screen becomes.

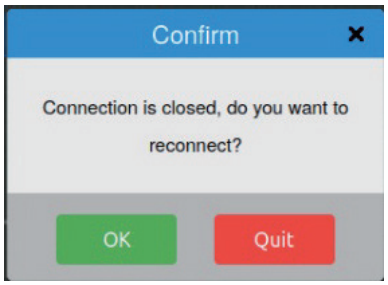


Session



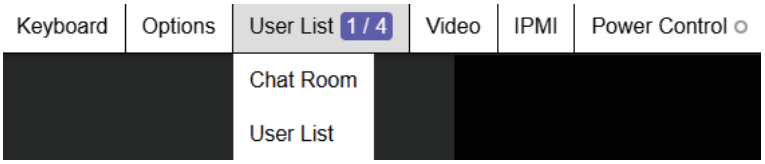
Timeout
- The "Session Timeout" contains two options:
  1. Enable Session Timeout:
     - Enable or disable session timeout
  2. Set Session Timeout:
     - Set the value of the session timeout.
     - The value of session timeout is between 1 to 99999 minutes.

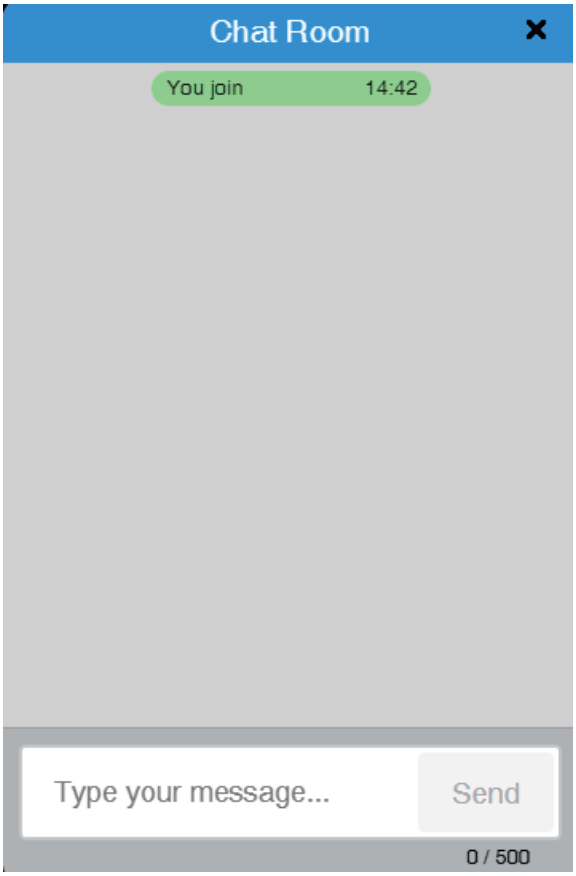
Additional Confirmation Window
- If the network is disconnected for some reason, this dialog will appear to notify user.
- This dialog user can chose the reconnect or not



User List

Chat Room



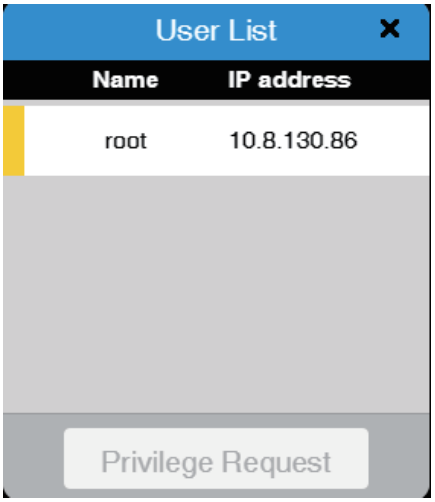


1. Click to open chatroom.
2. Greet message. Include user joined and leave.
3. Normal message bubble. Show the user name, ip address and time.
4. Whisper message bubble.
5. Input message area. Press "Enter" key or click "Send" button to send message.

- How to whisper other user
  - You can also send whisper messages by using the format on the message @<username> <message>
  - Notice: Currently, the maximum size of message is 500 words.

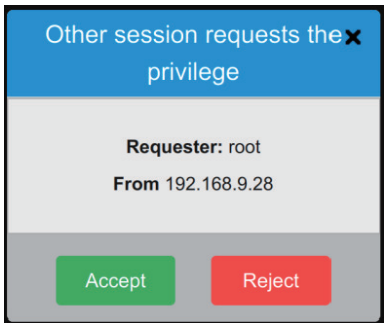
User List

- Click to open the userlist.



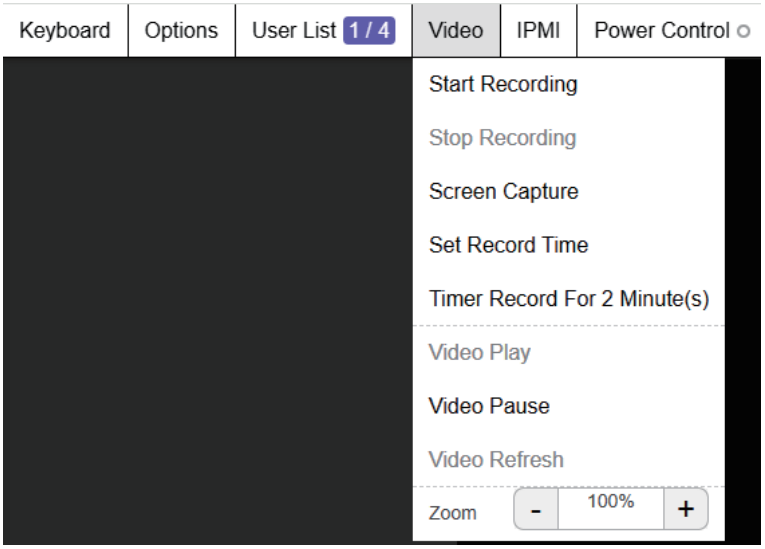
1. Show number of users who are using iKVM.
2. Click to open userlist window
3. 3Drag area
4. iKVM users, the yellow head bar is current privilege owner who can control ikvm, and the grey head is not.

- The user can click the Privilege Request button to request iKVM control privileges.
- The user who has control privileges will receive the privilege request from the (Video only) user.



Video

- Click to open record functions.



1. Start to record video of iKVM. The video format is webm.
2. Stop the video recording then save file to local filesystem. Capture the screen of iKVM then save PNG file to local filesystem.
3. Setup recording time for timer recording function, default value is 1 minute. Maximum is 180 minutes.
4. This is will be displayed as Timer recording for x minute(s) which x depends on recording time. Clicking this function will record video for x minutes. User can use the "Stop recording" function to save
5. the video before timeout.
6. Play the host display
7. Pause the host display
8. Refresh the host display
9. Zoom in/out the host display

IPMI

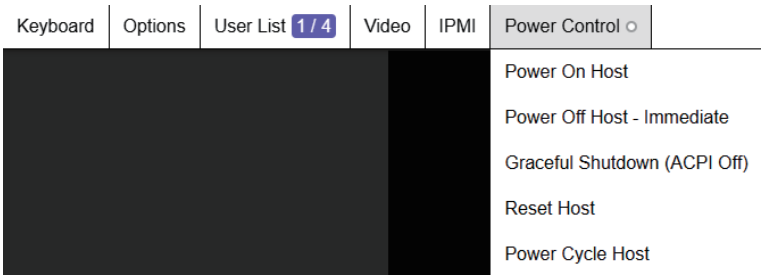
- Click to open ipmi window.



10. Enter the ipmi command to input field and press "Enter" key to send.
11. The ipmi request command.
12. The ipmi response command.
    - NOTE: So far, the maximum size of command is 500 words.

Power Control

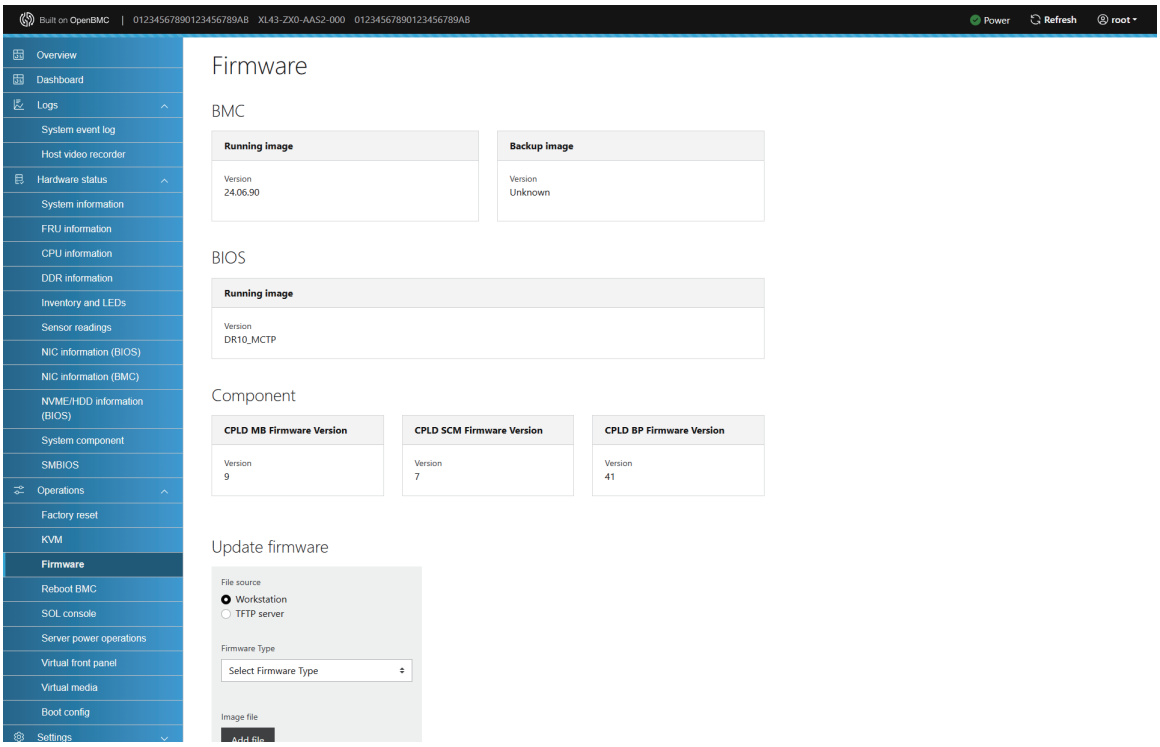
- Click to open power control function.



1. A.C. Power On the Host CRB Board
2. A.C. Power Off the Host CRB Board
3. Emulates OS Software Shutdown
4. A.C. Power reset Host CRB Board
5. A.C. Power Cycle Host CRB Board

2-5-3 Firmware

This page takes you through the process of firmware up gradation. A reset of the box will automatically follow if the upgrade is completed or canceled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.



Update Firmware

File Source

Select the file source:

- Workstation: Upload the firmware file directly from your local computer.
- TFTP Server: Download the firmware file from a remote server over the network using TFTP.

Firmware Type

- BMC
  - Active (physical BMC flash2)
  - Backup (physical BMC flash1)
  - Both

- BIOS
  - Active (physical BMC flash2)
  - Backup (physical BMC flash1)

- MB CPLD
- SCM CPLD
- BPB CPLD
- SKU

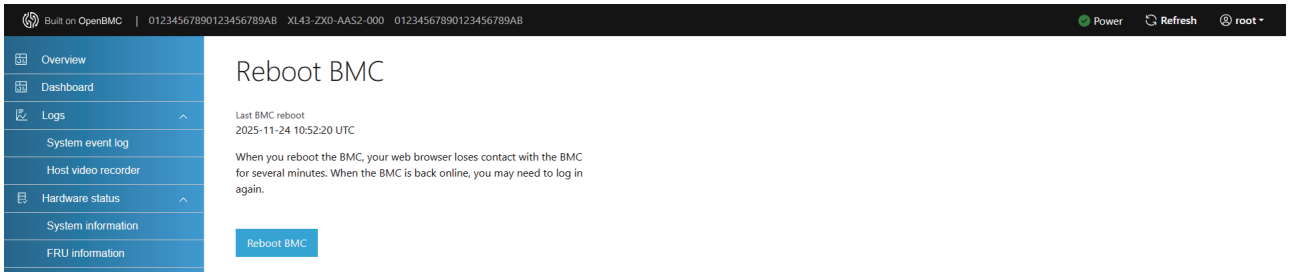
Select the firmware type by the drop-down list. Click **Add file** and Click **Start update** button to process the firmware update.

NOTE! Firmware images are required to be in the .tar file format.

2-5-4 Reboot BMC

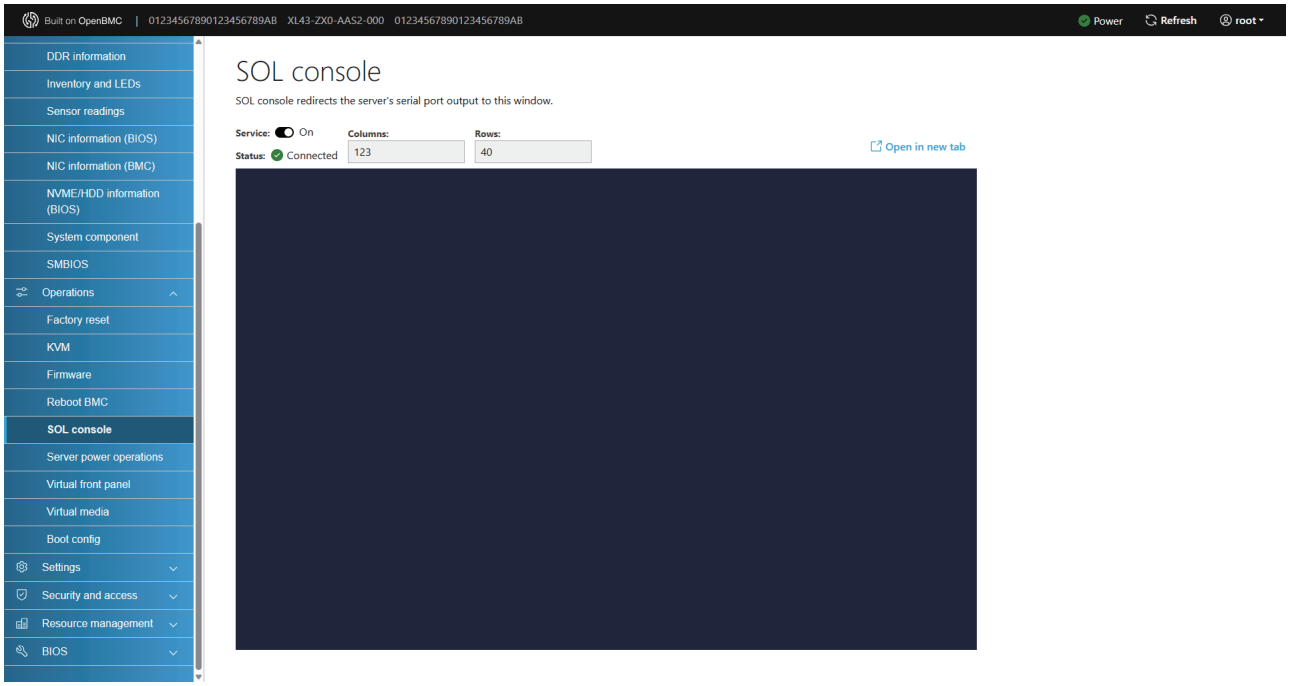
Click Reboot BMC to process BMC rebooting.

When you reboot the BMC, your web browser loses contact with the BMC for several minutes. When the BMC is back online, you may need to log in again.



2-5-5 SOL Console

To open SOL Page page, click Operations > SOL Console from the menu bar. A sample screenshot of the SOL COnsole Page is shown below.



Service: Configure the SOL service state (Enable/Disable).

NOTE! The activation process requires approximately 20–22 seconds before the service becomes fully operational.Recommended to set a large value for Rows.

Status: Displays the connection status.

Columns: This setting defines the horizontal resolution of the console display.

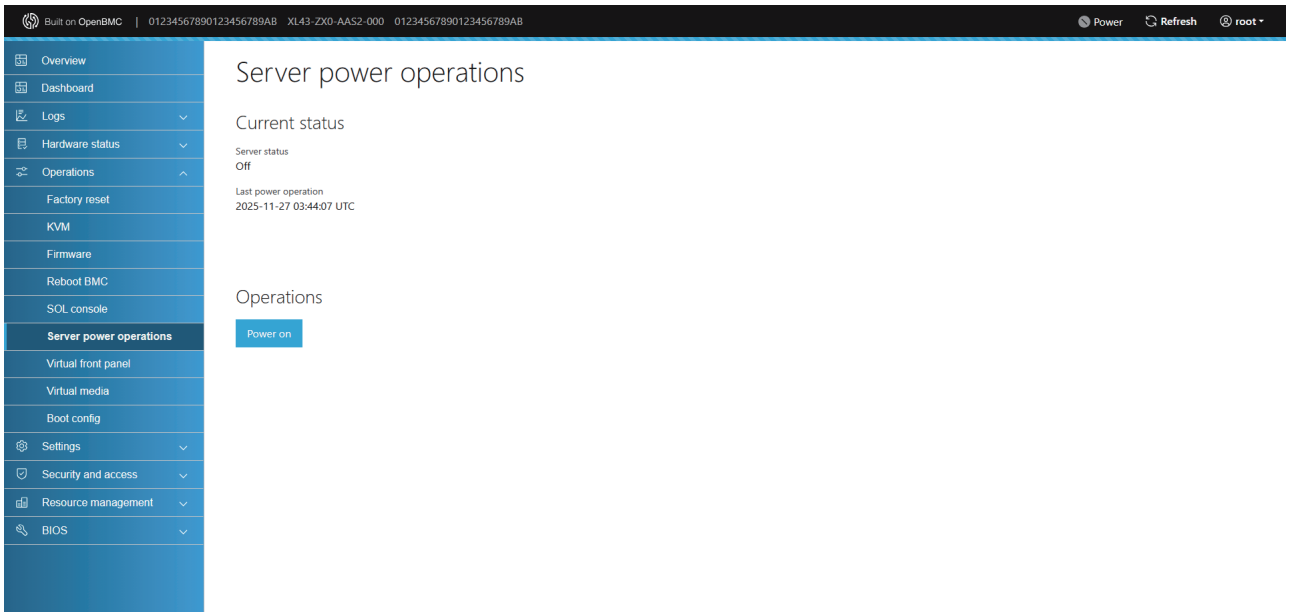
Rows: This setting defines the vertical resolution of the console display.

NOTE! Set a larger value is recommended.

2-5-6 Server power operations

This page allows you to view and control the power of your server.

To open Server power operations, click Operations > Server power operations from the menu bar. A sample screenshot of Server power operations is shown below.



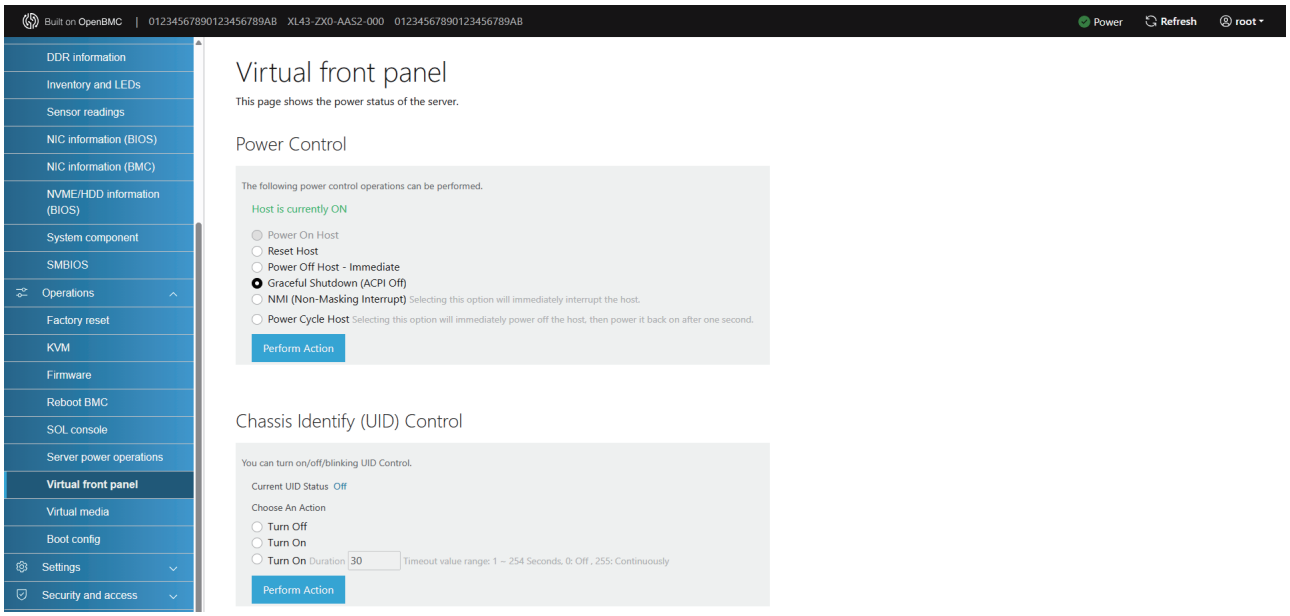
Current Status: Display server power operations.

Operations: Click to the button to process the power operation.

2-5-7 Virtual front panel

This page shows the power status of the server.

To open Virtual front panel, click Operations > Virtual front panel from the menu bar. A sample screenshot of Virtual front panel is shown below.



Power Control

This page shows the power status of the server. The following power control operations can be performed:

Power On Host

Selecting this option will power on the host.

Reset Host

Selecting this option will hard reset the host without powering off.

Power Off Host - Immediate

Selecting this option will immediately power off the host.

Graceful Shutdown (ACPI Off)

Selecting this option will soft power off the host.

NMI (Non-Masking Interrupt)

Selecting this option will immediately interrupt the host.

Power Cycle Host

Selecting this option will immediately power off the host, then power it back on after one second.

NOTE! All power control actions are done through the BMC and are immediate actions. It is suggested to gracefully shutdown the operating system via the iKVM interface or other interface before initiating power actions.

Perform Action

Click to execute the selected remote power command.

2-5-8 Virtual Media

This page enables the mounting of remote NFS/HTTPS images and exposes them to the system as local storage. To open Virtual Media, click Operations > Virtual Media from the menu bar. A sample screenshot of Virtual Media is shown below.

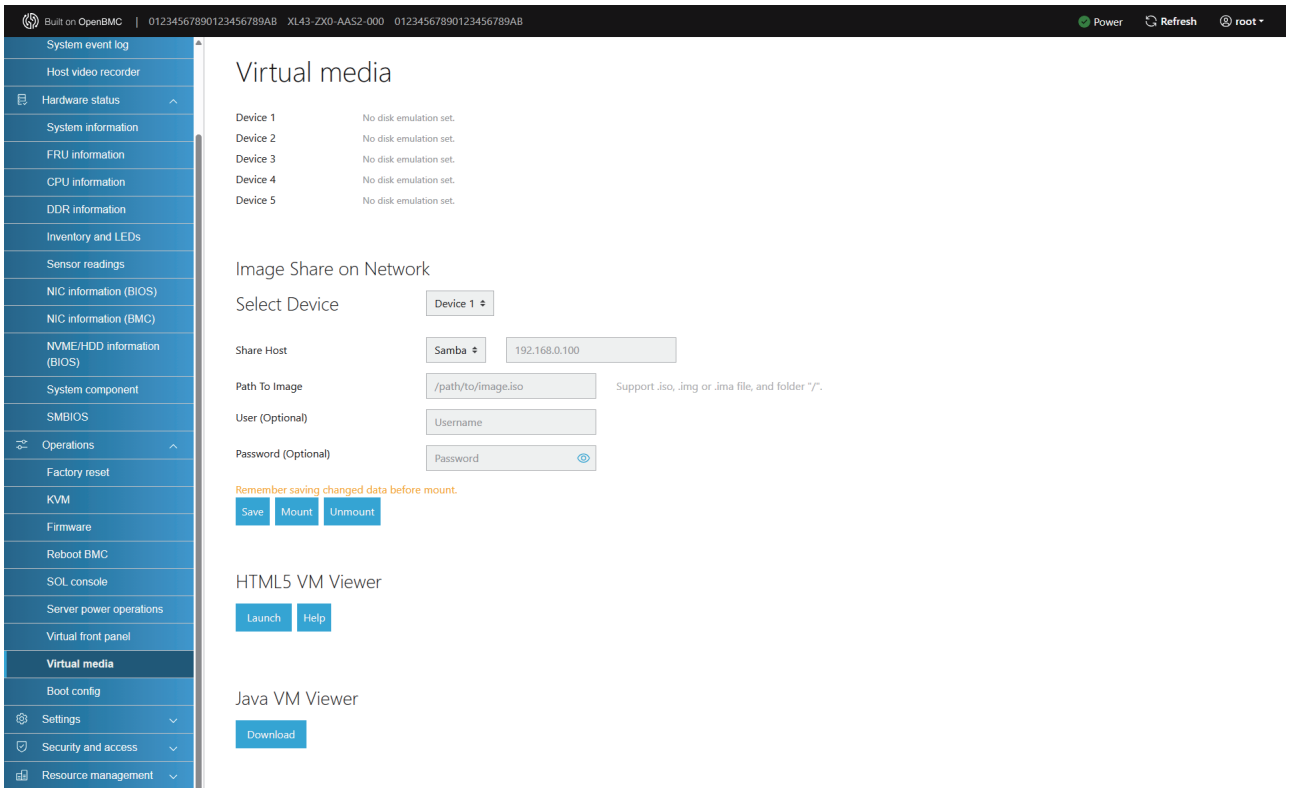


Image Share on Network
Select Device: Select virtual media Device.
Share Host: Select the host.
Path To Image: Enter the path to image. Note: Support .iso, .img or .ima file, and folder "/".
User (Optional): Enter the User account.
Password (Optional): Enter the Password.

Actions
Save
Click on the Save button to save the settings.

Mount
Click on the Mount button to mount the image file.

Unmount
Click on the Unmount button to unmount the image file.

Test Steps

1. Prepare a file server such as Samba, HTTPS or NFS. We will share media from the network.
2. Select Device: Select a device you want to use.
3. Share Host: Choose which file server you want to use for sharing media: Samba, HTTPS, or NFS. And enter ip address of file server.
4. Path To Image: Enter the path to the file you want to share from the file server.
5. User: Enter the user, if access to the file requires authentication.
6. Password: Enter the password, if access to the file requires authentication.
7. Save: Must be click on the Save button before click on the Mount button.
8. Mount: Mount the image file.
9. Unmount: Unmount the image file.

HTML5 VM Viewer

Click 'Launch' button to launch the Virtual Media window.

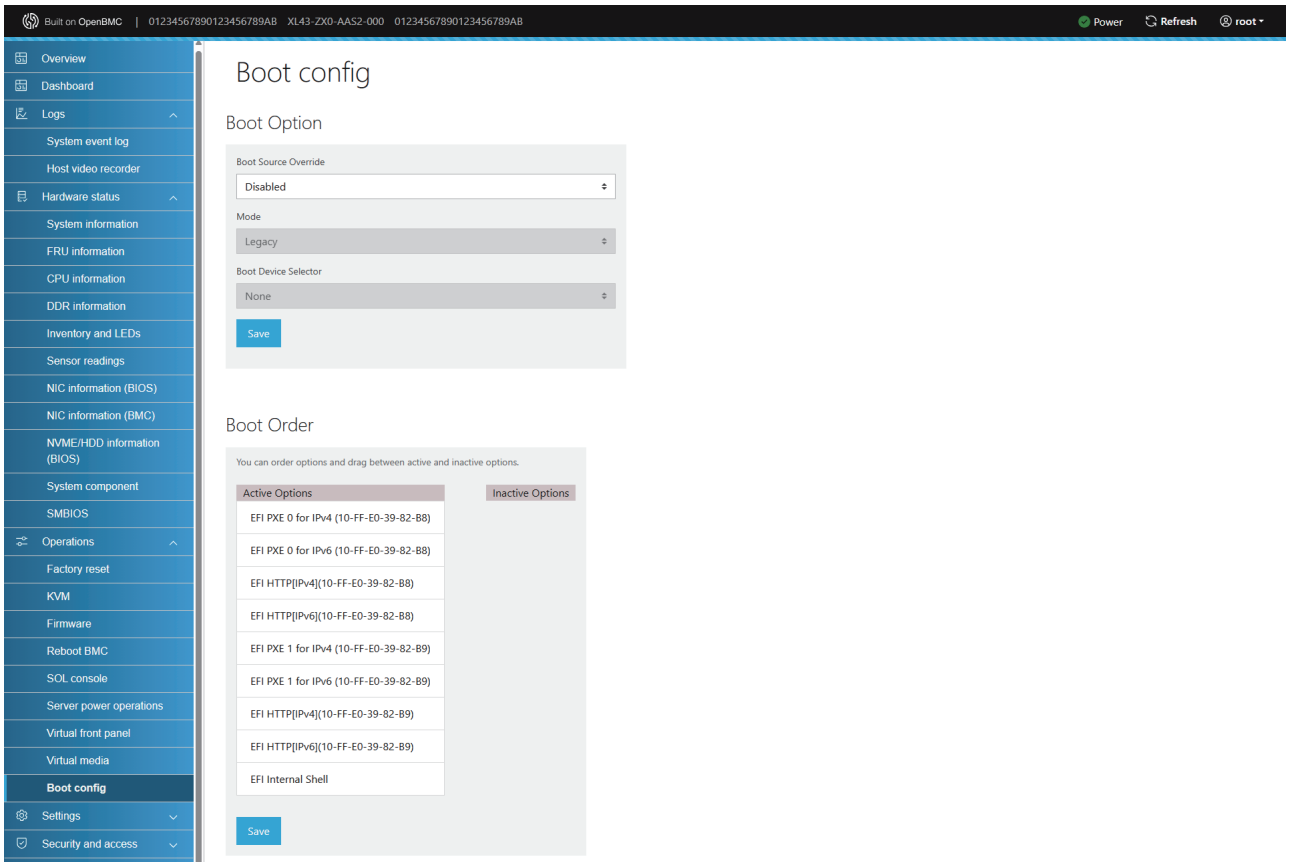
Java VM Viewer

Click ' Download ' button to download the VMviewer (.jar) file.

2-5-9 Boot Config

This page Display boot configuration information.

To open Boot Config, click Operations > Boot Config from the menu bar. A sample screenshot of Boot Config is shown below.



Boot Option: Select the device to boot.
Boot Order: Priority the Boot Order.

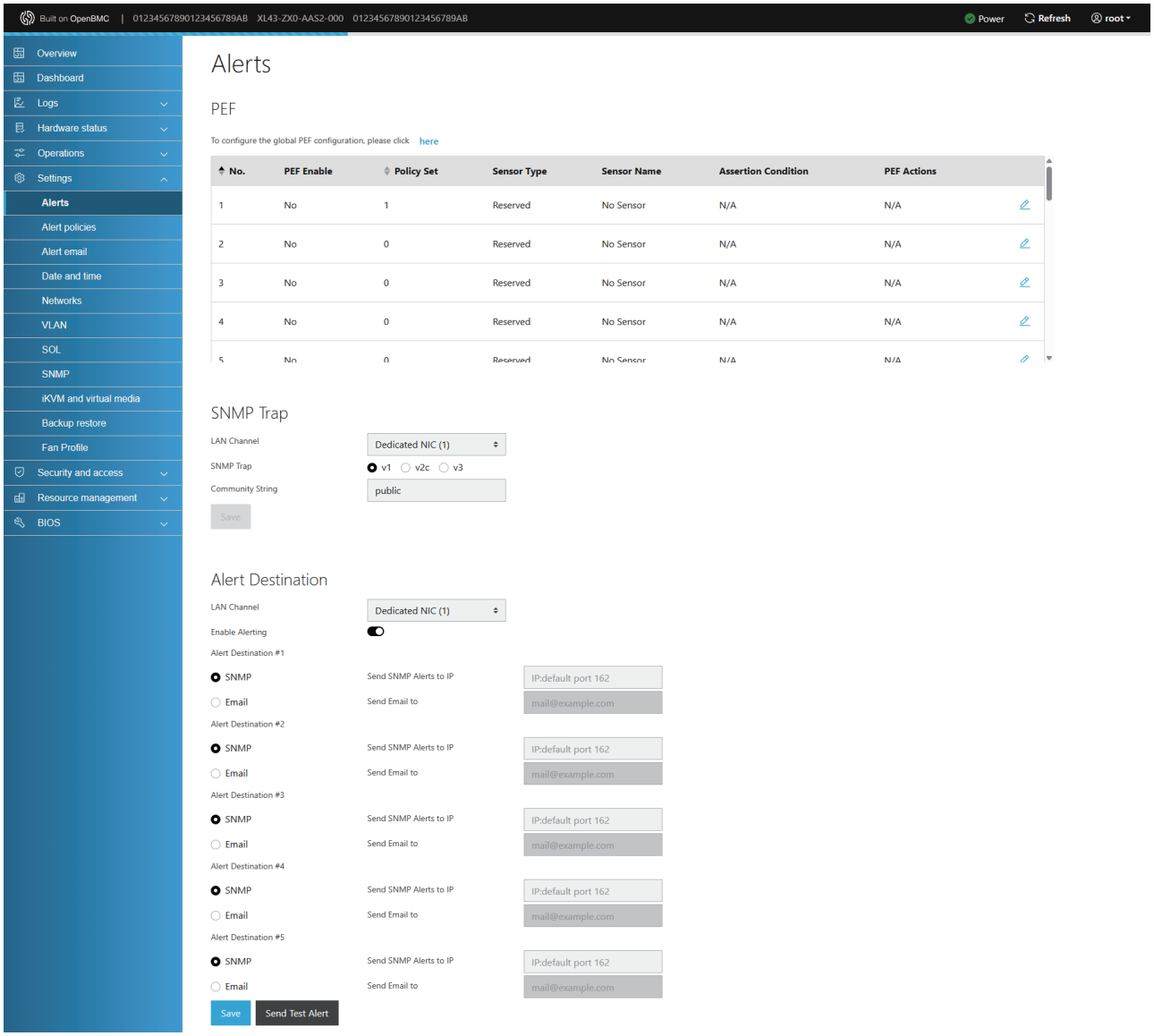
Actions

Save: Click on the Save button to save the option settings.

2-6 Settings

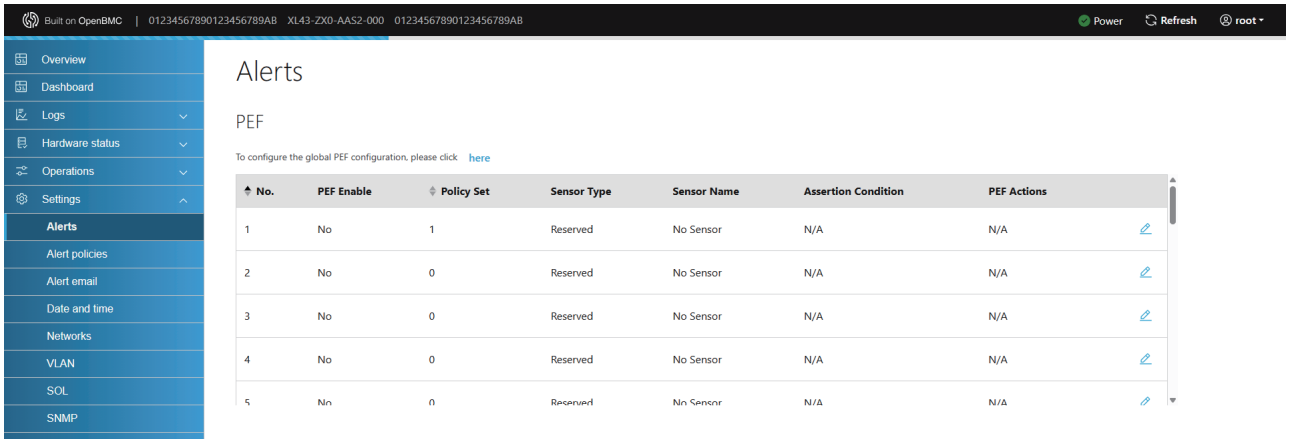
2-6-1 Alert

This page displays alerts information.
To open Alert page, click Settings > Alert from the menu bar. A sample screenshot of the Alert Page is shown below.



2-6-1-1 PEF Configuration

Platform Event Filter (PEF) provides a configurable mechanism that enables the BMC to **determine and execute predefined system actions** in response to both externally received and internally generated event messages. Supported actions **shall include** system power-off, system reset, and the initiation of alert generation. The PEF configuration shall consist of a global configuration section and up to **28 individually defined event filter entries**, each of which **must specify** event-matching conditions and the corresponding system response.



Navigate to Alerts Page: Find the PEF section.

Global PEF Configuration:

PEF Enable: This setting controls whether the entire PEF system is active.

- **Options:** Enable / Disable

Log Event on Filter Action: This setting determines whether events should be logged when a filter action is triggered.

- **Options:** On / Off

PEF Actions: These are the actions that can be taken when a filter is triggered. Multiple actions can be selected.

- **Options:** Alert, Power Off, Reset, Power Cycle, Graceful Shutdown, Diagnostic Interrupt

Configuring Event Filters:

- You can configure up to 28 event filters, each with its own settings.
- Event Filter Enable: This setting controls whether the specific event filter is active.
  - **Options:** On / Off

Alert: This setting determines whether an alert should be sent when the filter is triggered.

- **Options:** On / Off

Event Filter Action: These are the actions that will be taken when the filter is triggered. Multiple actions can be selected.

- **Options:** Alert, Power Off, Reset, Power Cycle, Graceful Shutdown, Diagnostic Interrupt

Policy Set: An option allows you to specify a set of actions that should be taken when this event filter is triggered.

Sensor Type: This setting specifies the type of sensor to monitor. You can choose a specific type or select "Match All" to include all sensors of that type.

- **Example:** Temperature, Voltage, Fan, etc.
- **Match All:** Select this option to include all sensors type.

Sensor Name: This setting specifies the name of the sensor to monitor. You can choose a specific sensor or select "Match All" to include all sensors under the specified type.

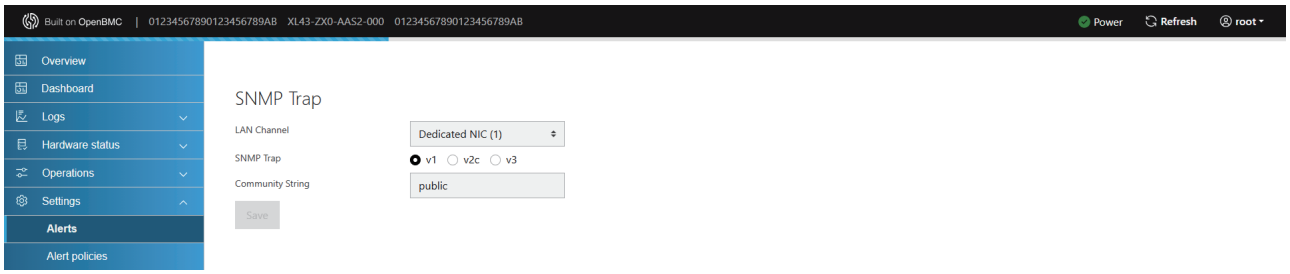
- **Example:** Sensor1, Sensor2, etc.
- **Match All:** Select this option to include all sensors under the specified type.

Assertion Condition (BIT EVENT): This setting specifies the conditions under which the event filter will be triggered. You can select multiple conditions.

Save the Settings: Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.

2-6-1-2 SNMP Trap Configuration

SNMP (Simple Network Management Protocol) TRAPs allow the system to send notifications to a network management system when specific events occur.



Navigate to Alerts Page: Go to the Settings Alerts and find the SNMP Trap sections.

Configure SNMP TRAP:
LAN Channel Selection: Choose between Shared NIC or Dedicated NIC for SNMP TRAP.

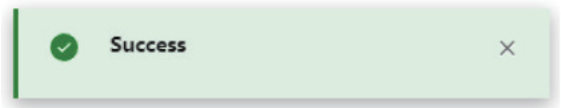
Note: Each LAN Channel's settings are saved separately, but only one set of settings can be saved at a time.

SNMP Version: Select the SNMP version to use:
SNMP v1/v2c:

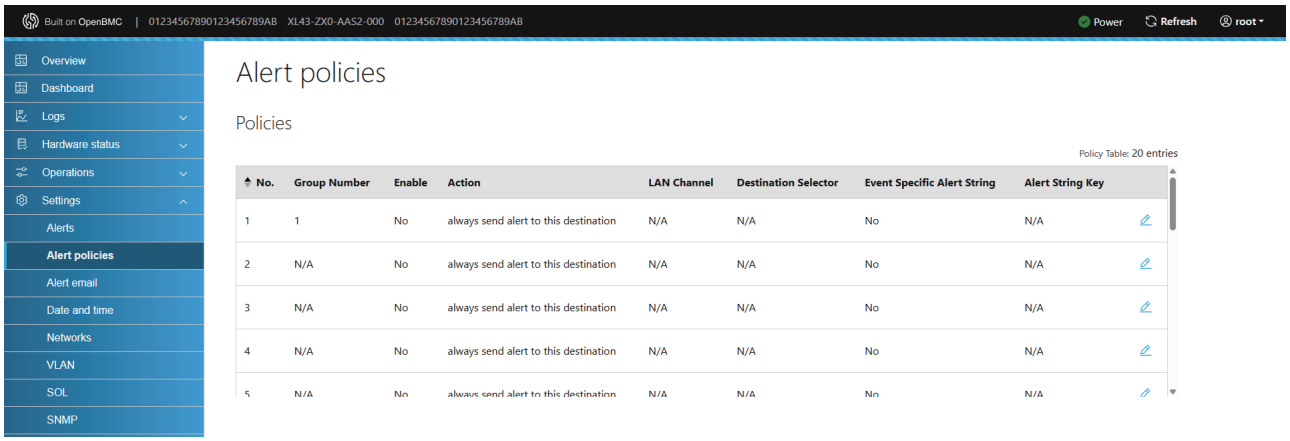
- Enter the community string.

SNMP v3:

- **Authentication Protocol:** Choose the authentication protocol (e.g., MD5, SHA).
- **Authentication Passphrase:** Enter the authentication passphrase.
- **Security Level:** Select the security level:
  - **authNoPriv:** Authentication without privacy.
  - **authPriv:** Authentication with privacy, which requires additional settings:
    - **Privacy Protocol:** Choose the privacy protocol (e.g., DES, AES).
    - **Privacy Passphrase:** Enter the privacy passphrase.
  - **SNMP TRAP Destination:** Enter the SNMP TRAP destination IP address.
  - **Severity Level:** Set the severity level of events to be trapped.
- **Save the Settings:** Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.



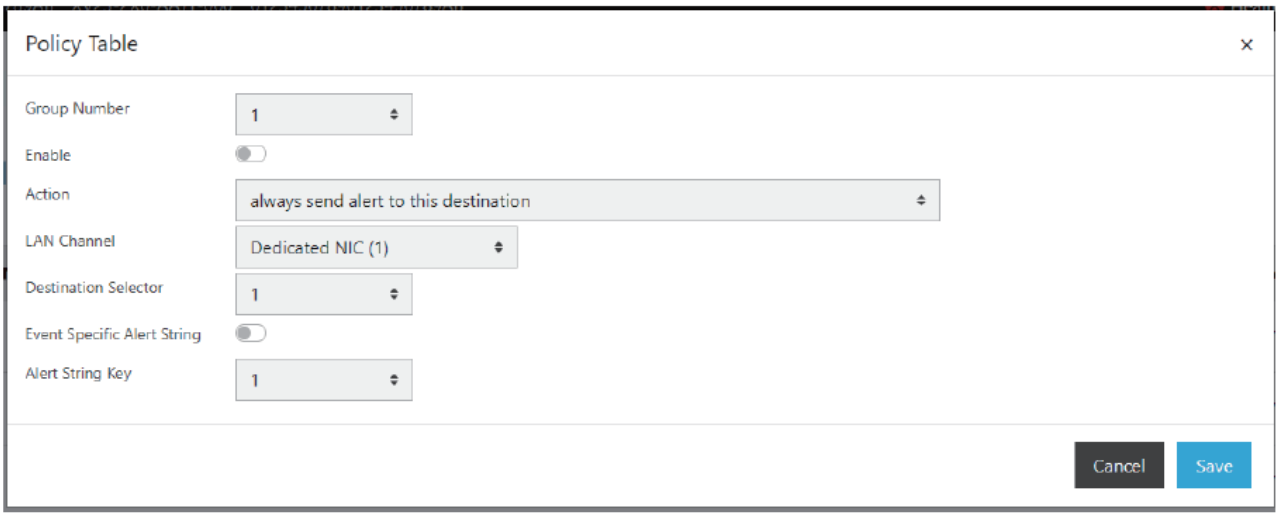
2-6-1-3 Alert Policies Configuration



The alert policy defines how alerts are sent based on specific conditions and destinations.

Description of each field of Policy table

The Alert Policy Table allows you to configure how alerts are delivered to various destinations. Each policy entry specifies different parameters that determine the alert behavior, including the destination and conditions under which the alert is sent.



Modify Alert Policy Entry by clicking the modify button of each entry:

- **No:** The entry number in the policy table.
- **Group Number:** This value identifies the entries belonging to a particular policy set. When an Alert Action is taken, the BMC will scan the Alert Policy Table and will attempt to generate alerts based on the entries that form the policy set.
- **Enable:** Yes means this entry enabled, and No means this entry disabled.
- **Action:** When an Alert Action is taken, the BMC will scan the Alert Policy Table and will attempt to generate alerts based on the entries that form the policy set.
- **LAN Channel:** Specifies the LAN channel to use for sending the alert.
- **Destination Selector:** Channel determines which set of destination is used.

- **Event Specific Alert String:** Yes means to use SEL decoded strings as the result alert string. No means the Alert String Set / Selector sub-field is interpreted as an Alert String Selector that provides a direct pointer to the desired Alert String from the PEF Configuration Parameters.
- **Alert String Key:** Sets the Alert String data. The string data that should be used is dependent on the Channel and Alert Type.

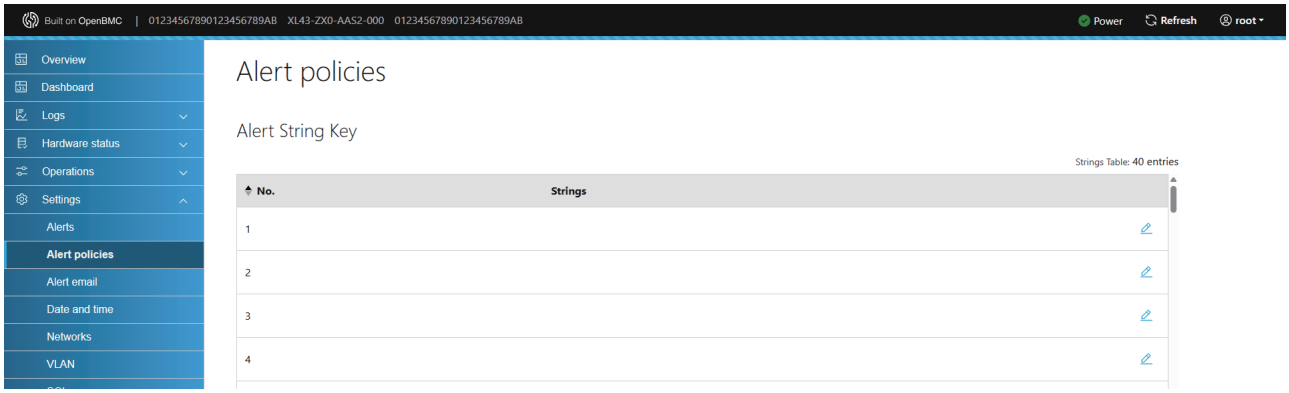
Important

- Within the same group, entries with a lower No. will be executed first. This means that the order of entries in a group determines the priority of execution.
- If Event Specific Alert String is Yes, the default message will be display.
- If Event Specific Alert String is No, the selected Alert String Key will be used.
- If Event Specific Alert String is No, and the selected Alert String Key is empty, you will receive a blank message without any information about the event.

The default message example:

- RID:0002 TS:01/11/2024 21:10:50 SN:Physical Scrty ST:Physical Security (Chassis Intrusion) ED:General Chassis Intrusion ET:Asserted EC:Critical RID:0002 RT:02 TS:65A0595A GID:0020 ER:04 ST:05 S#:E8 ET:6F ED:00 FF FF EX:02 FF FF FF FF FF FF FF

2-6-1-4 Alert String Key Configuration



Modify Alert String Key by clicking the modify button of each entry:

- PEF can be configured to handle two types of events: real sensor events from the BMC and virtual sensor events, as detailed below.
- **Save the Settings:** Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.

2-6-1-5 Alert Example

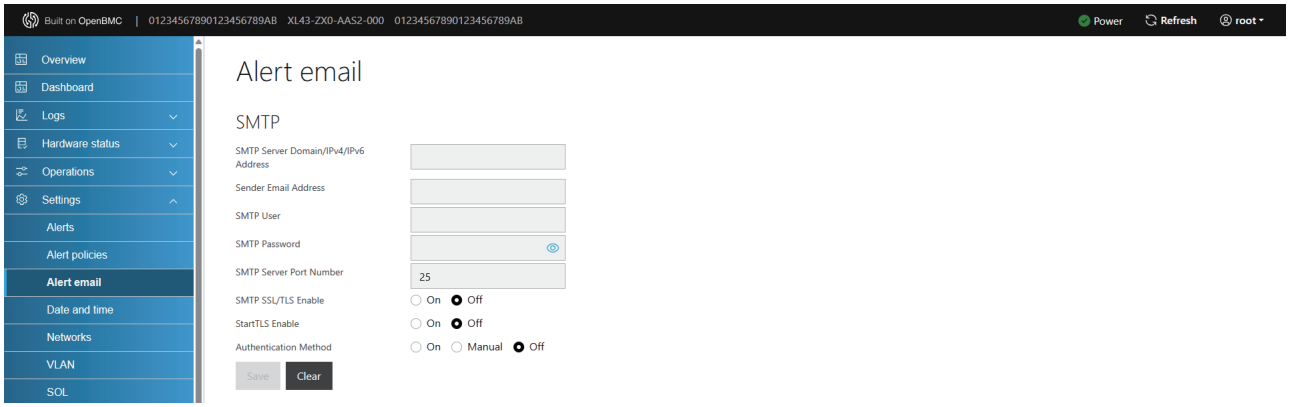
- Enter the string you want to display.
  - Real sensor events can be directly selected in the PEF configuration via the WebUI by specifying the sensor type and name.
  - Virtual sensor events, such as those generated by the BIOS, cannot be directly selected and require specific settings.
- Since System Event Log (SEL) entries generated by the BIOS or by virtual sensors are not associated with any physical BMC sensors, the PEF alert mechanism cannot match them using standard sensor identifiers. To enable PEF alert handling for these SELs, configure the Sensor Type and Sensor Name fields to “Match All”, and specify the appropriate Assertion Condition bits required for the intended event-trigger behavior.
- If the event is from a real sensor on the BMC, please refer to examples **System Event Log Cleared** and **All Temperature sensor** upper threshold. For BIOS or Virtual Sensor Events, refer to examples **BIOS Event (Example of Critical Interrupt: Front Panel NMI & PCIe AER Error)** and **BIOS Event(Example of Memory: Correctable ECC & Uncorrectable ECC)**.

The table below lists the BIOS events and virtual sensor events:

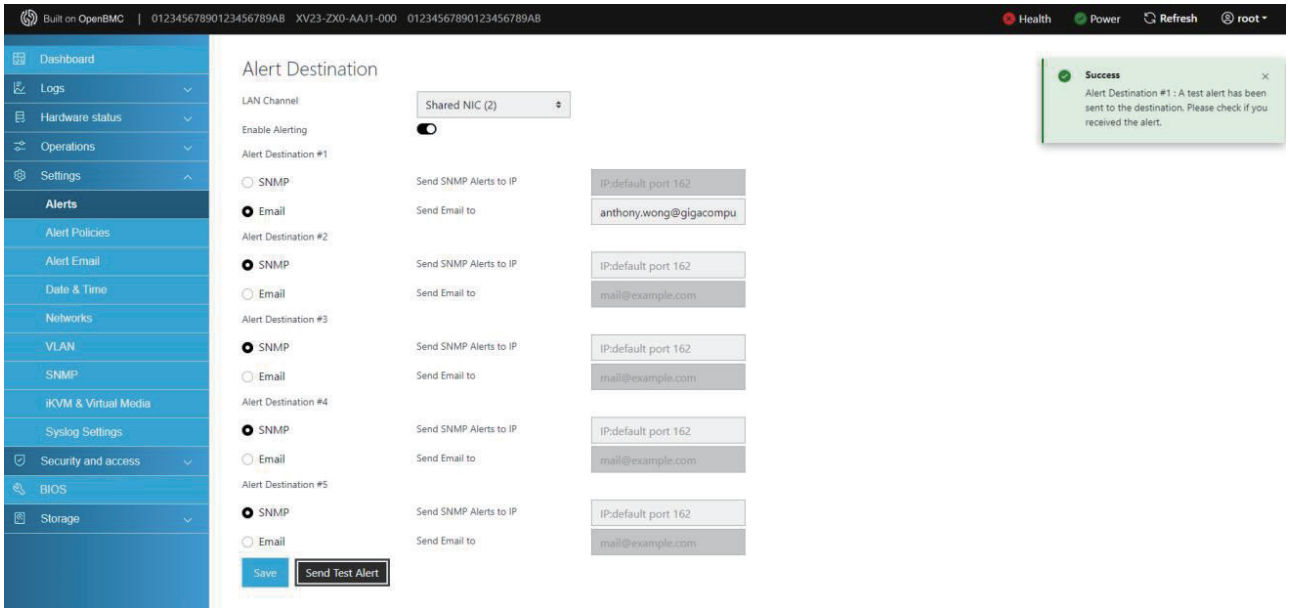
From	Sensor Type	Assertion Condition bit(s)
BMC	Drive Slot	0
BMC	BMC Recovery Detect(OEM)	0
BMC	BMC/BIOS Backup Log(OEM)	01,2,3
BMC	BMC/BIOS Update Log(OEM)	01,2,3,4,5,6,7,8,9
BMC	BIOS Switch Log(OEM)	0,1
BMC	Memory	0,1,4
BMC	Critical Interrupt	4,5
BMC	AMD EPYC CPU ERROR(OEM)	1,2

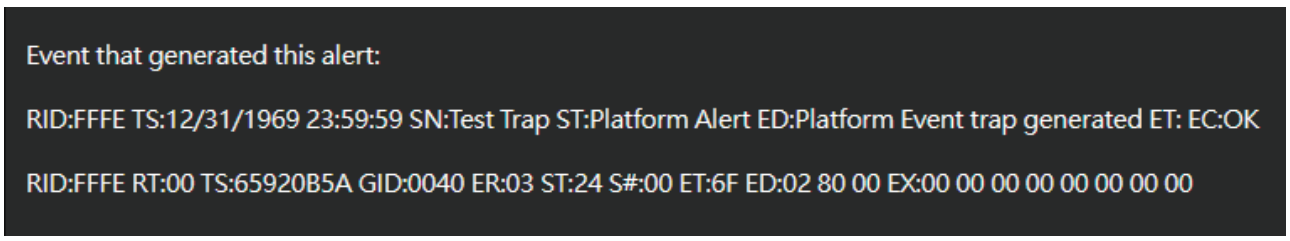
2-6-1-6 System Event Log Cleared

1. Go to **Setting**->**Alert email** and **SMTP** setup page.

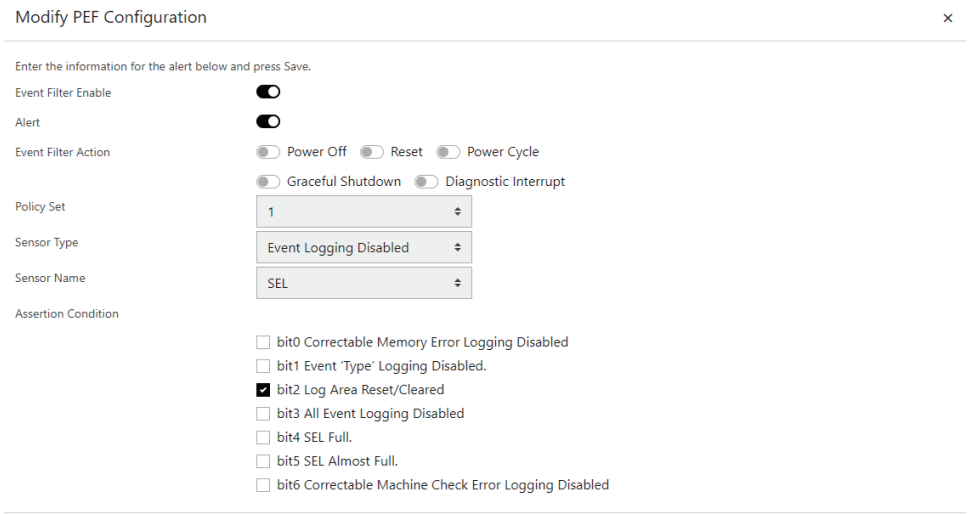


2. Go to **Setting**->**Alert** -> and **Alert Destination** setup page. Save the settings, and then click Send Test Alert. You will receive a email intended for testing purposes only, containing no real information.

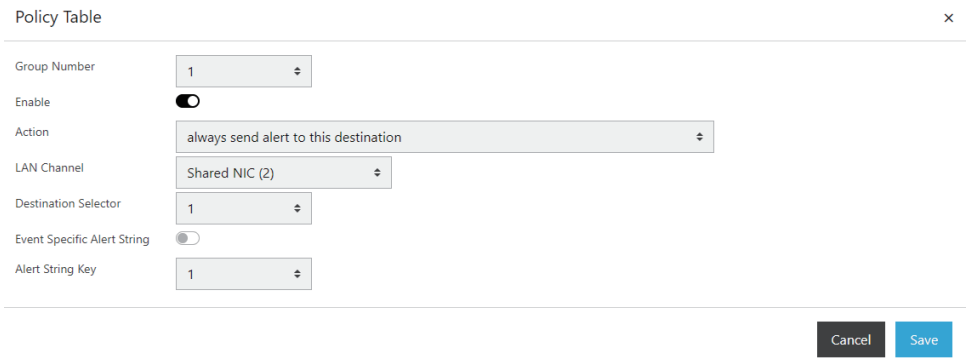




3. Set up the PEF and save the configuration.In the following example, the SEL cleared is used to illustrate the procedure.



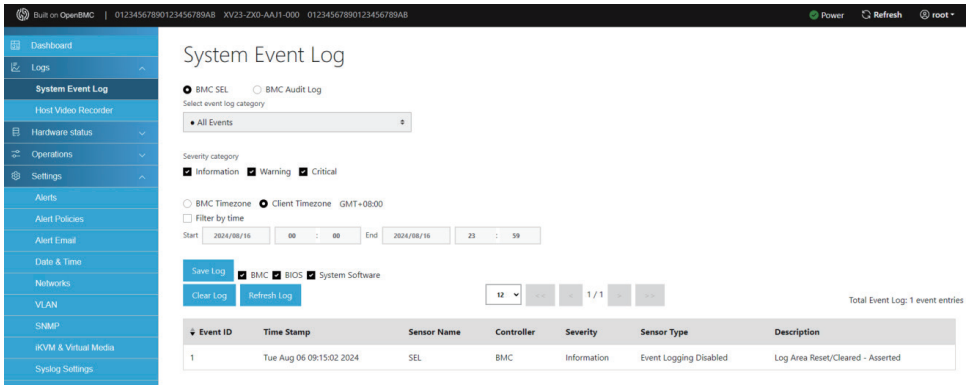
4. Go to **Alert Policies** Page, set up the Policies.



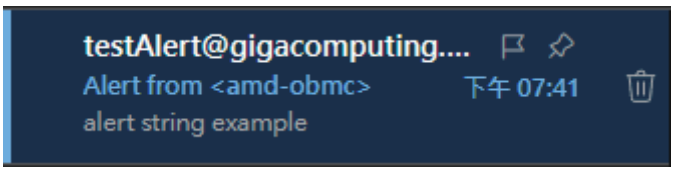
5. Set up Alert String Key



6. Go to **System Event Log** Page and clear log.

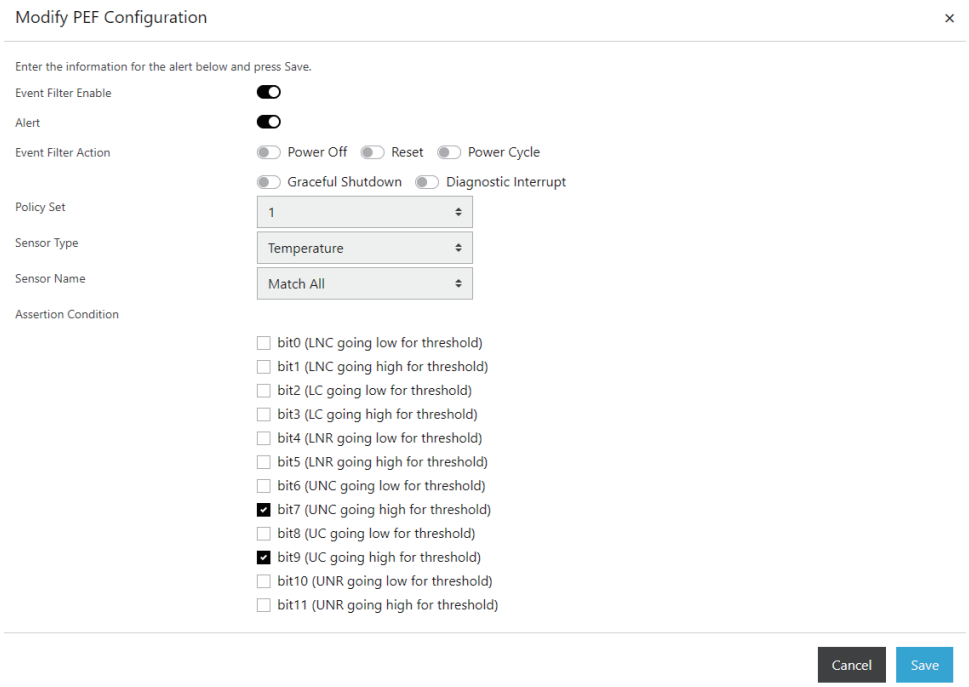


7. Check mailbox.

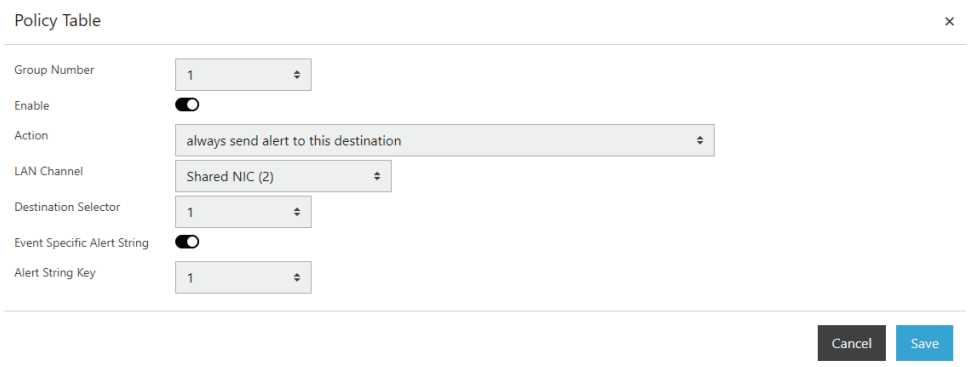


2-6-1-7 All Temperature sensor upper threshold

1. After configuring the PEF settings, save the configuration. In the following example, the Upper Threshold of the All Temperature Sensors group is used to illustrate the procedure.

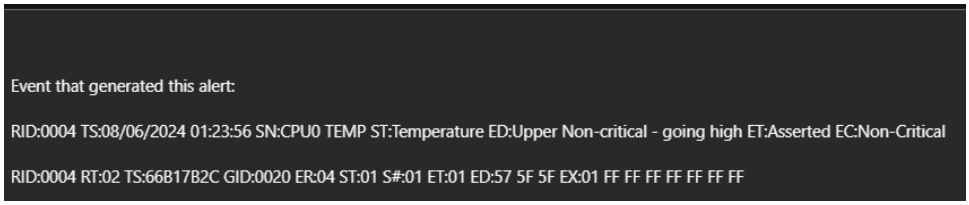


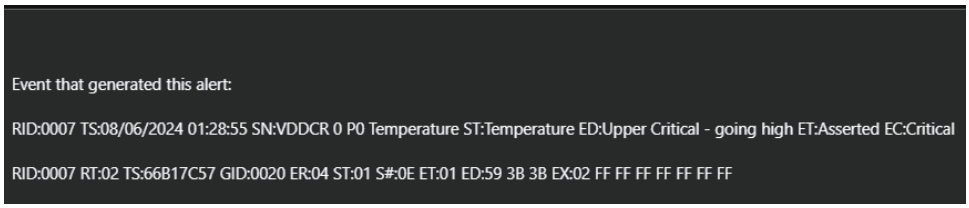
2. When Sensor Name is set to Match All, the Assertion Condition field does not display a description of the corresponding event, as each sensor type may have different event definitions and settings. For instance, in the case of a temperature sensor, bit 7 and bit 9 typically represent “UNC Going High” and “UC Going High”, respectively.
3. Go to **Alert Policies** Page, set up the Policies.



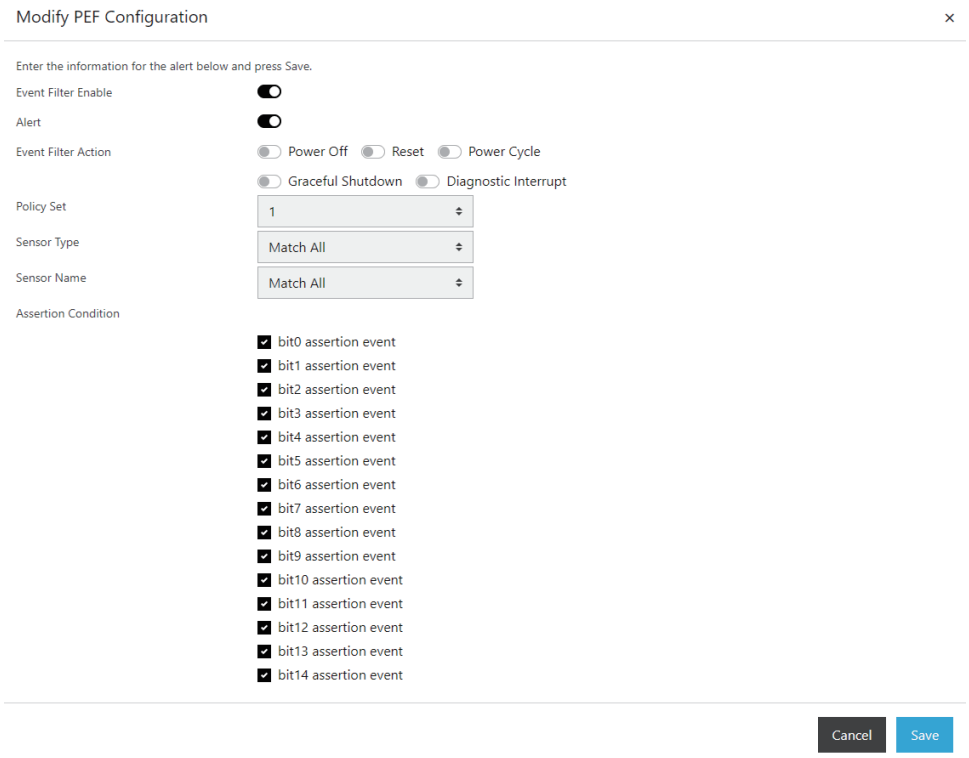
4. Raise the temperature to above the threshold.

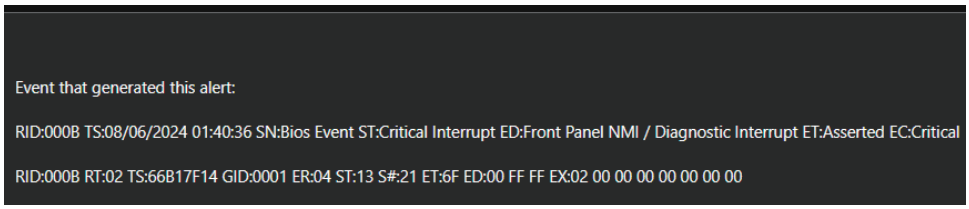
5. Check mailbox.
    - In the following example, shows two Temperature sensor crossed the threshold.
        - CPU0_TEMP
        - VDDCR_0_P0_TMP

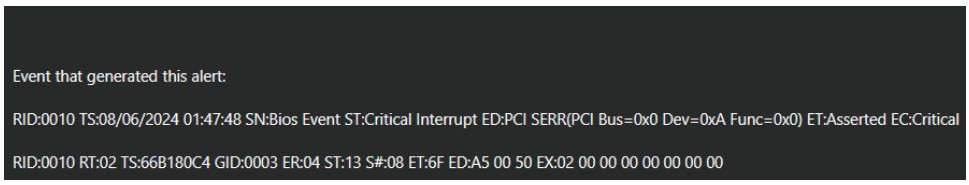




2-6-1-8 BIOS Event (Example of Critical Interrupt: Front Panel NMI & PCIe AER Error)

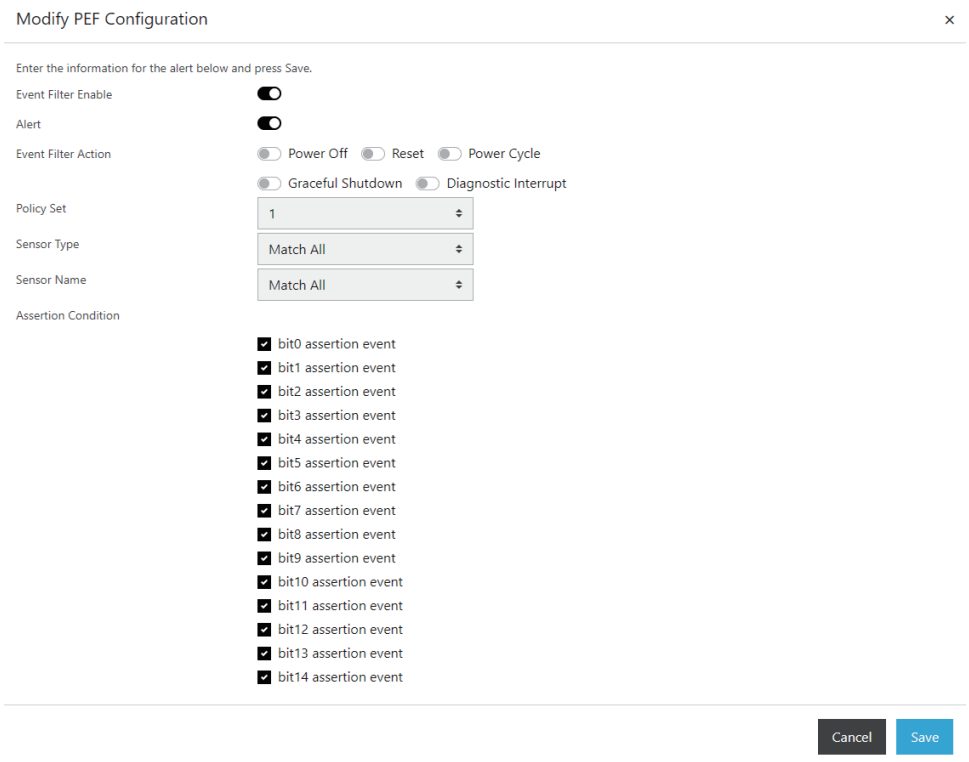


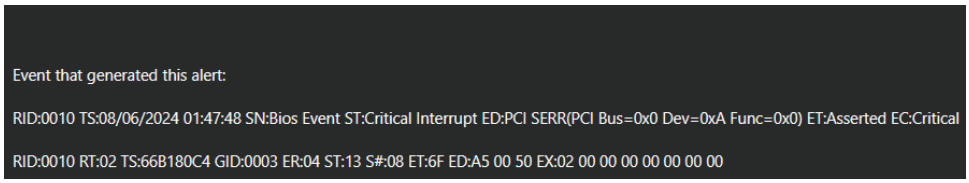


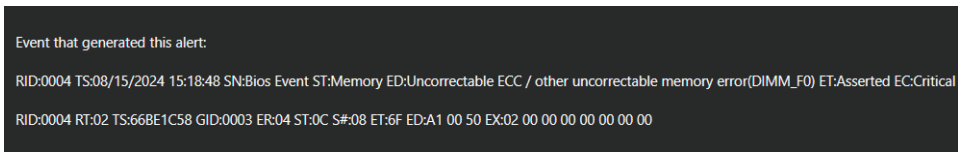


2-6-1-9 BIOS Event(Example of Memory: Correctable ECC & Uncorrectable ECC)

As described in the BIOS Event section, BIOS-generated events do not correspond to actual BMC sensors. Therefore, for PEF configuration, both Sensor Type and Sensor Name should be set to “Match All”, and all relevant Assertion Condition bits should be selected in this example.



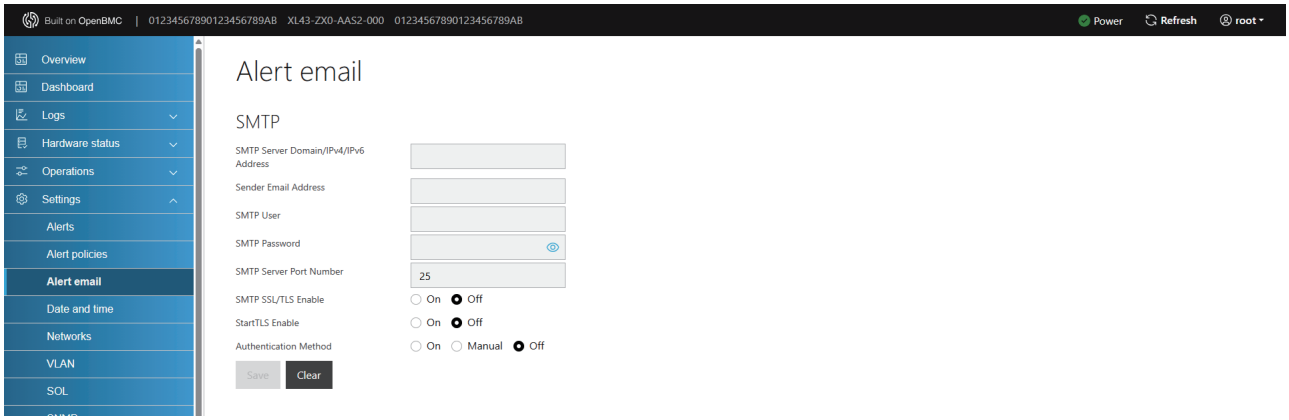




Please refer **Appendix** for **Assertion Condition (BIT EVENT) References**

2-6-2 Alert Email

Display alert email information.



Navigate to the Alert Email Page: Find the Alert Email section.
Configure SMTP Settings:

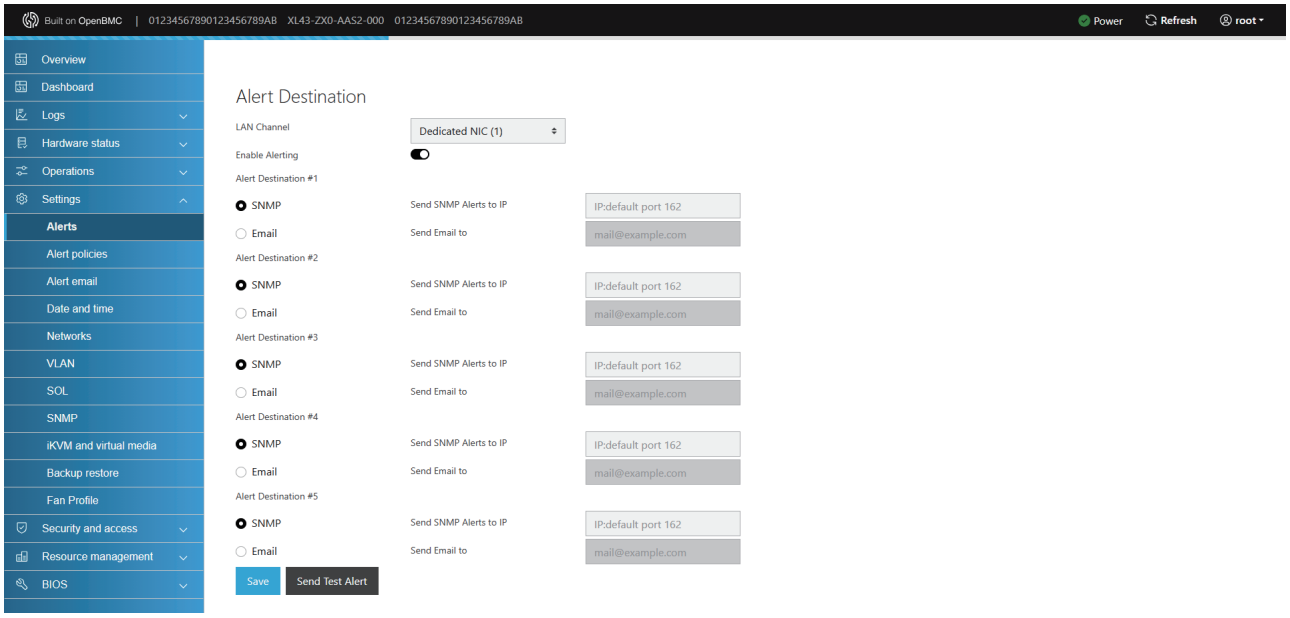
- **SMTP Server Domain/IPv4/IPv6 Address:** Enter the domain name or IP address (IPv4/IPv6) of the SMTP server.
- **Sender Email Address:** Provide the email address that will appear as the sender of the alert emails
  SMTP User: Enter the username for the SMTP server authentication.
- **SMTP Password:** Enter the password for the SMTP server authentication.
- **SMTP Server Port Number:** Specify the port number used by the SMTP server (commonly 25, 465, or 587).
- **SMTP SSL/TLS Enable:** Enable or disable SSL/TLS encryption for the SMTP connection.
  - Options: On / Off
- **StartTLS Enable:** Enable or disable StartTLS for the SMTP connection.
  - Options: On / Off
- **Authentication Method:** Choose the method of authentication for the SMTP server.
  - Options: On / Manual / Off
    - On: The system will automatically handle authentication.
    - Manual: If selected, choose one of the following methods:
      - PLAIN: Simple base64-encoded authentication.
      - CRAM-MD5: Challenge-response authentication mechanism.
      - EXTERNAL: Use an external mechanism for authentication.
      - LOGIN: Two-step authentication with separate username and password steps.
  - Off: No authentication will be used.

Important Notes:
Click **Save** button to save all configurations.

- **SSL/TLS and STARTTLS:** Only one of these should be enabled at a time. If both are enabled, STARTTLS will typically be used.
  - **SSL/TLS:** Provides encryption from the start of the connection on a dedicated port (commonly port 465).
  - **STARTTLS:** Begins as an unencrypted connection and then switches to encryption after the STARTTLS command is issued (commonly used on ports 25 or 587).
- **Authentication Method:** If "Off" is selected for Authentication Method, SSL/TLS and STARTTLS settings will not be used.

Save the Settings: Click the Save button to save the configuration. A dialog message pops up when the setting is successfully configured.

2-6-3 Alert Destination Configuration



Navigate to the Alert Page: Find the Alert Destination section.
LAN Channel Selection:
Select LAN Channel:

- **Select LAN Channel:** Choose either Dedicated NIC or Shared NIC from the dropdown menu. Each NIC has its own separate configuration.
- **Enable Alerting:** Toggle the switch to enable or disable alerting for the selected NIC.
- **StartTLS Enable:** Enable or disable StartTLS for the SMTP connection.

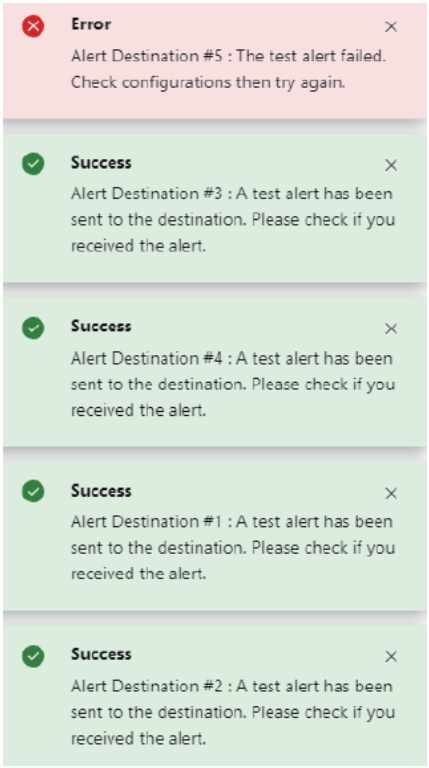
Configure Destinations:
You can configure up to 5 alert destinations. For each destination, you can choose between SNMP and Email.

- **Alert Destination #1 to #5:**
  - **SNMP:**
    - **Select SNMP:** Choose the SNMP option to send SNMP alerts.
    - **Enter IP Address:** Provide the IP address and port for SNMP alerts in the format 192.168.1.1:1234. If no port is specified, the default port 162 will be used.
  - **Email (SMTP):**
    - **Select Email:** Choose the Email option to send alerts via email.
    - **Enter Email Address:** Provide the email address to which alerts should be sent.

Save the Settings: Click the Save button to save your configurations for the selected NIC.

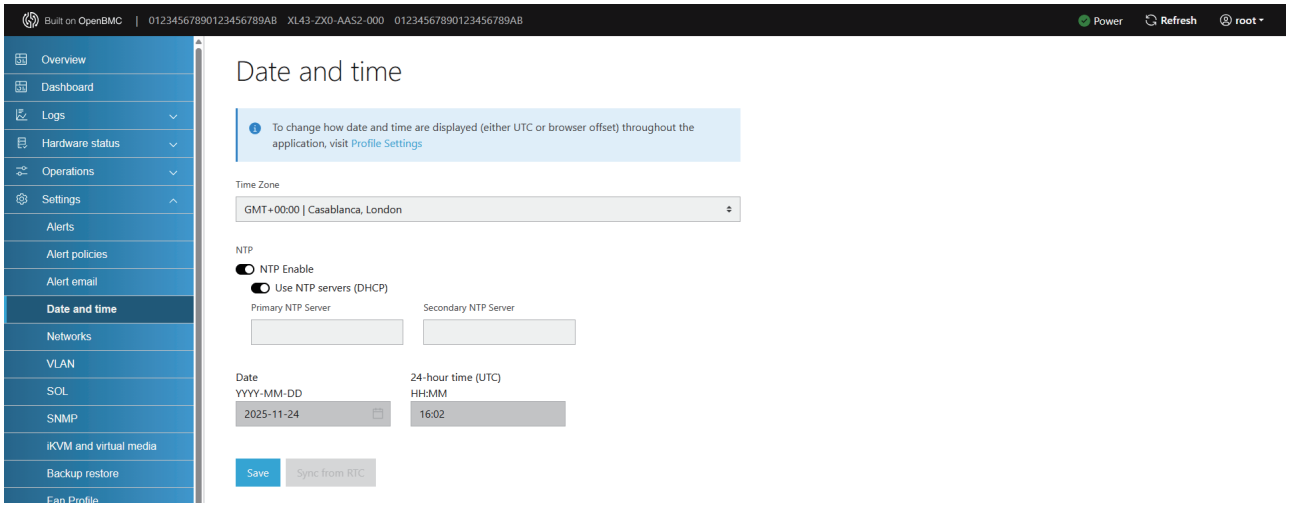
Send Test Alert: You can click the Send Test Alert button to test the alert settings.

- The system sequentially dispatches alert messages to each configured destination and automatically bypasses any entries with undefined parameters (i.e., missing IP address or email address).
- During the test procedure, the system generates a diagnostic email or SNMP trap containing no operational data; its sole purpose is to validate the alert configuration and verify network connectivity between the host system and the designated SNMP server.
- For each transmission attempt, the interface displays either a success or failure status, as illustration below:



- If an alert transmission fails, verify that the selected NIC has proper network reachability to the target SNMP or SMTP server, and ensure that the SMTP email parameters are correctly configured.

2-6-4 Date and Time



Time Zone
The time zone setting will valid after BMC reboot.

NTP Enable
Enable/disable NTP service.

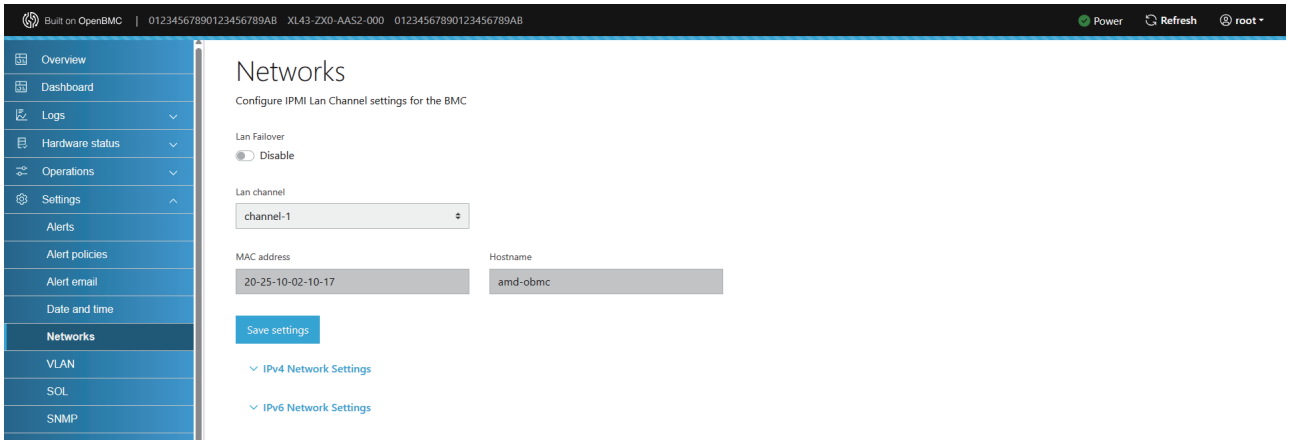
Primary NTP Server
Secondary NTP Server
Date (YYYY-MM-DD)
Time (24-hour)(HH:MM)
NOTE: The date and time can not be set more than Tue Jan 19 03:14:07 2038 .

Sync from RTC
Click the 'Sync from RTC' button to Synchronize BMC system time from BMC RTC time.

Save
Click the 'Save' button to save the new Date Time configuration.
If NTP is enable, just only update BMC system time.
If NTP is disable, update BMC system time and BMC RTC time.

2-6-5 Networks

This page provides configure IPMI Lan Channel settings for the BMC.



- Lan Failover
  - Enable: Bind all interfaces together.
  - Disable: Each interface has its own configuration.

- Lan channel: Select LAN channel to configure.
- MAC address: Set MAC address.
- Hostname: Set host name.
- IPv4 Network Settings
- IPv6 Network Settings

IPv4 Network Settings

Network interface

- Link Disabled: This option disables the network interface.
- Static IP Address: This option allows you to manually configure the network settings by assigning a fixed IP address, subnet mask, and gateway.
- DHCP Enabled: This option enables the network interface to automatically obtain an IP address, subnet mask, and gateway from a DHCP server.

Gateway

When using a static IP, you manually set the gateway; with DHCP, it's provided automatically.

IP Address

An IP address is a unique identifier assigned to each device on a network.

Subnet mask

A subnet mask defines the network and host portions of an IP address, allowing devices to identify which network they belong to.

DNS Server

The Domain Name System (DNS) is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

Note

1. An IPv4 address consists of 32 bits, divided into four groups (or blocks) of 8 bits each, written in decimal and separated by dot (".").

2. Each group ranges from 0 to 255
3. First group must not be 0 (IP address range 0.0.0.0/8 is reserved exclusively as a source address).
4. When the network source changes from DHCP to Static, the Static IP, Subnet Mask, and Gateway settings remain the same as those provided by the DHCP source.

IPv6 Network Settings

Network interface

- **Link Disabled: This option disables the network interface.**
- **Link Enabled: This option enables the network interface.**

Gateway (Static)

This setting allow you to manually configure a gateway for the network, even if DHCPv6 or SLAAC (Stateless Address Autoconfiguration) is enabled. When a static gateway address is set, it takes precedence over any dynamically assigned gateway address provided by DHCPv6/SLAAC. This means that even if DHCPv6/SLAAC is enabled and assigns a dynamic gateway address, the system will prioritize the static gateway address for network routing.

Gateway (Dynamic)

This setting allow user to configure a gateway dynamically. It dynamically configures Ipv6 address using DHCP (Dynamic Host Configuration Protocol).

Link-local address

Link-local address is a type of IPv6 address that is automatically configured and used for communication within a local network segment. These addresses are not routable across the broader internet and are only valid within a single network link. They start with the prefix fe80::/10, and each device on a network segment uses a unique Link-local address to communicate directly with other devices on the same link.

DHCPv6/IPv6 DHCPv6/SLAAC

IPv6 DHCPv6 and SLAAC can be set to either enable or disable to control how an IPv6 address is assigned to a device. DHCPv6 and SLAAC are enabled simultaneously, where SLAAC assigns the address, and DHCPv6 provides additional network configuration like DNS servers.
If this option is enabled, dynamic IP address and its prefix length will be displayed.

IP Address

A static IPv6 address that is manually assigned and does not change over time. When a static IPv6 address is configured, it takes priority over any dynamically assigned IP addresses (from DHCPv6 or SLAAC). Even if the device also receives a dynamic address, the static address will be preferred for outbound communication, routing, or any services bound to it.

DNS Server

As same as ipv4 DNS Server settings but uning ipv6 address.

Note

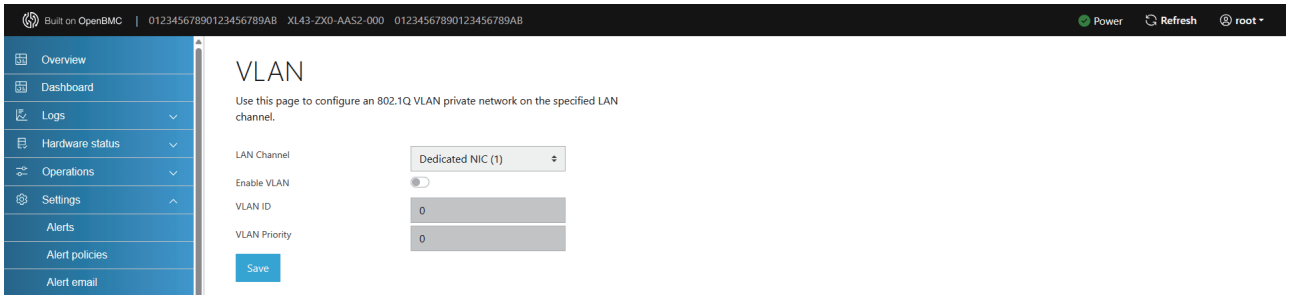
1. Unlike IPv4, an IPv6 interface can have multiple addresses, such as link-local, global, and unique local addresses.
2. You can setup only one static ipv6 address.
3. An IPv6 address consists of 128 bits, divided into eight groups (or blocks) of 16 bits each, written in hexadecimal and separated by colons (":"). For example 2001:0db8:85a3:0000:0000:8a2e:0370:7334
4. Each block represents 16 bits, and leading zeros in each block can be omitted for brevity. Additionally, consecutive blocks of zeros can be replaced with "::" once in an address.

Save settings

Click the 'Save settings' button to save the new Date Time configuration.

2-6-6 VLAN

This page is used to configure BMC VLAN settings.

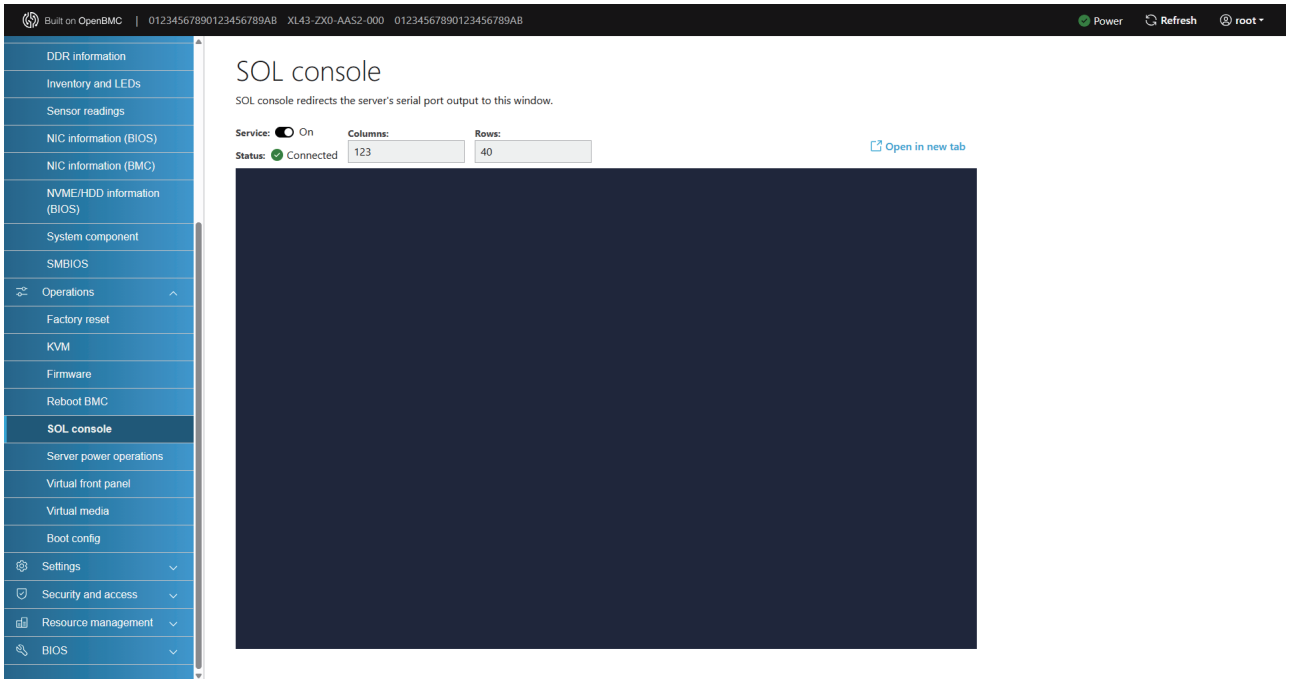


- Lan channel: Select LAN channel to configure.
- Enable VLAN: Enable/disable VLAN.
- VLAN ID: 1-4094
- VLAN Priority: 0-7

Save

Click the 'Save' button to save the VLAN configuration.

2-6-7 SOL



Serial Over LAN
Enable or disable serial over LAN communications.
Enable or disable Serial Over LAN for each LAN channel.

LAN Channel
Select which LAN Channel.

Enable SOL for Baseboard Mgmt
Click for enable or disable SOL for Baseboard Mgmt.

Baud Rate
9600 bps/19200 bps/38400 bps/57600 bps/115200 bps can be selected.

Flow Control
The options are None, RTS/CTS, and XON/XOFF.

Privilege Level
The options are User/Operator and Administrator.

SOL SSH
Customize the settings of the service used by Serial Over LAN Secure Shell (SOL SSH).
Allows changing the settings about service enable/disable, timeout and port used by the SOL (Serial Over LAN) SSH.
Changing this setting will immediately terminate all the sessions which are using SOL
SSH service.

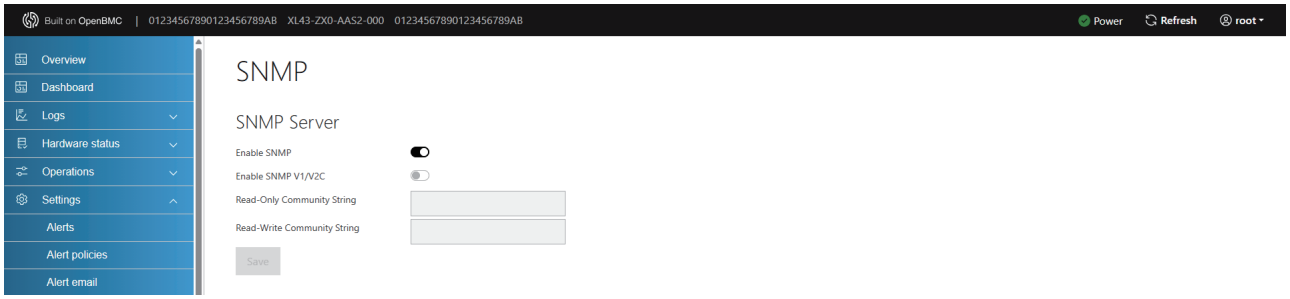
SOL SSH
Checking/Unchecking the checkbox to enable/disable SOL SSH service.

Port
Port range is 1 ~ 65535.

Timeout (sec.)
Timeout used for the idle sessions. (Units: seconds, default: 600, Range: 60-65535).

Save
Click the 'Save' button to save the SOL SSH configuration.

2-6-8 SNMP



SNMP Server
Enable SNMP
Enable/disable SNMP Server.

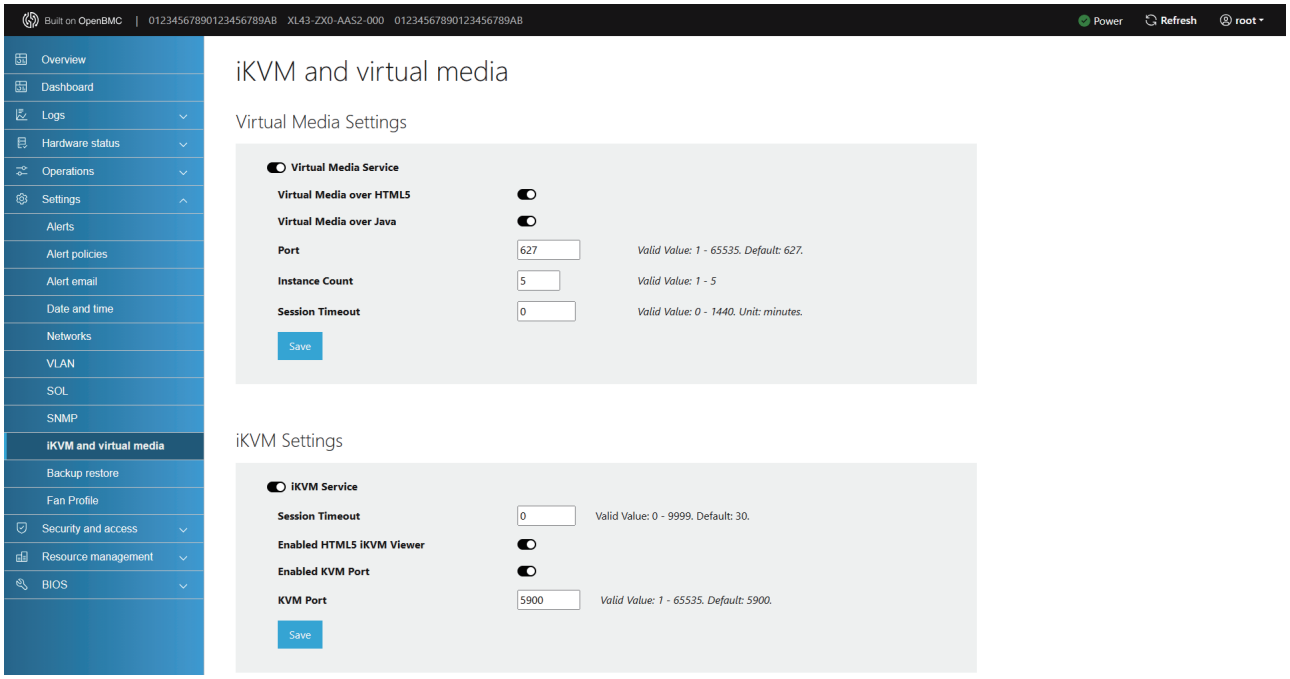
Enable SNMP V1/V2
Enable/disable SNMP Server.

Read-Only Community String
Set read-only Community "public"

Read-Write Community String
Set read-write Community "public"

Save
Click the 'Save' button to save the configuration.

2-6-9 iKVM and virtual media

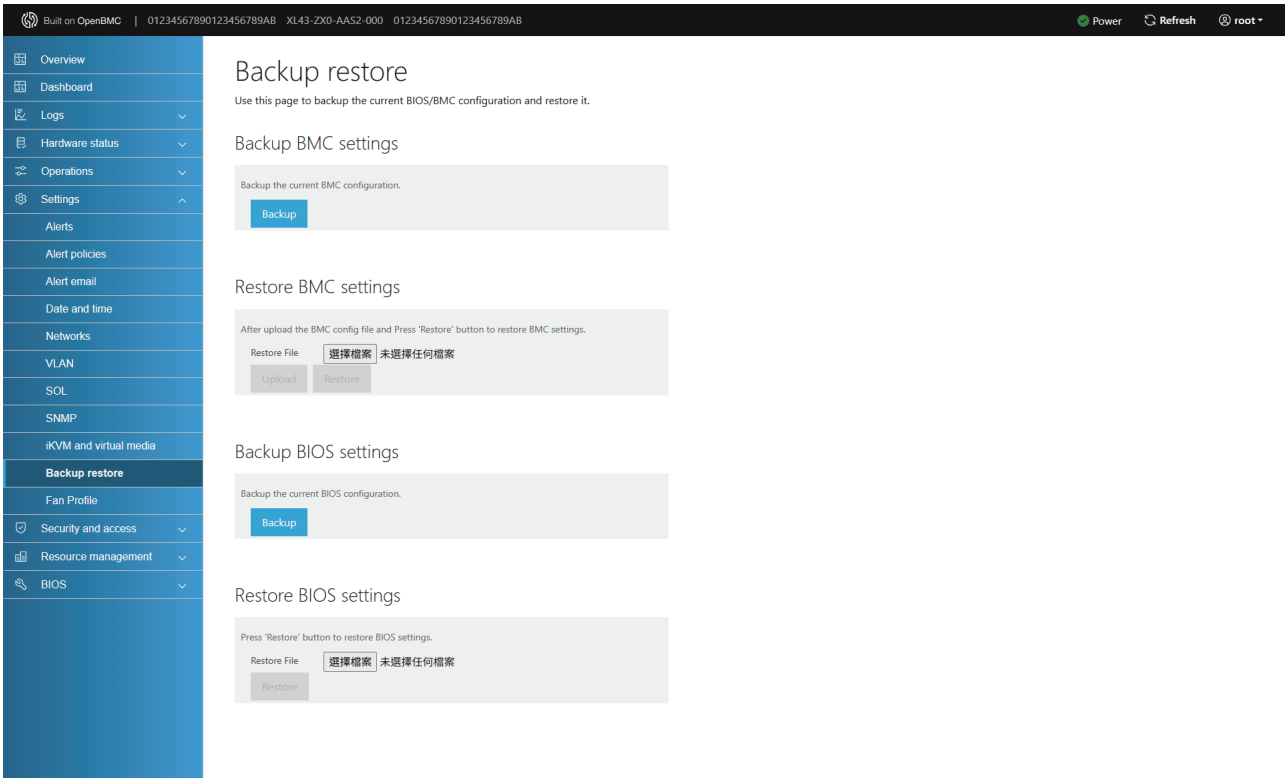


Virtual media settings
Display iKVM and Virtual Media.

Save
Click the 'Save' button to save the configuration.

2-6-10 Backup restore

Use this page to backup the current BIOS/BMC configuration and restore it.



Backup BMC settings

Click the 'Backup' button to backup the current BMC configuration.

Restore BMC settings

Click the 'Restore' button to restore BMC settings.

Backup BIOS settings

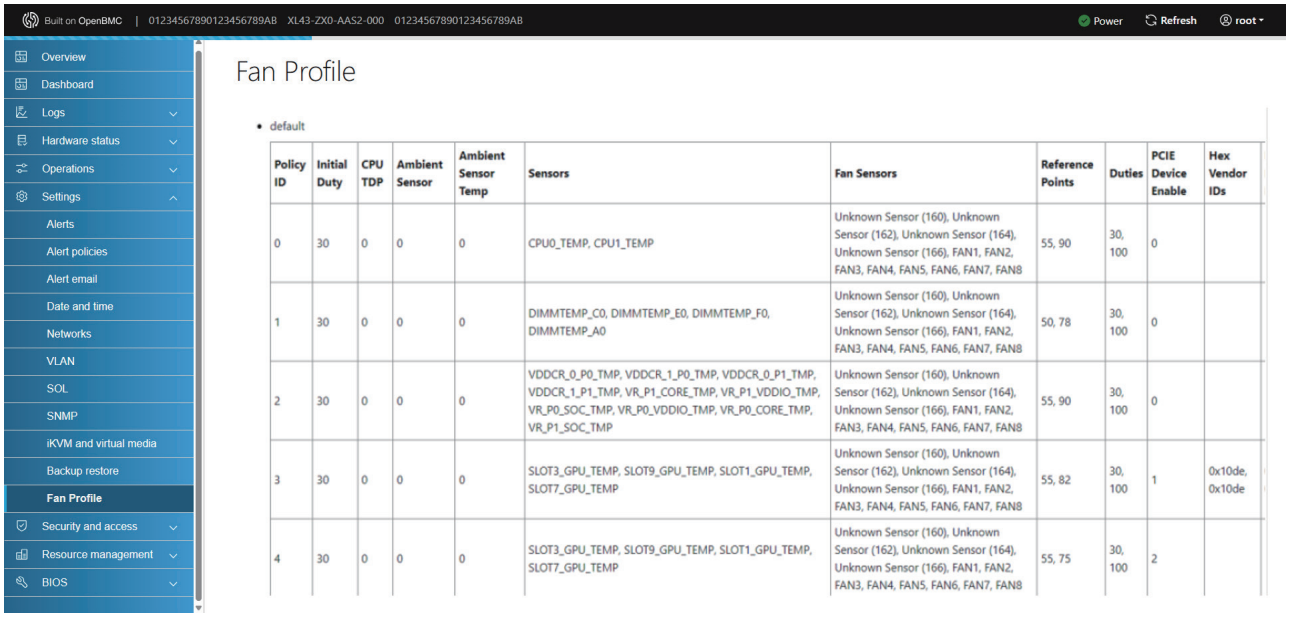
Click the 'Backup' button to backup the current BIOS configuration.

Restore BIOS settings

Click the 'Restore' button to restore BIOS settings.

2-6-11 Fan Profile

This page is used to display total fan policys of System.



Policy ID	Initial Duty	CPU TDP	Ambient Sensor	Ambient Sensor Temp	Sensors	Fan Sensors	Reference Points	Duties	PCIE Device Enable	Hex Vendor IDs
0	30	0	0	0	CPU0_TEMP, CPU1_TEMP	Unknown Sensor (160), Unknown Sensor (162), Unknown Sensor (164), Unknown Sensor (166), FAN1, FAN2, FAN3, FAN4, FAN5, FAN6, FAN7, FAN8	55, 90	30, 100	0	
1	30	0	0	0	DIMMTEMP_C0, DIMMTEMP_E0, DIMMTEMP_F0, DIMMTEMP_A0	Unknown Sensor (160), Unknown Sensor (162), Unknown Sensor (164), Unknown Sensor (166), FAN1, FAN2, FAN3, FAN4, FAN5, FAN6, FAN7, FAN8	50, 78	30, 100	0	
2	30	0	0	0	VDDCR_0_P0_TMP, VDDCR_1_P0_TMP, VDDCR_0_P1_TMP, VDDCR_1_P1_TMP, VR_P1_CORE_TMP, VR_P1_VDDIO_TMP, VR_P0_SOC_TMP, VR_P0_VDDIO_TMP, VR_P0_CORE_TMP, VR_P1_SOC_TMP	Unknown Sensor (160), Unknown Sensor (162), Unknown Sensor (164), Unknown Sensor (166), FAN1, FAN2, FAN3, FAN4, FAN5, FAN6, FAN7, FAN8	55, 90	30, 100	0	
3	30	0	0	0	SLOT3_GPU_TEMP, SLOT9_GPU_TEMP, SLOT1_GPU_TEMP, SLOT7_GPU_TEMP	Unknown Sensor (160), Unknown Sensor (162), Unknown Sensor (164), Unknown Sensor (166), FAN1, FAN2, FAN3, FAN4, FAN5, FAN6, FAN7, FAN8	55, 82	30, 100	1	0x10de, 0x10de
4	30	0	0	0	SLOT3_GPU_TEMP, SLOT9_GPU_TEMP, SLOT1_GPU_TEMP, SLOT7_GPU_TEMP	Unknown Sensor (160), Unknown Sensor (162), Unknown Sensor (164), Unknown Sensor (166), FAN1, FAN2, FAN3, FAN4, FAN5, FAN6, FAN7, FAN8	55, 75	30, 100	2	

Default

Fan Profile default.

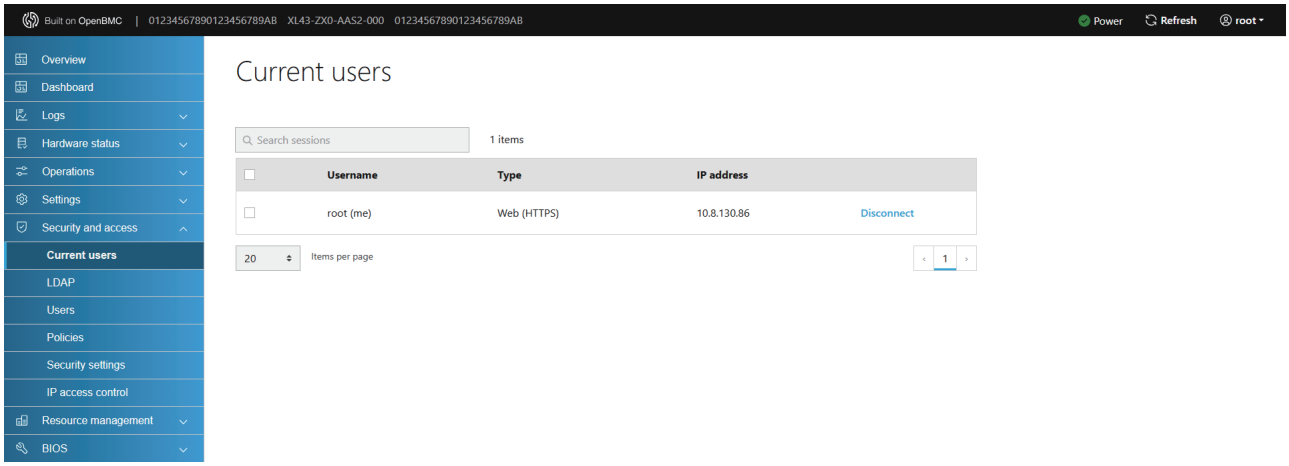
SPECpower

Fan Profile SPECpower.

2-7 Security and access

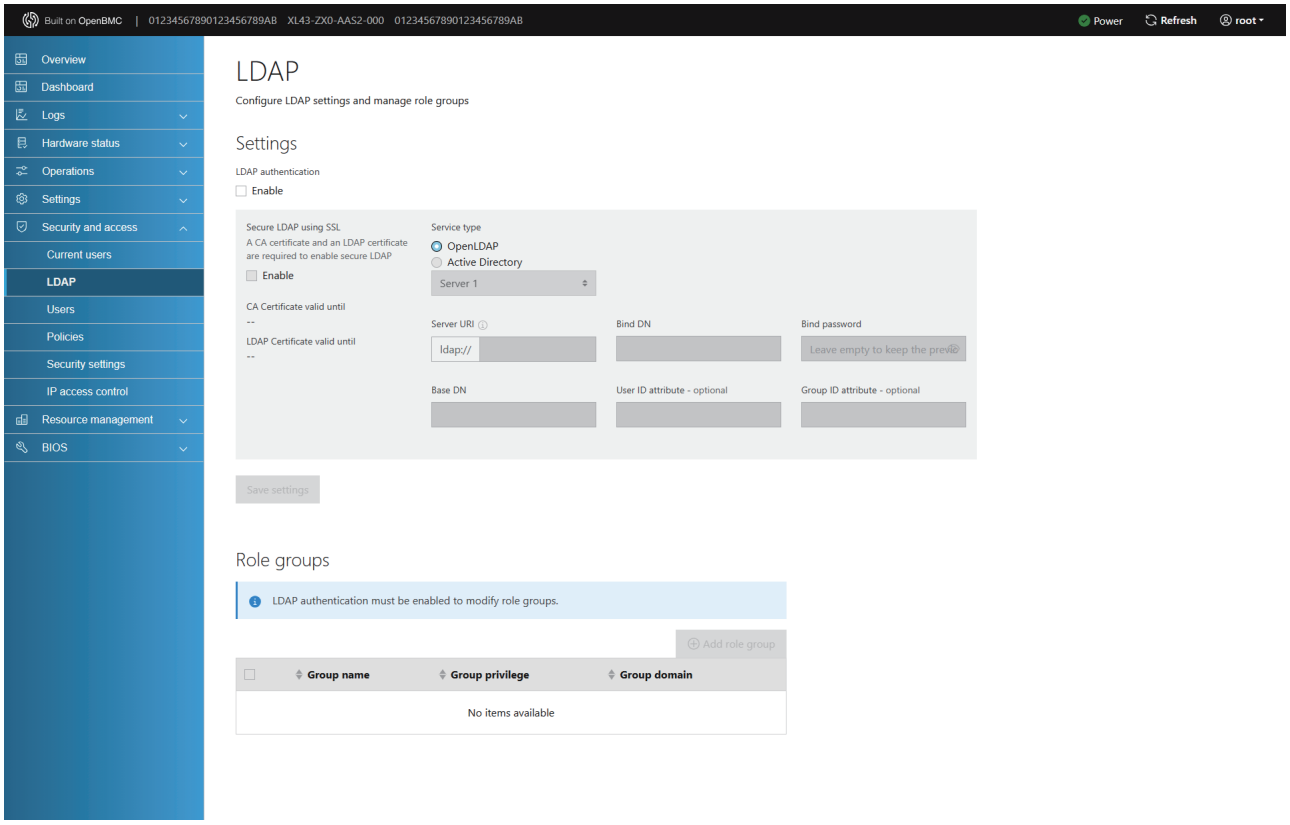
2-7-1 Current users

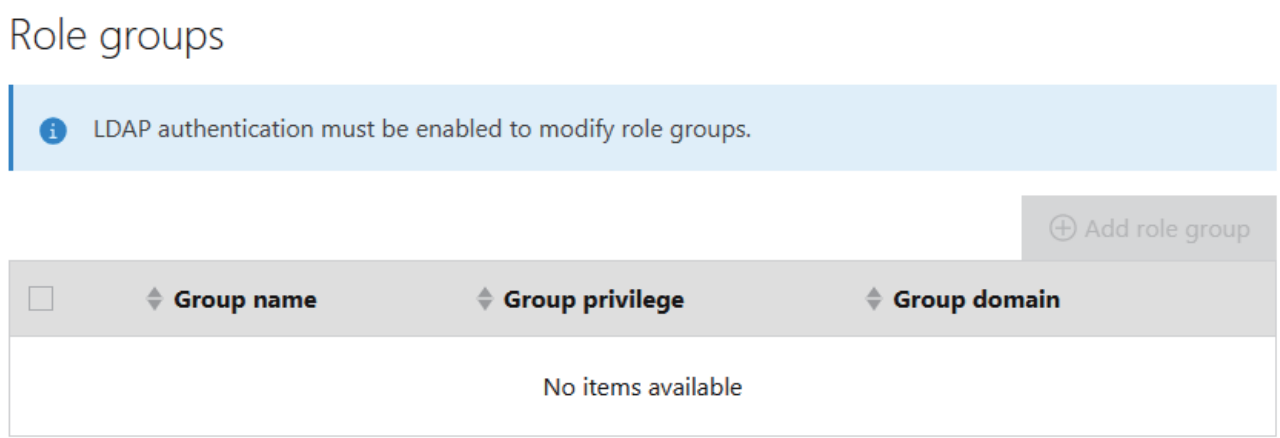
This page is used to display Current Users.



2-7-2 LDAP

The **Lightweight Directory Access Protocol (LDAP)/E-Directory** Settings is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.
In Web GUI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the BMC. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group based policies to control access.





2-7-2-1 Configuring on BMC server (Active Directory Login)

Settings

- Service type: Active Directory/OpenLDAP
- Server URI: Your AD server IP
- Bind DN: (AD user name)@(AD domain name)
  - e.g. good@adtest.local.com
- Bind password: AD user password
- Base DN: AD domain name
  - e.g. dc=adtest,dc=local,dc=com

Note: User ID and Group ID is optional and could keep empty

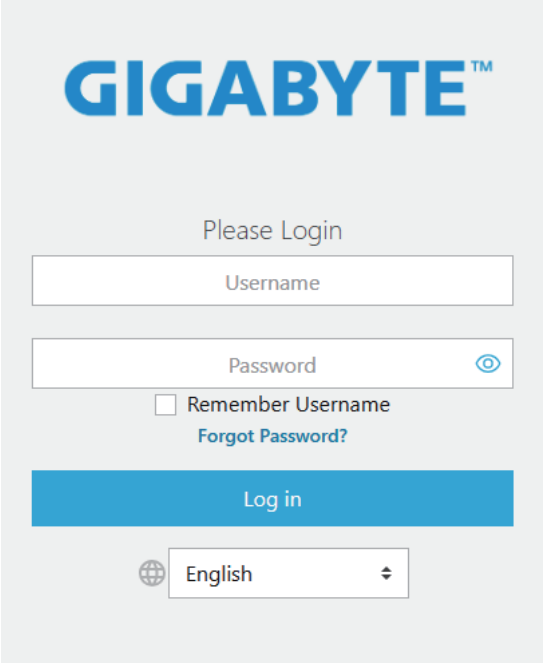
- Add role group
- Group name: Your AD user primary group
  - e.g. davidtest

Note: If you didn't setup AD user's primary group, default primary group will be Domain Users

- Group privilege: Select login access ability
  - e.g. Administrator

Active Directory Login

Web GUI login screen with AD user and password



OpenLDAP
Environment setup
Prompt when installing:
OS : Ubuntu 20.04
sudo apt-get install slapd ldap-utils gnutls-bin ssl-cert
1. Administrator password => admin (Please input your LDAP admin password)
2. Confirm password => admin

Configuring slapd
In Ubuntu, there is a terminal UI to reconfigure slapd.
sudo dpkg-reconfigure slapd Follow the steps below to set your environment:
1. Omit OpenLDAP server configuration? => No
2. DNS domain name => sc1.test (Domain name will be your base DN)
3. Organization name => bmc
4. Administrator password => admin (Please input your LDAP admin password)
5. Confirm password => admin
6. Do you want the database to be removed when slapd is purged => No
7. Move old database => yes

LDAP Browser/Editor After configuring LDAP is finished, reviewing or editing the LDAP tree can be done through the LDAP browser/editor application. We will use phpldapadmin for the following example:

1. Install phpldapadmin for LDAP management

sudo apt-get install phpldapadmin

2. Edit phpldapadmin configurations

sudo vi /etc/phpldapadmin/config.php

```
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=sc1,dc=test'));

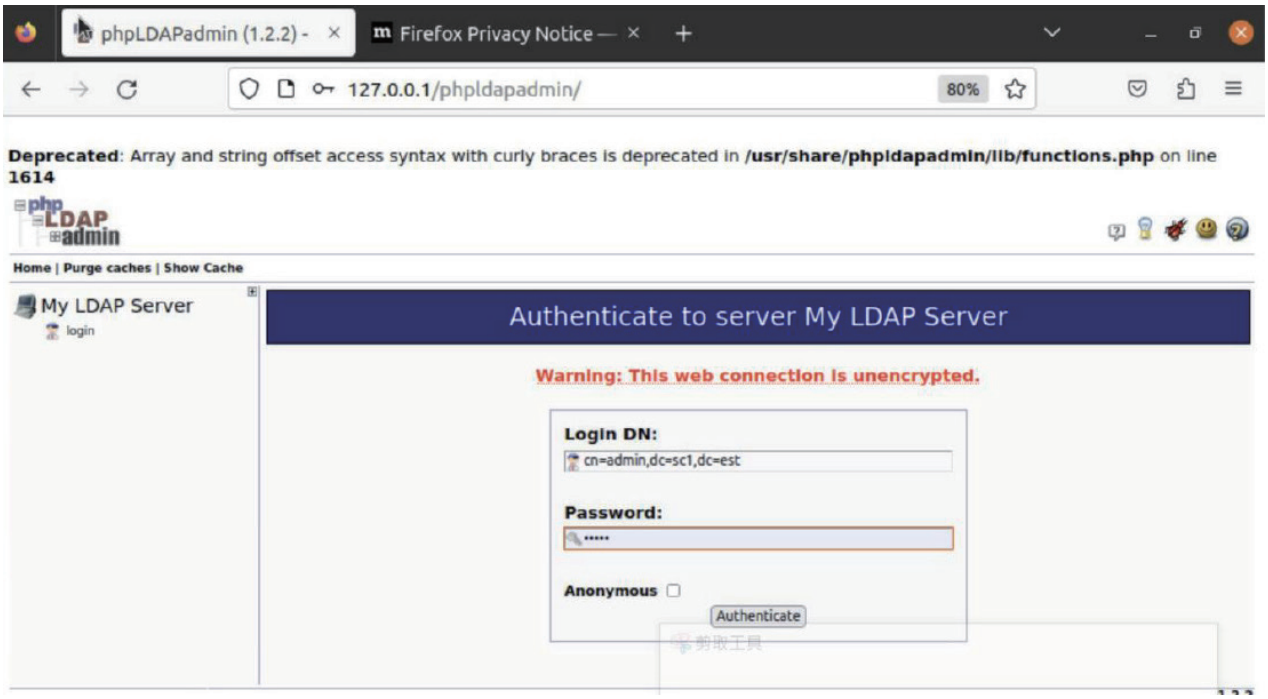
/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password
```

```
$config->custom->appearance['hide_template_warning'] = true;
#  $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');

/* Your LDAP password. If you specified an empty bind_id above, this MUST also
```

Login to phpLDAPadmin to set LDAP users

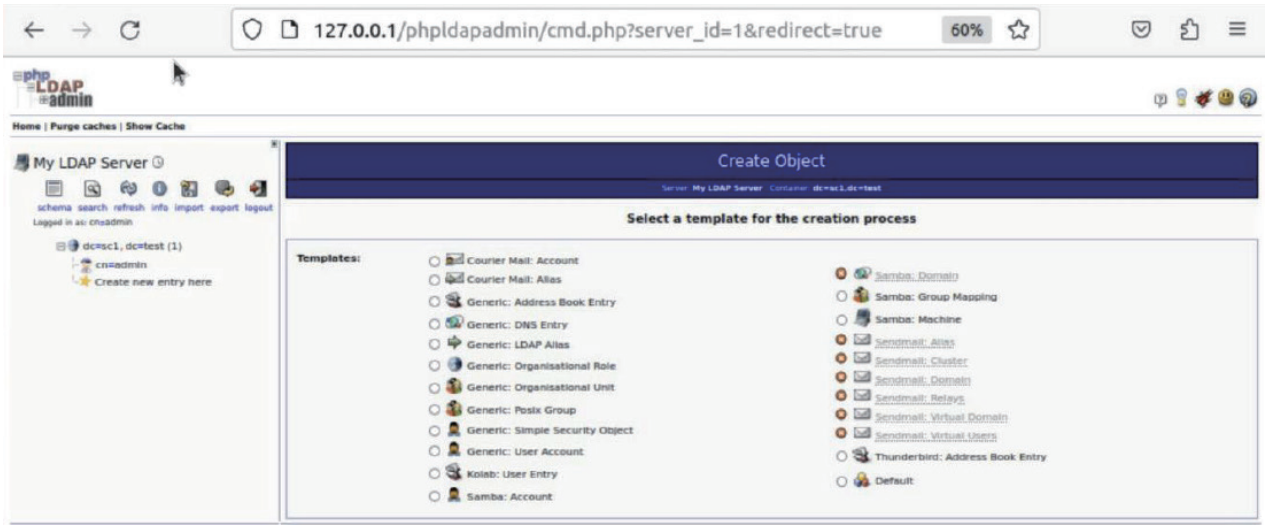
http://localhost/phpldapadmin



Login DN: cn=admin,dc=sc1,dc=test

Login password: admin

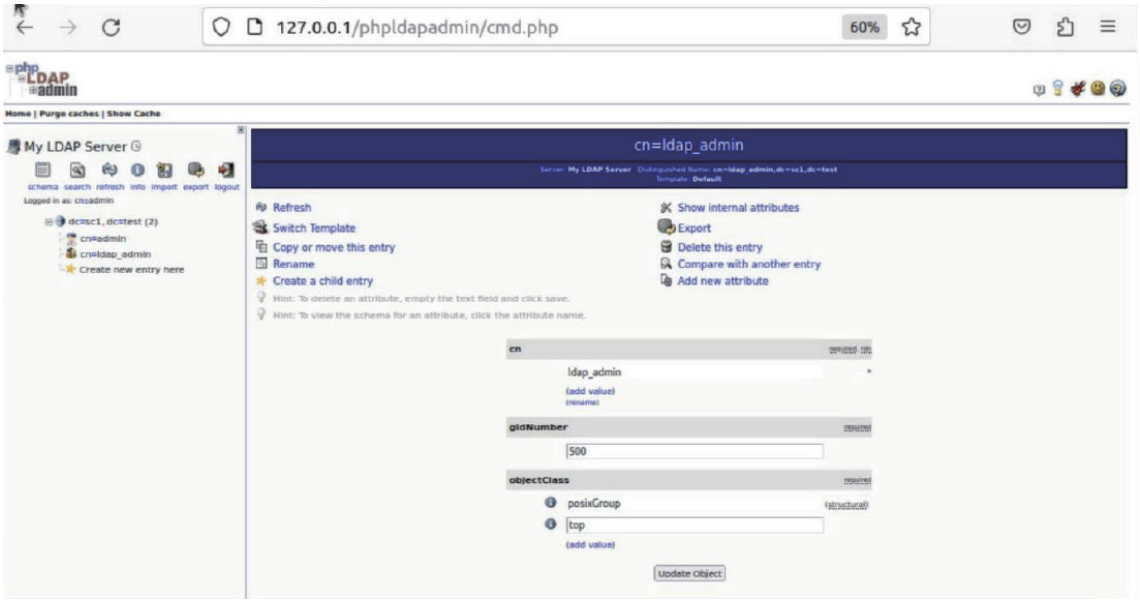
Setting on LDAP server



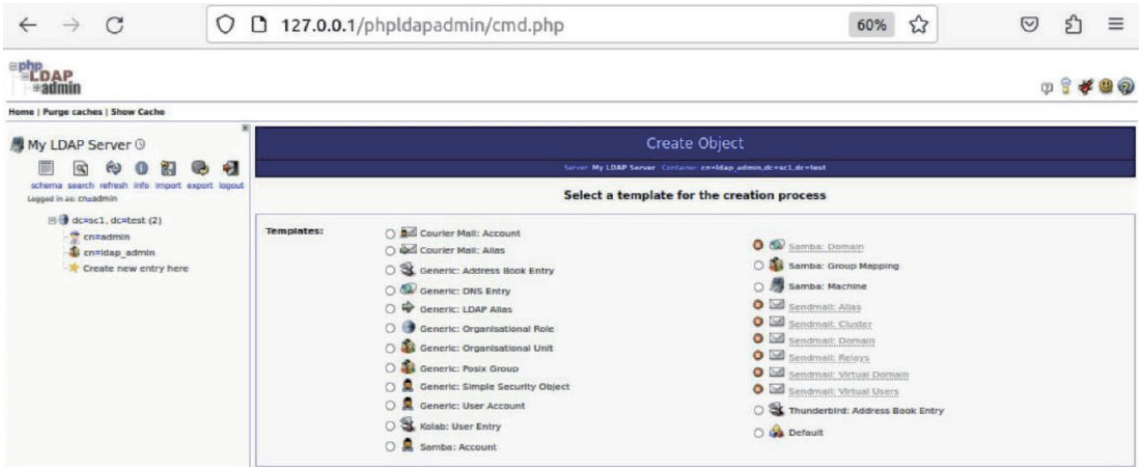
1. Click Create a child entry
2. Click Generic: Posix Group



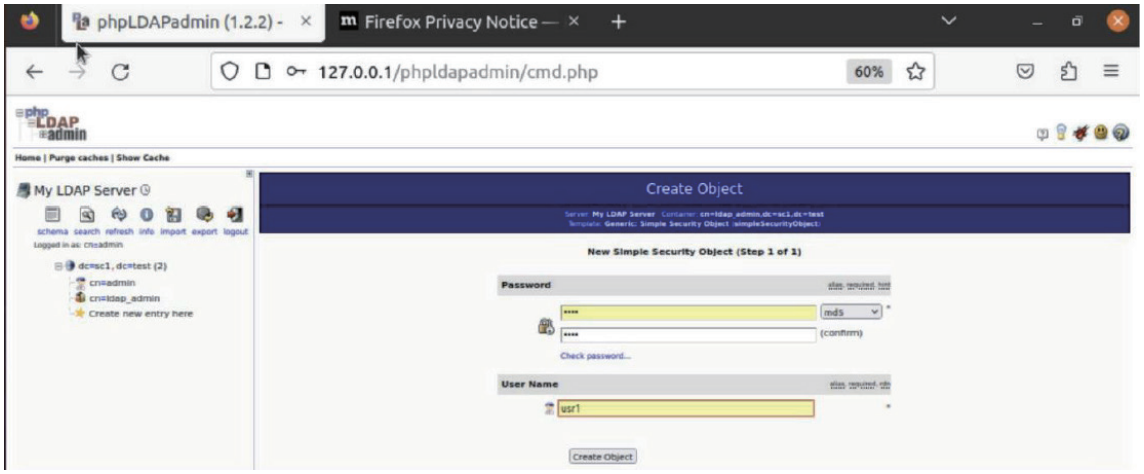
3. Input ldap_admin and click Create object



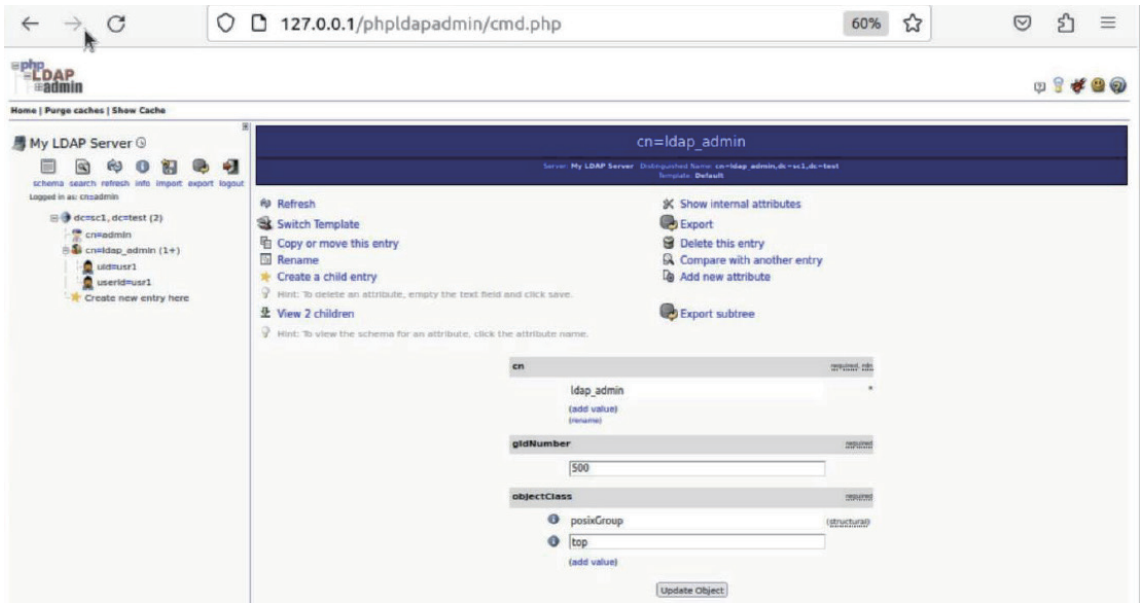
4. Input ldap_admin and click Create a child entry



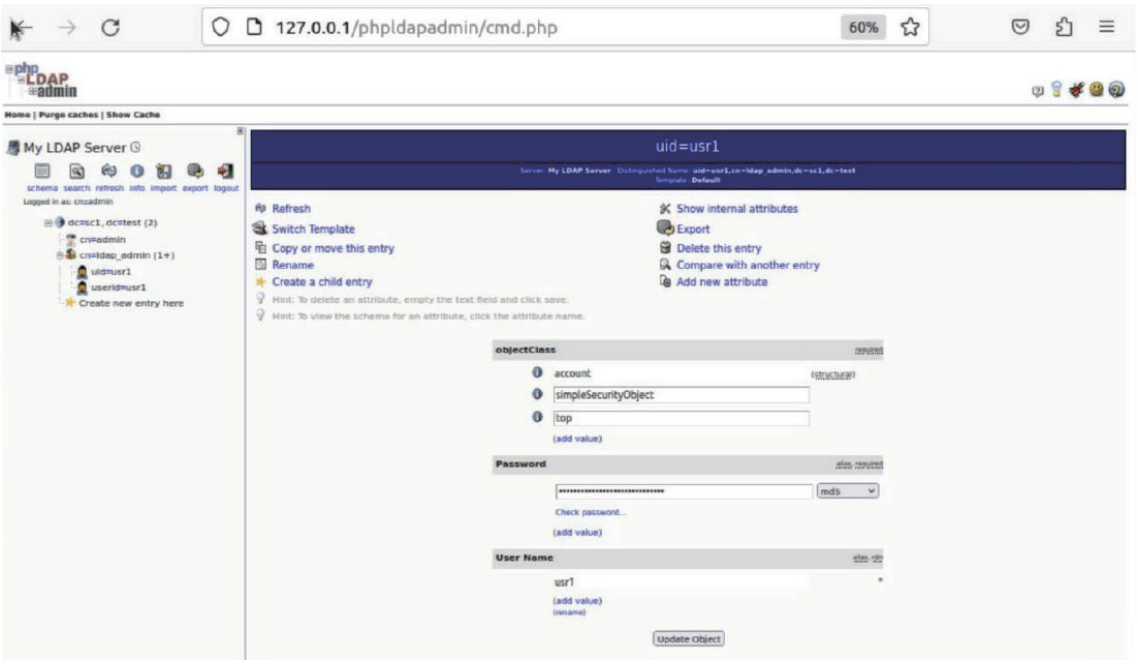
5. Click Generic: Simple Security Object



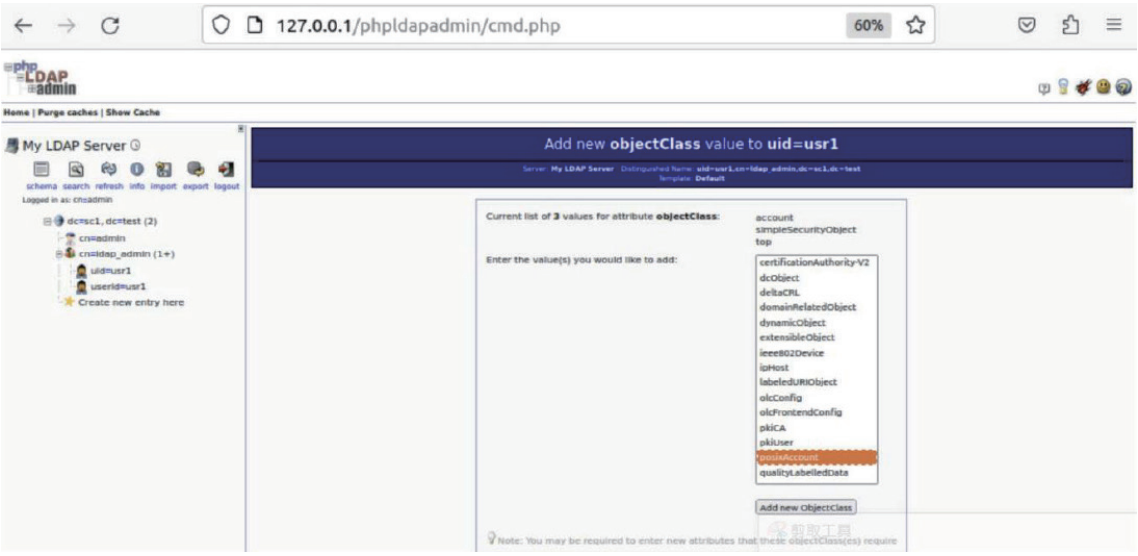
6. Input password pwd1 and User Name usr1



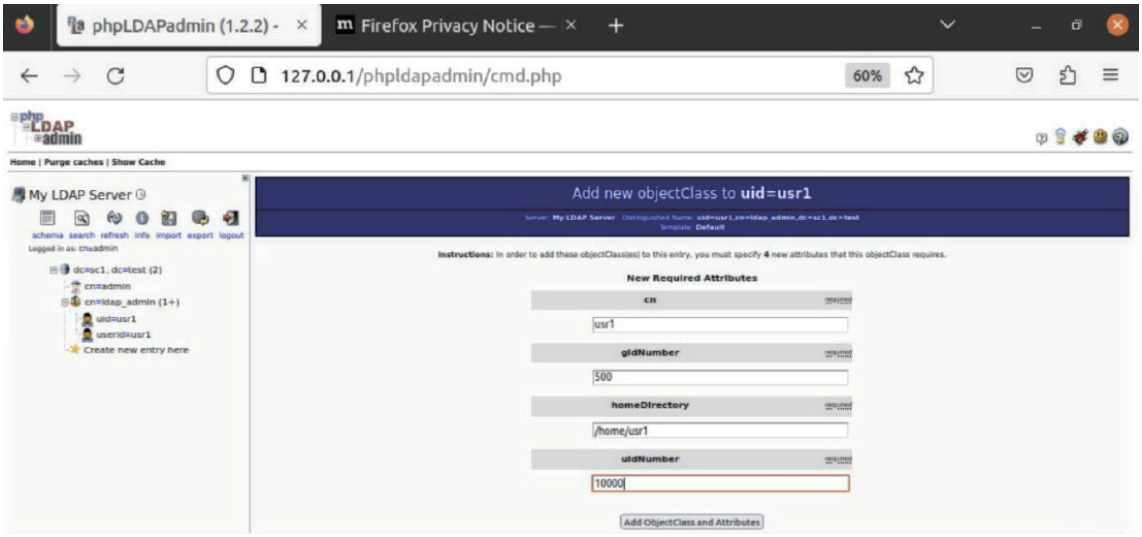
7. Click cn=ldap_admin and check the gid, it's 500 in this example



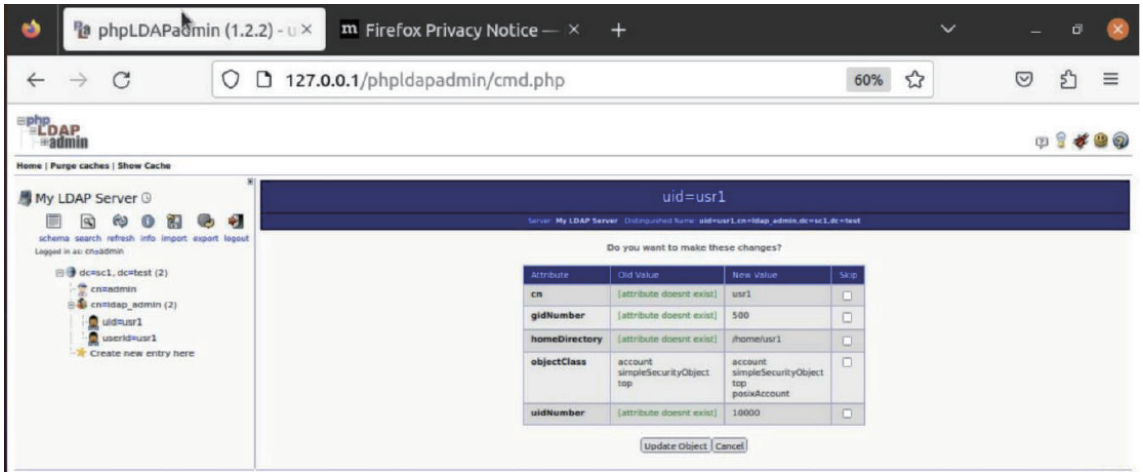
8. Click userid=usr1 and add value to attribute objectClass



9. Select posixAccount

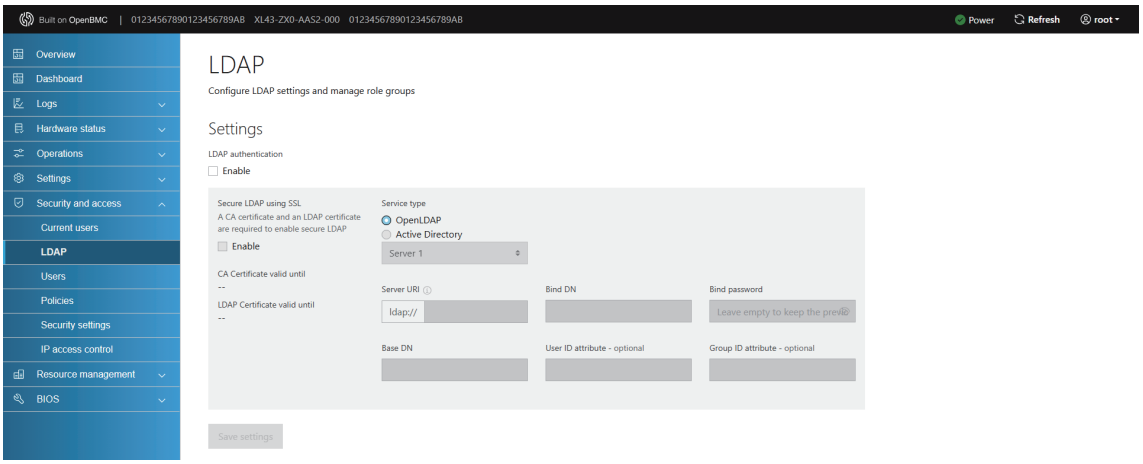


10. Input attribute
    - cn is usr1
    - gidNumber is the gid of ldap_admin, it's 500 in this example
    - homeDirectory is /home/usr1 (no effect)
    - uidNumber is 10000 (no effect)



2-7-2-2 Configuring on BMC server (OpenLDAP)

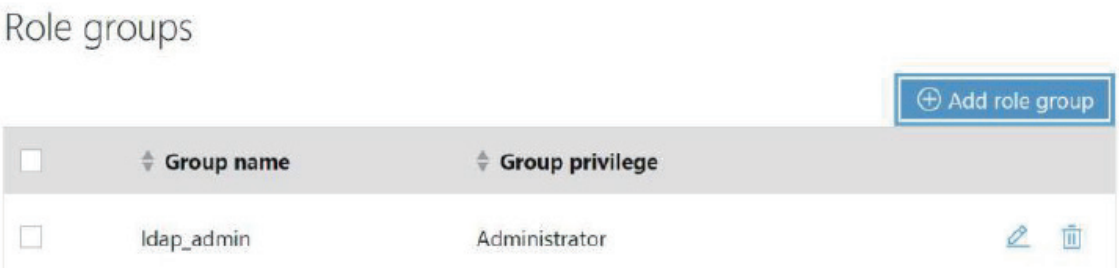
To enable/disable LDAP, check or uncheck the "Enable LDAP Authentication" checkbox respectively.



Settings

Web login -> Security and access Page -> LDAP page.

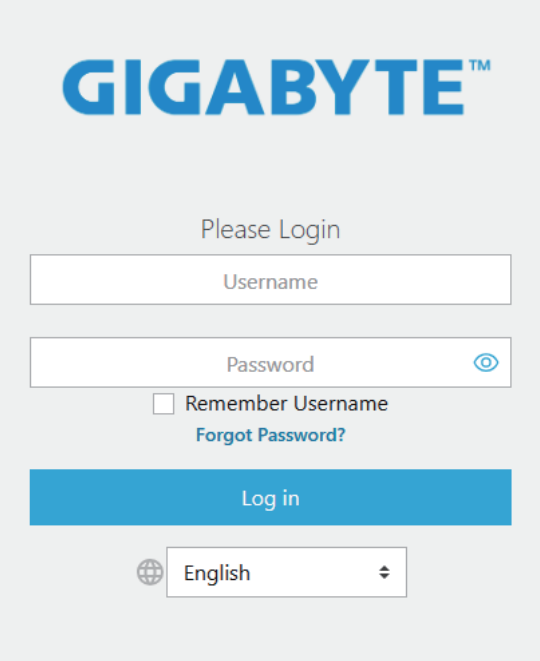
- Enable LDAP authentication
- Choose Service type **OpenLDAP**
- Enter LDAP Server URI
- Bind DN is **cn=admin,dc=sc1,dc=test**
- Bind Password is **admin**
- Bind DN is **dc=sc1,dc=test**
- User ID attribute is **cn**
- Group ID attribute is **gidNumber**
- Click Save settings, then you can add role group



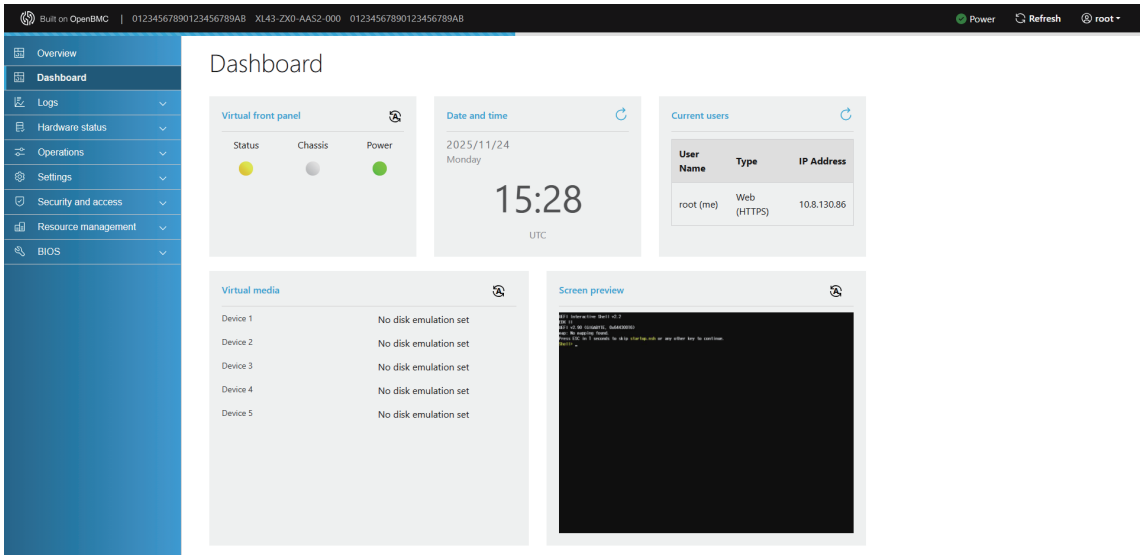
Click "Add role group"

- Group name is **ldap_admin**
- Group privilege **Administrator**
- Click Add

Active Directory Login



Login in WebUI successfully



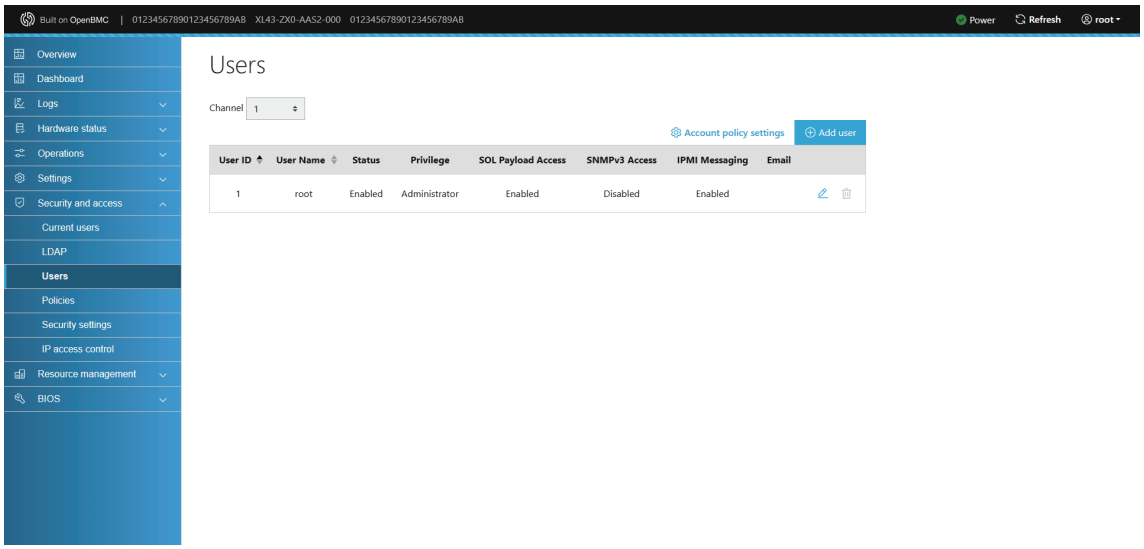
Login Web test

Now you can login with LDAP user **usr1** with password **pwd1**

2-7-3 Users

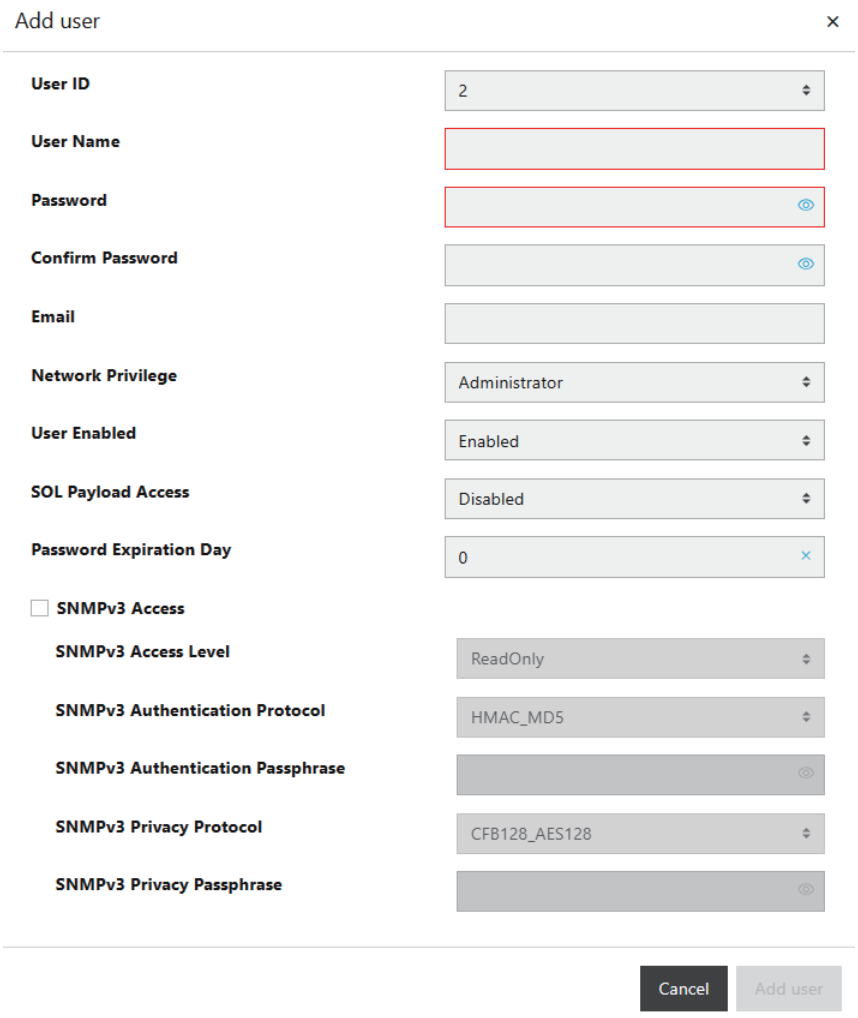
In Web GUI, the User page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click **Security and access > Users** from the menu bar. A sample screenshot of User Management Page is shown below.



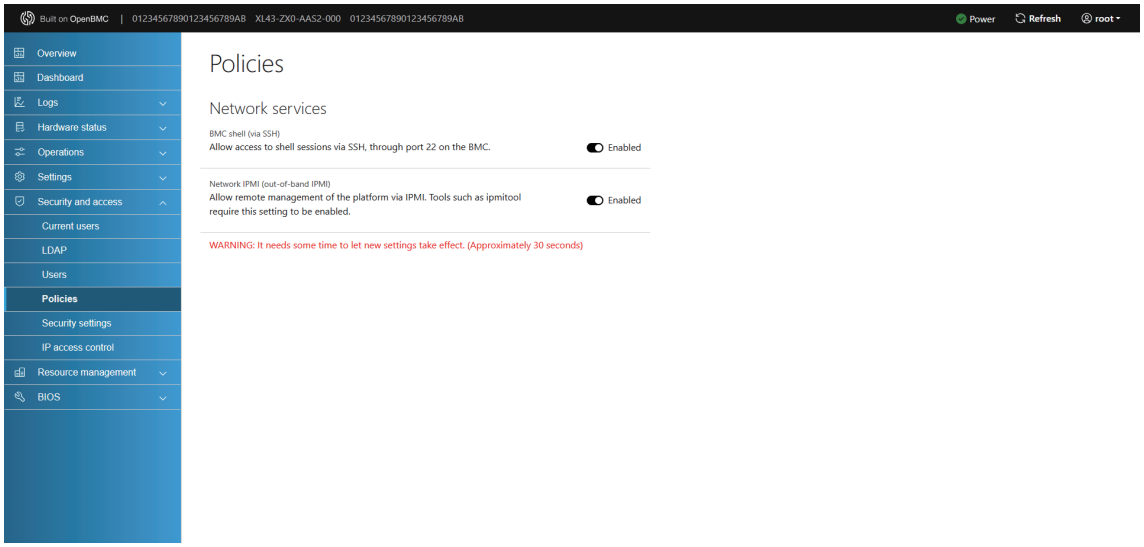
Click "Add user' for advanced configuration.

Fill in related the new user information and click 'Save user' to create a user.



2-7-4 Policies

This page is used to configure Policies.



Network services

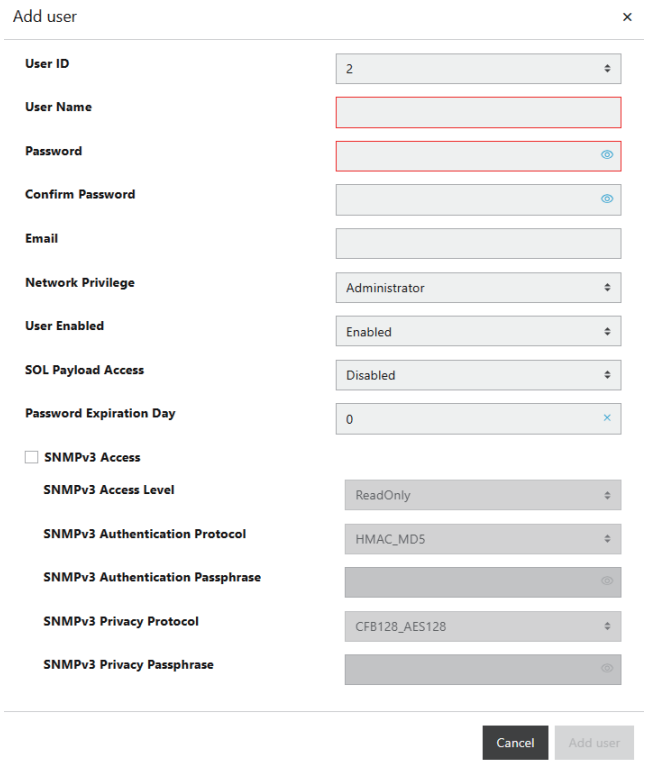
- BMC shell (via SSH)
- Network IPMI (out-of-band IPMI)

BMC shell (via SSH)

Allow access to shell sessions via SSH, through port 22 on the BMC.

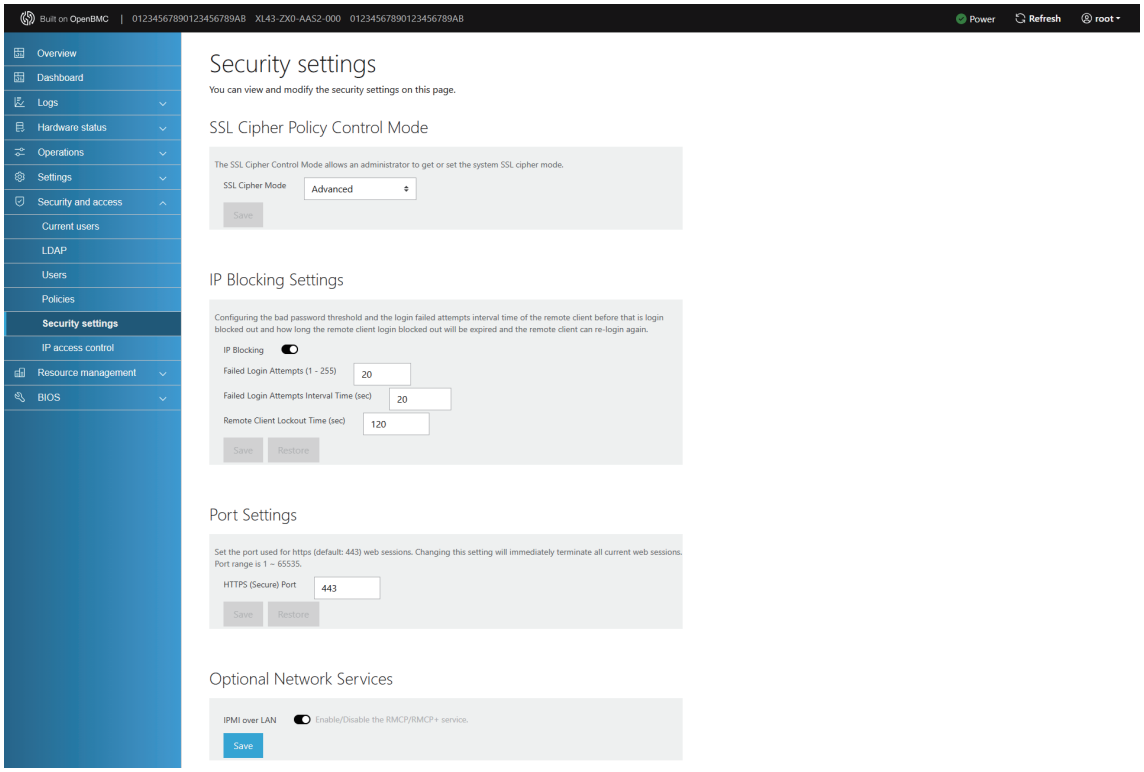
Network IPMI (out-of-band IPMI)

Allow remote management of the platform via IPMI. Tools such as ipmitool require this setting to be enabled.



2-7-5 Security settings

You can view and modify the security settings on this page.



Network services

- BMC shell (via SSH)
- Network IPMI (out-of-band IPMI)IPMI over LAN

BMC shell (via SSH)

Allow access to shell sessions via SSH, through port 22 on the BMC.

Network IPMI (out-of-band IPMI)

Allow remote management of the platform via IPMI. Tools such as ipmitool require this setting to be enabled.

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode allows an administrator to get or set the system SSL cipher mode.
Select the SSL Cipher Mode and click 'Save' to save the configuration.

IP Blocking Settings

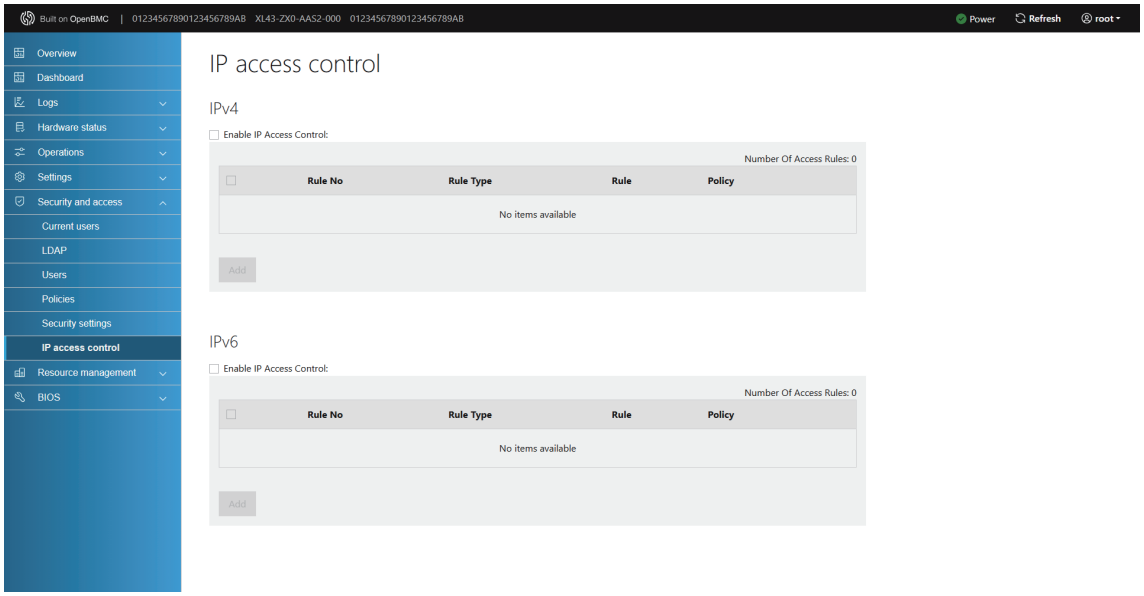
Configuring the bad password threshold and the login failed attempts interval time of the remote client before that is login blocked out and how long the remote client login blocked out will be expired and the remote client can re-login again.

Optional Network Services

- IPMI over LAN: Enable or disable the RMCP/RMCP+ service. Click 'Save' to save the configuration.

2-7-6 IP access control

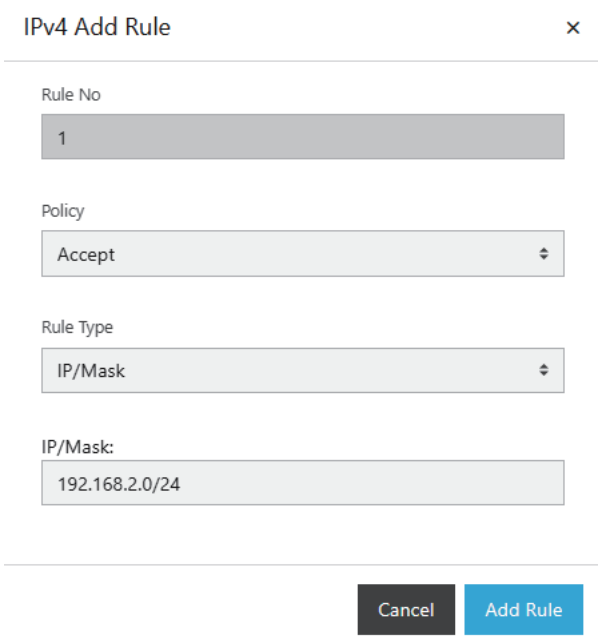
Use this page to add, edit or remove IP access rules.



IPv4

Enable IP Access Control

- Click for enable or disable IP Access Control policy.



Add

Add a new rule.

Insert

Insert a new rule.

Modify

Modify the existed rule.

Delete
Delete the existed rule.

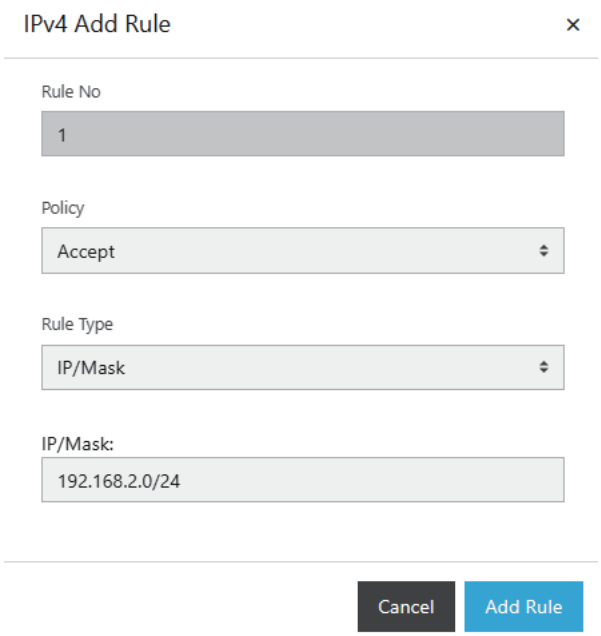
Rule No
Show current Rule No.

Policy
- accept
- drop

Rule Type
- ipMask: Enter IP/Mask.
- ipRange: Enter IP Range Start and End.
- Mac: Enter mac address
- Port: Enter tcp/udp protocol

Add Rule
Click on the Add button to add new rule.

IPv6
Enable IP Access Control
Click for enable or disable IP Access Control policy.



Add
Add a new rule.

Insert
Insert a new rule.

Modify
Modify the existed rule.

Delete
Delete the existed rule.

Rule No
Show current Rule No.

Policy
- accept
- drop

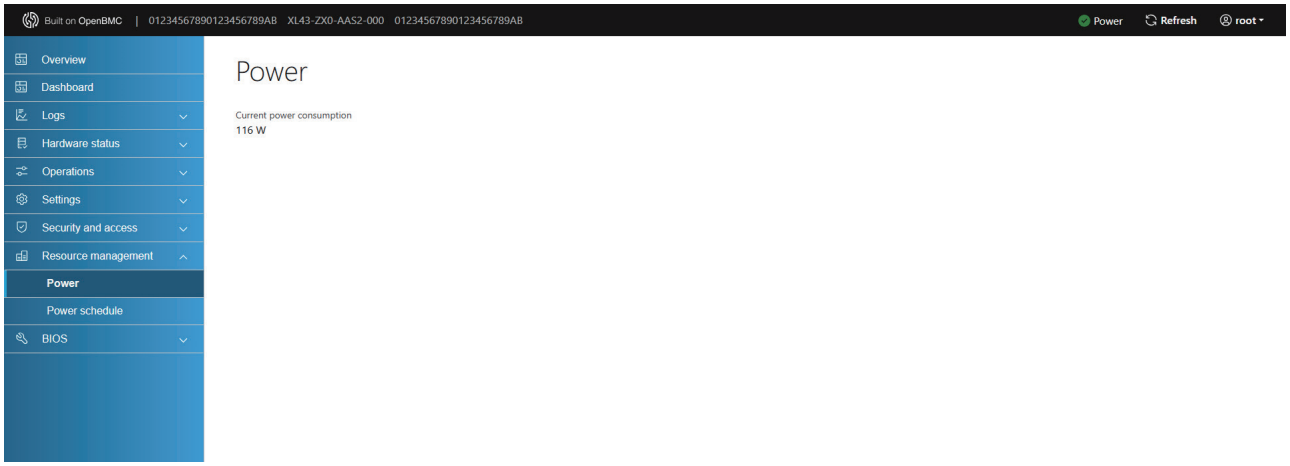
Rule Type
- ipMask: Enter IP/Mask.
- ipRange: Enter IP Range Start and End.
- Mac: Enter mac address
- Port: Enter tcp/udp protocol

Add Rule
Click on the Add button to add new rule.

2-8 Resource Management

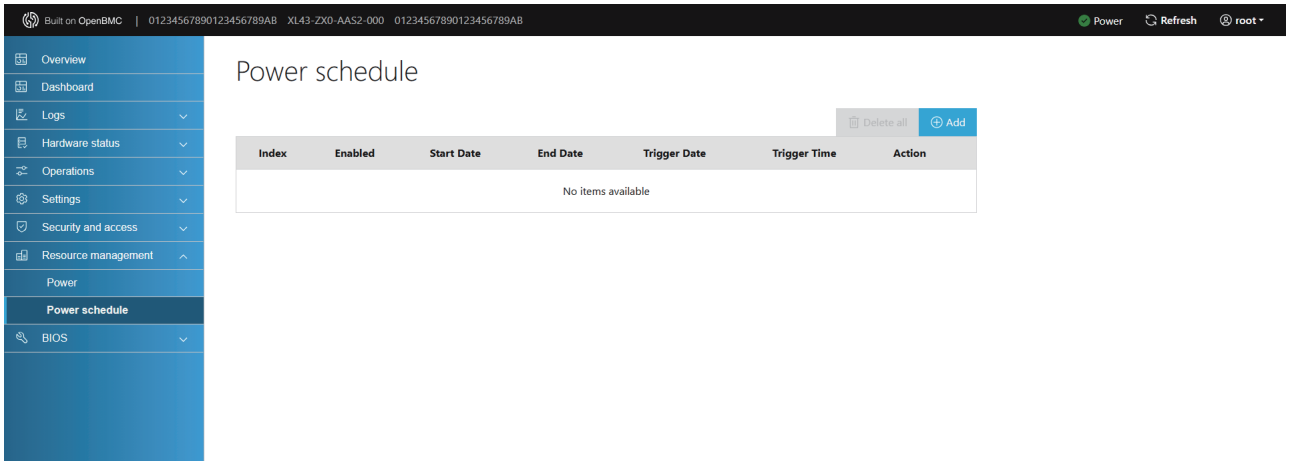
2-8-1 Power

Displays system power information.



2-8-2 Power Schedule

Displays power schedule.

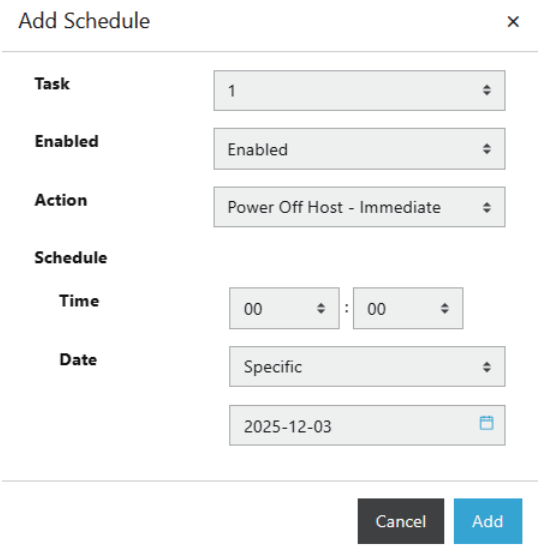


Delete all

Click on the Delete all button to delete all data.

Add

Click on the Add button to add new data. Add Schedule window pops up. Enter values and click 'Save' to add a new power schedule.

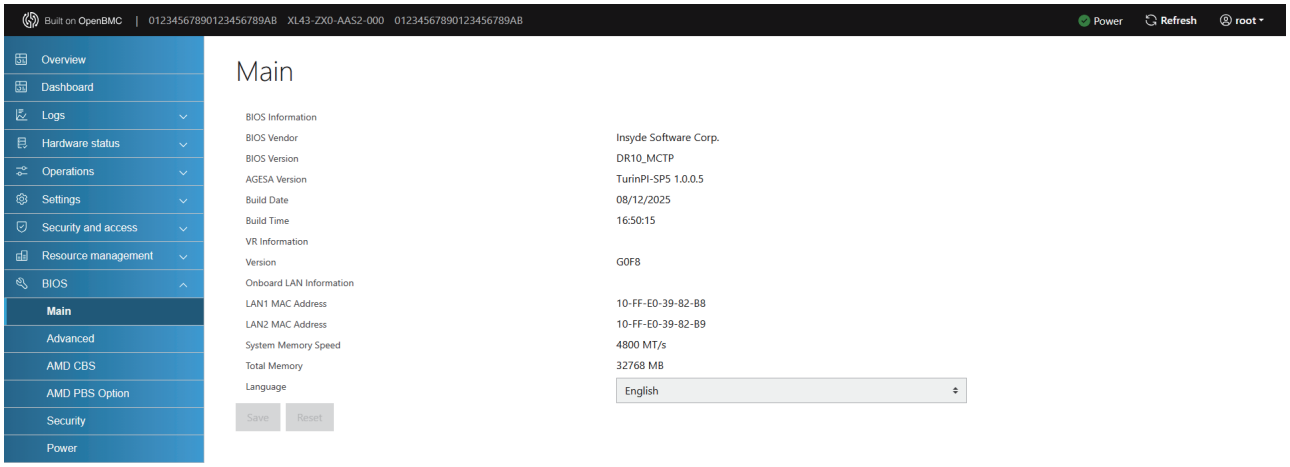


2-9 BIOS (AMD BIOS joint feature)

This is Insyde BIOS joint feature. You should turn on the host and wait for the BIOS to upload the relevant data.

2-9-1 Main

The page show all BIOS configurations.



Save

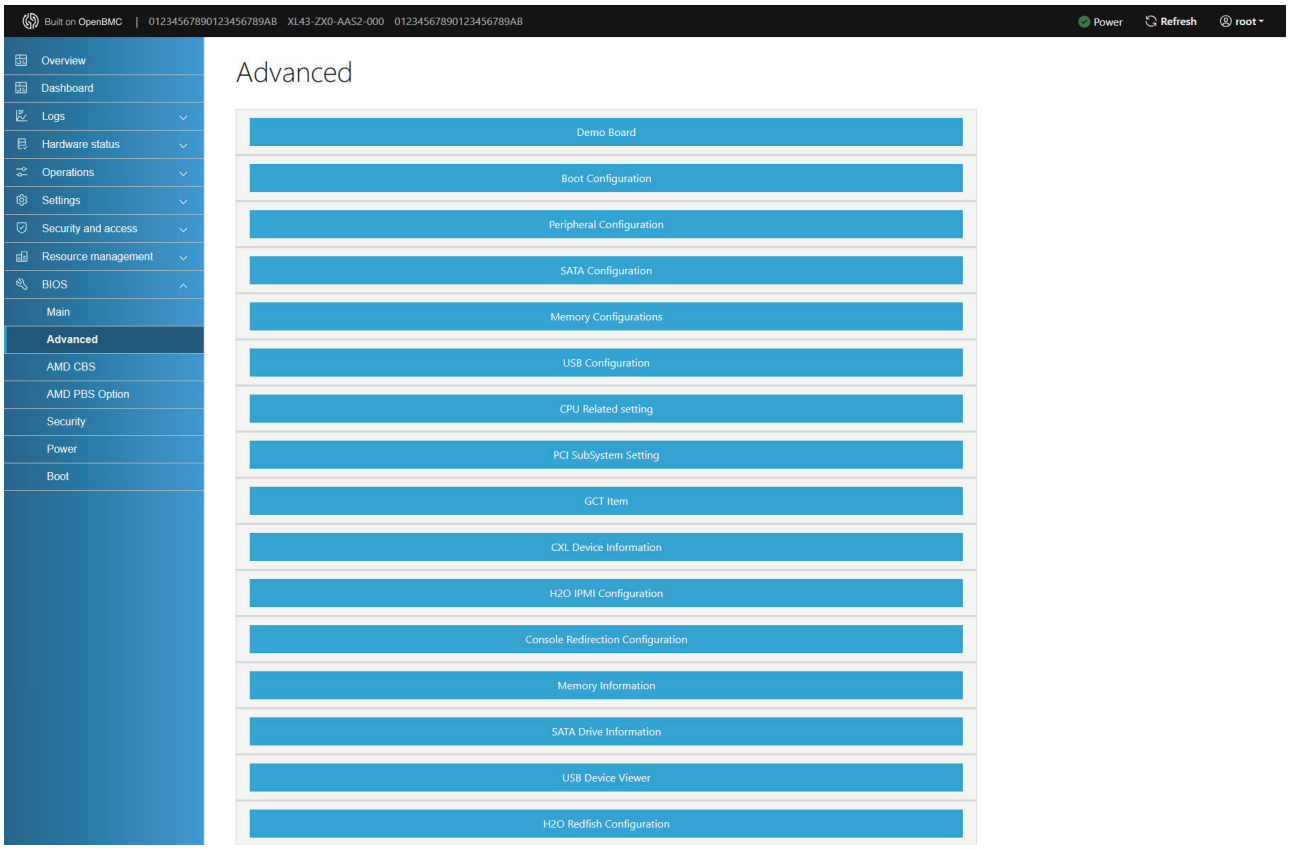
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-2 Advanced

The page shows all BIOS advanced page configurations.



Save

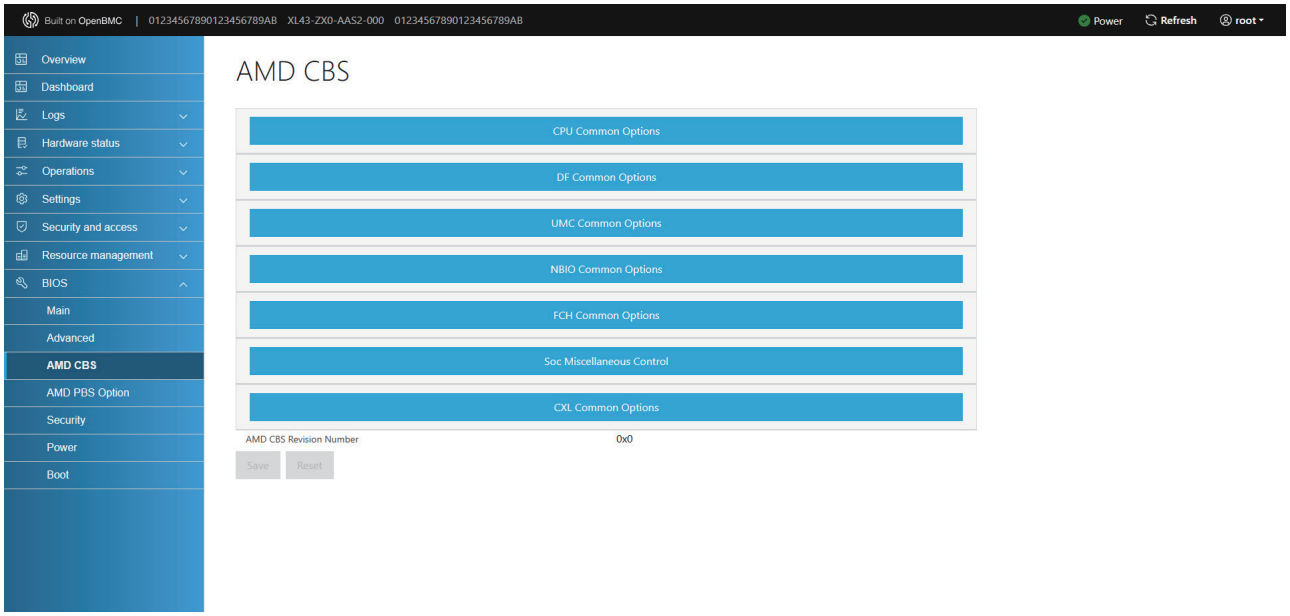
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-3 AMD CBS

This page page includes the common items for configuration of AMD system-related information.



Save

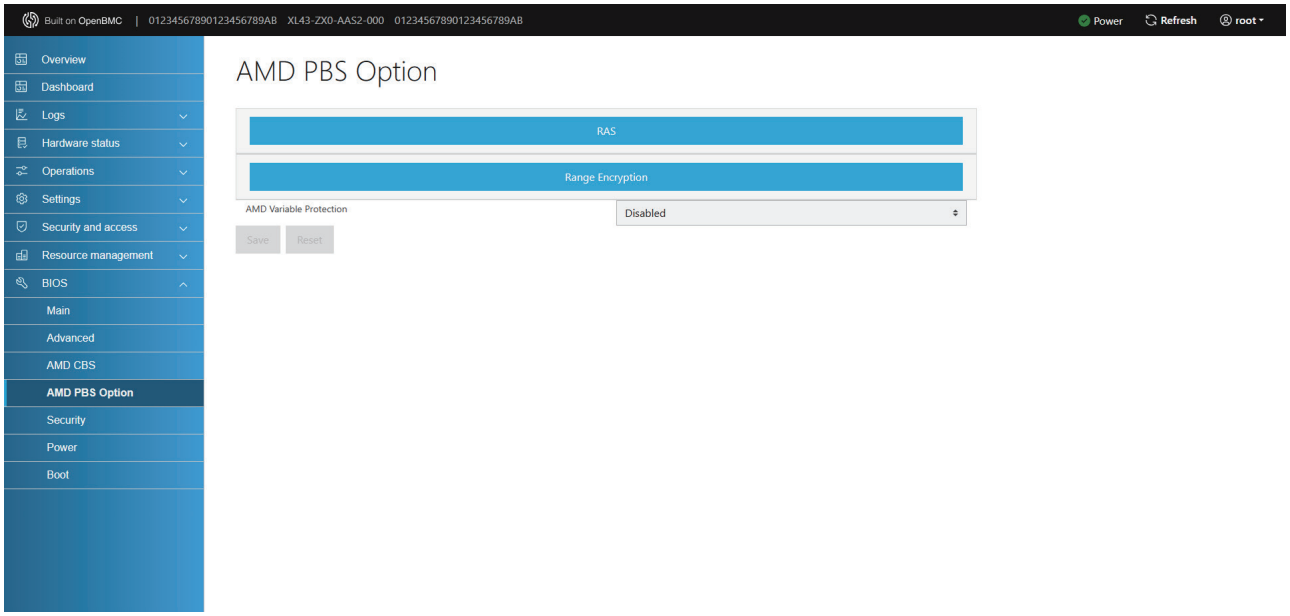
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-4 AMD PBS Option

This setup page includes the common items for configuration of AMD CPM RAS related settings.



Save

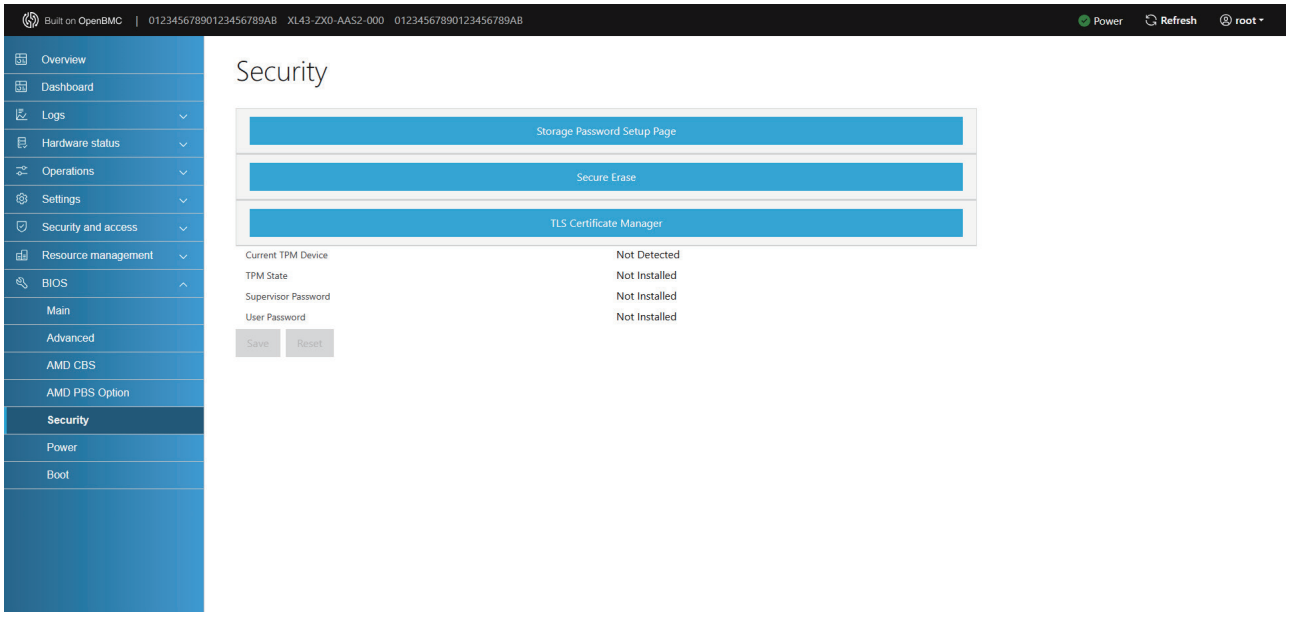
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-5 Security

Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.
A supervisor password allows you to make changes in BIOS Setup.
A user password only allows you to view the BIOS settings but not to make changes.



Save

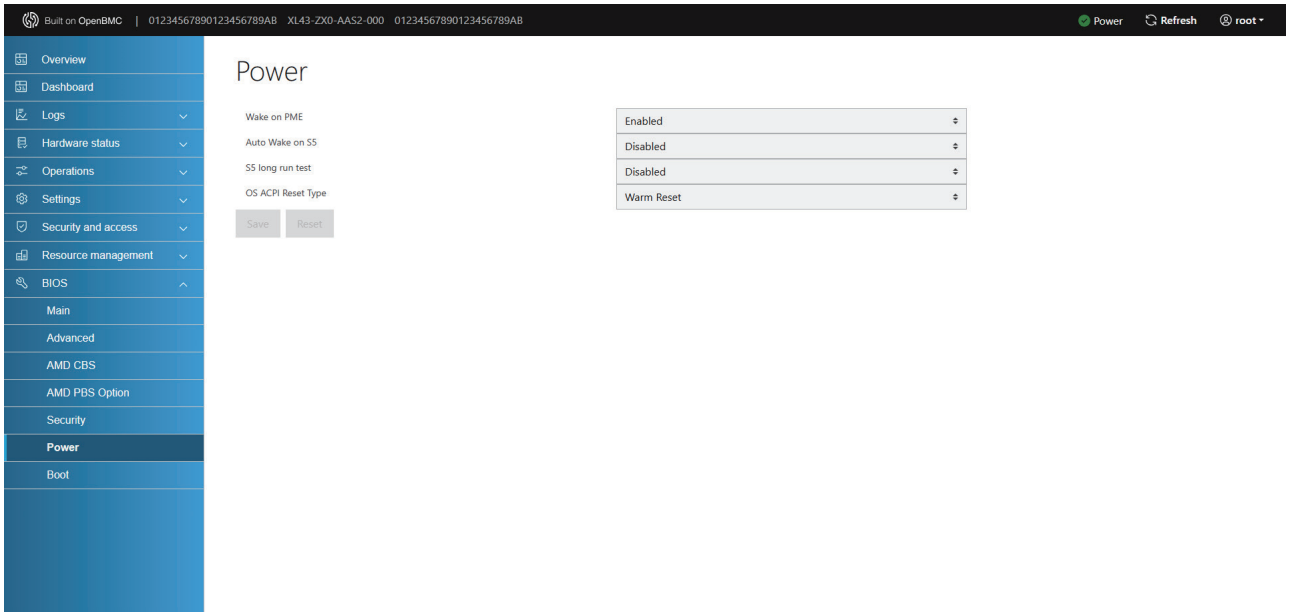
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-6 Power

Displays BIOS power information.



Save

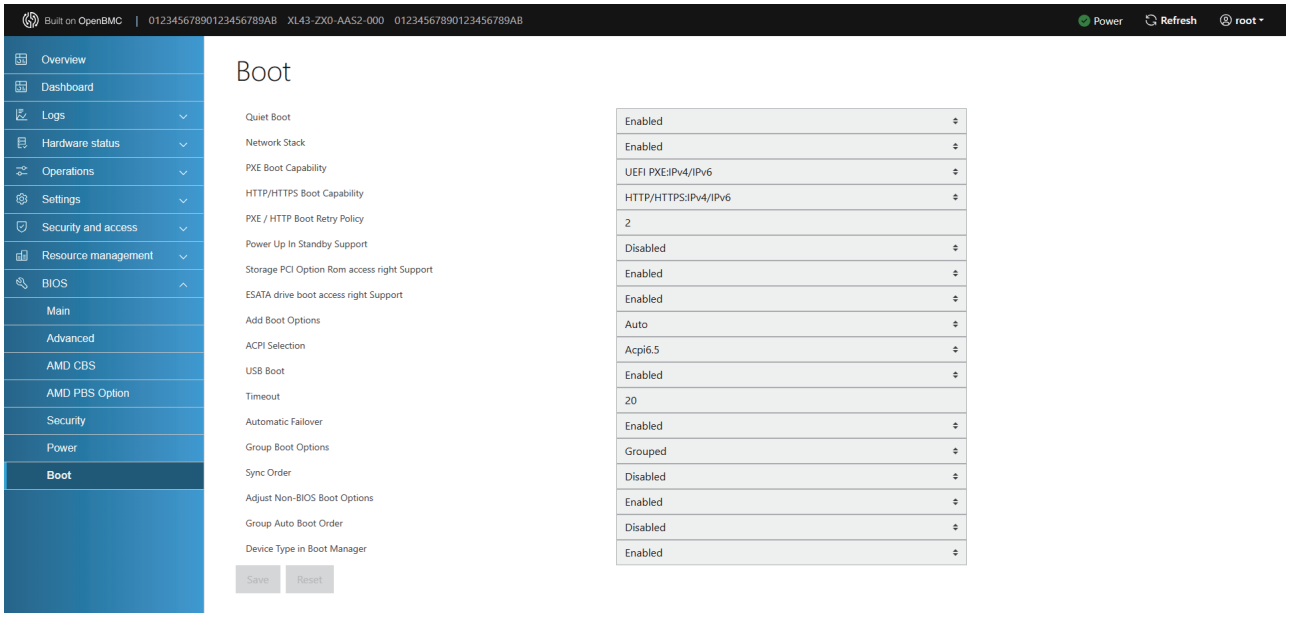
Click on the Save button to apply your configuration to host after next boot on.

Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-9-7 Boot

Displays BIOS boot information and provides items for configuration of the boot sequence.



Save

Click on the Save button to apply your configuration to host after next boot on.

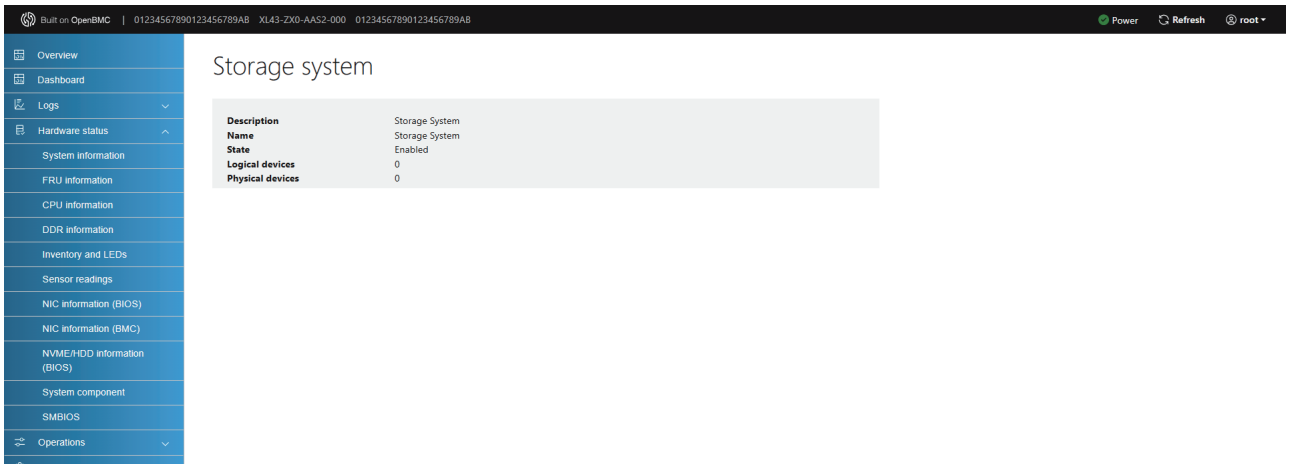
Reset

Click on the Reset button to reset all your modification, and reload page as current BIOS configuration.

2-10 Storage (will become visible when RAID Card is installed)

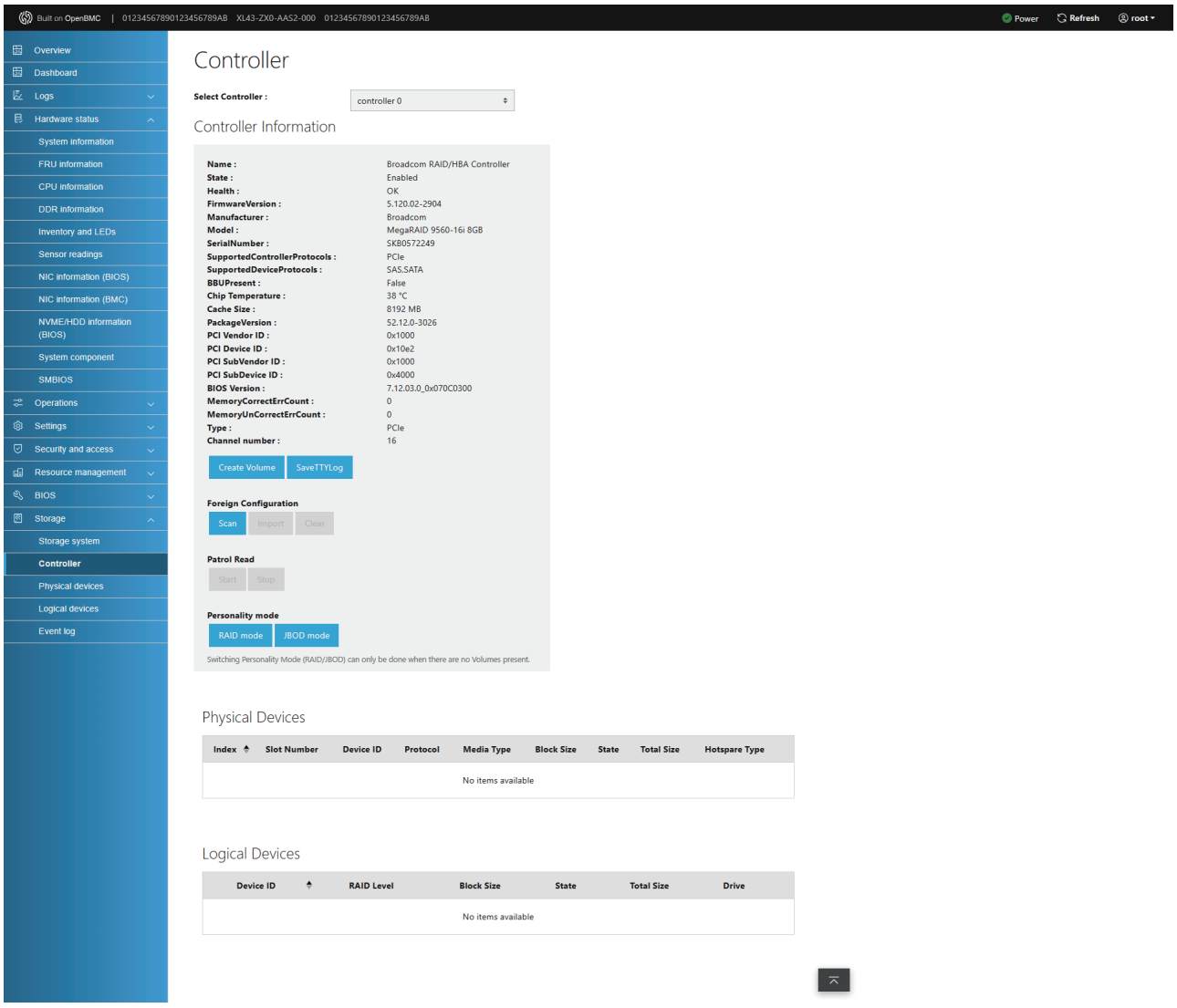
2-10-1 Storage System

Represents information about the storage set, including the number of physical devices, the number of logical devices, the state of the storage system, and the operating status.



2-10-2 Controllers

Use this page to view controller information / actual hard disks / logical disk arrays / and provided features.



SaveTTYLog:

- Download TTY logs.

Foreign Configuration

Foreign configuration provides the following three functions, namely scan / import / clear.

- **Scan:** Finding a drive with an external configuration.
- **Import:** You can synchronize the RAID information in the hard disk to the RAID card.
- **Clear:** Clear the foreign configuration in the hard disk.

Patrol Read

Check your system for hard drive errors that may cause drive failure.
It is only run for all RAID levels or for all hot spare drives.

Procedures:

Create Volume

Press the Create Volume menu and a dialog will pop up to guide you through the three steps of creating a disk array. You can press Cancel at any step to leave. If there are currently no physical hard
disks available for creation, the alert info dialog will show up.

- **Step 1:** Set RAID level and select available drive disks.
- **Step 2:** Set the parameter volume disk name/size/strip size/disk cache policy/access policy/initial state.
- **Step 3:** Confirm the parameter values of the disk array to be created. If you want to modify, press the back button to modify the parameters.

SaveTTYLog

Click on the SaveTTYLog button to download TTY logs.

Foreign Configuration

- **Scan:** Click this option to start scanning any foreign configuration on the physical hard disk.
- **Import:** If an existing hard drive has a foreign configuration, it can be imported into a RAID controller.
- **Clear:** Click this option to clear the external configuration of the existing hard drive.

Patrol Read:

Patrol Read is composed of two small functions: Start and Stop.

- **Start:** Click Start of Patrol Read and click OK in the dialog box, will to start Patrol Read on the physical hard disk. If the hard disk meets this function, the Background Tasks area will be displayed, and the progress of the inspection on the hard disk will be displayed.
- **Stop:** The Stop function only works if Patrol Read has started. Click Stop to cancel the Patrol Read function of the hard disk.

2-10-3 Event Log

This page uses page navigation to display event log messages.



SeqNo	Level	Event ID	Time	Description
5047	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	PD 07(e0xfc/s2) Inquiry info: Info- ATA SAMSUNG MZ7LH1T9 NY0R639791 1 TB
5048	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 08(e0xfc/s3)
5049	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 08(e0xfc/s3) Info: enclPd=fc, scsiType=0, portMap=00, sasAddr=300062b207c3cec4,0000000000000000
5050	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	PD 08(e0xfc/s3) Inquiry info: Info- ATA SAMSUNG MZ7LH1T9 NY0R639793 1 TB
5051	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 09(e0xfc/s1)
5052	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 09(e0xfc/s1) Info: enclPd=fc, scsiType=0, portMap=20, sasAddr=0000000000000000,300062b207c3cec6
5053	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	PD 09(e0xfc/s1) Inquiry info: Info- ATA SAMSUNG MZ7LH1T9 NY0R639792 1 TB
5054	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 0a(e0xfc/s0)
5055	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 0a(e0xfc/s0) Info: enclPd=fc, scsiType=0, portMap=03, sasAddr=300062b207c3cec7,0000000000000000
5056	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	PD 0a(e0xfc/s0) Inquiry info: Info- ATA SAMSUNG MZ7LH1T9 NY0R639783 1 TB
5057	Information	499	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:14 (h:m:s)	Boot Device reset, setting target ID as invalid
5058	Information	44	10/11/2023 ; 7:26:6	Time established as 10/11/23 7:26:06; (73 seconds since power on)
5059	Information	389	10/11/2023 ; 7:26:34	Host driver is loaded and operational
5060	Information	0	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:8 (h:m:s)	Firmware initialization started (PCI ID 10e2/1000/4000/1000)
5061	Information	1	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:8 (h:m:s)	Firmware version 5.120.02-2904
5062	Information	141	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:11 (h:m:s)	Battery Present
5063	Information	261	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:11 (h:m:s)	Package version 52.12.0-3026
5064	Information	266	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:11 (h:m:s)	Board Revision 00002
5065	Information	242	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:44 (h:m:s)	Battery charge complete
5066	Information	149	Time elapsed since power on : 0 years, 0 months, 0 days: 0:0:44 (h:m:s)	Battery temperature is normal
5067	Information	167	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Enclosure PD fa(c None/p1) communication restored
5068	Information	167	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Enclosure PD fc(c None/p1) communication restored
5069	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: Encl PD fa
5070	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD fa(c None/p1) Info: enclPd=fa, scsiType=d, portMap=00, sasAddr=300162b207c3cec8,0000000000000000
5071	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Encl PD fa Inquiry info: Info- BROA VirtualSES 0 GB
5072	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: Encl PD fc
5073	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD fc(c None/p1) Info: enclPd=fc, scsiType=d, portMap=00, sasAddr=300162b207c3cec0,0000000000000000
5074	Information	547	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Encl PD fc Inquiry info: Info- BROA VirtualSES 0 GB
5075	Information	91	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 07(e0xfc/s2)
5076	Information	247	Time elapsed since power on : 0 years, 0 months, 0 days: 0:1:5 (h:m:s)	Inserted: PD 07(e0xfc/s2) Info: enclPd=fc, scsiType=0, portMap=01, sasAddr=300062b207c3cec5,0000000000000000

Events Log

The event log is composed of the following 5 materials.

- **SeqNo:** Event log sequence number.
- **Level:** Type of Event log, Information, Error ...etc.
- **Event ID:** Event ID of Event log.
- **Time:** Time when the event log was generated.
- **Description:** Event log detailed description.

Patrol Read:

Patrol Read is composed of two small functions: Start and Stop.

- **Start:** Click Start of Patrol Read and click OK in the dialog box, will to start Patrol Read on the physical hard disk. If the hard disk meets this function, the Background Tasks area will be displayed, and the progress of the inspection on the hard disk will be displayed.
- **Stop:** The Stop function only works if Patrol Read has started. Click Stop to cancel the Patrol Read function of the hard disk.

Appendix

3-1 Appendix A - Assertion Condition (BIT EVENT) References

3-1-1 Sensor type: Temperature, Voltage, Current, Fan

bit0. Lower Non-critical - going low
bit1. Lower Non-critical - going high
bit2. Lower Critical - going low
bit3. Lower Critical - going high
bit4. Lower Non-recoverable - going low
bit5. Lower Non-recoverable - going high
bit6. Upper Non-critical - going low
bit7. Upper Non-critical - going high
bit8. Upper Critical - going low
bit9. Upper Critical - going high
bit10. Upper Non-recoverable - going low
bit11. Upper Non-recoverable - going high
To open the Overview page, click **Overview** from the menu bar. It displays the following:

3-1-2 Sensor type: Physical Security

bit0. General Chassis Intrusion
bit1. Drive Bay intrusion
bit2. I/O Card area intrusion
bit3. Processor area intrusion
bit4. LAN Leash Lost (system is unplugged from LAN)
bit5. Unauthorized dock
bit6. FAN area intrusion

3-1-3 Sensor type: Processor

bit0. IERR
bit1. Thermal Trip
bit2. FRB1/BIST failure
bit3. FRB2/Hang in POST failure

bit4. FRB3/Processor Startup/Initialization failure (CPU didn't start)
bit5. Configuration Error
bit6. SM BIOS 'Uncorrectable CPU-complex Error'
bit7. Processor Presence detected
bit8. Processor disabled
bit9. Terminator Presence Detected
bit10. Processor Automatically Throttled
bit11. Machine Check Exception (Uncorrectable)
bit12. Correctable Machine Check Error

3-1-4 Sensor type: Power supply

bit0. Presence detected
bit1. Power Supply Failure detected
bit2. Predictive Failure
bit3. Power Supply input lost (AC/DC)[2]
bit4. Power Supply input lost or out-of-range
bit5. Power Supply input out-of-range, but present
bit6. Configuration error
bit7. Power Supply Inactive (in standby state)

3-1-5 Sensor type: Other Units-based Sensor

bit0. Lower Non-critical - going low
bit1. Lower Non-critical - going high
bit2. Lower Critical - going low
bit3. Lower Critical - going high
bit4. Lower Non-recoverable - going low
bit5. Lower Non-recoverable - going high
bit6. Upper Non-critical - going low
bit7. Upper Non-critical - going high
bit8. Upper Critical - going low
bit9. Upper Critical - going high
bit10. Upper Non-recoverable - going low
bit11. Upper Non-recoverable - going high

3-1-6 Sensor type: Memory

bit0. Correctable ECC / other correctable memory error
bit1. Uncorrectable ECC / other uncorrectable memory error
bit2. Parity
bit3. Memory Scrub Failed (stuck bit)
bit4. Memory Device Disabled
bit5. Correctable ECC / other correctable memory error logging limit reached
bit6. Presence detected
bit7. Configuration error
bit8. Spare
bit9. Memory Automatically Throttled
bit10. Critical Overtemperature

3-1-7 Sensor type: Event Logging Disabled

bit0. Correctable Memory Error Logging Disabled
bit1. Event 'Type' Logging Disabled
bit2. Log Area Reset/Cleared
bit3. All Event Logging Disabled
bit4. SEL Full (SEL is in circular mode, so this event will not be triggered.)

bit5. SEL Almost Full (SEL is in circular mode, so this event will not be triggered.)
bit6. Correctable Machine Check Error Logging Disabled

3-1-8 Sensor type:Critical Interupt

bit0. Front Panel NMI / Diagnostic Interrupt
bit1. Bus Timeout
bit2. I/O channel check NMI
bit3. Software NMI
bit4. PCI PERR
bit5. PCI SERR
bit6. EISA Fail Safe Timeout
bit7. Bus Correctable Error
bit8. Bus Uncorrectable Error
bit9. Fatal NMI (port 61h, bit 7)
bit10. Bus Fatal Error
bit11. Bus Degraded (bus operating in a degraded performance state)

Designed by

