GIGABYTE™

Gigabyte Server Management Console

User's Guide

Rev. 1.0

Copyright

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 GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: http://reseller.b2b.gigabyte.com

For further technical assistance, please contact your GIGABYTE representative or visit https://esupport.gigabyte.com/ to create a new support ticket

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

Table of Contents

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

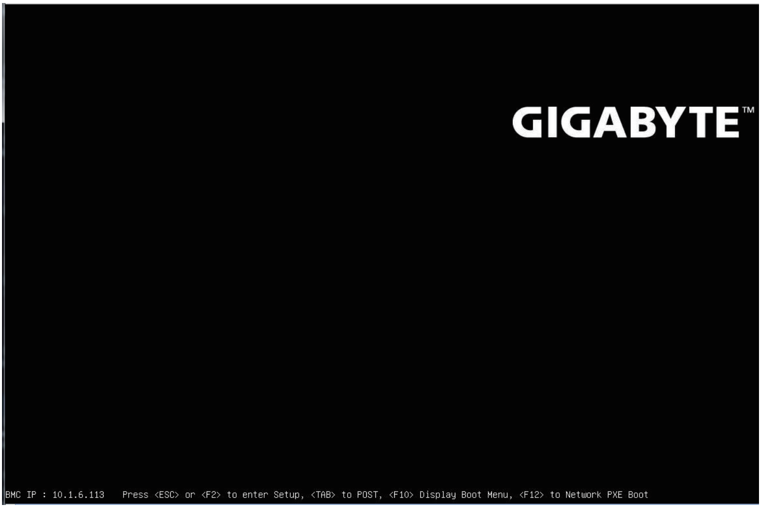
- Chrome latest version.
- IE 11 and above.
- Firefox (with limited support).

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

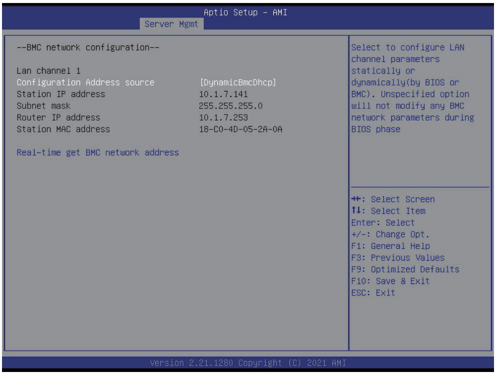
Follow the instruction to enable the console redirection function.

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



```
BMC IP : 10.1.6.113    Press <ESC> or <F2> to enter Setup, <TAB> to POST, <F10> Display Boot Menu, <F12> to Network PXE Boot
```

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.

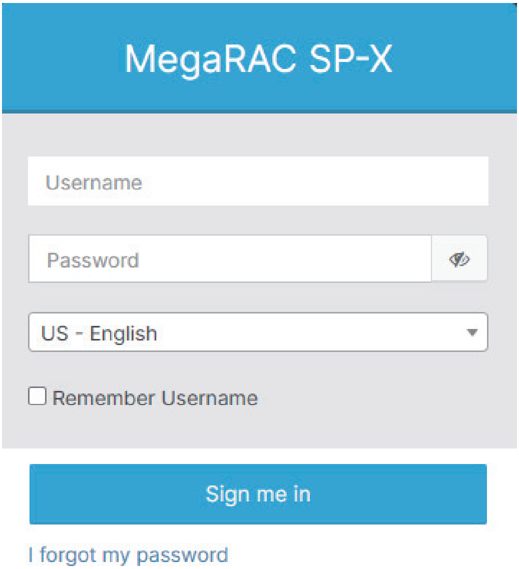


```
                              Aptio Setup - AMI
                        Server Mgmt
 --BMC network configuration--                          Select to configure LAN
                                                        channel parameters
 Lan channel 1                                          statically or
 Configuration Address source      [DynamicBmcDhcp]     dynamically(by BIOS or
 Station IP address                10.1.7.141           BMC). Unspecified option
 Subnet mask                       255.255.255.0        will not modify any BMC
 Router IP address                 10.1.7.253           network parameters during
 Station MAC address               18-C0-4D-05-2A-0A    BIOS phase

 Real-time get BMC network address
                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/-: Change Opt.
                                                        F1: General Help
                                                        F3: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Exit
                                                        ESC: Exit

                    Version 2.21.1280 Copyright (C) 2021 AMI
```

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.

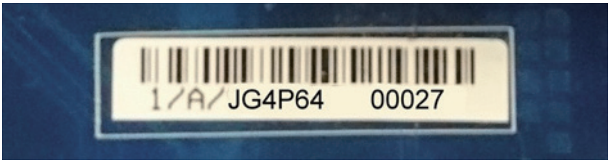


The fields are explained as follows:
For basic login to the MegaRAC UI, use the following login:

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

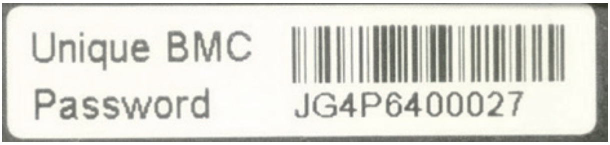
NOTE!
If your motherboard / server version is older than G9 (upgrade version), then use the following login:
Username: admin
Password: password

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



1/A/JG4P64 00027

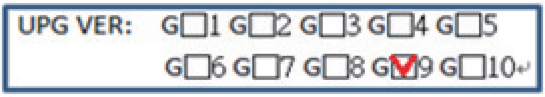
GIGABYTE will also affix new stickers that display the unique BMC password (example below) to both the product box (packaging) and to the CPU cover (for motherboards sold separately) or the server chassis.



Unique BMC Password JG4P6400027

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.



UPG VER: G□1 G□2 G□3 G□4 G□5
G□6 G□7 G□8 G☑9 G□10

Remember Username: Check this option to remember your login credentials.
Sign me in: After entering the required credentials, click the **Sign me in** to login to GUI.
I forgot my 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.

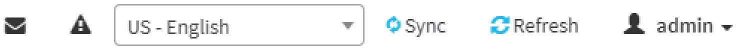
1-3-1 Required Browser Settings:

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.



User Information

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:

Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are five kinds of privileges.

User: Only valid commands are allowed.

Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.

Administrator: All BMC commands are allowed.

No Access: Login access denied.

OEM: All OEM commands are allowed.

Refresh: Click the icon to reload the current page.

Sync: Click the icon to synchronize with Latest Sensor and Event Log updates.

US - English: Click to select the language of the Web GUI.

Warning: Click to view the warning messages.

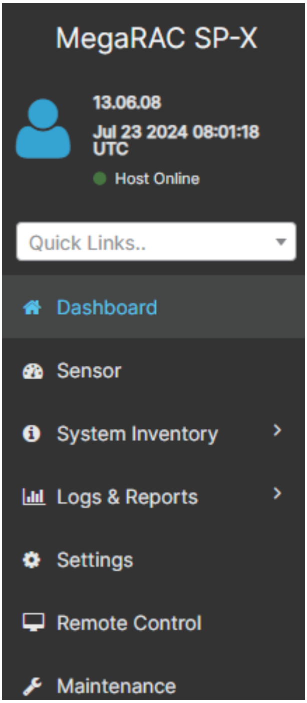
Notification: Click the icon to view the notification messages.

1-5 Help

Help - The Help icon (?) is Located at the top right of the each page in Web GUI. Click this help icon to view more detailed field descriptions.

1-6 Menu Bar

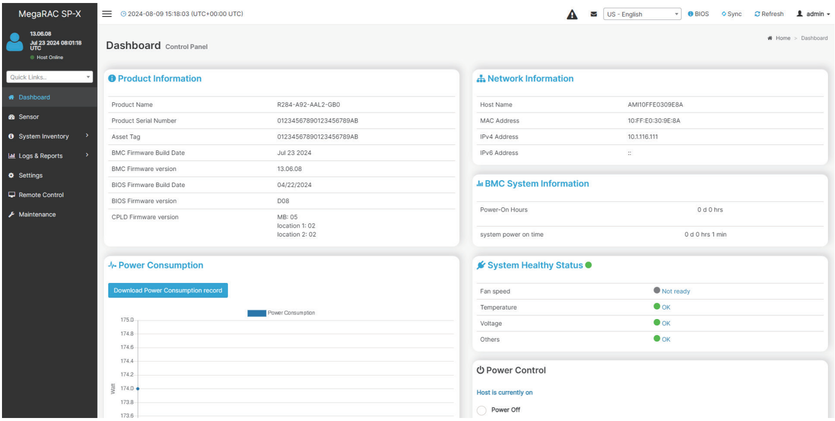
The menu bar displays the following:



Chapter 2 Enter Gigabyte Management Console

2-1 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 Control Panel

Product Information

Product Name	R284-A92-AAL2-GB0
Product Serial Number	01234567890123456789AB
Asset Tag	01234567890123456789AB
BMC Firmware Build Date	Jul 23 2024
BMC Firmware version	13.06.08
BIOS Firmware Build Date	04/22/2024
BIOS Firmware version	D08
CPLD Firmware version	MB: 05 location 1: 02 location 2: 02

Network Information

Host Name	AMI10FFE0309E8A
MAC Address	10:FF:E0:30:9E:8A
IPv4 Address	10.1.116.111
IPv6 Address	::

BMC System Information

Power-On Hours	0 d 0 hrs
system power on time	0 d 0 hrs 1 min

Power Consumption

System Healthy Status ●

Fan speed	● Not ready
Temperature	● OK
Voltage	● OK
Others	● OK

Power Control

Host is currently on

○ Power Off

Dashboard

A brief description of the Dashboard page is given below.

Product Information

Displays the technical information for the system.

Power Consumption

Displays the current power consumption information.

Network Information

Displays the network information of the system.

BMC System Information

Displays the system BMC information of the system.

System Health Status

Displays the summary of hardware device sensors. If the device is detected, the screen will display 'OK' or 'NG' according to the hardware status. If the device is not detected, it will display 'Not Ready', usually indicating that the system is powered off.

Power Control

Allows you to view and control the power of your server. The various options of Power Control are given below:

- **Power Off**: To immediately power off the server.
- **Power On**: To power on the server.
- **Power Cycle**: This option will first power off, and then reboot the system (cold boot).
- **Hard Reset**: This option will reboot the system without powering off (warm boot)

BIOS POST CODE

Click the blue tab to download POST code record.

Task Summary

Displays the task summary schedule information.

Remote KVM

Click **Refresh** to see the screen of the remote system.

IPMI Event Log

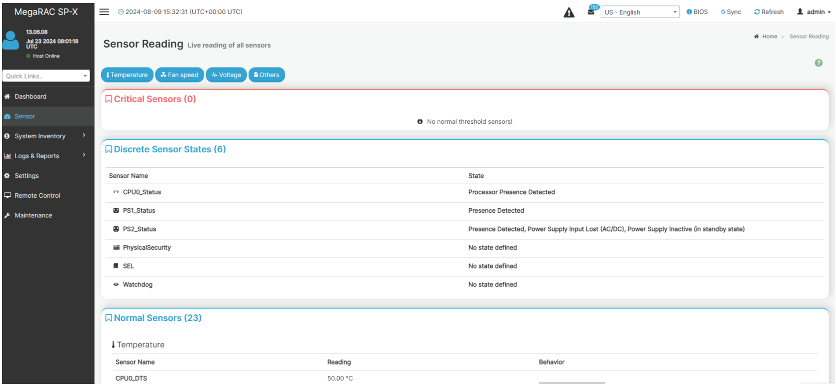
Displays the list of event logs occurred by the different sensors on this system.

2-2 Sensor

The Sensor Readings page displays all the sensor related information.
To open the Sensor Readings page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

The sensors are sorted through temperature, fan speed, voltage, and other sensors. The buttons at the top of the page are used to control the display of information for each category.

A sample screenshot of Sensor Readings page is shown below.



Sensor Reading Live reading of all sensors

Critical Sensors (0)

No normal threshold sensors!

Discrete Sensor States (6)

Sensor Name	State
CPU0_Status	Processor Presence Detected
PS1_Status	Presence Detected
PS2_Status	Presence Detected, Power Supply Input Lost (AC/DC), Power Supply Inactive (in standby state)
PhysicalSecurity	No state defined
SEL	No state defined
Watchdog	No state defined

Normal Sensors (23)

Temperature

Sensor Name	Reading	Behavior
CPU0_DTS	50.00 °C	

The Sensor Readings page contains the following information:

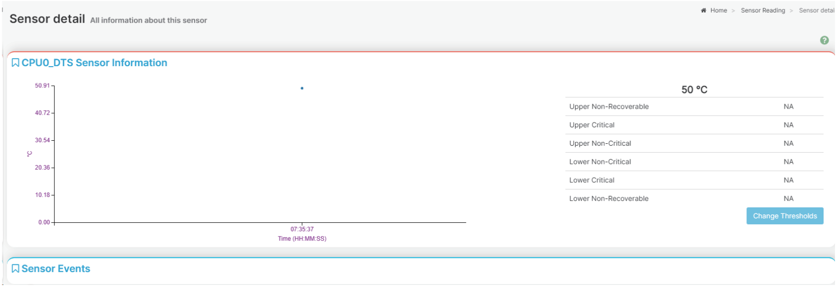
In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior will be appeared, else you can choose the sensor type that you want to display from the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.
Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

2-2-1 Sensor Detail

Select a particular sensor from the Critical Sensor or Normal Sensor lists. The Sensor Information as Live Widget and Thresholds for the selected sensor will be displayed as shown below.

Note: For Illustrative Purpose, a sample screenshot of Sensor detail page with Change Thresholds option is shown and explained below.



Sensor detail All information about this sensor

Home > Sensor Reading > Sensor detai

CPU0_DTS Sensor Information

50 °C

Upper Non-Recoverable	NA
Upper Critical	NA
Upper Non-Critical	NA
Lower Non-Critical	NA
Lower Critical	NA
Lower Non-Recoverable	NA

Sensor Events

Note: Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live data of the last widget that is kept opened.

For the selected sensor, this widget gives a dynamic representation of the readings for the sensor.

There are six types of thresholds:

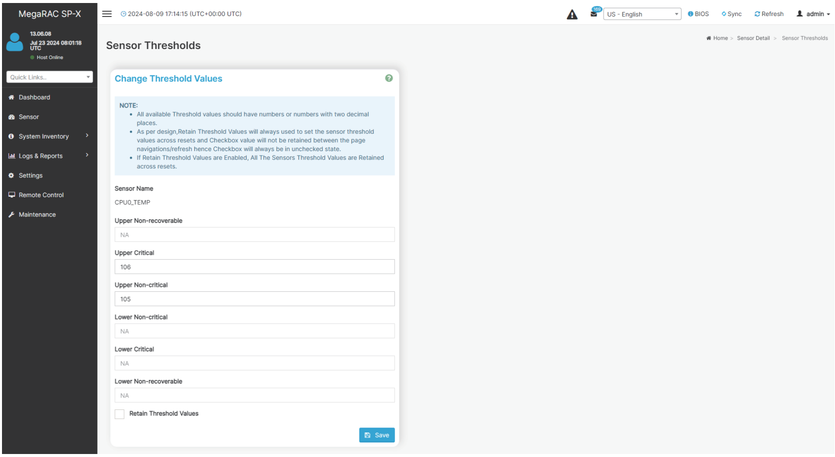
- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

The threshold states could be Lower Non-critical - going low, Lower Non-critical - going high, Lower Critical - going low, Lower Critical - going high, Lower Non-recoverable - going low, Lower Non-recoverable - going high, Upper Non-critical - going low, Upper Non-critical - going high, Upper Critical - going low, Upper Critical - going high, Upper Non-recoverable - going low, Upper Non-recoverable - going high.

A graphical view of these events (Number of Entries vs. Thresholds) can be viewed as shown in the Sensor Readings page screenshot.

2-2-3 Threshold Settings

Click Change Thresholds to configure threshold settings. A sample screenshot is given below.



Sensor Thresholds

Change Threshold Values

NOTE:

- All available Threshold values should have numbers or numbers with two decimal places.
- As per design,Retain Threshold Values will always used to set the sensor threshold values across resets and Checkbox value will not be retained between the page navigations/refresh hence Checkbox will always be in unchecked state.
- If Retain Threshold Values are Enabled, All The Sensors Threshold Values are Retained across resets.

Sensor Name: CPU0_TEMP

Upper Non-recoverable: NA

Upper Critical: 106

Upper Non-critical: 105

Lower Non-critical: NA

Lower Critical: NA

Lower Non-recoverable: NA

☐ Retain Threshold Values

Save

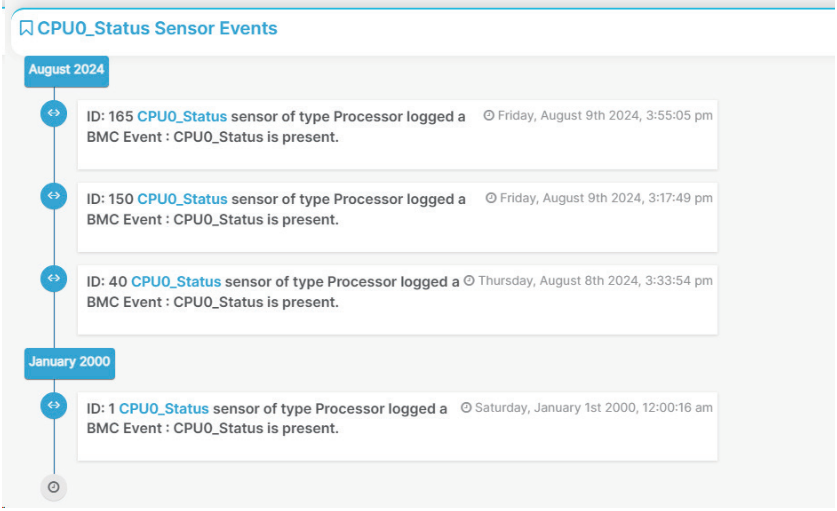
Enter the Threshold values and click **Save** to configure the threshold values.

Note: The Threshold Settings will be enabled only for administrator or operator privilege users. For other users the Threshold Settings option will be disabled, and they can’t access to perform this action.

Note: The Threshold Settings must follow the rule: UNR > UC > UNC > LNC > LC > LNR.

2-2-2 Sensor Events

The Sensor Events page displays information about events that have triggered the system's sensor. A sample screenshot of Sensor Events page is shown below.



CPU0_Status Sensor Events

August 2024

ID: 165 CPU0_Status sensor of type Processor logged a BMC Event : CPU0_Status is present. Friday, August 9th 2024, 3:55:05 pm

ID: 150 CPU0_Status sensor of type Processor logged a BMC Event : CPU0_Status is present. Friday, August 9th 2024, 3:17:49 pm

ID: 40 CPU0_Status sensor of type Processor logged a BMC Event : CPU0_Status is present. Thursday, August 8th 2024, 3:33:54 pm

January 2000

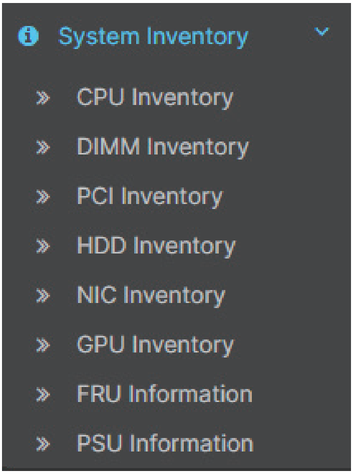
ID: 1 CPU0_Status sensor of type Processor logged a BMC Event : CPU0_Status is present. Saturday, January 1st 2000, 12:00:16 am

2-3 System Inventory

The System Inventory page displays the following information:

- CPU Inventory
- DIMM Inventory
- PCI Inventory
- HDD Inventory
- NIC Inventory
- GPU Inventory
- FRU Inventory
- PSU Inventory

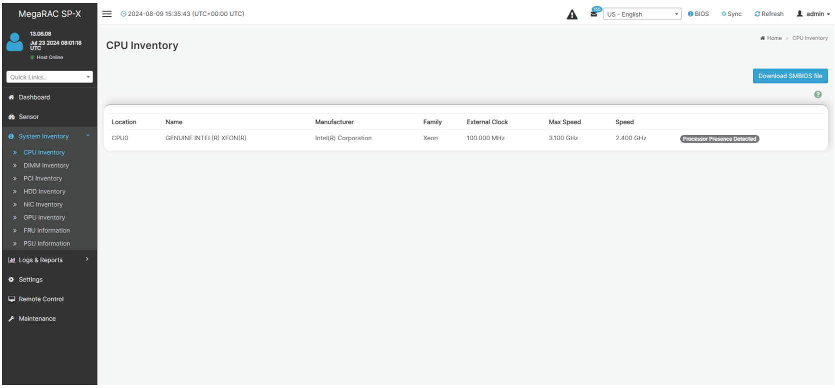
A screenshot displaying the menu items under System Inventory is shown below.



A detailed description of System Inventory is given below.

2-3-1 CPU Inventory

This page displays all detected CPUs on this device. Select one CPU to see the details of that entry. Click Download **SMBIOS file** to download the SMBIOS file.

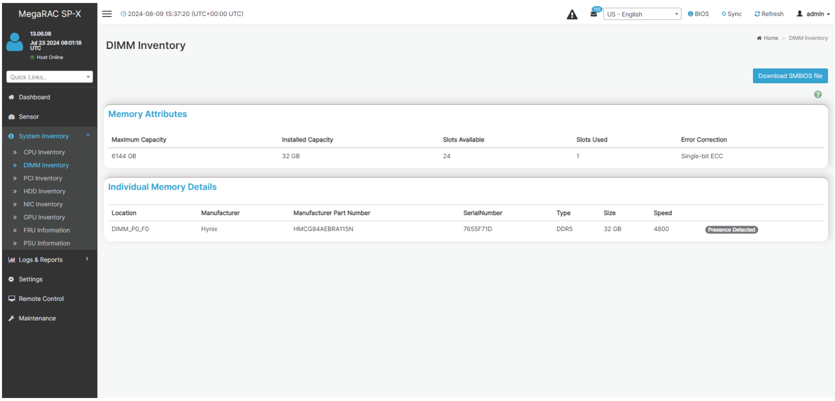


CPU Inventory

Location	Name	Manufacturer	Family	External Clock	Max Speed	Speed	
CPU0	GENUINE INTEL(R) XEON(R)	Intel(R) Corporation	Xeon	100.000 MHz	3.100 GHz	2.400 GHz	Processor Presence Detected

2-3-2 DIMM Inventory

This page displays all detected DIMMs on this device. It allows you to see memory attributes, individual memory details. Click **Download SMBIOS file** to download the SMBIOS file.



DIMM Inventory

Memory Attributes

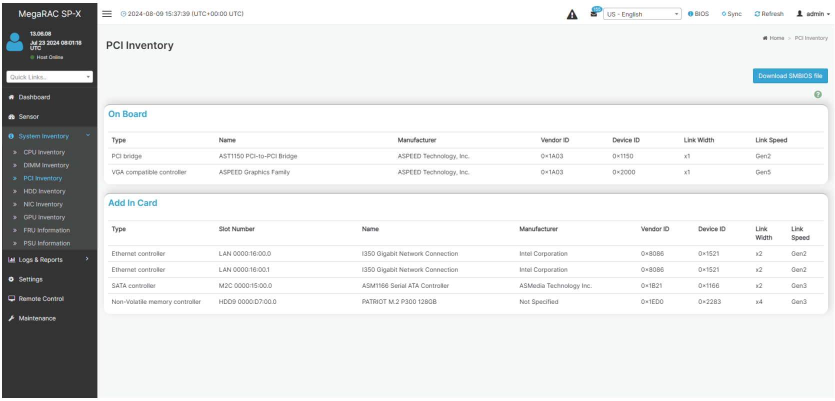
Maximum Capacity	Installed Capacity	Slots Available	Slots Used	Error Correction
6144 GB	32 GB	24	1	Single-bit ECC

Individual Memory Details

Location	Manufacturer	Manufacturer Part Number	SerialNumber	Type	Size	Speed	
DIMM_P0_F0	Hynix	HMCG84AEBRA115N	7655F71D	DDR5	32 GB	4800	Presence Detected

2-3-3 PCI Inventory

This page displays all detected PCI cards on this device. It allows you to see on-board PCI cards, add-on PCI cards. Click **Download SMBIOS file** to download the SMBIOS file.



PCI Inventory

On Board

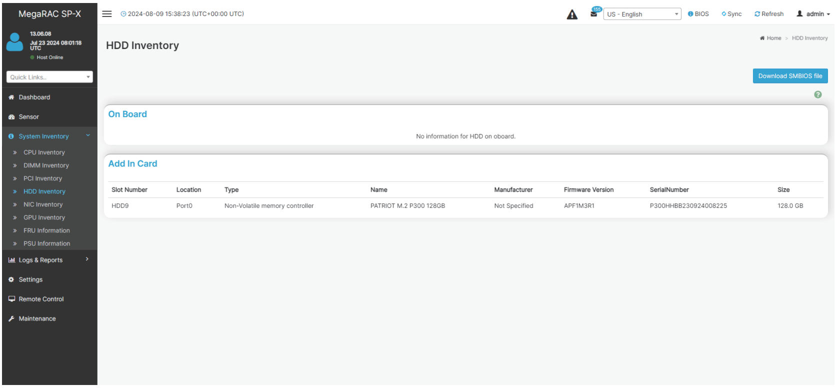
Type	Name	Manufacturer	Vendor ID	Device ID	Link Width	Link Speed
PCI bridge	AST1150 PCI-to-PCI Bridge	ASPEED Technology, Inc.	0×1A03	0×1150	x1	Gen2
VGA compatible controller	ASPEED Graphics Family	ASPEED Technology, Inc.	0×1A03	0×2000	x1	Gen5

Add In Card

Type	Slot Number	Name	Manufacturer	Vendor ID	Device ID	Link Width	Link Speed
Ethernet controller	LAN 0000:16:00.0	I350 Gigabit Network Connection	Intel Corporation	0×8086	0×1521	x2	Gen2
Ethernet controller	LAN 0000:16:00.1	I350 Gigabit Network Connection	Intel Corporation	0×8086	0×1521	x2	Gen2
SATA controller	M2C 0000:15:00.0	ASM1166 Serial ATA Controller	ASMedia Technology Inc.	0×1B21	0×1166	x2	Gen3
Non-Volatile memory controller	HDD9 0000:D7:00.0	PATRIOT M.2 P300 128GB	Not Specified	0×1ED0	0×2283	x4	Gen3

2-3-4 HDD Inventory

This page displays all detected HDDs on this device. It allows you to see on-board HDDs, add-on HDDs. Click **Download SMBIOS file** to download the SMBIOS file.



HDD Inventory

On Board

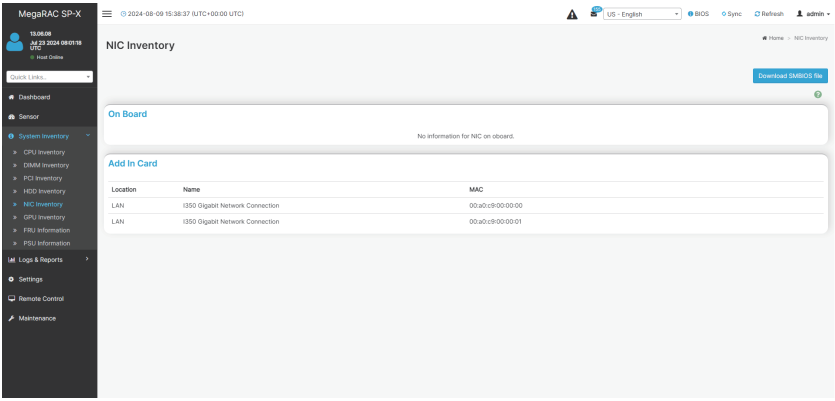
No information for HDD on oboard.

Add In Card

Slot Number	Location	Type	Name	Manufacturer	Firmware Version	SerialNumber	Size
HDD9	Port0	Non-Volatile memory controller	PATRIOT M.2 P300 128GB	Not Specified	APF1M3R1	P300HHBB230924008225	128.0 GB

2-3-5 NIC Inventory

This page displays all detected NICs on this device. It allows you to on-board NICs, add-on NICs. Click **Download SMBIOS file** to download the SMBIOS file.



NIC Inventory

On Board

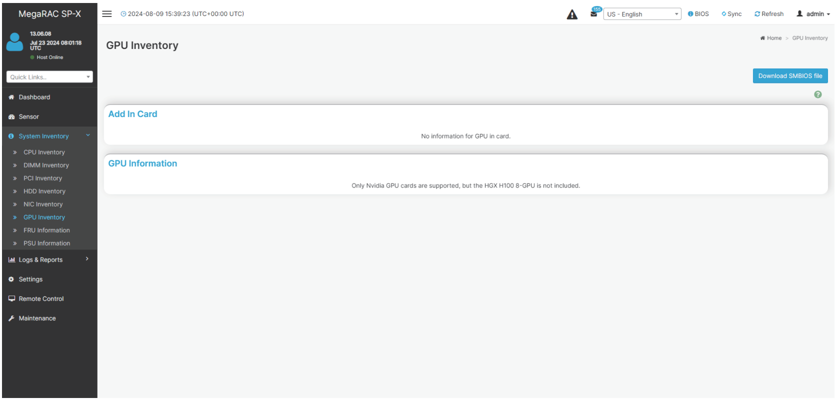
No information for NIC on oboard.

Add In Card

Location	Name	MAC
LAN	I350 Gigabit Network Connection	00:a0:c9:00:00:00
LAN	I350 Gigabit Network Connection	00:a0:c9:00:00:01

2-3-6 GPU Inventory

This page displays all detected GPU cards on this device. It allows you to to see on-board GPU cards, add-on PCI cards. Click **Download SMBIOS file** to download the SMBIOS file.



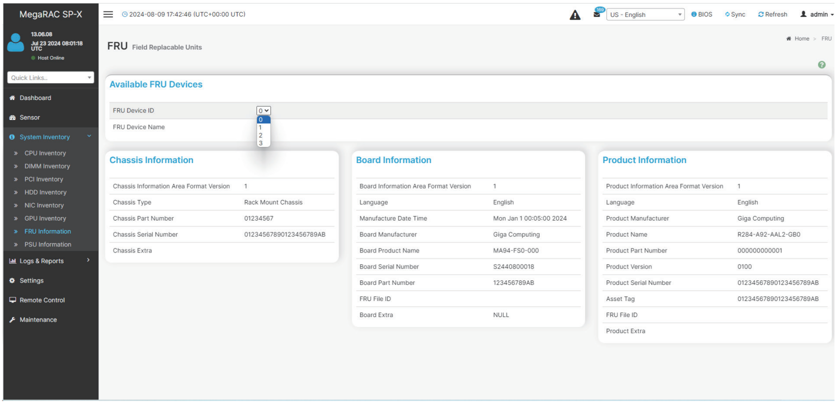
No information for GPU in card.

Only Nvidia GPU cards are supported, but the HGX H100 8-GPU is not included.

2-3-7 FRU Inventory

FRU Inventory page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information Page, click **System Inventory** from the menu bar and select **FRU inventory**. Select a FRU Device ID from the FRU Information section to view the details of the selected device. A screenshot of FRU
Information page is given below.



FRU Field Replacable Units

Available FRU Devices

FRU Device ID	0 0 1 2 3
FRU Device Name	

Chassis Information

Chassis Information Area Format Version	1
Chassis Type	Rack Mount Chassis
Chassis Part Number	01234567
Chassis Serial Number	01234567890123456789AB
Chassis Extra	

Board Information

Board Information Area Format Version	1
Language	English
Manufacture Date Time	Mon Jan 1 00:05:00 2024
Board Manufacturer	Giga Computing
Board Product Name	MA94-FS0-000
Board Serial Number	S2440800018
Board Part Number	123456789AB
FRU File ID	
Board Extra	NULL

Product Information

Product Information Area Format Version	1
Language	English
Product Manufacturer	Giga Computing
Product Name	R284-A92-AAL2-GB0
Product Part Number	000000000001
Product Version	0100
Product Serial Number	01234567890123456789AB
Asset Tag	01234567890123456789AB
FRU File ID	
Product Extra	

The following fields are displayed here for the selected device.

Available FRU Devices

- FRU device ID - Select the device ID from the drop-down list.
  Note: 0/1 is for BMC, the others are for PSU.
- FRU Device Name - The device name of the selected FRU device.

Chassis Information

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

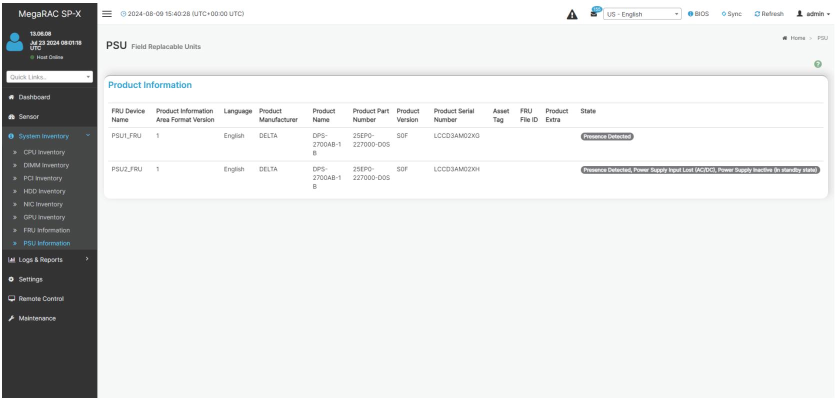
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number

Product Information

- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

2-3-8 PSU Inventory

This page displays information about PSU Information.



PSU Field Replacable Units

Product Information

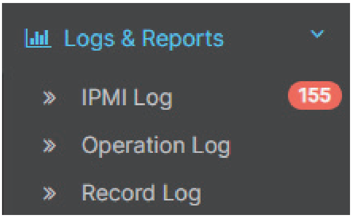
FRU Device Name	Product Information Area Format Version	Language	Product Manufacturer	Product Name	Product Part Number	Product Version	Product Serial Number	Asset Tag	FRU File ID	Product Extra	State
PSU1_FRU	1	English	DELTA	DPS-2700AB-1 B	25EP0-227000-D0S	S0F	LCCD3AM02XG				Presence Detected
PSU2_FRU	1	English	DELTA	DPS-2700AB-1 B	25EP0-227000-D0S	S0F	LCCD3AM02XH				Presence Detected, Power Supply Input Lost (AC/DC), Power Supply Inactive (in standby state)

2-4 Logs & Reports

The Logs & Reports page displays the following information:

- IPMI Event Log
- Operation Log
- Record Log

A screenshot displaying the menu items under Logs & Reports is shown below.



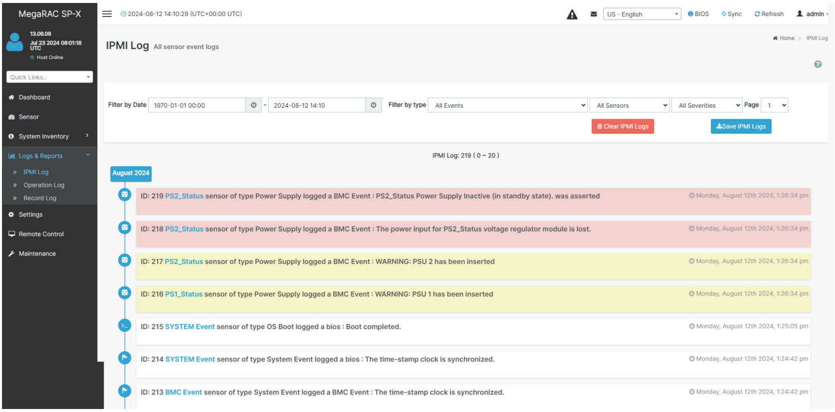
A detailed description of Logs & Reports is given below.

2-4-1 IPMI Log

This page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Logs & Reports > IPMI Log** from the menu bar.

A sample screenshot of Event Log page is shown below.



IPMI Log All sensor event logs

Filter by Date 1970-01-01 00:00 - 2024-08-12 14:10 Filter by type All Events | All Sensors | All Severities | Page 1

IPMI Log: 219 (0 ~ 20)

August 2024

```
ID: 219 PS2_Status sensor of type Power Supply logged a BMC Event : PS2_Status Power Supply Inactive (in standby state). was asserted    Monday, August 12th 2024, 1:26:34 pm
ID: 218 PS2_Status sensor of type Power Supply logged a BMC Event : The power input for PS2_Status voltage regulator module is lost.    Monday, August 12th 2024, 1:26:34 pm
ID: 217 PS2_Status sensor of type Power Supply logged a BMC Event : WARNING: PSU 2 has been inserted    Monday, August 12th 2024, 1:26:34 pm
ID: 216 PS1_Status sensor of type Power Supply logged a BMC Event : WARNING: PSU 1 has been inserted    Monday, August 12th 2024, 1:26:34 pm
ID: 215 SYSTEM Event sensor of type OS Boot logged a bios : Boot completed.    Monday, August 12th 2024, 1:25:05 pm
ID: 214 SYSTEM Event sensor of type System Event logged a bios : The time-stamp clock is synchronized.    Monday, August 12th 2024, 1:24:42 pm
ID: 213 BMC Event sensor of type System Event logged a BMC Event : The time-stamp clock is synchronized.    Monday, August 12th 2024, 1:24:42 pm
```

The Event Log page consists of the following fields:

Filter By Date: Filtering can be done by selecting **Start Date** and **End Date** using **Calendar.**
Note: Date should be in MM/DD/YYYY format. By default, all log time will be displayed in BMC time zone.

Filter By Type: The category could be either All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console Software Events, Terminal Mode Remote Console Software Events, and Event-Only Records.

Note: Once the Filter By Date and Filter type are selected, the list of events will be displayed with the Event ID, Time Stamp, Sensor Type, Sensor Name and Description.

Clear IPMI Logs: Deletes all the IPMI logs.
Save IPMI Logs: Download and save the IPMI logs.

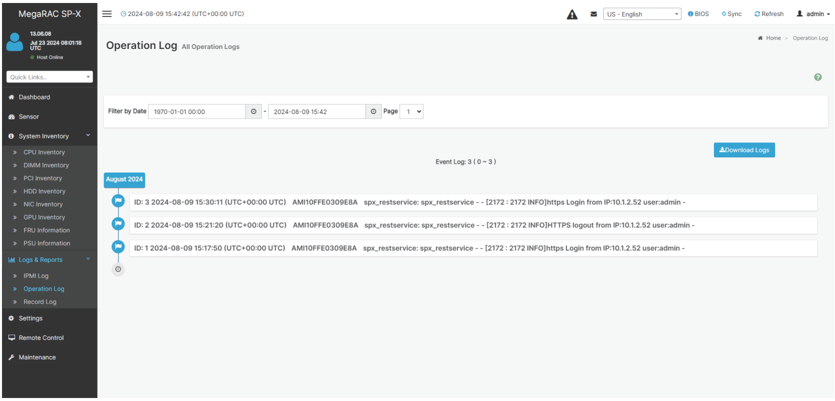
Procedure

1. From the **Filter By Date** field, select the time period by **Start Date** and **End Date** using Calendar for the event categories. The events will be displayed according to the selected date.
2. From the **Filter By Type** field, select the **Type** of the event and **Sensor** and **Severities** to view the events for the date. The events will be displayed based on the selected time period.
3. To clear all events from the list, click **Clear All IPMI Logs**.
4. To download the event logs, click **Download IPMI Logs**.

2-4-2 Operation Log

Operation log displays all the system events occurred in this device that has been already configured.
Note: Logs must be configured under **Settings > Monitoring > Log Settings > Advanced Log Settings** in order to display any entries.

To open the Operation Log page, click **Logs & Reports > Operation Log** from the menu bar.
A sample screenshot of Video Log page is shown below.
Note: For configuration, go to **Settings > Log Settings > Advanced Log Settings**.



Filter by Date 1970-01-01 00:00 - 2024-08-09 15:42 Page 1

Event Log: 3 (0 ~ 3)

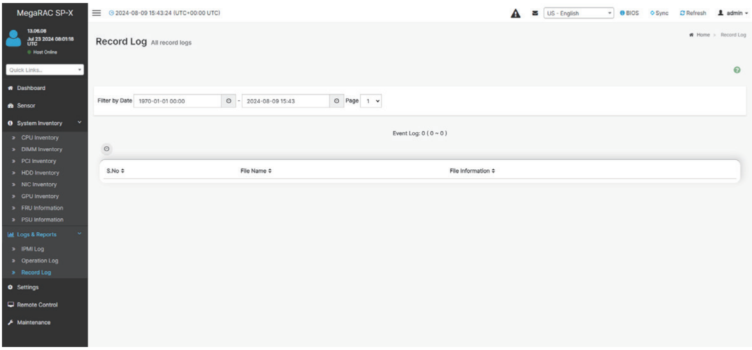
```
ID: 3 2024-08-09 15:30:11 (UTC+00:00 UTC)   AMI10FFE0309E8A   spx_restservice: spx_restservice - - [2172 : 2172 INFO]https Login from IP:10.1.2.52 user:admin -
ID: 2 2024-08-09 15:21:20 (UTC+00:00 UTC)   AMI10FFE0309E8A   spx_restservice: spx_restservice - - [2172 : 2172 INFO]HTTPS logout from IP:10.1.2.52 user:admin -
ID: 1 2024-08-09 15:17:50 (UTC+00:00 UTC)   AMI10FFE0309E8A   spx_restservice: spx_restservice - - [2172 : 2172 INFO]https Login from IP:10.1.2.52 user:admin -
```

Procedure

1. From the **Filter By Date** field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. To download the event logs, click **Download Logs**.

2-4-3 Record Log

To open the Record Log page, click **Logs & Reports > Record Log** from the menu bar.
A sample screenshot of Video Log page is shown below.
Note: Video Trigger Settings should be enabled, to display the Record Log page. Video Trigger Settings can be configured under **Settings > Monitoring > Video Recording > Auto Video Settings > Video Trigger Settings**.



Record Log All record logs

Filter by Date 1970-01-01 00:00 - 2024-08-09 15:43 Page 1

Event Log: 0 (0 ~ 0)

S.No	File Name	File Information

ICON	Description
Download	⬇
Play/Pause	▶ ⏸
Delete	✖

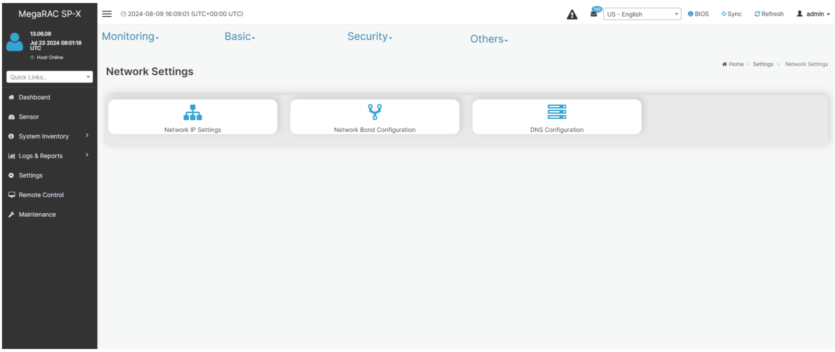
Procedure

Click on the Record Log entry to view the Record.
You can Download, Play/Pause and Delete the video by clicking the respective icons.

Note: Video will be allowed to play/download only if file size is lesser than 40MB. Browsers have various memory restrictions, due to this browser cannot store and process data greater than 40MB (approximately). If file size is greater than 40MB, user will be notified with a message to use Java player Application.

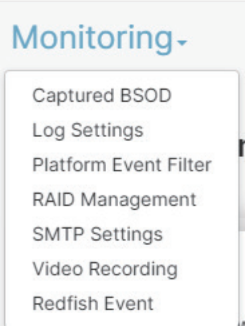
2-5 Settings

This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



A detailed description of the Settings menu is given below.

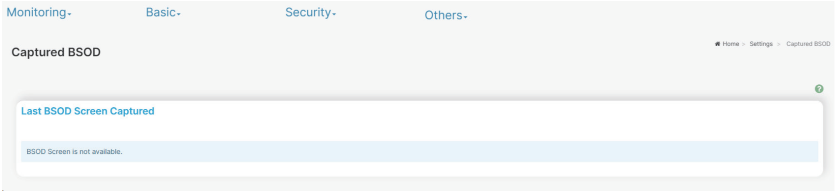
2-5-1 Monitoring



2-5-1-1 Captured BSOD

This menu displays a snapshot of the blue screen captured at the time when/if the host system crashed since the last reboot. A sample screenshot of Captured BSOD is shown below.

Note: KVM service should be enabled to display the BSOD. This can be configured under **Settings > Services > KVM**.

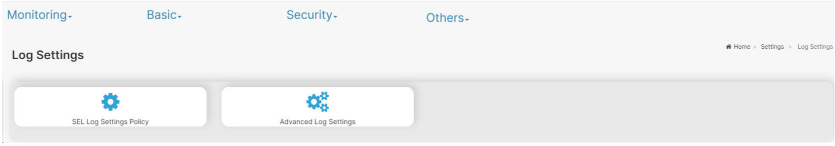


BSOD Screen is not available.

2-5-1-2 Log Settings

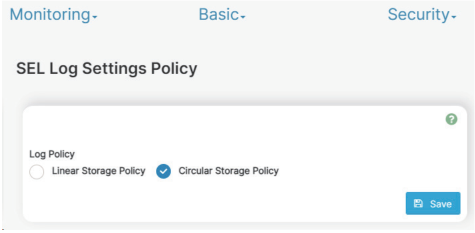
In Web GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.

To open Log Settings page, click **Settings > Monitoring > Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



SEL Log Settings Policy

To open SEL Log Settings Policy page, click **Settings > Monitoring > Log Settings > SEL Log Settings Policy** from the menu bar. The SEL Log Settings Policy page allows users to configure the log policy for the event log. A sample screenshot of SEL Log Settings Policy page is shown below.

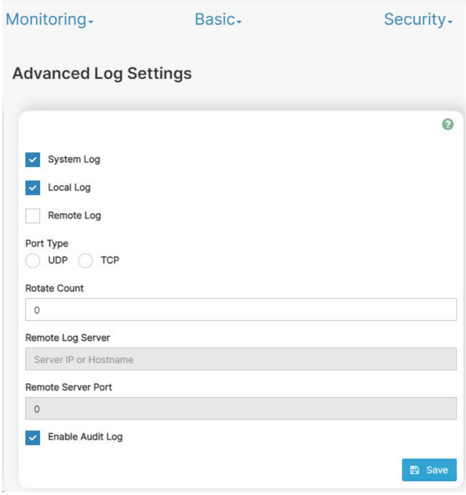


Log Policy

○ Linear Storage Policy ● Circular Storage Policy

Advanced Log Settings

To open Advanced Log Settings page, click **Settings > Log Settings > Advanced Log Settings** from the menu bar. A sample screenshot of Advanced Log Settings page is shown below.



Advanced Log Settings

☑ System Log

☑ Local Log

□ Remote Log

Port Type
○ UDP ○ TCP

Rotate Count
0

Remote Log Server
Server IP or Hostname

Remote Server Port
0

☑ Enable Audit Log

The fields in the Advanced Log Settings page are explained below.
System Log: Check/uncheck to enable/disable the System Logs.
Local Log: Select local log to save the logs locally (BMC).
Note: Local file resides at /var/log/

Remote Log: Select remote log to save the logs in a remote machine.
Port Type: When Remote Log is enabled, user can select either UDP or TCP per requirement.

Rotate Count: Backs up the log information in back up files.
Note: Values supported are 0 and 1.
When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, then old log information gets cleared permanently.
File Size and Rotate Count options will be available only when Local Log is enabled.

Remote Log Server: This field is to specify the remote server address to log the system events.
Note: Server address will support the following:
IPv4 and IPv6 address format.
FQDN (Fully qualified domain name) format.

Remote Server Port: This field is to specify the remote server port to log the system events.
Note: Remote Log Server and Remote Server Port options will be available only when Remote

Log is enabled.
Enable Audit Log: Enables/Disables the audit log.
Save: Saves the current changes.

Procedure

1. In the **System Log** field, enable or disable the option.
2. Select the **Log type**: Local Log or Remote Log.
3. If Local Log is selected, enter the file size in the **File Size** field and rotate count in the **Rotate Count** field.

Note: If Remote Log is selected, the fields file size and rotate count need not be mentioned.

4. If remote log is selected specify the **Port Type**, **Server Address** and **Server Port** of the remote server, where the system events are logged.
5. In the **Audit Log** field, check or uncheck the **Enable** option as needed.
6. Click **Save** to save the changes.

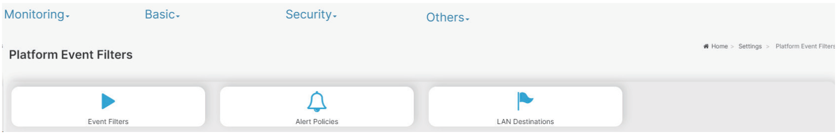
Steps to configure the remote server to enable syslogging
Note: This example uses FC13 as the remote machine to log syslog.
On FC machine, disable the following lines for UDP in /etc/rsyslog.conf.

1. MODLOAD imudp
2. UDPSERVER 514

2-5-1-3 Platform Event Filters

Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.
In Web GUI, the PEF Management allows users to configure the following settings.

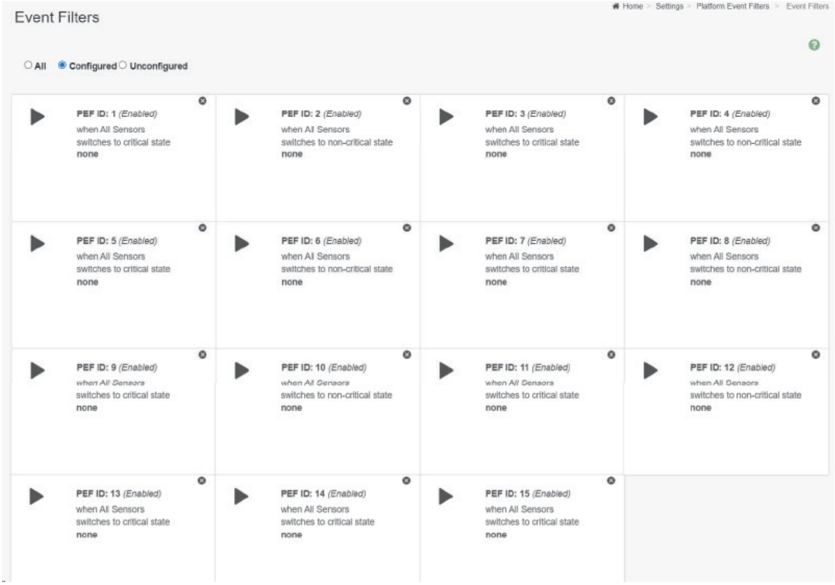
- Event Filters
- Alert Policies
- LAN Destinations



To open PEF Management Settings page, click **Settings > Monitoring > Platform Event Filter** from the menu bar.
Each tab is explained below.

Event Filters

A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use – so this ratio of preconfigured entries to run-time configurable entries can be reallocated if necessary.



Home > Settings > Platform Event Filters > Event Filters

Event Filters

○ All ● Configured ○ Unconfigured

PEF ID: 1 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 2 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 3 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 4 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 5 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 6 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 7 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 8 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 9 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 10 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 11 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 12 *(Enabled)*
when All Sensors
switches to non-critical state
none

PEF ID: 13 *(Enabled)*
when All Sensors
switches to critical state
none

PEF ID: 14 *(Enabled)*
when All Sensors
switches to critical state
none

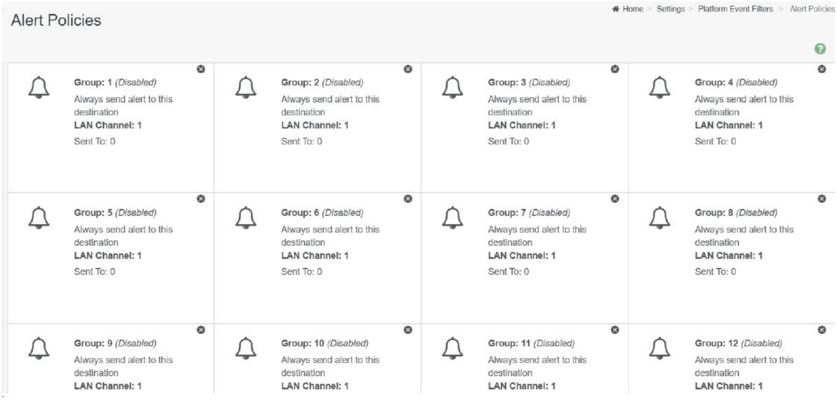
PEF ID: 15 *(Enabled)*
when All Sensors
switches to critical state
none

The fields of Platform Event Filters Tab are explained below.
This page contains pre-configured 40 Events with PEF IDs. Click Delete icon (x) on the top right corner to directly delete an item from the list.

All: Display all the event filters.
Configured: Display the configured event filters.
Unconfigured: Display the unconfigured event filters.

Alert Policies

This page allows user to configure of the Alert Policy for the PEF configuration. You can add, delete, or modify an entry in this page.



Group: 1 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 2 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 3 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 4 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 5 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 6 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 7 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 8 *(Disabled)*
Always send alert to this destination
LAN Channel: 1
Sent To: 0

Group: 9 *(Disabled)*
Always send alert to this destination
LAN Channel: 1

Group: 10 *(Disabled)*
Always send alert to this destination
LAN Channel: 1

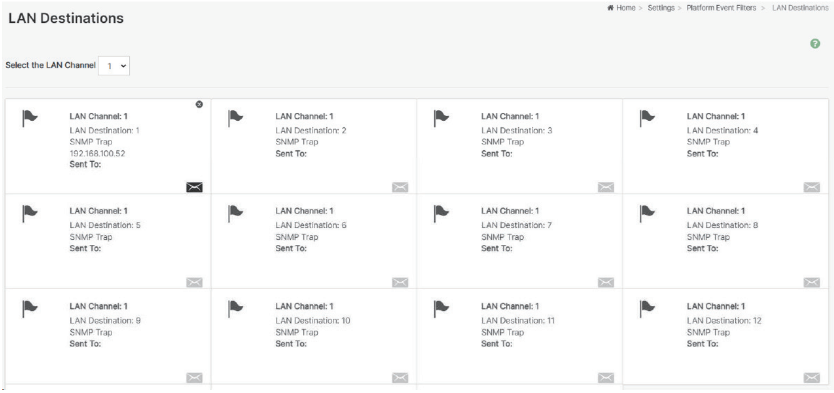
Group: 11 *(Disabled)*
Always send alert to this destination
LAN Channel: 1

Group: 12 *(Disabled)*
Always send alert to this destination
LAN Channel: 1

The fields of Platform Event Filter – Alert Policies section are explained below.
Policy Group Number: Displays the Policy number of the configuration.
Enable this alert: To enable or disable the policy settings.
Policy Action: To choose any one of the Policy set values (0-5) from the list.
0 – Always send alert to this destination.
1 – If alert to previous destination was successful, do not send alert to this destination.
Proceed to next entry in this policy set.
2 – If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.
3 – If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.
4 – If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
LAN Channel: To choose a particular channel from the available channel list.
Destination Selector: To choose a particular destination from the configured destination list.
Note: LAN Destination must be configured – under **Settings -> Monitoring -> Platform Event Filters -> LAN Destinations.**
Event Specific Alert String: To specify an event-specific Alert String.
Alert String Key: To specify which string is to be sent for this Alert Policy entry.
Save: To save the Alert Policies entries.
Delete: To delete the selected configured Alert Policy.

2-5-1-4 LAN Destinations

This page provides function to configure the LAN destination of PEF configuration. A sample screenshot of LAN Destination Page is given below.



LAN Destinations

Home > Settings > Platform Event Filters > LAN Destinations

Select the LAN Channel 1

LAN Channel: 1
LAN Destination: 1
SNMP Trap
192.168.100.52
Sent To:

LAN Channel: 1
LAN Destination: 2
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 3
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 4
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 5
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 6
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 7
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 8
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 9
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 10
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 11
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 12
SNMP Trap
Sent To:

The fields of **Platform Event Filters – LAN Destinations** are explained below.
Select any empty slot to configure LAN Destinations.
Select the LAN Channel: To select the LAN Channel number.
LAN Channel: Displays LAN Channel Number for the selected slot (read-only).
LAN Destination: Displays ID for setting Destination Selector of Alert Policy (read-only).
Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields – SNMP Destination Address, BMC Username, Email subject and Email message needs to be filled. The SMTP server information also must be added – under **Settings -> Monitoring -> SMTP Settings**. For SNMP Trap, only the SNMP Destination Address must be filled.
SNMP Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- Ipv4 address format.
- Ipv6 address format.

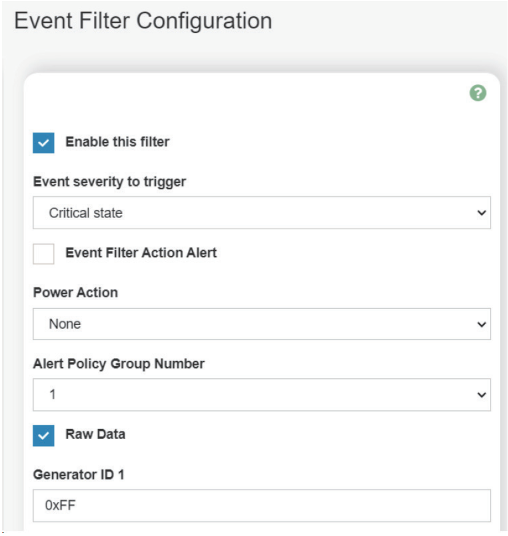
BMC Username: If Destination type is Email Alert, then choose the user to whom the email alert has to be sent.
Email address for the user has to be configured under Settings **->** Security**->** Users Management.
Email Subject & Email Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body. These fields are not applicable for 'AMI-Format' email users.
Note: User should be configured under **Settings -> Security -> Users Management**

Save: To add a new entry to the device. Alternatively, double click on a free slot.
Delete: To delete the selected configured LAN Destination.

Procedure:

To configure Event Filter

1. Click the **Event Filters** section to configure the event filters in the available slots.
2. To Add an Event Filter entry, select a free section to open the Event Filter Entry Page. A sample screenshot of Event Filter Configuration page is shown below.



Event Filter Configuration

☑ Enable this filter

Event severity to trigger: Critical state

□ Event Filter Action Alert

Power Action: None

Alert Policy Group Number: 1

☑ Raw Data

Generator ID 1: 0xFF

In the Event Filter Configuration section,

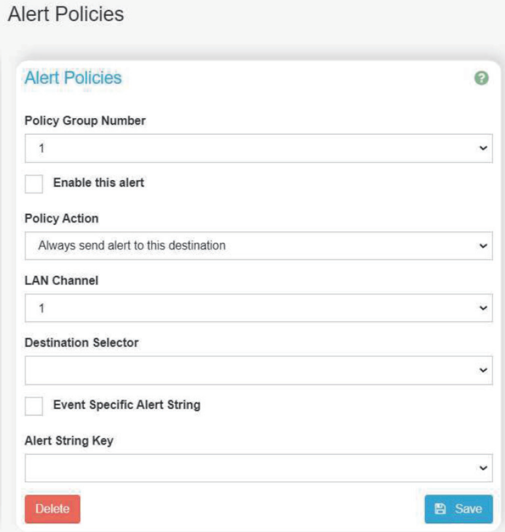
- In **Enable this filter**, check this option to enable the PEF settings.
- In **Event Severity to trigger**, select any one of the Event severities from the list.
- **Event Filter Action Alert**: It is checked by default. This action enables PEF Alert action(read-only).
- Select any one of the **Power Action** either Power down, Power reset or Power cycle from the drop-down list.
- Choose any one of the configured Alert Policy Group Number from the drop-down list.
  Note: Alert Policy has to be configured – under Settings->PEF->Alert Policy.
- Check **Raw Data** option to fill the Generator ID with raw data.
- **Generator ID 1** field is used to give raw generator ID1 data value.
- **Generator ID 2** field is used to give raw generator ID2 data value.
  Note: In RAW data field, specify hexadecimal value prefix with '0x'.

- Select any one of the **Power Action** either Power down, Power reset or Power cycle from the drop-down list.
- In the **Generator Type** section, choose the event generator as Slave Address – if event was generated from IPMB.
- Otherwise as System Software ID – if event was generated from system software.
- In the **Slave Address/Software ID** field, specify corresponding I2C Slave Address or System Software ID.
- Choose the particular **Channel Number** that event message was received over. Or choose ‘0’ if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding IPMB Device LUN if event generated by IPMB.
- Select the **Sensor Type** of sensor that will trigger the event filter action.
- In the **Sensor name** field, choose the particular sensor from the sensor list.
- Choose **Event Option** to be either All Events or Sensor Specific Events.
- **Event Trigger** field is used to give Event/Reading type value.
  Note: Value ranges from 1 to 255.
- **Event Data 1 AND Mask** field is used to indicate wildcarded or compared bits.
  Note: Value ranges from 0 to 255.
- **Event Data 2 AND Mask** field is similar to Event Data 1 AND Mask.
- **Event Data 2 Compare 1 & Event Data 2 Compare 2** fields are similar to **Event Data 1**
- **Compare 1** and **Event Data 1 Compare 2** respectively.
- **Event Data 3 AND Mask** field is similar to **Event Data 1 AND Mask**.
- **Event Data 3 Compare 1** & **Event Data 3 Compare 2** fields are similar to **Event Data 1 Compare 1** and **Event Data 1 Compare 2** respectively.

3. Click **Save** to save the changes and return to event filter list.
4. Click **Delete** to delete the existing filter.

To Configure Alert Policies

1. In the Alert Policies Section, select the slot for which you have to configure the Alert policy. That is, In the Alert Policies page, if you have chosen Alert Policy Group Number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click on the empty slot to open the Alert Policies page as shown in the screenshot below.



Alert Policies

Alert Policies

Policy Group Number

1

□ Enable this alert

Policy Action

Always send alert to this destination

LAN Channel

1

Destination Selector

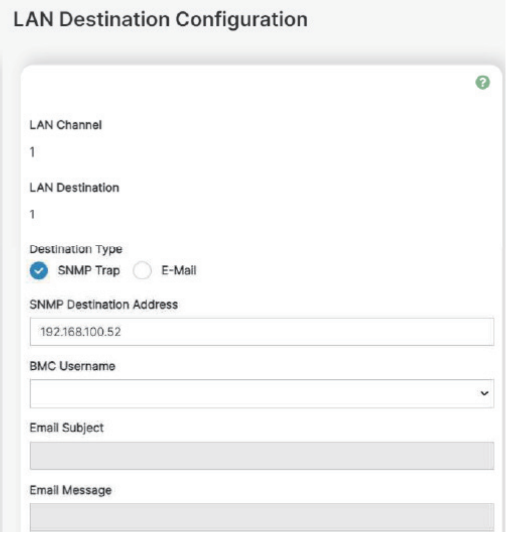
□ Event Specific Alert String

Alert String Key

3. Select Policy Group Number from the drop-down list.
4. Check Enable this alert to enable the policy settings.
5. Choose any of the Policy Action from the list.
6. Choose particular LAN Channel from the available channel list.
7. In the Destination Selector, choose particular destination from the configured destination list.
   Note: LAN Destination must be configured under **Settings -> Monitoring -> Platform Event Filters -> LAN Destinations**. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destinations tab.
8. Enable Event Specific Alert String if the Alert policy entry is Event Specific.
9. In the Alert String Key field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
   Note: Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled/disabled. There is an option to select only the alert string keys, but alert strings have to be configured using IPMI Command (Set PEF Config Parameter “Alert String”).
10. Click Save to save the new alert policy and return to Alert Policy list.
11. Click Delete if you want to delete a configuration.

To configure LAN Destinations

1. In the LAN Destinations section, choose the number of slots to be configured. This should be the same number of slot that you have selected in the Alert Policies – Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policies page of Alert Policies tab, then you have to configure the 4th slot of LAN Destination Page.
2. Select the slot and click on the empty slot. This opens the **LAN Destination entry**.



LAN Destination Configuration

LAN Channel

1

LAN Destination

1

Destination Type

● SNMP Trap ○ E-Mail

SNMP Destination Address

192.168.100.52

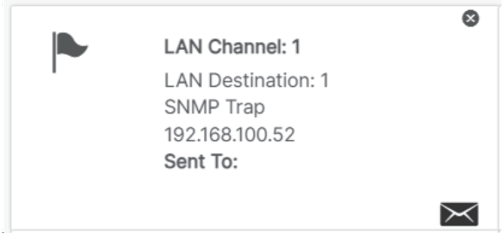
BMC Username

Email Subject

Email Message

3. In the LAN Channel Number field, the LAN Channel Number for the selected slot is displayed and this is a read only field.
4. In the LAN Destination field, the destination for the newly configured entry is displayed and this is a read only field.
5. In the Destination Type field, select the one of the types.
6. In the SNMP Destination Address field, enter the destination address.
   Note: If Destination type is E-mail Alert, then give the e-mail address that will receive the e-mail.
7. If the destination type is Email alert, select the BMC Username from the list of users.
   Note: E-mail address should be configured under Settings -> User Management.
8. In the Email Subject field, enter the subject.
9. In the Email Message field, enter the message.
10. Click Save to save the new LAN destination and return to LAN destination list.
11. Click Delete if you want to delete a configuration.

12. Click Send Test Alert ✉ to send sample alert to configured destination.



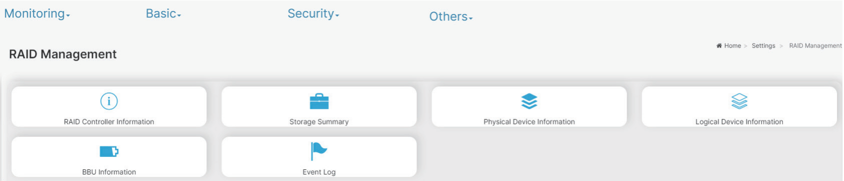
LAN Channel: 1

LAN Destination: 1
SNMP Trap
192.168.100.52
Sent To:

Note: Test alert can send only with enabled SMTP configuration. SMTP support can be enabled under Settings- >SMTP Settings.

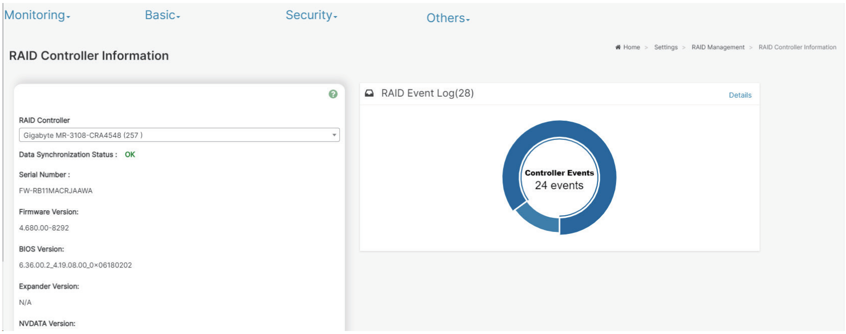
2-5-1-5 RAID Management

To open the RAID Controller Information, click **Settings > Monitoring > RAID Management**. The RAID Management page allows you to view the Storage Summary, RAID Controller information, Physical Device Information, Logical Device Information and Event Log.


Monitoring
Basic
Security
Others
RAID Management
Home > Settings > RAID Management
RAID Controller Information
Storage Summary
Physical Device Information
Logical Device Information
BBU Information
Event Log

RAID Controller Information

To open the RAID Controller Information, click Settings > Monitoring > RAID Management > RAID Controller Information from the menu bar. A sample screenshot of RAID Controller Information section is shown below.



RAID Controller Information

RAID Controller
Gigabyte MR-3108-CRA4548 (257)

Data Synchronization Status : OK

Serial Number :
FW-RB11MACRJAAWA

Firmware Version:
4.680.00-8292

BIOS Version:
6.36.00.2_4.19.08.00_0×06180202

Expander Version:
N/A

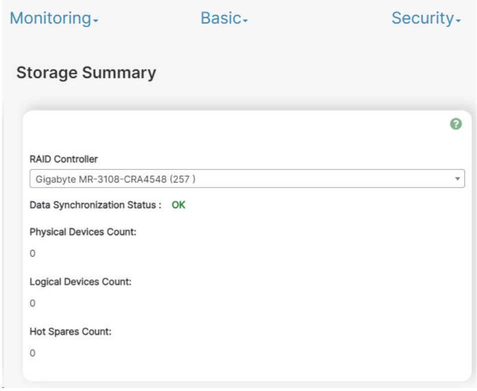
NVDATA Version:

Note: You can get RAID Controller Information only when Host is in Power ON state.

- Serial Number - Displays the Serial number of the RAID Controller.
- Package Version - Displays the Package Version number of the RAID Controller.
- BIOS Version - Displays the BIOS Version number of the RAID Controller.
- Expander Version - Displays the Expander Version number of the RAID Controller.
- NVDATA Version - Displays the NVDATA Version number of the RAID Controller.
- SEEPROM Version - Displays the SEEPROM Version number of the RAID Controller.
- CPLD Version - Displays the CPLD Version number of the RAID Controller.
- Package Version - Displays the Package Version number of the RAID Controller.
- PCI Vendor Id - Displays the PCI Vendor Id of the RAID Controller.
- PCI Device Id - Displays the PCI Device Id of the RAID Controller.
- PCI Subvendor ID - Displays the PCI Subvendor Id of the RAID Controller.
- PCI Subsystem Id - Displays the PCI Sub-Device Id of the RAID Controller.
- ROC Temp (°C) - Displays ROC temperature.
- Expander Temp (°C) - Displays the Expander temperature.
- RAID Event Log - Displays a graphical representation of all events incurred by the RAID Controller and %occupied/available space in logs. If you click on the Details link, you can view a list of available events.

Storage Summary

This tab displays a brief summary of storage devices available under the RAID controller. To open the Storage Summary section, click Settings > Monitoring > RAID Management > Storage Summary from the menu bar. A sample screenshot of Storage Summary section is shown below.



Storage Summary

RAID Controller
Gigabyte MR-3108-CRA4548 (257)

Data Synchronization Status : OK

Physical Devices Count:
0

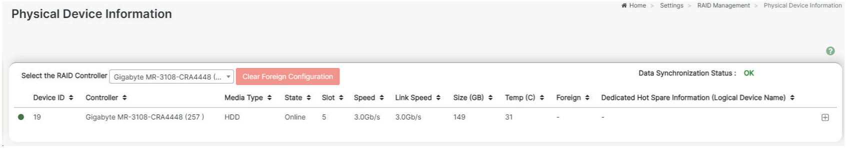
Logical Devices Count:
0

Hot Spares Count:
0

- Physical Devices Count - Displays the number of Physical Devices connected to the controller.
- Logical Devices Count - Displays the number of Logical Devices configured and available under the controller.

Physical Device Information

This tab displays the details about the Physical Devices connected to the RAID controller. To open the Physical Device Information, click Settings > Monitoring > RAID Management > Physical Device Information from the menu bar. A sample screenshot of Physical Device Information section is shown below.



Physical Device Information

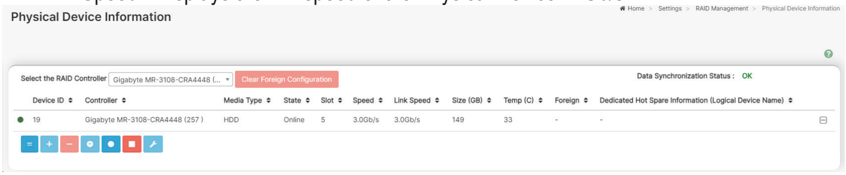
Home > Settings > RAID Management > Physical Device Information

Select the RAID Controller: Gigabyte MR-3108-CRA4448 (... | Clear Foreign Configuration

Data Synchronization Status : OK

	Device ID	Controller	Media Type	State	Slot	Speed	Link Speed	Size (GB)	Temp (C)	Foreign	Dedicated Hot Spare Information (Logical Device Name)
●	19	Gigabyte MR-3108-CRA4448 (257)	HDD	Online	5	3.0Gb/s	3.0Gb/s	149	31	-	-

- RAID Controller - To view the details of specific RAID Controller.
- Device Id - Displays the Device ID of physical device available under selected RAID controller.
- Controller - Displays the name of RAID controller to which the physical device is attached.
- Media Type - Displays the media type of physical device that is attached to the selected RAID controller.
- State - Displays State of the Physical Device (either online, or offline).
- Slot - Displays Slot number, through which Physical Device is connected to the back plane.
- Speed - Displays the speed of the Physical Device in Gb/s.
- Link Speed - Displays the link speed of the Physical Device in Gb/s.



Physical Device Information

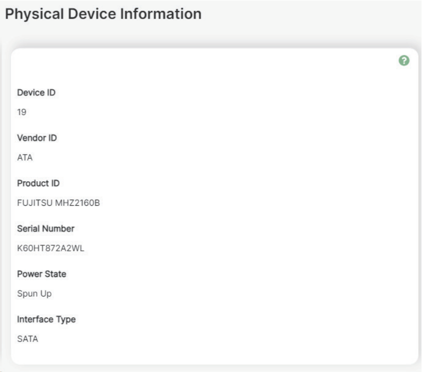
Home > Settings > RAID Management > Physical Device Information

Select the RAID Controller: Gigabyte MR-3108-CRA4448 (... | Clear Foreign Configuration

Data Synchronization Status : OK

	Device ID	Controller	Media Type	State	Slot	Speed	Link Speed	Size (GB)	Temp (C)	Foreign	Dedicated Hot Spare Information (Logical Device Name)
●	19	Gigabyte MR-3108-CRA4448 (257)	HDD	Online	5	3.0Gb/s	3.0Gb/s	149	33	-	-

View Physical Device Information: Click View Icon to view more details about the Physical Device Information, including Device Id, Vendor Id, Product Id, Serial Number, Power State, and Interface Type. A sample screenshot of View Physical Device Information page is shown below.



Physical Device Information

Device ID
19

Vendor ID
ATA

Product ID
FUJITSU MHZ2160B

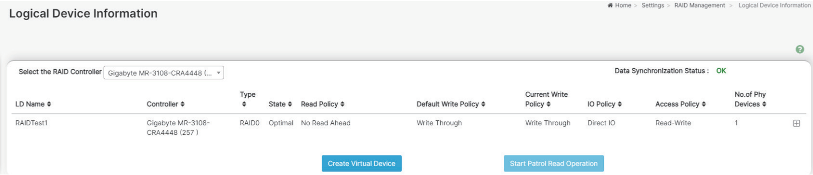
Serial Number
K60HT872A2WL

Power State
Spun Up

Interface Type
SATA

Logical Device Information

This tab displays the details about the Logical Devices configured under the RAID controller. To open the Logical Device Information section, click Settings > Monitoring > RAID Management > Logical Device Information from the menu bar. A sample screenshot of Logical Device Information section is shown below.



Logical Device Information
Home > Settings > RAID Management > Logical Device Information
Create Virtual Device
Start Patrol Read Operation

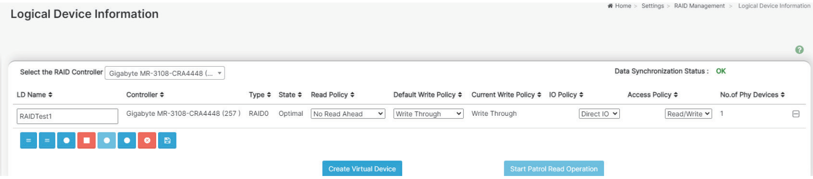
Select the RAID Controller: Gigabyte MR-3108-CRA4448 (...

Data Synchronization Status : OK

LD Name	Controller	Type	State	Read Policy	Default Write Policy	Current Write Policy	IO Policy	Access Policy	No.of Phy Devices
RAIDTest1	Gigabyte MR-3108-CRA4448 (257)	RAID0	Optimal	No Read Ahead	Write Through	Write Through	Direct IO	Read-Write	1

- Select the RAID Controller - To view the details of the Logical devices configured under the specific RAID controller.
- LD Name - Displays the name of the Logical Device configured under selected RAID controller.
- Controller - Displays the Name of the RAID Controller under which the Logical Devices are configured.
- Type - Displays the type of RAID level in which the Logical Device is configured, e.g. RAID O or RAID 1 etc.
- State - Displays the state of the Logical Device (either online or offline).
- Read Policy - Displays the Read Policy details of the Logical Device.
- Default Write Policy - Displays the Default Write Policy of the Logical Device.
- Current Write Policy - Displays the Current Write Policy of the Logical Device.
- IO Policy - Displays the IO Policy details of the Logical Device.
- Access Policy - Displays the Access Policy of the Logical Device.
- No.of Physical Devices - Displays the number of Physical Devices available under the specific Logical device.

To perform additional operations, click on the slot or expand the (+) icon available for each Logical Device. A sample screenshot is shown below.



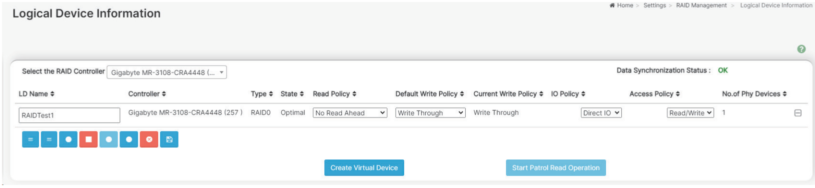
Logical Device Information
Home > Settings > RAID Management > Logical Device Information
Create Virtual Device
Start Patrol Read Operation

Select the RAID Controller: Gigabyte MR-3108-CRA4448 (...

Data Synchronization Status : OK

LD Name	Controller	Type	State	Read Policy	Default Write Policy	Current Write Policy	IO Policy	Access Policy	No.of Phy Devices
RAIDTest1	Gigabyte MR-3108-CRA4448 (257)	RAID0	Optimal	No Read Ahead	Write Through	Write Through	Direct IO	Read/Write	1

View Physical Device info for selected Virtual Device - Clicking on the icon will display the Logical Physical Device Information page, It lists the information of physical devices configured for specified logical device. A sample screenshot of View page is shown below.



Logical Device Information

Home > Settings > RAID Management > Logical Device Information

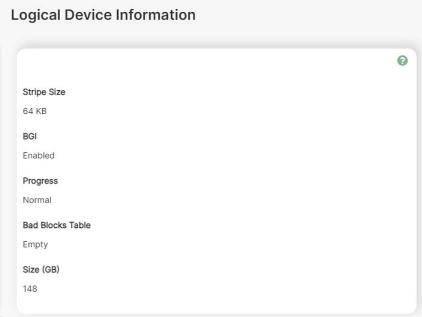
Select the RAID Controller: Gigabyte MR-3108-CRA4448 (...

Data Synchronization Status : OK

LD Name	Controller	Type	State	Read Policy	Default Write Policy	Current Write Policy	IO Policy	Access Policy	No.of Phy Devices
RAIDTest1	Gigabyte MR-3108-CRA4448 (257)	RAID0	Optimal	No Read Ahead	Write Through	Write Through	Direct IO	Read/Write	1

Create Virtual Device
Start Patrol Read Operation

Check Advanced Properties – Click icon to view the advanced properties of the selected Logical device. A sample screenshot is shown below.



Logical Device Information

Stripe Size
64 KB

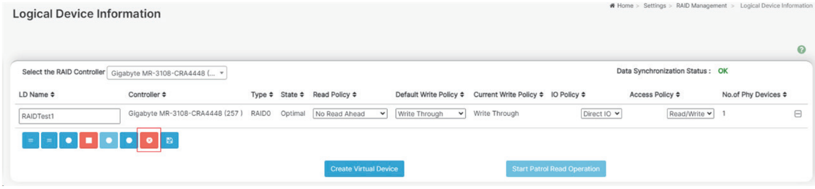
BGI
Enabled

Progress
Normal

Bad Blocks Table
Empty

Size (GB)
148

Delete Virtual Drive - Click icon to delete selected virtual device. A pop-up message prompts you to confirm your choice. Upon confirmation, you will be informed about the status.



Logical Device Information

Select the RAID Controller: Gigabyte MR-3108-CRA4448 (...

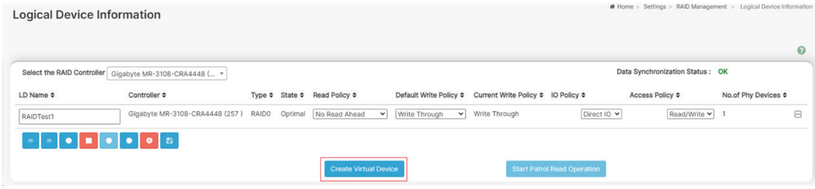
Data Synchronization Status : OK

LD Name	Controller	Type	State	Read Policy	Default Write Policy	Current Write Policy	IO Policy	Access Policy	No.of Phy Devices
RAIDTest1	Gigabyte MR-3108-CRA4448 (257)	RAID0	Optimal	No Read Ahead	Write Through	Write Through	Direct IO	Read/Write	1

Home > Settings > RAID Management > Logical Device Information
Create Virtual Device
Start Patrol Read Operation

To Create Virtual Device:

1. Click Create Virtual Device to create Logical Volume of the Device. A sample screenshot of Create Virtual Device page is shown below.


Home > Settings > RAID Management > Logical Device Information
Create Virtual Device
Start Patrol Read Operation

Logical Device Information

Select the RAID Controller: Gigabyte MR-3108-CRA4448 (...

Data Synchronization Status : OK

LD Name	Controller	Type	State	Read Policy	Default Write Policy	Current Write Policy	IO Policy	Access Policy	No.of Phy Devices
RAIDTest1	Gigabyte MR-3108-CRA4448 (257)	RAID0	Optimal	No Read Ahead	Write Through	Write Through	Direct IO	Read/Write	1

2. Select Controller Name from the drop-down lists.
3. Select RAID Level from the drop-down lists. A sample screenshot of RAID Levels is as shown below.
   Note: Only RAID Levels RAID00,RAID10,RAID50 and RAID60 will support Span Creation.

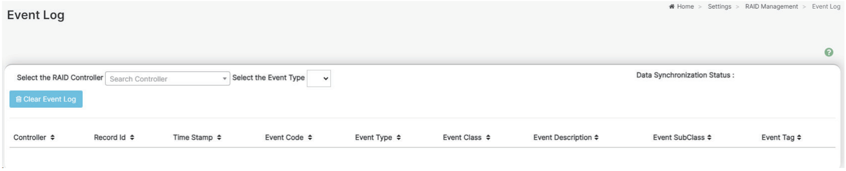
4. Enter the depth of the Span in Span Depth field.
5. Enter the number of Drives in Drives per Span field.
6. Select UnConfig Physical Drives from the drop-down lists.
   Note: UnConfigured Physical Drives should be equal to multiples of Span Depth and Drives per Span.
7. Click Create Span for mapping Span Id's to the selected Physical Drives. The mapped Span Id for the selected Unconfigured Physical Drives will be displayed as shown in the above screenshot.
8. Enter Logical Name of the Device.
9. Select Initialization type from the drop-down lists.
10. Select Stripe Size (KB), Read Policy, Default Write Policy, IO Policy, Access Policy, Disk Cache Policy and UnConfigured Physical Drives details from the respective drop-down lists.
11. Click Save to add the information to the Logical Device Information. The information will be added and displayed in the Logical Device Information page.

Event Log

This page displays all the RAID Controller events occurred that has been already configured. To open the Event Log section, click Settings > Monitoring >RAID Management > Event Log from the menu bar.

Note: All the events mentioned here are read-only and cannot be edited.

A sample screenshot of Event Log section is shown below.


Event Log
Home > Settings > RAID Management > Event Log
Select the RAID Controller
Search Controller
Select the Event Type
Data Synchronization Status :
Clear Event Log

Controller	Record Id	Time Stamp	Event Code	Event Type	Event Class	Event Description	Event SubClass	Event Tag

The Event Log page consists of the following Fields.

Select the Event Type: This field is to filter the type of event to be viewed among all available events under specified RAID controller. The category could be either All Events, LD events, PD Events, Enclosure Events, BBU Events, SAS Events, Controller Events, Configuration Events and Cluster Events.

> **Note**: Filtering can be done with the Events mentioned in the list. Once the Event Log category is chosen in the Event type drop-down list then the filtered events will be displayed with the Record ID, Time Stamp, Event Code, Event Type and Event Class.

Navigational arrows can be used to selectively access different pages of the Event Log.

Clear Event Log: To delete all the event logs.

Procedure

1. Select the RAID Controller from the drop-down list.
2. Select the Event Type from the drop-down list.
3. To clear all events from the list, click Clear Event Log.

2-5-1-6 SMTP Settings

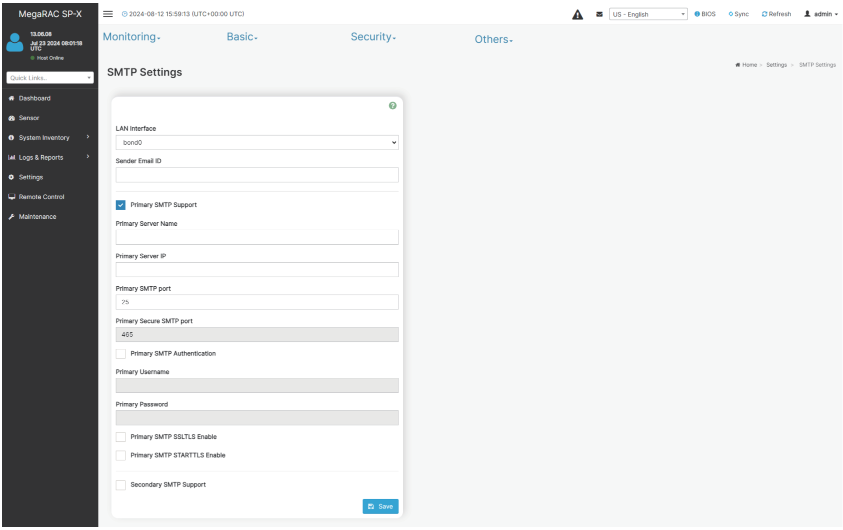
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across

Internet Protocol (IP) networks.

Using Web GUI, you can configure the SMTP settings of the device.

To open SMTP Settings page, click **Settings > Monitoring > SMTP Settings** from the menu bar.

A sample screenshot of SMTP Settings Page is shown below.



SMTP Settings

LAN Interface: bond0

Sender Email ID:

☑ Primary SMTP Support

Primary Server Name:

Primary Server IP:

Primary SMTP port: 25

Primary Secure SMTP port: 465

□ Primary SMTP Authentication

Primary Username:

Primary Password:

□ Primary SMTP SSLTLS Enable

□ Primary SMTP STARTTLS Enable

□ Secondary SMTP Support

The fields of SMTP Settings Page are explained below.

LAN Interface: Displays the list of LAN channels available.

Sender Email ID: A valid 'Sender Address' to indicate the BMC, whenever e-mail is sent.

Primary Server Name: The 'Machine Name' of the BMC, from where the e-mail is sent.

Note:

Machine Name is a string of maximum 15 alpha-numeric characters.
Space, special characters are not allowed.

Primary SMTP Support: To enable/disable SMTP support for the BMC.

Primary SMTP Port: To specify the SMTP Normal Port.

Primary Secure SMTP Port: To specify the SMTP Secure Port.

Note:

- For Primary SMTP Port – Default Port is 25, and the Port value ranges from 1 to 65535.
- For Primary Secure SMTP Port – Default Port is 465, and the Port value ranges from 1 to 65535.

Primary Server IP: The IP address of the SMTP Server. It is a mandatory field.

Note:

- IP Address made of 4 numbers separated by dots as in "xxx.xxx. xxx.xxx".
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports Ipv4 Address format and Ipv6 Address format.

Primary SMTP Authentication: To enable/disable SMTP Authentication.

Note: SMTP Server Authentication Types supported are:

- CRAM-MD5
- LOGIN

- PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, **Authentication type is not supported by SMTP Server**.

Primary Username: Enter username to access SMTP Accounts.

Note:

- User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_).
- It must start with an alphabet.
- Other Special Characters are not allowed.

Primary Password: Enter password for the SMTP User Account.

Note:

- Password must be at least 4 characters long.
- White space is not allowed.
- This field will not allow more than 64 characters.

Primary SMTP STARTTLS Enable: To enable STARTTLS support for the SMTP Client.

Upload SMTP CA Certificate File: File that contains the certificate of the trusted CA certs. CACERT key file should be of pem type,

- Upload SMTP Certificate File: Client certificate filename. CERT key file should be of pem type.
- Upload SMTP Private Key: Client private key filename. SMTP key file should be of pem type.

Note: To enable STARTTLS support, the respective SMTP support option should be enabled.

Secondary SMTP Support: It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it tries with Secondary SMTP Server configuration.

Note: Options of Secondary SMTP Support are same as Primary SMTP Support.

Save: To save the new SMTP server configuration.

Procedure

1. Select the LAN Interface from the drop-down list.
2. Enter the Sender Email ID in the specified field.
3. Check Primary SMTP Support option to enable SMTP support for the BMC.
4. Enter the Machine Name of the SMTP Server in the Primary Server Name.

Note:

- Machine Name is a string of maximum 15 alpha-numeric characters.
- Space, special characters are not allowed.

5. Enter IP address of the SMTP Server in the Primary Server IP field. It is a mandatory field.
6. Enter the Primary SMTP Port in the specified field.
7. Enter the Primary Secure SMTP Port in the specified field.

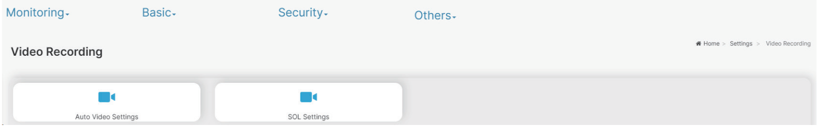
8. Enable the check box Primary SMTP Authentication if you want to authenticate SMTP Server.
9. Enter your Primary Username and Primary Password in the respective fields.
10. Enable the check box Primary SMTP SSLTLS Enable to send data through secure Port.

Note: If this option is selected, STARTTLS option and Normal Port will be hidden.

11. Check the Secondary SMTP Support option to enable Secondary SMTP support for the BMC.
12. Enter the Secondary Server Name, Secondary Server IP, Secondary SMTP Port and Secure Port values in the respective fields.
13. Enable the check box Secondary SMTP Authentication if you want to authenticate SMTP Server.
14. Enter your Secondary Username and Password in the respective fields.
15. Enable the check box Secondary SMTP SSLTLS to send data through secure Port.
    Note: If this option is selected, STARTTLS option and Normal Port will be hidden.
16. Click Save to save the entered details.

2-5-1-7 Video Recording

The Video Recording consists of the following. A sample screenshot of the Video Recording is given below.



Auto Video Settings

- Video Trigger Settings
- Video Remote Storage
- Pre-Event Video Recordings

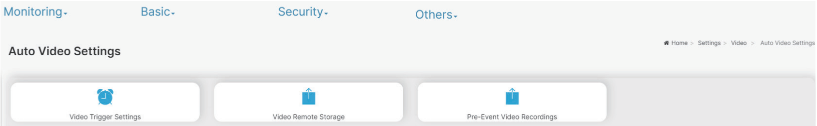
SOL Settings

- SOL Trigger Settings
- SOL Video Settings
- SOL Configurations

A detailed description of the menu items is given below.

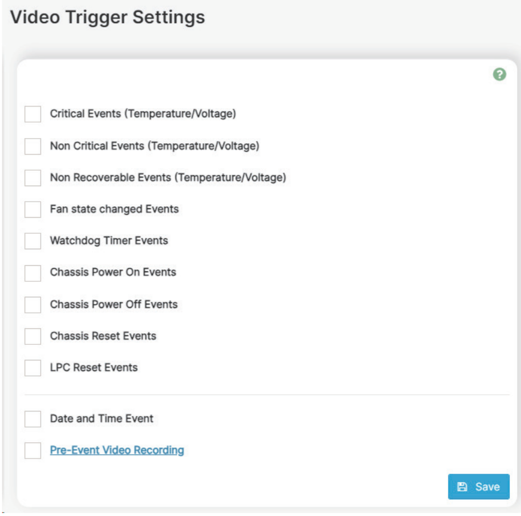
Auto Video Settings

This page allows user to configure the events that will trigger auto video recording function of the KVM server.
A sample screenshot of the Video Recording is given below.


Monitoring
Basic
Security
Others
Home > Settings > Video > Auto Video Settings
Video Trigger Settings
Video Remote Storage
Pre-Event Video Recordings

Auto Video Settings

To triggers for Auto Video Recording, click **Video Recording > Auto Video Settings > Video Trigger Settings** from the menu bar. A sample screenshot of Video Trigger Settings page is shown below.



Video Trigger Settings

□ Critical Events (Temperature/Voltage)
□ Non Critical Events (Temperature/Voltage)
□ Non Recoverable Events (Temperature/Voltage)
□ Fan state changed Events
□ Watchdog Timer Events
□ Chassis Power On Events
□ Chassis Power Off Events
□ Chassis Reset Events
□ LPC Reset Events

□ Date and Time Event
□ Pre-Event Video Recording

Video Trigger Settings

Event List: It shows the list of available events to be configured. The events are mentioned below.

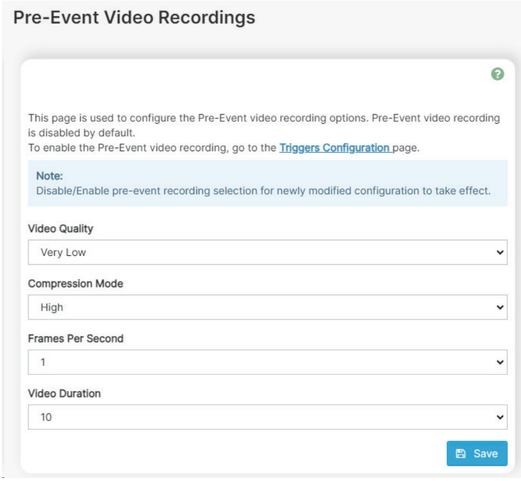
- Critical Events (Temperature/Voltage)
- Non Critical Events (Temperature/Voltage)
- Non Recoverable Events (Temperature/Voltage)
- Fan state changed Events
- Watchdog Timer Events
- Chassis Power on Events
- Chassis Power off Events
- Chassis Reset Events
- LPC Reset Events
- Date and Time Event
- Pre-Event Video Recording
  - Pre-crash
  - Pre-reset

Save: To save any changes made.

Procedure:

1. Check the events to be enabled.
2. To set particular Date and Time Event, check the option Date and Time Event.
   a. Choose the month, day and year from the Date field.
   b. Enter/Choose the Time in hh:mm format in the respective fields.
   Note: KVM service should be enabled to perform auto-video recording. The date and time should be in advance to the system date and time.
3. Click Pre-Event Video Recording to edit the Pre-Event video recording configurations.

A sample screenshot of Pre-Event Video Recordings page is shown as below.



Pre-Event Video Recordings

This page is used to configure the Pre-Event video recording options. Pre-Event video recording is disabled by default.
To enable the Pre-Event video recording, go to the Triggers Configuration page.

Note:
Disable/Enable pre-event recording selection for newly modified configuration to take effect.

Video Quality: Very Low

Compression Mode: High

Frames Per Second: 1

Video Duration: 10

To set video quality, select ranges (very low, low, high, average, and normal) from Video Quality drop-down list.

b. To set compression mode, select modes (high, normal, low, no) from Compression Mode drop-down list.

c. To set number of frames per second, select frames/sec (1-4) from Frames Per Second dropdown list.

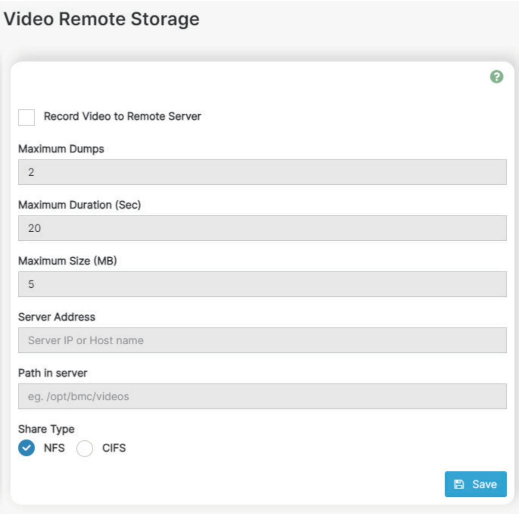
d. To set duration of video, select second (10-60) from Video Duration drop-down list.

e. Click Save to save the changes made on the Pre-Event Video Recording.

4. Select Crash Reset either Pre-crash or Pre-reset.
5. Click Save to save the changes.
   Note: Pre-Event video recording will not occur, while active KVM session or Post-event video recording is in progress.

Video Remote Storage

When a trigger event occurs, it will capture the host video and save it to the Video Remote storage, click **Video Recording > Auto Video Settings > Video Remote Storage**. A Sample screenshot of Video Remote Storage is as shown below.


Video Remote Storage

□ Record Video to Remote Server

Maximum Dumps: 2

Maximum Duration (Sec): 20

Maximum Size (MB): 5

Server Address: Server IP or Host name

Path in server: eg. /opt/bmc/videos

Share Type: ☑ NFS ○ CIFS

1. Check Record Video to Remote Server to enable the Remote Video Support.
   Note: By default, video files will be stored in local path of BMC. If remote video support is enabled, then the video files will be stored only in remote path, not within BMC.
2. Enter Maximum Dumps of the video.
3. Enter Maximum Duration (Sec) of the video.
4. Enter Maximum Size (MB) of the video.
   Note: The Maximum Duration of the video should be in the range from 1 to 3600 seconds. The Maximum Size of the video should be in the range from 1 to 500 mb. The Maximum Dumps should be in the range from 1 to 100. The

recorded video file should meet either the size constraint or duration constraint, according to the configured settings, depending on which constraint is met first.

5. Enter the Server Address.
   Note: Server address will support the following:
   - P Address (Both Ipv4 and Ipv6 format).
   - FQDN (Fully qualified domain name) format.
6. Enter the source path in Path in Server field.
7. Select the Share Type (NFS/CIFS). If the selected share type is (CIFS), Enter the Username, Password and Domain Name in the respective fields.
8. Click Save to save the settings.

Pre-Event Video Recording

Pre-Event video recording files will be named as per event captured. For example – if any video is recorded for Crash Event, the recorded file will be named as **pre_crash_video_x.dat**, where x is file count, similarly if it is recorded for reset event it will be named as pre_reset_video_x.dat.

Post-Event

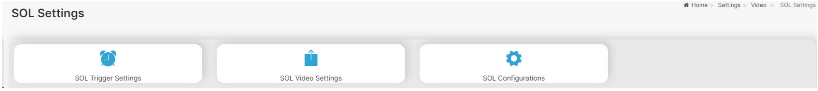
Post-Event video recording files will be named as shown below.

Video_dump_<Hostname>_%Y%m%dT%H%M%S.dat.

File Count and Duration for Pre and Post Event Recordings are as shown in the below table:

	Auto Video Recording (Post Event)	**Pre-Event Video Recording(only for Crash/reset event)**
Time Limits	20 seconds or 5.5MB video allowed if Local Storage.	Default-10sec but can be configurable up to 60sec.
	3600 seconds or 500MB video recording allowed if Remote Storage (Remote Path).	
Video File Count	Local Storage: 2 (After 2, if video recording starts, the oldest video file among the two files will be replaced with the new video)	1 if local storage/3 if remote storage. (Once Max file count reached, will Delete Old video file to store new file.)
	Remote Storage: maximum configured dump value of video files for Remote Storage.	

SOL Settings



The SOL Settings consists of the below fields.

- SOL Trigger Settings
- SOL Video Settings
- SOL Configuration

  Note: The “SOL Trigger Settings”, “SOL Video Setting” and “SOL Configuration” settings will be displayed only when “UARTLOG” feature is enabled.

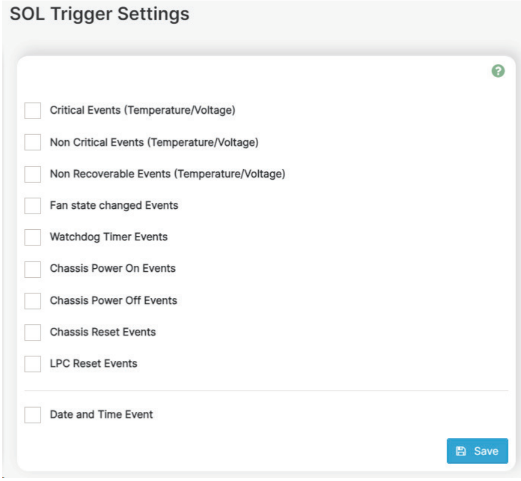
SOL Trigger Settings

Event List: It shows the list of available events to be configured. The events are mentioned below.

- Critical Events (Temperature/Voltage)
- Non Critical Events (Temperature/Voltage)
- Non Recoverable Events (Temperature/Voltage)

- Fan state changed Events
- Watchdog Timer Events
- Chassis Power on Event
- Chassis Power off Event
- Chassis Reset Events
- Date and Time Events
- LPC Reset Events Save: To save any changes made.

A sample screenshot of SOL Trigger Settings page is shown as below.



SOL Trigger Settings

☐ Critical Events (Temperature/Voltage)

☐ Non Critical Events (Temperature/Voltage)

☐ Non Recoverable Events (Temperature/Voltage)

☐ Fan state changed Events

☐ Watchdog Timer Events

☐ Chassis Power On Events

☐ Chassis Power Off Events

☐ Chassis Reset Events

☐ LPC Reset Events

☐ Date and Time Event

Procedure:

1. Check the events to be enabled to configure which event on the page will trigger the SOL video recording option to start.
2. To set particular Date and Time Event, check the option Date and Time Event.Choose the month,

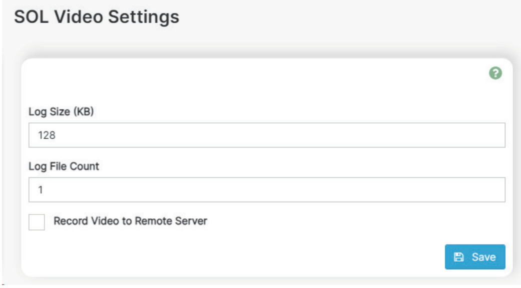
   a. Choose the month, day and year from the Date field.

   b. Enter the Time in hh:mm:ss format in the respective fields.

   Note: The date and time should be in advance to the system date and time.
3. Click Save to save the changes.

SOL Video Settings

This page allows you to configure recorded video files. The sample screenshot and various fields of **SOL Video Settings** are given below.



SOL Video Settings

Log Size (KB)

128

Log File Count

1

□ Record Video to Remote Server

Procedure for SOL Video Settings:

1. Click SOL Video Settings.
2. Enter Log Size (KB). The value will support maximum length of 10 digits.
3. Enter Log File Count. The Maximum number of Log files count is 1.
4. Check Record Video to Remote Server to enable the Remote Video Support.
   Note: The Server Address, Source Path and Share Type will be enabled only if the Remote Video Support option is enabled.
5. Enter the **Server Address**.
   Note: Server address will support the following:
   - IP Address (Both Ipv4 and Ipv6 format).
   - FQDN (Fully qualified domain name) format.
6. Enter the source path in Path in server filed.
7. Select the Share Type(NFS/CIFS). If the selected share type is CIFS, Enter the Username, Password and Domain Name in the respective fields.
8. Click Save to save the settings.

Note:

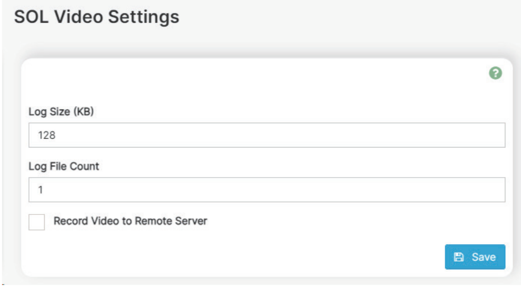
- If the proper SOC specific video driver is installed in the host, only video changes will be captured during the video recording process.
- The host cursor data, in this case, will not be a part of the video changes, and hence the host cursor will not be available in the recorded video file (DAT file).

SOL Configuration

Configuration List: It shows the list of available configurations to be configured. The configurations are mentioned below.

- Volatile Bit Rate
- Non-Volatile Bit Rate

The sample screenshot and various fields of SOL Configuration are given below.


SOL Video Settings

Log Size (KB): 128

Log File Count: 1

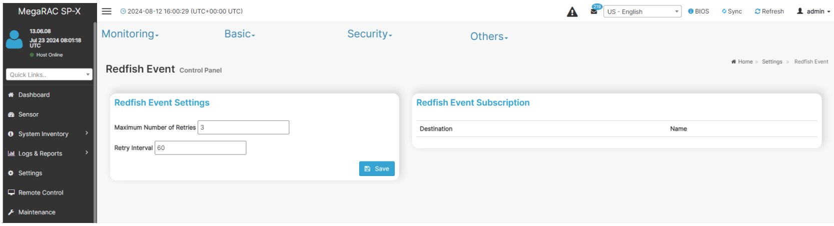
□ Record Video to Remote Server

Procedure :

1. Choose **Volatile Bit rate** to determine which baud rate will be used for both of IPMI and HTML based SOL, this field will be overwritten as same as Non-Volatile Bit rate after reboot.
2. Choose **Non-Volatile Bit** rate to determine which baud rate will be saved, it will set to Volatile Bit rate after reboot.
3. Click **Save** to save the current changes.

2-5-1-8 Redfish Event

This page displays the Redfish Event. The sample screenshot and various fields of Redfish Event are given below.


Redfish Event Control Panel

Redfish Event Settings

Maximum Number of Retries: 3

Retry Interval: 60

Redfish Event Subscription

Destination	Name

Redfish Event Settings

Maximum Number of Retries: The maximum number of retries.

Retry Interval: The interval of every retry.

Save: To save the configuration.

Redfish Event Subscription

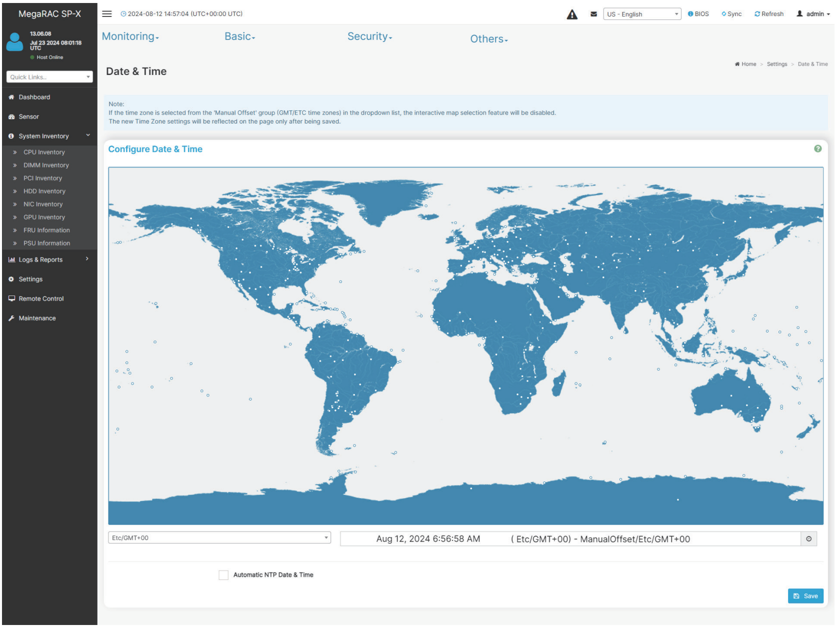
Destination: Display the destination of Redfish Event.

Name: Display the name of Redfish Event.

2-5-2 Basic

2-5-2-1 Date & Time

This field is used to set the date and time on the BMC. A Sample screenshot of **Date & Time** is shown as below.



Date & Time

Note:
If the time zone is selected from the 'Manual Offset' group (GMT/ETC time zones) in the dropdown list, the interactive map selection feature will be disabled.
The new Time Zone settings will be reflected on the page only after being saved.

Configure Date & Time

Etc/GMT+00

Aug 12, 2024 6:56:58 AM (Etc/GMT+00) - ManualOffset/Etc/GMT+00

□ Automatic NTP Date & Time

The Date & Time section consists of the following fields.

Configure Date & Time: Displays Time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.
Select Time Zone: This field is used to set the date and time on the BMC.
Automatic NTP Date & Time: Automatically synchronizes Date and Time with the NTP Server.

- **Primary NTP Server**: Configures a primary NTP server to use when automatically setting the date and time.
- **Secondary NTP Server**: Configures a secondary NTP server to use when automatically setting the date and time.

Save: Saves the configured settings.

Procedure

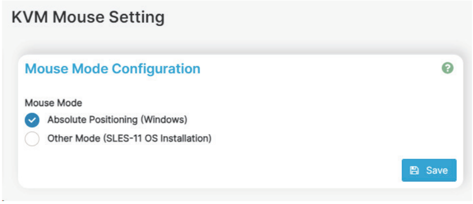
1. Select the Time zone location from the map.
2. Enable **Automatic NTP Date & Time**.
   a. In the Primary NTP Server and Secondary NTP Server fields, specify the NTP servers of the device respectively.

Note: Secondary NTP server is optional field. If the Primary NTP server is not working fine, then the Secondary NTP Server will be tried.

3. Click **Save** button to save the settings.

2-5-2-2 KVM Mouse Settings

In Web GUI, Redirection Console handles mouse emulation from local window to remote screen in either of three methods. User has to be an Administrator to configure this option. To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.
To open KVM Mouse setting page, click **Settings > Basic > KVM Mouse Settings** from the menu bar. A sample screenshot of KVM Mouse Settings Page is shown below.



KVM Mouse Setting

Mouse Mode Configuration

Mouse Mode
● Absolute Positioning (Windows)
○ Other Mode (SLES-11 OS Installation)

The fields of KVM Mouse Settings page are explained below.
Absolute Positioning (Windows): The absolute position of the local mouse is sent to the server.
Other Mode (SLES-11 OS Installation): To have the calculated displacement from the local mouse in the center position sent to the server.
Save: To save the changes made.

Procedure

1. Choose either of the following as your requirement:
   - Set mode to Absolute

Note: Applicable for all Windows versions, versions above RHEL6, and versions above FC14

   - Set mode to Other Mode

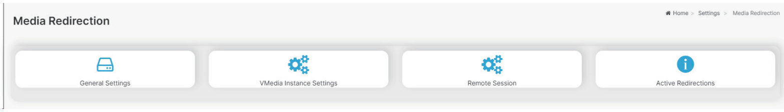
Note: Recommended for SLES-11 OS Installation

2. Click Save button to save the changes made.

Note: If the client and host mouse position is not in sync, then check the release notes of the Host OS to verify any additional configuration to be needed in the Host.

2-5-2-3 Media Redirection Settings

This page is used to configure the media into BMC for redirection. To open Media Redirection page, click **Settings > Basic > Media Redirection Settings** from the menu bar.
A sample screenshot of Media Redirection page is shown below.



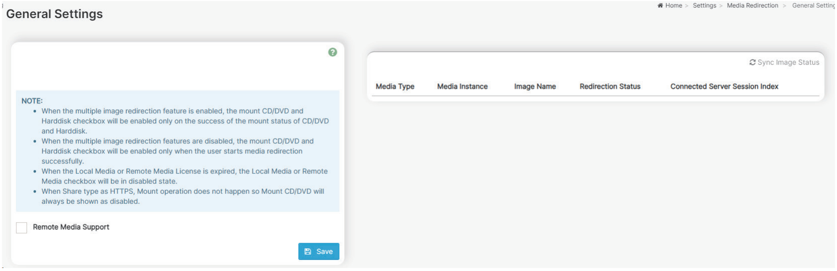
Media Redirection

The fields of Media Redirection page are explained below.
- General Settings
- Vmedia Instance Settings
- Remote Session

- Active Redirections

General Settings

This option is used to configure General Media Settings.
To open General Media Settings section, click **Settings > Basic > Media Redirection Settings > General Settings.**



Home > Settings > Media Redirection > General Setting

General Settings

NOTE:
- When the multiple image redirection feature is enabled, the mount CD/DVD and Harddisk checkbox will be enabled only on the success of the mount status of CD/DVD and Harddisk.
- When the multiple image redirection features are disabled, the mount CD/DVD and Harddisk checkbox will be enabled only when the user starts media redirection successfully.
- When the Local Media or Remote Media License is expired, the Local Media or Remote Media checkbox will be in disabled state.
- When Share type as HTTPS, Mount operation does not happen so Mount CD/DVD will always be shown as disabled.

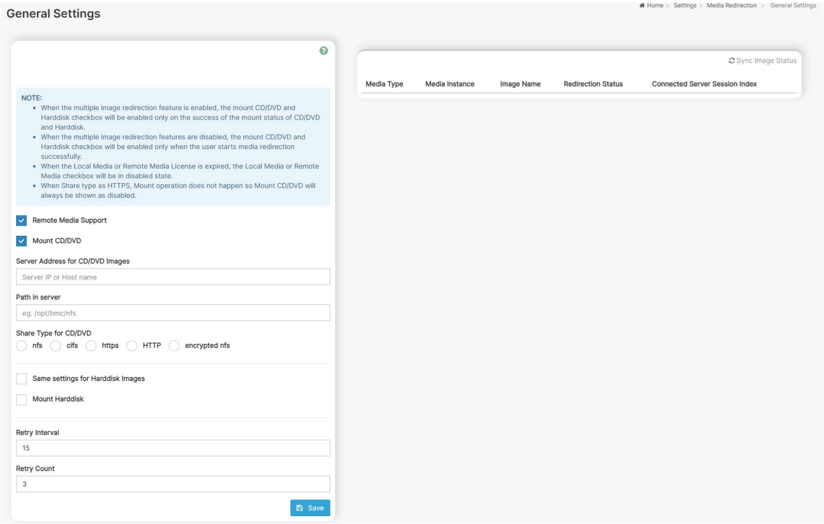
□ Remote Media Support

Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index

Remote Media Support: To enable or disable Remote Media support, check/uncheck the ‘Enable’ check box.
If it is selected, then the following Remote Media types will be displayed.

- Mount CD/DVD
- Mount Harddisk

On selecting the individual media types, its respective configurations will be displayed. You can configure different settings for different Remote Media types. A sample screenshot of General Settings page is shown below.



Home > Settings > Media Redirection > General Settings

General Settings

NOTE:
- When the multiple image redirection feature is enabled, the mount CD/DVD and Harddisk checkbox will be enabled only on the success of the mount status of CD/DVD and Harddisk.
- When the multiple image redirection features are disabled, the mount CD/DVD and Harddisk checkbox will be enabled only when the user starts media redirection successfully.
- When the Local Media or Remote Media License is expired, the Local Media or Remote Media checkbox will be in disabled state.
- When Share type as HTTPS, Mount operation does not happen so Mount CD/DVD will always be shown as disabled.

☑ Remote Media Support

☑ Mount CD/DVD

Server Address for CD/DVD Images: Server IP or Host name

Path in server: eg. /opt/bmc/nfs

Share Type for CD/DVD: ○ nfs ○ cifs ○ https ○ HTTP ○ encrypted nfs

□ Same settings for Harddisk Images

□ Mount Harddisk

Retry Interval: 15

Retry Count: 3

Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index

Mount CD/DVD: Enable/Disable to Mount CD/DVD.

Server Address for CD/DVD Images: Address of the server where the Remote media images are stored.

Path in server: Source path to the Remote media images.

Share Type for CD/DVD: To select Share Type for CD/DVD either NFS/ CIFS /HTTPS/ SMBE/ encrypted NFS.

Mount Harddisk: Enable/Disable to Mount Harddisk.

Server Address for Harddisk Images: Address of the server where the Remote media images are stored.

Path in server: Source path to the Remote media images.

Share Type for Harddisk: To Select Share Type for Harddisk either NFS or CIFS.

Domain Name, Username, and Password: If share Type is Samba(CIFS), then enter user credentials to authenticate on the server.

Username, and Password: If share Type is HTTPS, then enter user credentials to authenticate on the server.

Default Realm Name, KDC Server name, Domain Realm1, Domain realm2, Principal Name, Principal Password,

Key Version Number, and Encryption Type: If share Type is encrypted NFS(Kerberos), then enter the user credentials to authenticate on the server.

Retry Interval: Enter the retry interval to reconnect RMedia.

Retry Count: Enter the retry count to reconnect RMedia.

Save: To save the settings.

> **Note**: More than one image can be configured for each image type. At maximum 4 images can be configurable.
> To configure the image, you need to enable Remote Media support under Settings->Media Redirection -> General Settings.
> To start/stop redirection and to delete an image, you must have Administrator Privileges.
> Free slots are denoted by “~”.

Supported CD/DVD format: ISO9660, UDF(v1.02~v2.60).
Supported CD/DVD media file type: (*.iso), (*.nrg).
Supported HDD media file type: (*.img), (*.ima).

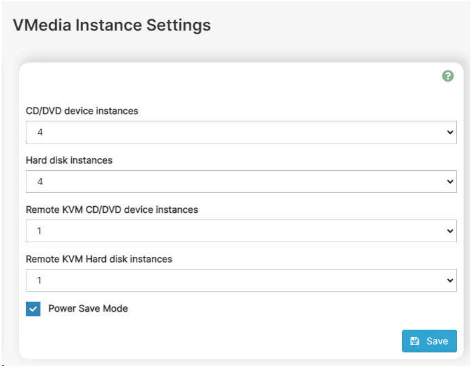
The fields of Remote Media tab are as follows:
Media Type: Displays type of Media such as CD/DVD and Harddisk.
Media Instance: Displays total media instance count.
Image Name: Displays the default recovery image name on the server.
Status: Displays the status of the media.
Session Index: Displays Media Server Session Index.
Start/Stop Redirection: To start or stop Media redirection.
Pause: To Pause the Media redirection.
Sync Image Status: To get latest Image lists from the Remote Storage.

Procedure:
Select **Remote Media Support** option.

1. Select **Mount CD/DVD**.
2. Enter **Server Address for CD/DVD Images**.
3. Enter **Path in server**.
4. Select **Share Type for CD/DVD**.
5. Select **Same settings for Harddisk Images** if required.
6. Select **Mount Harddisk**.
7. Enter **Server Address for Harddisk Images**.
8. Enter **Path in server**.
9. Select **Share Type for Harddisk**.
10. Enter **Retry Interval**.
11. Enter **Retry Count**.
12. Click **Save**.

Vmedia Instance Settings

This page is used to configure Virtual Media device settings. To open Vmedia Instance Settings page, click **Settings > Basic > Media Redirection Settings > Vmedia Instance Settings** from the menu bar.
A sample screenshot of Vmedia Instance Settings Page is shown below.



VMedia Instance Settings

CD/DVD device instances: 4

Hard disk instances: 4

Remote KVM CD/DVD device instances: 1

Remote KVM Hard disk instances: 1

☑ Power Save Mode

The following fields are displayed in this page.

CD/DVD device instances: The number of CD/DVD devices supported for Virtual Media redirection.

Harddisk instances: The number of harddisk devices supported for Virtual Media redirection.

Remote KVM CD/DVD device instances: The number of CD/DVD devices supported for KVM Virtual Media redirection.

Remote KVM Hard disk instances: The number of Hard disk devices supported for KVM Virtual Media redirection.

Power Save Mode: To enable or disable the virtual USB devices visibility in the host. If this option is enabled, Virtual media devices will be connected to the Host machine only at the instance launching KVM session. If this option is disabled, Virtual media devices will remain connected to the host machine all the time irrespective of KVM session
status.

Save: To save the configured settings.

> **Note**: Virtual Media configuration changes will restart all the media services. So configuration changes will be blocked when any active media redirection is present.

Procedure

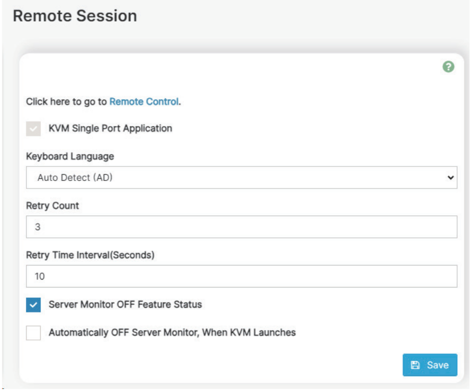
1. Select the number of **CD/DVD devices, Harddisk devices** and **Remote KVM CD/DVD** and **Hard disk Devices** from the respective drop-down list.
   Note: Maximum of four devices can be added in CD/DVD and Harddisk drives.
2. Select the **Emulate SD Media as USB disk to Host** option to enable/disable the SD card support in the host.

3. Check the **Power Save Mode** option to enable/disable the Virtual USB devices visibility in the host.
4. Click **Save** to save the changes made else click Reset to reset the previously saved values.
   Note: When KVM is launched from Standalone Application, If there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.
   Unmounting device will make the driver disconnect device when using Auto Attach.
   Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected.

Remote Session

In Web GUI, this page is used to configure Remote Session configuration settings. "KVM Single Port Application" is enabled by default.

To open Remote Session page, click **Settings > Basic > Media Redirection Settings > Remote Session** from the menu bar. A sample screenshot of Remote Session Page is shown below.



Remote Session

Click here to go to Remote Control.

☑ KVM Single Port Application

Keyboard Language: Auto Detect (AD)

Retry Count: 3

Retry Time Interval(Seconds): 10

☑ Server Monitor OFF Feature Status

☐ Automatically OFF Server Monitor, When KVM Launches

The fields of Configure Remote Session Page are explained below.

KVM Single Port Application: To Enable/Disable single port support by runtime. On changing this configuration, KVM and Vmedia Sessions will be restarted. If this support is enabled, KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via Web Port. If this support is disabled, KVM and Web sessions will use their own dedicated ports respectively.

Keyboard Language: This option is used to select the keyboard supported languages.

Retry Count: This option is used to retry the redirection session for certain number of attempts.

Retry Time Interval(Seconds): This option is used to give time interval for each attempts.

Server Monitor OFF Feature Status: To enable/disable Server Monitor OFF. If this option is enabled, You can Lock or Unlock the Local host monitor from the remote KVM window. If this option is disabled, you cannot Lock or Unlock the Local host monitor from the remote KVM window.

Automatically OFF Server Monitor, When KVM Launches: To enable/disable Automatically OFF Server Monitor, When KVM Launches.

Save: To save the current changes.

Note: It will automatically close the existing remote redirection either KVM or Virtual media sessions on Single Port enable/Disable or KVM Encryption Enable/Disable.

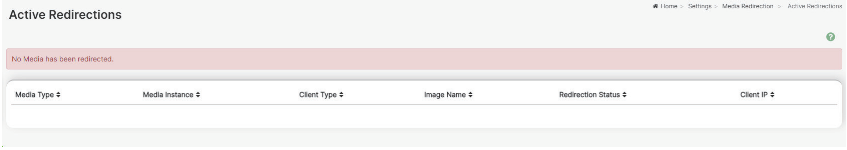
Procedure

1. Choose the **Keyboard Language** from the list of keyboard supported languages.
2. Enter a value in the **Retry Count** field to set the number of attempts for retrying the redirection session.
3. Enter a value in the **Retry Time Interval(Seconds)** field to give time interval for each attempts.
4. Check the **Server Monitor OFF Feature Status** check box to enable Local Monitor ON/OFF command during runtime.
5. Check the **Automatically OFF Server Monitor, When KVM Launches** check box to automatically Lock the local monitor during H5Viewer launch.
6. Click **Save** to save the current changes.

Active Redirections

This page is used to display the active redirected media. Information like Media type, Media Instance, Client Type,

Image Name, Redirection status, Client IP will be displayed. To open Active Redirections page, click **Settings > Basic > Media Redirection Settings > Active Redirections** from the menu bar. A sample screenshot of Active Redirections Page is shown below.



Active Redirections

No Media has been redirected.

Media Type ⇕	Media Instance ⇕	Client Type ⇕	Image Name ⇕	Redirection Status ⇕	Client IP ⇕

The following fields are displayed in this page.

Media Type: The type Media devices (CD/DVD) supported for Active Redirections.

Media instances: The number of Media devices supported for Active Redirections.

Client Type: The type Media devices (CD/DVD) supported for Active Redirections.

Image Name: The name of Media devices supported image for Active Redirections.

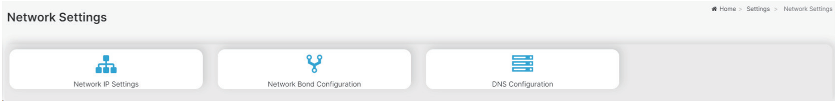
Redirection Status: The status Media for Active Redirections.

Client IP: The IP of the connected Media devices (CD/DVD) supported for Active Redirections.

> **Note**: Local/Remote Media connection will use loopback socket for communication. So '~' symbol will be displayed for loopback ip(127.0.0.1 (or) ::1) in media session information page.

2-5-2-4 Network Settings

In Web GUI, the Network Settings Page is used to configure the network settings for the available LAN channels.



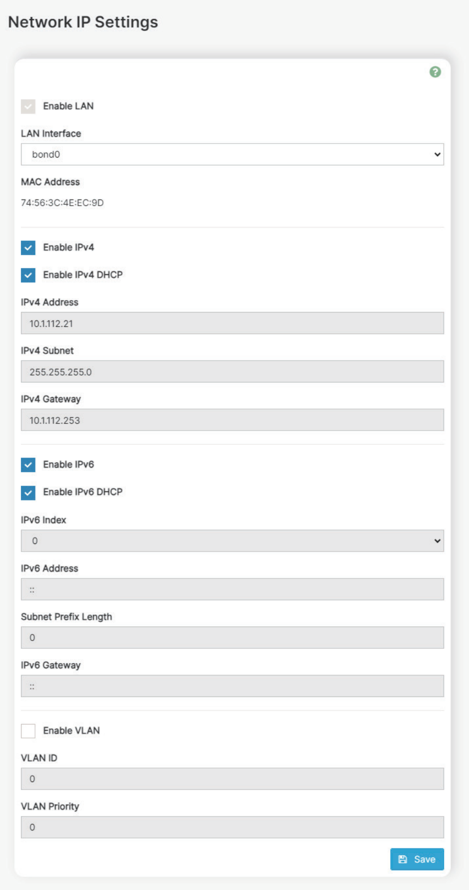
Network Settings

Home > Settings > Network Settings
Network IP Settings
Network Bond Configuration
DNS Configuration

Network IP Settings

To open Network Settings page, click Settings > Basic > Network Settings > Network IP Settings from the menu bar.

A sample screenshot of Network IP Settings Page is shown below.



Network IP Settings

☑ Enable LAN

LAN Interface: bond0

MAC Address: 74:56:3C:4E:EC:9D

☑ Enable IPv4

☑ Enable IPv4 DHCP

IPv4 Address: 10.1.112.21

IPv4 Subnet: 255.255.255.0

IPv4 Gateway: 10.1.112.253

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index: 0

IPv6 Address: ::

Subnet Prefix Length: 0

IPv6 Gateway: ::

☐ Enable VLAN

VLAN ID: 0

VLAN Priority: 0

The fields of Network IP Settings page are explained below.
Enable LAN: To enable or disable the LAN Settings.
LAN Interface: Lists the LAN interfaces.
MAC Address: This field displays the MAC Address of the device. This is a read only field.
Enable Ipv4: This option is to enable/disable the Ipv4 settings in the device.
Enable Ipv4 DHCP: This option is to enable Ipv4 DHCP support for the selected interface.
Ipv4 Address, Ipv4 Subnet Mask, and Ipv4 Default Gateway: These fields are for specifying the static Ipv4 address,Subnet Mask and Default Gateway to be configured to the device.

Note:

- IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
- Each Number ranges from 0 to 255.

- First Number must not be 0.

Enable Ipv6: To Enable/Disable the Ipv6 configuration settings.

Enable Ipv6 DHCP: To Enable/Disable the Ipv6 settings in the device. It dynamically configures Ipv6 address using DHCP (Dynamic Host Configuration Protocol).

Ipv6 Index: To specify a static Ipv6 Index to be configured to the device. E.g.: 0

Ipv6 Address: To specify a static Ipv6 address to be configured to the device. Eg: 2004::2010

Subnet Prefix length: To specify the subnet prefix length for the Ipv6 settings.
Note: Value ranges from 0 to 128.
Default Gateway: Specify v6 default gateway for the Ipv6 settings.
Note: If core feature IPV6_COMPLIANCE is enabled, the IPV6 default Gateway field will not be displayed.
Enable VLAN: To enable/disable the VLAN support for selected interface.
VLAN ID: The Identification for VLAN configuration.
Note: Value ranges from 2 to 4094.
VLAN Priority: The priority for VLAN configuration.
Note:

- Value ranges from 0 to 7.
- 7 is the highest priority for VLAN.

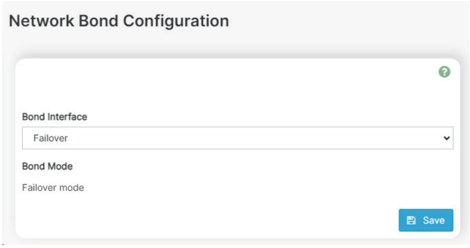
Save: To save the entries.

Procedure

1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select the **LAN Interface** to be configured.
3. Check Enable Ipv4 to enable Ipv4 support for the selected interface.
4. Check **Enable Ipv4 DHCP** to dynamically configure Ipv4 address using DHCP.
5. If the field is disabled, enter the I**pv4 Address, Ipv4 Subnet Mask** and **Ipv4 Default Gateway** in the respective fields.
6. In Ipv6 Configuration, if you wish to enable the Ipv6 settings, check **Enable Ipv6**.
7. If the Ipv6 setting is enabled, enable or disable the option **Enable Ipv6 DHCP**.
8. If the field is disabled, enter the **Ipv6 Address, Subnet Prefix length** and **Ipv6 Index** in the given field.
9. In VLAN Configuration, if you wish to enable the VLAN settings, check **Enable LAN**.
10. Enter the **VLAN ID** in the specified field.
11. Enter the **VLAN Priority** in the specified field.
12. Click **Save** to save the entries.

Network Bond Configuration

To open Network Settings page, click **Settings > Basic > Network Settings > Network Bond Configuration** from the menu bar. A sample screenshot of Network IP Settings Page is shown below.


Network Bond Configuration

Bond Interface

Failover

Bond Mode

Failover mode

The fields of Network Bond Configuration page are explained below.
Bond Interface: This option is used to select bond interface.
Bond Mode: Display the current bond mode.

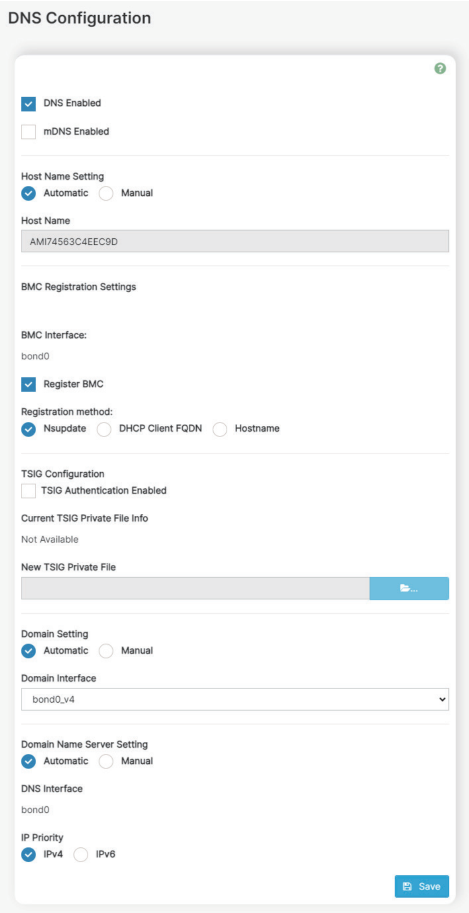
Procedure

1. Choose the Bond Interface from the list of bond interface.
2. Click Save to save the configuration.

DNS Configuration

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.
The DNS Server settings page is used to manage the DNS settings of a device.

To open DNS Server Settings page, click **Settings > Basic > Network Settings > DNS Configuration** from the menu ar. A sample screenshot of DNS Configuration page is shown below.



DNS Configuration

☑ DNS Enabled

□ mDNS Enabled

Host Name Setting
● Automatic ○ Manual

Host Name
AMI74563C4EEC9D

BMC Registration Settings

BMC Interface:
bond0

☑ Register BMC

Registration method:
● Nsupdate ○ DHCP Client FQDN ○ Hostname

TSIG Configuration
□ TSIG Authentication Enabled

Current TSIG Private File Info
Not Available

New TSIG Private File

Domain Setting
● Automatic ○ Manual

Domain Interface
bond0_v4

Domain Name Server Setting
● Automatic ○ Manual

DNS Interface
bond0

IP Priority
● IPv4 ○ IPv6

The fields of DNS Configuration page are explained below.

Domain Name Service Configuration

DNS Enabled: To enable/disable all the DNS Service Configurations.

mDNS Enable: To enable/disable the mDNS Support Configurations.

Note: After enabling mDNS, users can access the web UI using the hostname through the browser.

Host Name Settings: Choose either Automatic or Manual settings.

Host Name: It displays host name of the device. If the Host setting is chosen as Manual, then specify the host name of the device.

Note:

- Value ranges from 1 to 64 alpha-numeric characters.
- Special characters '-'(hyphen) and '_'(underscore) are allowed.
- It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_) character.

BMC Registration Settings

BMC Interface: Options to register the BMC through the Interfaces (eth0&eth1).

Register BMC: To register BMC through registration method.

Registration Method

Options to register the BMC are through **NS Update** or **DHCP Client FQDN** or **Hostname**.

TSIG Configuration

Both: Check this option to modify TSIG authentication for both interfaces.

Eth 0&1:

TSIG Authentication Enabled: Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.

Current TSIG Private File: The information of Current TSIG private file along with its uploaded date/time will be displayed (read-only).

New TSIG Private File: Browse and navigate to the TSIG private file.

Note: TSIG file should be of private type.

Domain Setting: Select whether the domain interface will be configured manually or automatically.

- **Automatic** – If you Select Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** – If the Domain setting is chosen as Manual, then specify the domain name of the device.
- **Note**: If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name".
- **Domain Name**: It displays the domain name of the device.

Domain Name Server Setting

Automatic – If you select Automatic "DNS Interface" option should be explained.

Manual – Specify the DNS (Domain Name System) server address to be configured for the BMC.

IP Priority:

- If IP Priority is Ipv4, it will have 2 Ipv4 DNS servers and 1 Ipv6 DNS server.
- If IP Priority is Ipv6, it will have 2 Ipv6 DNS servers and 1 Ipv4 DNS server.
- **Note**: This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

To specify the DNS (Domain Name System) server address to be configured for the BMC.

Note:

- Ipv4 Addresses should be given in dotted decimal representation.
- Ipv6 Addresses are supported and must be global unicast addresses.

DNS Server Address will support the following:

- Ipv4 Address format.
- Ipv6 Address format.

Save: To save the entered changes.

Procedure:

1. In **Domain Name Service Configuration**, Enable **DNS Service**.
   - Check the option DNS Enabled to enable all the DNS Service Configurations.
2. Choose the Host Name Setting either Automatic or Manual
   Note: If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.
3. Enter the Host Name in the given field if you have chosen Manual Configuration.
4. Under **Register BMC**, choose the BMC's network port to register with DNS settings.
   - Check Register BMC option to register with DNS settings. **Nsupdate** – Choose
   - **Nsupdate** option to register with DNS server using nsupdate application.
   - **DHCP Client FQDN** – Choose **DHCP Client FQDN** option to register with DNS Server using DHCP option 81.
   - **Hostname** – Choose Hostname option to register with DNS server using DHCP option 12.

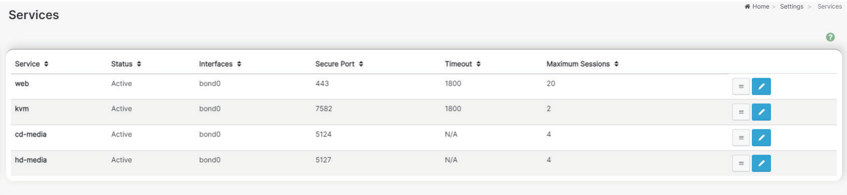
   Note: Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.
5. Check Both option to modify TSIG authentication for both interfaces (eth0&1).
6. In **Eth 0&1 TSIG Configuration**, Check T**SIG Authentication Enabled** option to enable/disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in Current TSIG Private file info field.
   - To view a new one, click New TSIG private file to browse and navigate to the TSIG private file.
7. In the **Domain Settings**,
   - Select the domain settings (Automatic or Manual).
   - Enter the **Domain Name** in the given field if the option "**Manual**" is being selected in domain settings field.

8. In **Domain Name Server Setting**,
   - Select the domain name server settings (Automatic or Manual).
   - Choose the IP Priority, either Ipv4 or Ipv6 if the option "**Automatic**" is being selected in domain name server settings field.
   - In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC if the option "Manual" is being selected in domain name server settings field.
9. Click **Save** to save the entries.

2-5-2-5 Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click Settings > Basic > Services from the menu bar. A sample screenshot of Services Page is shown below.



Services

Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions
web	Active	bond0	443	1800	20
kvm	Active	bond0	7582	1800	2
cd-media	Active	bond0	5124	N/A	4
hd-media	Active	bond0	5127	N/A	4

The fields of Services Page are explained below.

Services: Displays service name of the selected slot (read-only).

Status: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Non-secure Port: This port is used to configure non secure port number for the service.

- Web default port is 80
- KVM default port is 7578
- CD Media default port is 5120
- HD Media default port is 5123

  Note: If Single port feature is enabled, KVM, CD Media and HD Media ports cannot be edited. Port value ranges from 1 to 65535.

"ALLOW_NON_SECURE_COMMUNICATION" feature (if applicable) and port 80 will be disabled by default due to the security reasons. Hence, use _https://<ip address> (port 443) instead of _http://<ip address> (port80).

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- KVM default port is 7582
- CD Media default port is 5124
- HD Media default port is 5127

  Note:If single port feature is enabled, KVM, CD Media and HD Media ports cannot be edited. Port value ranges from 1 to 65535.

Port listening status on various feature settings:

	Single port enabled	Single port disabled	Only KVM encryption enabled	Only Media encryption enabled	Both KVM and Media encryption enabled
Adviser (video server)	7578 (LP)	7578 (LP) 7578 (EO)	7578 (LP) 7582 (EO)	7578 (LP) 7578 (EO)	7578 (LP) 7582 (EO)
Cdserver	5120 (LP)	5120 (LP) 5120 (EO)	5120 (LP) 5120 (EO)	5120 (LP) 5124 (EO)	5120 (LP) 5124 (EO)
Hdserver	5123 (LP)	5123 (LP) 5123 (EO)	5123 (LP) 5123 (EO)	5123 (LP) 5127 (EO)	5123 (LP) 5127 (EO)

Note: LP – Loopback, EO – Exposed Outside.
The adviser will always be listening to loopback as well as kvm configured interface as mentioned in the above table. So that the H5Viewer client can connect to the video server.
The media servers will be listening to loopback as well as configured interface as mentioned in the above table.So that the Imedia/rmedia and H5Viewer client can connect to the media servers.

Timeout: Displays the session timeout value of the service. For web, user can configure the session timeout value.

Note:

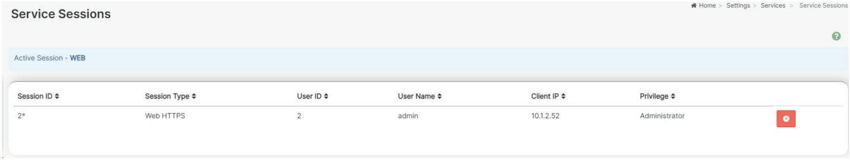
- Web timeout value ranges from 300 to 1800 seconds.
- KVM timeout value ranges from 300 to 1800 seconds.
- If KVM is launched then the web session timeout will not take effect.

Maximum Sessions: Displays the maximum number of allowed sessions for the service.
Active Sessions: To view the current active sessions for the service.

To view the Active Sessions:

Procedure:

1. Click View Icon ( ) to view the details about the active sessions for the service.
2. This opens the Active Session screen (for example – Service Sessions) as shown in the screenshot below.



Service Sessions

Active Session - **WEB**

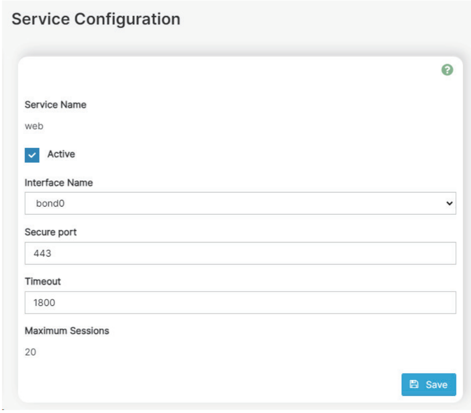
Session ID	Session Type	User ID	User Name	Client IP	Privilege
2*	Web HTTPS	2	admin	10.1.2.52	Administrator

Session ID: Displays the ID of the active sessions.
Session Type: Displays the type of the active sessions.
User ID: Displays the ID of the user.
User Name: Displays the name of the user.
Client IP: Displays the IP addresses that are already configured for the active sessions.
Privilege: Displays the access privilege of the user.

3. Select a slot and click Terminate icon ⊗ to terminate the particular session of the service.

To modify the existing services:

1. Select a slot and click Edit icon ✎ to modify the configuration of the service.
   Note: Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.
2. This opens the **Service Configuration** screen as shown in the screenshot below.



Service Configuration

Service Name
web

☑ Active

Interface Name
bond0

Secure port
443

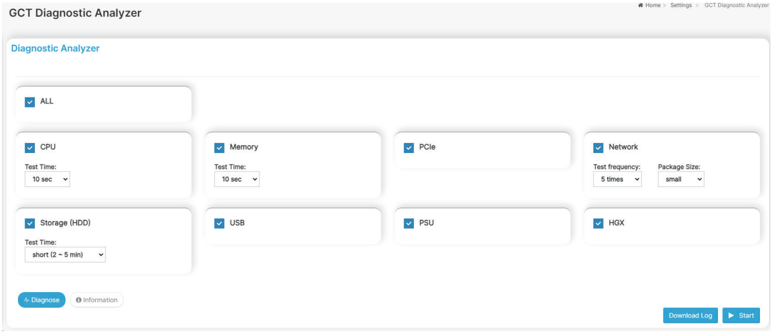
Timeout
1800

Maximum Sessions
20

3. Service Name is a read only field.
4. Activate the Current State by enabling the Active check box.
   Note: Interfaces, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.
5. Choose any one of the available interfaces from the Interface Name drop-down list.
6. Enter the Secure Port Number in the Secure Port field.
7. Enter the timeout value in the Timeout field.
   Note: The values in the Maximum Sessions field cannot be modified.
8. Click Save to save the entered changes else click Cancel to exit.

2-5-2-6 GCT Diagnostic Analyzer

The GCT Diagnostic Analyzer in BMC to provides the function of stress tests on major server components and sub-systems such as CPU, Memory, Storage, PSU, PCIe, Network, serial I/O, USB, BIOS, and System. With a specify image and BMC FW version you can easily run the diagnosis on a BMC Web page and have results immediately.



☑ ALL

☑ CPU — Test Time: 10 sec

☑ Memory — Test Time: 10 sec

☑ PCIe

☑ Network — Test frequency: 5 times — Package Size: small

☑ Storage (HDD) — Test Time: short (2 ~ 5 min)

☑ USB

☑ PSU

☑ HGX

Preparation

To build a GCT diagnostic tool, please prepare followings in advanced.
Diagnostic Tool:gct_diagnostic_analyzer_hgx_v1.0_pre3.iso.
Note: To download the diagnostic tool, go to Gigabyte offical website and go to product download page, select Firmware, and download **GCT Diagnostic Analyzer** zip file.
BMC Revision: version v13.06.08 or above

Working PC for local:
USB sticker: 4G recommend or above
rufus: tool to burn the GCT Diagnostic Analyzer Tool in a USB device for remote
PC server: plays as the NFS or HTTP or CIFS server which saves the gct_diagnostic_analyzer_hgx_v1.0_pre3.iso file

Installation

To perform this diagnostic tool, you need to install an image which consists of an Ubuntu OS and a diagnostic application. You can choose to run the diagnosis locally or remotely and setup the testing environment accordingly.

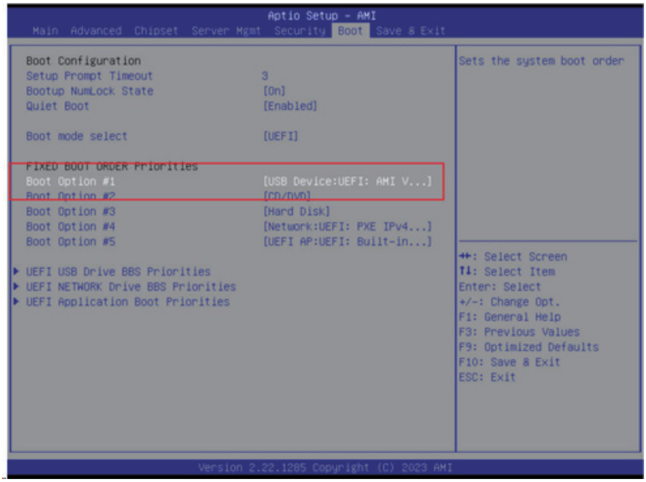
Configure a local test environment

To run a local test, please have the GCT Diagnostic Analyzer Tool image be installed in an USB sticker and insert that USB to the server which will be evaluated. Later you can execute those diagnostic functions directly from this local USB device.

Burn the GCT diagnostic analyzer tool image

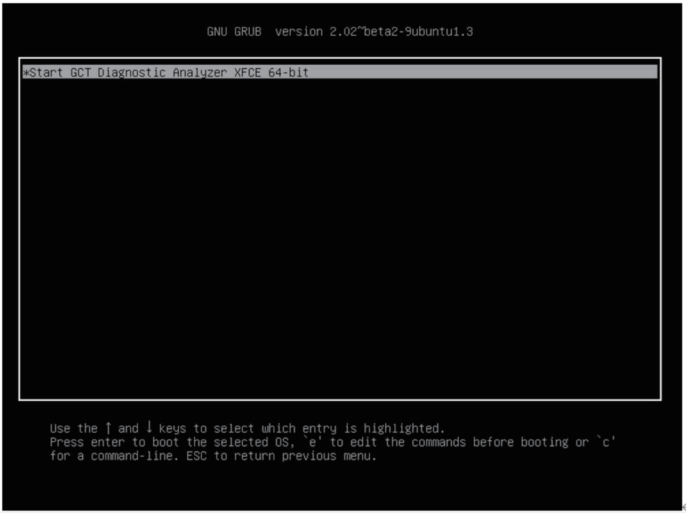
Below is the sample of using "rufus" to burn GCT Diagnostic Analyzer Tool image to a USB device. You can always use other image burning tools as you want. Insert USB device on your working PC then execute rufus.

Once you have the working USB sticker ready, plugin it to that server which you are going to diagnose then power on that server to enter BIOS setting page as follow. Make sure the USB be selected as the priority first boot device.



```
                              Aptio Setup - AMI
  Main  Advanced  Chipset  Server Mgmt  Security  Boot  Save & Exit

  Boot Configuration                                    Sets the system boot order
  Setup Prompt Timeout          3
  Bootup NumLock State          [On]
  Quiet Boot                    [Enabled]

  Boot mode select              [UEFI]

  FIXED BOOT ORDER Priorities
  Boot Option #1                [USB Device:UEFI: AMI V...]
  Boot Option #2                [CD/DVD]
  Boot Option #3                [Hard Disk]
  Boot Option #4                [Network:UEFI: PXE IPv4...]
  Boot Option #5                [UEFI AP:UEFI: Built-in...]
                                                        ↔: Select Screen
▶ UEFI USB Drive BBS Priorities                          ↑↓: Select Item
▶ UEFI NETWORK Drive BBS Priorities                      Enter: Select
▶ UEFI Application Boot Priorities                       +/-: Change Opt.
                                                        F1: General Help
                                                        F3: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Exit
                                                        ESC: Exit

                  Version 2.22.1285 Copyright (C) 2023 AMI
```

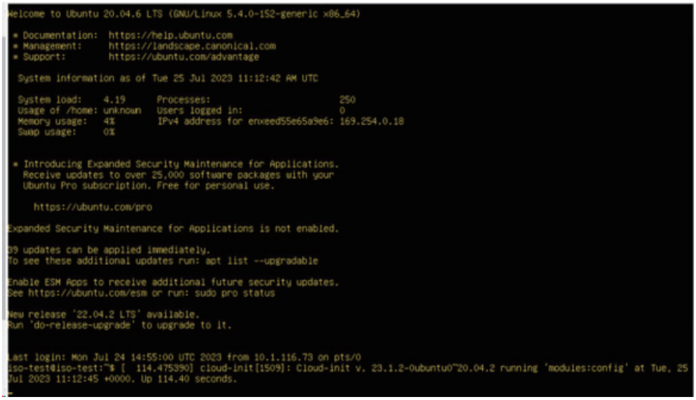
After the BIOS boot media is selected then restart server select the “GCT Diagnostic Analyzer XFCE 64-bit” as the target image. Press ENTER to start the GCT Diagnostic Analyzer Tool installation.



```
                        GNU GRUB  version 2.02~beta2-9ubuntu1.3

 *Start GCT Diagnostic Analyzer XFCE 64-bit





    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c'
    for a command-line. ESC to return previous menu.
```

Installation Complete

You can either connect a terminal to server or open the BMC KVM function to monitor the GCT Diagnostic Analyzer Tool installation progress. When the following screen shows then image creation is done, and you are ready to diagnose your server.

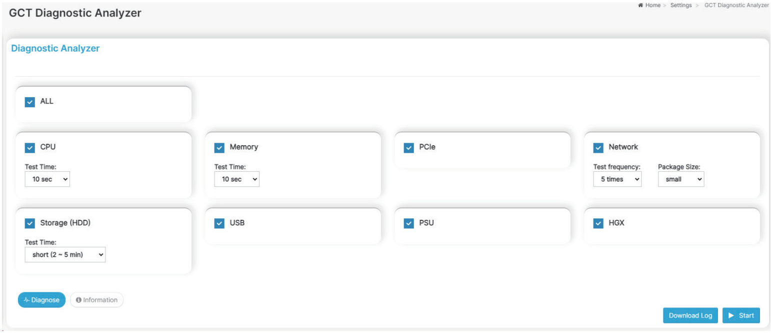


```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-152-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 25 Jul 2023 11:12:42 AM UTC

  System load:    4.19      Processes:                       250
  Usage of /home: unknown   Users logged in:                 0
  Memory usage:   4%        IPv4 address for enxeed55e65a9e6: 169.254.0.18
  Swap usage:     0%


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

39 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Jul 24 14:55:00 UTC 2023 from 10.1.116.73 on pts/0
iso-test@iso-test:~$ [  114.475390] cloud-init[1509]: Cloud-init v. 23.1.2-0ubuntu0~20.04.2 running 'modules:config' at Tue, 25
Jul 2023 11:12:45 +0000. Up 114.40 seconds.
```

Execution

After login BMC UI, go to **Settings > Basic > GCT Diagnostic Analyzer**.

Start the various of diagnosis. Following is an example of getting CPU information, executing CPU diagnosis, and retrieving diagnostic data. If OS not ready, you use GCT Diagnostic Analyzer to stress any item.



GCT Diagnostic Analyzer

Diagnostic Analyzer

☑ ALL

☑ CPU
Test Time: 10 sec

☑ Memory
Test Time: 10 sec

☑ PCIe

☑ Network
Test frequency: 5 times
Package Size: small

☑ Storage (HDD)
Test Time: short (2 ~ 5 min)

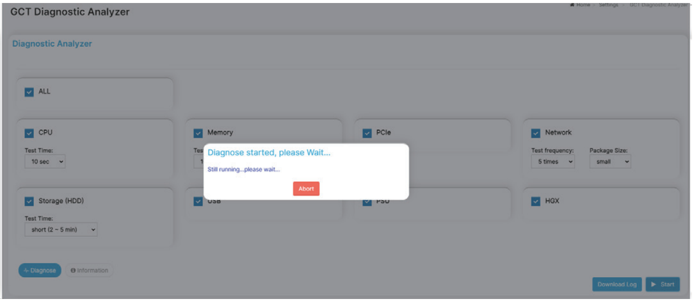
☑ USB

☑ PSU

☑ HGX

Test Result

Click Start to view the diagnostic result.



Test Time: 10 sec

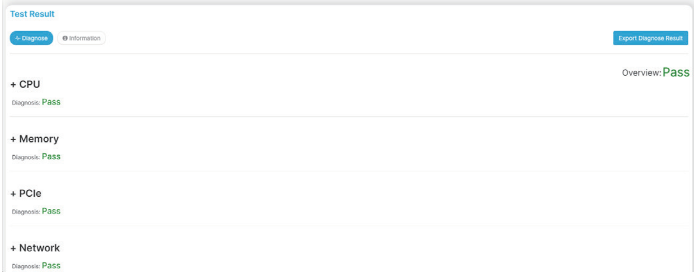
Test frequency: 5 times

Package Size: small

Test Time: short (2 ~ 5 min)

Diagnose started, please Wait...

Still running...please wait...



Overview: Pass

+ CPU

Diagnosis: Pass

+ Memory

Diagnosis: Pass

+ PCIe

Diagnosis: Pass

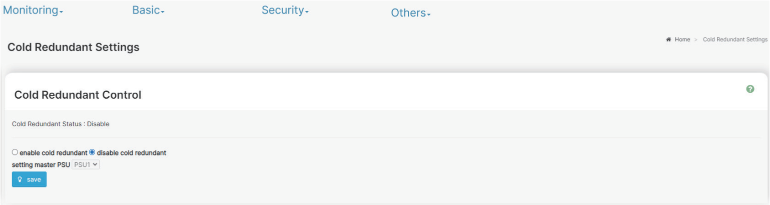
+ Network

Diagnosis: Pass

2-5-2-7 Cold Redundant Settings

This page is used to. To open Cold Redundant page, click **Settings > Basic > Cold Redundant Settings** from the menu bar.

A sample screenshot of Cold Redundant Settings page is shown below.



Cold Redundant Status : Disable

○ enable cold redundant ● disable cold redundant

setting master PSU PSU1

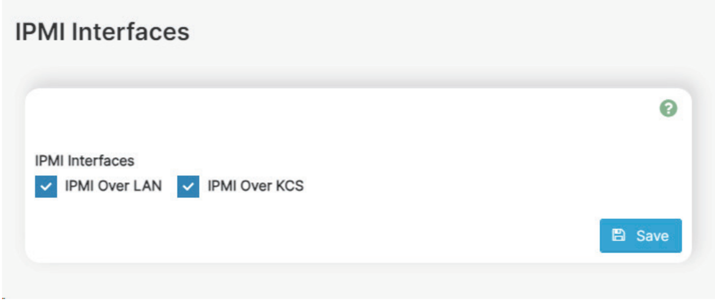
Cold Redundant Status: Display the status of Cold Redundant.
Enable cold redundant: Enable cold redundant.
Disable cold redundant: Disable cold redundant.
Setting master PSU: Display the list of PSU.
Save: Save the settings.

Procedure:

1. Choose **Enable cold redundant**.
2. Choose the matser PSU from the list of Setting master PSU.
3. Click **Save** to save the configuration.

2-5-2-8 IPMI Interfaces

This page is used to configure the IPMI Interfaces. To open IPMI interfaces page, click **Settings > Basic > IPMI** Interfaces from the menu bar.
A sample screenshot of IPMI Interfaces page is shown below.


IPMI Interfaces

IPMI Interfaces

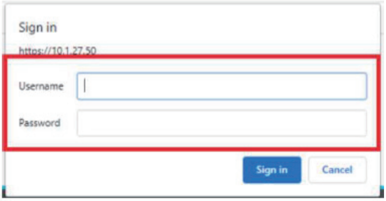
☑ IPMI Over LAN ☑ IPMI Over KCS

This page displays the following interfaces like IPMI Over LAN and IPMI Over KCS.
Procedure

- IPMI Over LAN - Check or uncheck the IPMI Over LAN interface which allows the user to perform IPMI communication over LAN.
- IPMI Over KCS - Check or uncheck the IPMI Over KCS interface which allows the user to perform IPMI communication over KCS.
  Note: IPMI Communication will not be performed over LAN /KCS interface if it is disabled.
- **Save**: Click Save to save the configured interfaces.

2-5-2-9 BIOS

This page is used to configure the BIOS. To open BIOS page, click Settings > Basic > BIOS from the menu bar. The web will pop up another window. User needs to enter Username and Password to Sign in.

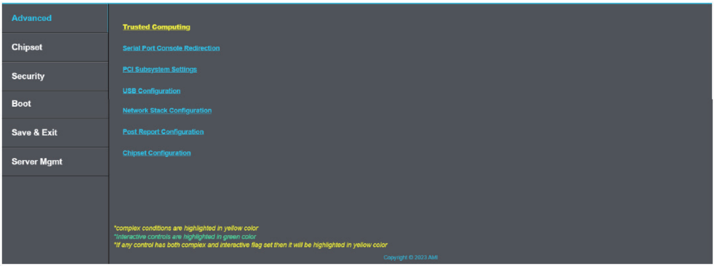

Sign in

https://10.1.27.50

Username

Password

A sample screenshot of BIOS page is shown below.



Trusted Computing
Serial Port Console Redirection
PCI Subsystem Settings
USB Configuration
Network Stack Configuration
Post Report Configuration
Chipset Configuration

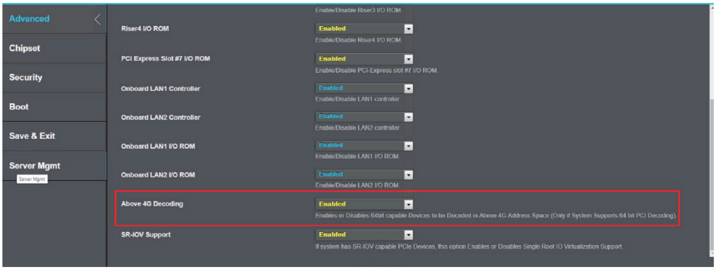
*complex conditions are highlighted in yellow color
*Interactive controls are highlighted in green color
*If any control has both complex and interactive flag set then it will be highlighted in yellow color

Copyright © 2023 AMI

Procedure

To modify Setup item current value

1. Please wait the system boot completely
2. Select the item which you want to modify. For example: Above 4G Decoding.



Enable/Disable Riser3 I/O ROM.

Riser4 I/O ROM: Enabled
Enable/Disable Riser4 I/O ROM.

PCI Express Slot #7 I/O ROM: Enabled
Enable/Disable PCI-Express slot #7 I/O ROM.

Onboard LAN1 Controller: Enabled
Enable/Disable LAN1 controller.

Onboard LAN2 Controller: Enabled
Enable/Disable LAN2 controller.

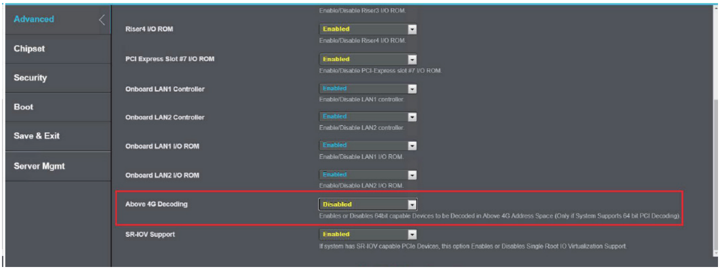
Onboard LAN1 I/O ROM: Enabled
Enable/Disable LAN1 I/O ROM.

Onboard LAN2 I/O ROM: Enabled
Enable/Disable LAN2 I/O ROM.

Above 4G Decoding: Enabled
Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).

SR-IOV Support: Enabled
If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.

3. Modify the item value.



Enable/Disable Riser3 I/O ROM.

Riser4 I/O ROM: Enabled
Enable/Disable Riser4 I/O ROM.

PCI Express Slot #7 I/O ROM: Enabled
Enable/Disable PCI-Express slot #7 I/O ROM.

Onboard LAN1 Controller: Enabled
Enable/Disable LAN1 controller.

Onboard LAN2 Controller: Enabled
Enable/Disable LAN2 controller.

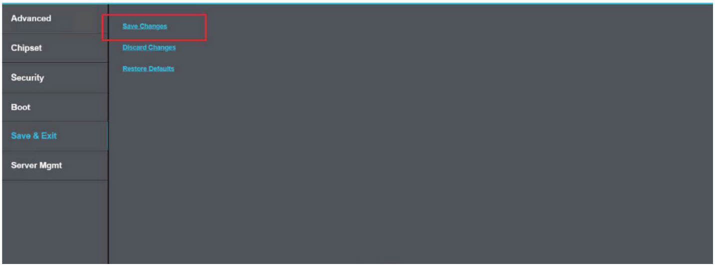
Onboard LAN1 I/O ROM: Enabled
Enable/Disable LAN1 I/O ROM.

Onboard LAN2 I/O ROM: Enabled
Enable/Disable LAN2 I/O ROM.

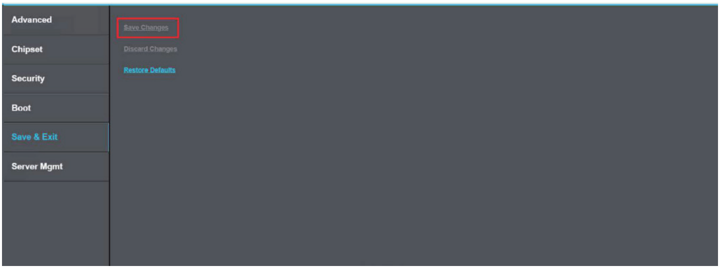
Above 4G Decoding: Disabled
Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).

SR-IOV Support: Enabled
If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.

4. Go to Save & Exit page, and press Save Changes.

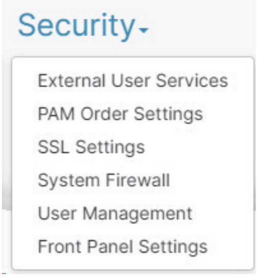


5. If the system save changes successfully, the “Save Changes” will gray out.



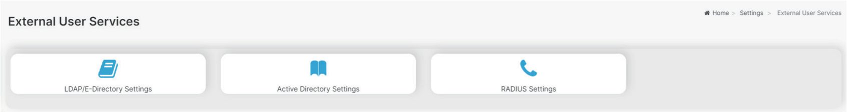
6. Please Reboot the system, and wait for the system boot completely.

2-5-3 Security



2-5-3-1 External User Services

To open External User Services page, click **Settings > Security > External User Services** from the menu bar. A sample
screenshot of External User Services page is shown below.


External User Services
Home > Settings > External User Services
LDAP/E-Directory Settings
Active Directory Settings
RADIUS Settings

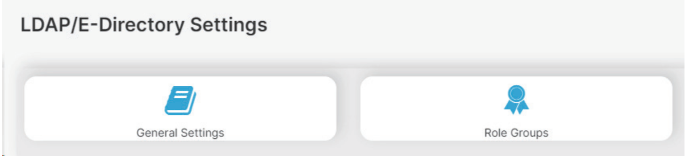
LDAP/E-Directory Settings

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.

To open LDAP/E-DIRECTORY Settings page, click **Settings > Security > External User Services > LDAP/E-Directory Settings** from the menu bar.

A sample screenshot of External User Services page is shown below.



The fields of LDAP/E-Directory Settings Page are explained below.

General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory

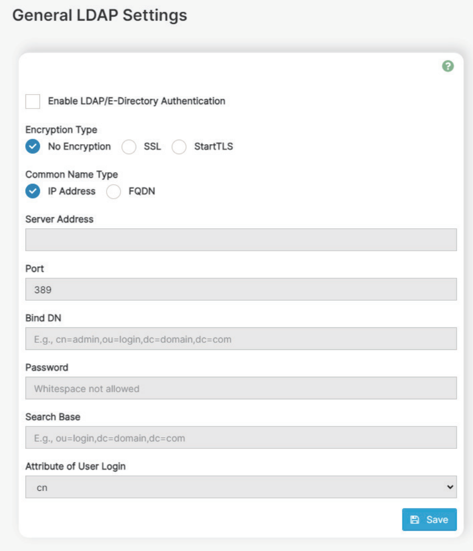
Authentication, IP Address, Port and Search base.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure

Entering the details in General LDAP/E-Directory Settings Page

1. In the LDAP/E-Directory Settings Page, click General Settings. A sample screenshot of General LDAP Settings page is given below.



General LDAP Settings

□ Enable LDAP/E-Directory Authentication

Encryption Type
● No Encryption ○ SSL ○ StartTLS

Common Name Type
● IP Address ○ FQDN

Server Address

Port
389

Bind DN
E.g., cn=admin,ou=login,dc=domain,dc=com

Password
Whitespace not allowed

Search Base
E.g., ou=login,dc=domain,dc=com

Attribute of User Login
cn

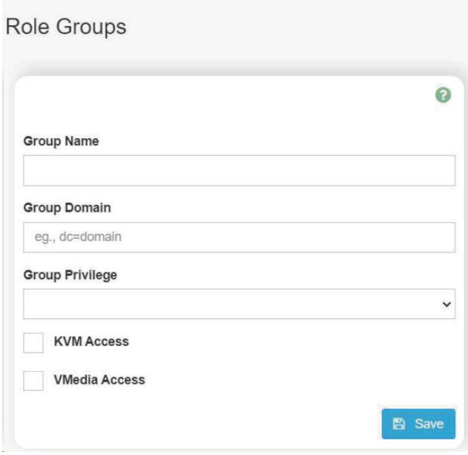
2. Click **Enable LDAP/E-Directory Authentication**, to enable LDAP/E-Directory Settings.
   Note: During login prompt, use username to login as an LDAP Group member.
3. Select the encryption type for LDAP/E-Directory from the Encryption Type.
   Note: Configure proper port number when SSL is enabled. For SSL connections, default port is 636. For No-Encryption & StartTLS, default port is 389.
4. Select the **Common Name Type** as **IP Address**.
5. Enter the IP address of LDAP server in the Server Address field.
   Note:
   IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
   Each Number ranges from 0 to 255.
   First Number must not be 0.
   Supports IPv4 Address format and IPv6 Address format.
   Configure FQDN address, when using StartTLS with FQDN.
6. Specify the LDAP Port in the **Port** field.
   Note:
   Default Port is 389. For SSL connections, default port is 636. The Port value ranges from 1 to 65535.
7. Specify the Bind DN that is used during bind operation, which authenticates the client to the server.

Note:
Bind DN is a string of 4 to 64 alpha-numeric characters.
It must start with an alphabetical character.
Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
Example: cn=manager, ou=login, dc=domain, dc=com

8. Enter the password in the **Password** field.
   Note:
   Password must be at least 1 character long.
   White space is not allowed.
   This field will not allow more than 48 characters.
9. Enter the **Search Base**. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory.
   Note:
   Search base is a string of 4 to 63 alpha-numeric characters.
   It must start with an alphabetical character.
   Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
   Example: ou=login, dc=domain, dc=com
10. Select **Attribute of User Login** to find the LDAP/E-Directory server which attribute should be used to identify the user.
    Note: It only supports cn or **uid**.
11. Select **CA Certificate File** from the Browse field to identify the certificate of the trusted CA certs.
12. Select the Certificate File to find the client certificate filename.
13. Select Private Key to find the client private key filename.
    Note: All the 3 files are required, when StartTLS is enabled.
    Note: For the SSL section, the three certificate files are also supported, and it is optional to upload these three files.
14. Click **Save** to save the settings.

To add a new Role Group

1. In the LDAP/E-Directory Settings Page, Click Role Groups and select a blank row.
2. Click **Add Role Group** or alternatively double click on the blank row to open the Add Role group Page as shown in the screenshot below.



3. In the **Group Name** field, enter the name that identifies the role group.
4. In the **Group Domain** field. Enter the Role Group Domain where the role group is located.
   Note:
   Domain Name is a string of 4 to 64 alpha-numeric characters.
   It must start with an alphabetical character.
   Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
   Example: cn=manager, ou=login, dc=domain, dc=com
5. In the **Group Privilege** field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
6. Select the required options or both

- KVM Access
- VMedia Access

7. Click Save to save the new role group and return to the Role Group List.

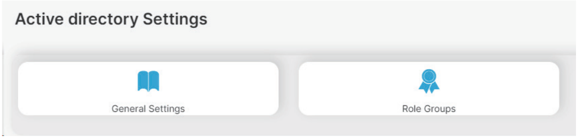
Active Directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as AD) does a variety of functions including the ability to provide information on objects. It also helps to organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

In Web GUI application, Active Directory allows you to configure the Active Directory Server Settings. The displayed table shows any configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group.

Note: To view the page, you must be at least a User and to modify or add a group, you must be an Administrator.

To open Active Directory Settings page, click Settings > Security > External User Settings > Active Directory from the menu bar. A sample screenshot of Active Directory Settings page is shown below.

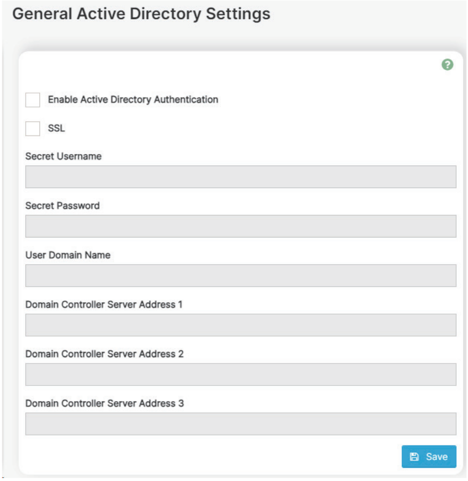


Active directory Settings

General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret Username, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.
Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure:

1. Click on **General Settings** to open the General Active Directory Settings Page.



General Active Directory Settings

□ Enable Active Directory Authentication

□ SSL

Secret Username

Secret Password

User Domain Name

Domain Controller Server Address 1

Domain Controller Server Address 2

Domain Controller Server Address 3

2. In the Active Directory Settings page, check or uncheck the Enable **Active directory Authentication** check box to enable or disable Active Directory Authentication respectively.
   Note:If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.
3. **SSL**: Check or uncheck to enable or disable the SSL.
4. Specify the Secret username and password in the Secret Username and Secret Password fields respectively.
   Note:

- Secret username/password for AD is not mandatory. When secret username & password is empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So, it is recommended to keep

AD in the last location in PAM order.

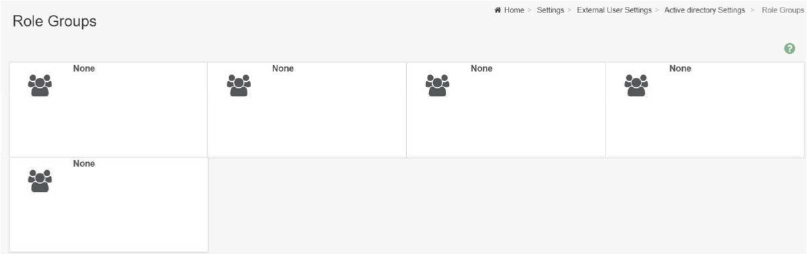
- User Name is a string of 1 to 64 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.
- Password must be at least 6 character long and will not allow more than 127 characters.
- White space is not allowed.

5. Specify the Domain Name for the user in the **User Domain Name** field. E.g. MyDomain.com
6. Configure IP addresses in **Domain Controller Server Address1, Domain Controller Server Address2** and Domain Controller **Server Address3**

   Note:
   - IP address of Active Directory server: At least one Domain Controller Server Address must be configured.
   - IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
   - Each number ranges from 0 to 255.
   - First number must not be 0.
7. Click **Save** to save the entered settings and return to Active Directory Settings Page.

Role Groups

To open Role Group page, click **Settings > Security > External User Settings > Active Directory > Role Groups** from the menu bar. A sample screenshot of Role Groups page is shown below.


Role Groups

Home > Settings > External User Settings > Active directory Settings > Role Groups

None

None

None

None

None

The fields of Role Group page are explained below.

Role Group Name: The name that identifies the role group in the Active Directory.

Note:
Role Group Name is a string of 64 alpha-numeric characters.
Special symbols hyphen and underscore are allowed.

Group Domain: The domain where the role group is located.

Note:
Domain Name is a string of 255 alpha-numeric characters.
Special symbols hyphen, underscore and dot are allowed.

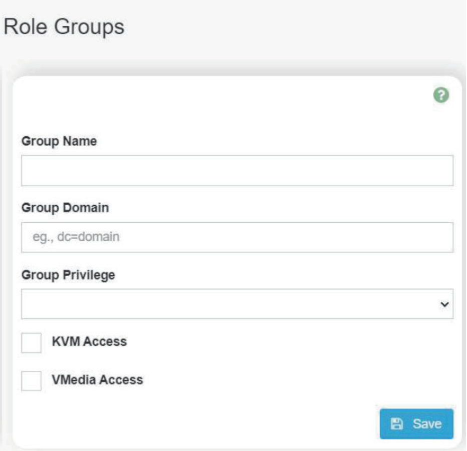
Group Privilege: The level of privilege to assign to this role group.

KVM Access: To provide access to KVM for AD authenticated role group user.

VMedia Access: To provide access to VMedia for AD authenticated role group user.

To add a new Role Group

1. In the Active Directory Settings Page, select a Role Group and click Add Role Group or alternatively double click on the blank row to open the Add Role Group Page as shown in the screenshot below.



Role Groups

Group Name

Group Domain

eg., dc=domain

Group Privilege

□ KVM Access

□ VMedia Access

2. In the Group Name field, enter the name that identifies the role group in the Active Directory.
   Note:
   - Role Group Name is a string of 64 alpha-numeric characters.
   - Special symbols hyphen and underscore are allowed.
3. In the Group Domain field, enter the domain where the role group is located.
   Note:
   - Domain Name is a string of 255 alpha-numeric characters.
   - Special symbols hyphen, underscore and dot are allowed.
4. In the **Group Privilege** field, enter the level of privilege to assign to this role group.
5. Select the required options

- KVM Access
- VMedia Access

6. Click Save to add the

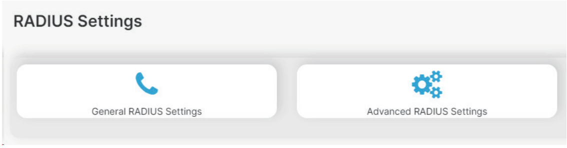
6. Click Save to add the new role group and return to the Role Group List.

To Delete a Role Group

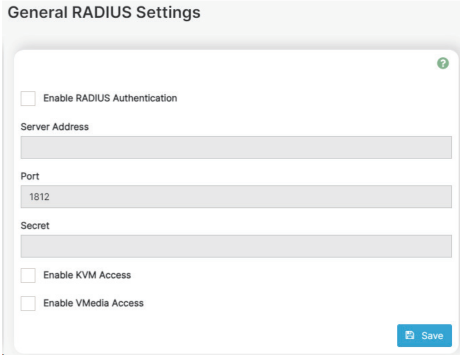
1. In the Role Groups Page, select the row that you wish to delete.
2. Click **Delete Role Group**.

RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.
In Web GUI, this page is used to set the RADIUS Authentication.
To open RADIUS Settings page, click **Settings > Security > External User Settings > RADIUS Settings** from the menu ar. A sample screenshot of RADIUS Settings Page is shown below.



General RADIUS Settings



General RADIUS Settings

□ Enable RADIUS Authentication

Server Address

Port

1812

Secret

□ Enable KVM Access

□ Enable VMedia Access

The fields of General RADIUS Settings Page are explained below.
Enable RADIUS Authentication: Option to enable/disable RADIUS authentication.
Server Address: The IP address of RADIUS server.

Note:
IP Address (Both IPv4 and IPv6 format).
FQDN (Fully Qualified Domain Name) format.

Port: The RADIUS Port number.

Note:
Default Port is 1812.
Port value ranges from 1 to 65535.

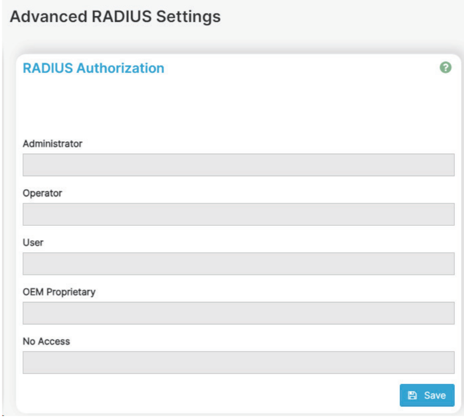
Secret: The Authentication Secret for RADIUS server.

Note:
This field will not allow more than 31 characters.
Secret must be at least 4 characters long.
White space is not allowed.

Enable KVM Access: This field provides access to KVM for RADIUS authenticated users.
Enable VMedia Access: This field provides access to VMedia for RADIUS authenticated users.
Save: To save the settings.

Procedure

1. Enable the RADIUS Authentication check box to authenticate the RADIUS.
2. Click Advanced RADIUS Settings. This opens the Radius Authorization window as shown below.



Advanced RADIUS Settings

RADIUS Authorization

Administrator

Operator

User

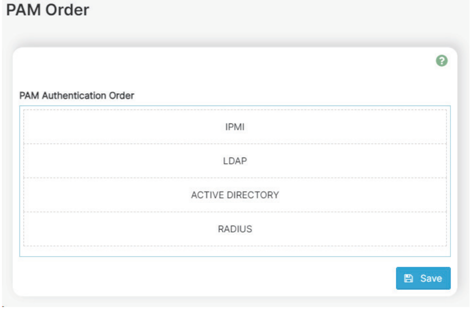
OEM Proprietary

No Access

3. Click **Save** to save the changes made.
   Note: For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.
   Example:1
   testadmin Auth-Type :=PAP, Cleartext-Password:=”admin”
   Auth-Type :=PAP, Vendor-Specific=”H=4”
   Example:2
   testoperator Auth-Type := PAP, Cleartext-Password := “operator”
   Auth-Type :=PAP, Vendor-Specific=”H=3”
   If you change the Vendor-Specific value in server then you should change the same values in this page.

2-5-3-2 PAM Order Settings

This page is used to configure the PAM ordering for user authentication into the BMC.
To open PAM Ordering page, click **Settings > Security > PAM Order Settings** from the menu bar. A sample screenshot of PAM Order Page is shown below.



PAM Order

PAM Authentication Order

IPMI

LDAP

ACTIVE DIRECTORY

RADIUS

The fields of **PAM Ordering** page are explained below.
PAM Module: It shows the list of available PAM modules supported in BMC.

Note: It is recommended to not to keep same username for different PAM modules.
If Authentication fails, the reason of fail could be invalid User or Invalid Password.
If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So, it is always treated as Invalid username error and PAM will try other Authentication Methods.
If AD contains secret username & password as empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended to keep AD in the last location in PAM order.

Procedure

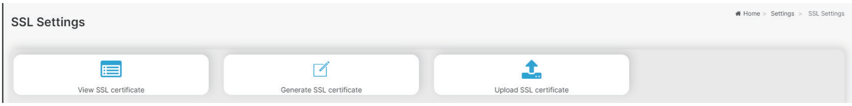
1. Select the required PAM module and click and drag the required PAM module. It can be moved UP or DOWN to change its arrangement order.
2. Click Save to save any changes made.
   Note: Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.

2-5-3-3 SSL Settings

The Secure Socket Layer protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions.

Using Web GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open SSL Certificate Configuration page, click **Settings > Security > SSL Settings** from the menu bar. There are three tabs in this page.



The fields of SSL Settings – Upload SSL Settings tab are explained below.

Current Certificate: Current certificate and uploaded date/time will be displayed (read-only).

New Certificate: Certificate file should be of pem type.

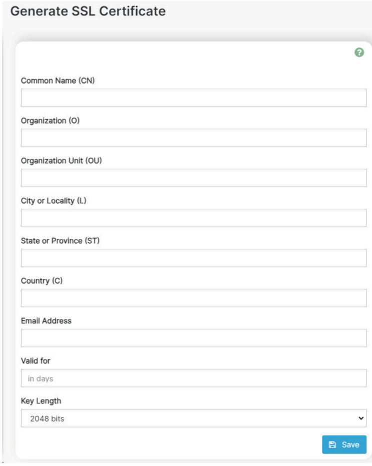
Current Private Key: Current Private key information will be displayed (read-only).

New Private Key: Private key file should be of pem type.

Current trusted CA Certificate: Current trusted CA certificate and uploaded date/time will be displayed (read-only).

Trusted CA Support: If the Trusted CA Support checkbox is enabled then user can able to upload the Trusted CA Certificates in BMC, otherwise user can able to upload New Certificate & New Private key only.

> **Note**: If Redfish feature is disabled, Trusted CA Support checkbox wi te and privacy key into the BMC.
>
> **Note**: After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.



Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for: in days

Key Length: 2048 bits

Save

The fields of SSL Settings – Generate SSL Certificate are explained below.

Common Name(CN): Common name for which certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization(O): Organization name for which the certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

City or Locality(L): City or Locality of the organization (mandatory).

- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

State or Province(ST): State or Province of the organization (mandatory).

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Country(C): Country code of the organization (mandatory).

- Only two characters are allowed.
- Special characters are not allowed.

Email Address: E-mail Address of the organization (mandatory).

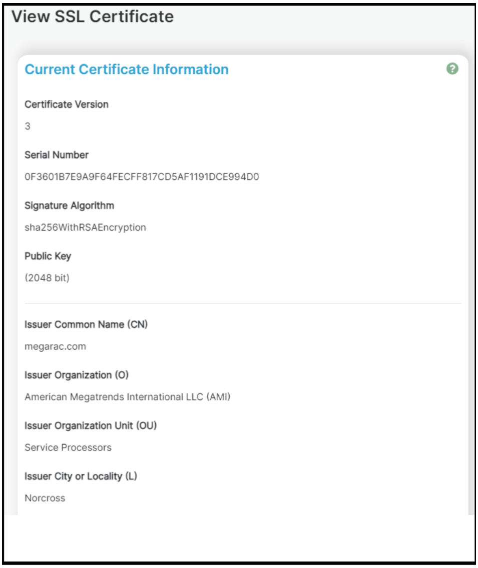
Valid for: Validity of the certificate.

- Value ranges from 1 to 3650 days.

Key Length: The key length bit value of the certificate.

Save: To generate the new SSL certificate.

Note: HTTPs service will get restarted, to use the newly generated SSL certificate.



View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

0F3601B7E9A9F64FECFF817CD5AF1191DCE994D0

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

megarac.com

Issuer Organization (O)

American Megatrends International LLC (AMI)

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Norcross

The fields of SSL Settings – View SSL Certificate are explained below.
Basic Information: This section displays the basic information about the uploaded SSL certificate. It displays the following fields.

- Version Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name(CN)
- Issuer Organization(O)
- Issuer Organization Unit(OU)
- Issuer City or Locality(L)
- Issuer State or Province(ST)
- Issuer Country(C)
- Issuer E-mail Address
- Valid From
- Valid Till
- Issued to Common Name(CN)
- Issued to Organization(O)
- Issued to Organization Unit(OU)
- Issued to City or Locality(L)
- Issued to State or Province(ST)
- Issued to Country(C)
- Issued to E-mail Address

Procedure

1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.

3. In Generate SSL Certificate, enter the following details in the respective fields.

- The Common Name for which the certificate is to be generated.
- The Organization for which the certificate is to be generated.
- The Organization Unit name for which certificate to be generated.
- The City or Locality of the organization
- The State or Province of the organization
- The Country of the organization
- The Email address of the organization.
- The number of days the certificate will be valid in the Valid For field.

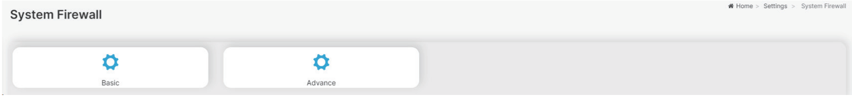
4. Choose the Key Length bit value of the certificate
5. Click Save to generate the certificate.
6. Click View SSL Certificate tab to view the uploaded SSL certificate in user readable format.

Note:

- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your Generic BMC securely using the following format in your IP Address field from your Internet browser: https://<your BMC's IP address here>
- For example, if your BMC's IP address is 192.168.0.30, enter the following: https://192.168.0.30
- Please note the <s> after <http>. You must accept the certificate before you are able to access your Generic BMC.

2-5-3-4 System Firewall

In Web GUI, the System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.
To open System Firewall page, click **Settings > Security > System Firewall** from the menu bar.

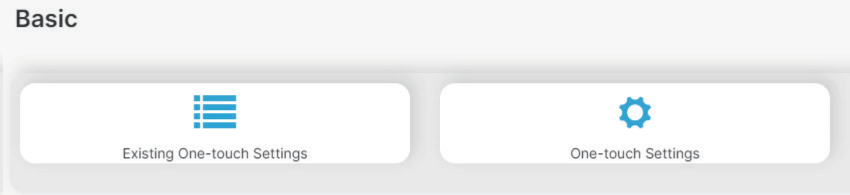


- Basic
  - Existing One-touch Settings
  - One-touch Settings
- Advance
  - General Firewall Settings
  - IP Address Firewall Rules
  - Port Firewall Rules

A detailed description of the menu items is given below.

Basic

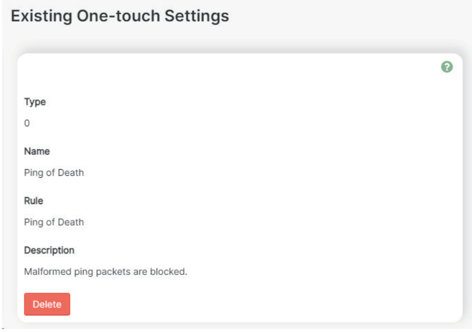
This page is used to configure the One-touch settings. A sample screenshot of Basic is given below.



Existing One-touch Settings

This page is used to configure the One-touch settings. A sample screenshot of Basic is given below.

A blank page will be opened if you did not add anything in “One-touch settings”. If there is no One-touch Settings
Exists, add a new One-touch settings by clicking link One-touch Settings page.



Existing One-touch Settings

Type
0

Name
Ping of Death

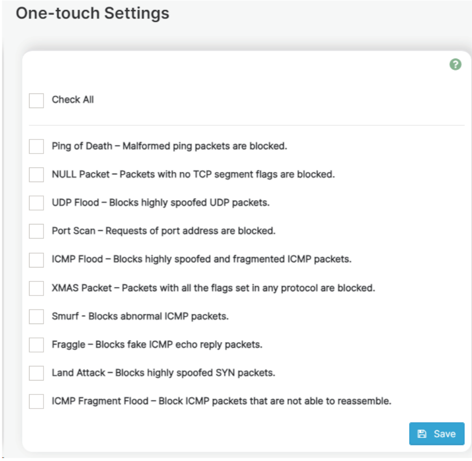
Rule
Ping of Death

Description
Malformed ping packets are blocked.

Type: The type of the one-touch setting.
Name: The name of the one-touch setting.
Rule: The rule of the setting.
Description: The description of the one-touch setting.
Delete: To delete the one-touch setting.

Add One-touch Settings

1. Click **Basic > One-touch Settings**. This opens the One-touch Settings page as shown below.



One-touch Settings

□ Check All

□ Ping of Death – Malformed ping packets are blocked.
□ NULL Packet – Packets with no TCP segment flags are blocked.
□ UDP Flood – Blocks highly spoofed UDP packets.
□ Port Scan – Requests of port address are blocked.
□ ICMP Flood – Blocks highly spoofed and fragmented ICMP packets.
□ XMAS Packet – Packets with all the flags set in any protocol are blocked.
□ Smurf - Blocks abnormal ICMP packets.
□ Fraggle – Blocks fake ICMP echo reply packets.
□ Land Attack – Blocks highly spoofed SYN packets.
□ ICMP Fragment Flood – Block ICMP packets that are not able to reassemble.

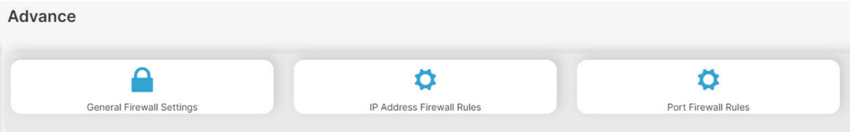
Check All: Select all the options below.
Ping of Death: Malformed ping packets are blocked.
NULL Packet: Packets with no TCP segment flags are blocked.
UDP Flood: Blocks highly spoofed UDP packets.
Port Scan: Requests of port address are blocked.
ICMP Flood: Blocks highly spoofed and fragmented ICMP packets.
XMAS Packet: Packets with all the flags set in any protocol are blocked.
Smurf: Blocks abnormal ICMP packets.

Fraggle: Blocks fake ICMP echo reply packets.
Land Attack: Blocks highly spoofed SYN packets.
ICMP Fragment Flood: Block ICMP packets that are not able to reassemble.

2. Select the box of options required.
3. Click Save to save the configuration.

Advance

This page is used to configure firewall settings. A sample screenshot of Advance is given below.



General Firewall Settings

Click **General Firewall Settings** page. A sample screenshot of General Firewall Settings page is shown below.

The fields of **Firewall Settings** tab are explained below.

Existing Firewall Settings

A blank page will be opened if you did not add anything in “Add Firewall settings”. If there is no Firewall Settings

Exists, add a new firewall setting by clicking link Add Firewall Settings page.

Procedure

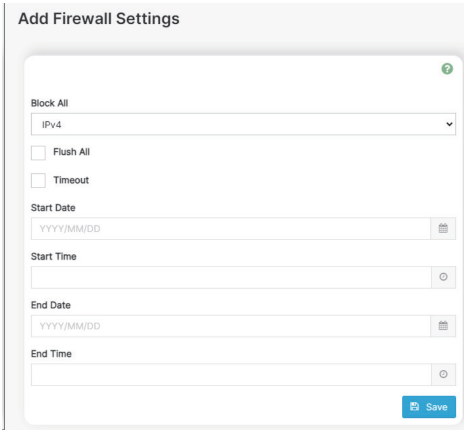
To add Firewall settings

Click General **Firewall Settings > Existing Firewall Settings** icon. A sample screenshot of Existing Firewall Settings page is shown below.

- Block All: The blocked incoming IP’s and Port’s can be viewed.
- Flush All: To flush all the system firewall rules (Read-Only).
- Select Timeout to enable or disable firewall rules with timeout.
- Time Out : The respective firewall rule effect Start Time, End Date, Start Time, End Time will be displayed.
- Delete: To Delete the system firewall rules.

Add Firewall Settings

1. Click **General Firewall Settings > Add Firewall Settings**. This opens the Existing Firewall Settings page as shown below.



Add Firewall Settings

Block All

IPv4

□ Flush All

□ Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

YYYY/MM/DD

End Time

2. Select Block All to block all the incoming IP's and Port's.
3. Select Flush All to flush all the system firewall rules.
4. Select Timeout to enable or disable firewall rules with timeout.
5. Enter Start Time to start the respective firewall rule effect from this time.
6. Enter End Time to end the respective firewall rule effect from this time.
   Note: The time should be in the dd-mm-yy:hh-mm format.
7. Click Save to save the changes made else click Cancel to go back to the previous screen.

IP Address Firewall Rules

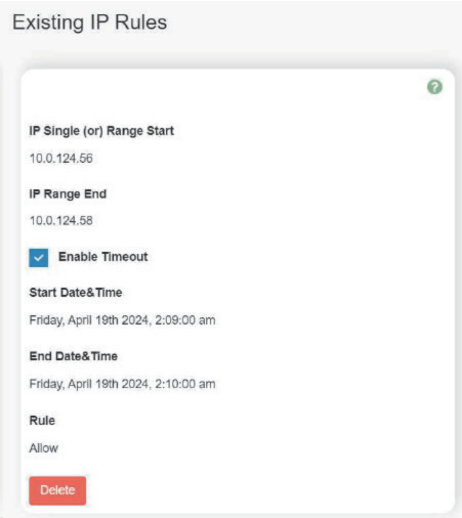
To View Existing IP Rules or a range of IP Addresses,

A blank page will be opened if you did not add anything in "Add IP Rule". If there is no Add IP Rule Exists, add a new
IP Rule by clicking link **Add IP Rule** page.

Procedure

To add IP Rule

1. Click **Settings** > **Security** > **System Firewall** > **Advance** > **IP Address Firewall Rules** > **Existing IP Rules**. A blank page will be opened if you did not add anything in "Add IP Rule". If any rule is added, then the added rule will be listed in "Existing IP Rules" page.
2. Click the IP Addresses tab. A sample screenshot of **IP Addresses** tab is shown below.



Existing IP Rules

IP Single (or) Range Start

10.0.124.56

IP Range End

10.0.124.58

☑ Enable Timeout

Start Date&Time

Friday, April 19th 2024, 2:09:00 am

End Date&Time

Friday, April 19th 2024, 2:10:00 am

Rule

Allow

IP Single (or) Range Start : To show the configured Port Address or Range of Ports.
IP Range End : To show the configured Port Address or Range of Ports.
Enable Timeout : To enable/disable Timeout.
Start Date : The respective firewall rule effect will start from this date.
Start Time : The respective firewall rule effect will start from this time.
End Date : The respective firewall rule effect will end from this date.
End Time : The respective firewall rule effect will end from this time.
Rule: To indicate the current setting.
Delete: To delete the selected slot.

Procedure

To add an IP address or range of IP addresses,

1. Click Settings > Security > System Firewall > Advance > IP Address Firewall Rules > Add New IP Rule to add a new IP or range of IP address.
2. In the Add new rule for IP page, Enter the IP address and a range of IP addresses in the IP Single or IP Range Start field.

   Note: - IP Address will support IPv4 Address format only:

- IPv4 Address made of 4 numbers separated by dots as in xxx.xxx.xxx.xxx.
- Each number ranges from 0 to 255.
- First number must not be 0.
- IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

3. Enter IP range end value in the IP Range End field.
4. Enable Timeout to enable firewall rules with timeout.
5. Enter Start Date to start the respective firewall rule effect from this date.
6. Enter End Date to end the respective firewall rule effect from this date.
7. Enter Start Time to start the respective firewall rule effect from this time.
8. Enter End Time to end the respective firewall rule effect from this time.

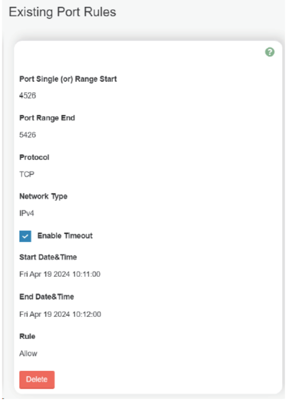
Note: The date and time should be in the YYYY/MM/DD and hh-mm format respectively.

9. Determine the rule to block or accept.
10. Click Save to save the changes made.

Port Firewall Rules

To view Existing Port Rules

Click **Settings > Security > System Firewall > Advance > Port Firewall Rules > Existing Port Rules**. A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page. A sample screenshot of Port tab is shown below.



Existing Port Rules

Port Single (or) Range Start
4526

Port Range End
5426

Protocol
TCP

Network Type
IPv4

☑ Enable Timeout

Start Date&Time
Fri Apr 19 2024 10:11:00

End Date&Time
Fri Apr 19 2024 10:12:00

Rule
Allow

The fields of System Firewall - Existing Port Rules page are explained below.

Port Single (or) Range Start : To configure the Port or Range of Port Addresses.

Port Range End :To configure the Port or Range of Port Addresses.

Protocol : This field specifies the protocols for the configured Port or Port Ranges.

Network Type : This field specifies the affected network type for the particular Port or Port Ranges.

Enable Timeout :To enable or disable firewall rules with timeout.

Start Date : The respective firewall rule effect will start from this time.

Start Time : The respective firewall rule will start from this time.

End Date : The respective firewall rule effect will end on this date.

End Time : The respective firewall rule will end at this time.

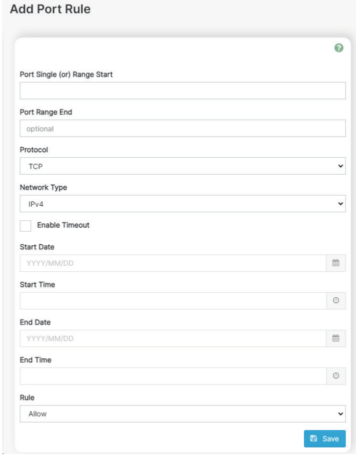
Rule : To indicate **Allow** or **Block** status.

Delete : To delete the entry to the firewall rules list.

Procedure

To Add Port/Range of ports

1. To add a new rage of Port address, click the **Add** button.



Add Port Rule

Port Single (or) Range Start

Port Range End: optional

Protocol: TCP

Network Type: IPv4

□ Enable Timeout

Start Date: YYYY/MM/DD

Start Time

End Date: YYYY/MM/DD

End Time

Rule: Allow

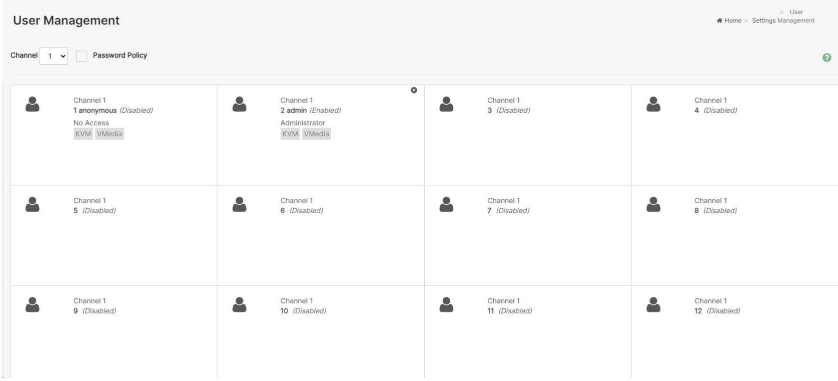
Save

2. In the Add new rule for Port window, enter the port number or a range of port numbers in the Port Single (or) Range Start field.
   Note: Port value ranges from 1 to 65535.
3. Enter the end value in the Port Range End field.
4. Select the Protocol to be either TCP or UDP or Bot.
5. Select the Network Type. It may be IPv4 or IPv6 or Both.
6. Select Timeout to enable or disable firewall rules with timeout.
7. Enter Start Time to start the respective firewall rule effect from this time.
8. Enter Start Date to start the respective firewall rule effect from this date.
9. Enter End Date to end the respective firewall rule effect on this date.
10. Enter End Time to end the respective firewall rule effect at this time.
    Note: The time should be in the YYYY/MM/DD:hh-mm format.
11. Select the Rule to determine the rule to Block or Allow.
12. Click Save to save the changes made.

2-5-3-5 User Management

In Web GUI, the User Management 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 **Settings > Security > User Management** from the menu bar. A sample screenshot of User Management Page is shown below.



User Management

Home > Settings > User Management

Channel 1 □ Password Policy

Channel 1 1 anonymous *(Disabled)* No Access KVM VMedia	Channel 1 2 admin *(Enabled)* Administrator KVM VMedia	Channel 1 3 *(Disabled)*	Channel 1 4 *(Disabled)*
Channel 1 5 *(Disabled)*	Channel 1 6 *(Disabled)*	Channel 1 7 *(Disabled)*	Channel 1 8 *(Disabled)*
Channel 1 9 *(Disabled)*	Channel 1 10 *(Disabled)*	Channel 1 11 *(Disabled)*	Channel 1 12 *(Disabled)*

Click user icon 👤 and select any free slot to add a new user from the User Management main page.

Click Delete icon (x) on the top right corner to directly delete an item from the list.

Note: The Free slots are shown as “Disabled” in all columns for the slot.

The fields of User Management Page are explained below.

Channel: To choose a particular channel from the available channel list.

User ID: Displays the ID number of the user.

Note: The list contains a maximum of ten users only.

Username: Displays the name of the user.

User Access: To enable or disable the access privilege of the user.

Network Privilege: Displays the network access privilege of the user.

SNMP Status: Displays if the SNMP status for the user is enabled or Disabled.

E-mail ID: Displays e-mail address of the user.

Add User: To add a new user.

Delete User: To delete an existing user.

Password Policy: To enable or disable using password policy.

Note: Password field is mandatory and should have a minimum of 6 characters. If Password Policy is checked.

Password is composed of numbers, uppercase and lowercase letters, and special characters. The length of password must be at least 8 characters and cannot be the same as 3 characters in succession of Name.

Procedure

To add a new User

1. To add a new user, select a free section and click on the empty section. This opens the Add User screen as shown in the screenshot below.
2. Enter the name of the user in the Username field.

   Note:

- User Name is a string of 1 to 16 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters '-'(hyphen), '_'(underscore), '@'(at sign), '.'(dot) are allowed.
- For 20 Bytes password, LAN session will not be established.

3. Set Password Size for the new password.
4. In the Password and Confirm Password fields, enter and confirm your new password.

Note:

- Password should be the combination of alphabets, numbers, symbol and upper-case characters.
- White space is not allowed.
- This field will not allow more than 16/20 characters based on Password size field value.
- This field will not allow the below mentioned characters.
- The password should be a string, if you try to set password using "ipmitool user set password".

5. In Enable User Access, select this option to enable the network access for the appropriate user.

   Note:

- Enabling User Access will intern assign the IPMI messaging privilege to user.
- It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, while creating User through IPMI.

6. In Enable Channel Access field, select the channel/channels to enable the network access for the appropriate channels.
7. In the Privilege field, enter the privilege assigned to the user which could be Administrator, Operator, User, OEM or None.
8. Check KVM Access to assign the KVM privilege for the user.
9. Check VMedia Access assign the Vmedia privilege for the user.

   Note: It is recommended that the privileges support to KVM and Vmedia should be provided only to the ADMIN user and shouldn't be provided to USER and OPERATOR privilege level users. The Admin user can provide the privilege support to USER and OPERATOR privilege level users at their own risk.

   Vmedia Privilege only restricts initiating / starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions. Which includes 'KVM Privilege only' sessions as well.

10. Check the SNMP Access check box to enable SNMP access for the user.

    Note: Password field is mandatory if SNMP Status is enabled.

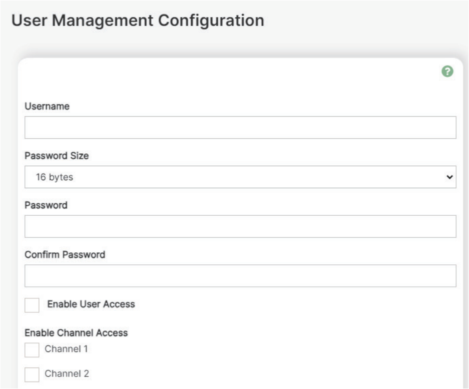
11. Choose the SNMP View from the drop-down list - this feature is for the security of access and the SNMP view is added to prevent the SNMP users from accessing the data with excessive privileges. In the SNMP View drop-down list, select the assigned SNMP user which could be

Administrator, Operator, User or OEM.
Note: SNMP View field is mandatory, if SNMP Status is enabled.

12. Choose the SNMP Access level option for user from the SNMP Access level (SHA) drop-down list. Either it can be Read Only or Read Write.
13. Choose the SNMP Authentication Protocol (SHA) to use for SNMP settings from the drop-down list.Note: Password field is mandatory if Authentication protocol is changed.
14. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol (AES or DES) dropdown list.
15. In the Email ID field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.
    Note: SMTP Server must be configured to end emails.
    Email Format: Two types of formats are available:
    AMI-Format: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.
    Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.
16. Click Save to save the new user and return to the users list.

To Modify User

1. To modify the existing user, click on the active user tab. This opens a User screen as shown in the screenshot below.



User Management Configuration

Username

Password Size
16 bytes

Password

Confirm Password

□ Enable User Access

Enable Channel Access
□ Channel 1
□ Channel 2

2. Enter the Username in the given field.
3. Mention the same password which is initially given to the login page in Logged-In Password field.
   Note: User must enter the logged-in password again for confirmation. If it is successful only, user modifying operation can be done otherwise error message will pop-up.
4. Check Change Password, if you wish to change the existing Password.
   Note: If user login with admin and testuser in two different Web-Browsers and change the pass word for testuser account from admin account then the testuser account will automatically get logged-out from Web-Browser where the testuser is logged in.

5. Follow the steps (3 to 15) of Procedure to add a new User.
6. Click Save to save the changes and return to the users list.
7. Click Delete to delete the user.

    Note:

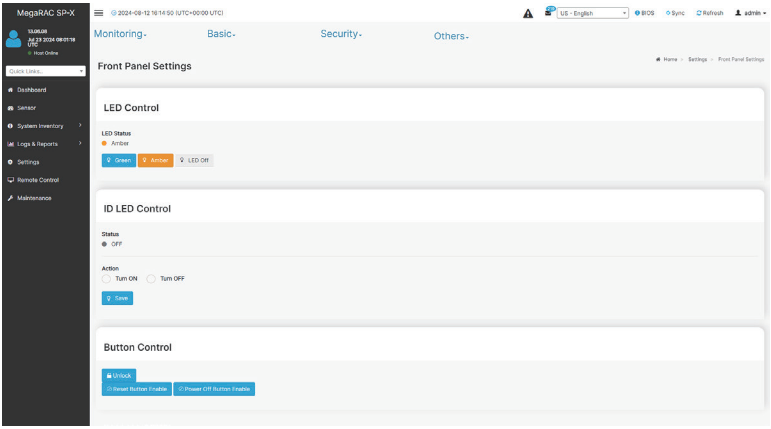
    Reserved Users: There are certain reserved users which cannot be added as BMC Users. The list of reserved users is

    given below,

- sysadmin
- daemon
- ntp
- root

2-5-3-6 Front Panel Settings

This page is used to configure Front Panel Settings. To open User Management page, click **Settings > Security > Front Panel Settings** from the menu bar. A sample screenshot of Front Panel Settings Page is shown below.



LED Status
● Amber

Status
● OFF

LED Control

LED Status: Display the status of LED.
Green: Change the LED to green.
Amber: Change the LED to amber.
LED Off: Turn off the LED.

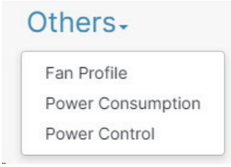
ID LED Control

Status: Display the status of ID LED.
Action: Turn on or Turn of the ID LED.
Save: To save the configuration.

Button Control

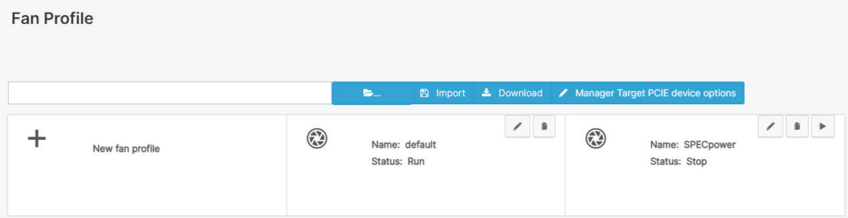
Unlock: Unlock all the buttons.
Reset Button Disable: Disable the Reset button.
Power Off Button Disable: Disable the Power Off button.

2-5-4 Others



2-5-4-1 Fan Profile

This page can edit fan profile settings in this page.

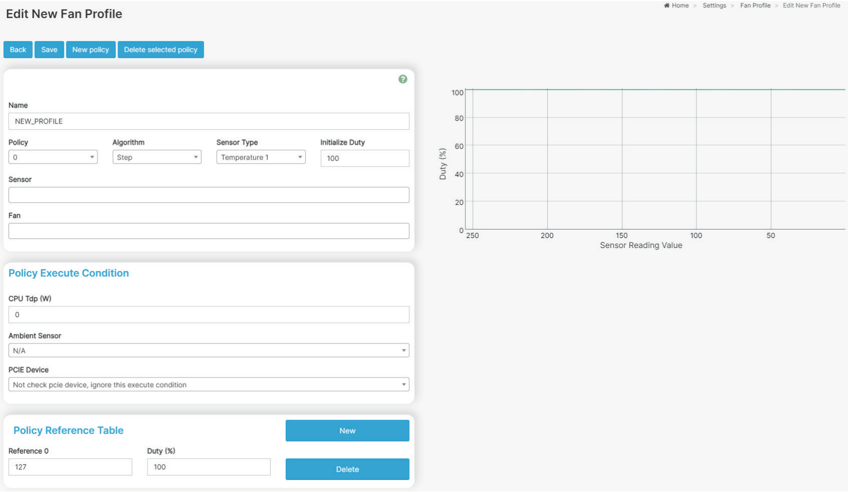

Fan Profile

Name: default
Status: Run

Name: SPECpower
Status: Stop

📂... **& Import**: To upload and import the configuration.
Download: To download the current configurations.
Manager Target PCIE device options: To modify Manager Target PCIE device options.

Edit New Fan Profile


Edit New Fan Profile

Name: NEW_PROFILE

Policy: 0
Algorithm: Step
Sensor Type: Temperature 1
Initialize Duty: 100

Sensor:

Fan:

Policy Execute Condition

CPU Tdp (W): 0

Ambient Sensor: N/A

PCIE Device: Not check pcie device, ignore this execute condition

Policy Reference Table

Reference 0: 127
Duty (%): 100

Back: To go back to the previous page.
Save: To save the configuration.
New Policy: To add a new policy.
Delete selected policy: To delete the selected policy.
Name: The name of the fan profile.
Policy: To select the policy.
Algorithm: To select the algorithm.
Sensor Type: To select the sensor type.
Initialize Duty: The initialize duty.
Senor: The sensor to be detected.
Fan: The fan to be used with this profile.

Policy Execute Condition

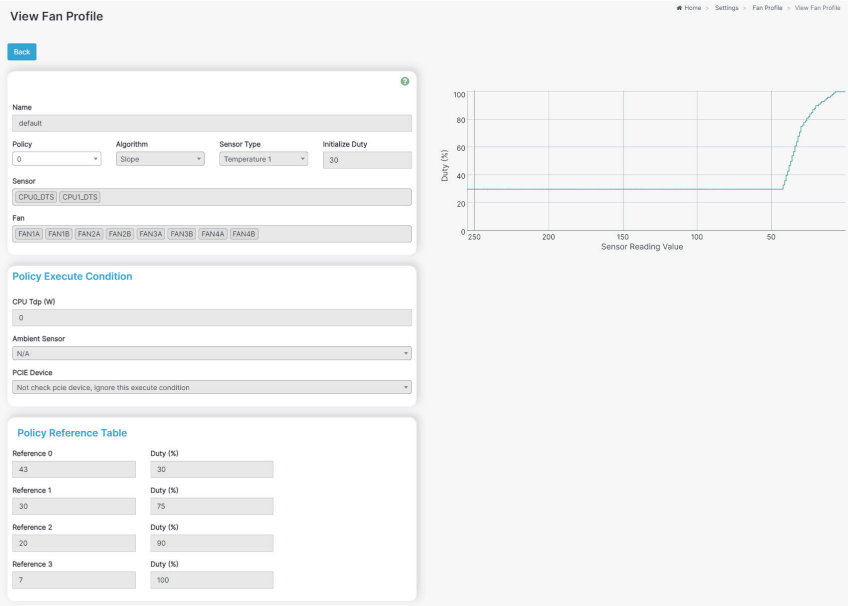
CPU Tdp (W): The TDP of the CPU.
Ambient Sensor: The sensor to be detected.
PCIE Device: To execute the policy based on the presence or absence of the PCIE device.

Policy Reference Table

New: To add a new reference and duty.
Delete: To delete the reference and duty.
Reference: The sensor value.
Duty: The target duty.

View Fan Profile

This page displays the configuration of the fan profile.



View Fan Profile

Name: default

Policy: 0
Algorithm: Slope
Sensor Type: Temperature 1
Initialize Duty: 30

Sensor: CPU0_DTS CPU1_DTS

Fan: FAN1A FAN1B FAN2A FAN2B FAN3A FAN3B FAN4A FAN4B

Policy Execute Condition

CPU Tdp (W): 0

Ambient Sensor: N/A

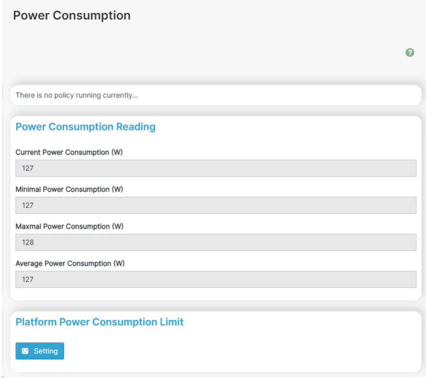
PCIE Device: Not check pcie device, ignore this execute condition

Policy Reference Table

Reference 0: 43	Duty (%): 30
Reference 1: 30	Duty (%): 75
Reference 2: 20	Duty (%): 90
Reference 3: 7	Duty (%): 100

2-5-4-2 Power Consumption

On this page you can look current power consumption reading, current execute power limit policy, and configuration power limit.



Power Consumption

There is no policy running currently...

Power Consumption Reading

Current Power Consumption (W)

127

Minimal Power Consumption (W)

127

Maxmal Power Consumption (W)

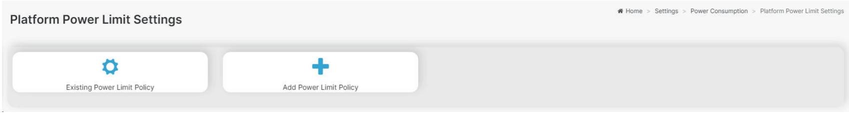
128

Average Power Consumption (W)

127

Platform Power Consumption Limit

Platform Power Consumption Limit Settings include the Existing Power Limit Policy page and the Add Power Limit Policy page.

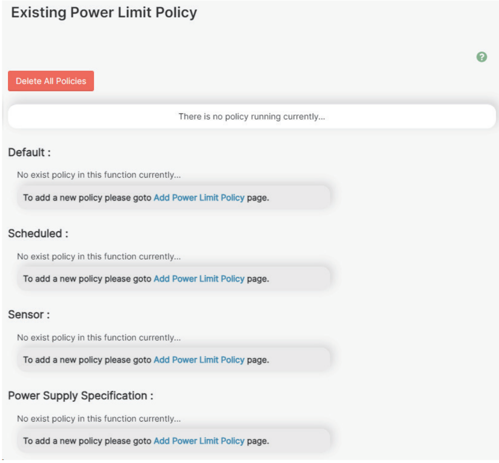


Platform Power Limit Settings

Home > Settings > Power Consumption > Platform Power Limit Settings
Existing Power Limit Policy
Add Power Limit Policy

Existing Power Limit Policy

This page includes all the power limit policy settings and the current execute policy.



Existing Power Limit Policy

There is no policy running currently...

Default :

No exist policy in this function currently...

To add a new policy please goto Add Power Limit Policy page.

Scheduled :

No exist policy in this function currently...

To add a new policy please goto Add Power Limit Policy page.

Sensor :

No exist policy in this function currently...

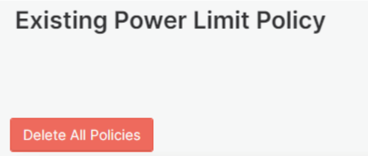
To add a new policy please goto Add Power Limit Policy page.

Power Supply Specification :

No exist policy in this function currently...

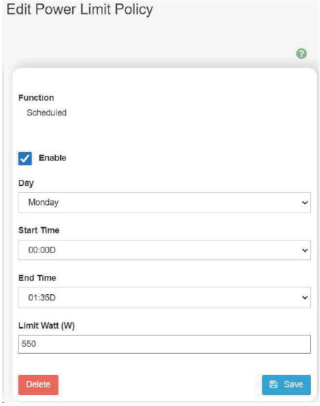
To add a new policy please goto Add Power Limit Policy page.

Click the “**Delete All Policies**” button can delete all policy settings.



Existing Power Limit Policy

If you want to modify the policy, you can click the setting policy to modify.



Edit Power Limit Policy

Function
Scheduled

☑ Enable

Day: Monday

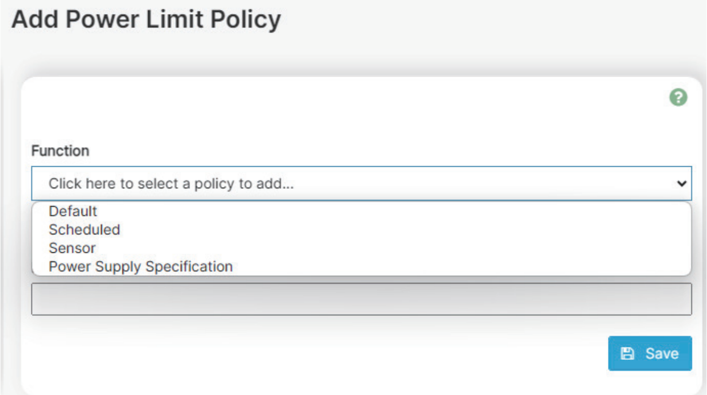
Start Time: 00:00D

End Time: 01:35D

Limit Watt (W): 550

Add Power Limit Policy

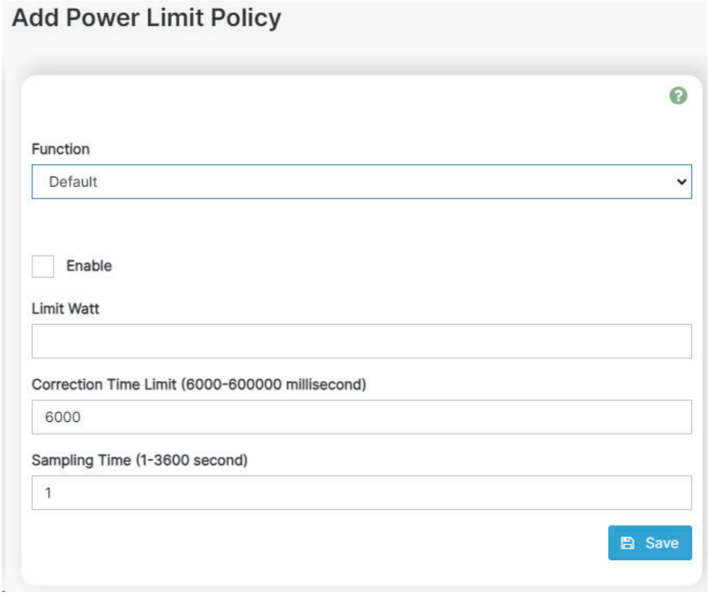
This page can add new power limit policy settings, including Default, Scheduled, Sensor, and Power Supply Specification functions.



Add Power Limit Policy

Function: Click here to select a policy to add...

(a) Default function



Add Power Limit Policy

Function

Default

□ Enable

Limit Watt

Correction Time Limit (6000-600000 millisecond)

6000

Sampling Time (1-3600 second)

1

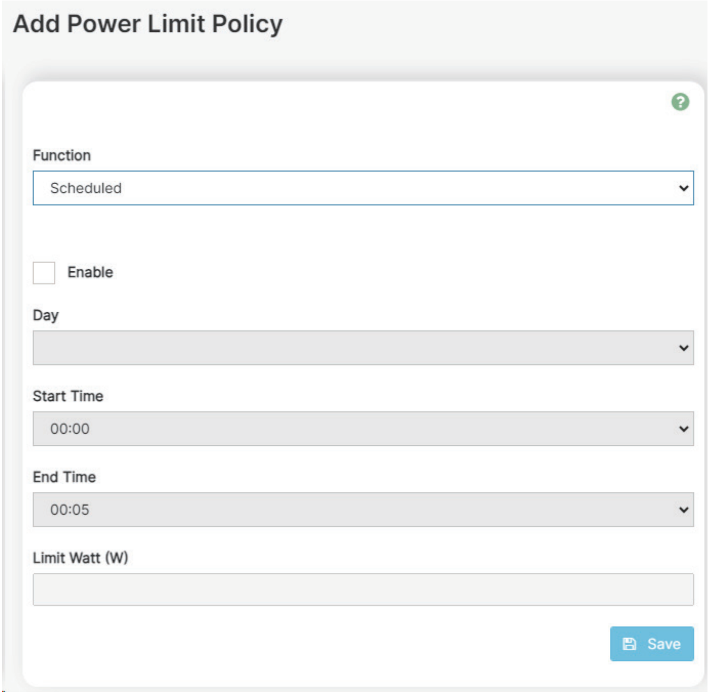
Limit Watt: Power Limit Requested in [Watts].

Correction Time Limit: Correction time limit in milliseconds. Maximum time taken to limit the power, otherwise, exception action will be taken as configured. The Exception Action shall be taken if the system power usage constantly exceeds the specified power limit for more than the Correction Time Limit interval. The Correction Time Limit timeout automatically restarts if the system power meets or drops elow the Power Limit.

Sampling Time: Management application Statistics Sampling period in seconds.

Exception Action: Exception actions. Actions are taken if the power limit is exceeded and cannot be controlled within the correction time limit.

(b) Scheduled function



Add Power Limit Policy

Function: Scheduled

□ Enable

Day:

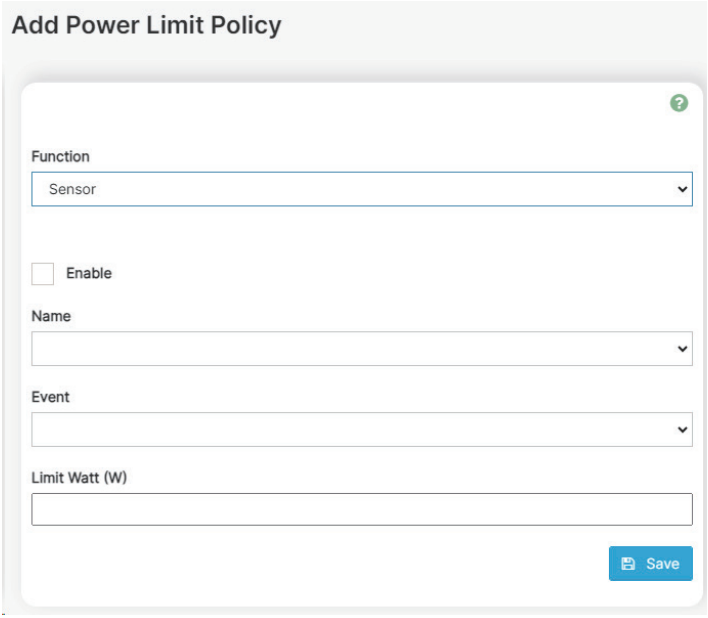
Start Time: 00:00

End Time: 00:05

Limit Watt (W):

Day: Monday – Sunday
Start Time: Start executing Scheduled Policy time (each 6 min as a unit).
End Time: Exit execute Scheduled Policy time (each 6 min as a unit).
Limit Watt: Power Limit Requested in [Watts].
*The interval between start time and end time must be greater than or equal to 12 minutes
**scheduled function must click the enable button to save the settings

(c) Sensor function


Add Power Limit Policy

Function

Sensor

□ Enable

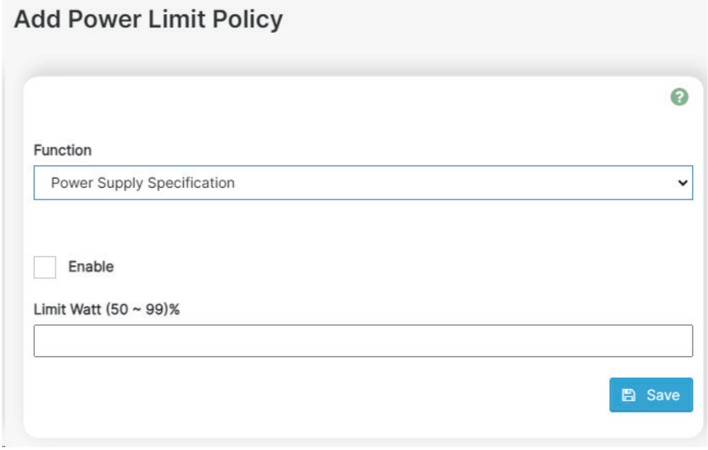
Name

Event

Limit Watt (W)

Name: Sensor name
Event: Sensor critical event condition
Limit Watt: Power Limit Requested in [Watts]

(d) Power Supply Specification function



Add Power Limit Policy

Function: Power Supply Specification

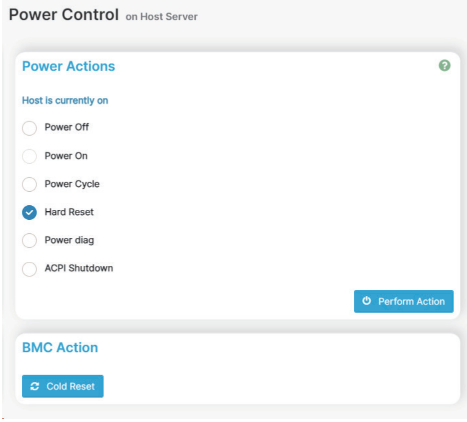
□ Enable

Limit Watt (50 ~ 99)%

Limit Watt (50 ~ 99) %: Dynamically set limits based on PSU MAX wattage.
Additional feature (2U4N)
Chassis : Power Consumption Reading: Display total chassis power consumption currently.
Chassis : Platform Power Consumption Limit: The function is that you can set the power limit through CMC. Then, CMC will distribute the power limit to other currently power nodes. For example, if you set 1000w and 4 nodes power on currently, CMC will set a power limit of 250w for each node.

2-5-4-3 Power Control

This page allows you to view and control the power of your server.
To open Power Control, click **Settings > Others > Power Control** from the menu bar. A sample screenshot of Power Control is shown below.



Power Control on Host Server

Power Actions

Host is currently on

○ Power Off
○ Power On
○ Power Cycle
● Hard Reset
○ Power diag
○ ACPI Shutdown

Perform Action

BMC Action

Cold Reset

The various options of Power Control are given below.
Power Off: To immediately power off the server.
Power On: To power on the server.
Power Cycle: This option will first power off, and then reboot the system (cold boot).
Hard Reset: This option will reboot the system without powering off (warm boot).
ACPI Shutdown: This option initiates the operating system shutdown before the shutdown.
Perform Action: Click this option to perform the selected operation.
Cold Reset: Click this option to reset BMC.

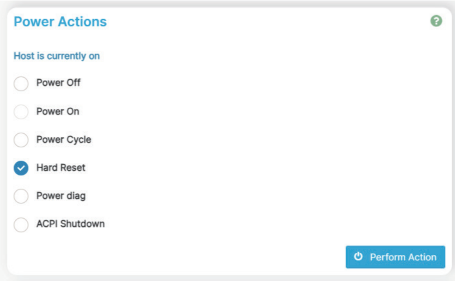
Procedure

Select an action and click Perform Action to proceed with the selected action.
Note: During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after a few minutes.

Additional feature (2U4N)

In 2U4N, the additional feature is that the current node can control another node's power status.

Node Device ID: Selected device ID to control power status.



Power Actions

Host is currently on

○ Power Off

○ Power On

○ Power Cycle

● Hard Reset

○ Power diag

○ ACPI Shutdown

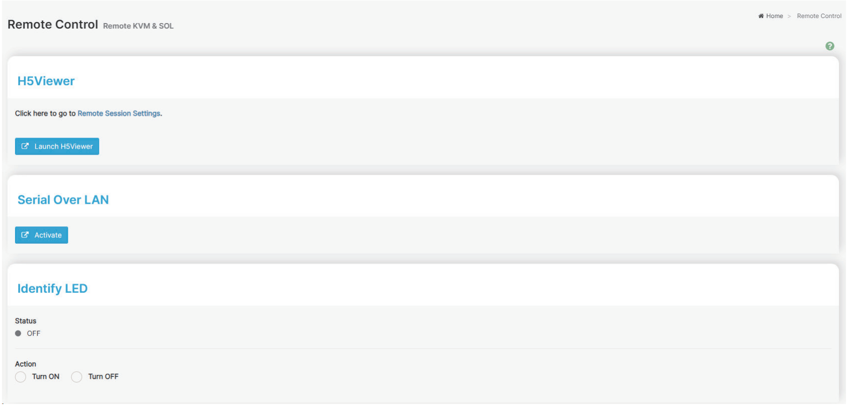
2-6 Remote Control

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 the Remote Control page, click Remote Control from the menu bar. A sample screenshot of the Remote Control page is shown below.



Click here to go to Remote Session Settings.

Status
● OFF

A detailed description of the menu items is given below.

H5Viewer

Click the 'Launch H5Viewer' button to launch the H5viewer window.

Serial Over LAN

Click the 'Activate' button to launch the HTML5 Serial Over LAN window.

Identify LED

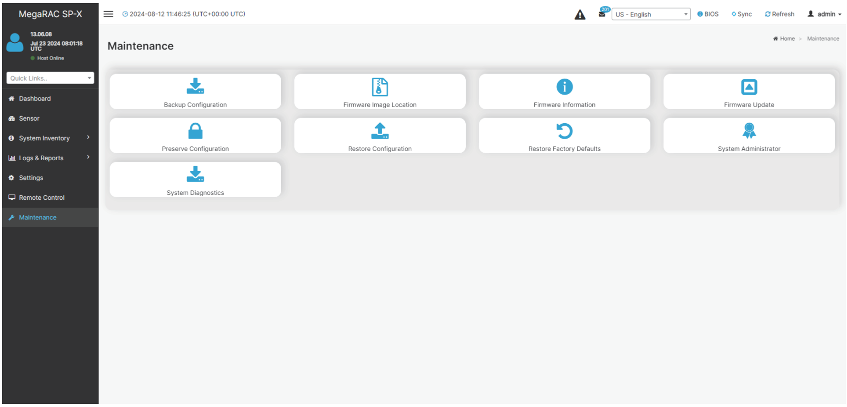
Status shows the status of the Identify LED.
Click 'Turn On' or 'Turn Off' to configure the Identify LED.

2-7 Maintenance

This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Backup Configuration
- Image Location
- Firmware Information
- Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

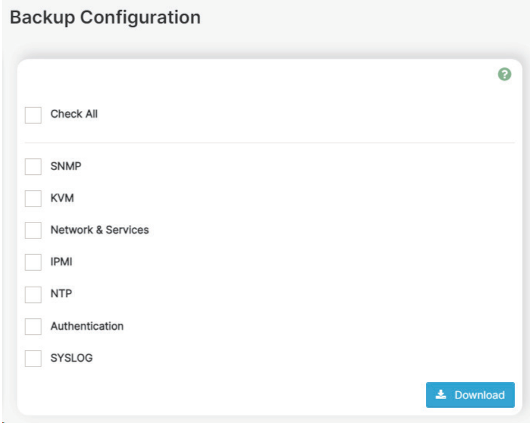
A detailed description is given below.



2-7-1 Backup Configuration

This page allows you to select the specific configuration items to be backup in case of "**Backup Configuration**".

To open the Backup Configuration page, click Maintenance > Backup Configuration from the menu bar. A sample screenshot of the Backup Configuration page is shown below.



Backup Configuration

□ Check All

□ SNMP

□ KVM

□ Network & Services

□ IPMI

□ NTP

□ Authentication

□ SYSLOG

The various fields of the Backup Configuration page are given below.

Check All: Select all the configuration lists.

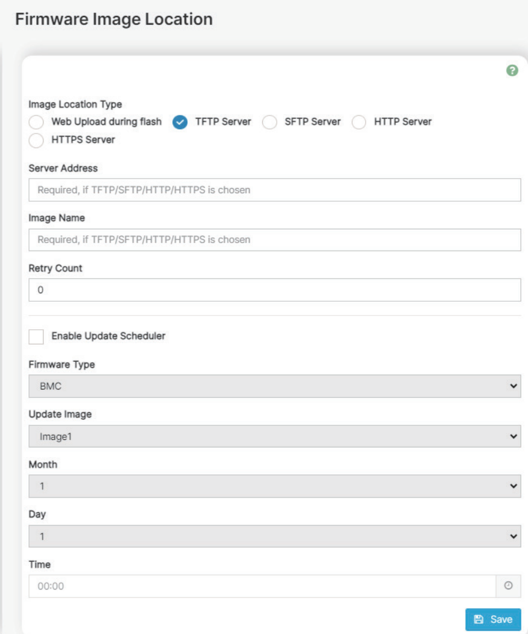
Download Config: To download and save the configuration files backup from BMC to the client system.

Procedure for Backup Configuration:

1. Click Check All to back up all the configuration items or check the configuration that needs backup. The Backup Configuration page will appear as shown in the above screenshot.
   Note: Network configurations are interrelated to IPMI, and hence by default IPMI configurations will be selected automatically when you select "Network and Services" to be backed up.
2. Click **Download Config** to save the backup file to the client system.

2-7-2 Firmware Image Location

This page is used to configure firmware image into the BMC.
To open Firmware Image Location, click Maintenance > Firmware Image Location from the menu bar. A sample screenshot of Firmware Image Location page is shown below.



Firmware Image Location

Image Location Type
○ Web Upload during flash ● TFTP Server ○ SFTP Server ○ HTTP Server
○ HTTPS Server

Server Address
Required, if TFTP/SFTP/HTTP/HTTPS is chosen

Image Name
Required, if TFTP/SFTP/HTTP/HTTPS is chosen

Retry Count
0

□ Enable Update Scheduler

Firmware Type
BMC

Update Image
Image1

Month
1

Day
1

Time
00:00

The various options for Image Transfer Protocol are given below.
Image Location Type: The type of location to transfer the firmware image into the BMC is either Web **Upload during Flash or TFTP/SFTP/HTTP/HTTPS Server.**
TFTP/SFTP Server Address: The address of the server where the firmware image is stored.

Note: The Server supports both IPv4 and IPv6 addresses

- IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
- Each number ranges from 0 to 255.
- The first number must not be 0.
- IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by the colon as in
- “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx”.
- Hexadecimal digits are expressed as lower-case letters.

TFTP/SFTP/HTTP/HTTPS Image Name: The full Source path with the filename of the firmware image is stored on the TFTP Server.
TFTP/SFTP/HTTP/HTTPS Retry Count: Number of times to be retried in case a transfer failure occurs. The retry count ranges from 0 to 255.
Save: To save the configured settings.
Enable Update Scheduler: Enable or disable update scheduler.

Firmware Type: Type of the firmware image.
Update Image: The image that will be updated.
Month: The month of the Update Scheduler.
Day: The day of the Update Scheduler.
Time: The Time of the Update Scheduler.

Procedure

1. Select the **Image Location Type (Web Upload during flash/TFTP Server/SFTP Server/ HTTP Server/HTTPS Server**).
2. If the protocol selected is **TFTP/SFTP/HTTP/HTTPS**, enter the IP address of the server in the **TFTP/SFTP/HTTP/HTTPS Server Address** field.
3. Enter the **TFTP/SFTP/HTTP/HTTPS** Image Name in the given field.
4. Enter the **TFTP/SFTP/HTTP/HTTPS** Retry Count value.
5. For the **SFTP** Server setting, enter your SFTP Username and Password.
6. Click **Save** to save the changes.

Procedure

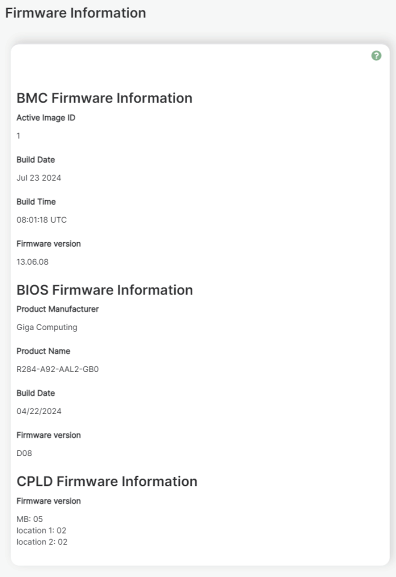
To Enable the Update Scheduler

1. Select the Image Location Type (Web Upload during flash/TFTP Server/SFTP Server/HTTP Server/HTTPS Server).
2. If the protocol selected is **TFTP/SFTP/HTTP/HTTPS**, enter the IP address of the server in the **TFTP/SFTP/HTTP/HTTPS** Server Address field.
3. Enter the **TFTP/SFTP/HTTP/HTTPS** Image Name in the given field.
4. Enter the **TFTP/SFTP/HTTP/HTTPS** Retry Count value.
5. For the SFTP Server setting, enter your SFTP Username and Password.
6. Select the box of Enable Update Scheduler.
7. Choose the Firmware Type.
8. Choose the Update image.
9. Choose the Month.
10. Choose the Day.
11. Choose the Time.
12. Click Save to save the changes.

2-7-3 Firmware Information

This page is used to display the Firmware Information settings.

To open the System Administrator page, click Maintenance > Firmware Information from the menu bar. A sample screenshot of Firmware Information page is shown below.



Firmware Information

BMC Firmware Information

Active Image ID

1

Build Date

Jul 23 2024

Build Time

08:01:18 UTC

Firmware version

13.06.08

BIOS Firmware Information

Product Manufacturer

Giga Computing

Product Name

R284-A92-AAL2-GB0

Build Date

04/22/2024

Firmware version

D08

CPLD Firmware Information

Firmware version

MB: 05
location 1: 02
location 2: 02

The various fields of the Firmware Information page are given below.

BMC Firmware Information:

Active Image ID: Describes the Image ID of the active BMC image.

Build Date: Describes the Build Date of the active BMC image.

Build Time: Describes the Build Time of the active BMC image.

Firmware version: Describes the Firmware version of the active BMC image.Image Location **Type**: The type of location to transfer the firmware image into the BMC is either Web Upload during Flash or TFTP/SFTP/HTTP/HTTPS Server.

BIOS Firmware Information:

Product Manufacturer: Describes the Product Manufacturer of the BIOS.

Product Name: Describes the Product Name of the BIOS.

Build Date: Describes the Build Date of the active BIOS.

Firmware version: Describes the Firmware version of the active BIOS.

CPLD Firmware Information

MB: Display the CPLD version of the Main Board.

SCM: Display the CPLD version of SCM.

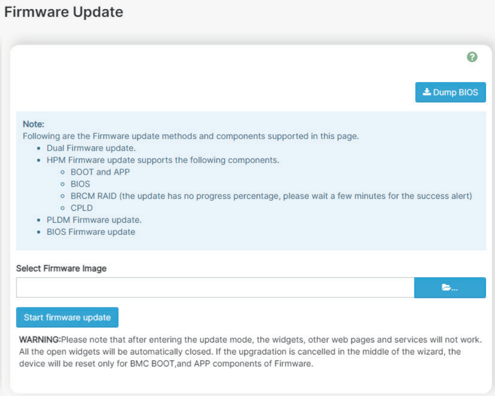
Location [nth]: Display the CPLD version of the nth Back Panel Board. If several Back Panel boards are connected, you will see the number increase.

2-7-4 Firmware Update

This wizard takes you through the process of firmware upgradation. 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.

> **Warning**: Please note that after entering update mode widgets, other web pages and services will not work.
> All open widgets will be closed automatically. If the upgrade process is canceled in the middle of the wizard, the device will be reset.
>
> **Note**: The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.
> Once you enter Update Mode and choose to cancel the firmware flash operation, the BMC card must be reset.
> This means that you must close the Internet browser and log back onto the BMC card before you can perform any other types of operations.
> Once the Firmware upgrade using the web is started, the regular IPMI command will not be allowed for safety concerns if Enable IPMI Command handling during flashing support is disabled in the project configuration.

To configure, choose 'Firmware Image Location' under Maintenance. To open Firmware Update page, click **Maintenance > Firmware Update** from the menu bar. A sample screenshot of Firmware Update Page is shown below.



Firmware Update

Note:
Following are the Firmware update methods and components supported in this page.

- Dual Firmware update.
- HPM Firmware update supports the following components.
  - BOOT and APP
  - BIOS
  - BRCM RAID (the update has no progress percentage, please wait a few minutes for the success alert)
  - CPLD
- PLDM Firmware update.
- BIOS Firmware update

Select Firmware Image

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

This wizard takes you through the process of AMI-based firmware up gradation. The protocol information to be used for firmware image transfer during this update is as follows.

> **Note**: All configuration items will be preserved/overwritten as default during the restore configuration operation.

Procedure

1. Click Browse to select firmware image.

Note: A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of the upload.

2. Click Start firmware update to load the Firmware Update information.
3. Click Preserve all Configuration to preserve all configurations.
   - Preserve all Configuration: To preserve all configuration.
   - Edit Preserve Configuration: To modify the Preserve status settings.

This wizard takes you through the process of AMI-based firmware upgradation. The protocol information to be used for firmware image transfer during this update is as follows.

Note: All configuration items will be preserved/overwritten as default during the restore configuration operation.

4. Click Proceed to Flash, it will prompt you with the warning message. Click OK to start the Firmware update.
5. The Firmware update undergoes the following steps:

a. Closing all active client requests.

b. Preparing the Device for Firmware Upgrade.

c. Uploading Firmware Image.

d. Verifying Firmware Image

In Section-Based Firmware Update, you can configure the firmware image for section-based flashing. Check the required sections and click Proceed to update the firmware.

If flashing is required for all images, select the option Full Flash.

If you select the Version Compare Flash option from the web, the current and uploaded module versions, FMHlocation, and sizes will be compared.

If the modules differ in size and location, proceed with force firmware upgrade.

If all the module versions are the same, restart BMC by saying all the module versions are similar.

If only a few module versions are different, those module will be flashed.

Note: Only selected sections of the firmware will be updated. Other sections are skipped. Before starting the flash operation, you are advised to verify the compatibility between image sections.

e. Flashing Firmware Image

f. Resetting the image. The sample screenshot of Firmware update is shown below.

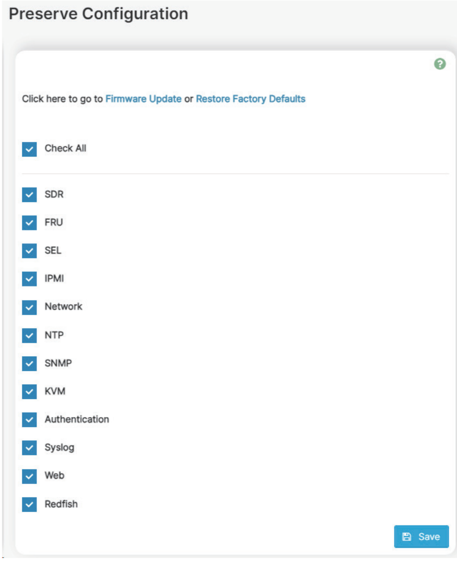
Note: The Firmware Update page will be disabled, and you will not be able to perform any other tasks until the firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if an update is canceled. The device will also reset upon successful completion of firmware update.

2-7-5 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration.

To open the Preserve Configuration page, click **Maintenance > Preserve Configuration** from the menu bar. A sample screenshot of Preserve Configuration page is shown below.

> **Note**: You can navigate to the Firmware Update Page and Restore Factory Defaults by clicking the respective links.



Preserve Configuration

Click here to go to Firmware Update or Restore Factory Defaults

☑ Check All

☑ SDR
☑ FRU
☑ SEL
☑ IPMI
☑ Network
☑ NTP
☑ SNMP
☑ KVM
☑ Authentication
☑ Syslog
☑ Web
☑ Redfish

The various fields of Preserve Configuration are as follows.

Click here to go to Firmware Update or Restore Configuration: This link will redirect to the Firmware Update or Restore Configuration page which needs to be preserved.

Check All: To check the entire configuration list.

Save: To save any changes made.

> **Note**: This configuration is used by the Restore Factory Defaults process.

Files Preserved

SDR

The following files will be preserved.

SDR.dat: This file contains the sensor data record information that is used in IPMI.

Dependency Configurations : NIL

FRU

The following files will be preserved.

FRU.bin: This file contains the logical field replaceable unit data that are used by IPMI

Dependency Configurations - SDR

SEL

The following files will be preserved when Delete SEL reclaim space is disabled.
SEL.dat: This file contains the system event logs that are being logged by the IPMI.
The following files will be preserved when Delete SEL reclaim space is enabled.
Selreclaiminfo.ini: The file contains the SEL repository information.
SEL folder: This folder contains the multiple files of event logs.
Dependency Configurations: IPMI

IPMI
The following files are preserved in IPMI configuration.
IPMI.conf: This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.
dcmi.conf: This file contains the DCMI1.5 specification parameters such as DHCP Timing1, DHCP Timing2, DHCP Timing3. The files are preserved only when the DCMI1.5 feature is enabled in the MDS project configuration.
pwdEncKey: This file contains the keys that are used to decrypt the passwords. When the user password option is enabled in the MDS project configuration, this file will be preserved.
Dependency Configurations: NIL

Network
To save network settings related to IPMI (LAN IP or DHCP configuration), select "IPMI" and "Network" options simultaneously. After restore the configuration, the Network Configuration will be preserved successfully. The following files will also be preserved.
dhcp.conf: This file is to configure the host
dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface.
hostname: This file is used to store the Hostname of the BMC.
hostname.conf: This file is used to configure the host name creation method Manual/Automatic for the BMC.
Vlaninterfaces: This file helps to enable the VLAN interface for the particular LAN interface.
vlansetting.conf: This file is to store the VLAN ID and VLAN priority for the particular VLAN interface entry.
bond.conf: This file is to enable the bond interface for the specified LAN interfaces.
Interfaces: This file is to configure the IP/IPV6 addresses for the LAN interface using the static/ DHCP method.
activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.
hosts: This file is used to store the host name to map the IP address.
hosts.allow: This file contains the list of hosts that have permission to access the system
hosts.deny : This file contains the list of hosts that do not allow accessing the system
resolved.conf: This file is used to store the nameserver and domain name for hostname registration.
dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.
dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.
ncsicfg.conf: This file is to configure the NCSI related configurations.
nsupdate.conf: This file is to configure the channel ID, and package ID for the NCSI interface.

phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.
dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.
Dependency Configurations: IPMI

NTP

The following files will be preserved.
ntp.conf: This file contains the NTP daemon protocol configuration parameters such as synchronization sources, nodes and other related information.
ntp.stat: This file contains the auto or manual network type protocols
adjtime: This file contains the time to synchronize the system clock.
Localtime: This file is the system link to the file's local time or to the correct time zone in the system timezone directly.
Dependency Configurations: IPMI
The following files will be preserved.
snmp_users.conf: This file contains the SNMP user configurations such as username and password encryption mechanism for specific users.
snmpcfg.conf: This file contains the SNMP user's privilege levels such as ro user and rw user.
Dependency Configurations: NIL

KVM

The following files will be preserved.
vmedia.conf: This file contains the modes of media such as cd, and hd and enables and disables flags for media, media and sd servers.
advised.conf: This file contains the mouse mode configurations and host machine physical keyboard language layout configured in the MDS project configuration.
autorecord.conf: This file contains the maximum size of the video record file, the maximum number of video record files, the maximum time length of the video record file and information about the remote machine path if it is enabled in the MDS project configuration.
stunnel.conf: This file contains information about the tunnel configuration. It will also contain the advisor and media server's secure port if a secure connection is enabled.
rmedia.conf: This file contains the image name and the remote machine information like IP address, username, password, domain name and share type.
Dependency Configurations: NIL

Authentication

The following files will be preserved.
active dir.conf: This file contains the configurations such as saleable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such **as name domain and privileges.**
openLdapGroup.conf: This file contains the open ldap role group information such as name domain and privilege.
nsswitch.conf: This file contains the sources to obtain the name service information in the range of categories and in what order.

pam_withunix: This file contains the PAM Order of modules such as IPMI, LDAP, RADIUS and UNIX.
pam_wounix: This contains the PAM Order of modules such as IPMI, LDAP and RADIUS.
group: This file contains the Linux group. It stores the group information or defines the user group information in Linux.
passwd: This file contains the user login information for the Linux system.
shadow: This file contains the encrypted password information for the clients.
ldap.conf: This file contains the LDAP server configuration details such as bindn, binpw, pam_password, nss_reconnect_tries, port, port secondary, host, and host secondary.
radius.conf: This file contains the radius server IP address, port number, secret, timeout, privilege etc.
Dependency Configurations: NIL

Syslog

The following files will be preserved.

syslog.conf
rotate.conf
rsyslog.conf

These files contain the system log configuration details to preserve different event categories such as alert, critical, error notification etc.
Dependency Configurations: NIL

Web

The following files will be preserved.
updatefirmware.conf : This file contains the firmware image location details to update the firmware configuration.
Dependency Configurations : NIL

Extlog

It preserves Extended SEL Log events.
This file contains Extended SEL events Log details.

Dependency Configurations : IPMI

> **Note**: This support is feature based. If this feature is enabled, then the Extlog option will be displayed in the Preserve configuration.

Redfish

Redfish preserves the Redis Database file.
redis-dump.rdb: This file contains the Redfish details.
Dependency Configurations: NIL

> **Note**: This support is feature based. If this feature is enabled, then the Redfish option will be displayed in the Preserve configuration.

Automation Engine

The following files will be preserved.

ae.sqlite: This file contains the tasks and scripts of the automation engine.

Dependency Configurations: NIL

> **Note**: This support is feature based. If this feature is enabled, then the Automation Engine option will be displayed in the Preserve configuration.

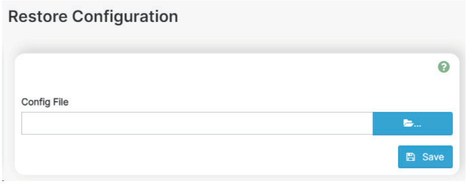
Procedure

1. Click the **Firmware Update or Restore Configuration** link to view the Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate check boxes or by selecting all or none using **Check All**.
3. Click **Save** to save the changes.

2-7-6 Restore Configuration

This page allows you to restore the configuration files from the client system to the BMC.

To open the Restore Configuration page, click Maintenance > Restore Configuration from the menu bar. A sample screenshot of the Restore Configuration page is shown below.



The various fields Restore Configuration page are given below.

Config File : This option is used to select the file that was backed up earlier.

Upload : Upload the backup file to restore the backup files.

Procedure for Restore Configuration:

1. Click **Browse** to select the configuration file that needs to be backed up and used to Restore the configuration, when needed.
2. Click **Upload** to restore the backup files. The Restore Configuration page will appear as shown below.
3. Click OK to upload the new configuration file and restore.

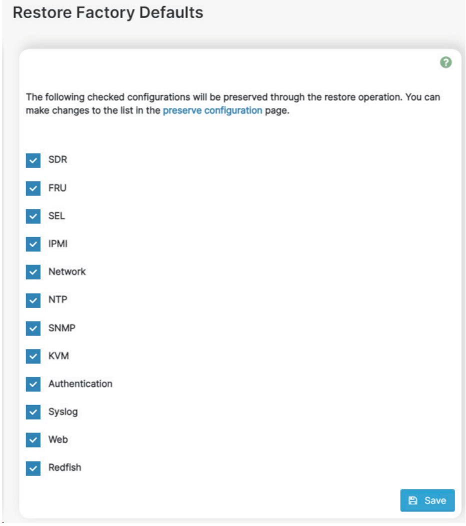
2-7-7 Restore Factory Defaults

In Web GUI, this option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during the restore factory default configuration.

> **Warning**: Please note that after entering restore 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 Restore Factory Defaults page, click Maintenance > Restore Factory Defaults from the menu bar. A sample screenshot of the Restore Factory Defaults Page is shown below.



Restore Factory Defaults

The following checked configurations will be preserved through the restore operation. You can make changes to the list in the preserve configuration page.

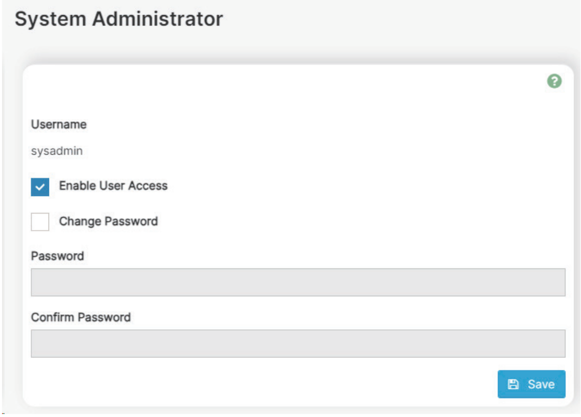
☑ SDR
☑ FRU
☑ SEL
☑ IPMI
☑ Network
☑ NTP
☑ SNMP
☑ KVM
☑ Authentication
☑ Syslog
☑ Web
☑ Redfish

Procedure

1. Click Preserve Configuration to redirect to the Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Factory Defaults to restore the factory defaults of the device firmware.
   Note: When the Restore Factory Defaults action is performed, there might be some log events present after performing the restore operation. Those events might be newly generated which can be verified using its timestamp.

2-7-8 System Administrator

This page is used to configure the System Administrator settings.
To open the System Administrator page, click **Maintenance > System Administrator** from the menu bar. A sample screenshot of the System Administrator page is shown below.



System Administrator

Username
sysadmin

☑ Enable User Access

□ Change Password

Password

Confirm Password

The various fields of the System Administrator page are given below.
Username: The username of the System Administrator is a read-only field.
Enable User Access: To enable user access for the system administrator.
Change Password: To change the user’s password.

> **Note**: This field will not allow more than 64 characters.
> Password must be at least 8 characters long and White space is not allowed.

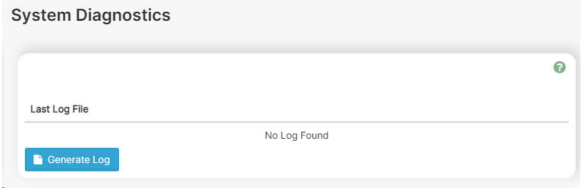
Save: To save the new configuration for the system administrator.

Procedure

1. Check **Enable User Access** to enable user access for the system administrator.
2. Enable **Change Password** option to change the user password. This action enables the password fields.
3. Enter the new password in the **Password** field.
4. Re-enter the password in the **Confirm Password** field.
5. Click **Save** to save the changes.

2-7-9 System Diagnostics

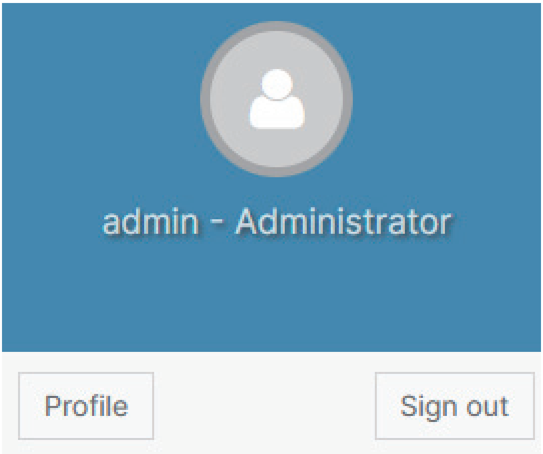
This page is used to generate the last logs file.
To open the System Administrator page, click **Maintenance > System Diagnostics** from the menu bar. A sample screenshot of the System Administrator page is shown below.



Click **Generate Log** to view the last log file.

2-8 Sign Out

To log out from the Web GUI, click the admin on the top right corner of the screen. A sample screenshot of admin option is shown below.



Click Sign Out to perform log out from the Web GUI. A Warning message will prompt you to proceed further, click OK to log out else Cancel to retain the Web GUI.