BMC

Sirius Server Board
User's Manual

UM_Sirius_BMC_v1.1_022725

Table of Contents

Preface i
Chapter 1. Introduction 1
1.1 Introduction to the BMC Platform 1
1.2 Overview of the ASPEED AST2600 BMC 1
1.3 AIC BMC Features 1
Chapter 2. UEFI BIOS Configuration for BMC 3
2.1 Enter UEFI BIOS 3
2.2 Enable the COM port for BMC's SOL (Serial Over LAN) 3
2.3 Configure BMC's IP Address by the UEFI BIOS 4
2.4 Save UEFI BIOS Configuring 5
Chapter 3. Log In to the Remote Console 6
3.1 Required Browser Settings 6
3.2 Username and Password 6
3.3 Default User Name and Password 8
3.4 Need to change password 9
Chapter 4. Menu Bar and Quick Button 11
4.1 Menu Bar 11
4.2 Quick Button and Logged-in User 12
Chapter 5. Dashboard 13
Chapter 6. Sensor 15
Chapter 7. System Inventory 19
7.1 System Info 19
7.2 Processor Info 19
7.3 Memory Controller Info 20
7.4 Base Board Info 20
7.5 Power Info 22
7.6 Thermal Info 23
7.7 PCIE Device Info 24
7.8 PCIE Function 24
7.9 Storage Info 25
Chapter 8. FRU Information 26
Chapter 9. PSU Information 28
Chapter 10. Logs & Reports 30
10.1 IPMI Event Log 31
10.2 System Log 33
10.3 Audit Log 34
10.4 Video Log 35
Chapter 11. Settings 37
11.1 Captured BSOD 38
11.2 Date and Time 39
11.3 External User services 42
11.3.1 LDAP/E-Directory Settings 42
11.3.2 Active Directory Settings 46
11.3.3 RADIUS Settings 51
11.4 KVM Mouse Settings 54
11.5 Log Settings 55

11.5.1 SEL Log Setting Policy 55
11.5.2 Advanced Log Settings 56
11.6 Media Redirection Settings 59
11.6.1 General Settings 60
11.6.2 VMedia Instance Settings 63
11.6.3 Remote Session 65
11.6.4 Active Redirections 67
11.7 Network Settings 68
11.7.1 Network IP Settings 68
11.7.2 Network Bond Configuration 71
11.7.3 Network Link Configuration 73
11.7.4 DNS Configuration 75
11.8 PAM Order Settings 79
11.9 Platform Event Filter 80
11.9.1 Event Filters 80
11.9.2 Alert Policies 84
11.9.3 LAN Destinations 87
11.10 RAID Management 90
11.10.1 RAID Controller Information 91
11.10.2 Storage Summary 92
11.10.3 Physical Device Information 93
11.10.4 Logical Device Information 97
11.10.5 BBU Information 105
11.10.6 Event Log 106
11.10.7 SES Enclosure Information 107
11.11 Service 108
11.12 SMTP Settings 112
11.13 SSL Settings 115
11.13.1 Upload SSL Certificate 116
11.13.2 Generate SSL Certificate 118
11.13.3 View SSL Certificate 120
11.14 System Firewall 122
11.14.1 General Firewall Settings 122
11.14.2 IP Address Firewall Rules 125
11.14.3 Port Firewall Rules 127
11.15 User Management 130
11.16 Video Recording 137
11.16.1 Auto Video Settings 138
11.16.2 SOL Settings 145
11.17 IPMI Interfaces 147
11.18 Fan Mode 148
11.19 SNMP Community String 149
11.20 Sensor Modification 150
11.21 BIOS Onetime Boot 152
11.22 Intrusion Switch Type 154
11.23 Power Redundancy Mode 155
11.24 Platform Integrity Check 156
Chapter 12. Remote Control 158

12.1 Launch H5Viewer 159
12.2 Serial Over LAN 171
Chapter 13. Images Redirection 173
13.1 Remote Images 174
Chapter 14. Chassis Identify 178
Chapter 15. Power Control 179
Chapter 16. Maintenance 180
16.1 Backup Configuration 180
16.2 Firmware Image Location 185
16.3 BMC Firmware Information 187
16.4 BMC Firmware Update 188
16.5 Preserve Configuration 195
16.6 Restore Configuration 201
16.7 Restore Factory Default 202
16.8 System Administrator 203
16.9 CPLD Firmware Information 204
16.10 BIOS Firmware Information 205
16.11 BIOS Firmware Update 206
16.12 CPLD Firmware Update 210
16.13 Post Code 214
16.14 BMC Reset 214
16.15 Download Data 215
Chapter 17. Sign Out 216
Chapter 18. Utility & Tool 217
18.1 Flash Tools 217
18.1.1 YAFUFlash 217
18.1.2 Installation in Windows 217
18.1.3 Installation in Linux 234
18.1.4 YAFUFlash OS Compatibility 251
18.1.5 Installation in DOS 251
18.2 VMCLI Tool 258
18.2.1 Installation in Windows 258
18.2.2 Installation in Linux 266
Chapter 19. LINUX OS Installation with nomodeset 272
19.1 SLES 12.x 272
19.2 Ubuntu 14.04.x and Ubuntu 16.04.x 274
19.3 RHEL 6.9 and 7.3 276
Chapter 20. SOL (Serial Over LAN) 278
Chapter 21. KVM OS and Browser Compatibility 279
Chapter 22. OTP (One Time Password) 281
Chapter 23. Thermal Management Support 284
Chapter 24. PTP IEEE 1588 support 285
Chapter 25. Web Privileges 287
Chapter 26. Technical Support 291
Appendix 292

Document Release History

Release Date	Version	Update Content
October, 2024	1	BMC user’s manual release to public.
February, 2025	1.1	1. Remove Secured Boot Support and ImageSigning tool and SMASHLITE 2. Add universal function description 3. Added "RAID Management" section 4. Updated descriptions in the “System Inventory”, “BIOS Onetime Boot”, “Intrusion Switch Type”, and “Platform Integrity Check” sections.

Copyright © 2024 AIC®, Inc. All Rights Reserved.

This document contains proprietary information about AIC® products and is not to be disclosed or used except in accordance with applicable agreements.

Preface

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photo-static, recording or otherwise, without the prior written consent of the manufacturer.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective holders.

Changes

The material in this document is for information purposes only and is subject to change without notice.

Warning

1. A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Disclaimer

AIC® shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither AIC® or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Instruction Symbols

Special attention should be given to the instruction symbols below.

NOTE	This symbol indicates that there is an explanatory or supplementary instruction.
CAUTION	This symbol denotes possible hardware impairment. Upmost precaution must be taken to prevent serious hardware damage.
WARNING	This symbol serves as a warning alert for potential body injury. The user may suffer possible injury from disregard or lack of attention.

Chapter 1. Introduction

1.1 Introduction to the BMC Platform

The BMC (Baseboard Management Controller) permits remote networking access to multiple users situated in different locations. In addition to this, it facilitates remote system health monitoring and computer event management for system administrators.

BMC operates independently from the operating system. Utilizing an IPMI management utility installed on the motherboard, the ASPEED AST2600 BMC establishes connectivity between the Platform Controller Hub (PCH) and other onboard components, enabling a remote network interface through serial links. Equipped with the AST2600 controller and integrated BMC firmware, the AIC motherboard empowers users to remotely access, monitor, diagnose, and manage a server using Console Redirection.

1.2 Overview of the ASPEED AST2600 BMC

The ASPEED AST2600 BMC is ASPEED's 7th generation Server Management Processor. Adopting the Dual-core ARM Cortex A7 processor, AST2600 can optimize the performance and computing power; also lower the power consumption significantly. Also, AST2600 support Secure Boot mode and ARM Cortex A7 TrustZone, which can provide customers excellent information security protection.

The BMC contains a specialized processor with 2D graphic and logic control features. It facilitates remote monitoring and management of server systems, providing a flexible motherboard design. The AST2600 BMC also serves as the VGA for BMC Graphics.

1.3 AIC BMC Features

The BMC functions supported by AIC are as follows.

- Hardware monitoring
- Overall health status display on the main page
- Remote KVM (graphical) console
- Remote server power control
- Remote serial over LAN (text console)
- Event Log support
- Automatic notifications and alerts (SNMP and email)
- Out-of-band management via shared or dedicated LAN
- Change LAN interface options at runtime
- VLAN

- SMASH/CLP
- Secure browser interface (Secure socket layer - SSL support)
- Lightweight Directory Access Protocol (LDAP) support
- Factory default settings from web support
- OS independent
- Backup and restore the configuration file
- Preview of the remote screen on the main page
- Video quality settings
- Update firmware via browser and OS
- KCS permission Control
- Redfish

Chapter 2. UEFI BIOS Configuration for BMC

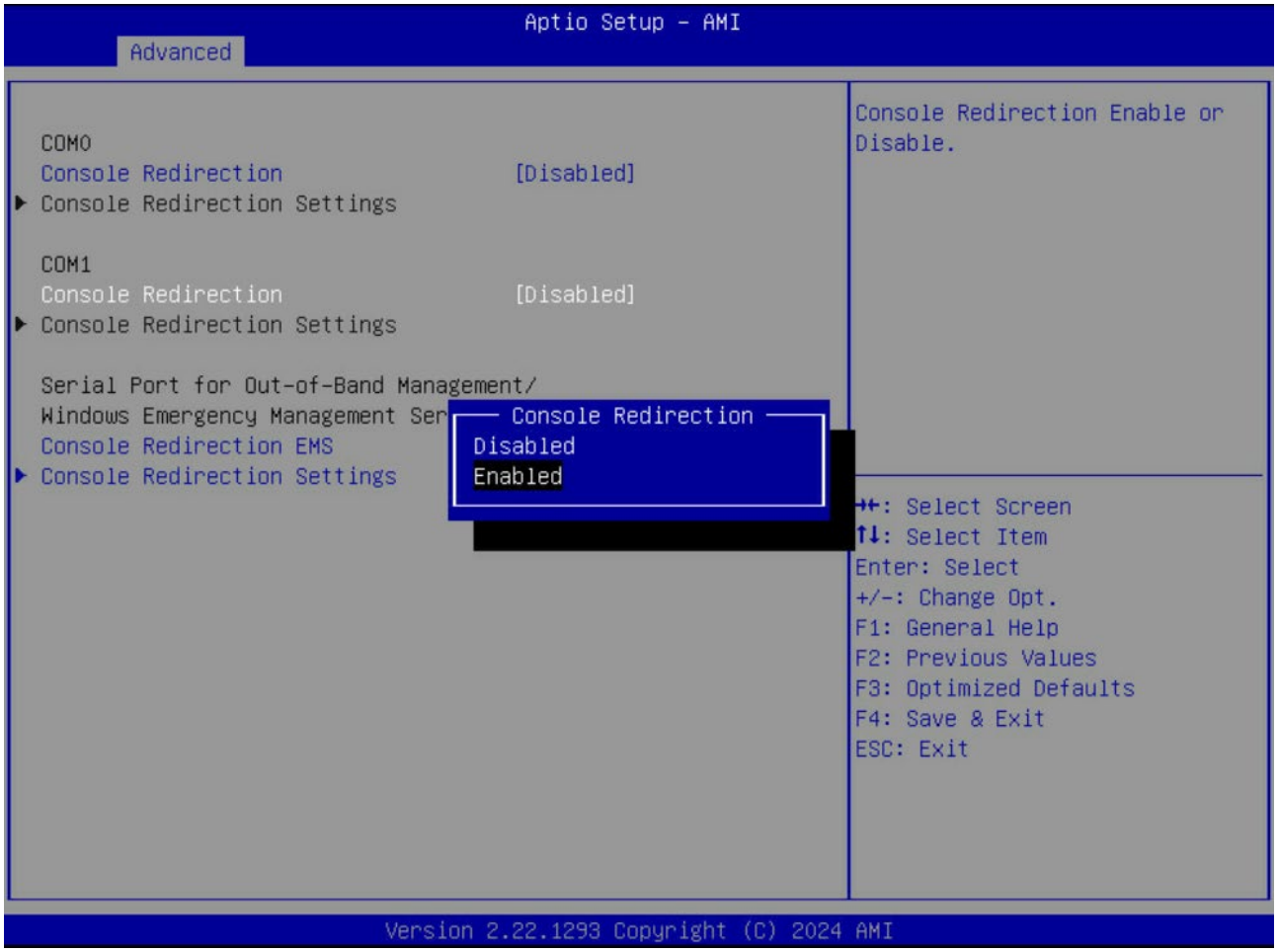
Before configuring the BMC, please follow the instructions below to configure the system UEFI BIOS settings.

2.1 Enter UEFI BIOS

1. During system startup, press the **<Del>** key to enter UEFI BIOS setting.
2. To navigate in the UEFI BIOS, use the arrow keys and press **<Enter>** key. To go back to previous screens, press **<Esc>** key.

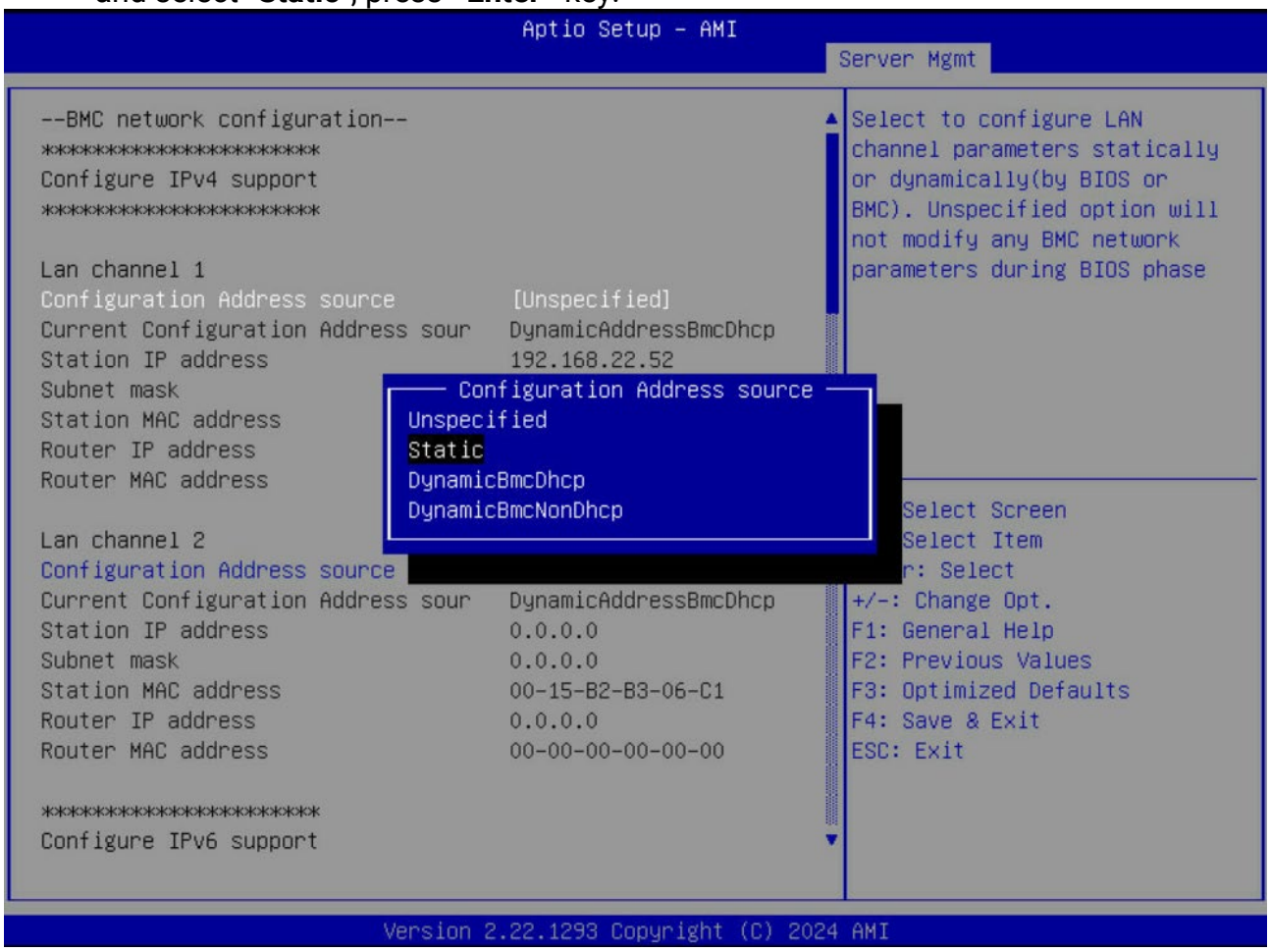
2.2 Enable the COM port for BMC's SOL (Serial Over LAN)

1. Select the **"Advanced"** tab from the UEFI BIOS setup menu.
2. Select **"Serial Port Console Redirection"** and press **<Enter>** key.
3. Highlight **"Console Redirection"** under **COM1**, press **<Enter>** key, and select "**Enabled**".



2.3 Configure BMC's IP Address by the UEFI BIOS

1. Select the "**Server Mgmt**" tab from the UEFI BIOS setup menu..
2. Select "**BMC network configuration**" and press **<Enter>** key.
3. Highlight "**Configuration Address Source**" under Lan channel 1, press **<Enter>** key, and select "**Static**", press **<Enter>** key.



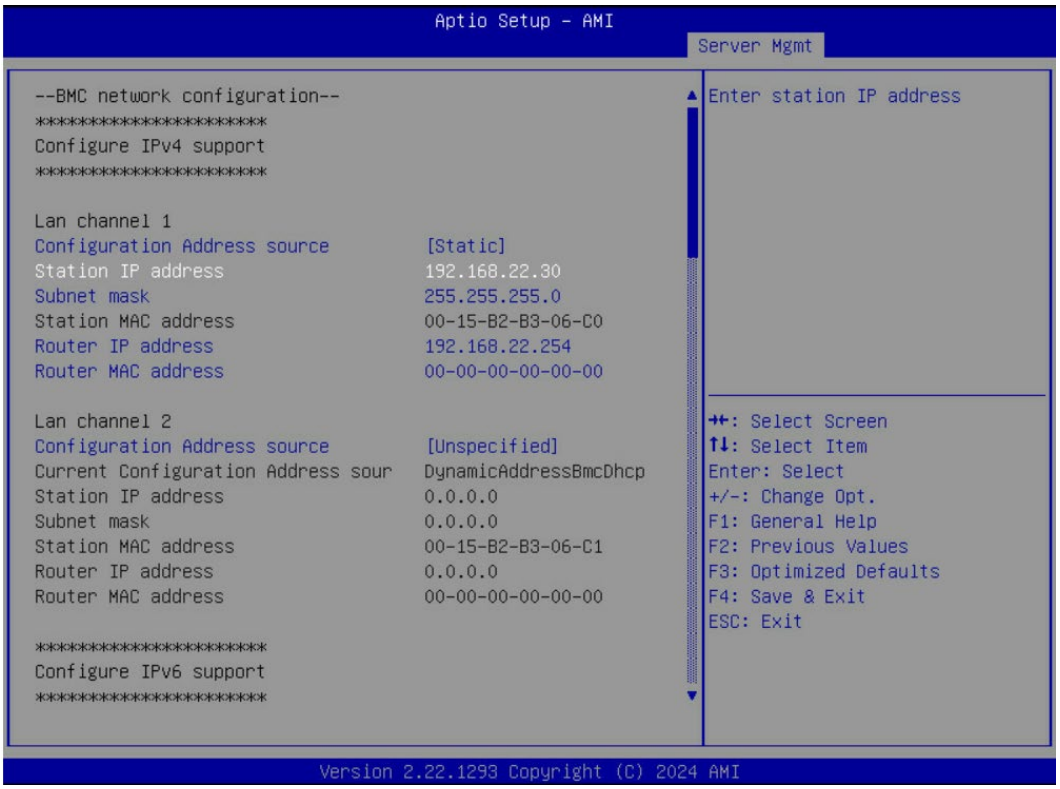
4. Set the "**Station IP address**", "**Subnet mask**" and "**Gateway IP Address**" fields. Select each of the three items and enter the values. Press **<Enter>** key when finished. The computer and BMC need to be on the same subnet. These settings must refer to your network environment.

   Example:

   Station IP address: 192.168.22.30

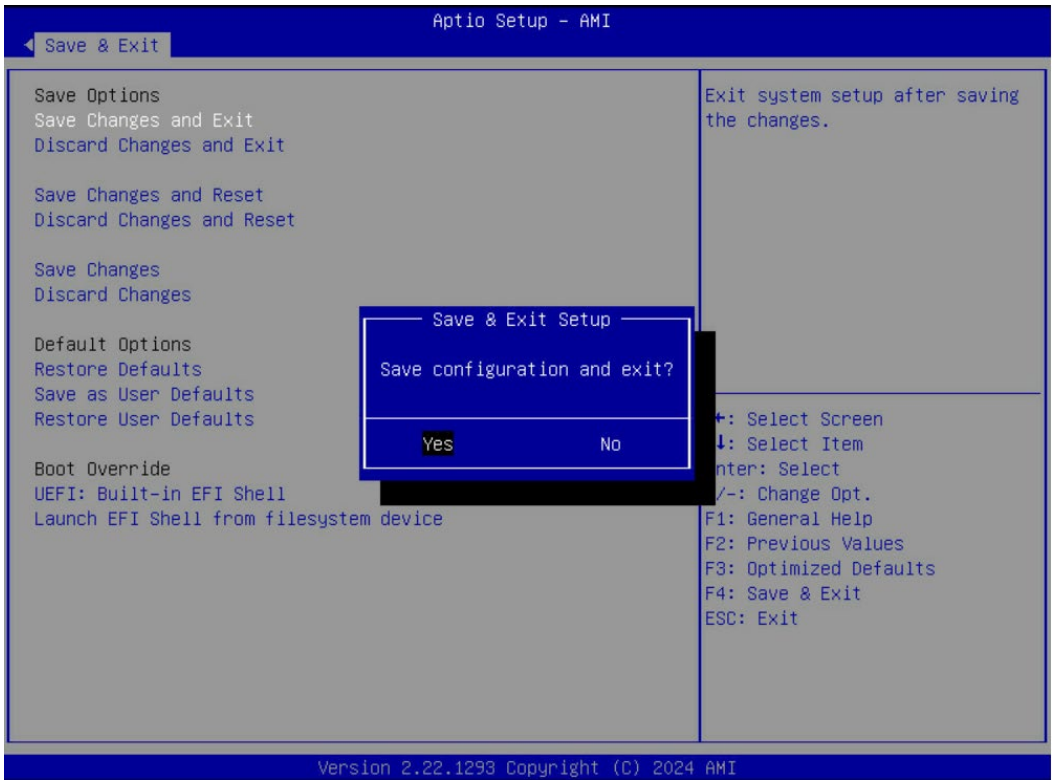
   Subnet mask: 255.255.255.0

   Router IP Address: 192.168.22.254



2.4 Save UEFI BIOS Configuring

1. Select the "**Save & Exit**" tab from the UEFI BIOS setup menu..
2. Highlight "**Save Changes and Exit**" and press **<Enter>** key, and select "**Yes**".



Chapter 3. Log In to the Remote Console

3.1 Required Browser Settings

Use a computer and configure its web browsers.

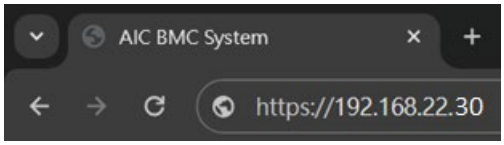
- Accept the file download when prompted in all browsers
- Javascript and cookie settings should be enabled in order to access the web site

NOTE
Cookies must be enabled in order to access the website.

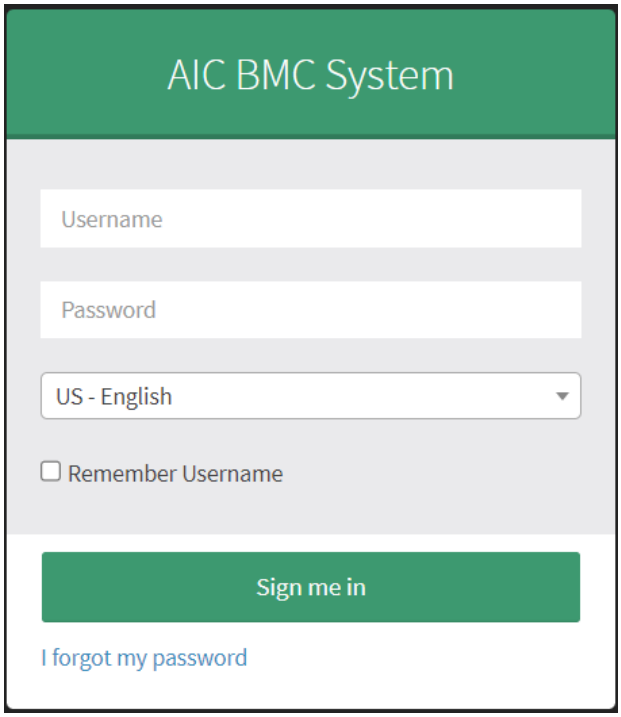
3.2 Username and Password

The computer and BMC need to be on the same subnet. After setting the static IP, they should be able to communicate. To establish a connection, follow the steps below.

1. Use the computer's terminal to ping the BMC IP address and ensure that it can be pinged.
2. If the BMC IP address is pingable, open a web browser on your computer, enter the BMC IP address in the URL bar.



3. Initial access prompts you to enter the User Name and Password. A sample screenshot of the login screen is given below.



The fields are explained as follows:

Fields Name	Description
Username	Enter your username in this field.
Password	Enter your password in this field.
Language Selection	Language selection drop-down will be populated based on supported languages in Web UI as a part of multi-language support feature. Drop-down option value will be selected based on the browser language. For example, if browser language is configured with Simplified Chinese language (ZH-CN), then option value will be auto selected as China. Default language will be selected as US-English if the browser configured language not supported by Web UI. Entire Web UI pages language strings will be displayed based on selected language from drop-down.
Remember Username	Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.
Sign me in	After entering the required credentials, click the **Sign me in** to login.
I forgot my password	If you forget your password, you can generate a new password using this link.

3.3 Default User Name and Password

Default Username: **admin**

Default Password: **admin**

NOTE
The default user name and password are in lower-case characters. When you log in using the user name and password, you get full administrative rights. It is advised to change your password once you login.

Duplicate user names shouldn't exist across various authentication methods like AD, LDAP or IPMI since the privilege of one Authentication method is overwritten by another authentication method when login and hence the correct privilege can't be returned properly. Duplicate user names shouldn't be existed across different channels in IPMI.

If any changes occurred for RADIUS in authentication order, then the User ID's of logged in users using other authentication services will be shown as RADIUS User ID. So, it is recommended to keep RADIUS as last in PAM Order.

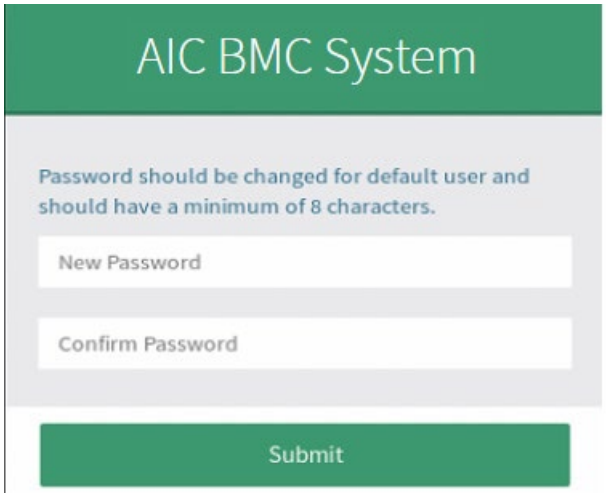
Warning:
Once you login to the application, it is recommended not to use the following options.

- Refresh button of the browser
- *Refresh menu of the browser*
- *Back and Forward options of the browser*
- *F5 on the keyboard*
- *Backspace on the keyboard*

The changes done in user account properties through IPMI/Redfish interfaces will not be reflected in current active web sessions.

3.4 Need to change password

It is mandatory to change the password for the default user at first successful login due to California Law SB-327 security fix. If the authentication is successful, then Web UI will prompt a new page which will ask to change the user password. Once the password is changed, login page will be reloaded. Enter the username and modified password to Login. A sample screenshot is given below.



Default User's password can be changed using any of the following method.

- Web UI
- IPMI Tool
- Redfish (If Redfish Support is enabled)

> **NOTE**
> The last password used cannot be used to reset the password.

Password Change Required Case

1. When the BMC boots with factory firmware, user needs to change the default password on first boot.
2. When user upgrades the BMC firmware without preserve configuration, default password needs to be changed on first boot.
3. When user does a factory restore and reboot BMC, default password needs to be changed on reboot.
4. Whenever user detect the BMC conf corruption and restore the conf with factory setting, on next boot, default password needs to be changed.

Limitations

If the current Firmware in BMC is without CA law enabled and the default password is modified and user tries to preserve configuration and upgrade firmware with CA law enabled firmware image, BMC will still prompt to change the user password.

Reason: In BMC firmware default password is not preserved or stored anywhere, so it is not possible to check if the default password is modified or not. Default password can also be modified during Build time in PMCP file as required by OEM.

Chapter 4. Menu Bar and Quick Button

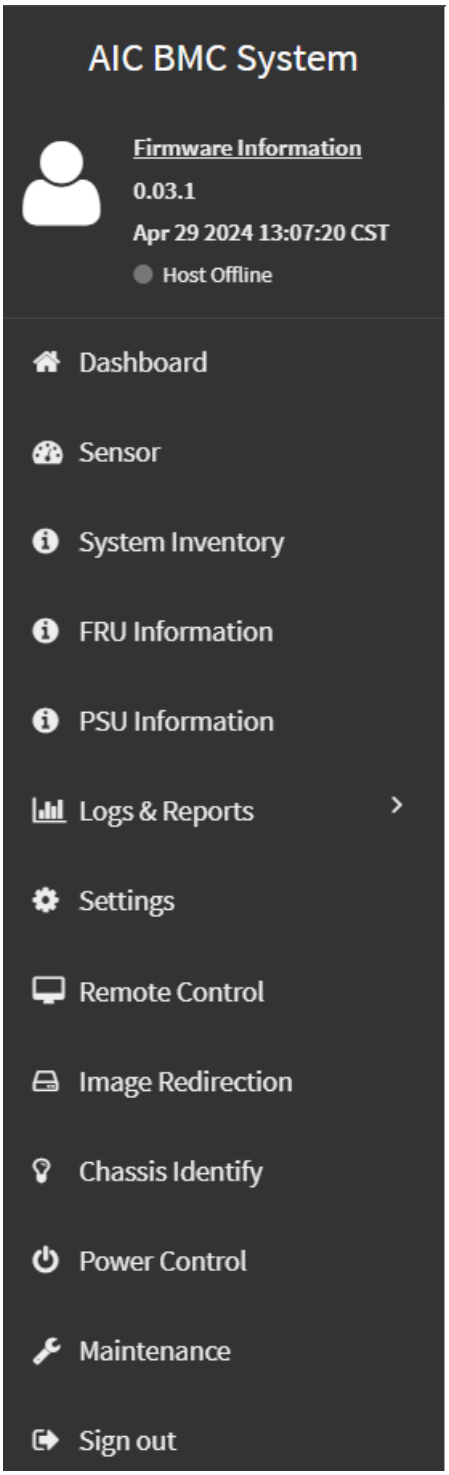
4.1 Menu Bar

The menu bar displays the following.

Firmware Information will be displayed with the latest version, date and time details.

Power Control Status will be displayed as Host Online. To change the Power Control Status, click **Host Offline** link.

- Dashboard
- Sensor
- System Inventory
- FRU Information
- PSU Information
- Logs & Report
- Settings
- Remote Control
- Image Redirection
- Chassis Identify
- Power Control
- Maintenance
- Sign out



4.2 Quick Button and Logged-in User

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

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.

Message: Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the Logs and Reports page.

Notification: Click to view the notification received.

Language Selection: Change the language to view the language strings in different languages.

Sync: Click the Sync icon to synchronize with Latest Sensor and Event Log updates. By default, it will be in disabled mode.

Refresh: Click the Refresh icon or pressing key F5 to reload the current page.

Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are list of privileges mentioned as below.

Administrator: All BMC commands are allowed.

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.

No Access: Login access denied.

OEM: All OEM commands are allowed.

Sign out: Click the Sign out icon to log out.

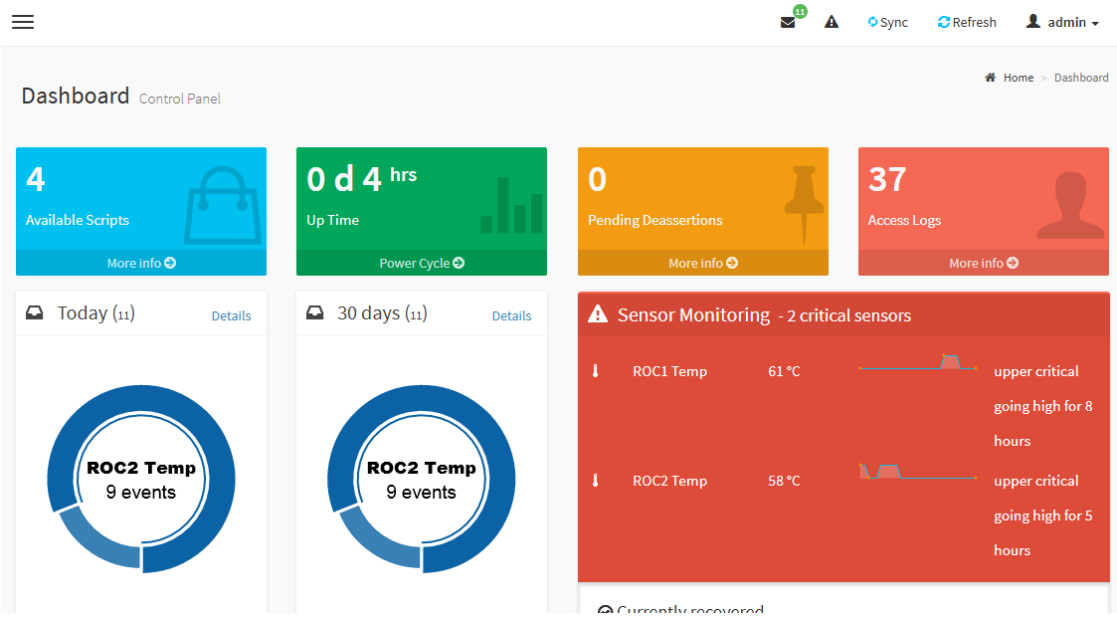
Help

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

Chapter 5. 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. A sample screenshot of the Dashboard page is shown below.

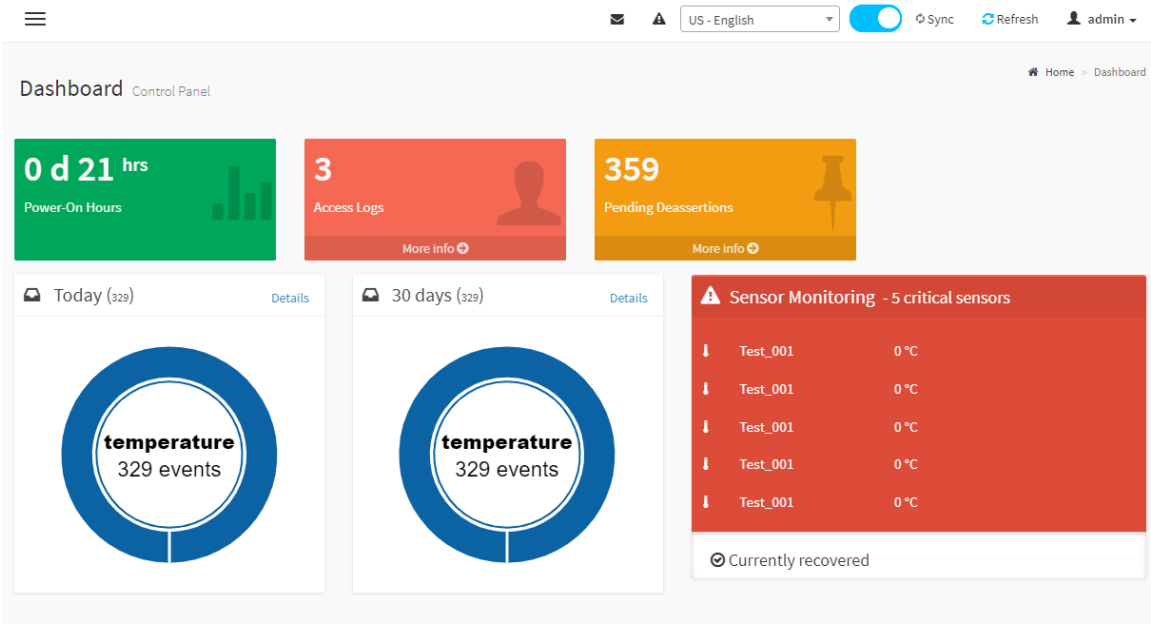


A brief description of the Dashboard page is given below.

The **Dashboard** page displays **Power On Hours** and **Access Logs** information alone, when the toggle button is in OFF state in Dashboard page.

When toggle button is switched to ON state, it displays the **Power On Hours**, **Access Logs**, **Pending Deassertions**, **Today & 30 Days (Event Logs)** and **Sensor Monitoring** information. A sample screenshot is displayed below.

Note: This toggle button is available only in Dashboard page to display the information based on requirement.



Language Selection

Change the language to view the language strings in different languages.

Power On Hours

BMC Power-On Hours will keep on accumulated and will be reset to zero when you flash a new image.

Pending Deassertions

It lists all the asserted events which are waiting for deassert state. To know about the pending events details, click the **More info** link. This navigates to the **Event Log** page and display all the asserted events that are waiting for deassertion.

Access Logs

A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed. If you click on the **More info** link, you can view the **Audit Log** page.

Today & 30 Days (Event Logs)

This page displays the list of event logs occurred by the different sensors on this device. Click **Details** link on Today and 30 days to view the event logs for Today and 30 days respectively.

Sensor Monitoring

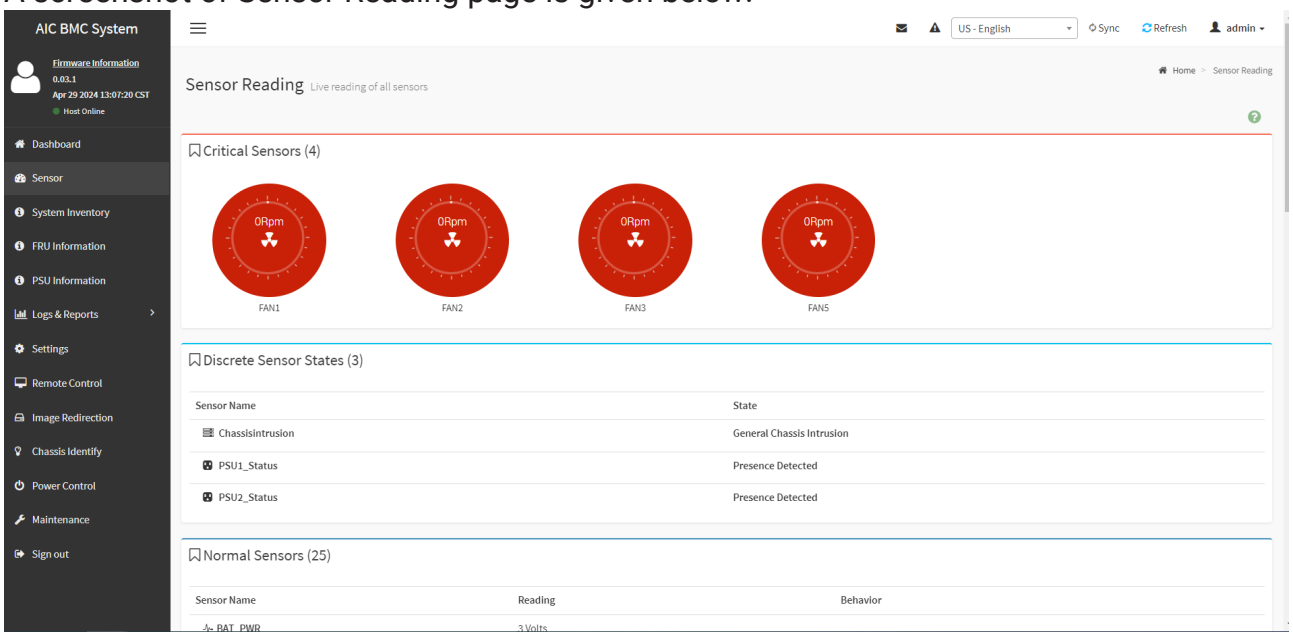
It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

Chapter 6. Sensor

The Sensor Reading page displays all the sensor related information.

To open the Sensor Reading 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.

A screenshot of Sensor Reading page is given below.



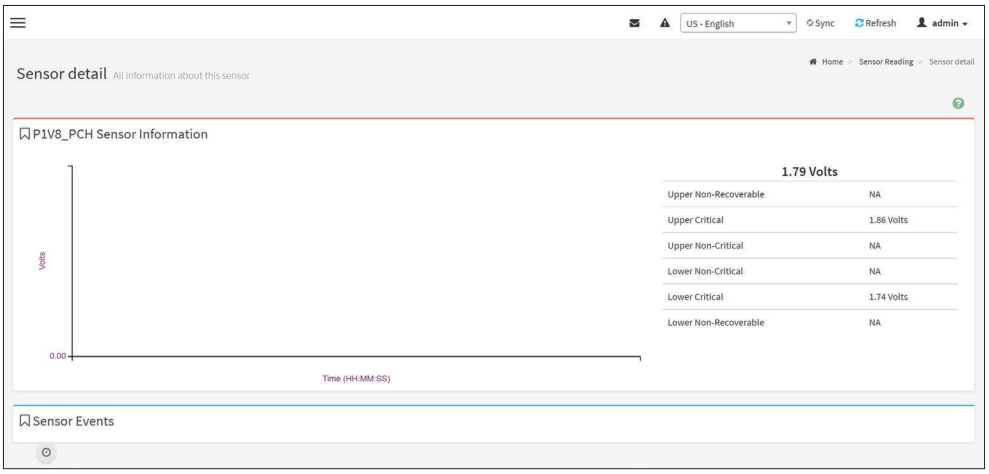
Sensor Readings Page

The Sensor Reading 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.

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.



Sensor detail

> **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.

Sensor Events

You can view the event logs for the selected sensor.

Thresholds are of six types:

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

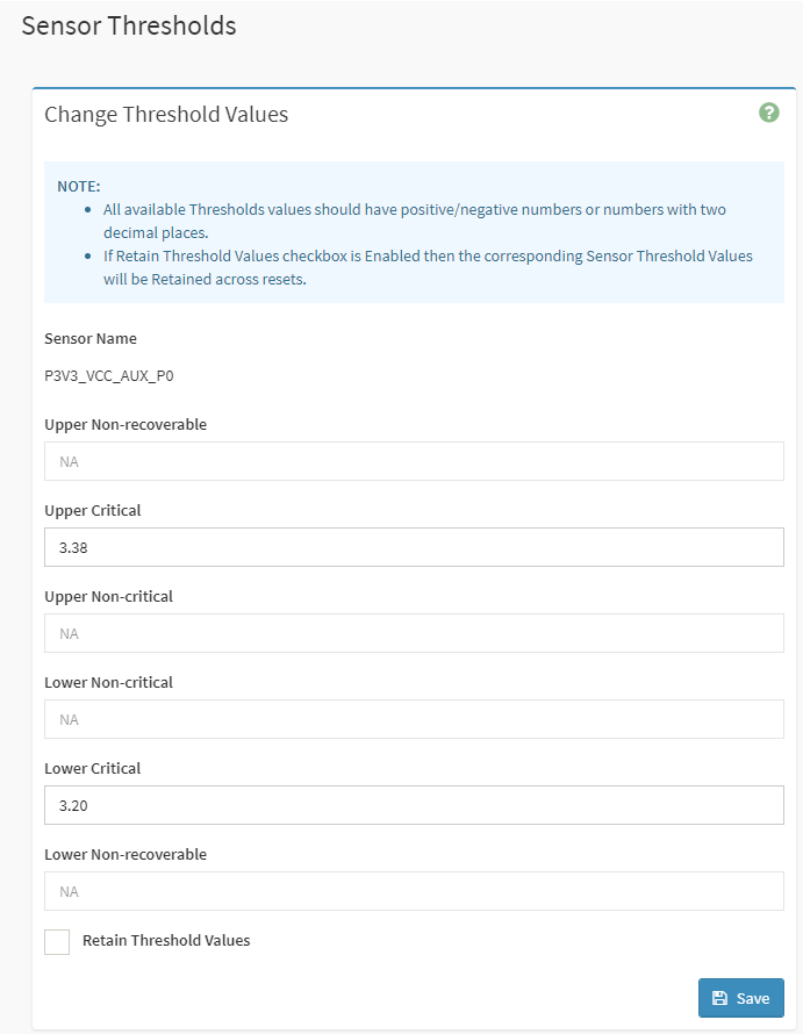
The threshold states could be

- 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

Threshold Settings

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



Threshold Settings

2. Enter the Threshold values.

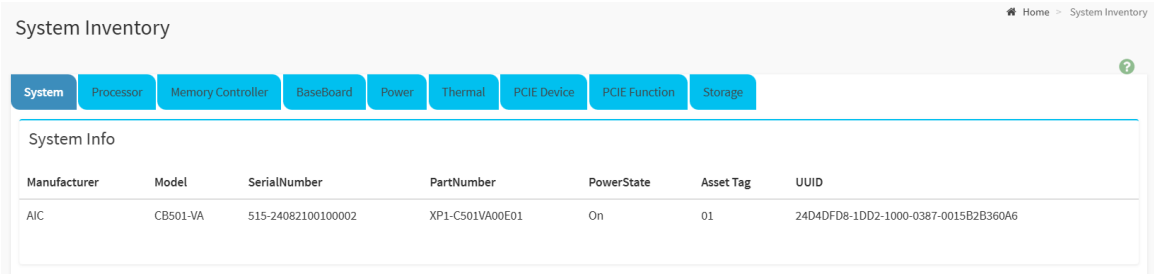
> **NOTE**
> The Threshold Settings will be enabled only for administrator or operator privilege users.
> For other users the Threshold Settings option will be disabled and they can't access to perform this action.

3. Retain Threshold Values - If Retain Threshold Values checkbox is enabled, then the corresponding Sensor Threshold values will be retained across resets.
4. Click **Save** to configure the threshold values.

Chapter 7. System Inventory

To open System Inventory main page, click **System Inventory** from the menu bar.

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

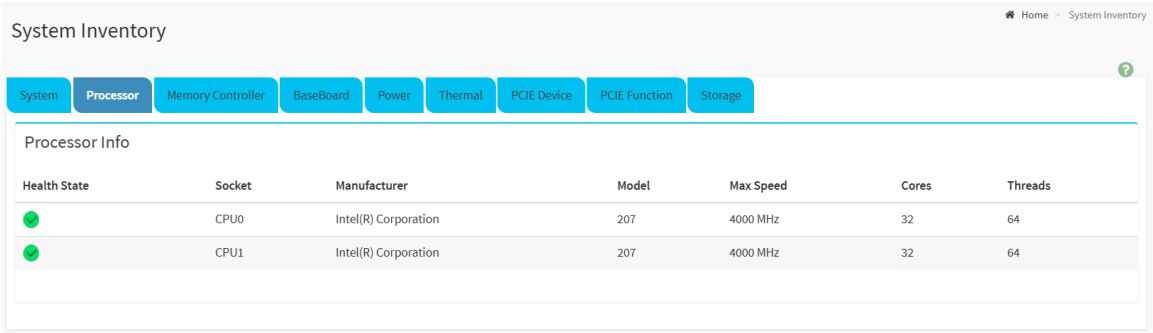


7.1 System Info

This page displays the System information in the System tab. The System tab displays the fields like Manufacturer, Model, Serial Number, Part Number, Power State, Asset Tag and UUID.

7.2 Processor Info

This tab displays Processor information. A sample screenshot of Processor Info is displayed below.



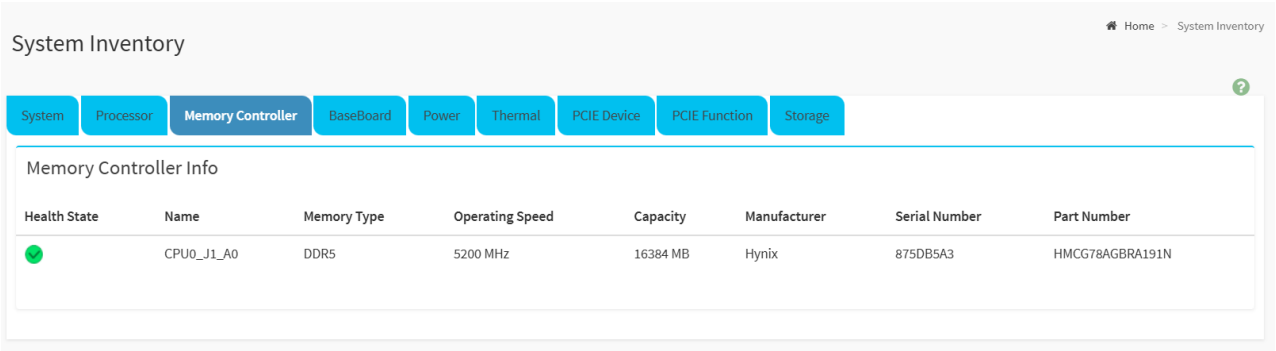
The Processor information displays the fields like Health State, Socket, Manufacturer, Model, Max Speed, Cores and Threads.

The meaning of the Health Status icons:

- Normal
- Critical
- Does not exis

7.3 Memory Controller Info

This tab displays Memory Controller information. A sample screenshot of Memory Controller Info is displayed below.



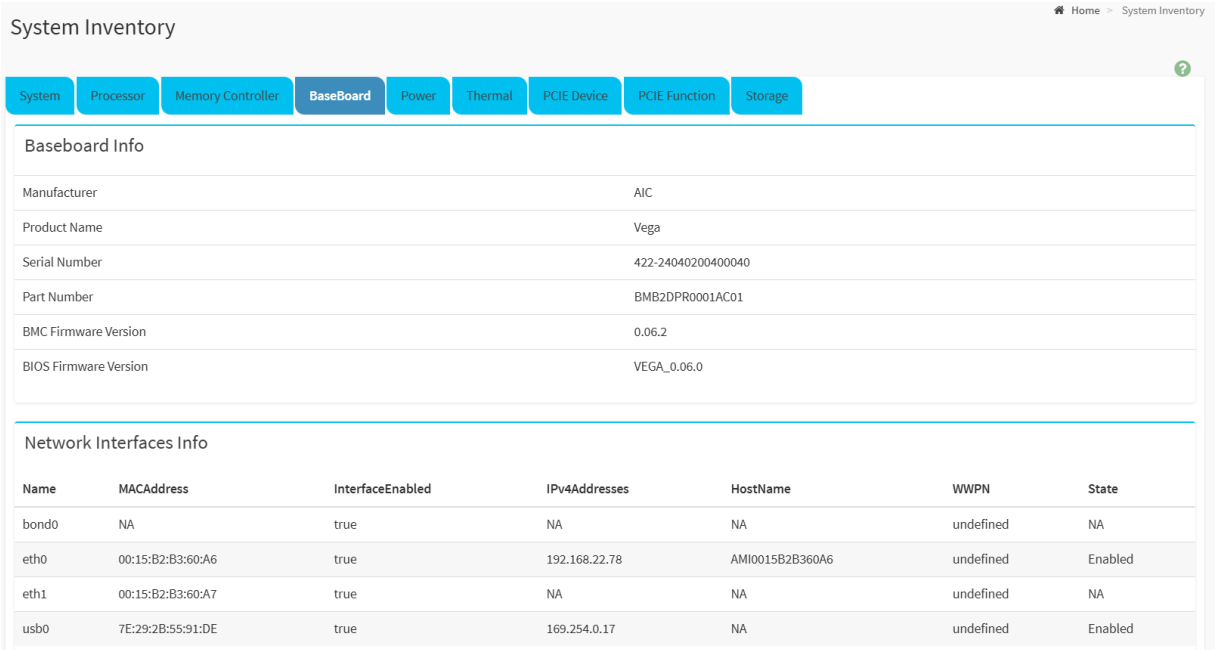
The various fields of Memory Controller information are as follows. The fields are Health State, Name, Memory Type, Operating Speed, Capacity, Manufacturer, Serial Number and Part Number.

The meaning of the Health Status icons:

- Normal
- Critical

7.4 Base Board Info

This tab displays Base Board information and Network interfaces information. A sample screenshot of BaseBoard Info is displayed below.



The various fields of Baseboard Info are mentioned below.

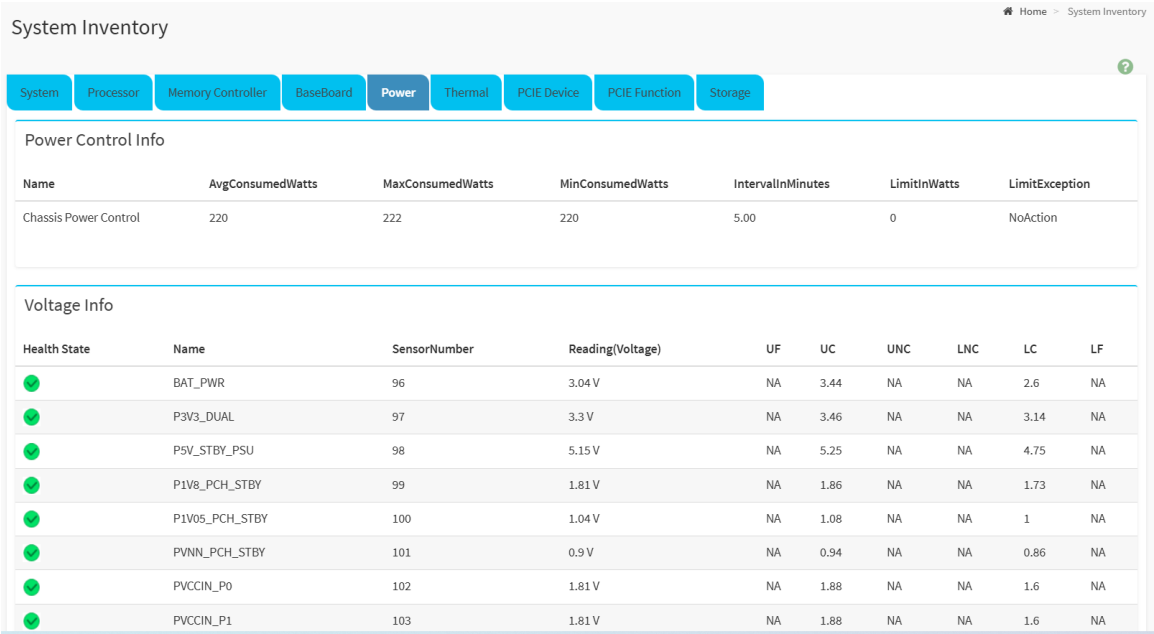
- Manufacturer
- Product Name
- Serial Number
- Part Number
- BMC Firmware Version
- BIOS Firmware Versoion

The various fields of Network Interfaces Info are mentioned below.

- Name
- IPv4 Addresses
- State
- MAC Address
- Host Name
- Interface Enabled
- WWPN

7.5 Power Info

This tab displays Power information including Power Control and Voltage information. A sample screenshot of Power Info is displayed below.



Name	AvgConsumedWatts	MaxConsumedWatts	MinConsumedWatts	IntervalInMinutes	LimitInWatts	LimitException
Chassis Power Control	220	222	220	5.00	0	NoAction

Health State	Name	SensorNumber	Reading(Voltage)	UF	UC	UNC	LNC	LC	LF
	BAT_PWR	96	3.04 V	NA	3.44	NA	NA	2.6	NA
	P3V3_DUAL	97	3.3 V	NA	3.46	NA	NA	3.14	NA
	P5V_STBY_PSU	98	5.15 V	NA	5.25	NA	NA	4.75	NA
	P1V8_PCH_STBY	99	1.81 V	NA	1.86	NA	NA	1.73	NA
	P1V05_PCH_STBY	100	1.04 V	NA	1.08	NA	NA	1	NA
	PVNN_PCH_STBY	101	0.9 V	NA	0.94	NA	NA	0.86	NA
	PVCCIN_P0	102	1.81 V	NA	1.88	NA	NA	1.6	NA
	PVCCIN_P1	103	1.81 V	NA	1.88	NA	NA	1.6	NA

The various fields of Power Control information are as follows. The Power Control information contains each field like Name, Avg Consumed Watts, Max Consumed Watts, Min Consumed Watts, Interval In Minutes, Limit In Watts, and Limit Exception.

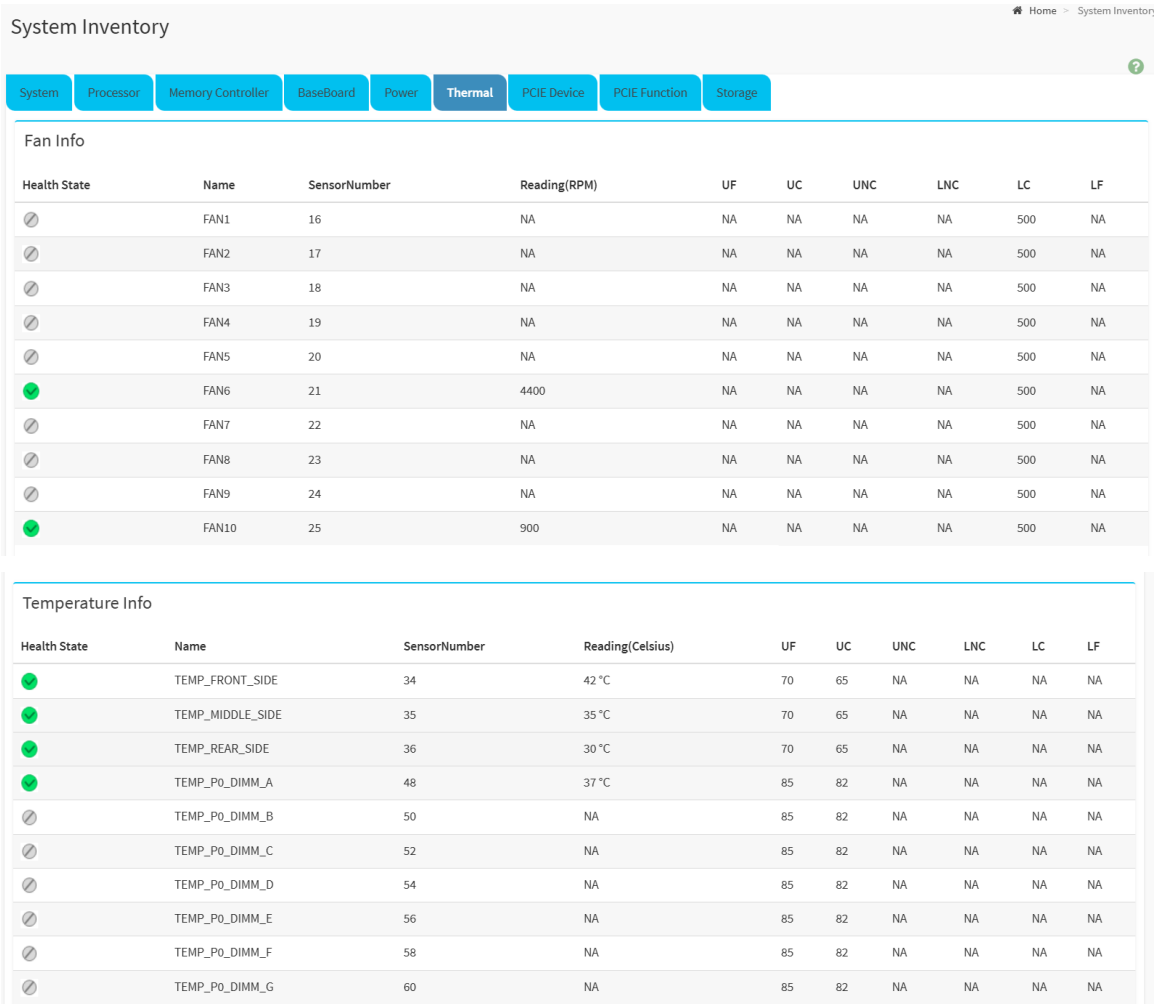
The Voltage information contains each field like Health State, Name, Sensor Number, Reading (Voltage), UF, UC, UNC, LNC, LC and LF.

The meaning of the Health Status icons:

- Normal
- Critical
- Does not exis

7.6 Thermal Info

This tab displays Thermal information including Voltage and Temperature information. A sample screenshot of Thermal Info is displayed below.



Health State	Name	SensorNumber	Reading(RPM)	UF	UC	UNC	LNC	LC	LF
	FAN1	16	NA	NA	NA	NA	NA	500	NA
	FAN2	17	NA	NA	NA	NA	NA	500	NA
	FAN3	18	NA	NA	NA	NA	NA	500	NA
	FAN4	19	NA	NA	NA	NA	NA	500	NA
	FAN5	20	NA	NA	NA	NA	NA	500	NA
	FAN6	21	4400	NA	NA	NA	NA	500	NA
	FAN7	22	NA	NA	NA	NA	NA	500	NA
	FAN8	23	NA	NA	NA	NA	NA	500	NA
	FAN9	24	NA	NA	NA	NA	NA	500	NA
	FAN10	25	900	NA	NA	NA	NA	500	NA

Health State	Name	SensorNumber	Reading(Celsius)	UF	UC	UNC	LNC	LC	LF
	TEMP_FRONT_SIDE	34	42 °C	70	65	NA	NA	NA	NA
	TEMP_MIDDLE_SIDE	35	35 °C	70	65	NA	NA	NA	NA
	TEMP_REAR_SIDE	36	30 °C	70	65	NA	NA	NA	NA
	TEMP_P0_DIMM_A	48	37 °C	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_B	50	NA	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_C	52	NA	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_D	54	NA	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_E	56	NA	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_F	58	NA	85	82	NA	NA	NA	NA
	TEMP_P0_DIMM_G	60	NA	85	82	NA	NA	NA	NA

The various fields of Thermal information are as follows. The Fan Info contains the fields like Health State, Name, Sensor Number, Reading (RPM), UF, UC, UNC, LNC, LC and LF.

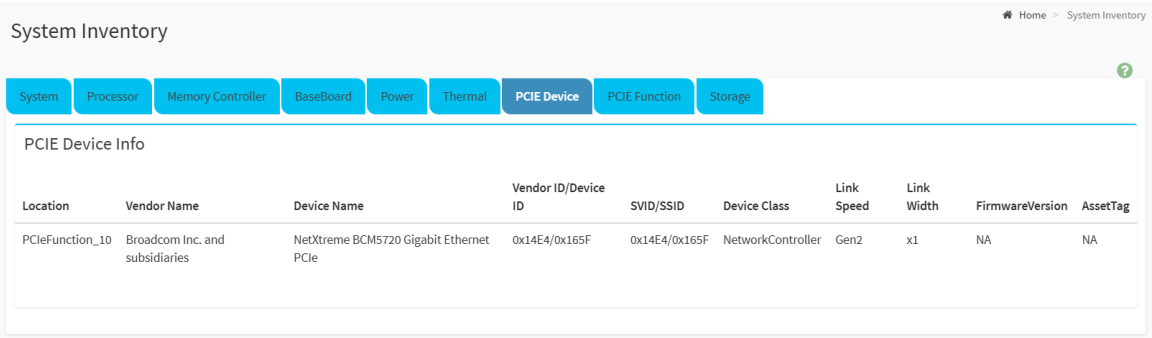
The Temperature information contains each field like Health State, Name, Sensor Number, Reading (Celsius), UF, UC, UNC, LNC, LC and LF.

The meaning of the Health Status icons:

- Normal
- Critical
- Does not exis

7.7 PCIE Device Info

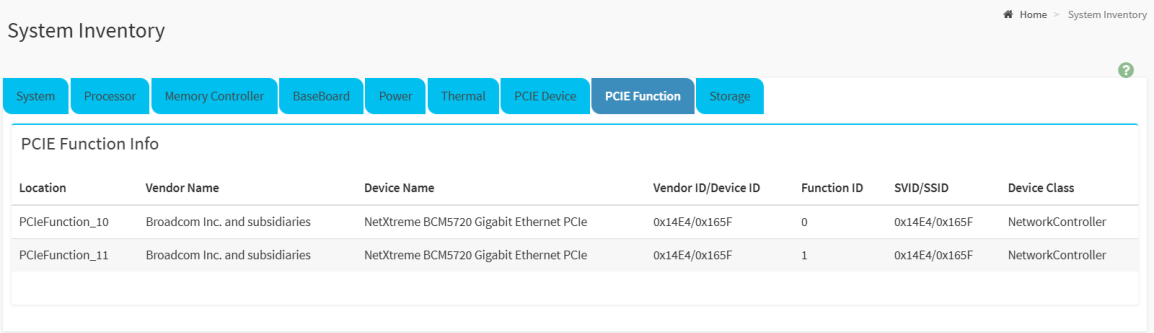
This tab displays PCIE Device information. A sample screenshot of PCIE Device Info is displayed below.



The PCIE Device information displays the fields like Location, Vendor Name, Device Name, Vendor ID/Device ID, SVID/SSID, Device Class, Link Speed, Link Width, FirmwareVersion and AssetTag.

7.8 PCIE Function

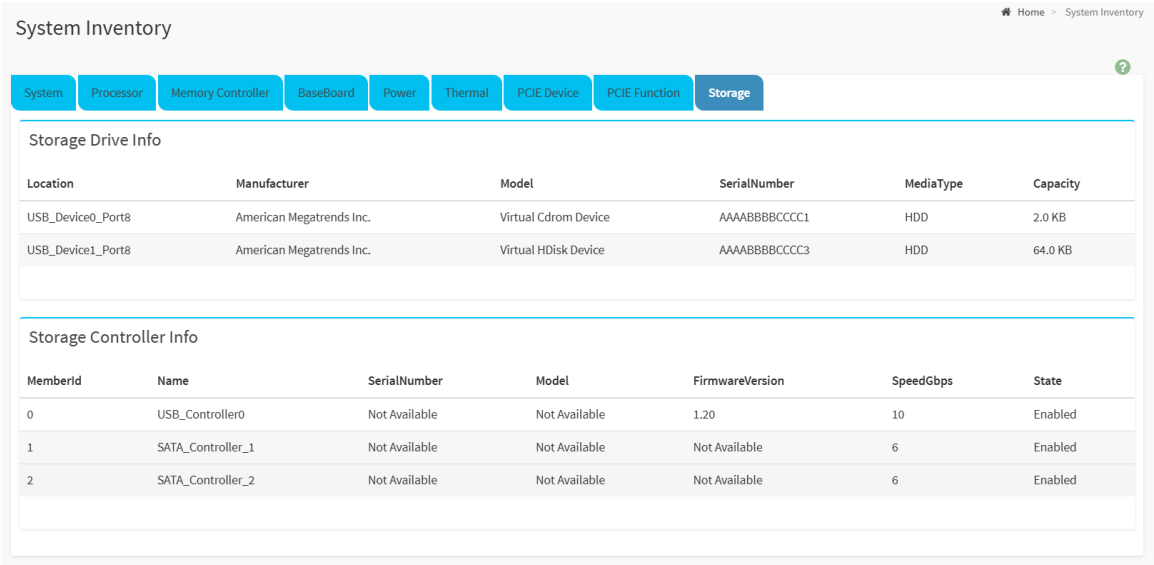
This tab displays PCIE Function information. A sample screenshot of PCIE Function Info is displayed below.



The PCIE Function information displays the fields like Location, Vendor Name, Device Name, Vendor ID/Device ID, Function ID, SVID/SSID, and Device Class.

7.9 Storage Info

This tab displays the Storage information including Storage Drive and Storage Controller information. A sample screenshot of Storage Info is displayed below.



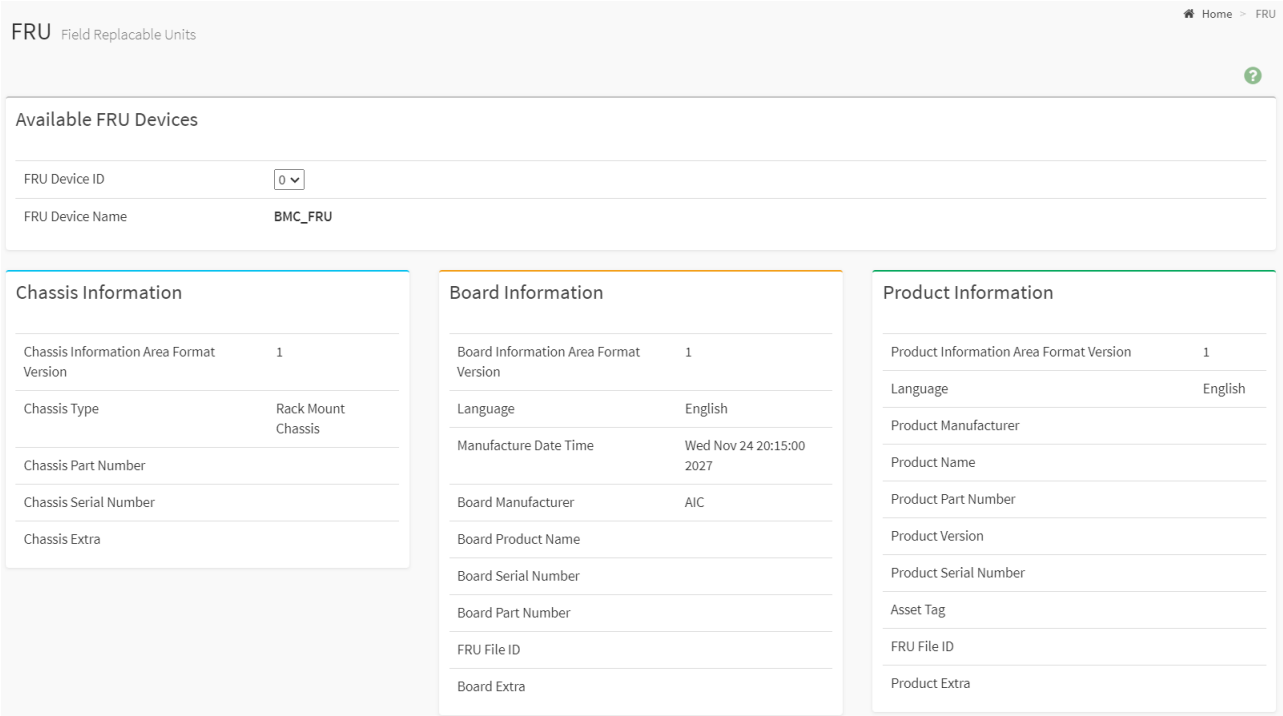
The various fields of Storage Drive Info are as follows. The Storage Drive Info contains each field like Location, Manufacturer, Model, Serial Number, Media Type and Capacity.

The Storage Controller Info contains each field lick MemberId, Name, Serial Number, Model, Firmware Version, SpeedGbps and state.

Chapter 8. FRU Information

FRU Information 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 **FRU Information** from the menu bar. 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 Information Page

The following fields are displayed here for selected device.

Available FRU Devices

- FRU device ID - Select the device ID from the drop down list
- 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

Board Information

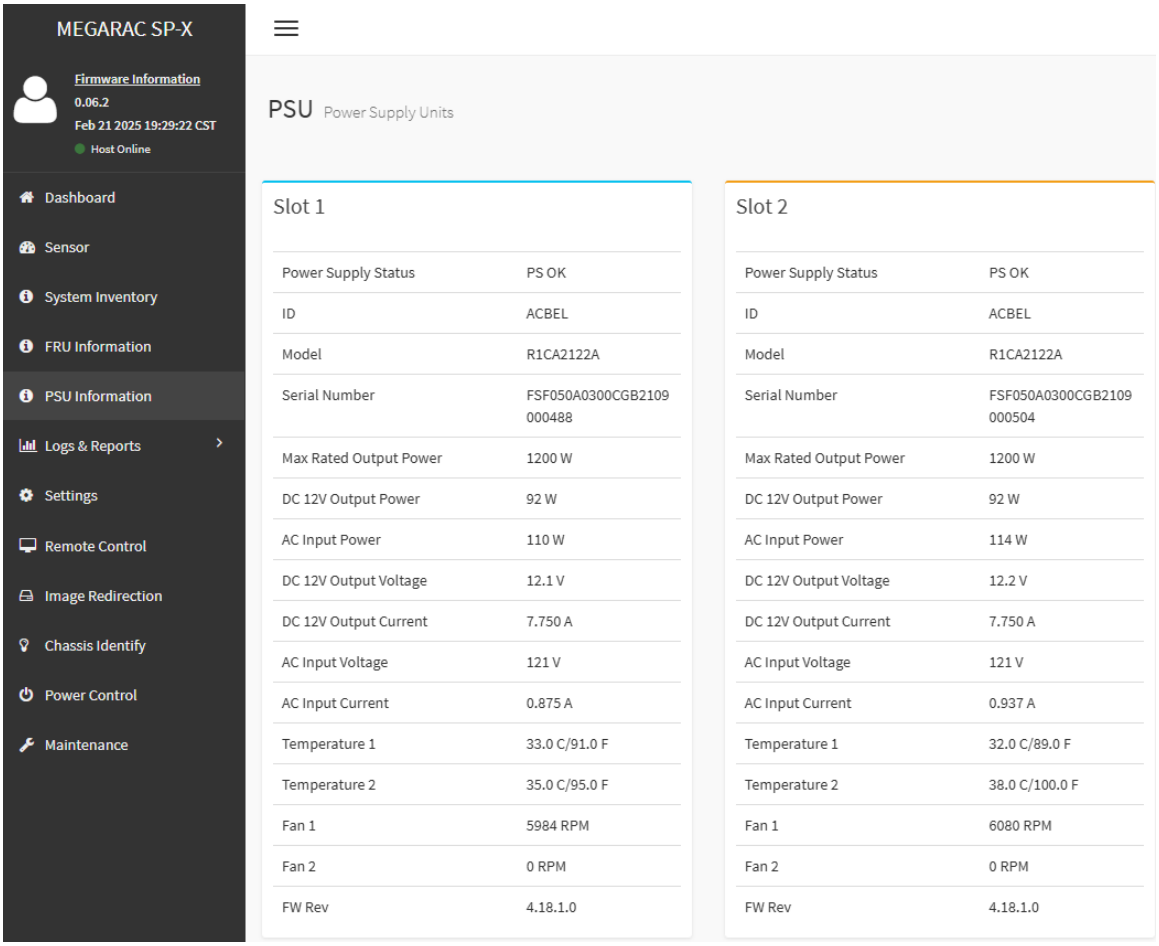
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

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

Chapter 9. PSU Information

To open the PSU Information page, click **PSU Information** from the menu bar. A screenshot of PSU Information page is given below.



The following fields are displayed here.

- **Slot 1/2/3/4**: Represents PSU1/2/3/4
- **Power Supply Status**:
  - PS OK: Indicates the status when the power supply is functioning normally.
  - PS Off: Indicates the status when the power supply is turned off or not operational.
- **ID**: Specifies vender ID of the power supply unit.
- **Model**: Specifies the model number of the power supply unit.
- **Serial Number**: Provides the unique serial number assigned to the power supply unit.
- **Max Rated Output Power**: Shows the maximum rated output power of the power supply unit.
- **DC 12V Output Power**: Shows the total power output from the power supply unit.
- **AC Input Power**: Displays the power consumed by the power supply unit from the AC

source.

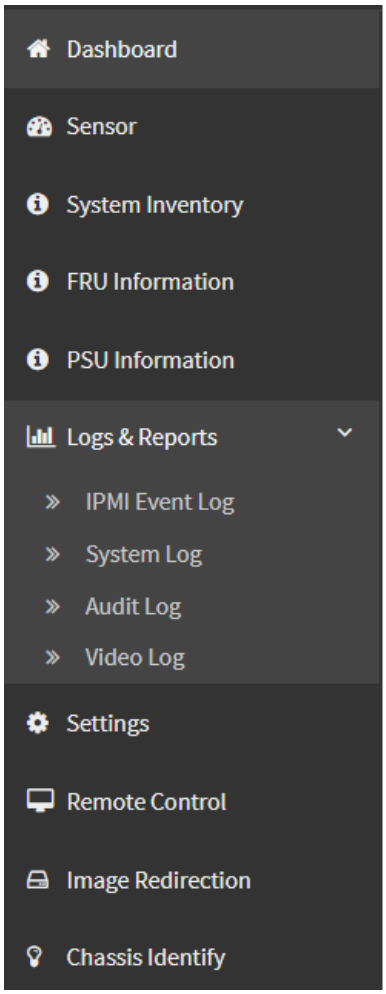
- **DC 12V Output Voltage**: Indicates the voltage output from the power supply unit.
- **DC 12V Output Current**: Shows the current being supplied by the power supply unit.
- **AC Input Voltage**: Shows the input voltage from the AC power source.
- **AC Input Current**: Displays the current drawn from the AC power source.
- **Temperature 1**: Displays the temperature reading from sensor 1 on the power supply unit.
- **Temperature 2**: Displays the temperature reading from sensor 2 on the power supply unit.
- **Fan 1**: Indicates the rotational speed of the fan 1 on the power supply unit.
- **Fan 2**: Indicates the rotational speed of the fan 1 on the power supply unit.
- **FW Rev**: Indicates the firmware revision of the power supply unit.

Chapter 10. Logs & Reports

To open the Logs & Reports page, click **Logs & Reports** from the menu bar. The Logs & Reports page displays the following information.

- IPMI Event Log
- System Log
- Audit Log
- Video Log

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

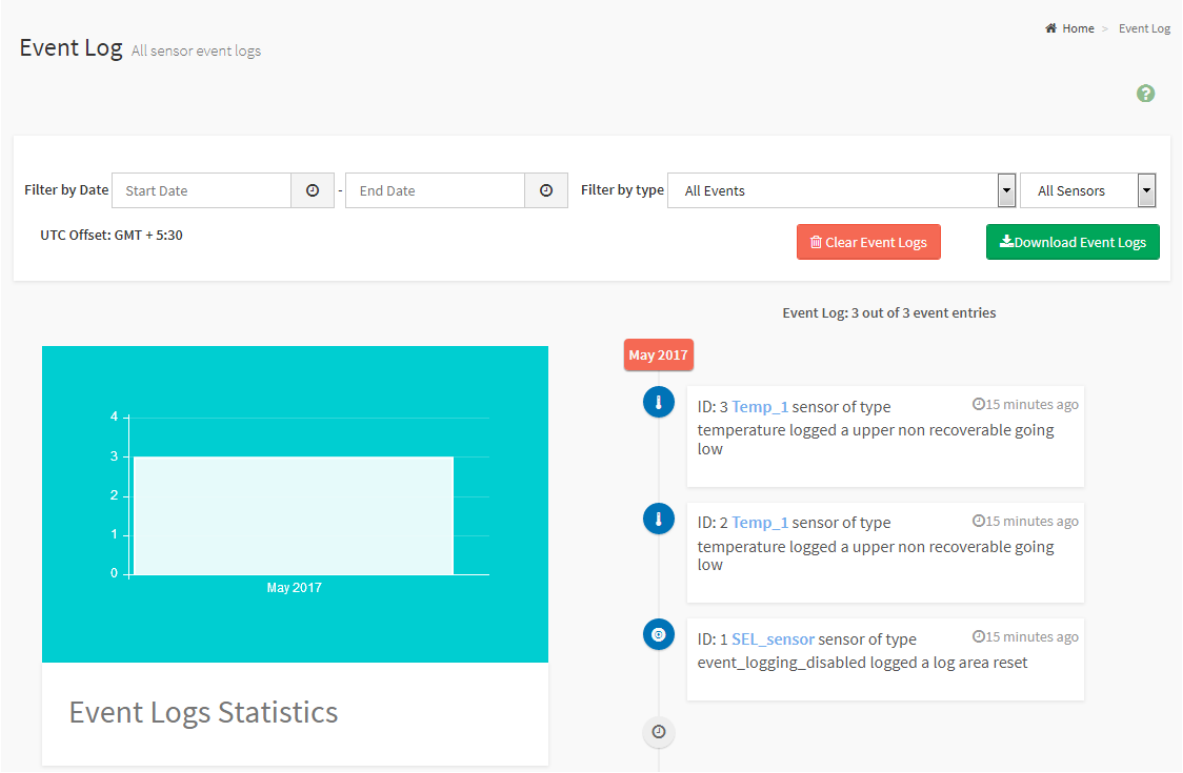


10.1 IPMI Event Log

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 Event** from the menu bar.

A sample screenshot of Event Log page is shown below.



Event Log Page

The Event Log page consists of the following Fields.

Filter By Date: Filtering can be done by selecting **Start Date** and **End Date** using **Calender**.

> **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.

> **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.

UTC Offset: Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.

Event Log Statistics: Displays the statistical graph for the selected date.

Clear Event Logs: To delete all the event logs.

Download Event Logs: To download the event 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** name 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 Event Logs**.
4. To download the event logs, click **Download Event Logs**.

> **NOTE**
> When Clear All Event Logs action is performed, there might be some events present even after clearing those events are generated after performing clear operation which can be verified using its time stamp.

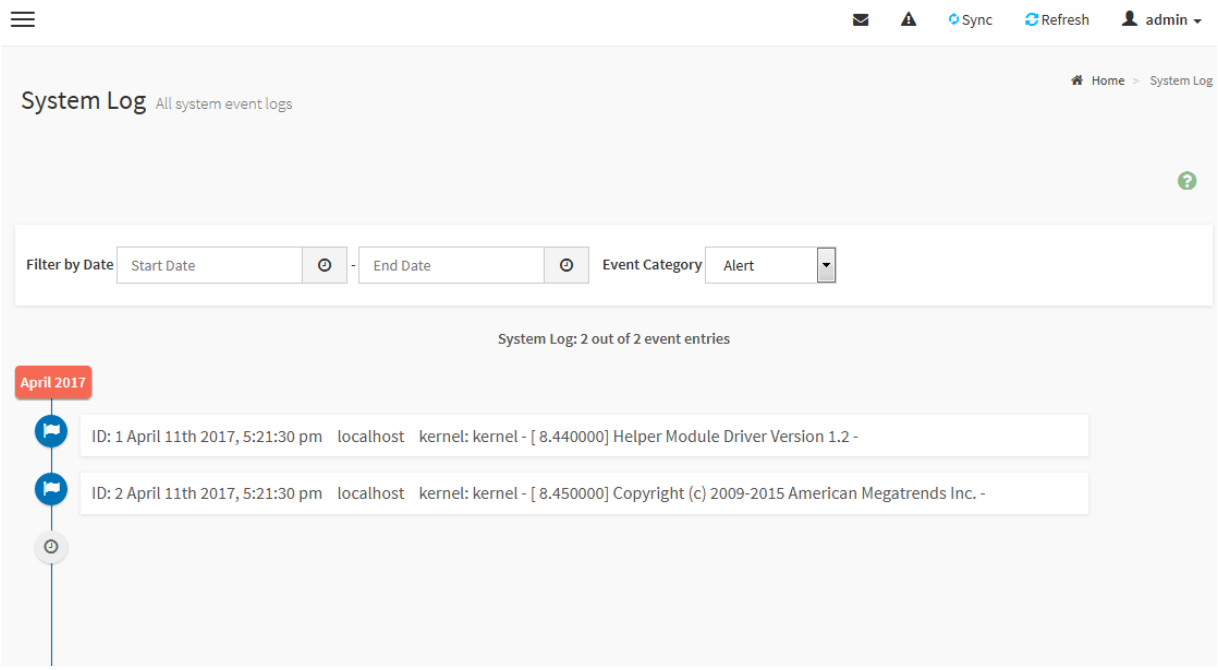
10.2 System Log

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

> **NOTE**
> Logs have to be configured under **Settings** → **Log Settings** in order to display any entries.

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

A sample screenshot of System Log page is shown below.



Procedure

To view **System Log**, click the **System Log** tab to view all system events. Entries can be filtered based on **Filter By Date** (Start Date and End Date) and **Event Category** like Alert, Critical, Error, Notification, Warning, Debug, Emergency and Information.

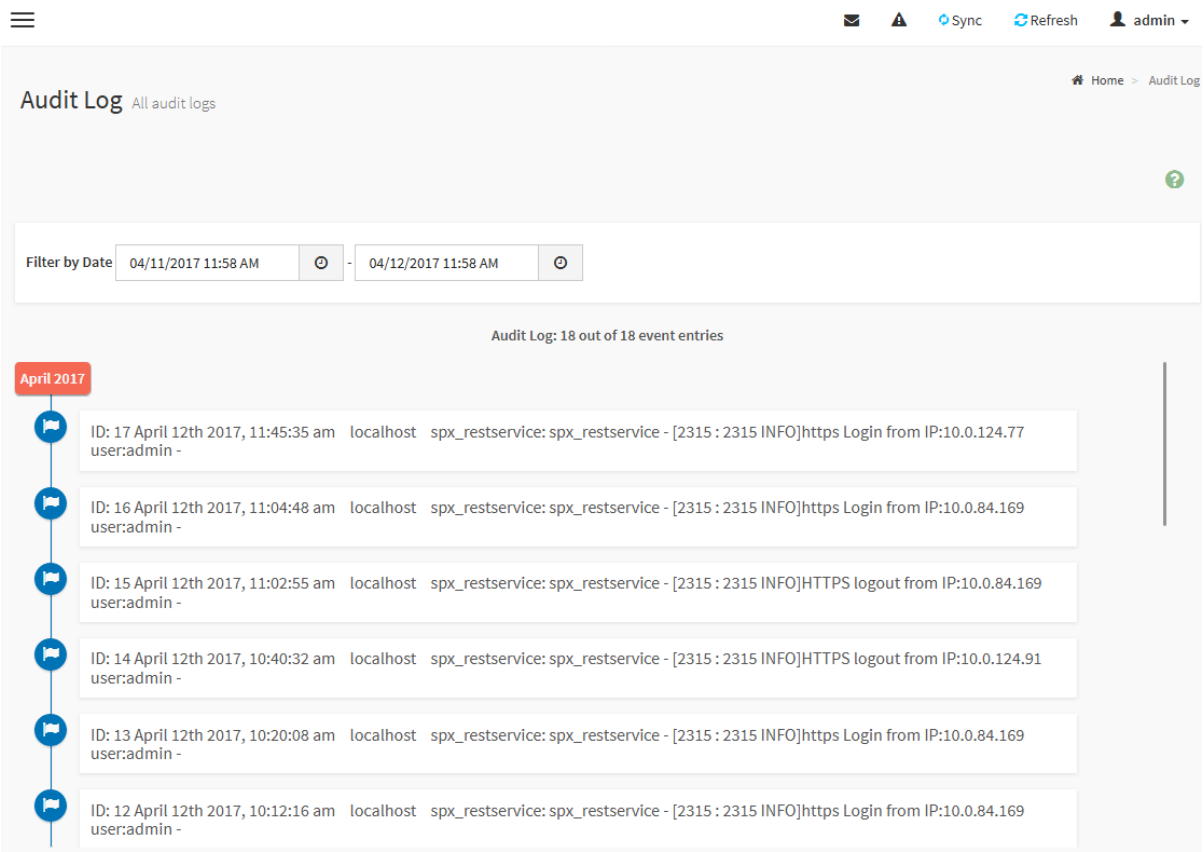
10.3 Audit Log

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

> **NOTE**
> Logs have to be configured under **Settings → Log Settings → Advanced Log Settings** in order to display any entries.

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

A sample screenshot of Audit Log page is shown below.



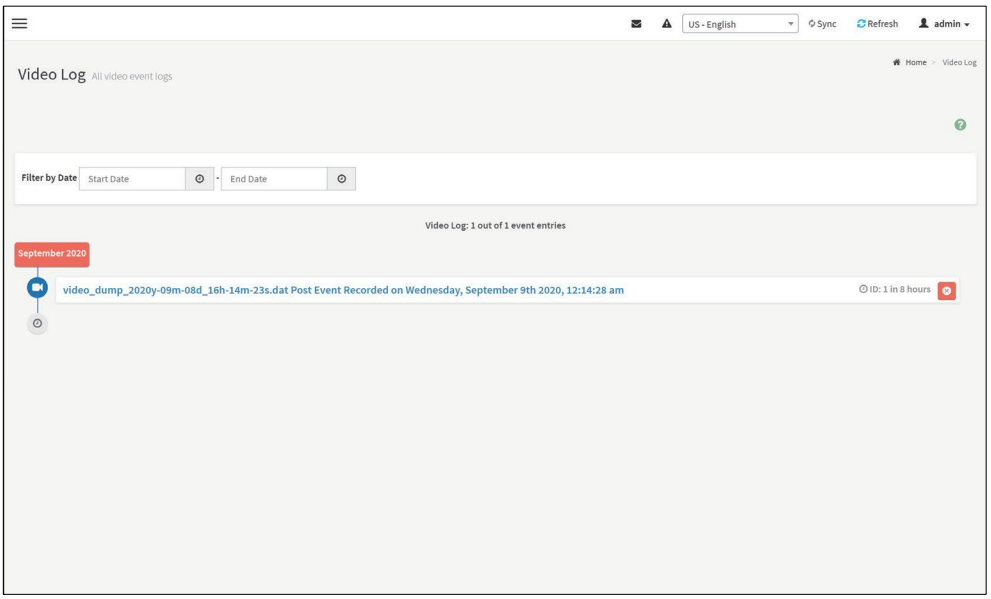
Procedure

To view Audit Log, click the **Audit Log** tab to view all audit events for this device.

10.4 Video Log

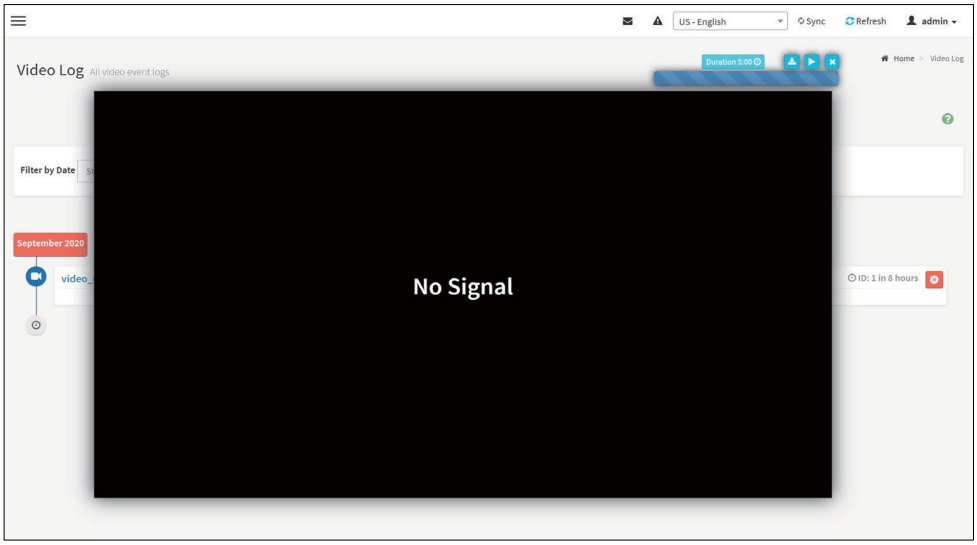
To open the Video Log page, click **Logs & Reports** → **Video Log** from the menu bar. A sample screenshot of Video Log page is shown below.

> **NOTE**
> 1. Video Trigger Settings should be enabled, to display the Video Log page. Video Trigger Settings can be configured under **Settings → Video Recording → Auto Video Settings → Video Trigger Settings**.
> 2. When user navigates to new tab or web page while the video is still playing, then user needs to restart the video and WebUI will pop-up the error message like "Navigated to another tab or page. Kindly relaunch video player application".



Video Log

1. Click on the **Video Log entry** to view the Video. A sample screenshot of Video Log - Video page is shown below.

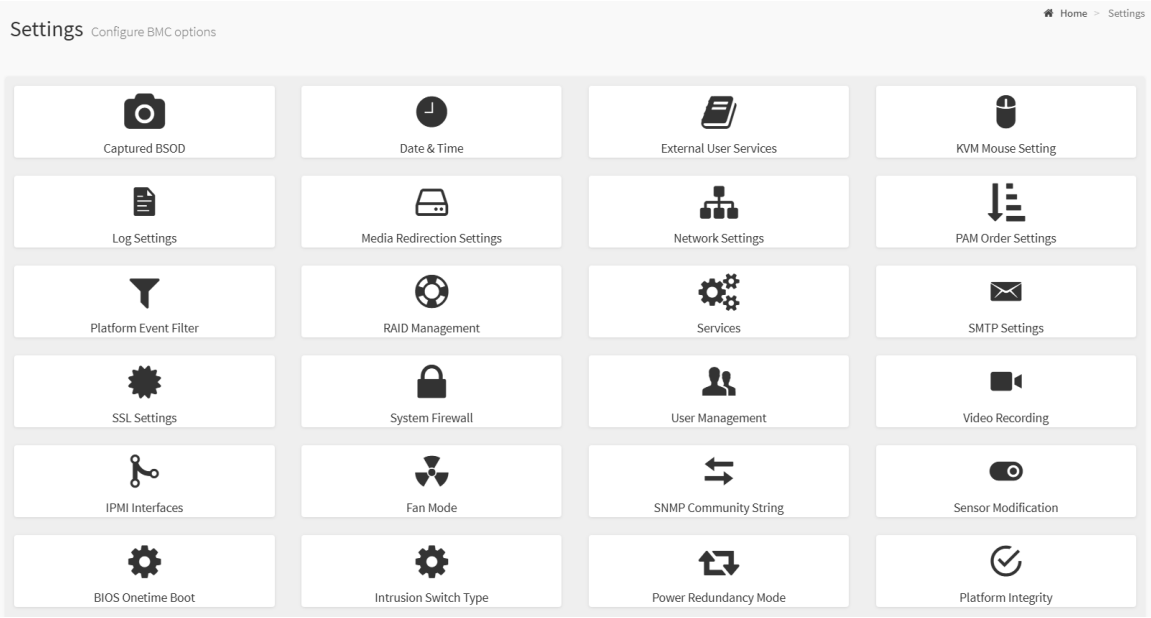


2. You can Download ( ), Play/Pause ( ) and Delete ( ) the video by clicking the respective icons.

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.
The video data may not be proper if the browser zoom in/out settings are changed during video playback.
The generated video file can be played only using WebUI or Java player application. It cannot be played using other media players.

Chapter 11. Settings

To open the Settings page, click **Settings** from the menu bar. This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.

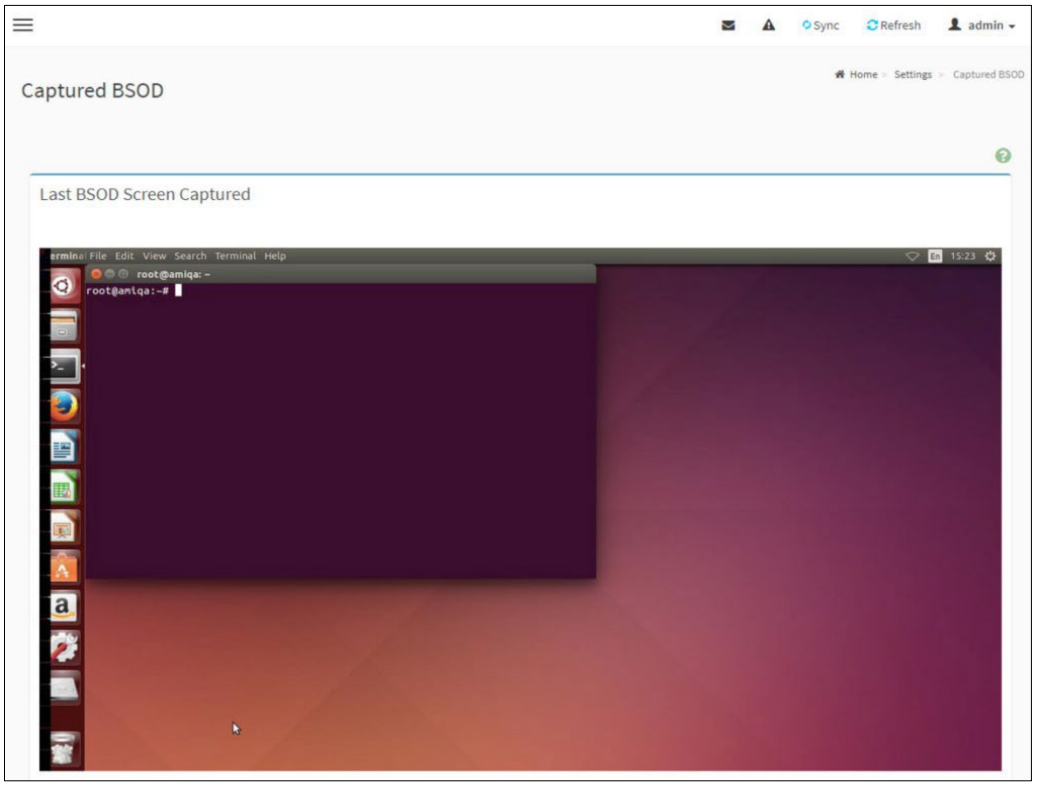


A detailed description of the Configuration menu is given below.

11.1 Captured BSOD

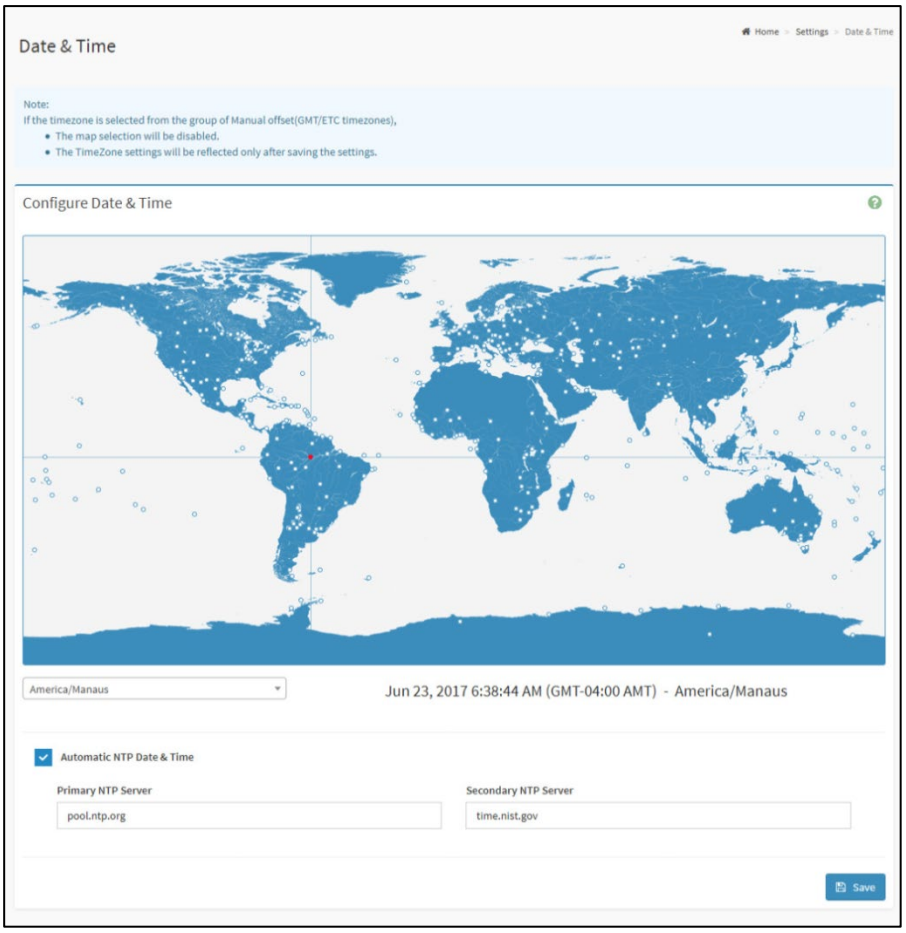
This page displays a snapshot of the blue screen captured if the host system crashed since last reboot. A screenshot of Captured BSOD is shown below.

> **NOTE**
> KVM service should be enabled to display the BSOD screen. KVM Service can be configured under **Settings → Services → KVM**.



11.2 Date and 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 - Automatic 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.

> **NOTE**
> Based on the manual selection of GMT or ETC/GMT, time zone alone will be changed and date & time will remain the same.

Automatic Date & Time: To automatically synchronize Date and Time with the NTP Server.

- **Primary NTP Server**: To configure a primary NTP server to use when automatically setting the date and time.

  The following address formats & Domain name format are supported.

  - IPv4 Address format

- IPv6 Address format
- Domain name format allowed ‘A-Z’, ‘a-z’, ‘0-9’, dash(-), underscore(_) and dot(.) characters

- **Secondary NTP Server**: To configure a secondary NTP server to use when automatically setting the date and time.

  The following address formats & Domain name format are supported.

  - IPv4 Address format
  - IPv6 Address format
  - Domain name format allowed ‘A-Z’, ‘a-z’, ‘0-9’, dash(-), underscore(_) and dot(.) characters
- **Automatic PTP Date & Time**: To enable/disable the use of PTP servers to automatically set the date and time.
- **PTP Interface**: To confifigure a PTP server interface to use when automatically setting the date and time.
- **PTP Preset**: To confifigure a PTP Preset type to use when automatically setting the date and time.
- **PTP Transport**: To confifigure a PTP Transport type to use when automatically setting the date and time.
- **PTP Ipmode**: To confifigure a PTP Ipmode type to use when automatically setting the date and time.
- **PTP Unicast IP**: To confifigure a Unicast ip when ipmode is unicast and server to use when automatically setting the date and time.
- **PTP Delay Mechanism**: To confifigure a PTP Delay Mechanism type to use when automatically setting the date and time.
- **PTP Inbound Latency**: To confifigure a Inbound latency of the server to use when automatically setting the date and time.
- **PTP Outbound Latency**: To confifigure a PTP outbound latency server to use when automatically setting the date and time.
- **PTP Priority1**: To confifigure a priority of PTP clock to use when automatically setting the date and time.
- **PTP Max Master capacity**: To confifigure a max master capacity of the PTP clock to use when automatically setting the date and time.
- **Panic Mode**: To confifigure a PTP clock to not reset if jump is more then 1 second, use when automatically setting the date and time.
- **PTP Log request delay**: To confifigure a PTP log request delay, use when automatically setting the date and time.

Save: To save the settings.

> **NOTE**
> If the timezone is selected as Manual Offset, the map selection will be disabled. The Time-Zone settings will be reflected only after saving the settings.
> If disable the Automatic Date & Time, the time needs to select by users themselves or the time would not change.

Procedure

1. Select the **Timezone** location either using drop down or Map.
2. Enable **Automatic Date & Time** option to enable/disable the use of NTP servers to automatically set the date and time.
   A. In the **Primary NTP Server** and **Secondary NTP Server** fields, specify the NTP servers of the device respectively.

> **NOTE**
> Primary NTP Server and Secondary NTP Server should be different.

3. Enable **Automatic PTP Date & Time** to enable/disable the use of PTP servers to automatically set the date and time.
   A. Enter the Interface, Preset, Transport, Ipmode, Unicast IP, Delay Mechanism, Inbound Latency, Outbound Latency, Priority1, Max Master capacity and Log request delay details in their corresponding fields.
   B. Enable/Disable **Panic Mode** to not reset if jump is more then 1 second, use when automatically setting the date and time.
4. Click **Save** button to save the settings.

11.3 External User services

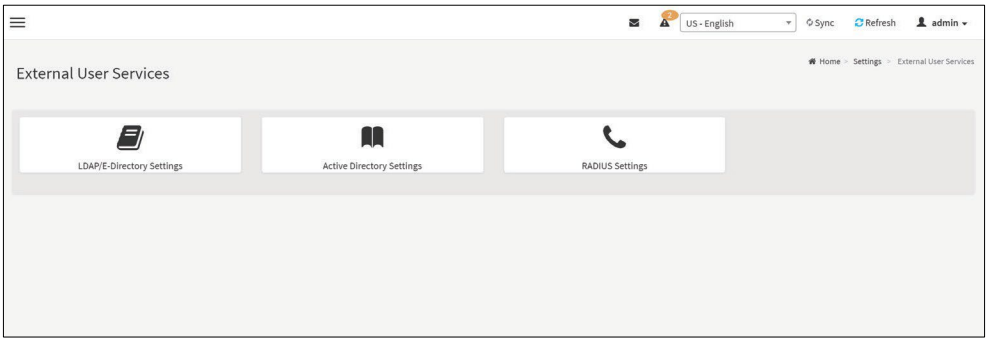
11.3.1 LDAP/E-Directory Settings

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.

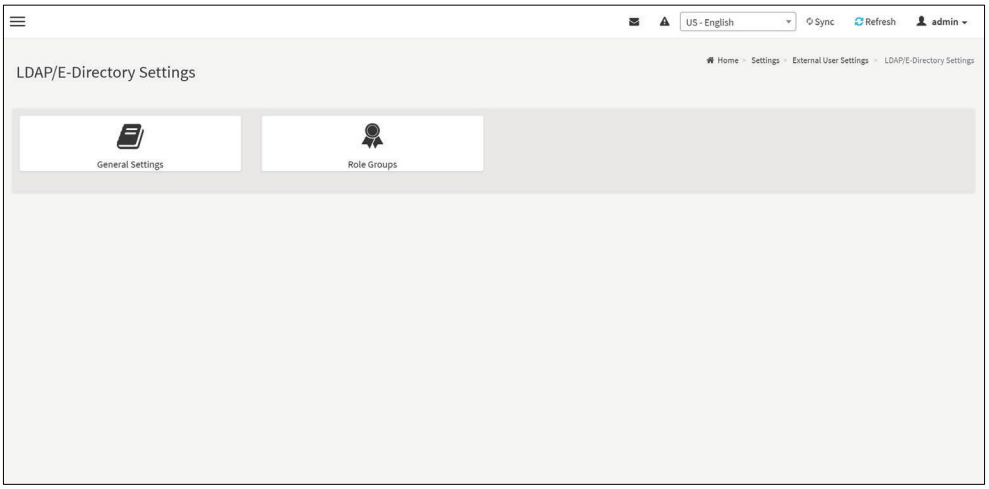
In GUI, LDAP is an Internet protocol that MegaRAC® card can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC® card users. This is done by passing login requests to your LDAP Server.

This means that there is no need to define an additional authentication mechanism, when using the MegaRAC card. 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 External User Services page, click **Settings** → **External User Services** from the menu bar. A sample screenshot of External User Services page is shown below.



To open LDAP/E-DIRECTORY Settings page, click **Settings** → **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.

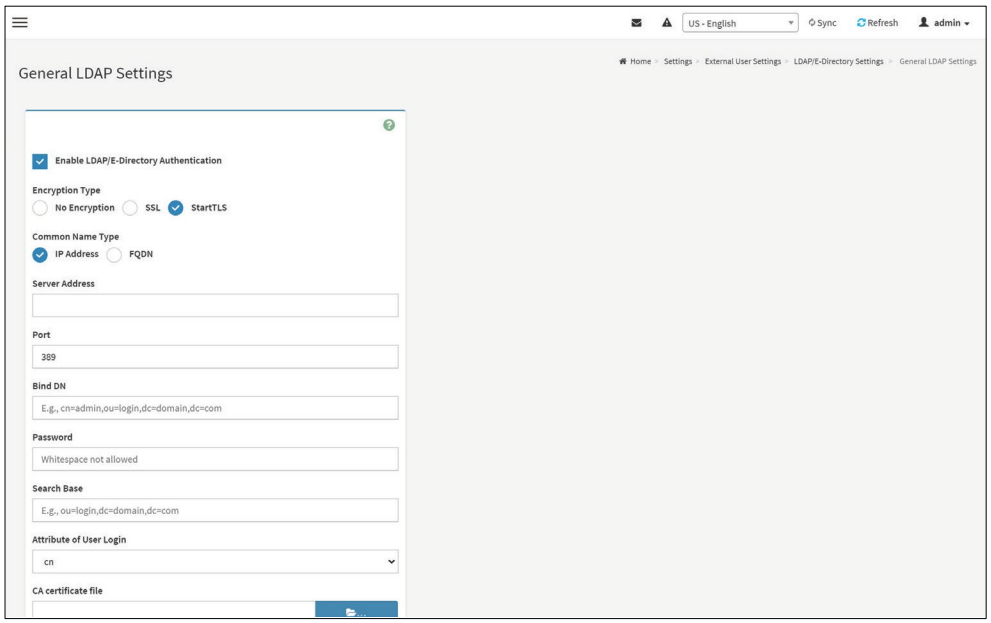
- **Role Groups**: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

> **NOTE**
> It is recommended to Enable LDAP configuration from configure general settings page otherwise error message will pop-up stating that “LDAP configuration is not enabled” while trying to create/view LDAP role groups.

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.



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.

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 FDQN address when using StartTLS with FDQN.

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 253 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 be allowed for 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 253 alpha-numeric characters.
> - It must start with an alphabetical character.
> - Special symbols like dots (.), 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.

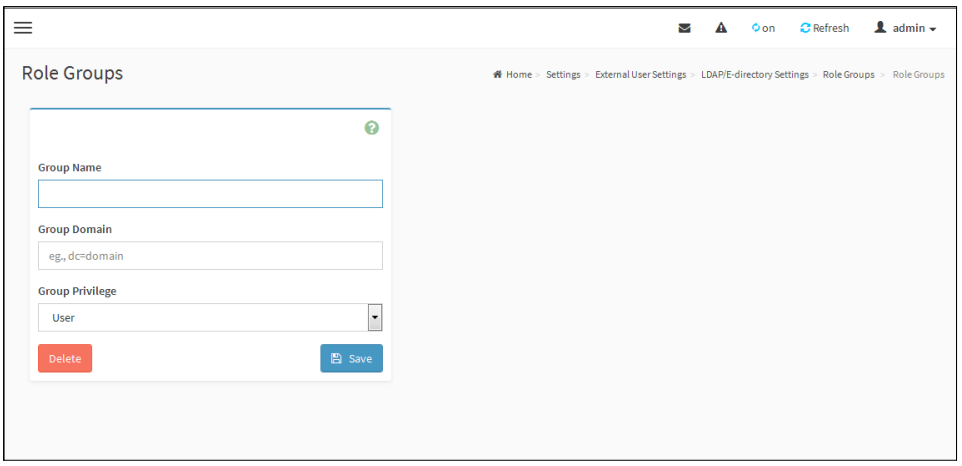
14. Click **Save** to save the settings.

To add a new Role Group

1. In the LDAP/E-Directory Settings page, click **Role Groups** and select a blank row.

> **NOTE**
> It is recommended to Enable LDAP configuration from configure general settings page otherwise error message will pop-up stating that “LDAP configuration is not enabled” while trying to create/view LDAP role groups.

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.

> **NOTE**
> Maximum size of Role Group Name is 255 bytes.
> Special symbols hyphen and underscore are allowed.

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 253 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.

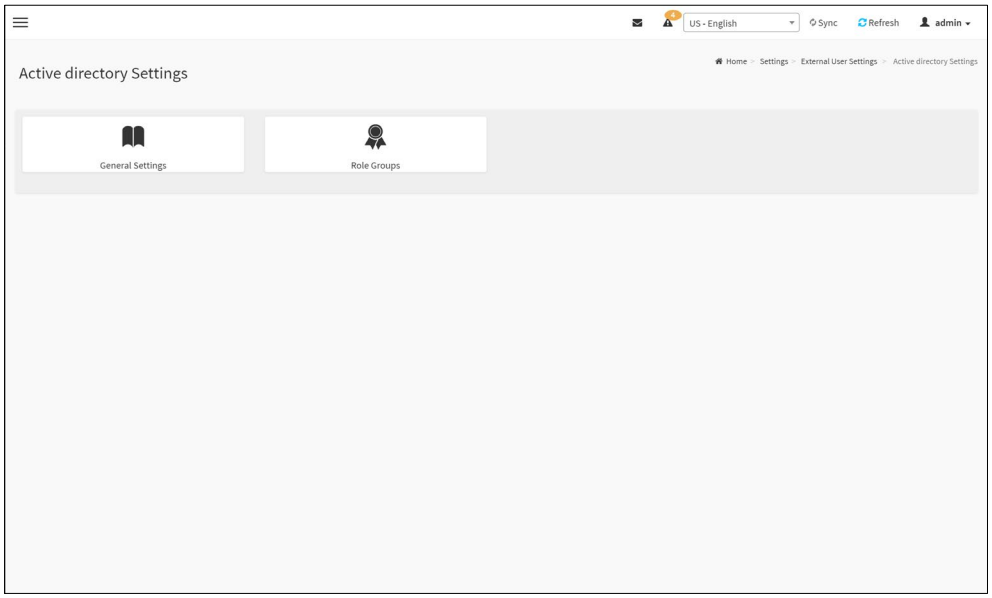
11.3.2 Active Directory Settings

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.

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** → **External User Settings** → **Active Directory** from the menu bar. A sample screenshot of Active Directory Settings page is shown below.



The fields of Active Directory page are explained below.

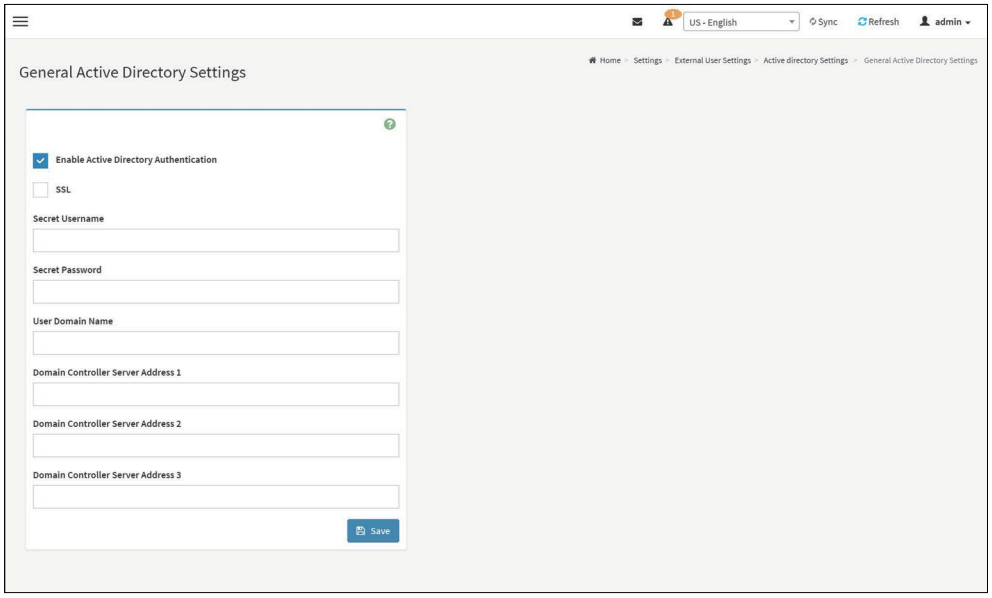
- **General Settings**: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.
- **Role Groups**: To add a new role group to the device.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

> **NOTE**
> It is recommended to Enable AD configuration from configure general settings page otherwise error message will pop-up stating that “AD configuration is not enabled” while trying to create/view AD role groups.

Procedure

Entering the details in General Active Directory Settings page

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



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 user name and password in the Secret User Name 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.
> - 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 characters long and will not allow more than 127 characters.

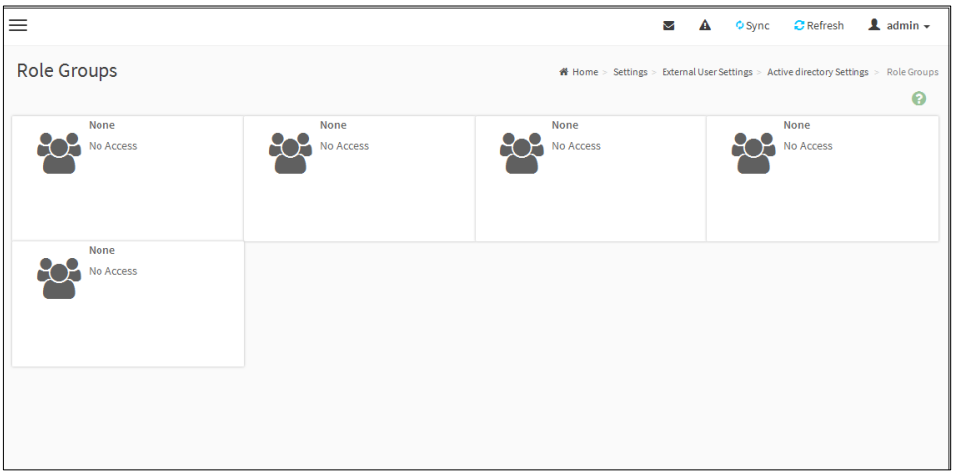
5. Specify the Domain Name for the user in the **User Domain Name** field. E.g. MyDomain.com
6. Configure IP addresses in **Domain Controller Server Address1**, **Domain Controller Server Address2** and **Domain Controller Server Address3**.
7. **Certificate File**: Click this button to choose which file to update as certificate file.

> **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.
> - Domain Controller Server Addresses will supports IPv4 Address format and IPv6 Address format.

8. Click **Save** to save the entered settings and return to Active Directory Settings page.

Role Groups

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



The fields of Role Group page are explained below.

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

> **NOTE**
> - Maximum size of Role Group Name is 255 bytes.
> - Special symbols hyphen and underscore are allowed.

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

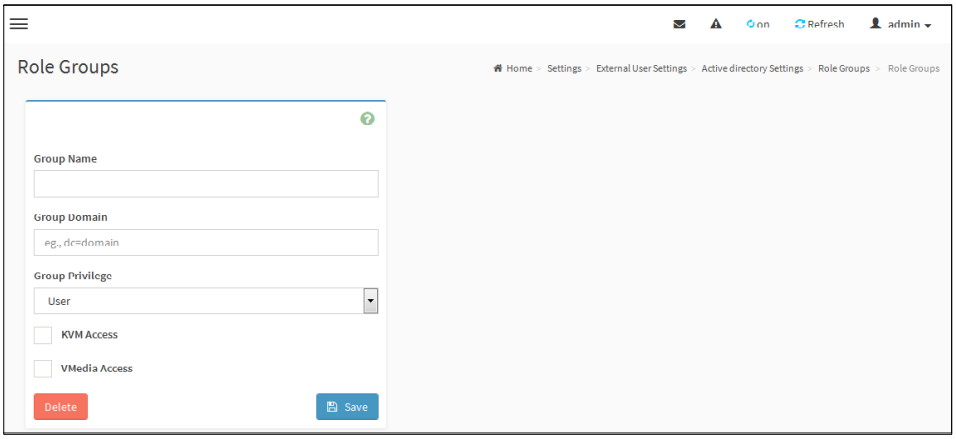
> **NOTE**
> - Maximum size of Group Domain Name is 255 bytes.
> - Special symbols hyphen, underscore and dot are allowed.

- **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.

> **NOTE**
> It is recommended to Enable AD configuration from configure general settings page otherwise error message will pop-up stating that “AD configuration is not enabled” while trying to create/view AD role groups.



2. In the **Group Name** field, enter the name that identifies the role group in the Active Directory.

> **NOTE**
> - Maximum size of Role Group Name is 255 bytes.
> - Special symbols hyphen and underscore are allowed.

3. In the **Group Domain** field, enter the domain where the role group is located.

> **NOTE**
> - Maximum size of Group Domain Name is 255 bytes.
> - 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

> **NOTE**
> VMedia privilege is not applicable for LMedia and RMedia clients

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

To Delete a Role Group

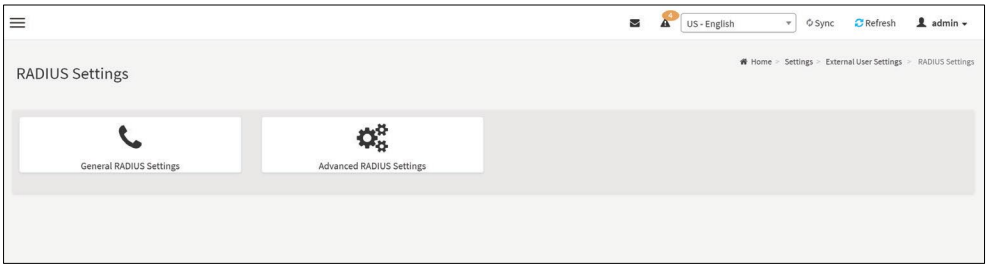
1. In the **Role Groups** page, select the row that you wish to delete.
2. Click **Delete Role Group**.

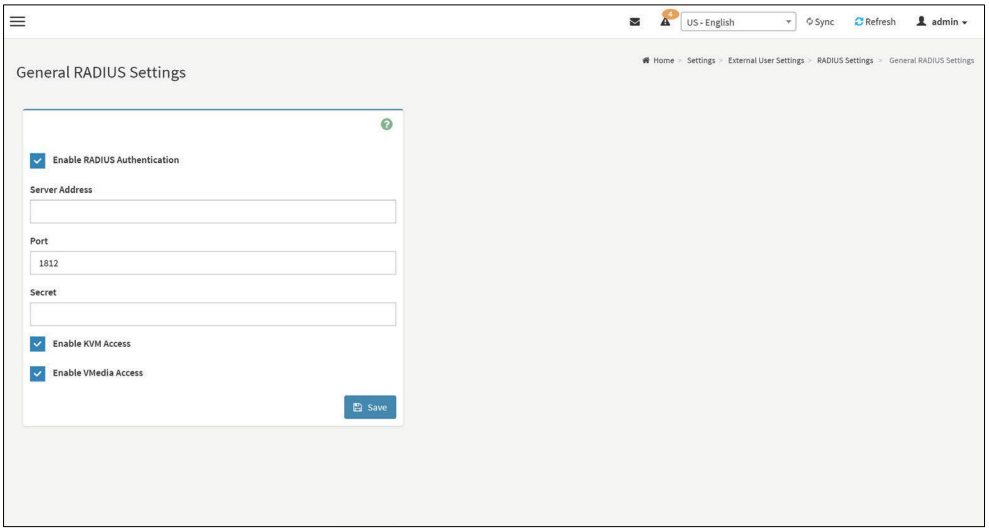
11.3.3 RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

This page is used to set the RADIUS Authentication.

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





General RADIUS Settings

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.

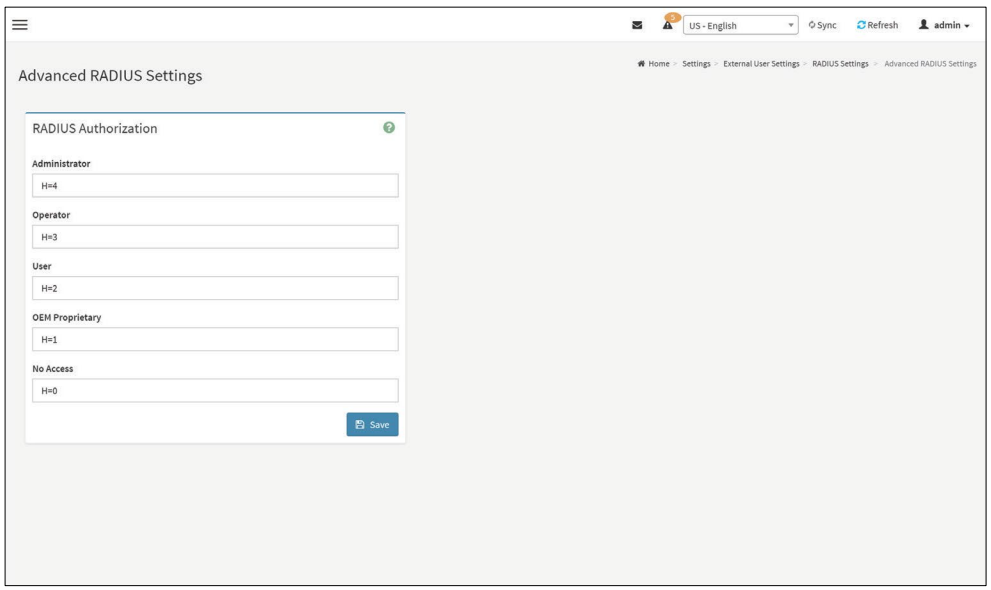
> **NOTE**
> - This field will not allow more than 31 characters.
> - Secret must be at least 4 characters long.
> - White space is not allowed.

- **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.

> **NOTE**
> - It will not allow more than 127 characters. Special characters like ';' and '#' are not allowed.
> - It is recommended to Enable Radius configuration from configure general RADIUS settings page otherwise error message will pop-up stating that "Radius configuration is not enabled" while trying to create/view Advanced RADIUS Settings.



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”

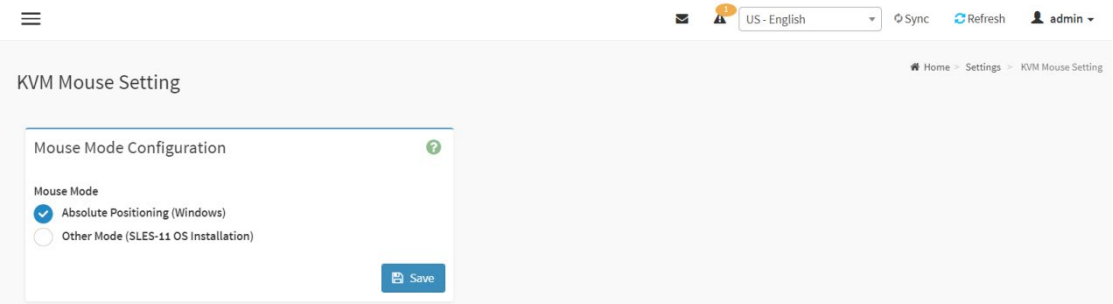
If you change the Vendor-Specific value in server then you should change the same values in this page.

3. Click **Save** to save the changes made.

11.4 KVM Mouse Settings

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** → **KVM Mouse Setting** from the menu bar. A sample screenshot of KVM Mouse Settings page is shown below.



The fields of KVM Mouse Settings page are explained below.

- **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

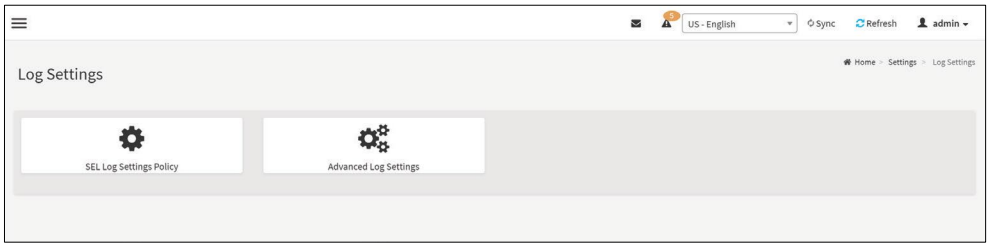
2. Click **Save** button to save the changes made.

> **NOTE**
> If the client and host mouse position is not in sync, then check the release note of the Host OS to verify any additional configuration to be needed in the Host.

11.5 Log Settings

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** → **Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



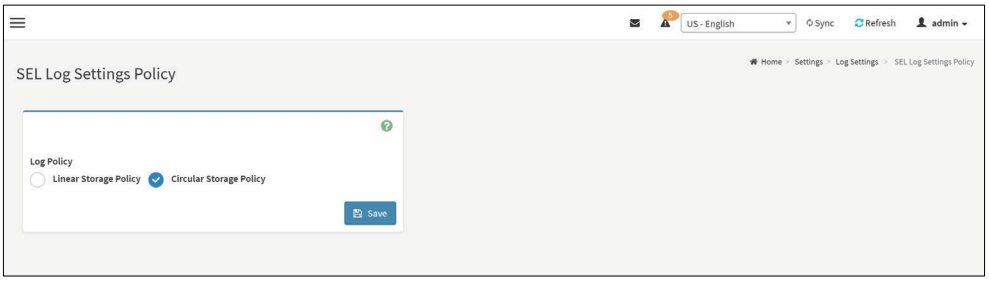
System and Audit Log Settings

The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

11.5.1 SEL Log Setting Policy

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

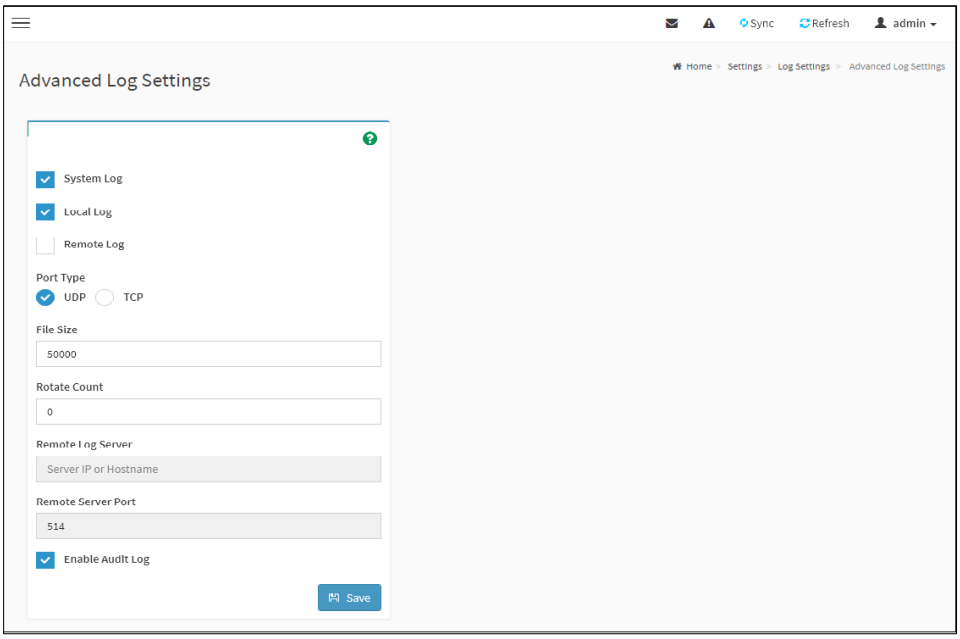


This page is used to configure the log policy for the event log. The fields are as followed.

- **Log Policy**: This field is to enable or disable the **Linear Storage Policy** or **Circular Storage Policy**.
- **Save**: To save the configured settings.

11.5.2 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 Policy** page is shown below.



This page is used to configure the log policy for the event log. The fields are as followed.

- **System Log:** This field is used to enable or disable the System Log. Select **System Log** to view all system events. Entries can be filtered based on their classification levels. Specifies the Location for system logs, whether it should be preserved in a **Local Log/ Remote Log**.
- **Local Log**: Select Local Log to save the logs locally (BMC).

> **NOTE**
> -You can select either **Local Log/Remote Log** or both Logs as per the requirement.
> - Either one of the Log selection is mandatory.
> - Local file resides at /var/log/

- **Remote Log**: Select Remote Log to save the logs in a remote machine.
- **Port Type**: Port Type is supported with the enable of Remote Log. You can select either UDP/TCP as per the requirement.
- **File Size**: This field is to specify the size of the file in bytes if the selected log type is local.

> **NOTE**
> Size ranges from 3 to 65535. Log files are rotated when they grow bigger than size bytes mentioned, with regards for the last rotation time interval (1 minute).

- **Rotate Count**: To back 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 address format
> - FQDN (Fully Qualified Domain Name) format
> - Maximum allowed size is 64 bytes

- **Remote Server Port**: This field is to specify the Remote Server port address 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**: To enable or disable the audit log.
- **CA Certificate File**: Browse and select the file that contains the certificate of trusted CA certs.

> **NOTE**
> - CA certificate file should be of the type pem.
> - CA Certificate file will be available only when the Remote Log and TCP are enabled.

- **Save**: To save the 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 **Server Address** of the remote server where the system events are logged.
5. In the **Audit Log** field, check or uncheck the **Enable** option as desired.
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.

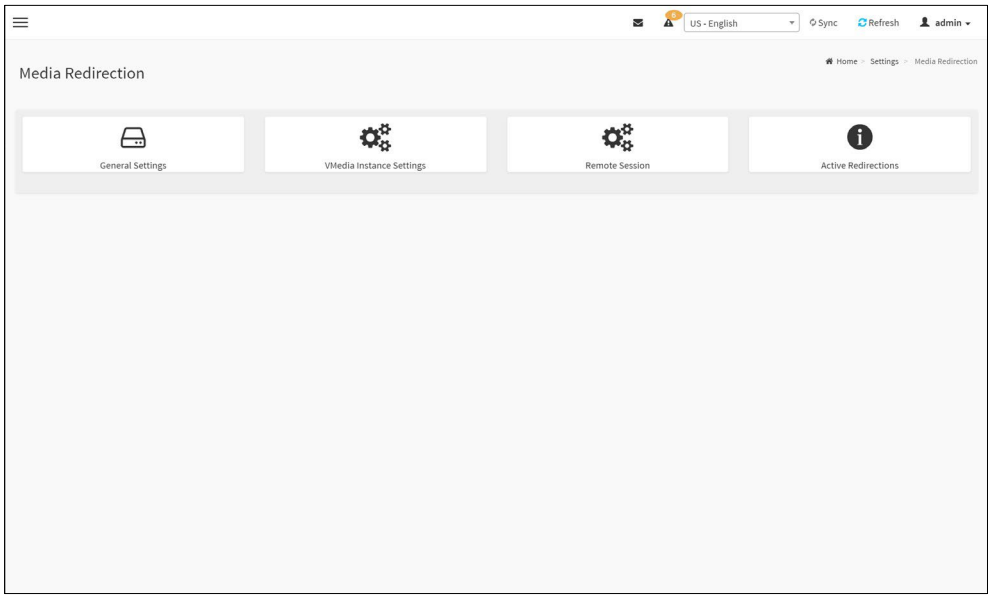
On FC machine, disable the following lines for UDP in /etc/rsyslog.conf.

1. MODLOAD imudp
2. UDPSERVER 514

11.6 Media Redirection Settings

This page is used to configure the media into BMC for redirection. To open Media Redirection page, click **Settings** → **Media Redirection Settings** from the menu bar.

A sample screenshot of Media Redirection page is shown below.



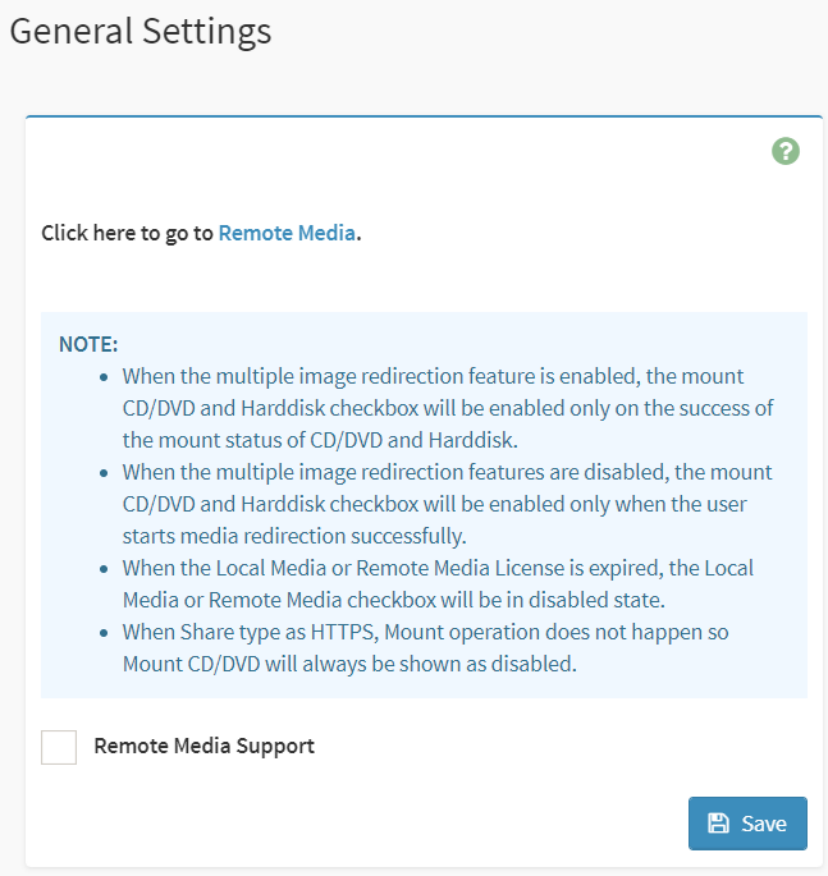
The fields of Media Redirection page are explained below.

- General Settings
- VMedia Instance Settings
- Remote Session
- Active Redirections

11.6.1 General Settings

This option is used to configure General Media Settings.

To open General Media Settings section, click **Settings** → **Media Redirection Settings** → **General Settings**.



General Settings

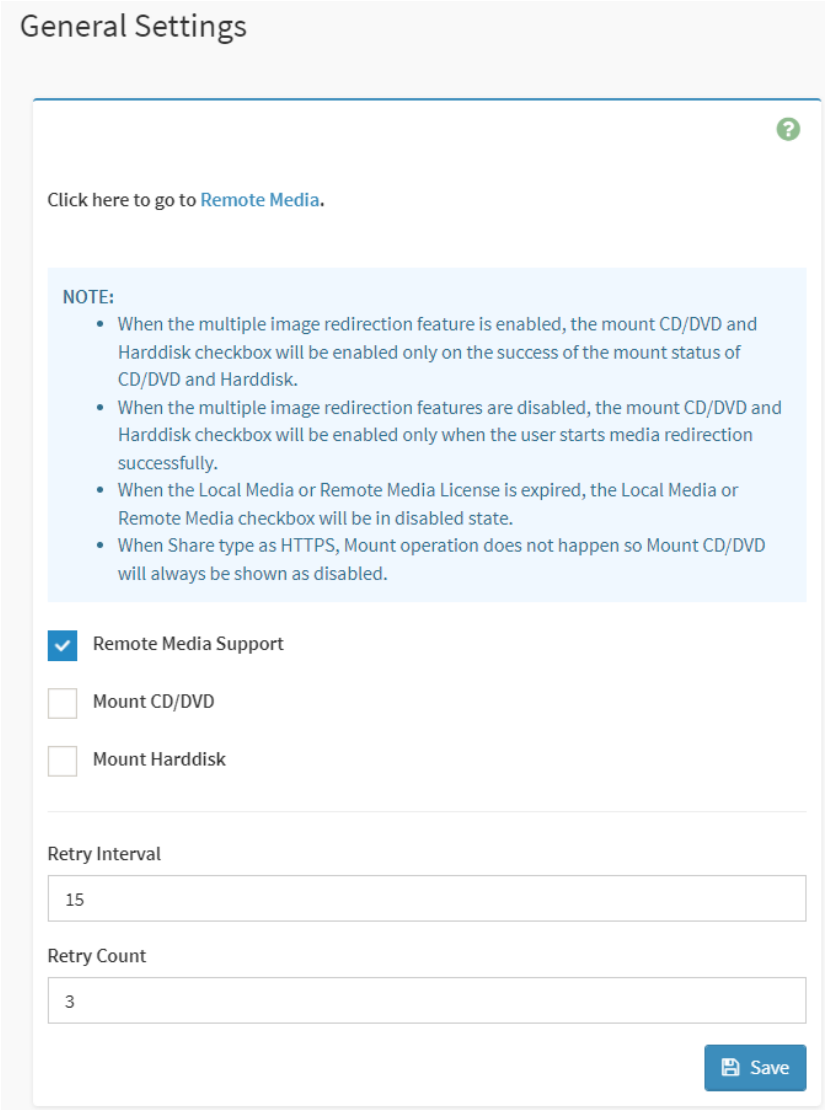
> **NOTE**
> When the Local Media or Remote Media license is expired, the Local Media or Remote Media check box will be in disabled state.

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.



- **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.

NOTE
Path must be alpha-numeric and the following special characters are only allowed: '/'(backward slash), '\'(forward slash), '_'(underscore), 'and .'(dot).
This field will not allow more than 256 characters.

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

- **Domain Name, Username, and Password**: If share Type is Samba(CIFS) or SMBE (Encrypted 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.

> **NOTE**
> If RMedia Reconnect Feature is enabled, the below Retry fields will be displayed to configure the retry interval and count.

Retry Interval: Enter the retry interval to reconnect RMedia.

Retry Count: Enter the retry count to reconnect RMedia.

> **NOTE**
> Retry count and interval are used only if there is any disruption in the active redirected image. During this case, the media will try to reconnect based on configured retry count and interval values.

Save: To save the settings.

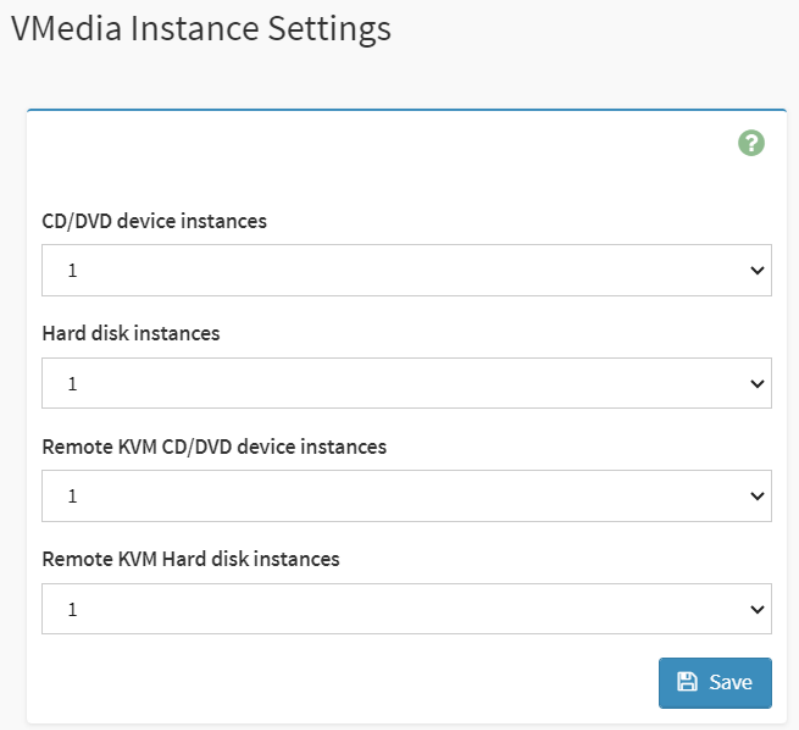
> **NOTE**
> For RMedia share types, we support the following NFS, CIFS, HTTPS, SMBE and encrypted NFS mount protocols, for mounting remote image share paths to the BMC.

Protocol	Versions
NFS	NFSv2, NFSv3, NFSv4, NFSv4.1
CIFS	SMBv1, SMBv2.1, SMBv3.x
encrypted NFS (Kerberos)	NFSv4

11.6.2 VMedia Instance Settings

This page is used to configure Virtual Media device settings. To open VMedia Instance Settings page, click **Settings** → **Media Redirection Settings** → **VMedia Instance Settings** from the menu bar.

A sample screenshot of VMedia Instance Settings page is shown below.



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.
- **Emulate SD Media as USB disk to Host**: To emulate SD Media on BMC as a USB device to Host Server.
- **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.

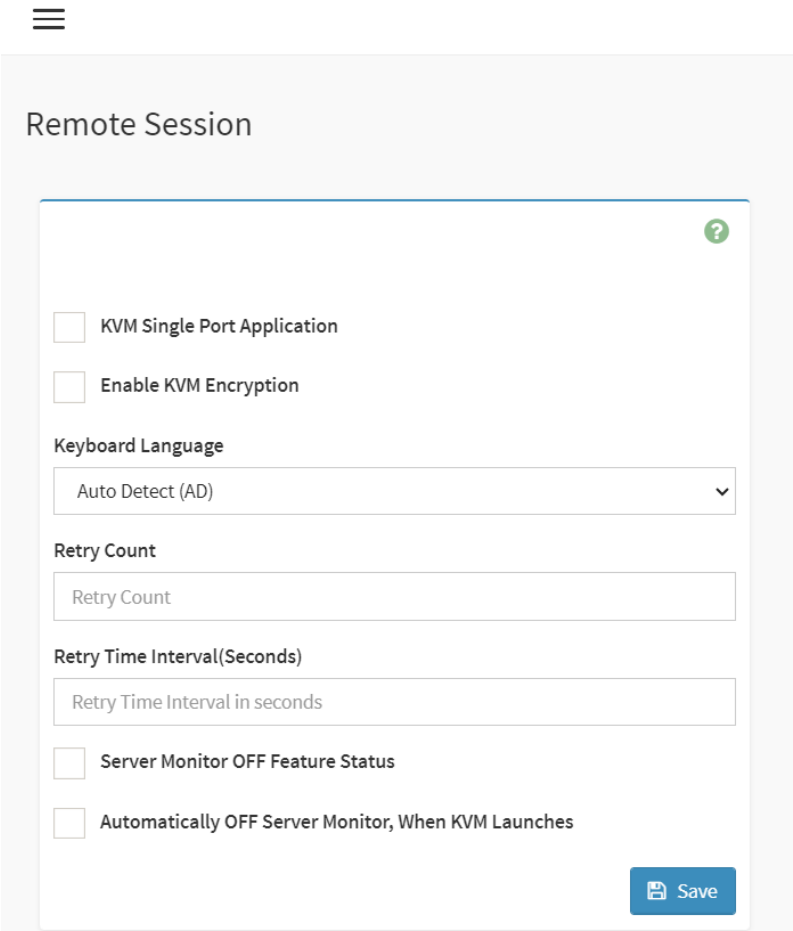
2. Click **Save** to save the changes made else click Reset to reset the previously saved values.

> **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.

11.6.3 Remote Session

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** → **Media Redirection Settings** → **Remote Session** from the menu bar. Click **Remote Control** for navigating to that page. A sample screenshot of Remote Session page is shown below.



The fields of Configure Remote Session page are explained below.

- **KVM Single Port Application**: This feature is enabled by default, KVM session will use its dedicated port whereas both Web and KVM sessions will be established only via Web Port. Since singleport application performs better when compared to kvm/media stunnel encryption, singleport feature will always be enabled. User can’t disable singleport support in runtime.
- **Keyboard Language**: This option is used to select the keyboard supported languages.
- **Retry Count**: This value specifies the number of attempts the KVM client will make to reconnect the KVM session. The retry count value ranges from 1 to 20.
- **Retry Time Interval (Seconds)**: This value specifies the time duration between two consecutive reconnect attempts. The KVM client will wait for a time interval equal to this value, after making a reconnect attempt, before trying to connect again. The retry interval value is mentioned in seconds and it ranges between 5 to 30 seconds.

- **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

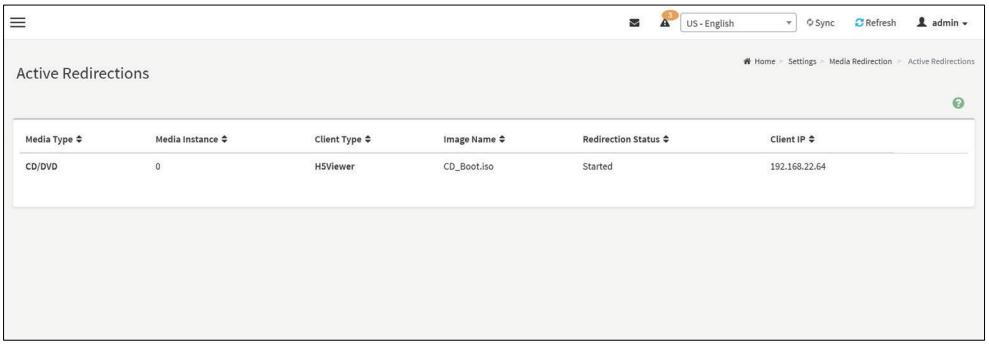
1. Choose the **Keyboard Language** from the list of keyboard supported languages.
2. Enter a value in the **Retry Count** field to set the number of attempts for retrying the redirection session.
3. Enter a value in the **Retry Time Interval (Seconds)** field to give time interval for each attempts.
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.

11.6.4 Active Redirections

This page is used to display the active redirected media, which are redirected via VMAPP/H5Viewer/LMedia/RMedia/VMCLI. Information like Media type, Media Instance, Client Type, Image Name, Redirection status, Client IP will be displayed.

To open Active Redirections page, click **Settings** → **Media Redirection Settings** → **Active Redirections** from the menu bar.

A sample screenshot of **Active Redirections** page is shown below.



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 Client type (VMAPP/H5Viewer/LMedia/RMedia/VMCLI) used for active media redirection.
- **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.

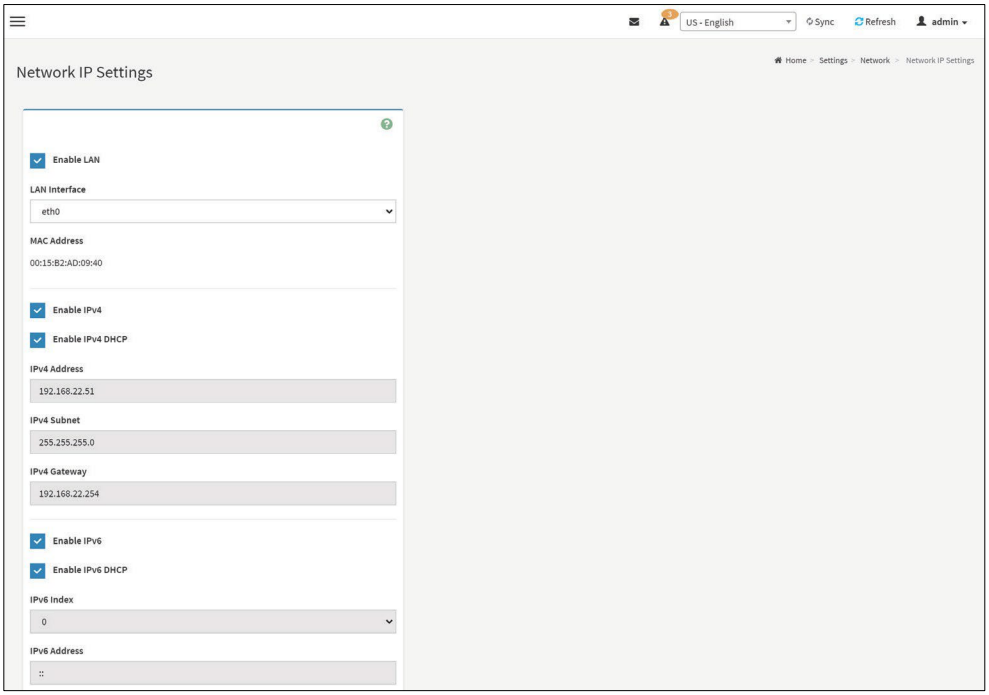
NOTE
Local/Remote Media connection will use loopback socket for communication. So '~' symbol will be displayed for loopback ip(127.0.0.1 (or) ::1) in media session information page.

11.7 Network Settings

The Network Settings page is used to configure the network settings for the available LAN channels.

11.7.1 Network IP Settings

To open Network Settings page, click **Settings** → **Network Settings** → **Network IP Settings** from the menu bar. A sample screenshot of Network IP Settings page is shown below.



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).

NOTE
Disable this Enable IPv6 DHCP field to enable and enter the values in following fields such as IPv6 Index, IPv6 Address, Subnet Prefix length and IPv6 Gateway.

- **IPv6 Index**: To specify a static IPv6 Index to be configured to the device. Eg: 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 and SUPPORT_IPMIIPV6_LAN_PARAM_ONLY are enabled, the IPv6 default Gateway field will not be displayed.

- **Clear IPv6 Address:** This field will be displayed to clear the IPv6 address only if the IPv6 address and Subnetwork Prefix Length is available for the selected index value.
- **Enable VLAN**: To enable/disable the VLAN support for selected interface.
- **VLAN ID**: Specify an ID for this VLAN configuration.
  - Value ranges from 2 to 4094.

NOTE
VLAN ID can't be changed without resetting the VLAN configuration.
VLAN 0, 1 & 4095 are reserved VLAN ID's.

  - **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

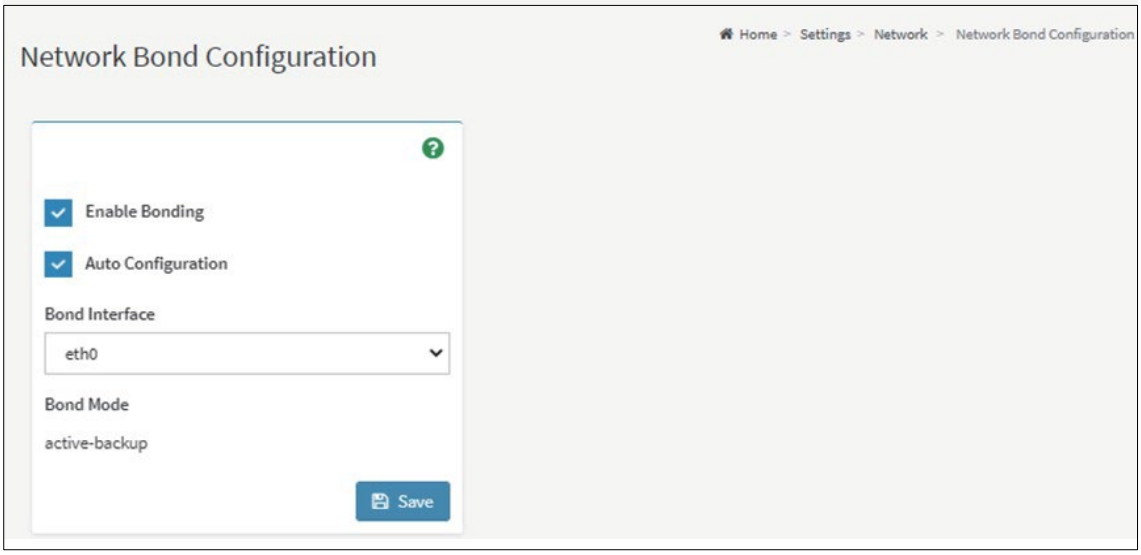
1. Check **Enable LAN** to enable LAN support for the selected interface..
2. Select the **LAN Interface** to be configured.
3. Check Enable **IPv4** to enable IPv4 support for the selected interface.
4. Check Enable **IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the **IPv4 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.

11.7.2 Network Bond Configuration

This page is used to configure the network bonding configuration for the network interfaces.

> **NOTE**
> Minimum of two network interfaces required to enable Network bonding for the device.

To open Network Settings page, click **Settings** → **Network Settings** → **Network Bond** from the menu bar. A sample screenshot of **Network Bonding** page is shown below.



The fields of Network Bond Configuration page are explained below.

- **Enable Bonding**: To enable or disable network bonding for network interfaces.
- **Auto Configuration**: To configure the interfaces in service configuration automatically.

> **NOTE**
> If Auto configuration is disabled, then interfaces in services can be configured via IPMI command.
>
> If Auto configuration is enabled, then all the services will be restarted automatically.

- **Bond Mode**: This field displays the Network bonding mode.

> **NOTE**
> This field can't be configured.

- **Save**: To save the current changes.

Procedure

> **NOTE**
> The Enable Bonding option is enabled. You can disable the option if needed.

1. Select the **Bond Interface** from the drop-down list.

> **NOTE**
> The Bond Interface can be selected only if the Enable Bonding option is enabled.

2. Check the **Auto Configuration** option to enable the auto configuration.

3. Click **Save** to save the configuration.

Bonding behaviour when bond channel IP source is modified.

Bond Interface has been assigned Channel 1.

Case 1: When Bond Interface Channel IP source is DHCP.

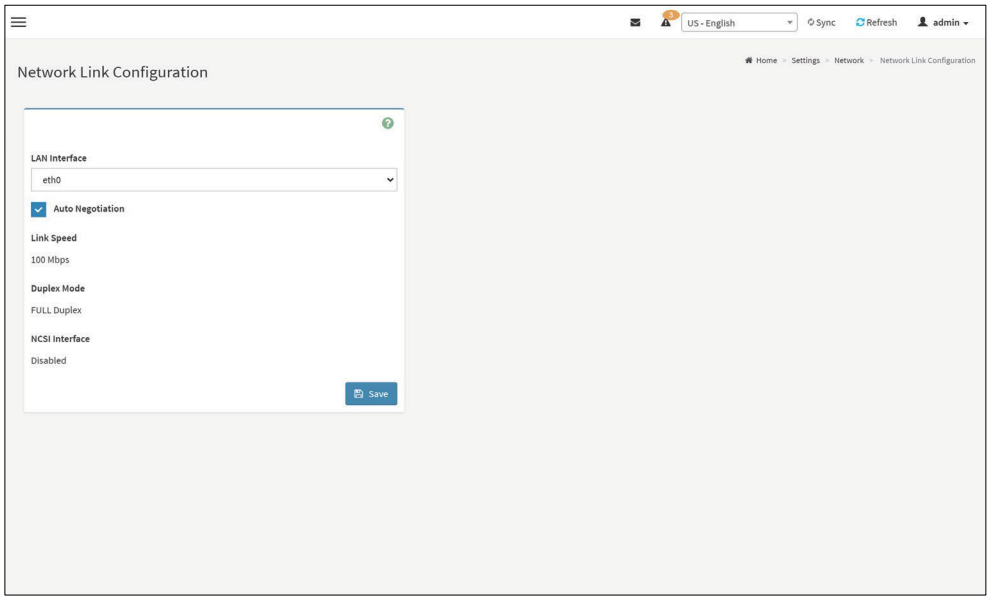
When Bond is enabled with active slave (e.g. eth0 or eth1) then ip will be leased for bond interface as per MAC address of active slave.

Case 2: When Bond Interface Channel IP source is Static Bond interface will be assigned a static IP address and other LAN Parameter as per Channel 1.

11.7.3 Network Link Configuration

This page is used to configure the network link configuration for available network interfaces.

To open Network Link page, click **Settings** → **Network Settings** → **Network Link** from the menu bar. A sample screenshot of Network Link Configuration page is shown below.



The fields of Network Link Configuration page are explained below.

- **LAN Interface**: Select the required network interface from the list to which the Link speed and duplex mode to be configured.
- **Auto Negotiation**: This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.
- **Link Speed**: Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps.

> **NOTE**
> Link speed of 1000 Mbps is not applicable, when Auto Negotiation is OFF.

- **Duplex Mode**: Duplex Mode could be either Half Duplex or Full Duplex.
- **NCSI Interface**: NCSI Interface status could be either Enabled or Disabled for the selected LAN interface.
- **Save**: To save the settings.

Procedure

1. Select the **LAN Interface** from the drop down list.
2. Select either **Enable** or **Disable** for **Auto Negotiation**.

> **NOTE**
> The Link Speed and Duplex Mode will be active only when Auto Negotiation is OFF.

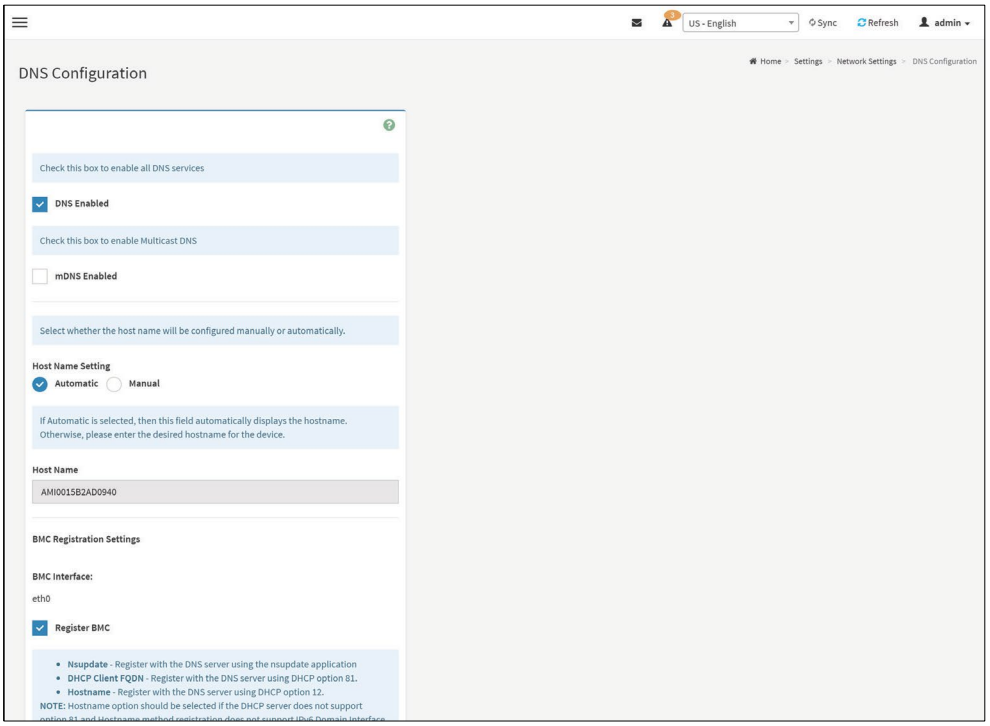
3. Select the **Link Speed** from the drop-down list.
4. Select the **Duplex Mode** either Full duplex or Half duplex.
5. Click **Save** to save the configuration.

11.7.4 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** → **Network Settings** → **DNS Configuration** from the menu bar. A sample screenshot of DNS Configuration page is shown below.



The fields of DNS Configuration page are explained below.

- **<u>Domain Name Service Configuration</u>**
- **DNS Enabled**: To enable/disable all the DNS Service Configurations.
- **mDNS Enable**: To enable/disable the mDNS Support Configurations.
- **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 character '-'(hyphen) is allowed.
- It must not start or end with a '-'(hyphen).
- The underscore (_) character and double hyphen (--) character are not a legal character for use in host names.

BMC Registration Settings

BMC Interface: Options to register the BMC are through an Interface (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 fifiles 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 (readonly).
- **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, or, if ‘Manual’ was selected, specify the domain name of the device.

> **NOTE**
> Domain name must be a string of 4 to 253 alphanumeric characters. (254 characters are allowed only if the last byte is dot.)
> It must start with a letter and end with a letter or digit. (Must contain atleast one dot character)
> Only letters, digits, dot and hyphen are allowed.

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.
   - **Hostname** - Choose **Hostname** option to register with DNS server using DHCP option.

NOTE
Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.
Hostname option is not support at DHCPv6, hence IPv6 will not register to DNS server at option hostname.

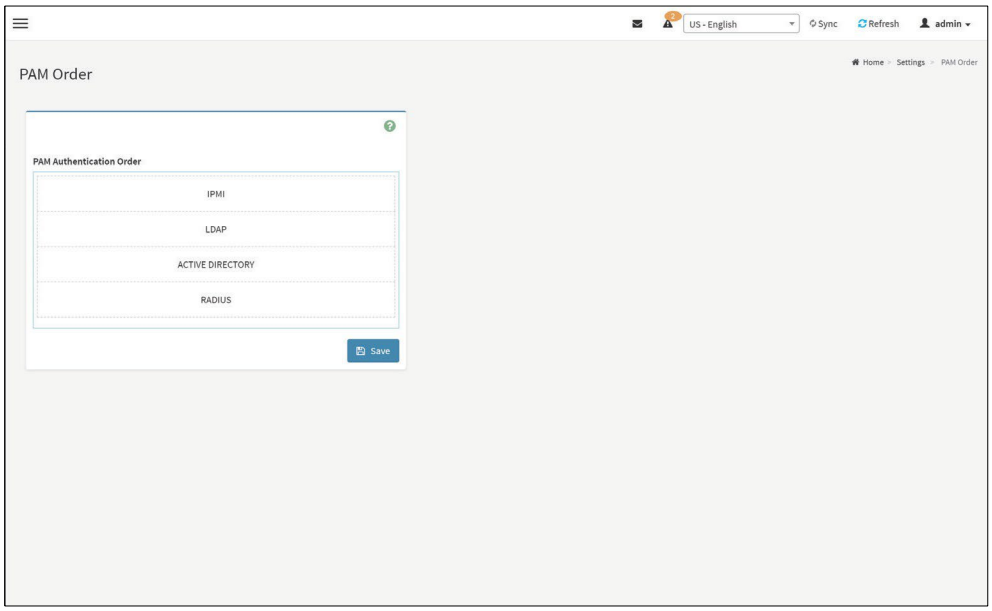
5. Check **Both** option to modify TSIG authentication for both interfaces (eth0&1).
6. In **Eth 0&1 TSIG Configuration**, Check **TSIG Authentication Enabled** option to enable/disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in **Current TSIG 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 **DNS Name Server Setting**.
   - Choose the IP Priority, either IPv4 or IPv6.
   - Enter the DNS Server address.
9. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
10. Click **Save** to save the entries

11.8 PAM Order Settings

This page is used to configure the PAM ordering for user authentication in to the BMC.

To open PAM Ordering page, click **Settings** → **PAM Order Settings** from the menu bar.

A sample screenshot of PAM Order page is shown below.



The fields of **Settings** → **PAM Order Settings** 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.
> - Radius must be last in PAM order for the same reason, if RADIUS is not last in PAM order, the User ID of logged in users using other authentication services will be shown as RADIUS User ID.
> - 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 before RADIUS if RADIUS Authentication is enabled or in the last location in PAM order if RADIUS Authentication is enabled.

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.

11.9 Platform Event Filter

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.

The PEF Management is used to configure the following

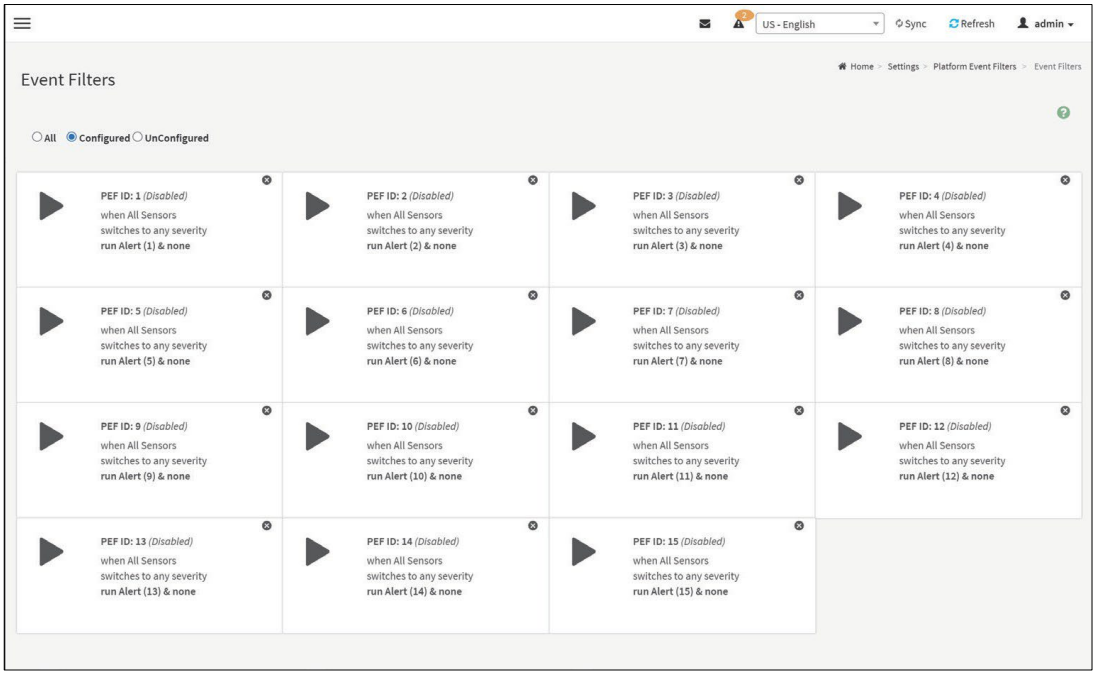
- Event Filters
- Alert Policies
- LAN Destinations

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

11.9.1 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.



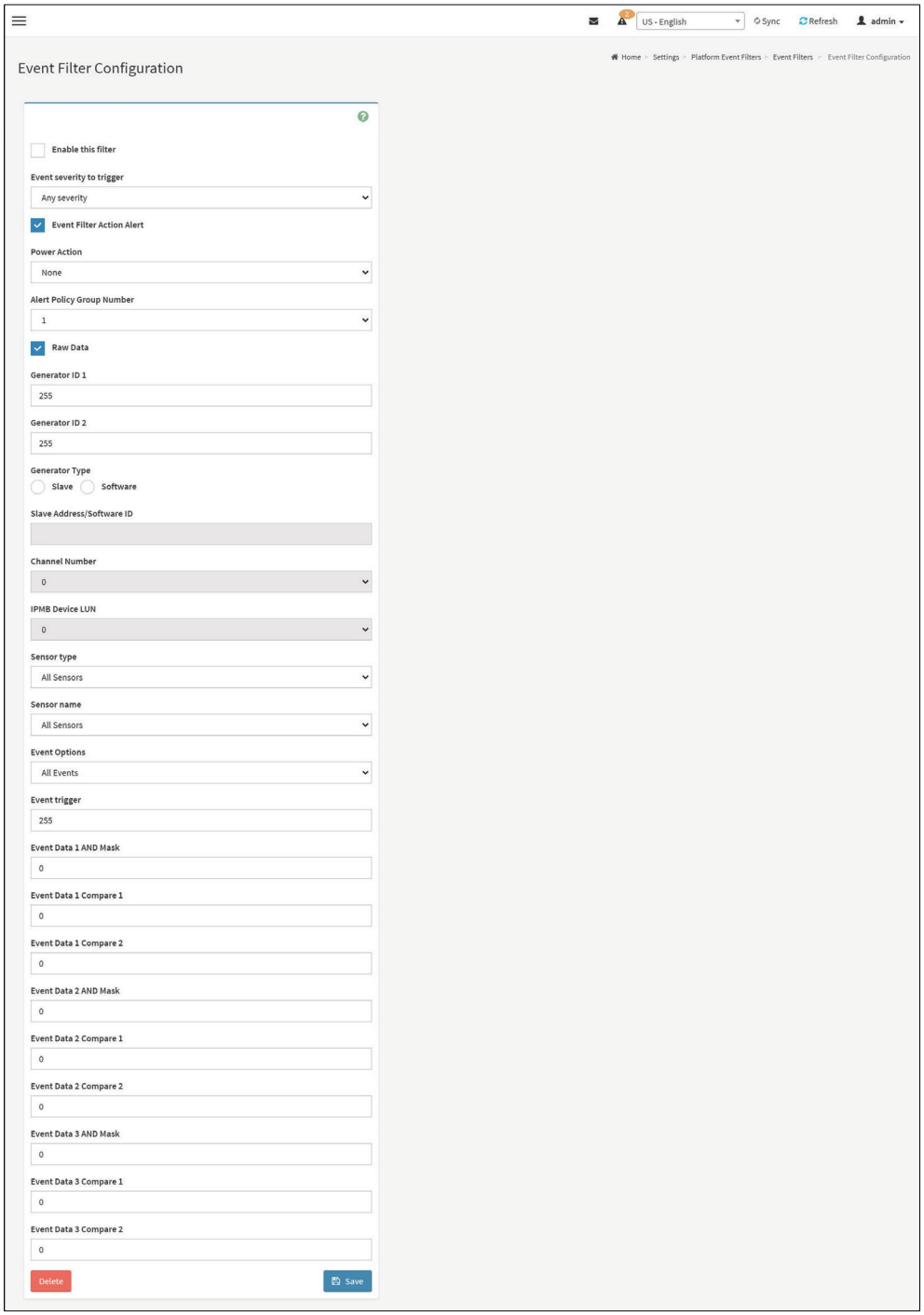
Platform Event Filters – Event Filters

The fields of Platform Event Filters Tab are explained below.

This page contains Pre- configured 40 Events with PEF IDs. Click Delete icon (⊗) on the top right corner to directly delete an item from the list.

Procedure

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

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 severity 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'.

- In the **Event Generator** 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 1 Compare 1 & Event Data 1 Compare 2** fields are used to indicate whether each bit position's comparison is an exact comparison or not.

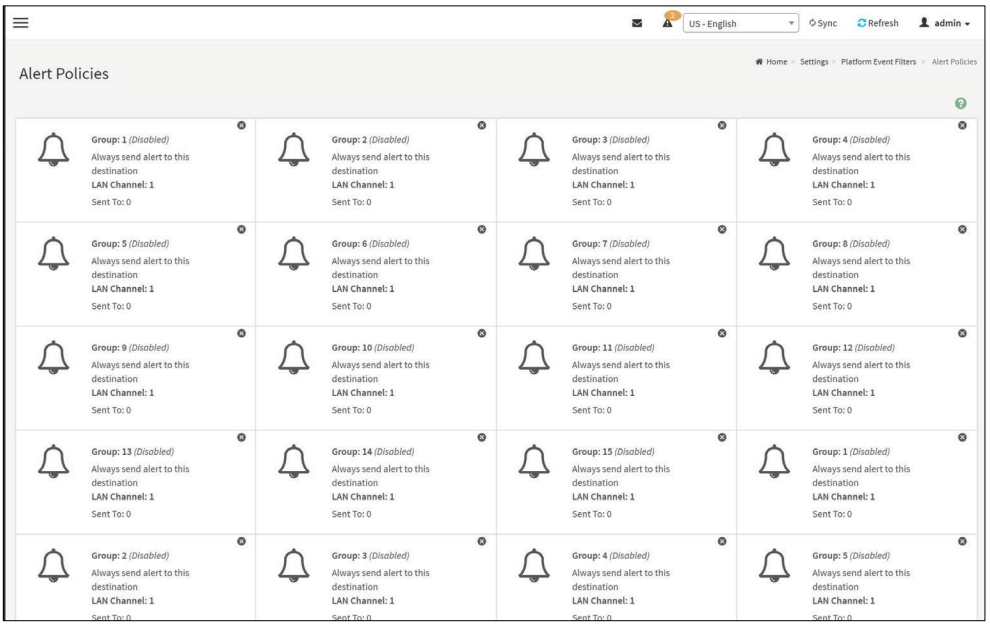
> **NOTE**
> Value ranges from 0 to 255.

- **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.

11.9.2 Alert Policies

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



Platform Event Filters – Alert Policies

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.

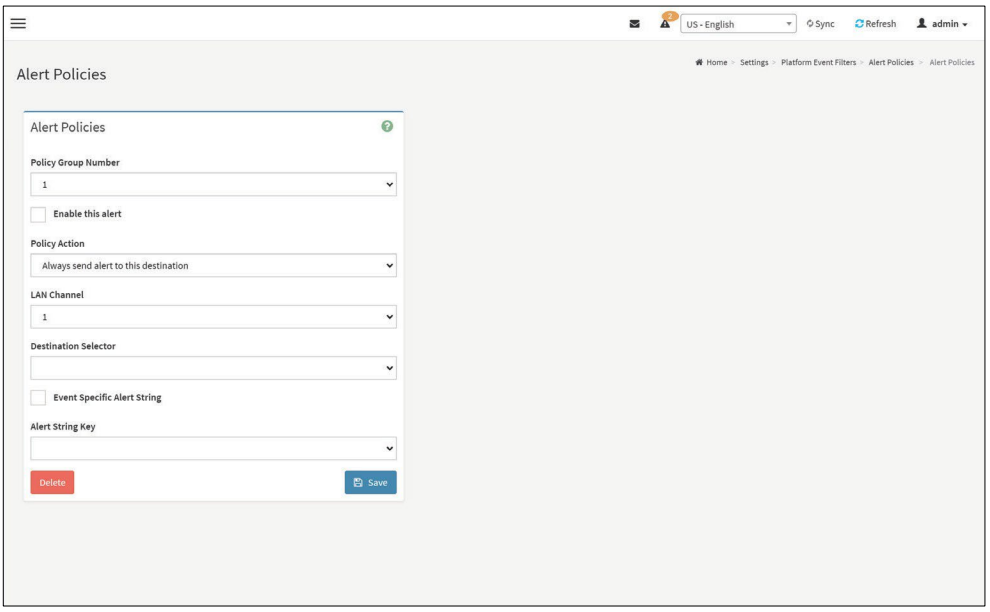
  4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
- **LAN Channel**: To choose a particular channel from the available channel list.
- **Destination Selector**: To choose a particular destination from the configured destination list.

> **NOTE**
> LAN Destination has to be configured under **Settings → 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.

Procedure

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.



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 has to be configured under **Settings** → **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.

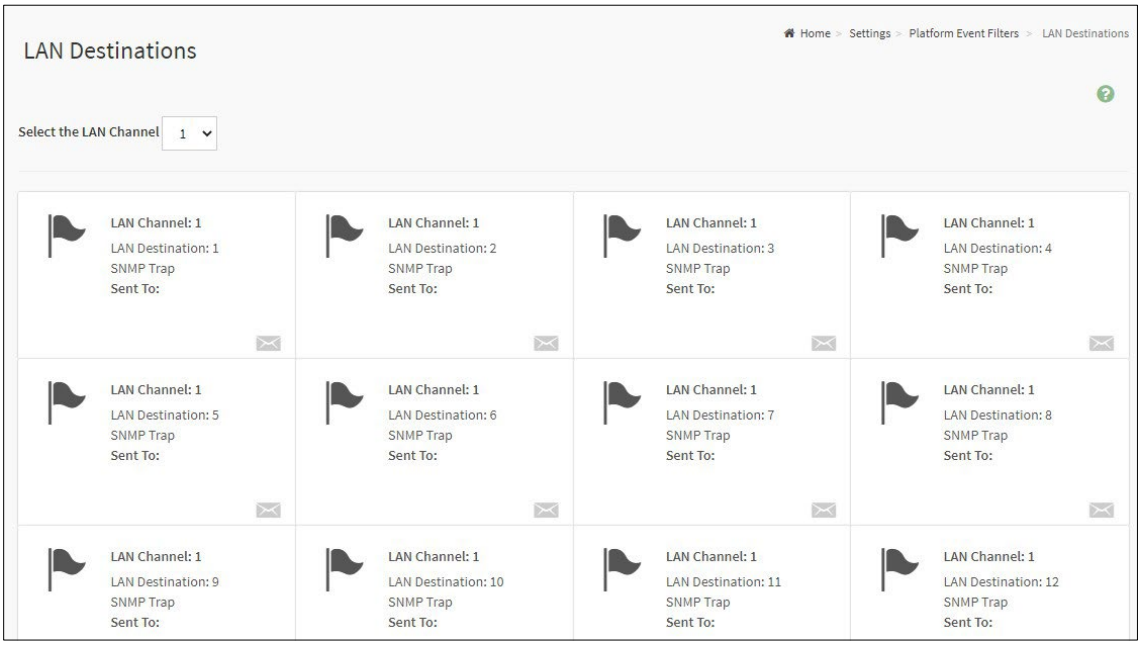
9. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

> **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 has to be configured using IPMI Command (Set PEF Config Parameter “Alert String”).
> # and ; symbols are not supported for PEF Alert string.

10. Click **Save** to save the new alert policy and return to Alert Policy list.
11. Click **Delete** to delete a configuration.

11.9.3 LAN Destinations

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



Platform Event Filters - LAN Destinations

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 (readonly).

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 User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under **Settings → SMTP Settings**. For SNMP Trap, only the SNMP Destination Address has to 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.
- FQDN (Fully Qualifified Domain Name) format
  - Maximum allowed size is 251 bytes

BMC User Name: 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 → 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.

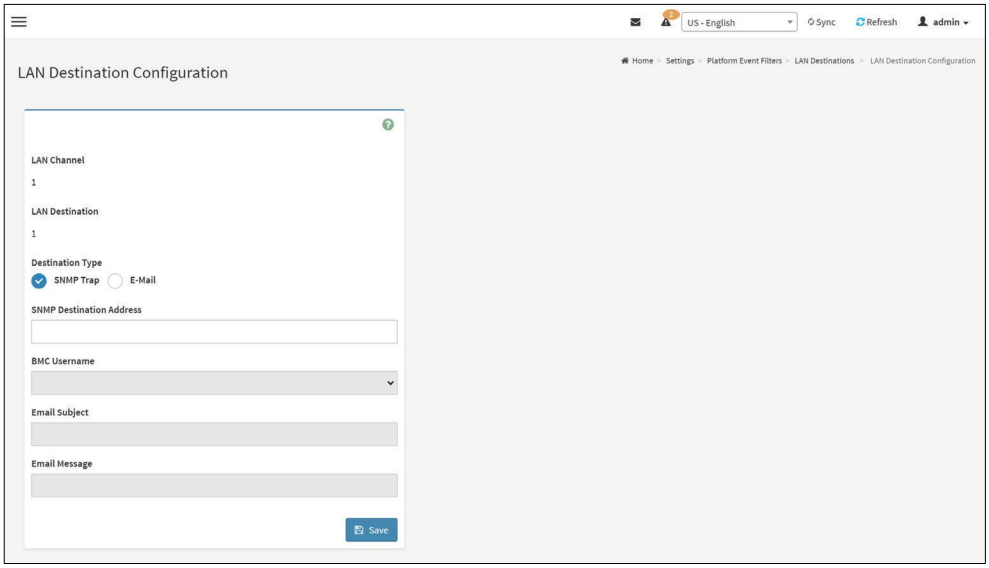
> **NOTE**
> User should be configured under **Settings → Users Management**

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

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**.



Add LAN Destination entry Page

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 User Name** from the list of users.

> **NOTE**
> E-mail address should be configured under **Settings → User Management**.

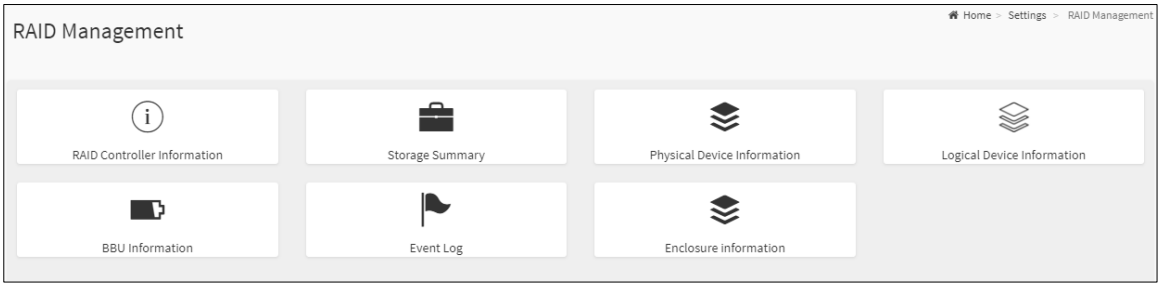
8. In the **Email Subject** field, enter the subject.
9. In the **Email Message** field, enter the message.
10. Click **Save** to save the new LAN destination and return to LAN destination list.
11. Click **Delete** to delete a configuration.
12. Click Message icon ( ) to send sample alert to configured destination.

> **NOTE**
> Test alert can sent only with enabled SMTP configuration. SMTP support can be enabled under **Settings → SMTP Settings**.
> **Limitations**: In the opensource SNMPtrap, the alert always sent to the destination through the channel 1, even though the channel was set to different channel.

11.10 RAID Management

The RAID Management page allows you to view the Storage Summary, RAID Controller information, Physical Device Information, Logical Device Information, BBU Information and Event Log.

To open RAID Management page, click **Settings** → **RAID Management** from the menu bar. A sample screenshot of RAID Management page is shown below.



RAID Management

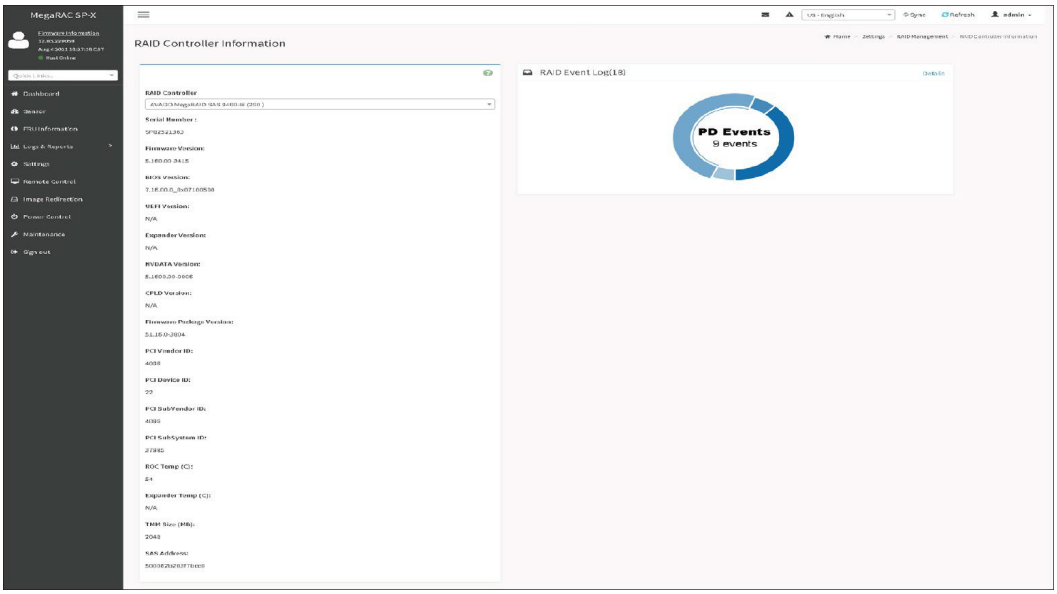
The following fields are displayed here for the selected RAID Controller.

- RAID Controller Information
- Storage Summary
- Physical Device Information
- Logical Device Information
- BBU Information
- Event Log
- SES Enclosure Information

NOTE
After pressing the POWER button to start up, it takes 6 minutes to use the functions in the WebUI RAID Manager.

11.10.1 RAID Controller Information

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



RAID Controller Information

> **NOTE**
> You can get RAID Controller Information only when Host is in Power ON state, else a warning message will be appeared as “Host is in Power Down State”.

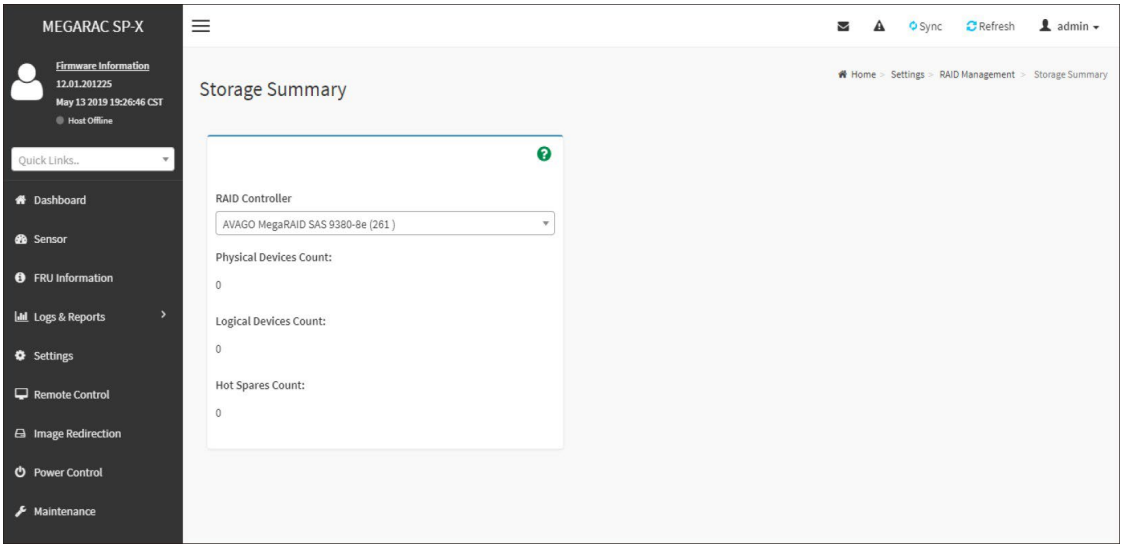
The fields of RAID Controller Information page are explained below.

- **Serial Number**: Displays the Serial number of the RAID Controller.
- **Firmware Version**: Displays the Firmware Version number of the RAID Controller.
- **BIOS Version**: Displays the BIOS Version number of the RAID Controller.
- **UEFI Version**: Displays the UEFI 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.
- **CPLD Version**: Displays the CPLD Version number of the RAID Controller.
- **Firmware Package Version**: Displays the Firmware 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.
- **SAS Address**: Displays the SAS address.
- **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.

11.10.2 Storage Summary

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



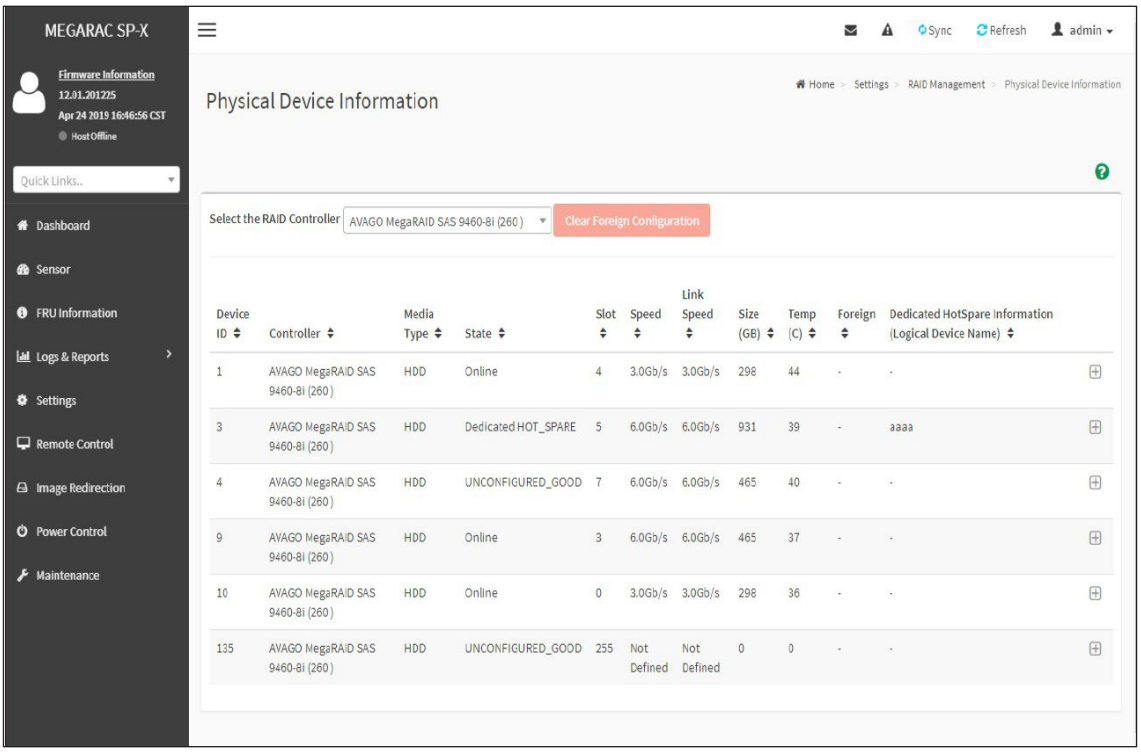
Storage Summary

Select a **RAID Controller** from the drop-down list to view the details of the selected RAID Controller.

- **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.
- **Hot Spares Count**: Displays the number of Hot Spares configured under the controller, it includes both Global Hot Spare and Dedicated Hot Spare.

11.10.3 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** → **RAID Management** → **Physical Device Information** from the menu bar. A sample screenshot of **Physical Device Information** section is shown below.



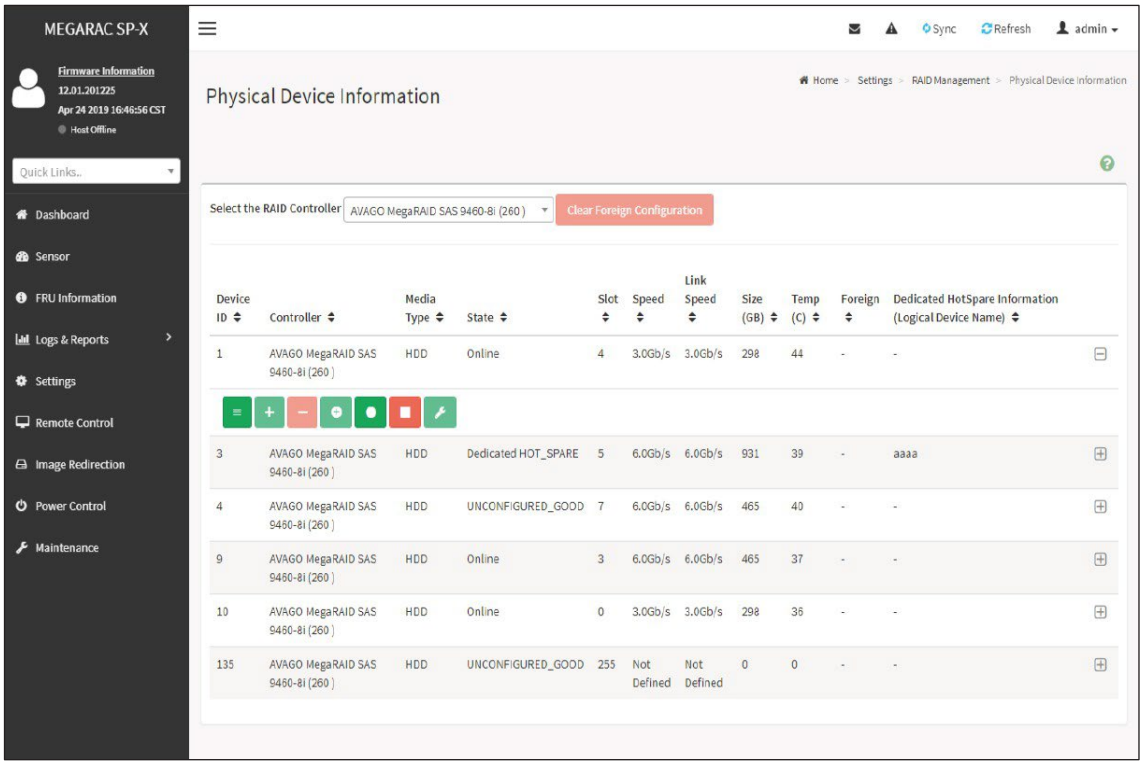
Physical Device Information

The fields of Physical Device Information page are explained below.

- **Select the RAID Controller**: To view the details of specific RAID Controller.
- **Clear Foreign Configuration**: To clear the Foreign Device.
- **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.
- **Size (GB)**: Displays the Size of the Physical Device.

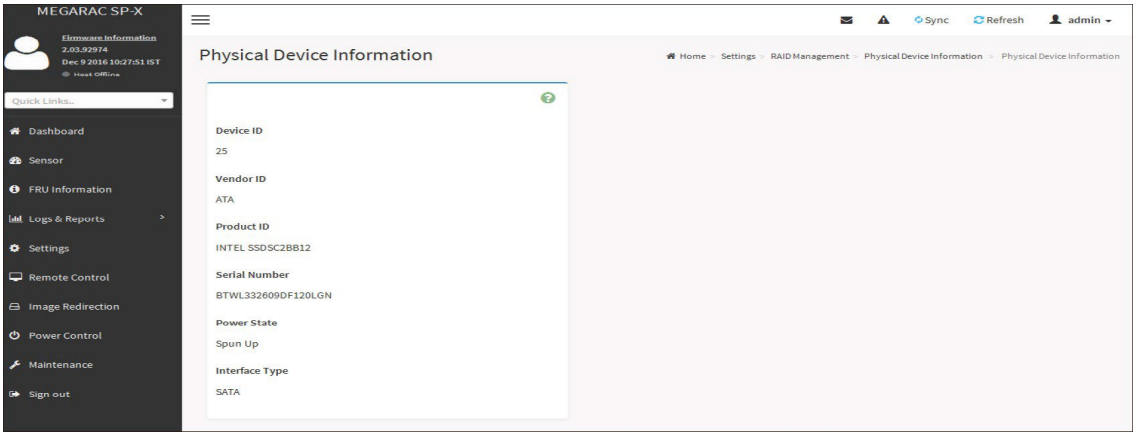
- **Temp (°C)**: Displays the Temperature of the Physical Device.
- **Select the RAID Controller**: To view the details of specific RAID Controller.
- **Clear Foreign Configuration**: To clear the Foreign Device.
- **Device Id**: Displays the Device ID of physical device available under selected RAID 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.
- **Size (GB)**: Displays the Size of the Physical Device.
- **Temp (°C)**: Displays the Temperature of the Physical Device.
- **Foreign**: Displays the foreign bit of Physical Device.
- **Dedicated HotSpare Information (Logical Device Name)**: Displays the name of dedicated hotspare for Physical Device.

To perform additional operations, click on the slot or expand the ( ) icon. A sample screenshot is shown below.



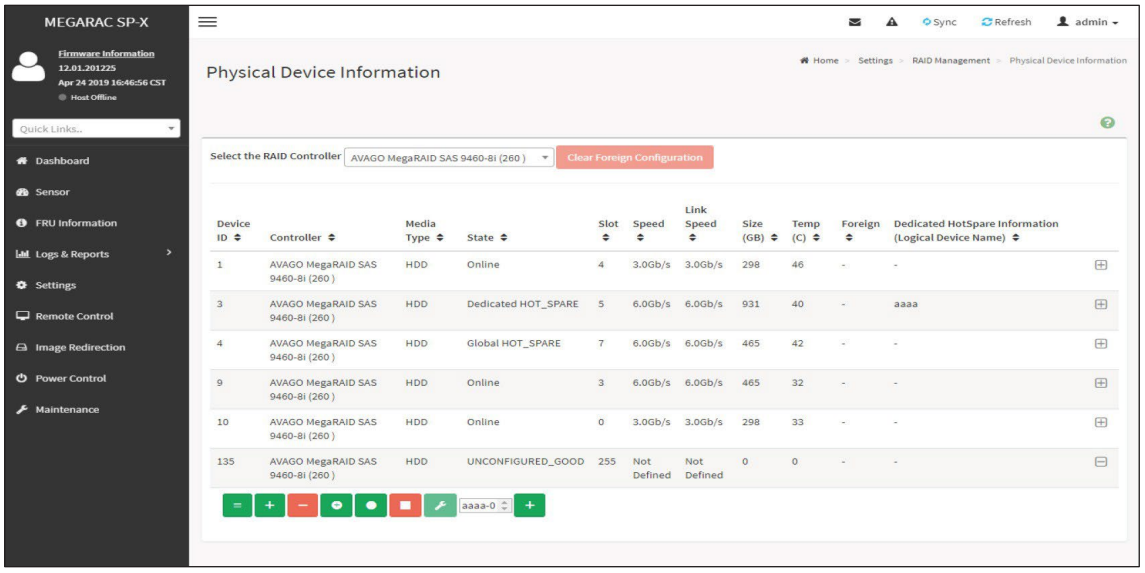
Physical Device Information

- **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.



View - Physical Device Information

- **Add as Global Hotspare**: Click ( ) icon and select the device to make the selected device as a Fail over/Global Hot spare drive.
- **Add/Remove Dedicated HotSpare**: Click ( ) icon and select the virtual device from the drop-down lists. A sample screenshot of View Physical Device Information page is shown below.



Physical Device Information

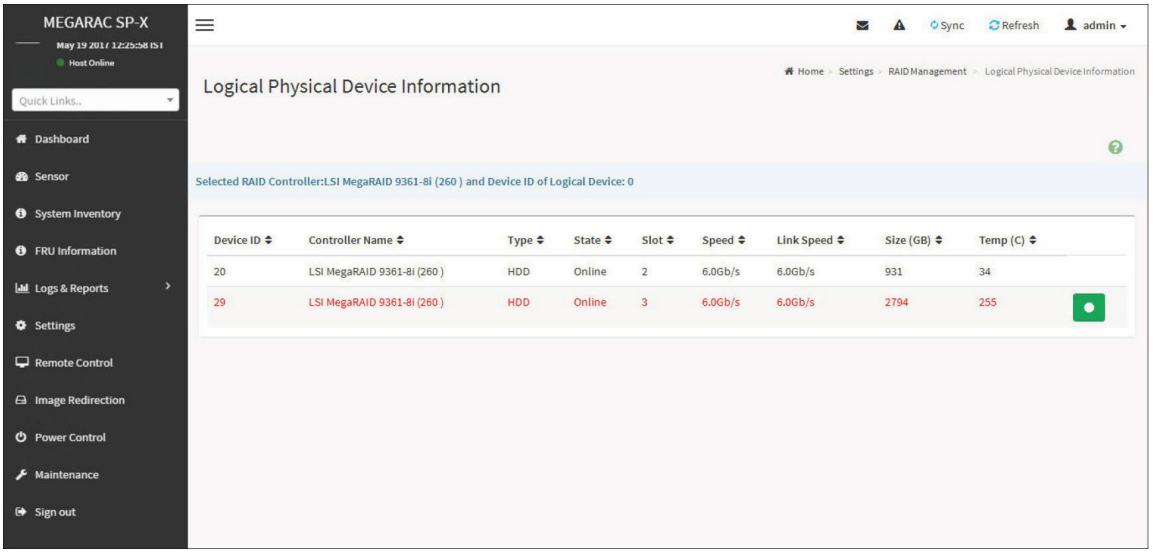
- **Prepare For Removal/Undo Prepare For Removal**: Click ( ) icon to remove selected physical device safely from the slot.
- **Start Locating Physical Device**: Click ( ) icon to start locating (LED glow) the selected Physical Device connected to back plane. A pop-up message prompts you to confirm your choice. Upon the confirmation, you will be informed about the status.

- **Stop Locating Physical Device**: Click ( ) icon to stop locating(LED glow) the selected Physical Device connected to back plane. A pop-up message prompts you to confirm your choice. Upon confirmation, you will be informed about the status.
- **Set Physical Device State as Unconfigured Good**: Click ( ) icon to set Physical Device State from Unconfigured Bad to Unconfigured Good.

> **NOTE**
> *Add/Remove as Dedicated HotSpare* and *Prepare For Removal/Undo Prepare For Removal* options will be enabled only when the State of the Device is UNCONFIGURED_GOOD.

Predictive Failure in Physical Device

This section displays the details about the Predictive Failure in the Physical Devices connected to the RAID controller.
To open the Physical Device Information, click **Settings** → **RAID Management** → **Physical Device Information** from the menu bar. A sample screenshot of Physical Device Information section is shown below.



Physical Device Information

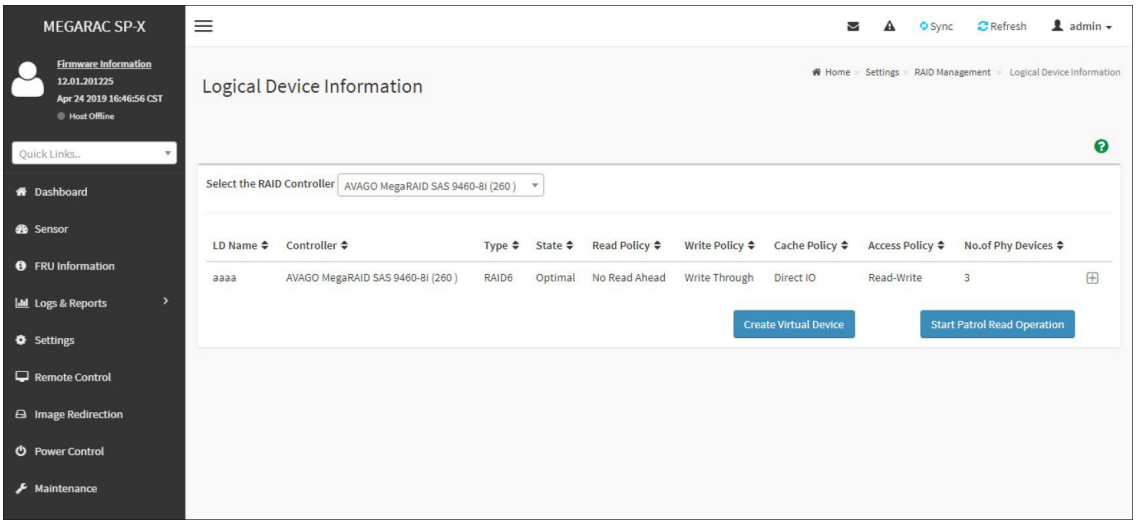
Set **Physical Device State as Unconfigured Good** option will be enabled while state is UNCON-FIGURED_BAD.

Clear Foreign Configuration option will be enabled while foreign bit is True.

> **NOTE**
> - If the predictive fail occurs, the Predictive Failure Devices will be highlighted in red color. Operations such as making hot spare/creating logical drive with HDD detected for predictive failure are disabled.
> - You can't make drive as predictive fail. If the drive becomes old, some of the LBA's may get corrupt and you can see predictive fail count in drives. Basically it depends on age of the drive.

11.10.4 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** → **RAID Management** → **Logical Device Information** from the menu bar. A sample screenshot of **Logical Device Information** section is shown below.

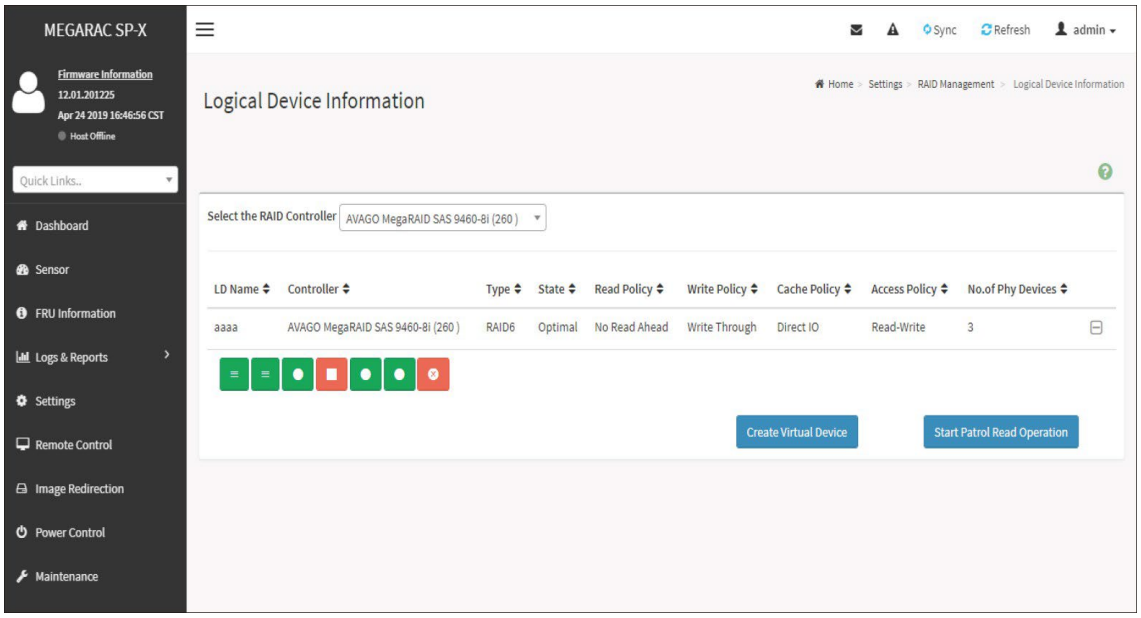


Logical Device Information

The fields of Logical Device Information page are explained below.

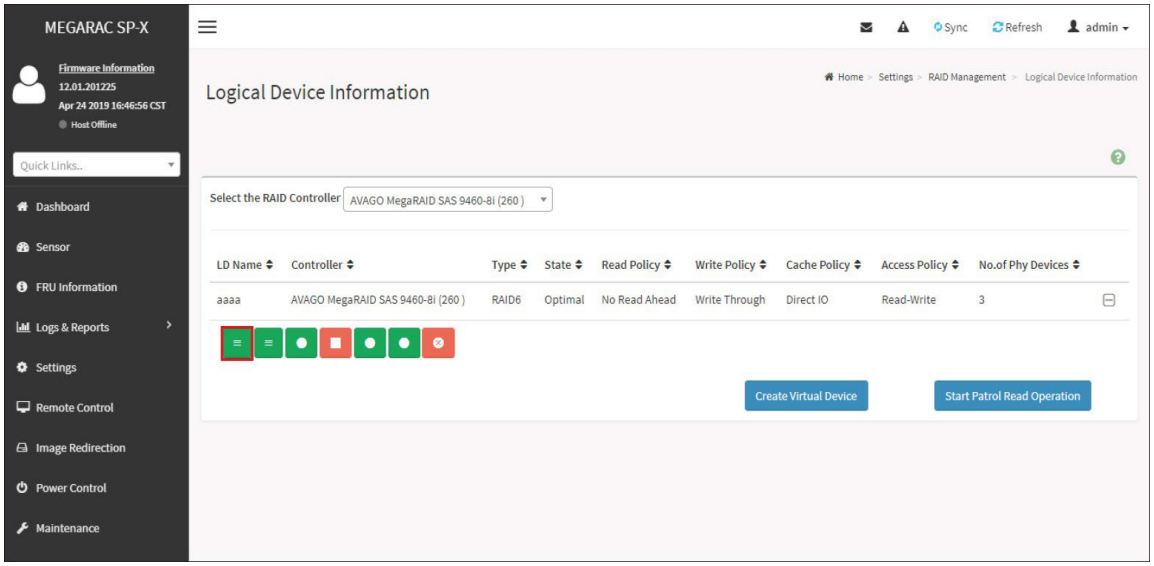
- **Select the RAID Controller**: To view the details of the Logical devices configured under the specific RAID controller.
- **LD Name**: Displays the name of the Logical Device configured under selected RAID controller.
- **Controller**: Displays the Name of the RAID Controller under which the Logical 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.
- **Write Policy**: Displays the Write Policy of the Logical Device.
- **Cache Policy**: Displays the Cache Policy details 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.



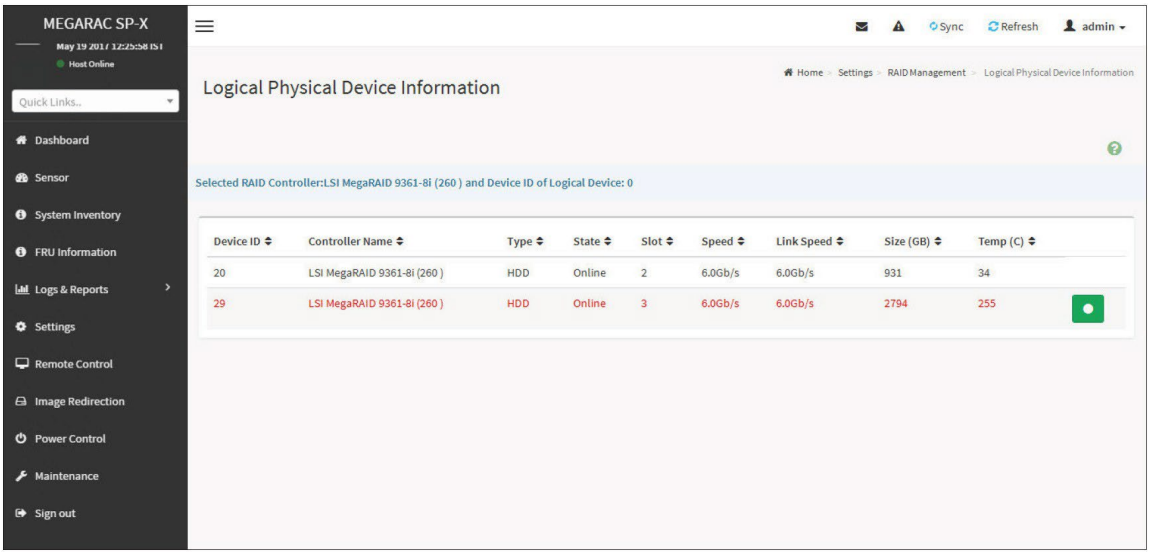
Logical Device Information

- **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.



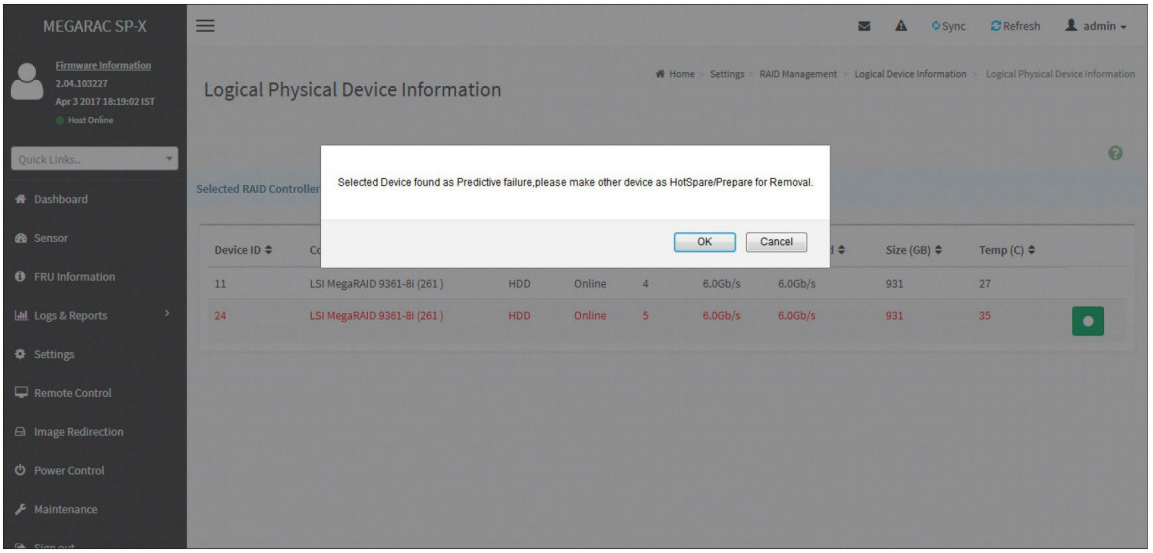
Logical Device Information

- **Predictive Failure in Logical Device**: This section displays the details about the Predic- tive Failure of Physical Device in the Logical Devices (RAID Level RAID 1) connected to the RAID controller. To open the **Logical Device Information**, click Settings → RAID Management → Logical Device Information from the menu bar. A sample screenshot of **Logical Device Information** section is shown below.



Logical Device Information

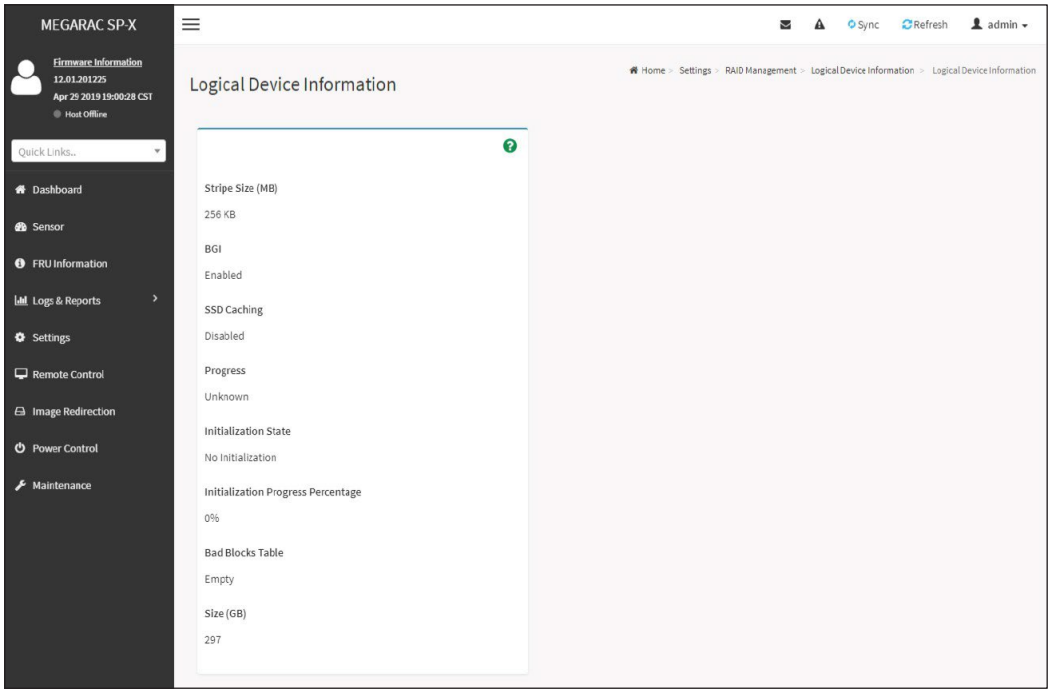
- Click (●) icon to change the physical device status as Online/Offline. A warning message will prompt you to make other device as HotSpare/Prepare for Removal. Click OK. A sample screenshot of Logical Device Information section is shown below.



Logical Device Information

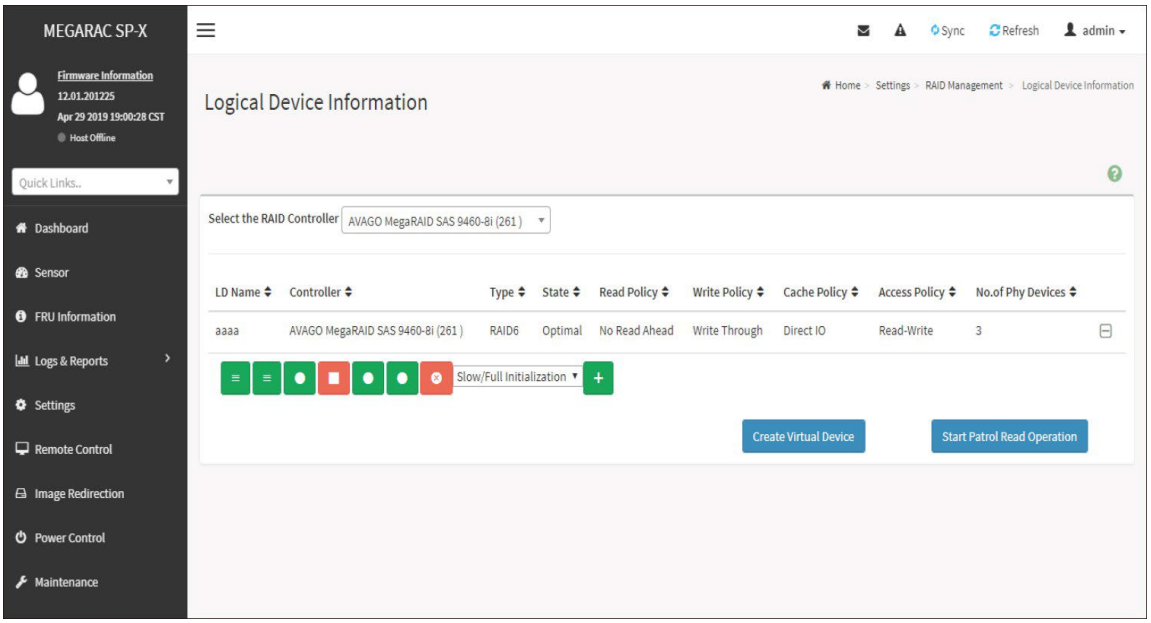
NOTE
Predictive Failure Devices will be highlighted in red color.

- **Check Advanced Properties**: Click ( ) icon to view the advanced properties of the selected Logical device. A sample screenshot is shown below.



Logical Device Information - Advanced properties

- **Start Locating Virtual Device**: Click ( ) icon to start locating the selected Virtual Device, LED of corresponding physical device configured for specified Logical Device will glow. A pop-up message prompts you to confirm your choice. Upon confirmation, you will be informed about the status.
- **Stop Locating Virtual Device**: Click ( ) icon to stop locating the selected Virtual Device, LED of corresponding physical device configured for specified Logical Device will stop glow. A pop-up message prompts you to confirm your choice. Upon confirmation, you will be informed about the status
- **Start/Cancel Consistency Check**: Click ( ) icon to start/cancel consistency check of the device. A pop-up message prompts you to confirm your choice. Upon confirmation, you will be informed about the status.
- **Check Initialize Check**: Click ( ) icon and select the Initialization type from the drop-down list. A sample screenshot is shown below. Then click on [+] button to start initialization.



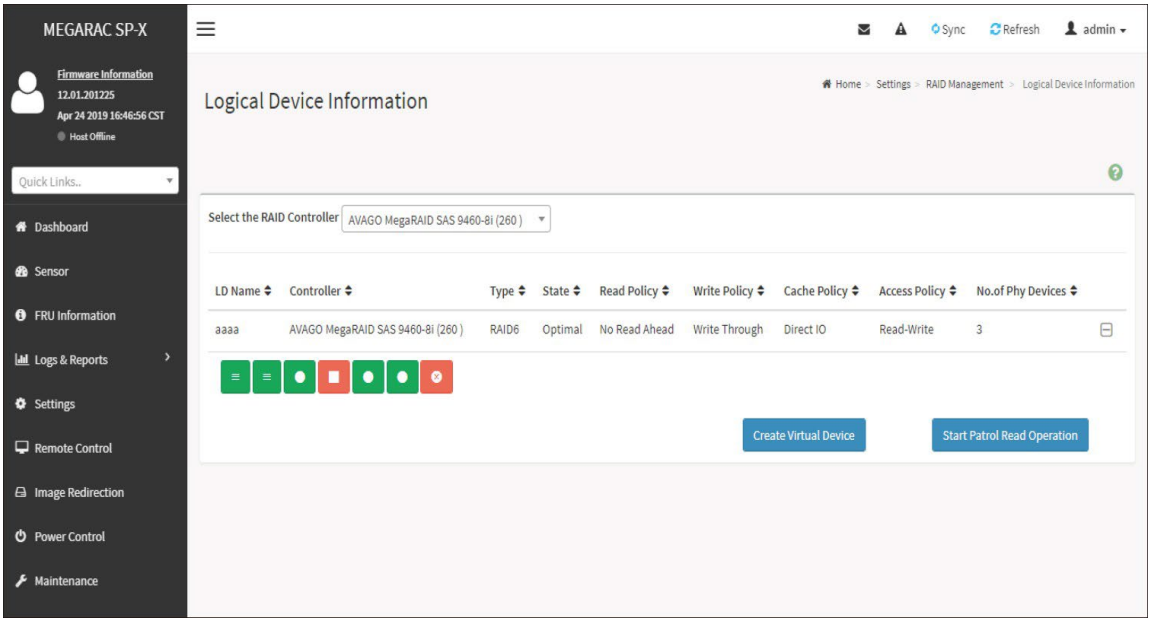
Logical Device Information - Initialize check

- **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.

To Start/Stop Patrol Read Operation

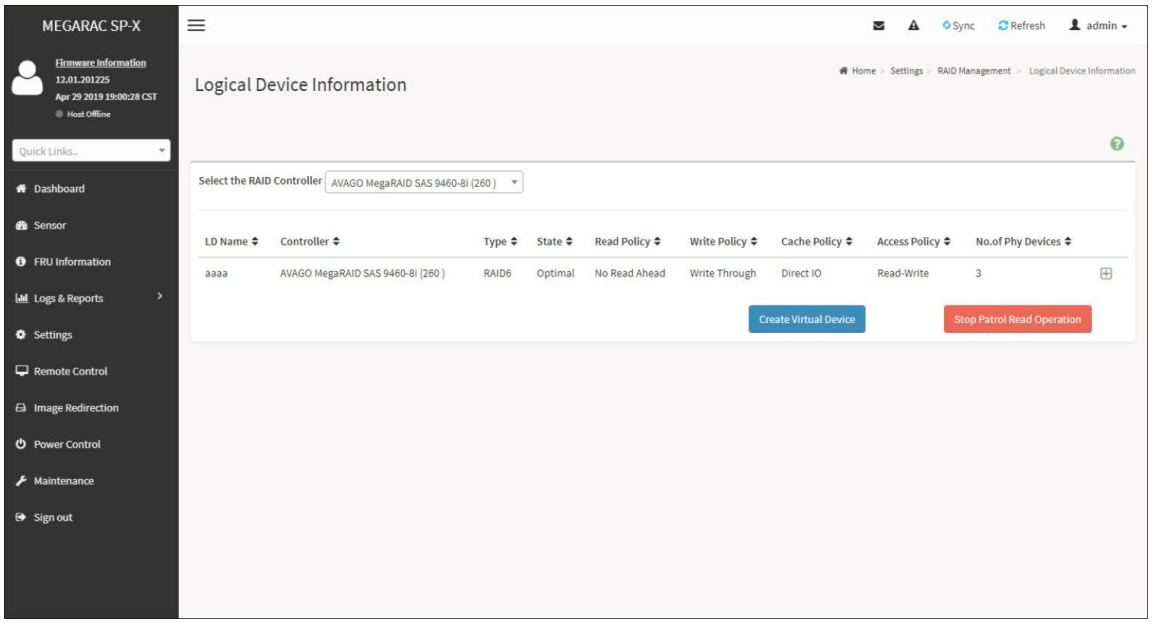
Start/Stop patrol read operation involves review of your system for possible drive errors that could lead to drive failure and then action to correct errors.

1. Click **Start Patrol Read Operation** to start Patrol read. A sample screenshot is displayed below.



Start Patrol Read

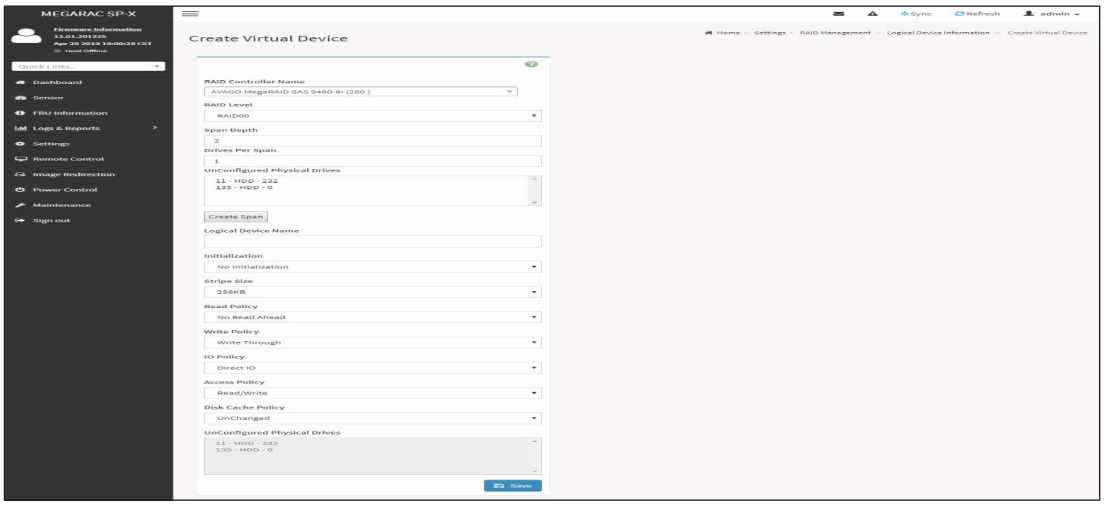
2. Click **Stop Patrol Read Operation** to stop Patrol read. A sample screenshot is displayed below.



Stop Patrol Read

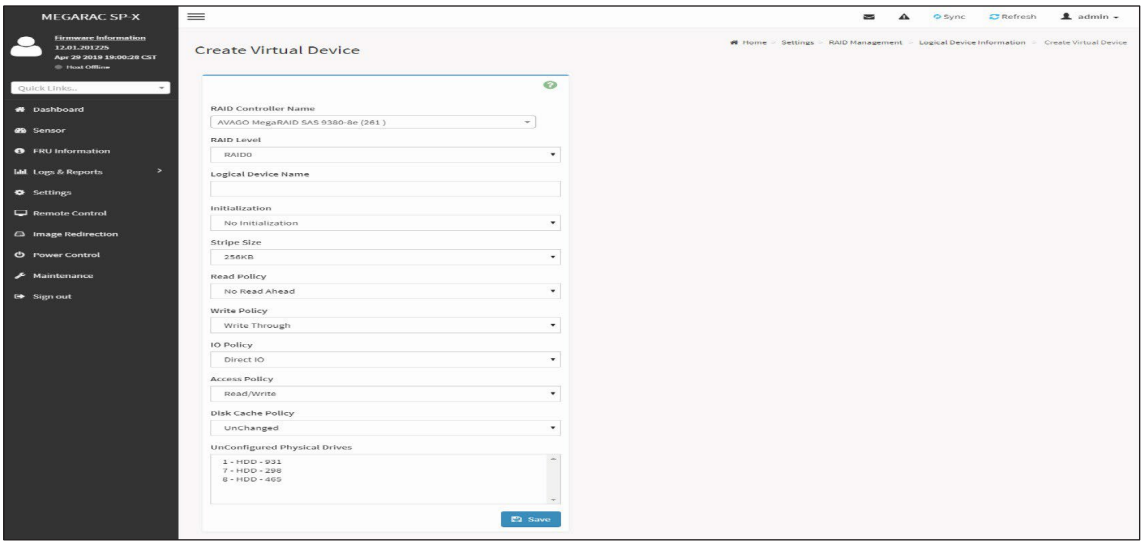
To Create Virtual Device

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

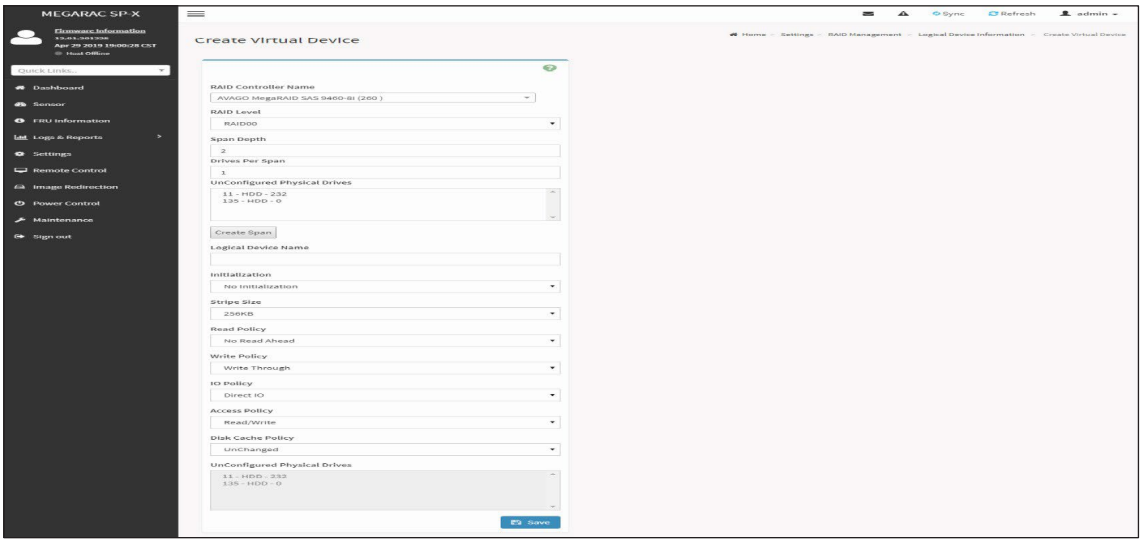


Create Virtual Device

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.



Create Virtual Device - RAID 0



Create Virtual Device - RAID 00

> **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 Unconfi gured 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**, **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.

To Delete Logical Device

1. Select the Device to be deleted and click **Delete Logical Device** to delete the selected logical volume. The selected virtual device will be deleted.

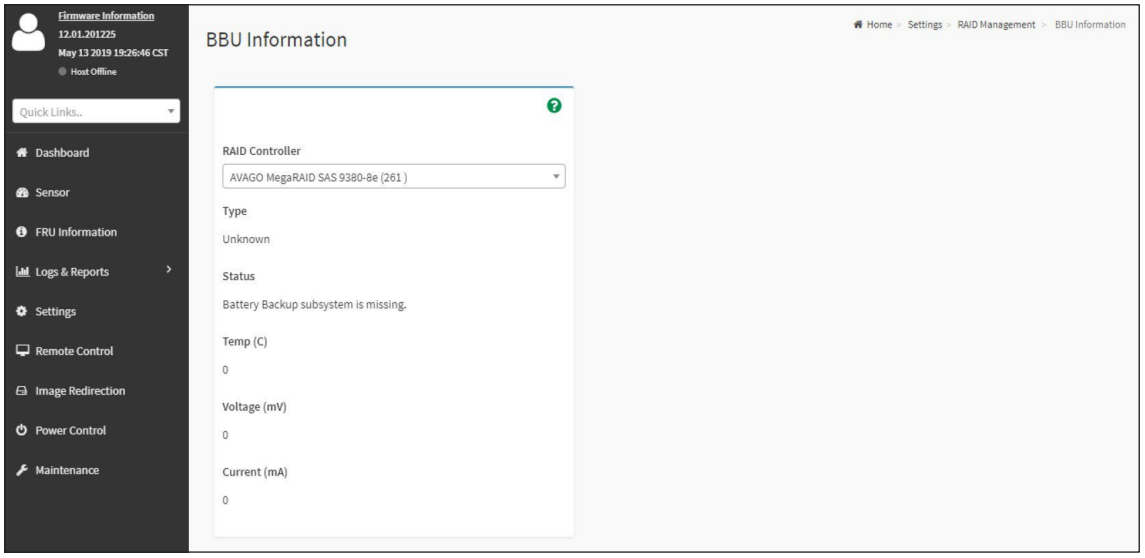
11.10.5 BBU Information

This tab displays the Battery Backup Unit Information. The battery backup units (BBUs) provide backup power to the storage controllers in the RAID environments to protect the data integrity.

- Type
- Status
- Temp (°C)
- Voltage (mV)
- Current (mV)

To open the BBU Information section, click **Settings** → **RAID Management** → **BBU Information** from the menu bar.

A sample screenshot of **BBU Information** section is shown below.



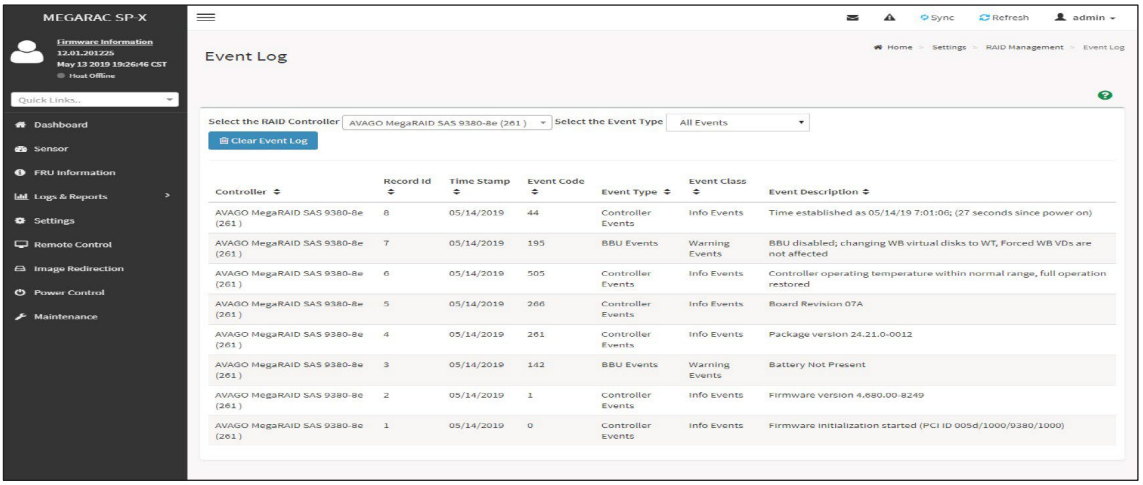
BBU Information

11.10.6 Event Log

This page displays all the RAID Controller events occurred that has been already configured. To open the Event Log section, click **Settings** → **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

The Event Log page consists of the following Fields.

Select a RAID Controller: To view the Event logs corresponding to the specific RAID Controller.

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.

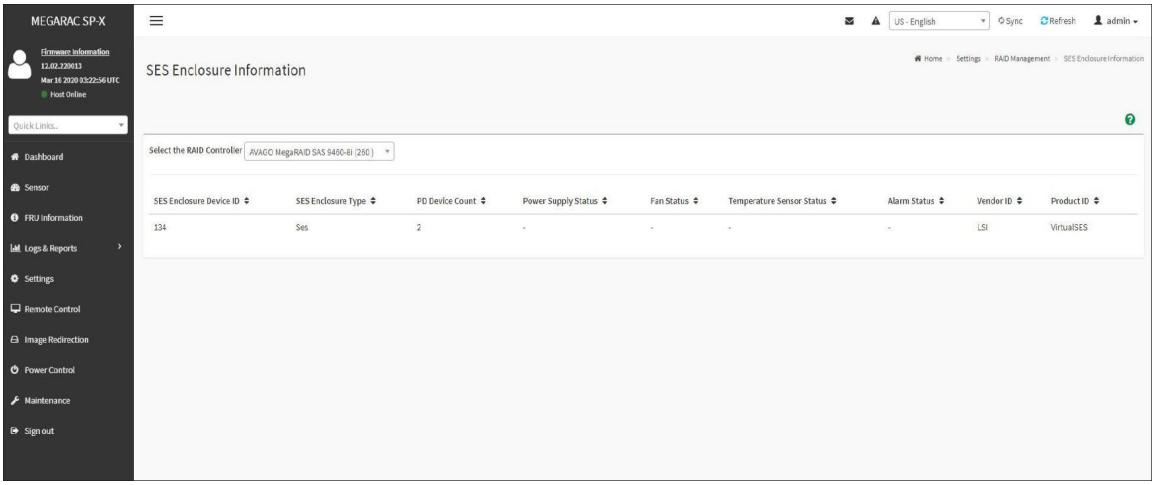
Procedure

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**.

11.10.7 SES Enclosure Information

This page displays the details about the SES Enclosure Information connected to the RAID controller.

To open the SES Enclosure Information section, click **Settings** → **RAID Management** → **SES Enclosure Information** from the menu bar. A sample screenshot of **SES Enclosure Information** is shown below.



SES Enclosure Information

On selecting any particular RAID Controller from the drop-down list, the SES Enclosure information will be displayed as follows.

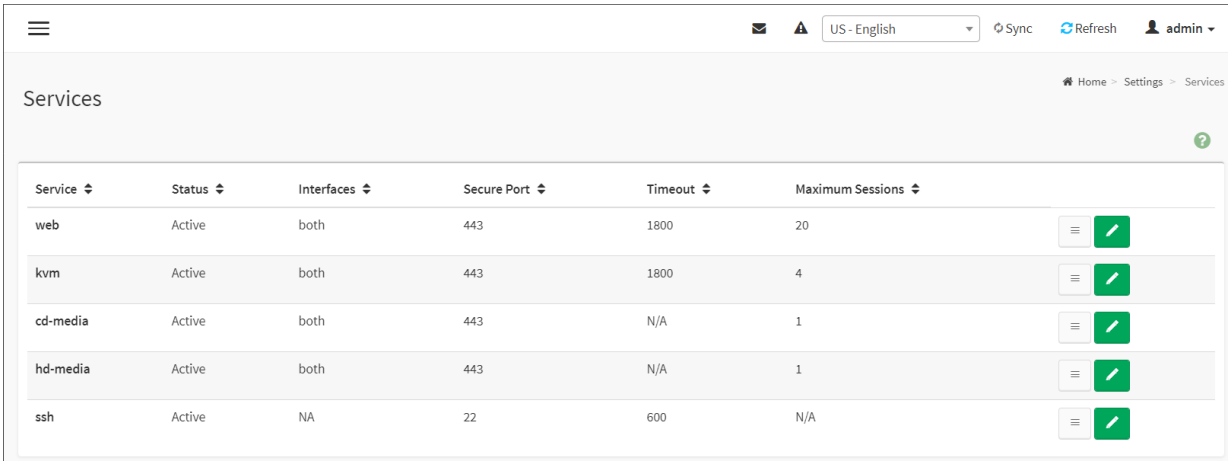
- **SES Enclosure Device ID**: Displays the SES Enclosure Device ID under selected RAID controller.
- **SES Enclosure Type**: Displays the SES Enclosure Type under selected RAID controller.
- **PD Device Count**: Displays the count of physical device under RAID controller.
- **Power Supply Status**: Displays the enclosure element status for connected power supply of RAID controller.
- **Fan Status**: Displays the enclosure element status for the connected fan of RAID controller.
- **Temperature Sensor Status**: Displays the enclosure element status for connected temperature sensor of RAID controller.
- **Alarm Status**: Displays the enclosure element status for connected alarm of RAID controller.
- **Vendor ID**: Displays the vendor ID under selected RAID controller.
- **Product ID**: Displays the product ID under selected RAID controller.

11.11 Service

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

To open Services page, click **Settings** → **Services** from the menu bar.

A sample screenshot of Services page is shown below.



Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions
web	Active	both	443	1800	20
kvm	Active	both	443	1800	4
cd-media	Active	both	443	N/A	1
hd-media	Active	both	443	N/A	1
ssh	Active	NA	22	600	N/A

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.

There is no determined port for the SOLSSH application since it is not running as service in BMC. It will use either of the ports from SSH/TELNET depending upon its activation.

- Web default port is 80
- KVM default port is 7578
- CD Media default port is 5120
- HD Media default port is 5123
- Telnet default port is 23

> **NOTE**
> SSH service will not support Non-secure port. 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
- SSH default port is 22
- VNC default port is 5901

NOTE
Telnet service and SOLSSH will not support secure port. If single port feature is enabled, KVM, CD Media, FD 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
Adviser (video server)	7578 (LP)
Cdserver	5120 (LP)
Hdserver	5123 (LP)

NOTE
LP – Loopback.
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.

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, 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.
- SSH and Telnet timeout value ranges from 60 to 1800 seconds.
- VNC timeout value ranges from 300 to 1800 seconds.
- SSH and telnet service will be using the same timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa.
- 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.

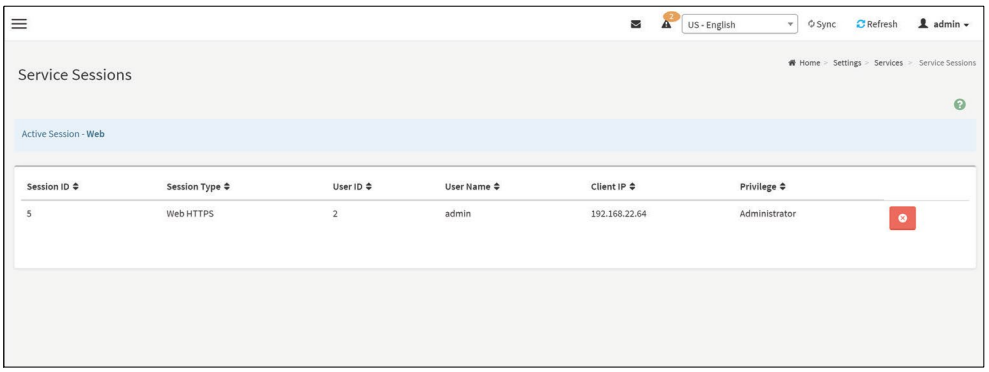
Active Sessions: To view the current active sessions for the service.

To view the Active Sessions:

> **NOTE**
> All active sessions in the BMC will be terminated if the BMC is rebooted.

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.



3. **Session Type**: Displays the type of the active sessions.
4. **User**: Displays the name of the user.
5. **Client IP**: Displays the IP addresses that are already configured for the active sessions.
6. **Privilege**: Displays the access privilege of the user.
7. Select a slot and click **Terminate** icon ( ) to terminate the particular session of the service.

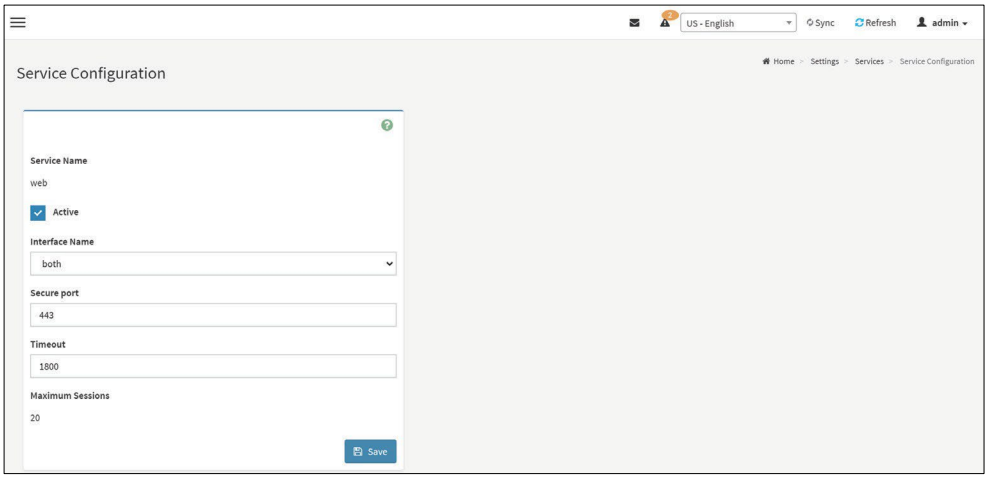
To modify the existing services:

Procedure

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.



3. **Service Name** is a read only field.
4. Activate the Current State by enabling the **Active** check box.

> **NOTE**
> Interfaces, 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.

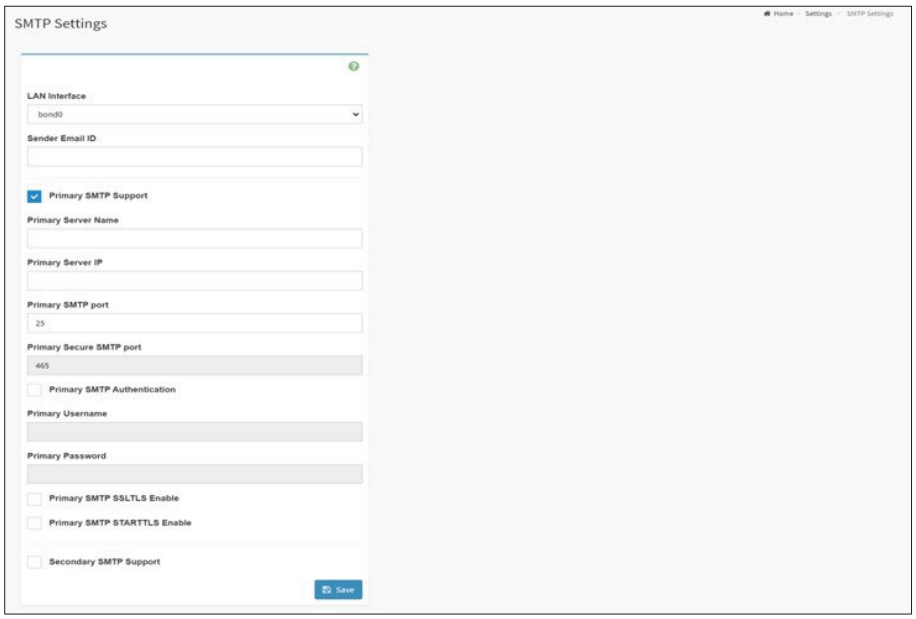
8. Click **Save** to save the entered changes else click **Cancel** to exit.

> **NOTE**
> Make sure that the SOLSSH service idle timeout should not be greater than the SSH idle timeout.

11.12 SMTP Settings

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

To open SMTP Settings page, click **Settings** → **SMTP Settings** from the menu bar. A sample screenshot of SMTP Settings page is shown below.



SMTP Settings Page

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(.), hyphen(-), at sign (@), and underscore(_).
> - 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 User name** 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 **SMTP Server Authentication** if you want to authenticate SMTP Server.
14. Enter your **Secondary User name** 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.

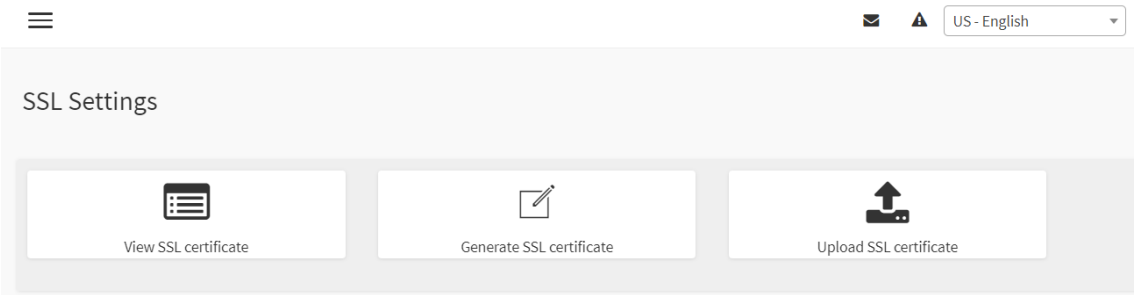
11.13 SSL Settings

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.

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** → **SSL Settings** from the menu bar. There are three tabs in this page.

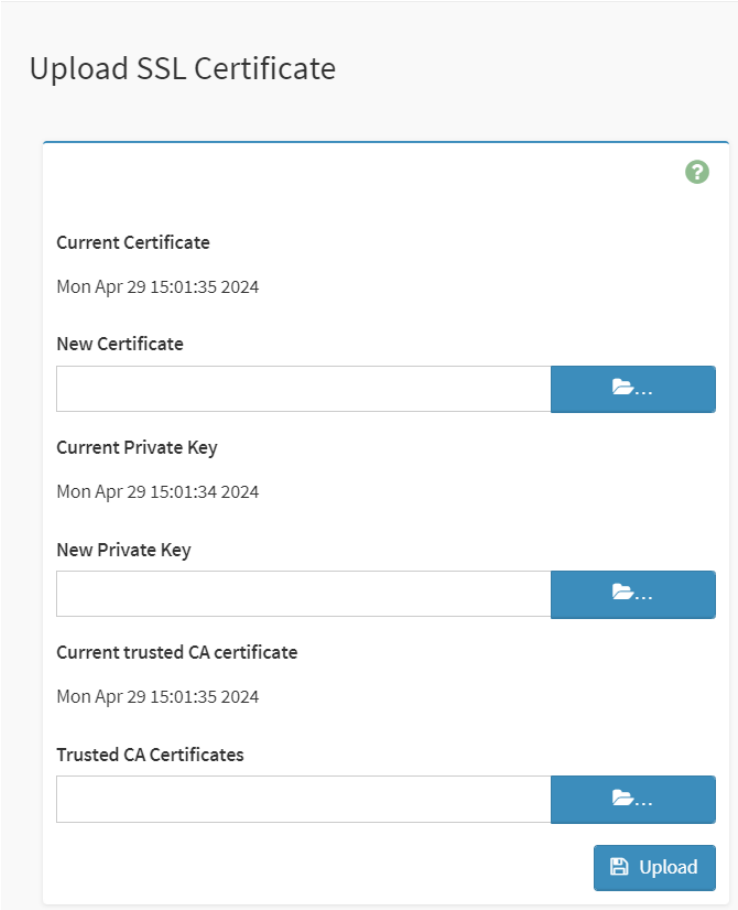
- **Upload SSL Certificate** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL Certificate** option is used to generate the SSL certificate based on configuration details.
- **View SSL Certificate** option is used to view the uploaded SSL certificate in readable format.



SSL Settings

11.13.1 Upload SSL Certificate

A sample screenshot of Upload SSL Certificate page is shown below.



SSL Settings – Upload SSL Certificate

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

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 will be displayed, and Trusted CA Support checkbox and Trusted CA Certificates fields are optional.
> If Redfish feature is enabled, Trusted CA Support checkbox will be hidden, and Trusted CA Certificates field is mandatory to upload.

Current trusted CA Certificate: Current trusted CA certificate and uploaded date/time will

be displayed (read-only).

Trusted CA Certificates: Certificate chain (or Chain of Trust) is made up of a list of certificates that start from a server's certificate and terminate with the root certificate. If your server's certificate is to be trusted, its signature has to be traceable back to its root CA.

If the user uploaded New Certificate, New Private key & Intermediate key means in bmc concatenate all three files together and serve as server.pem

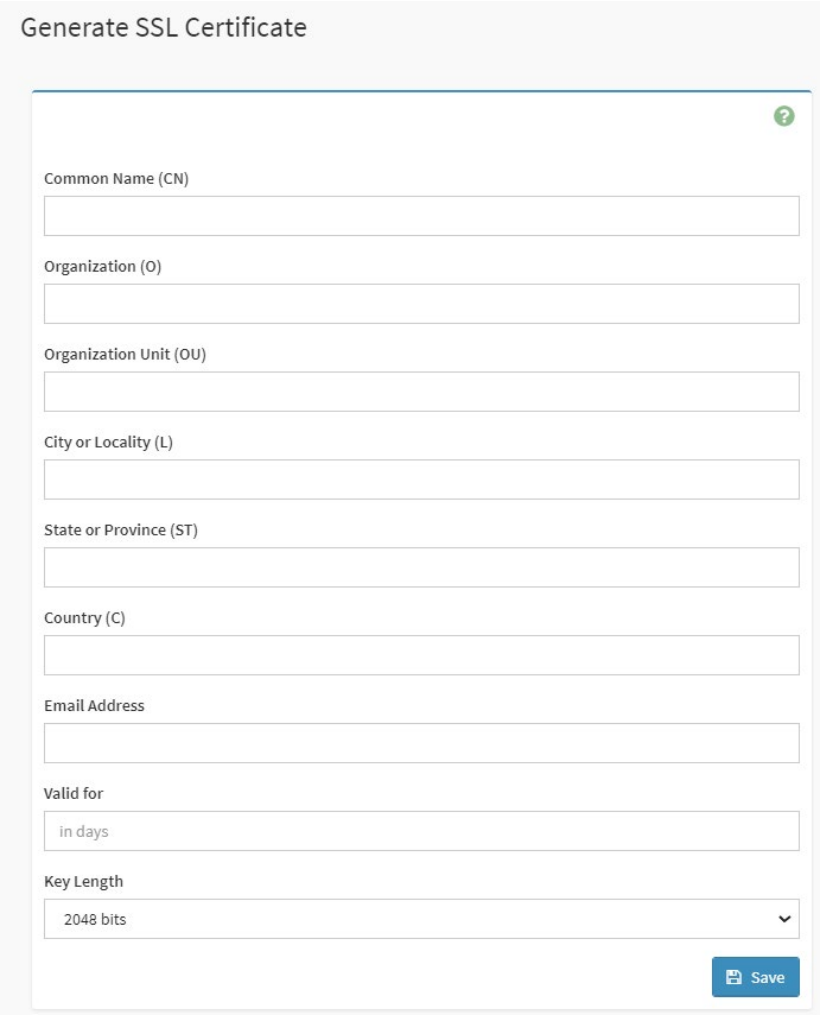
Based on the interlink between cacert & intermediate key shows the certificate chain.

Upload: To upload the SSL certificate and privacy key into the BMC.

NOTE
- Maximum New certificate size is 10240.
- Maximum New private key size is 10240.
- Uploading New Certificate and Private key should have 2048 bit.
- New Private key should not be encrypted.
- New Certificate should not expire.
- After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.
- If the user give Factory Restore Defaults, SSL certificate at the run-time will get vanish and it moves to the SSL certificate provided at the built-time.

11.13.2 Generate SSL Certificate

A sample screenshot of Generate SSL Certificate page is shown below.



SSL Settings – Generate SSL Certificate

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.

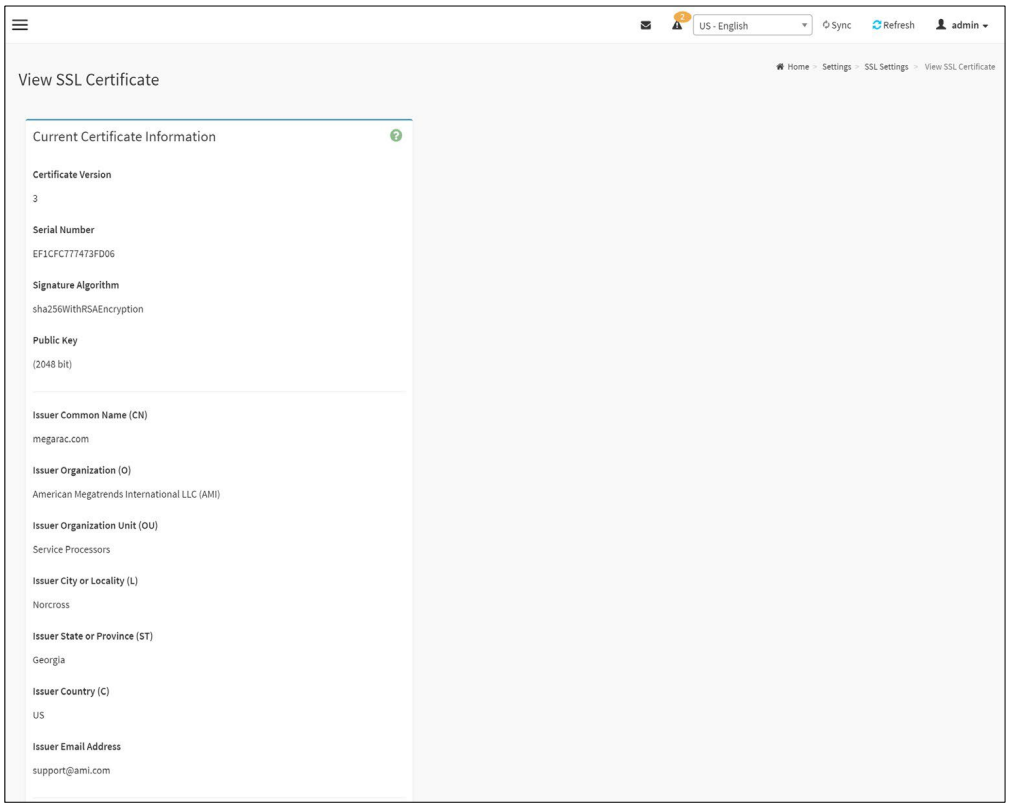
- Value ranges from 1 to 3650 days.

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.

11.13.3 View SSL Certificate



SSL Settings – View SSL Certificate

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

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.

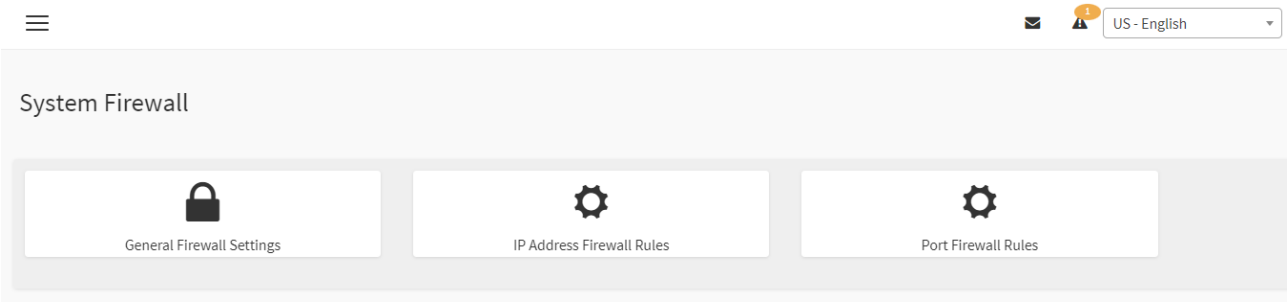
NOTE

- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your BMC securely using the following format in your IP Address field from your Internet browser: https://<your BMC address here>
- For example, if your BMC's IP address is 192.168.22.30, enter the following: https://192.168.22.30
- Please note the <s> after <http>. You must accept the certificate before you are able to access your BMC.

11.14 System Firewall

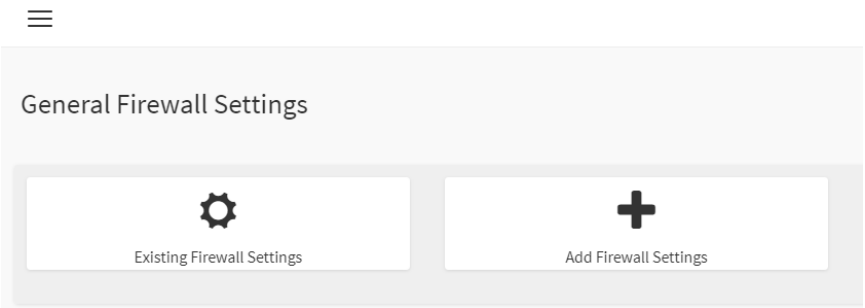
The System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

To open System Firewall page, click **Settings** → **System Firewall** from the menu bar.



11.14.1 General Firewall Settings

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



General Firewall Settings

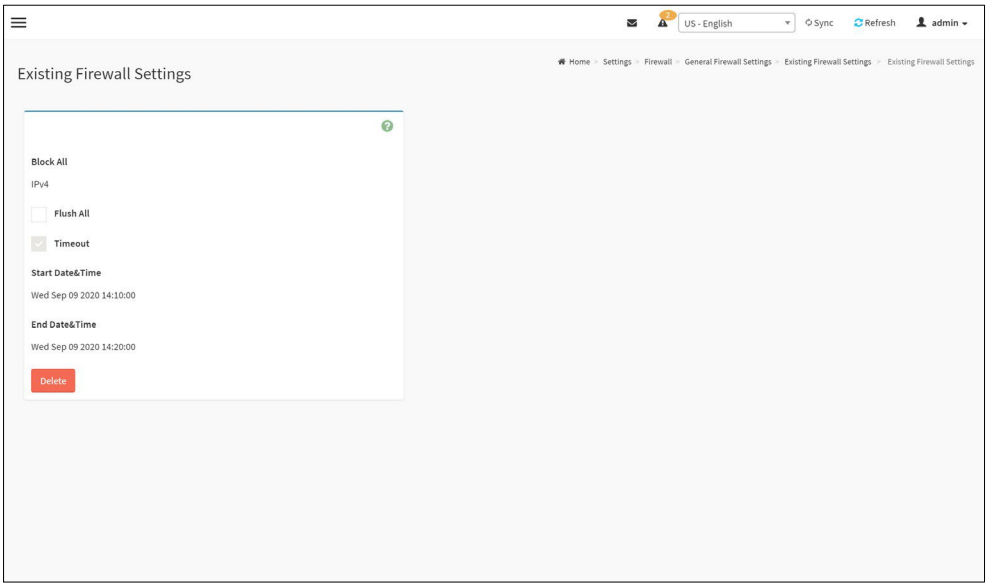
The fields of Firewall Settings tab are explained below.

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 settings 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.

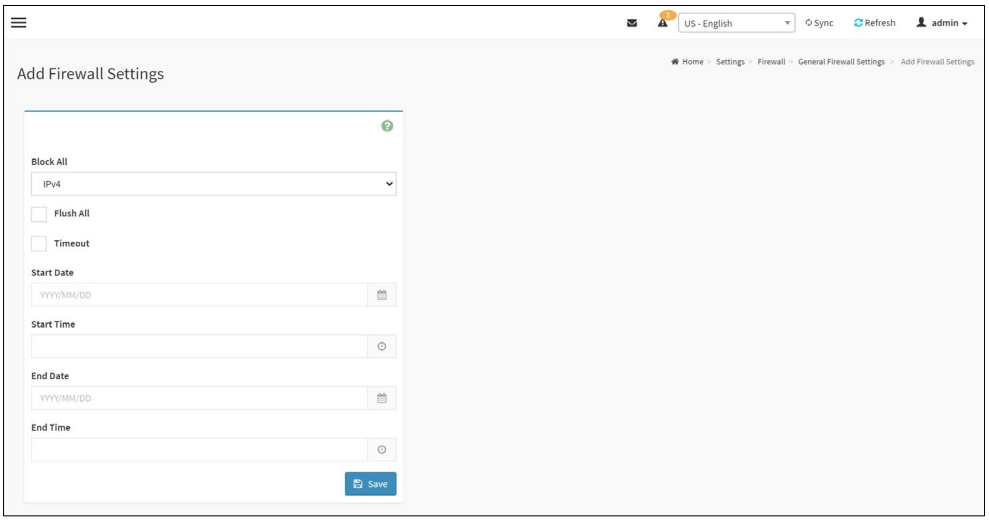


Existing Firewall Settings

- **Block All**: The blocked incoming IP's and Port's can be viewed.
- **Flush All**: To flflush all the system firewall rules (Read-Only).
- Select **Timeout** to enable or disable firewall rules with timeout.
- **Time Out**: The respective firewall rule effffect 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

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.

> **NOTE**
> User is recommended to enable either Flush All or Timeout Firewall rules to add firewall settings.

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 formart.

7. Click **Save** to save the changes made else click **Cancel** to go back to the previous screen.

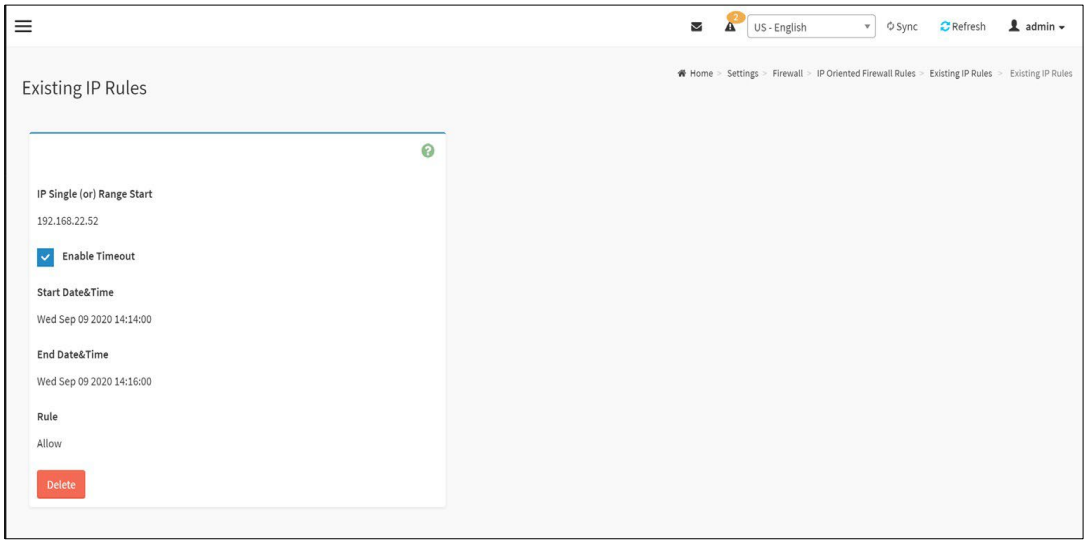
11.14.2 IP Address Firewall Rules

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** → **System Firewall** → **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.



System Firewall - Existing IP Rule

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.

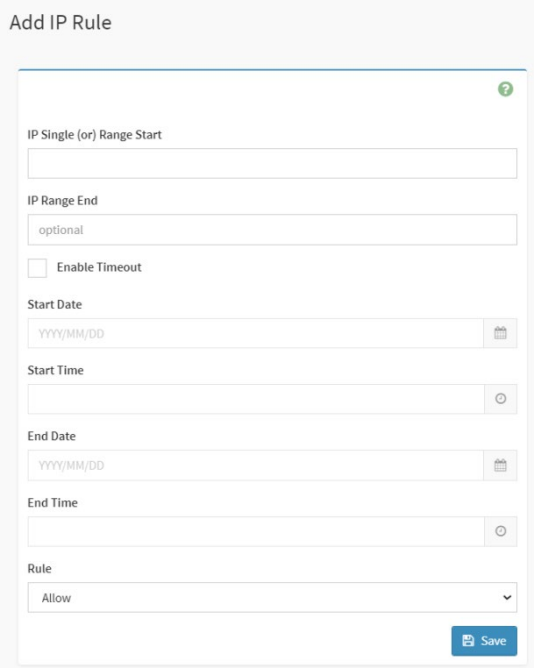
End Time: The respective firewall rule effect will end from this time.

Rule: To indicate the current setting of the listed Port or Range of Port rules (Allow or Block) status.

Delete: To delete the selected slot.

Procedure To add an IP address or range of IP addresses

1. Click **Settings** → **System Firewall** → **IP Address Firewall Rules** → **Add New IP Rule** to add a new IP or range of IP address.



Add IP Rule

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.

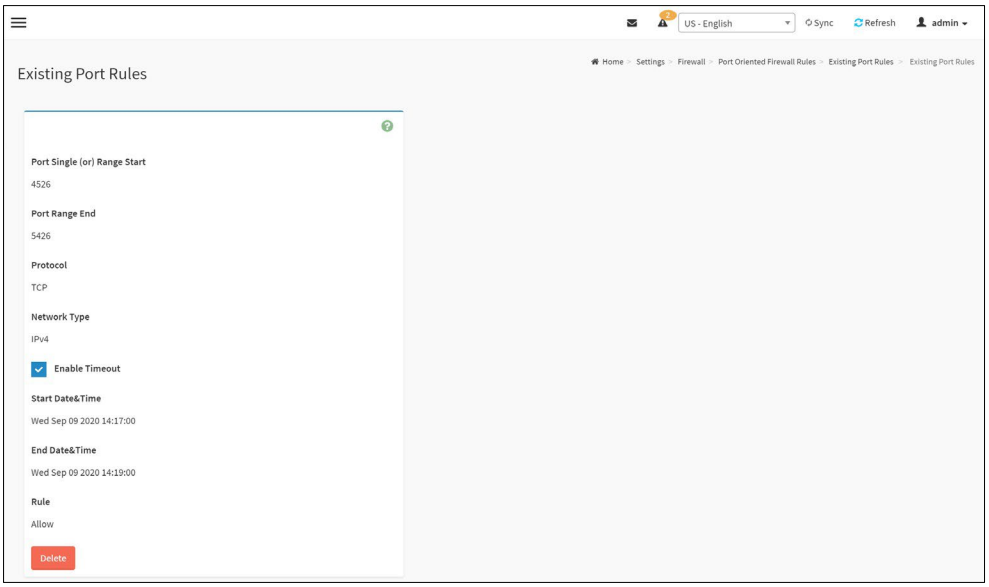
> **NOTE**
> The date and time should be in the YYYY/MM/DD and hh-mm formart respectively.

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

11.14.3 Port Firewall Rules

To view Existing Port Rules

1. Click **Settings** → **System Firewall** → **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.
2. Click the **Existing Port Rules**. A sample screenshot of Port tab is shown below.



System Firewall - Existing Port Rules

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.

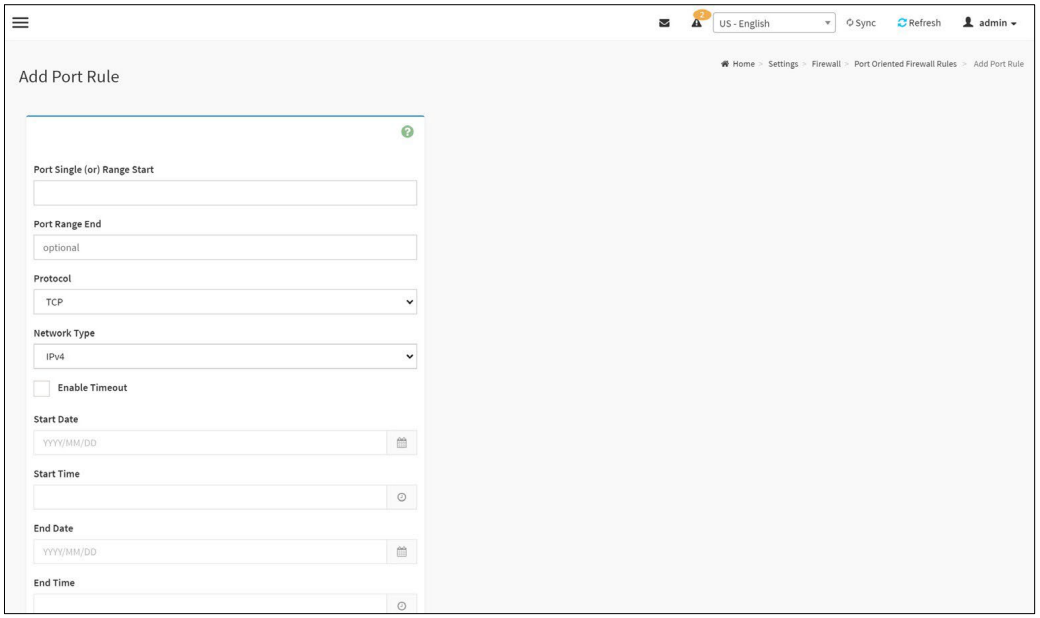
Rule: To indicate Allow or Block status.

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

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.

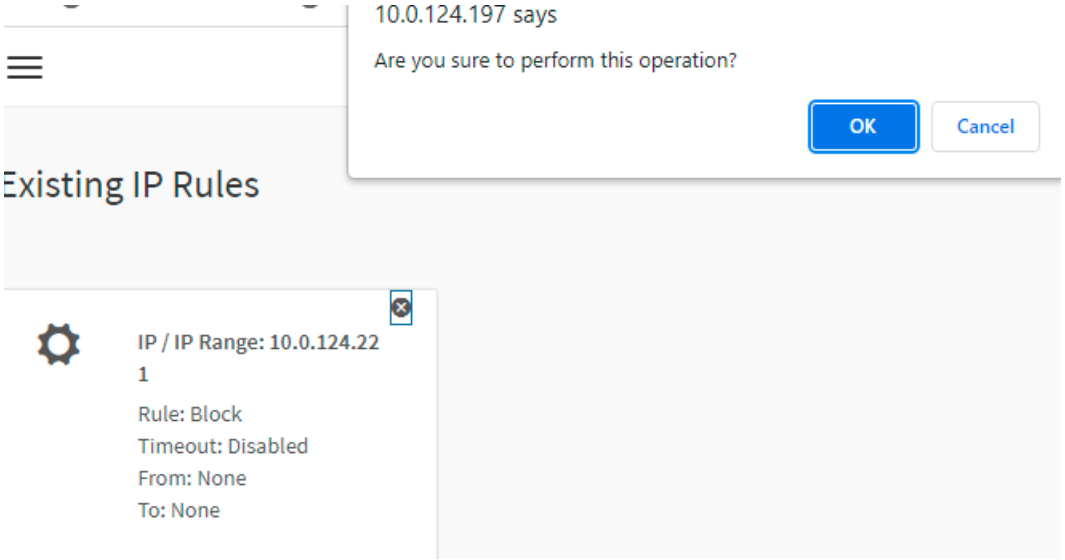
Procedure

To Recover Client System From Firewall

- A firewall rule will be added in BMC, if there is flood of packets like DoS attack from a client.
- This firewall will completely block the client IP so that no packets can reach BMC.
- Once the administrator makes sure that this firewall rule can be removed since there are no more attacks from the same IP, then the rule can be deleted from the existing firewall rules.

This firewall rule can be deleted by accessing WEBUI from a different client IP.

1. Click **General Firewall Settings** → **Existing Firewall Settings** icon. This action opens the Existng Firewall Settings page as shown in the screenshot below.

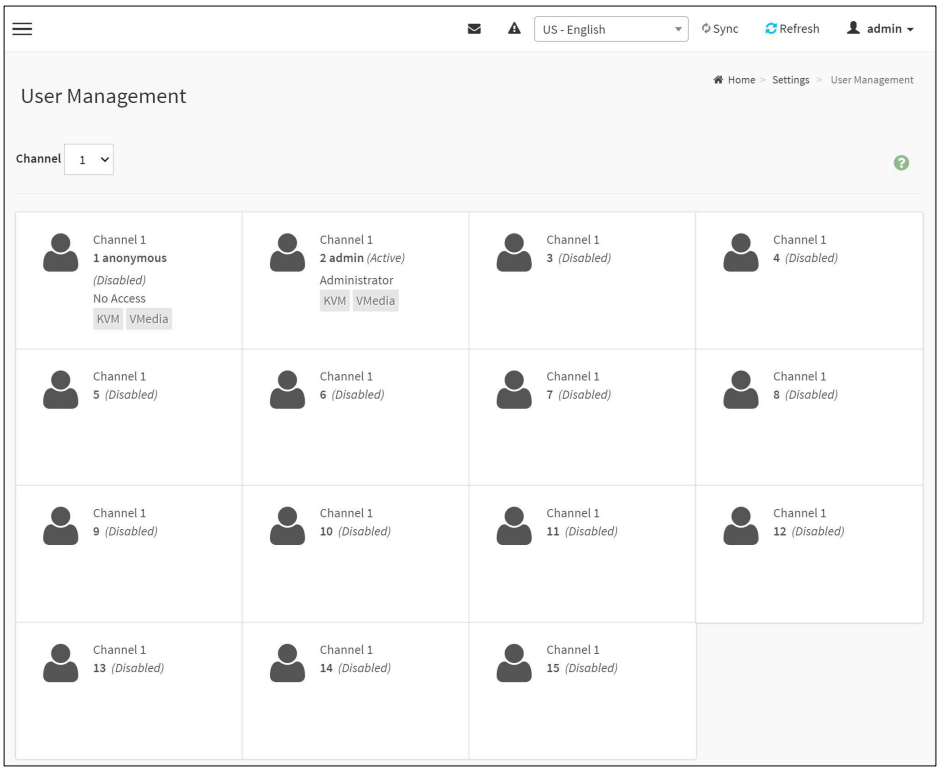


Existing Firewall Settings

11.15 User Management

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** → **User Management** from the menu bar. A sample screenshot of User Management page is shown below.



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 fifteen users only.

User Name: 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.

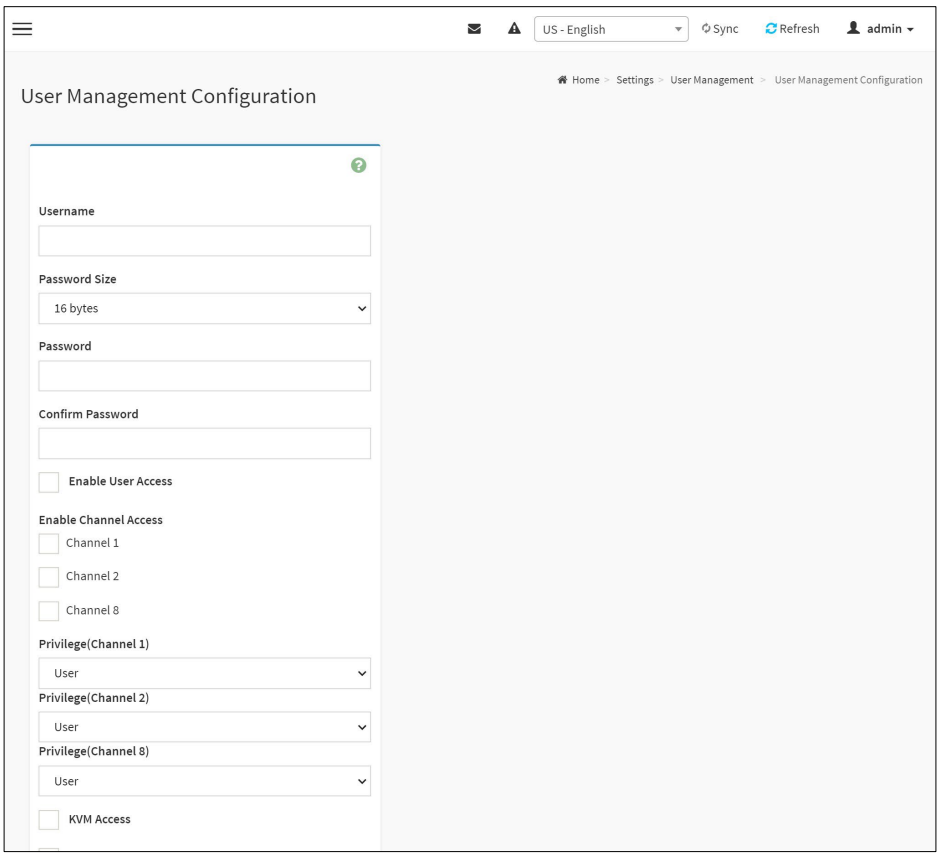
E-mail ID: Displays e-mail address of the user.

Add User: To add a new user.

Delete User: To delete an existing user.

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.



User Management Configuration

2. Enter the name of the user in the **User Name** 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”.

Hex	Char	Hex	Char
00	NUL ‘\0’	11	DC1 (device control 1)
01	SOH (start of heading)	12	DC2 (device control 2)
02	STX (start of text)	13	DC3 (device control 3)
03	ETX (end of text)	14	DC4 (device control 4)
04	EOT (end of transmission)	15	NAK (negative ack.)
05	ENQ (enquiry)	16	SYN (synchronous idle)
06	ACK (acknowledge)	17	ETB (end of trans. blk)
07	BEL ‘\a’ (bell)	18	CAN (cancel)
08	BS ‘\b’ (backspace)	19	EM (end of medium)
09	HT ‘\t’ (horizontal tab)	1A	SUB (substitute)
0A	LF ‘\n’ (new line)	1B	ESC (escape)
0B	VT ‘\v’ (vertical tab)	1C	FS (file separator)
0C	FF ‘\f ’ (form feed)	1D	GS (group separator)
0D	CR ‘\r’ (carriage ret)	1E	RS (record separator)
0E	SO (shift out)	1F	US (unit separator)
0F	SI (shift in)	20	SPACE
10	DLE (data link escape)	7F	DEL

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

NOTE
- Enabling Channel User Access will intern assign the IPMI messaging privilege to the specific Channel 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, select the privilege assigned to the user which could be Administrator, Operator, User, OEM or None. By default, the channel privileges will be displayed based on the channel availability.

NOTE
Callback privilege will be displayed in Privilege field only if its assigned by other interfaces.
By default, Callback privilege will not available to set privilege as like other privilege options from Web UI.

8. Check **KVM Access** to assign the KVM privilege for the user.

NOTE
While modifying the KVM access by logged in User, it will prompt you with the alert message to log out the current session to reflect the changes.

9. Check **VMedia Access** assign the VMedia privilege for the user.

NOTE
- The term VMedia represents H5Viewer, VMapp and VMCLI clients.
- 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.
- While modifying the KVM and VMedia access by logged in User, it will prompt you with the alert message to log out the current session to reflect the changes.

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** drop-down list. Either it can be Read Only or Read Write.

13. Choose the **SNMP Authentication Protocol** (SHA256, SHA384 and SHA512) to use for SNMP settings from the drop down list.

NOTE
Password field is mandatory, if Authentication protocol is changed. Currently only SHA256, SHA384 and SHA512 are supported. SHA and MD5 protocols are deprecated and can be used only if previously configured and preserved user has this protocol enabled.

14. Choose the **Encryption algorithm** to use for SNMP settings from the **SNMP Privacy protocol** drop-down 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.
    - Maximum allowed size for Email ID is 63 bytes, which includes username and domain name.
    - **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.

> **NOTE**
> SMTP Server must be configured to send emails.

16. In the **Upload SSH Key** field, click **Browse** and select the **SSH key file**.

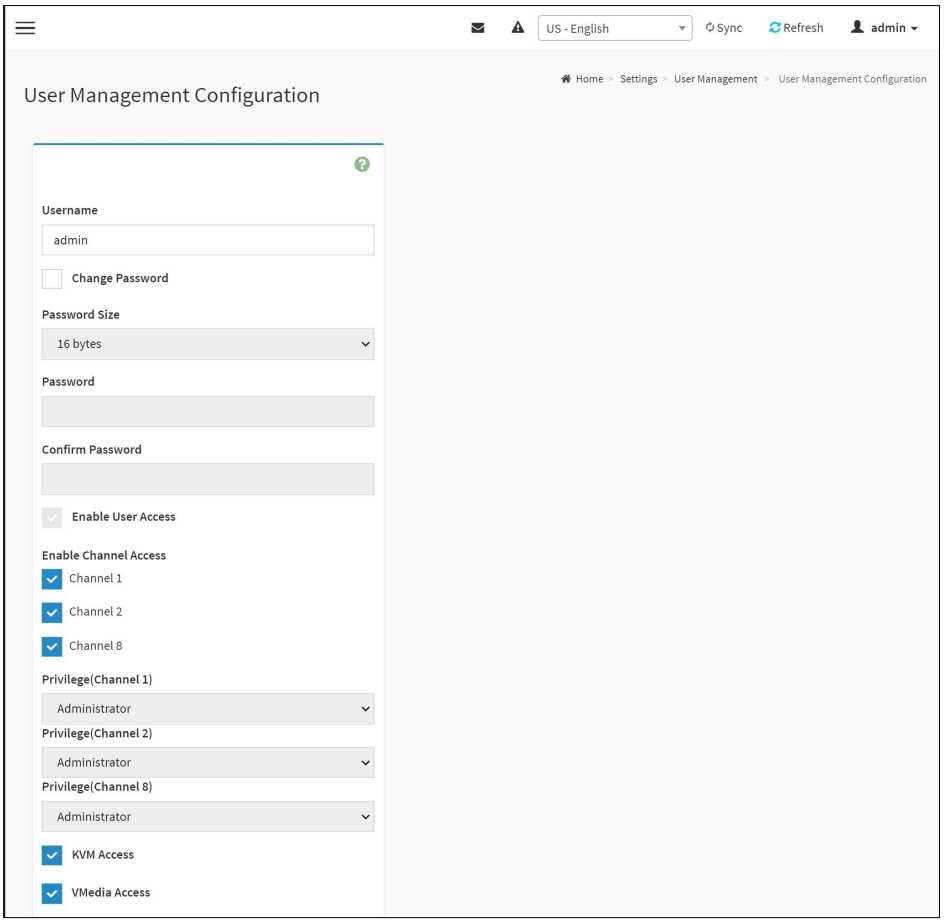
> **NOTE**
> SSH key file should be of pub type.

17. Click **Save** to save the new user and return to the users list.

To Modify User

> **NOTE**
> If any changes made in User Access/Privilege or KVM/VMedia access or Change Password, it will be reflected in the next login only.

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



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 password 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

There is a list of reserved users which cannot be added / modified as BMC users.

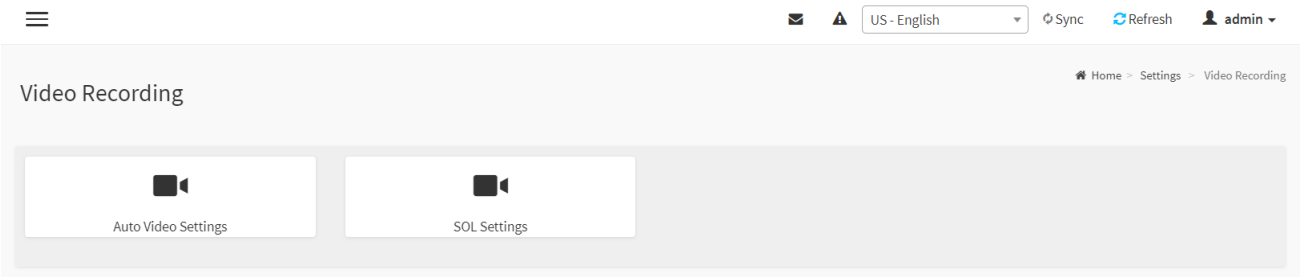
Important:

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

- sysadmin
- daemon
- sshd
- ntp
- root

11.16 Video Recording

To open SOL Set page, click **Settings** → **Video Recording** from the menu bar. A sample screenshot of the Video Recording is given below.

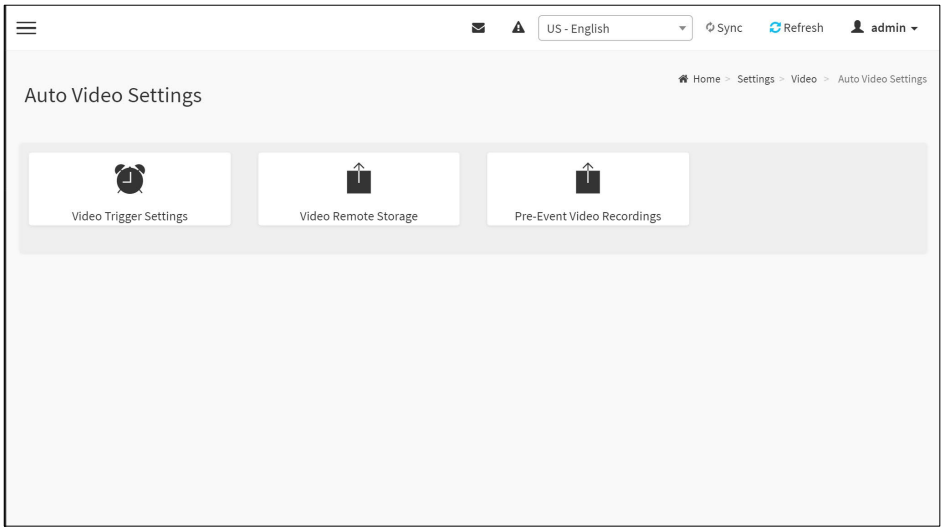


Video Recording

1. Auto Video Settings
   - Video Trigger Settings
   - Video Remote Storage
   - Pre-Event Video Recordings
2. SOL Settings
   - SOL Configurations

11.16.1 Auto Video Settings

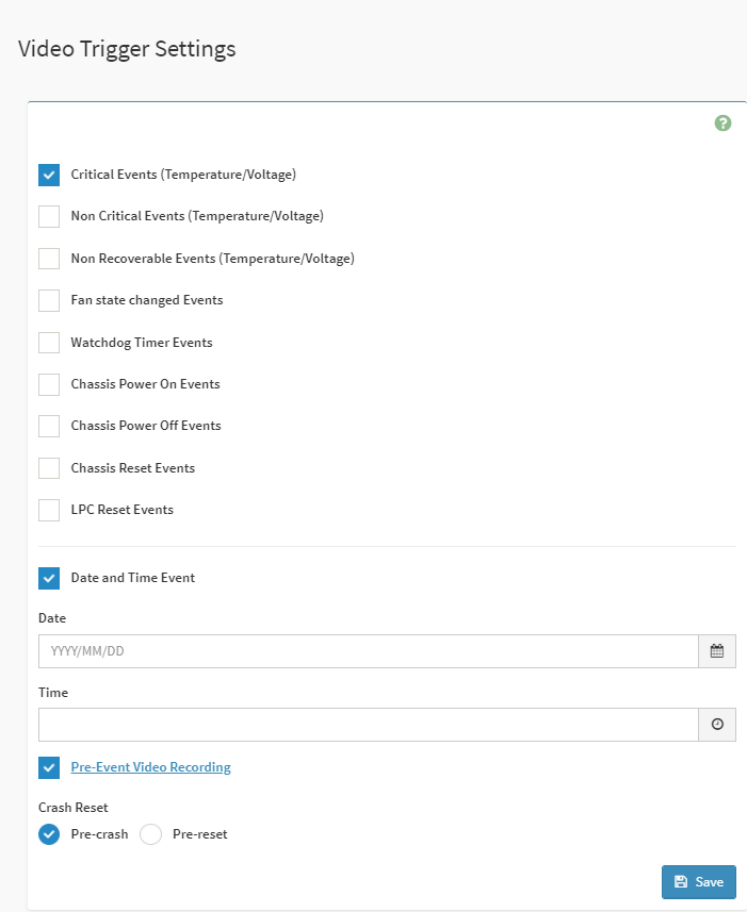
This page is used to configure the events that will trigger auto video recording function of the KVM server. A sample screenshot of the Video Recording is given below.



Auto Video Settings

11.16.1.1 Video Trigger 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.



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.

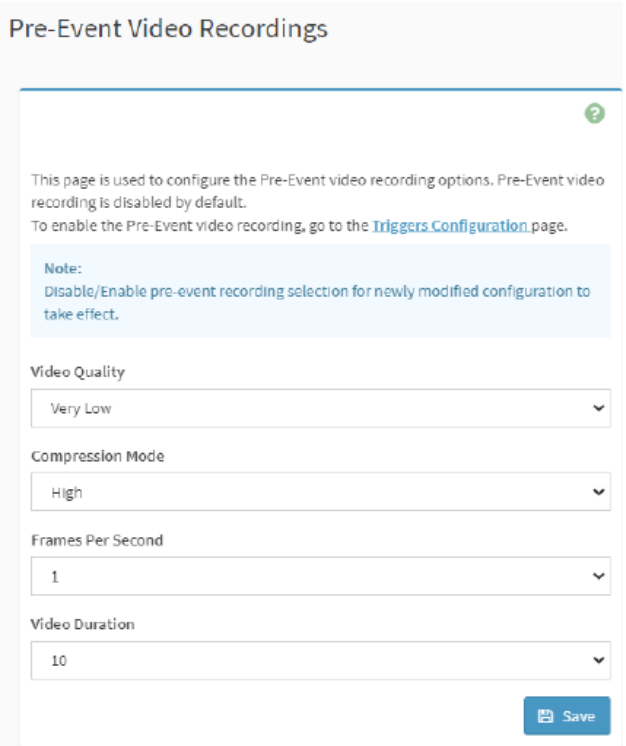
Procedure

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.

> **NOTE**
> Disable/Enable pre-event recording selection for newly modified configuration to take effect.



   A. 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.

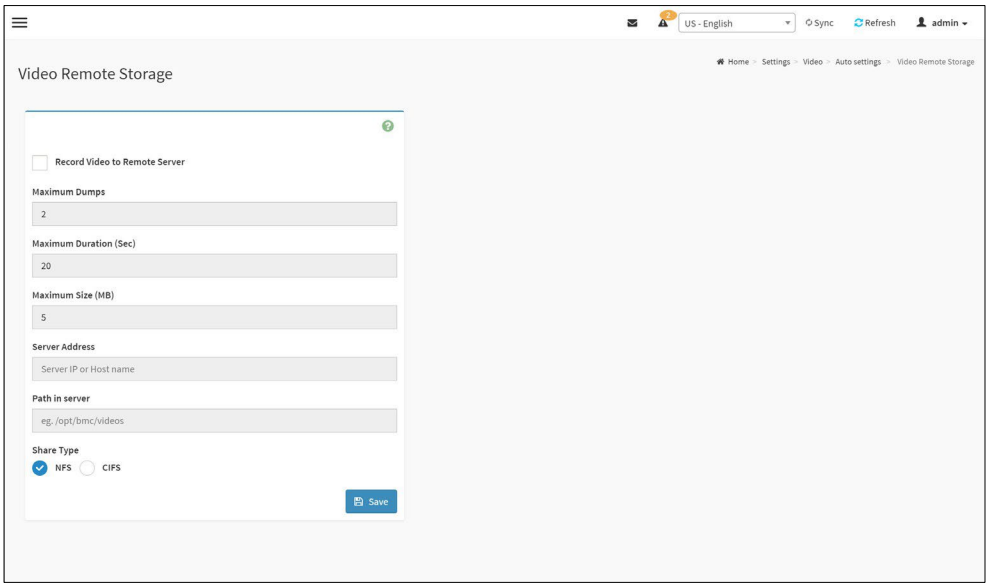
NOTE

Pre-Event video recording will not occur, while active KVM session or Post-event video recording is in progress.

For supporting video playback using standard video players (e.g. VLC), the downloaded AVI video file will be created with minimum of 3 FPS. Configured FPS value is not applicable here.

11.16.1.2 Video Remote Storage

To Video Remote Storage capture host video before critical event like crash or reset occurs, click **Video Recording** → **Auto Video Settings** → **Video Remote Storage**. A Sample screenshot of Video Remote Storage is as shown below.



Video Remote Storage

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 Duration (Sec)** of the video.
3. Enter **Maximum Size (MB)** of the video.
4. Enter **Maximum Dumps** 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:
> - IP Address (Both IPv4 and IPv6 format).
> - FQDN (Fully qualified domain name) format.

6. Enter the source path in **Path in Server** field.

> **NOTE**
> Path must be alpha-numeric and the following special characters are only allowed: '/'(backward slash), '\'(forward slash), '-'hyphen, '_'(underscore), '.'(dot) and ':'(colon). This field will not allow more than 256 characters.

7. Select the **Share Type** (NFS/CIFS). If the selected share type is (CIFS), enter the **User Name**, **Password** and **Domain Name** in the respective fields.
8. Click **Save** to save the settings.

Pre-Event

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.
	300 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.	

NOTE

- If video resolution change during auto-video recording then multiple video files will be downloaded. That is, a video file will be generated for each resolution change. So in case of resolution change, video file will be downloaded with name video_dump__%Y%m%dT%H%M%S_part.dat, where N is the number of files downloaded for a particular video recording.

  Multiple video files will be generated only for HTML video download option. In case of Java video download application, single video file will be downloaded even when resolution changes occurs. This behavior difference between HTML video download option and Java video download application is due to browser memory constrain.
- In some cases, the “power off” post-event cannot record the screen because of shutdown process, i.e.,host boot into BIOS/DOS, is too short.
- When the video file cannot be recorded due to some reasons, the video file cannot be downloaded /played.

11.16.2 SOL Settings

To open SOL Settings page, click **Settings** → **Video Recording** → **SOL Settings** from the menu bar. A sample screenshot of SOL Settings page is shown below.

SOL Settings

The SOL Settings consists of the fields as given below.

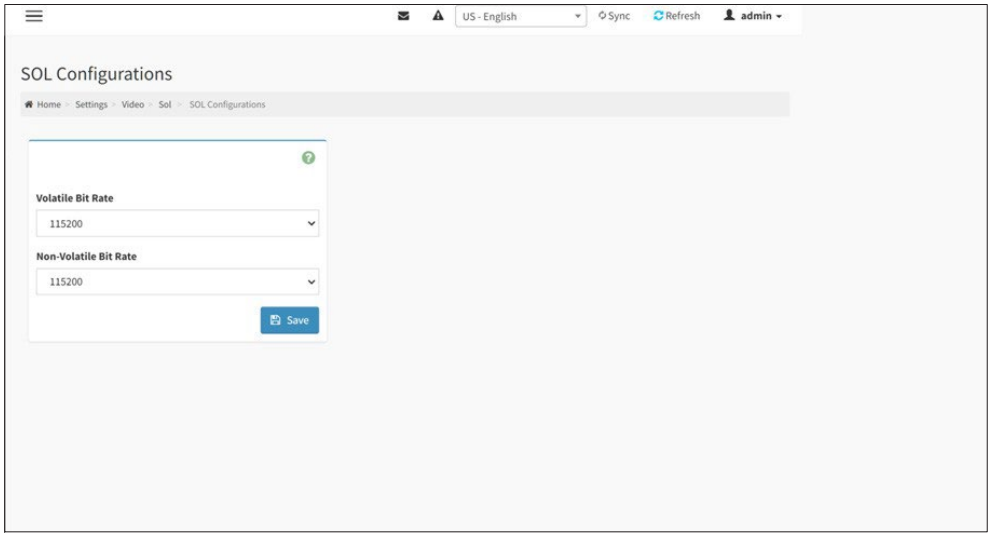
- SOL Configurations

11.16.2.1 SOL Configurations

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

- Volatile Bit Rate
- Non-Volatile Bit Rate

A sample screenshot of SOL Configurations page is shown below.



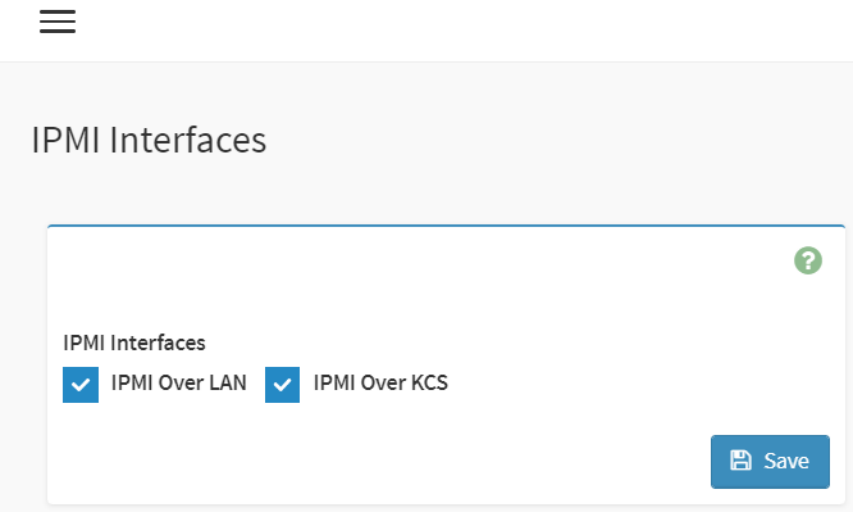
SOL Configurations

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.

11.17 IPMI Interfaces

This page is used to configure the IPMI Interfaces. To open IPMI interfaces page, click **Settings** → **IPMI Interfaces**. A sample screenshot of **IPMI Interfaces** page is displayed below.



IPMI Interfaces

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.

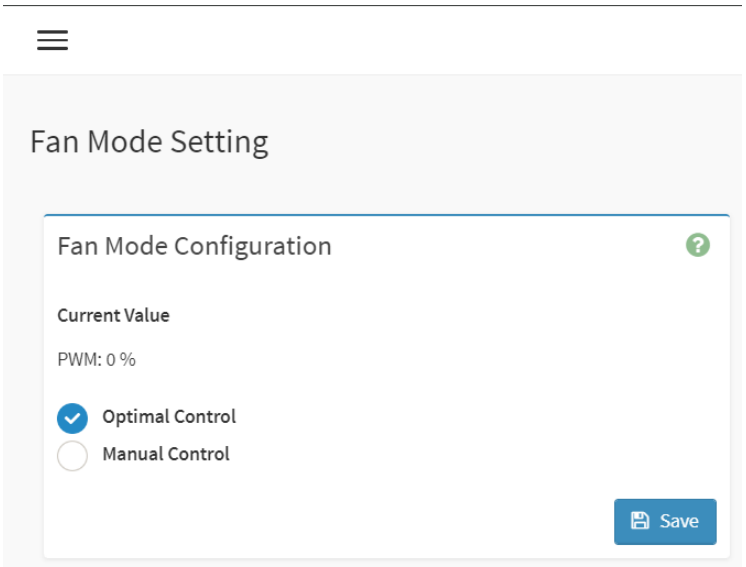
> **NOTE**
> IPMI Communication will not be performed over LAN /KCS interface if it is disabled.

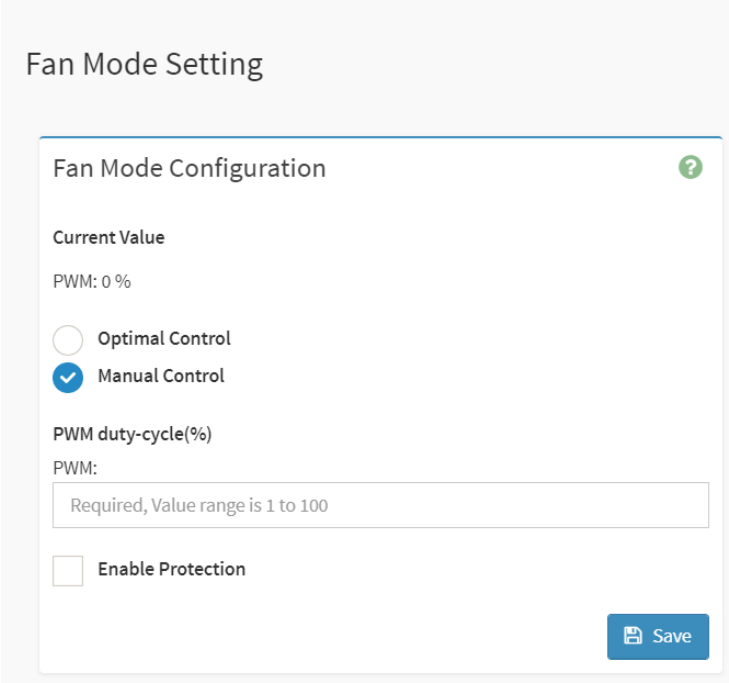
- **Save**: Click Save to save the configured interfaces

11.18 Fan Mode

Fan mode is used to set fan control policy on the device.

To open Fan Mode Setting page, click **Settings** → **Fan Mode** from the menu bar. A sample screenshot of Fan Mode Setting page is given as below.





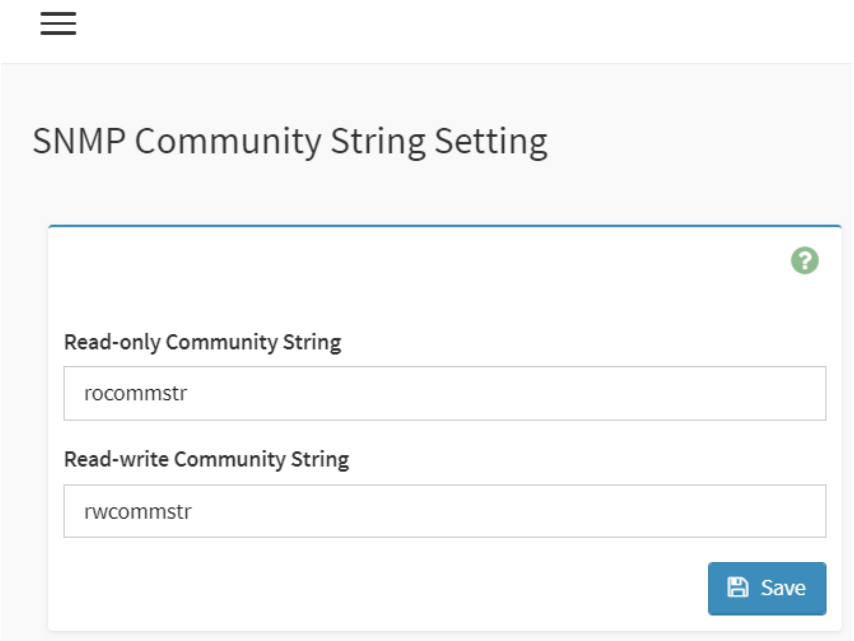
The fields of Fan Mode Setting page are explained below.

- **Optimal Control**: This mode will set all fans with smart fan algorithm.
- **Manual Control**: This mode will set all fans using manual PWM duty-cycle(%).
- **Save**: To save the changes made.

11.19 SNMP Community String

SNMP Community Strings are used for authentication and access control in SNMP (Simple Network Management Protocol) communication. They determine the level of access granted to devices within a network. The "read-only" community string allows devices to retrieve SNMP data, while the "read-write" community string enables devices to modify settings in addition to retrieving data.

To open SNMP Community String Setting page, click **Settings** → **SNMP Community String** from the menu bar. A sample screenshot of SNMP Community String Setting page is given as below.



The fields of SNMP Community String Setting page are explained below.

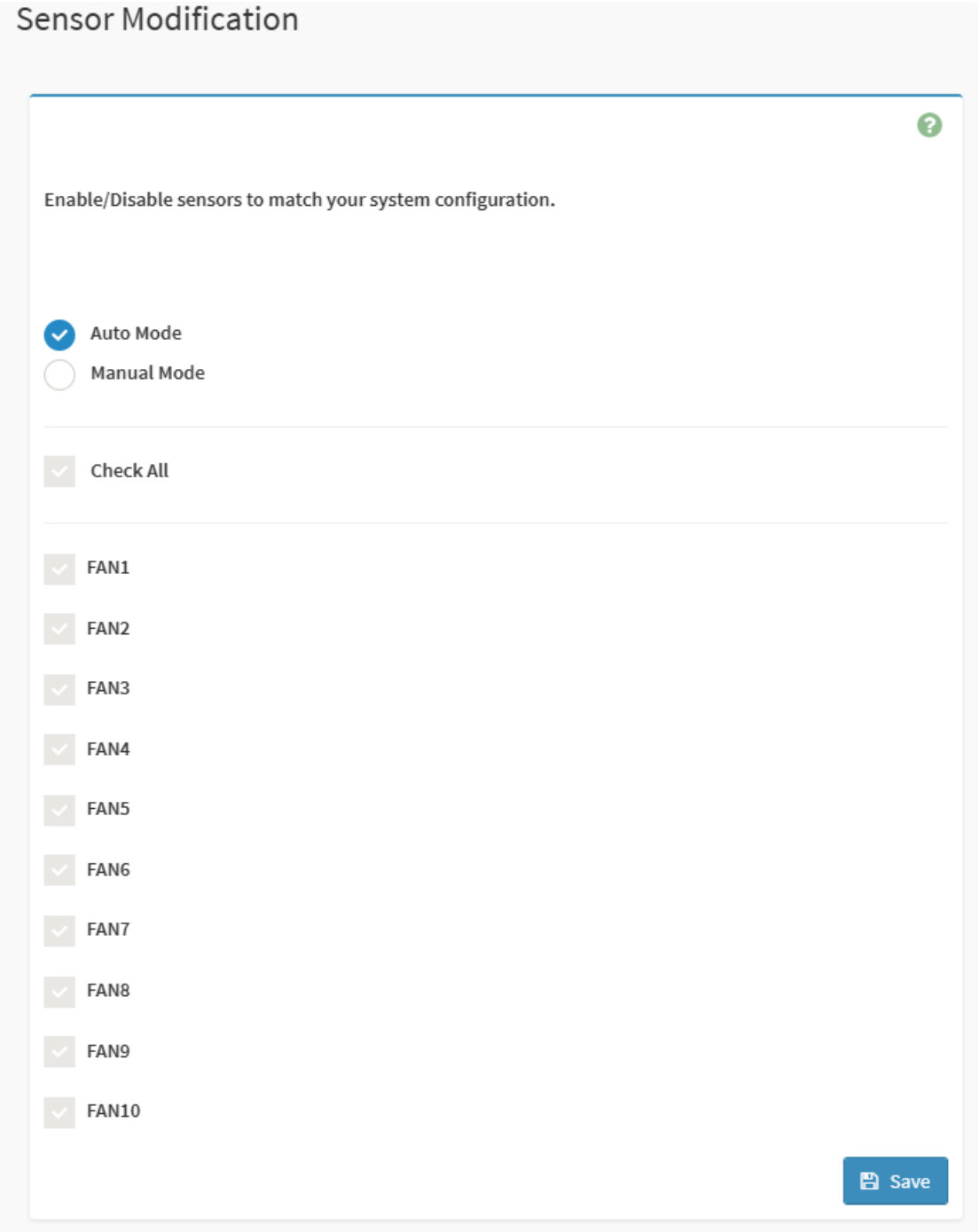
- **Read-only Community String**: This field specifies the community string used for read-only access to SNMP-enabled devices. Devices configured with this community string can retrieve SNMP data, but cannot modify any settings.
- **Read-write Community String**: This field specifies the community string used for read-write access to SNMP-enabled devices. Devices configured with this community string have the privilege to both retrieve SNMP data and modify device settings.
- **Save**: To save the changes made.

NOTE

1. SNMP community string is only used in **SNMP v1/v2c**.
2. Only accounts with "Administrator" privilege level can modify it.

11.20 Sensor Modification

This page is used to enable and disable sensor. To open Sensor Modification page, click **Settings** → **Sensor Modification**. A sample screenshot of **Sensor Modification** page is displayed below.



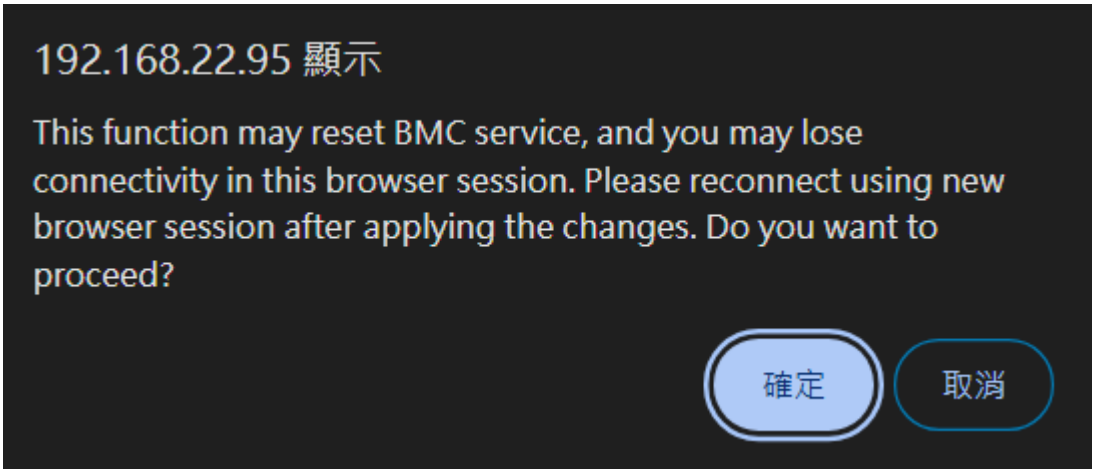
The fields of Sensor Modification Setting page are explained below.

- **Auto Mode**: This mode will enable all sensors.
- **Manual Mode**: This mode can enable/disable sensor manually.
- **Check All**: When in Manual Mode, checking this will select all selectable sensors.

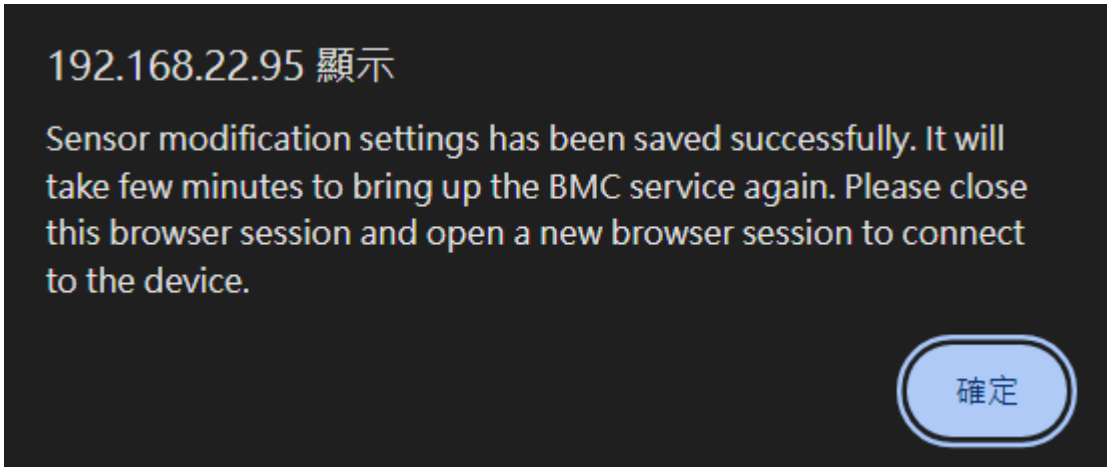
In **Manual Mode** there are settable fields like FAN1 to FAN10.

Procedure

1. Choose either of the following as your requirement:
   - Choose Auto Mode to enable all sensors.
   - Choose Manual Mode to enable selected sensors.
2. Click Save Button to save the changes made.
3. Confirm Button to apply the setting as below.



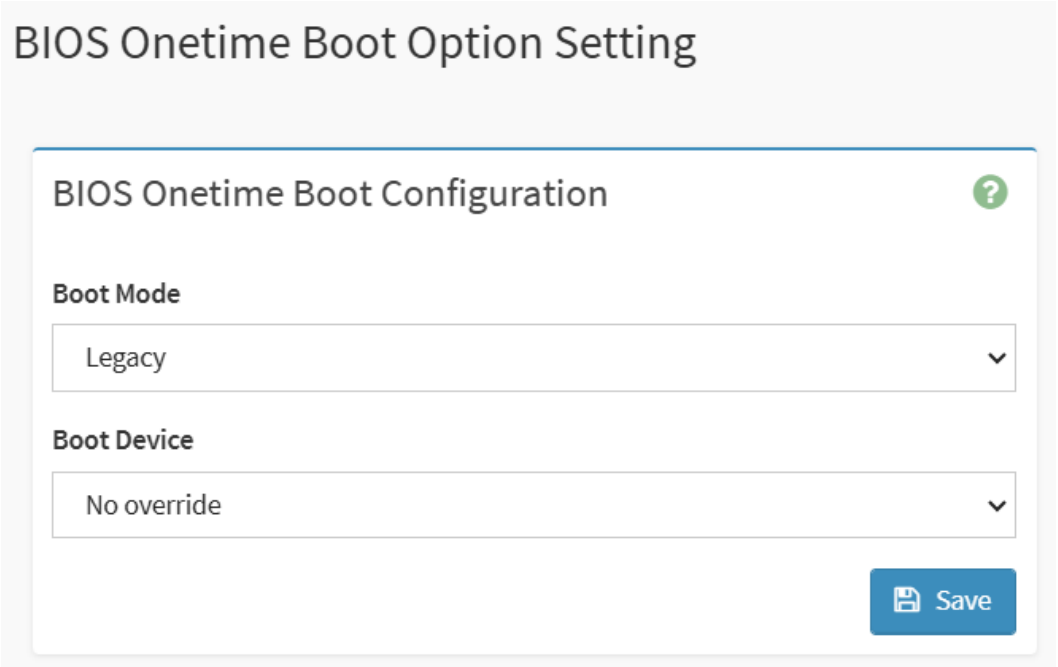
4. If saved successfully, below message will show.



5. Wait BMC reset to apply the setting.

11.21 BIOS Onetime Boot

This page is used to configure the BIOS onetime boot. To open BIOS Onetime Boot Option Setting page, click **Settings** →**BIOS Onetime Boot Opetion Setting**. A sample screenshot of **BIOS Onetime Boot Option Setting** page is displayed below.



- **Boot Mode**: This setting determines the boot mode for the next startup. You can select either Legacy or UEFI mode.
  - **Legacy**: This mode allows the system to boot using traditional BIOS methods, which may be necessary for older operating systems or hardware.
  - **UEFI**: Use the modern UEFI boot mode to support more modern hardware features and security.

- **Boot Device**: This setting specifies the device from which the system will boot for the next startup. The available options are as follows:
  - **No override**: The system will boot according to the default boot priority settings, without overriding the usual order.
  - **PXE**: The system will perform a network boot using PXE (Preboot Execution Environment), allowing it to load an operating system from a remote server.
  - **Hard drive**: The system will boot directly from the primary hard drive, where the operating system is installed.
  - **Hard drive(Safe mode)**: The system will boot from the hard drive but in Safe Mode, which is useful for troubleshooting and repairing issues.
  - **CD/DVD**: The system will boot from a CD or DVD inserted in the optical drive.

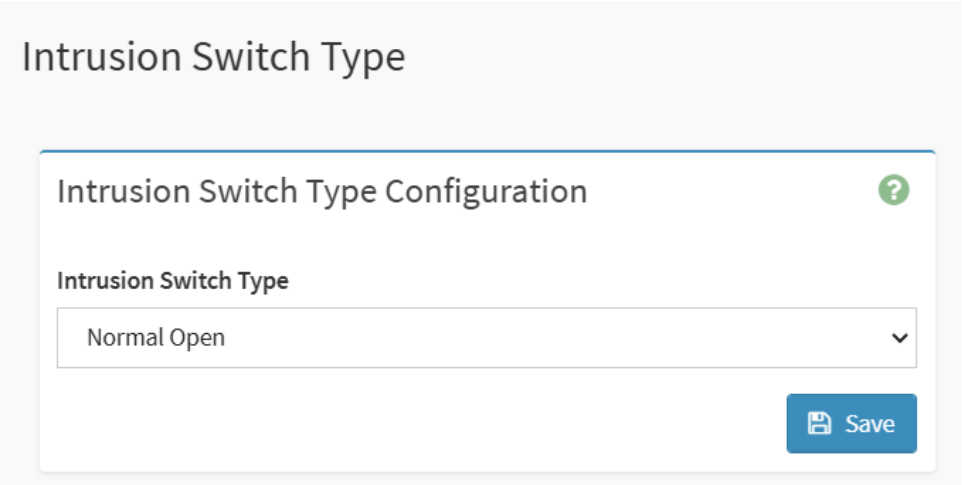
- **BIOS Setup**: The system will enter the BIOS setup interface, allowing you to configure BIOS settings.
- **Floppy/Primary removable media**: The system will attempt to boot from a floppy disk or other primary removable storage media.

Procedure

1. Choose **Boot Mode** to determine which mode will be used for next boot up..
2. Choose **Boot Device** to determine which device will be used for next boot up..
3. Click **Save** to save and apply the current setting.

11.22 Intrusion Switch Type

This page is used to configure the Intrusion Swtich Type. To open Intrusion Switch Type page, click **Settings** →**Intrusion Switch Type**. A sample screenshot of **Intrusion Switch Type** page is displayed below.



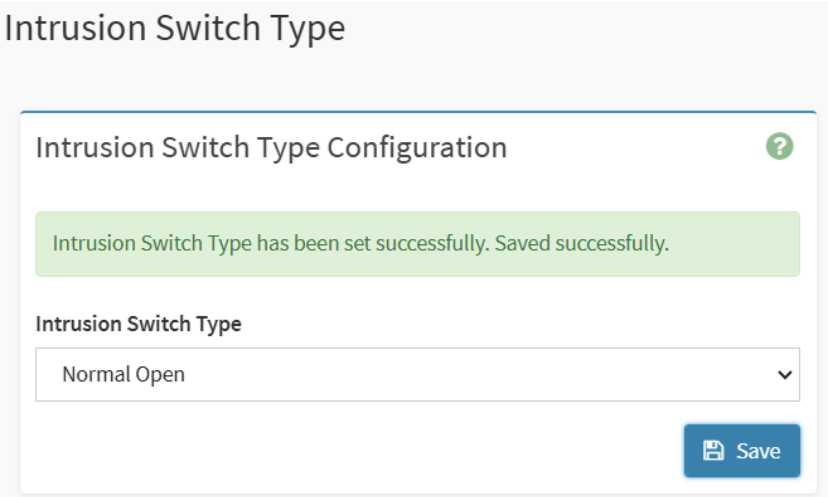
This setting need to correspond with the type of chassis intrusion switch connected to your system and must comply with the SSI standard.

The default value is set to "Normal Open".

- **Normal Open**: Select this option if your chassis intrusion switch is configured as a Normal Open switch.
- **Normal Close**: Select this option if your chassis intrusion switch is configured as a Normal Close switch.

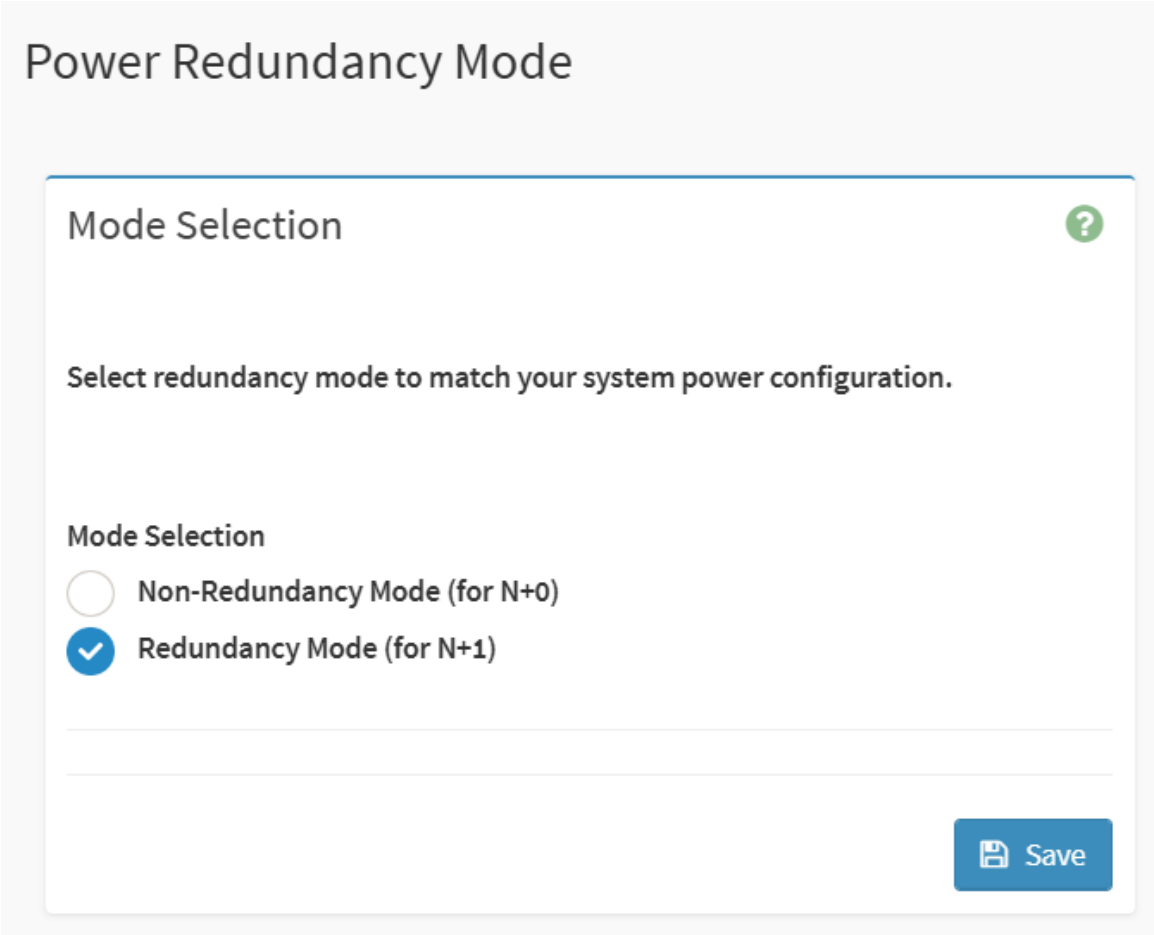
Procedure

1. The default setting for the intrusion switch type is **Normal Open**.
2. Choose **Intrusion Switch Type** to determine the chassis intrusion switch sensor type
3. Click **Save** to save and apply the current setting.



11.23 Power Redundancy Mode

This page is used to configure the system Power Redunancy Mode. To open Power Redundancy Mode page, click **Settings** →**Power Redundancy Mode**. A sample screenshot of **Power Redundancy Mode** page is displayed below.



The field of Power Redunancy Mode Setting page is explained below.

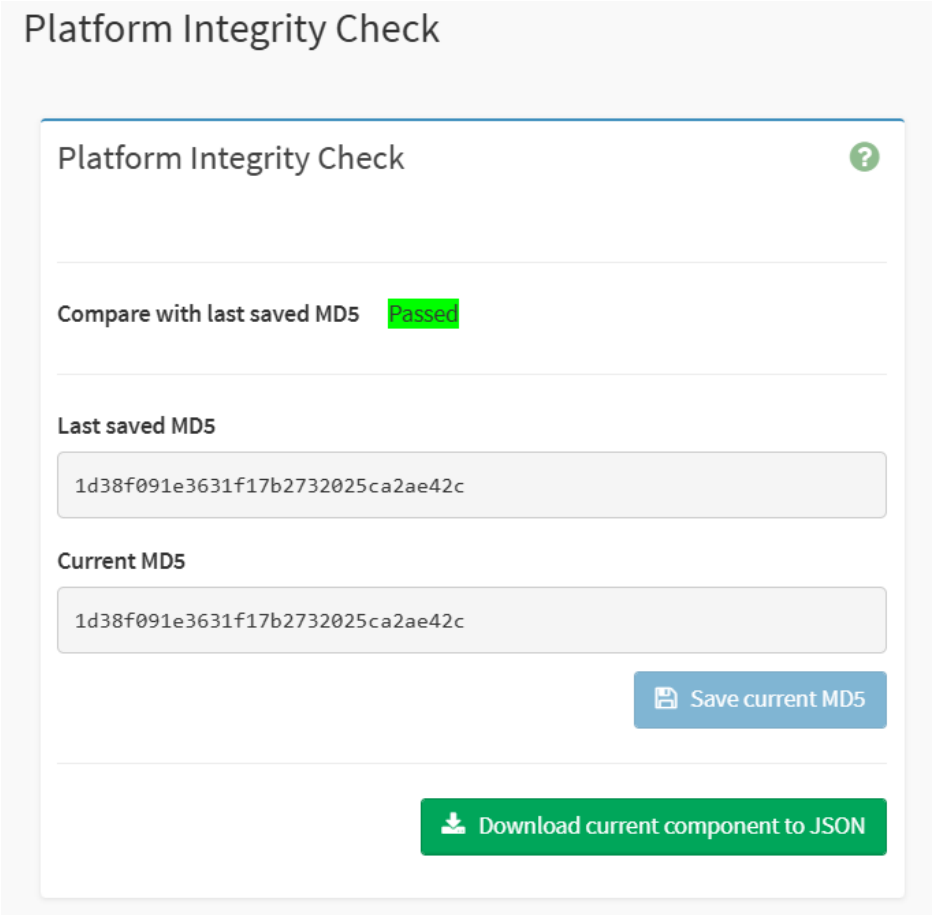
- **Redundancy Mode:** N+1 power redundancy mode ensures continuous server operation by adding one extra power supply module as a backup, allowing the system to remain functional even if one module fails.
- **Non-Redundancy Mode:** N+0 non-redundancy mode uses only the required number of power supplies without backups, meaning the system will fail if any module fails.

Procedure

1. Click the **Mode Selection** option to enable **Non-Redundancy Mode** or **Redundancy Mode.**
2. Click **Save** to save and apply the current setting.

11.24 Platform Integrity Check

This page is used to check if system device has changed. Platform Integrity calculation include components like CPU, memory, PCIe devices and storage. To open Platform Integrity Check page, click **Settings** →**Platform Integrity**. A sample screenshot of Platform Integrity Check page is displayed below.



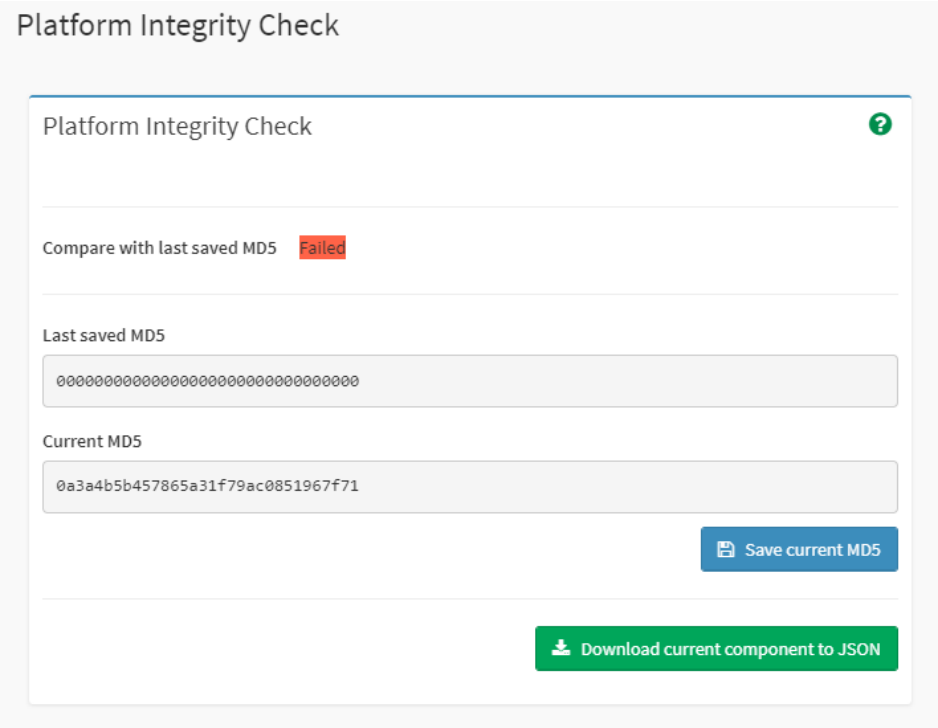
It will capture the internal information of the CPU, DIMM, storage, and PCIe devices to calculate the MD5. This is to ensure that the CPU, DIMM, storage, and PCIe devices have not changed after shipment.

The fields of Platform Integrity Check page are explained below.

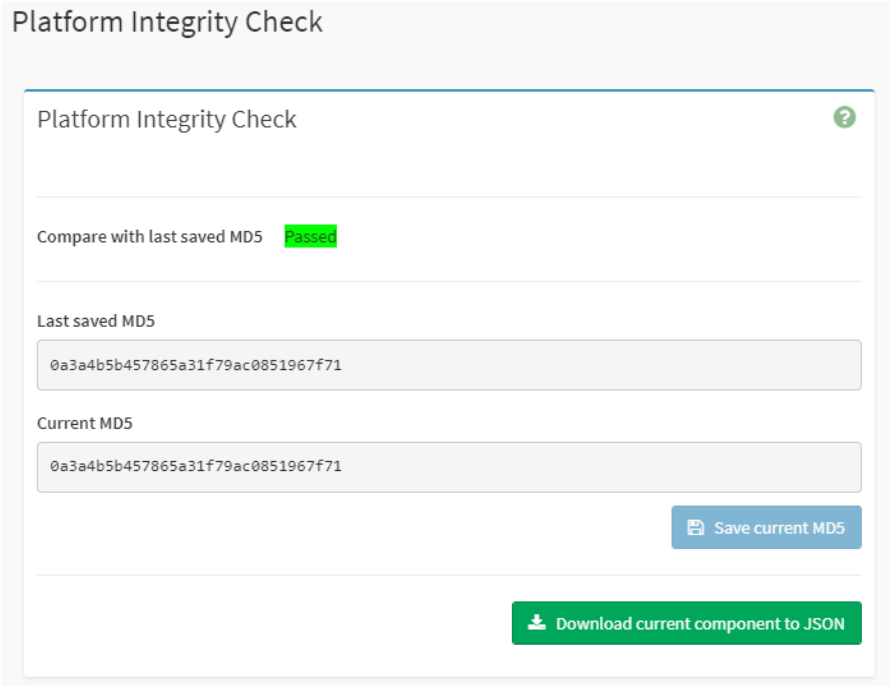
- **Compare with last saved MD5**: This will show the result of comparing **Last saved MD5** and **Current MD5**, if two are the same it shows Passed, if not it shows Failed.
- **Last saved MD5**: This shows the MD5 that saved last.
- **Current MD5**: This shows the current MD5.
- **Save current MD5**: This will replace the last saved MD5 with the currnet MD5.
- **Download current component to JSON**: This will download the current Platform Integrity component in the file type of JSON.

Procedure

1. First time BMC boot up, the Last save MD5 will be initialized to value of all zero, the compare result will be **Failed**.



2. Click **Save current MD5** to update the **Last Saved MD5**
3. Refresh and check Last saved MD5 updated and compare result.

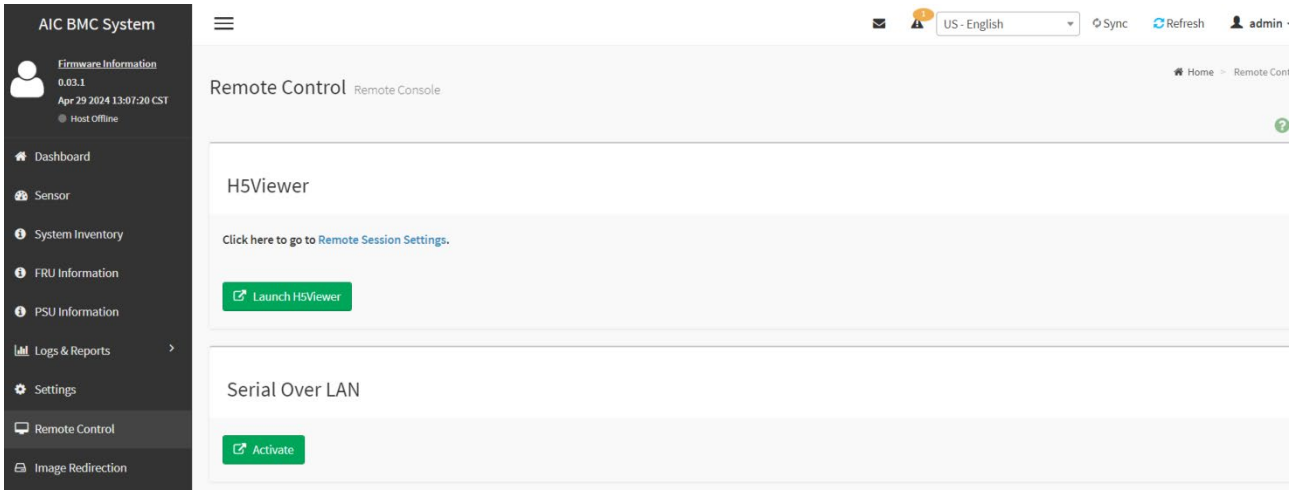


4. Click **Download current component to JSON** to check curreny platform integrity components.

Chapter 12. Remote Control

Click **Remote Control** from the menu bar. A sample screenshot is displayed below.

- Launch H5Viewer
- Serial Over LAN



Remote Control page

12.1 Launch H5Viewer

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

System Requirements

1. Client machine with 8GB RAM.
2. If the client machine has 4GB RAM or lower, there will be lag in Video/Keyboard/ Mouse/Media redirection functionality.

Supported Browsers

- Chrome latest version
- Firefox (with limited support)
- Microsoft Chromium-based Edge
- Safari (On Mac only)

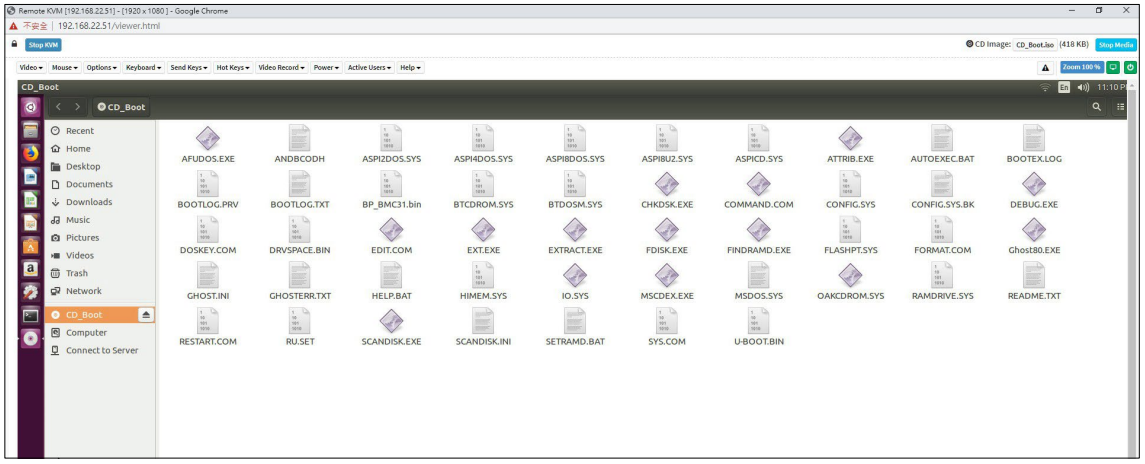
NOTE

- It is advisable to use Chrome for H5Viewer, since Firefox has its own memory limitations.
- When there is continuous full frame update in host video over a long period of time, it may result in browser OOM situation. This behavior is observed in all SPX supported web browsers.
- In Microsoft Windows operating systems, IPv4 addresses are valid location identifiers in Uniform Naming Convention (UNC) path names. However, the colon ':' is an illegal character in a UNC path name. Thus, the use of IPv6 addresses is also illegal in UNC names.
- For this reason, in IE browser the IPV6 address should be given in "Literal IPv6 addresses in UNC path names" format.
- Stopping an active KVM/Media session during host reboot will impact host boot time and host inventory feature of redfish (if redfish support is present in BMC). So suggests to avoid this action.

Example:
For web, 2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net:85
Where IP is 2001:db8:85a3:8d3:1319:8a2e:370:7348 and port is 85.

To open **Remote Control** page, click **Remote Control** from the menu bar. A detailed description of the menu items are given below.

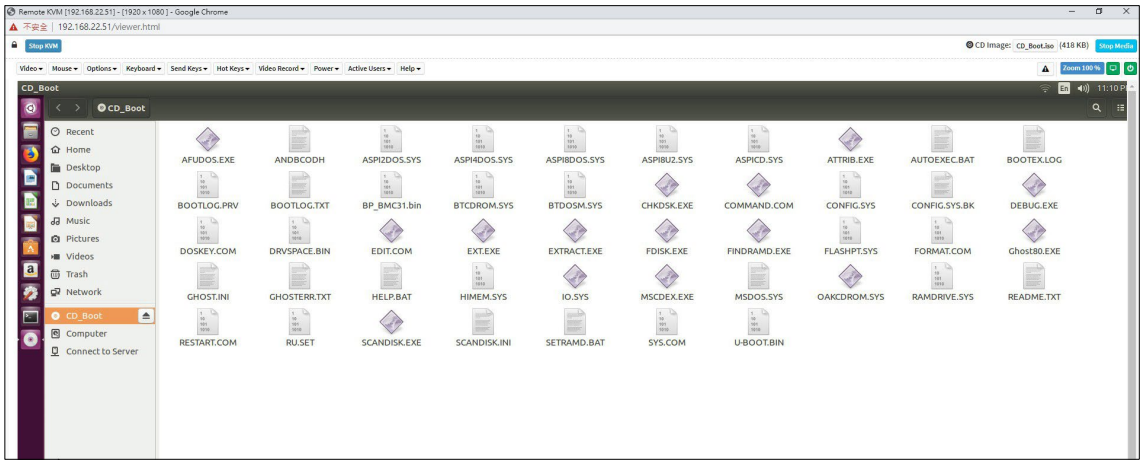
Open the Remote Control page, click **Launch H5Viewer**. A sample screenshot of the Remote KVM page is shown below.



Remote KVM

Procedure To Start KVM

1. Click **Launch H5Viewer** to open the Remote Control KVM page. A sample screenshot of the Remote KVM page is shown below.



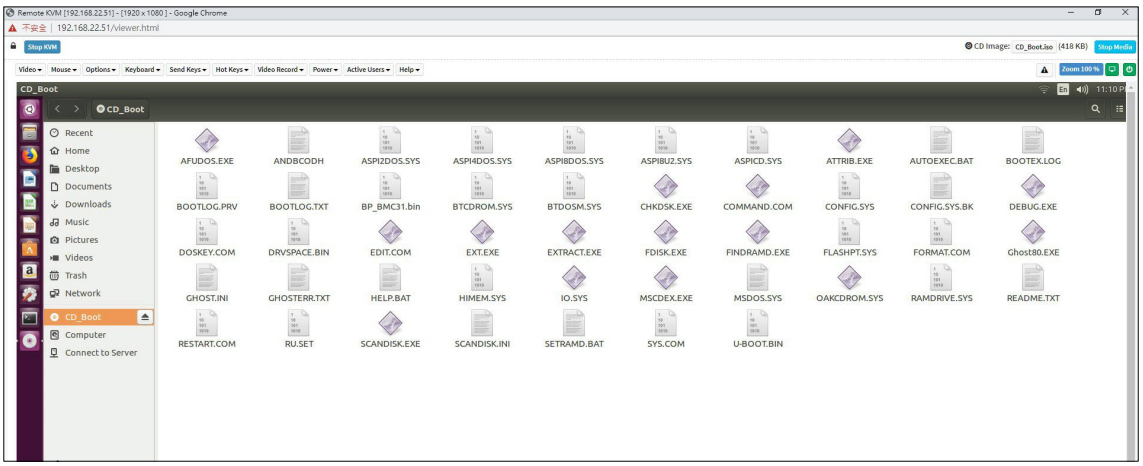
2. To stop the H5Viewer video redirection, click **Stop KVM**.

Procedure To Start / Stop Media

1. Click **Browse** to select CD/HD Image. After selecting the image, **Select/Unselect** media boost option for CD/DVD.
2. Click **Start Media** to redirect the selected CD/HD image file to the Host. A sample screenshot is as shown below.

NOTE

- If media boost mode is selected, the processes related to media redirection will have high priority than other processes. This will improve media performance but other processes will have limited access to CPU cycle. Media boost mode is only applicable for CD/DVD.
- If CD/DVD instance is started with media boost mode, the next CD/DVD instance will be started without any pop-up message.



3. To stop the CD/HD Image redirection, click **Stop Media**.

A detailed description of the menu items are given below.

Video

This menu contains the following sub menu items.

Pause Video: This option is used for pausing Console Redirection.

Resume Video: This option is used to resume the Console Redirection when the session is paused.

Refresh Video: This option can be used to update the display shown in the Console Redirection window.

Capture Screen: This option helps to take the screenshot of the host screen and save it in the client's system.

Mouse

Show Client Cursor: This menu item can be used to show or hide the local mouse cursor on the remote client system.

Mouse Mode: This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure

this option.

- **Absolute mouse mode**: The absolute position of the local mouse is sent to the server if this option is selected.
- **Other mouse mode**: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

> **NOTE**
> Suggest users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode.

Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

Options

Zoom:

Normal - By default this option is selected.

Zoom In - For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%

Zoom Out - For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%

Block Privilege Request: To enable or disable the access privilege of the user.

***Compression Mode**: This option helps to compress the Video data transfer to the specific mode.

***DTC Quantization Table**: This option helps to choose the video quality.

> **NOTE**
> *Specific to AST SOC.

Keyboard

Keyboard Layout: This feature is fully compatible when host and client have the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.

List of Host Physical Keyboard languages supported in H5Viewer:

1. English U.S.
2. English U.K.
3. German.
4. Japanese.

NOTE

- Some keys like Windows, Print Screen have OS precedence and due to this H5Viewer might not be able to capture those OS precedence key and send it to host.
- In some cases, after press OS precedence (Windows, Print Screen) keys press H5Viewer keyboard may not work as expected. This is due to browser focus loss. Since browser doesn't have control key press/release will not be done properly.
- It is highly recommended to use Windows key option from Send Keys or using Hot keys options.

Soft Keyboard: This option allows you to select the keyboard layout. It will show the dialog as similar to Windows On-screen keyboard. If the client and host languages are different, you can select the soft keyboard that corresponds to the host keyboard layout from the list shown in H5Viewer, and use it to avoid typo errors.

NOTE

- Different Linux systems follow different keyboard layouts. So the softkeyboard displayed uses standard windows keyboard layout irrespective of the host OS.
- Dragging soft keyboard window within video canvas bounds may cause lag in window movement. This behaviour is caused due to H5Viewer HID event listener.

We have list of List of Soft Physical Keyboard languages supported in H5Viewer:

1. English US
2. English UK
3. Spanish
4. French
5. German
6. Italian
7. Korean
8. Chinese Simplifified
9. Chinese Traditional

NOTE

Soft keyboard is applicable only for H5Viewer Application not for other application in the client system.

Send Keys

This option is used to key items. This menu contains the following sub menu items.

- Hold Down
- Press and Release

Hold Down

This menu contains the following sub menu items.

Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.

Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Press and Release

Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Context Menu Key: This menu item can be used to act as the context menu key, when in Console Redirection.

Print Screen Key: This menu item can be used to act as the print screen key, when in Console Redirection.

Hot Keys: This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.

This menu contains the following sub menu items.

- **Add Hot Keys** - This menu is used to enable macros. Click **Add** to macros.

Video Record

This menu contains the following sub menu items

Record Video: This option is to start recording the screen.

Stop Recording: This option is used to stop the recording.

Record Settings: This option is used to set video record duration and video compression value. Video record duration value should be in the range of 1 to 1800 seconds. Video Compression value should be in the range of 0.1 (Low image quality) to 0.9. (High image quality). In H5Viewer video recording, the recorded video duration will not be same as the configured duration. The recorded duration will be close to the configured duration.

Normalized video resolution to 1024 X 768 (*Specific to AST SOC): Host video will be scaled to 1024 x 768 in the recorded video file. Enabling this option improves client side video recording performance in H5Viewer.

Disable this option to record video at same resolution as host video. The host video capture depends on client system performance. If this option is disabled, recorded video file may have inconsistency. (i.e., Recorded video file duration may not be the same as configured value).

NOTE
The Maximum video file size allowed is around 40MB. If the video file size reaches its max size limit, the recorded file is downloaded and recording will be in progress until the configured video recording time is reached. The video file is saved as video_date-month-year_hr-min-sec_partno in client side video recording.

Users have to take care of saving the video files in different browsers.

When H5Viewer focus is lost and if video recording is in progress, the recording will be stopped with a notification message and the recorded video file will be discarded.

Due to browser limitation, Set timeout/set interval will be delayed from specified time of interval when browser window loses focus, Hence video server will not send the video packets to H5View¬er and so the video recording will be stopped.

Power

The power options are to perform any power cycle operation. Click on the required option to perform the following operation.

Reset Server: To reboot the system without powering off (warm boot).

Immediate Shutdown: To perform Power OFF Immediately.

Orderly Shutdown: To Power OFF the server in proper order.

Power ON Server: To Power ON the server.

Power Cycle Serve: To first power off, and then reboot the system (cold boot).

Active Users

Click this option to display the active users and their system ip address.

Active KVM Session can be terminated when there are multiple KVM Session From Master [FULL Privilege KVM Session].

Help

Click this option to get more information About H5Viewer. The KVM Remote Console utility version and plugin version will be displayed.

Quick Buttons

Quick Buttons: The upper right of H5Viewer window displays all the quick buttons. These quick buttons allow you to perform the below functions by clicking them.

Quick Buttons	Explanation
	This quick button will show/hide notifications dropdown menu, which will contains the list of notifications displayed by H5Viewer.
	It shows the current zoom value in percentage.
	This quick button is used to display the current host monitor status. If icon is in green color then host monitor is unlocked. If the icon is in red color host monitor is locked. By clicking the button host monitor status can be toggled.
	This quick button is used to display the current server power status. If the icon is in green color, the server status is powered on. If the icon is in red color, the server status is powered off. Click the button to toggle immediate power off / power on the host.

Status bar buttons

Num/Caps/Scroll lock buttons are LED status buttons that denotes the current status of Num/Caps/Scroll lock in the host.

Keyboard LED Sync

When the H5Viewer is launched, the keyboard locks status and LEDs denoting the lock status of the host machine, should be in sync with the client machine. That is, if the **Num/Caps/Scroll lock** is enabled/disabled in the client machine, the same should be updated in the host machine as well.

NOTE

Client Side Limitations

Due to web browser related security concerns, this feature has following limitations.

- Host LED status will be synced with client LED status, only if user presses any key in client keyboard when H5Viewer window is in focus.
- Client keyboard LED status cannot be updated from web browsers.
- The LED Caps lock status shown in H5Viewer indicates the Caps lock status of the host.
- However, if the Caps lock status is changed before launching H5Viewer, the LED status for Caps lock in H5viewer will not synchronize with the physical keyboard Caps lock status of the client.

Host Side Limitations

- In some Linux hosts, when the host is booted into text mode, CAPS LOCK LED status will not be updated properly. This limitation is caused by the OS, as the CAPS LOCK LED won't turn ON/OFF while changing the CAPS lock status in the host OS.
- In such cases, H5Viewer CAPS LOCK LED synchronization functionality will not work properly.

Control keys

This option provides the same functionality of **Send Keys → Hold Down** menu item. Select any of the menu item, it will highlight the corresponding status bar button in green color. Similarly by clicking the buttons will toggle the selection status of the corresponding menu item.

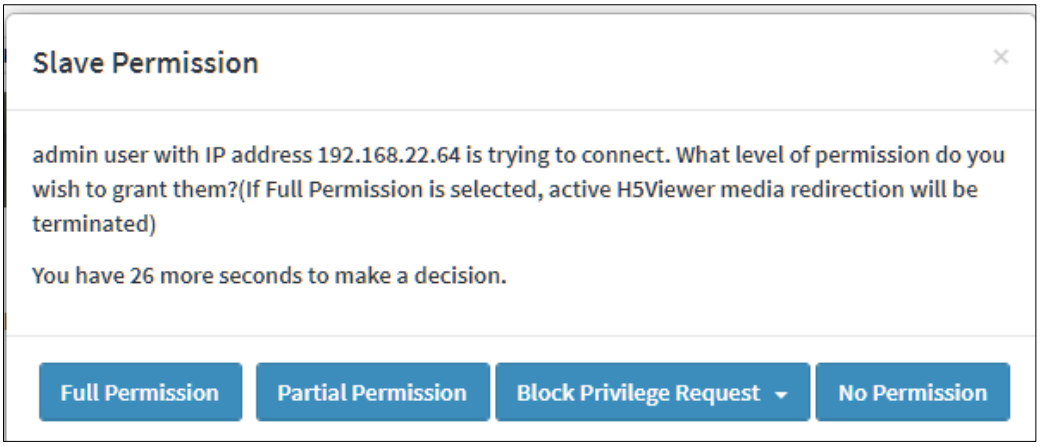
KVM Sharing

Support "N" number of KVM Redirection sessions. Only one full permission H5Viewer session at a time.

With Full permission in H5Viewer, the user can control the KVM redirection, and the other H5Viewer users can only view the video redirected from the server without intervention.

When the First user launches H5Viewer, the user will get full permission to control the host during KVM redirection. When another H5Viewer session is launched, the Video server will send KVM sharing permission request packet to the current session, for the new Requesting session.

Once the requesting session is authenticated, a packet containing the information such as the client IP/hostname and user name of the newly authenticated or logged in user, will be send to the current session. The first client shows the dialog as a shown below:



Clicking the button in the dialog box will trigger specified action:

Full Permission: When this button is clicked, the requesting session will receive full access permission, and the current (full permission) session will have a partial KVM access permission only.

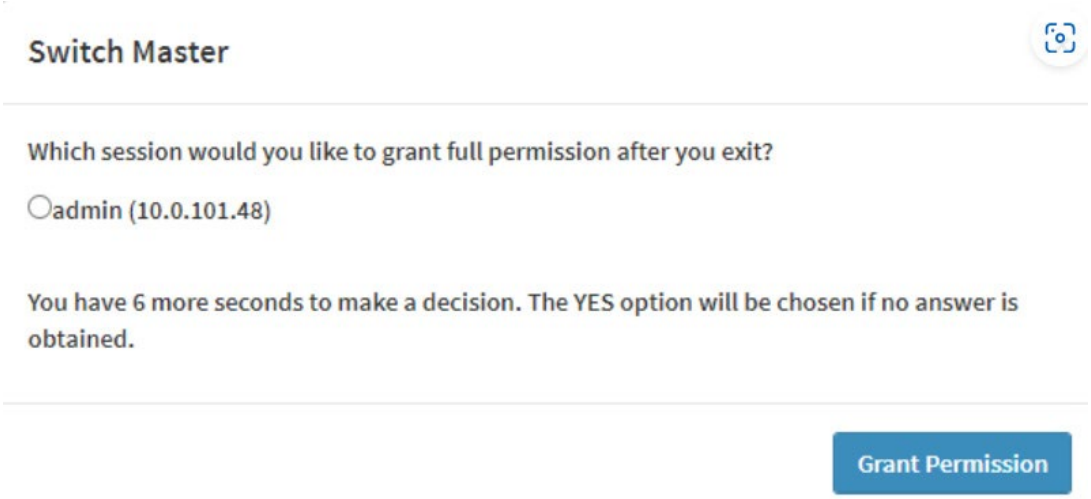
Partial Permission: When this button is clicked, the requesting session will receive partial permission and can only view server display (Video only).

Block Privilege Request → Partial Permission: Once this option is selected, both newly requesting session and active partial privileged session will get partial permission as auto response and can only view server display. Further request will be served by auto response mechanism.

Block Privilege Request → No Permission: Once this option is selected, both newly requesting session and active partial privileged session access will be denied as auto response. Further request will be served by auto response mechanism.

No Permission: When this button is clicked, the requesting session access will be denied.

If full privilege session is closed using stop KVM button and there is more than one active partial privilege session, then the user will be prompted to transfer the current privilege to any of the active sessions. Selected session will be notified about change in KVM permission.



NOTE

Note: Due to web browser limitation, this prompt will not be displayed when full privilege session is closed using “X” button in KVM window. In this case, partial privilege session needs to manually request for full permission.

Quick Buttons

The lower right of Console Redirection windows displays all the quick buttons. These quick buttons helps you to perform these functions by just clicking them.

NOTE

This option is available only when you launch the Java Console.

Quick Buttons	Explanation
	This key is used to play the Console redirection after being paused.
	This key can be used for pausing Console Redirection.
	This button is used to view the Console Redirection in full screen mode. **NOTE** Set your client system resolution same to host system resolution so that you can view the server in full screen.
	This quick button is used to show or hide the soft keyboard.
	Drag this to zoom in or out.
	This quick button is used to record the video.
	This quick button is used to show or hide the mouse cursor on the remote client system.
	Active Users
	This quick button will work like toggle button if icon is in green color server status is **power on** by clicking the button **immediate shutdown** action will be triggered in host If the icon is in red color server status is **power off**. Click the button to **power on** the host.
	This quick button displays the available hotkeys.

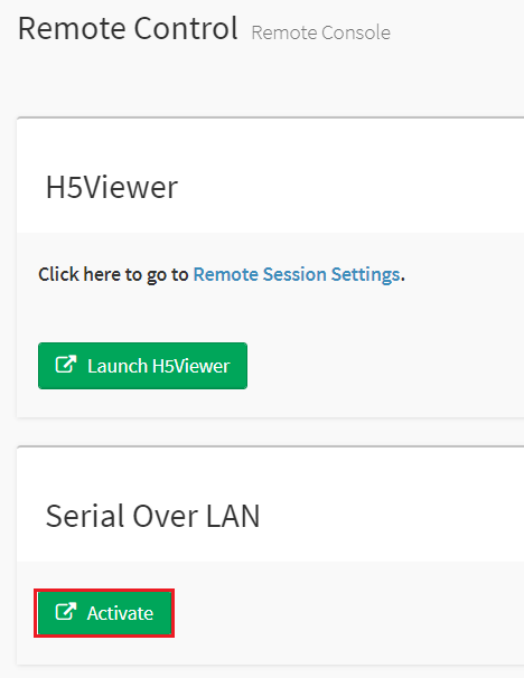
	These three quick buttons will pop up a virtual media where you can configure the media.

12.2 Serial Over LAN

Serial Over LAN (SOL) is a mechanism that enables the input and output of the serial port for a managed system to be redirected over IP; In this feature, Serial data is transmitted to HTML5 Web UI through websocket.

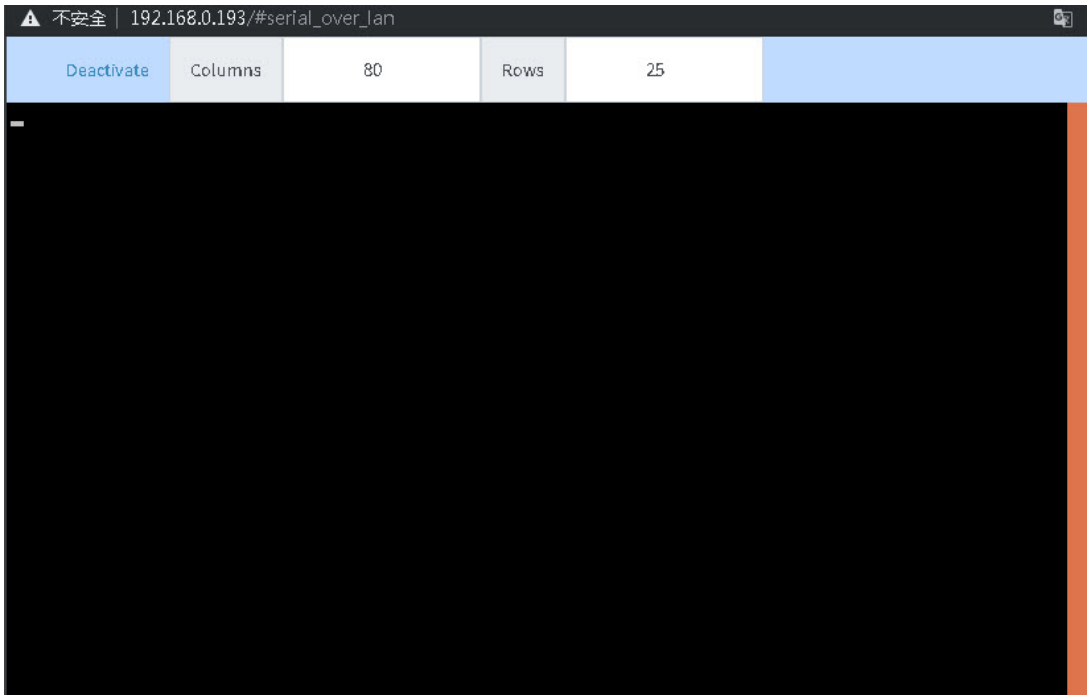
To activate SOL Support, follow the below procedures.

1. Click **Remote Control** from the menu bar. A sample screenshot of **Remote Control** page is shown as below.



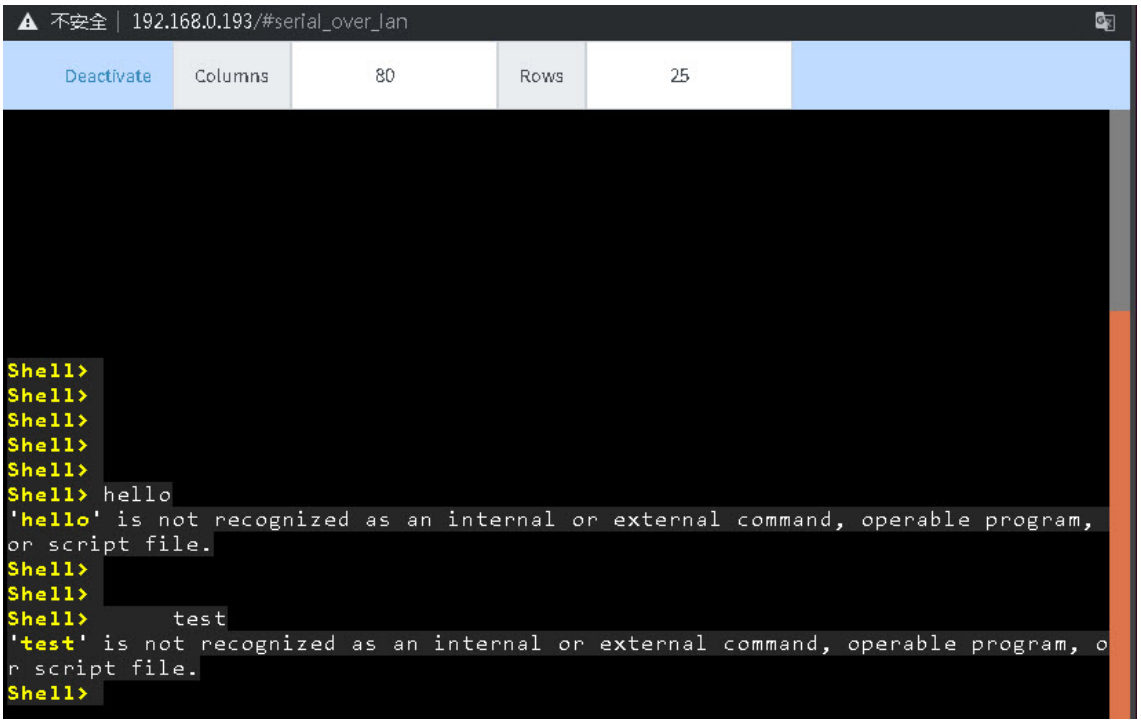
Remote Control - Serial Over LAN

2. Click **Activate** to activate SOL. The default text console size for SOL is 80x25. Columns and Rows cannot be edited and these values will change automatically based on resizing the popup window. A sample screenshot is displayed below.



Remote Control - Serial Over LAN

3. Press Enter. Enter your Login name, and again press Enter.
4. Enter your Password, and press Enter. SOL will be activated. A sample screenshot is as shown below.



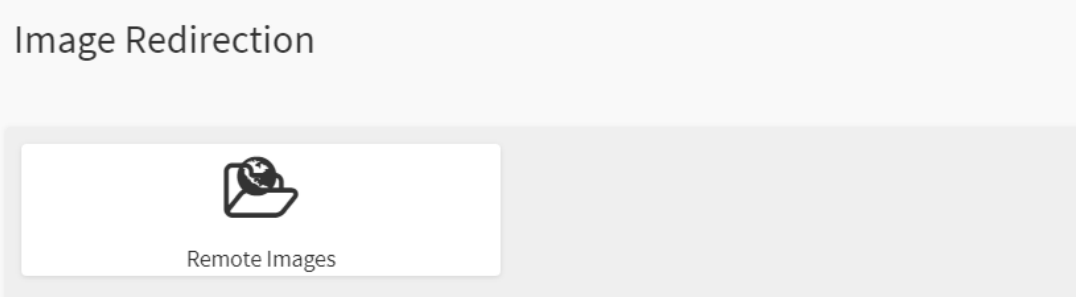
5. Click Deactivate to deactivate SOL.

Chapter 13. Images Redirection

This page is used to configure the images into BMC for redirection. This can be done either by uploading an image into BMC say, **Local Media** or by mounting the image from the remote system, **Remote Media**.

To open Images Redirection page, click **Images Redirection** from the menu bar.

A sample screenshot of Images Redirection page is shown below.



The fields of Images Redirection page are explained below.

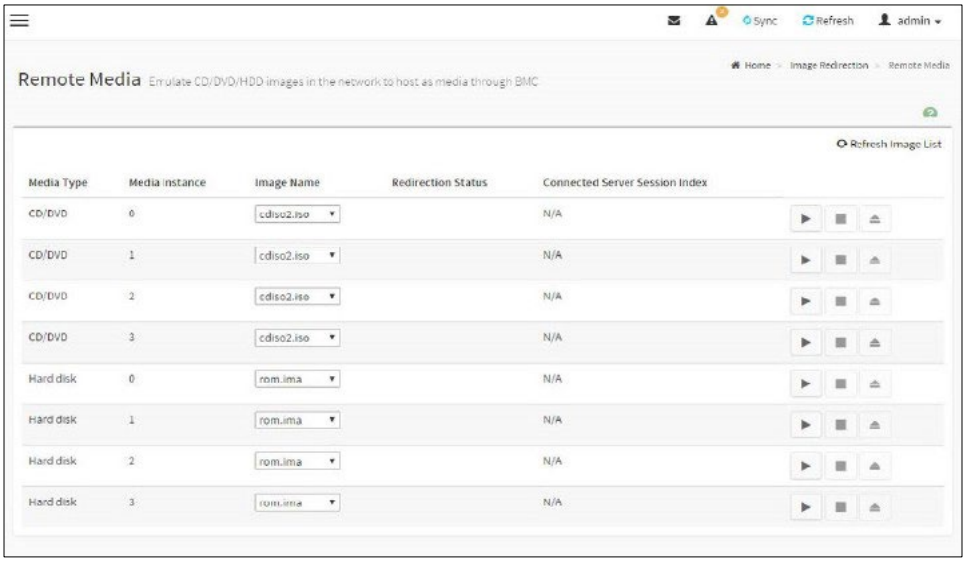
- Remote Images

> **NOTE**
> Media will always be redirected using the lowest available instance number, regardless of the instance slot opted in Web UI. This is applicable for both local and remote media images.

13.1 Remote Images

The displayed table shows configured images on BMC. You can configure images of the remote media server.

Click Media General Settings or Remote Media for navigating to the appropriate page.



> **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:

Multiple Image support in Image Redirection

Media Type: Displays type of Media such as CD/DVD.

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.

Refresh Image List: To get latest Image lists from the Remote Storage.

Sync Image Status: Click **Sync Image Status** to turn on/off the redirection status of images from the BMC.

Procedure

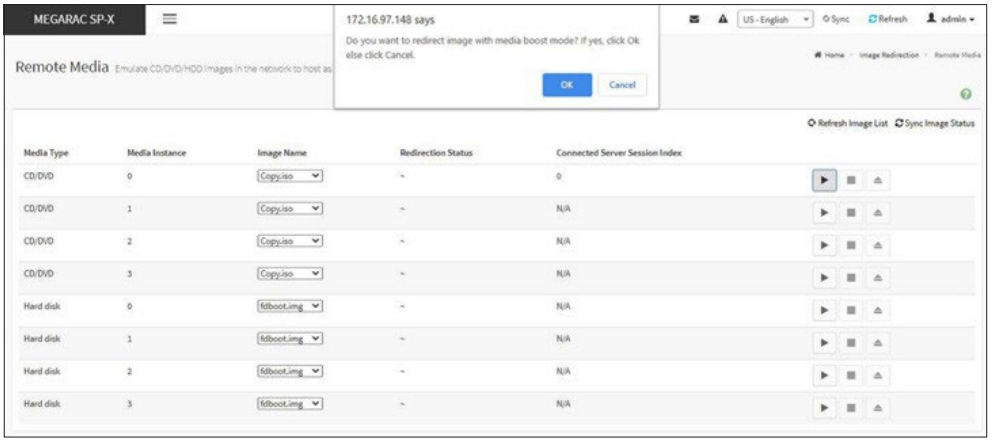
1. To **Start/Stop Redirection** and configure Remote media images, click (Start/Stop icon) and make sure **Remote Media Support** option is enabled.

2. Select a configured slot and click (**Start**/**Stop** icon) to start the Remote media redirection. It is a toggle button, if the image is successfully redirected, then click (**Start**/**Stop** icon) to stop the Remote media redirection. If you want to pause the Remote media Redirection, click (**Pause** icon).

> **NOTE**
> Redirection needs to be stopped to clear the image.
> Following special characters not allowed for image name
> {}()<>&*`|=?;[]$-#~!\"%/\\:+,'

3. **CD Redirection with Media Boost Mode:** To perform CD Redirection with Media Boost Mode.
   - Select CD media configured slot and click **Start** icon to start the remote media redirection.
   - This action prompts you with the message and click **OK** to redirect image with the media boost mode. Or else, click **Cancel** to stop this action. A sample screenshot is displayed below.

> **NOTE**
> If media boost mode is selected, the processes related to media redirection will have high priority than other processes. This will improve media performance but other processes will have limited access to CPU cycle.
> If CD/DVD instance is started with media boost mode, the next CD/DVD instance will be started without any pop-up message.



Media Boost Mode

4. To clear an image status, select an image and click (**Clear** icon) to clear image status from the device.

5. Click **Refresh Image** list to get latest Image lists from the Remote Storage. The Latest Image Names list will be displayed in the Image Name drop-down list.

Single Image support in Image Redirection

> **NOTE**
> Only Single image can be configured for each image type.
> 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 "~"

The fields of Remote Media tab are as follows:

Media Type: Displays type of Media such as CD/DVD and Harddisk.

Image Name: Enter the default recovery image name on the server.

Redirection Status: Displays the status of the media.

Start/Stop Redirection: To start or stop Media redirection.

Pause: To Pause the Media redirection.

Procedure

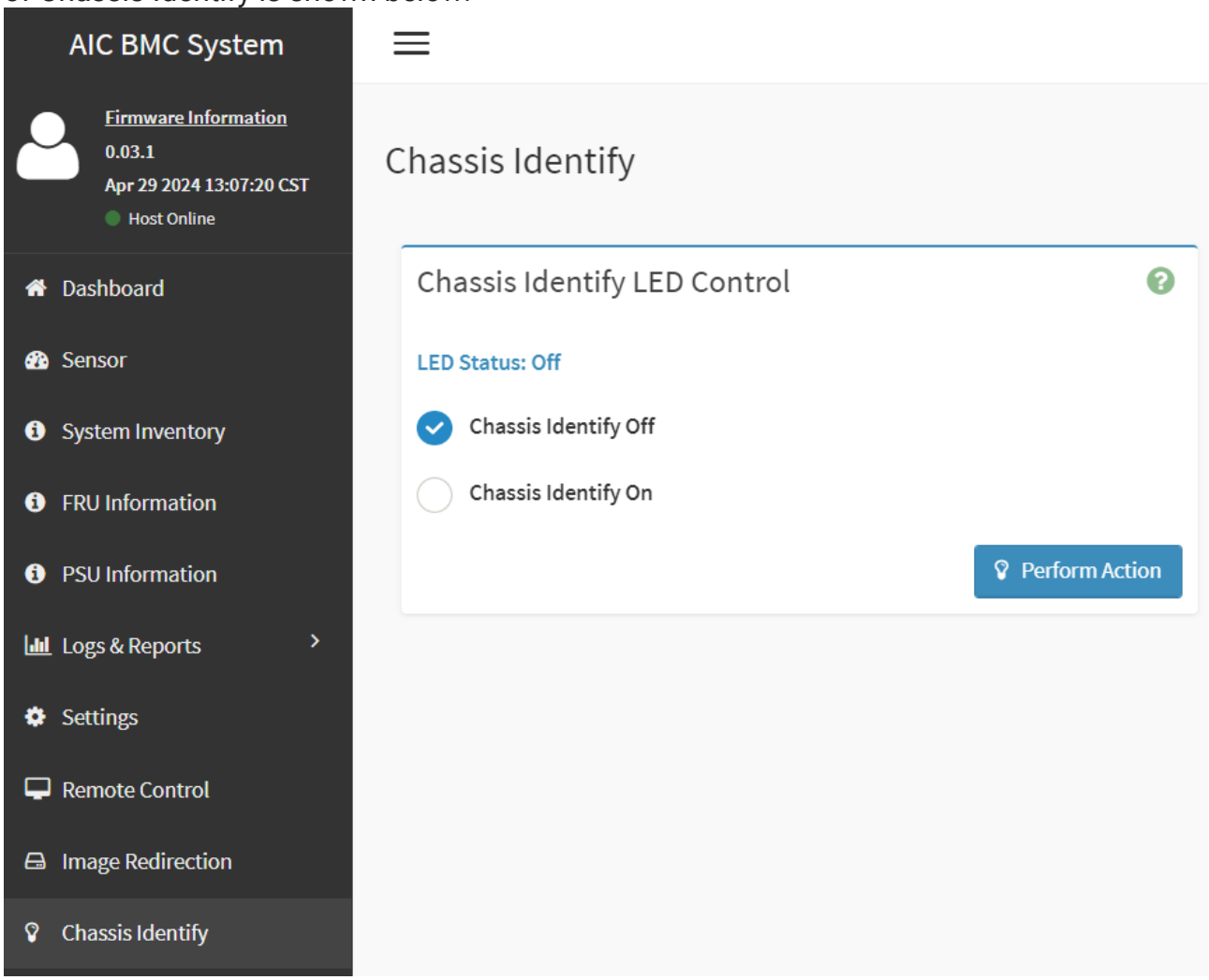
1. To **Start/Stop Redirection** and configure Remote media images, click ▶ (Start/Stop icon) and make sure **Remote Media Support** option is enabled.
2. Select a configured slot, and enter the default recovery image name on the server in the **Image Name** text field.
3. Click ▶ (**Start/Stop** icon) to start the Remote media redirection. It is a toggle button, if the image is successfully redirected, then click ▶ (**Start**/**Stop** icon) to stop the Remote media redirection. If you want to pause the Remote media Redirection, click ■ (**Pause** icon)

> **NOTE**
> Redirection needs to be stopped to clear the image.
> Following special characters not allowed for image name
> {}()<>&*`|=?;[]$-#~!\"%/\\:+,'

4. To clear an image status, select an image and click (⏏) (**Clear** icon) to clear image status from the device.

Chapter 14. Chassis Identify

To open Chassis Identify, click **Chassis Identify** from the menu bar. A sample screenshot of Chassis Identify is shown below.



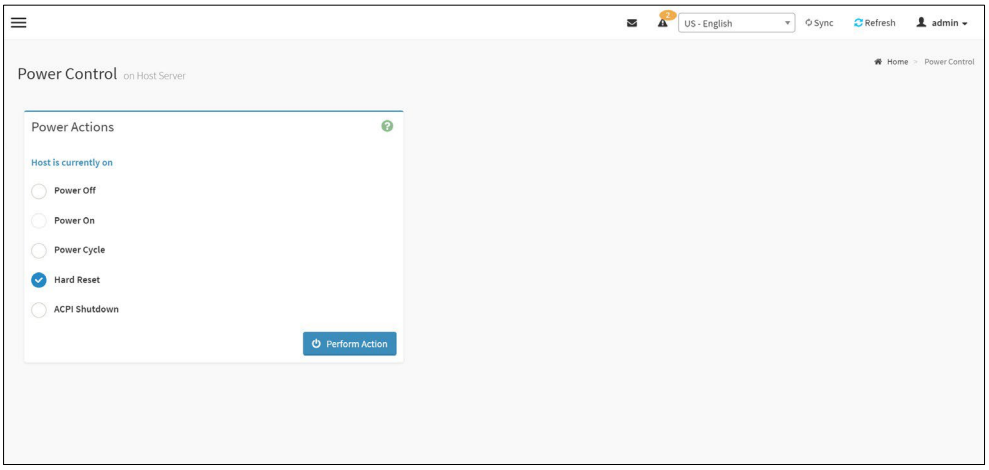
The various options of Chassis Identify are given below.

- Chassis Identify Off: This option will turn off the Chassis Identify LED.
- Chassis Identify On: This option will turn on the Chassis Identify LED.

Chapter 15. Power Control

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

To open Power Control, click **Power Control** from the menu bar. A sample screenshot of Power Control is shown below.



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 to initiate operating system shutdown prior to the shutdown.

Perform Action: Click this option to perform the selected operation.

Procedure

Select an action and click **Perform Action** to proceed with the selected action.

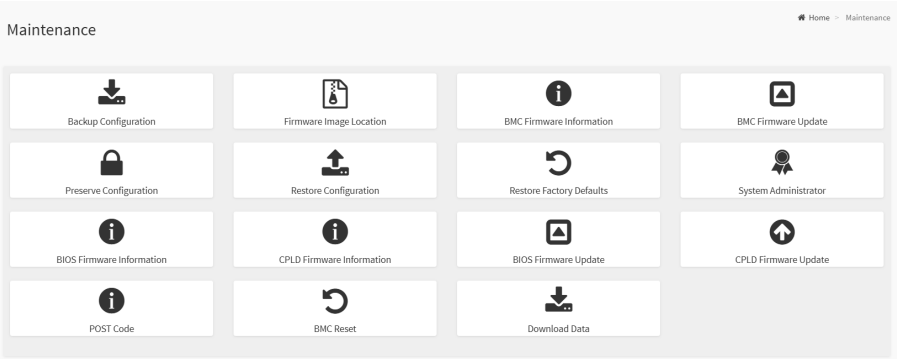
> **NOTE**
> During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

Chapter 16. Maintenance

To open the Maintenance page, click **Maintenance** from the menu bar. This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Backup Confifiguration
- Firmware Image Location
- BMC Firmware Information
- BMC Firmware Update
- Preserve Confifiguration
- Restore Confifiguration
- Restore Factory Defaults
- System Administrator
- BIOS Firmware Information
- CPLD Firmware Information
- BIOS Firmware Update
- CPLD Firmware Update
- POST Code
- BMC Reset
- Download Data

A sample screenshot of Maintenance page is displayed below.



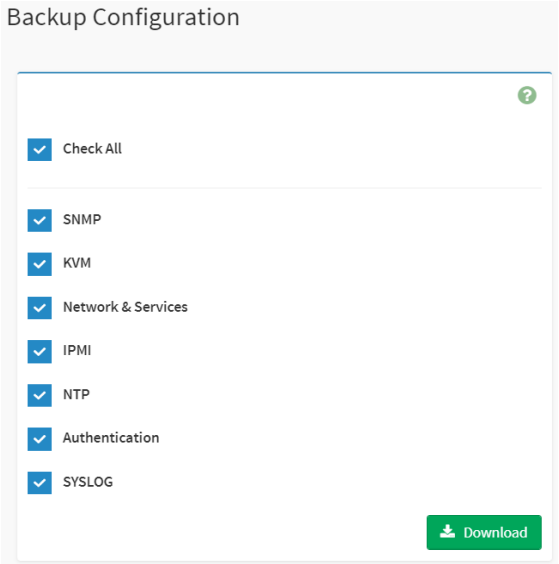
Maintenance

16.1 Backup Configuration

In order to encrypt the backup configuration, your BMC image needs to be signed with an AES key before back up, please refer to BACKUP and RESTORE KEY section.

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

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



The various fields of Backup Configuration page are given below.

Check All - To select all the configuration list.

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

> **NOTE**
> During backup, because of security concern, the mechanism parses sensitive data to filter it out and not backup sensitive files. All IPMI users password be set to default password. User has to set password again after restoring configuration by using default user in case of login failure.

Procedure for Backup Configuration

1. Click **Check All** to backup all the configuration items or check the configuration that needs to be backup. The Backup Configuration page will appear as shown in the above screenshot.

> **NOTE**
> Network configurations are inter-related 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.
3. Click **OK** to perform the backup action. The Backup file will be saved in the client system.
4. Click **Cancel** to cancel the backup process.

> **NOTE**
> If select sd/emmc for backup conf space, has to create /confbkup folder in sd/emmc partition before backup.

TFTP server configuration

The TFTP server configuration is used for exporting the backup file.

> **NOTE**
> Ensure that no other TFTP servers are enabled, if so remove all other servers with all configuration files. Login as “super” user means “root” user.

Procedure to make the default tftp server

1. Install the application which are needed.
   - apt-get install xinetd tftp tftpd
2. Edit the configuration file for TFTP.
   A. Edit tftp
   - vi /etc/xinetd.d/tftp

     Edit the file as below:

```
service tftp
{
protocol = udp
port = 69
socket_type = dgram
wait = yes
user = nobody
server = /usr/sbin/in.tftpd
server_args = <DIR to which the file to be access>
disable = no
}
#EOF
#example:server_args = /tftpboot
```

> **NOTE**
> No arguments to be passed to the server_args other than directory.

   B. Edit xinetd.conf
   - vi /etc/xinetd.conf

     Add to the file:

```
defaults
{
# Please note that you need a log_type line to use log_on_success and
#log_on_failure.
The default is the following :
# log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
```

3. Restart the server.

- /etc/init.d/xinetd restart

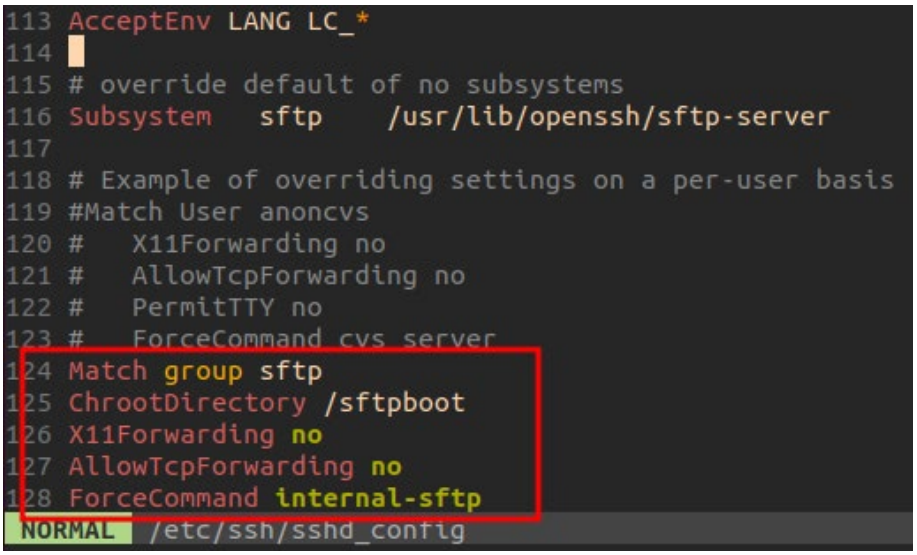
4. Give permission to the file to access by all.
   - mkdir <DIR>
   - chmod -R 777 <DIR>
   - chown -R nobody <DIR>

   For Example:
   - mkdir /tftpboot
   - chmod -R 777 /tftpboot
   - chown -R nobody /tftpboot
5. To receive the file you have to touch the file and give permission to access by all users
   - touch <DIR>/conf.bak
   - chmod 777 <DIR>/conf.bak
6. Even after all this step has been done and still facing error of timeout:
   A. Check with /etc/xinetd.d/tftp file and uncomment the EOF (Remove the '#' before the EOF alone).
   B. Restart the server.

SFTP Server Configuration

1. Install ssh if haven't installed.
   - sudo apt install ssh
2. Change the configuration of sshd_config.
   - sudo vi /etc/ssh/sshd_config
3. Paste below message at the end of the file.

```
Match group sftp
ChrootDirectory /sftpboot
X11Forwarding no
AllowTcpForwarding no
ForceCommand internal-sftp
```



Firmware Image Location

4. Restart SSH services.
   - sudo apt install ssh
5. Create sftp goup and user.
   - sudo addgroup sftp
   - sudo useradd -m sftp_test_user -g sftp
   - sudo passwd sftp_test_user -> Modify password to "Mom24697#@!"
6. Create a directory.
   - mkdir /sftpboot
   - chmod -R 755 /sftpboot

Above set up sftp server procedure could refer to below link:

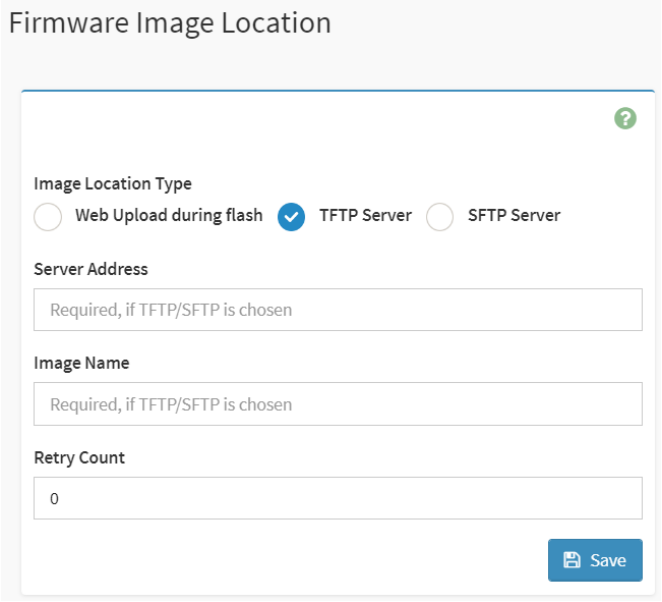
https://linuxhint.com/setup-sftp-server-ubuntu/

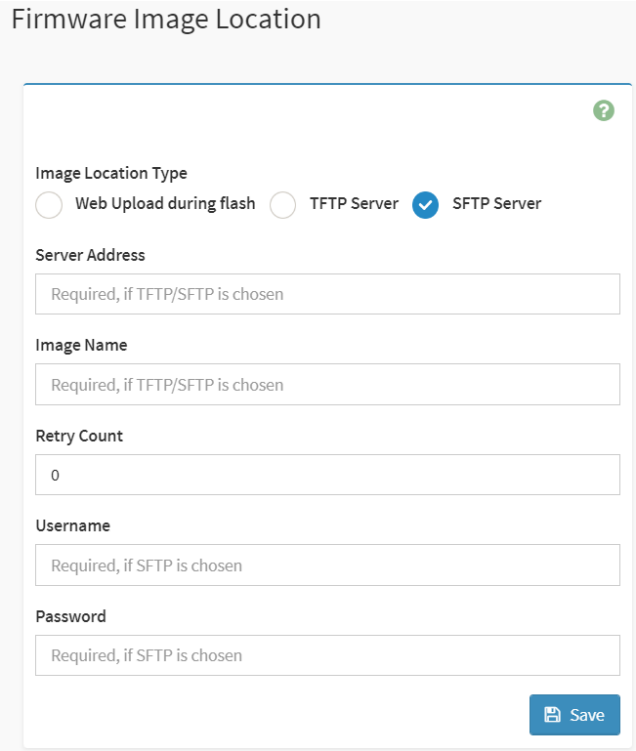
7. Put the rom.ima in the /sftpboot.

16.2 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.





The various options of Image Transfer Protocol are given below.

Image Location Type: Type of location to transfer the firmware image into the BMC either Web Upload during Flash or TFTP/SFTP Server.

TFTP/SFTP Server Address: 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.
> - 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”.
> - Hexadecimal digits are expressed as lower-case letters.

TFTP/SFTP Image Name: Full Source path with file name of the firmware image is stored on TFTP/SFTP Server.

TFTP/SFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

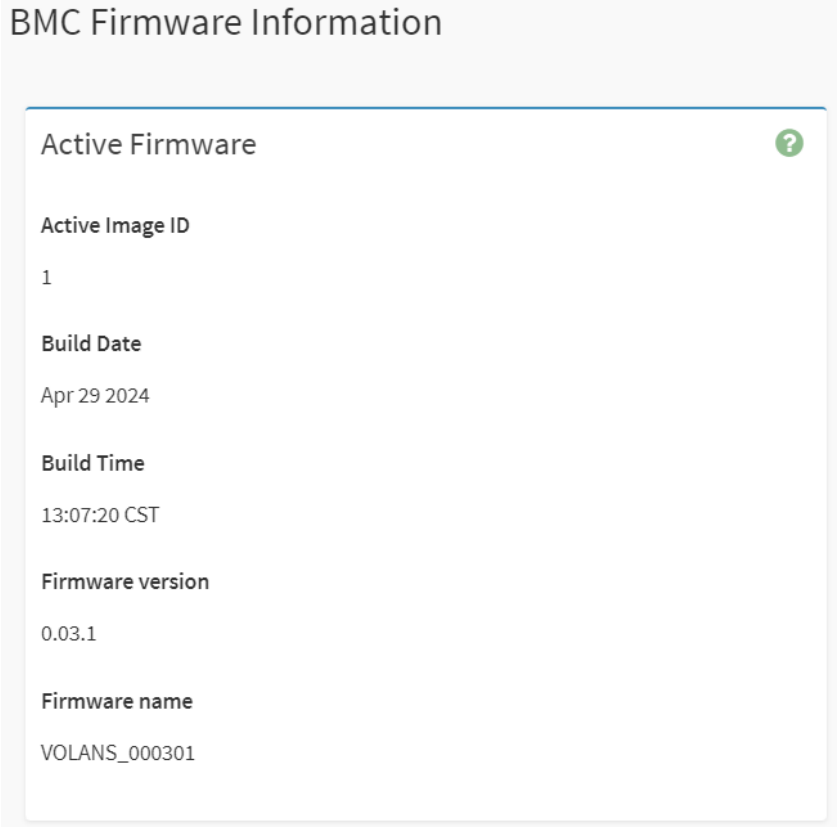
Procedure

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

16.3 BMC Firmware Information

This page is used to configure the Firmware Information settings.

To open BMC Firmware Information page, click **Maintenance** → **BMC Firmware Information** from the menu bar. A sample screenshot of BMC Firmware Information page is shown below.



The various fields of Firmware Information page are given below.

Active Image ID: Indicates the identifier of the active BMC firmware image currently in use.

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.

Firmware name: Describes the Firmware name of the active BMC image.

16.4 BMC 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 cancelled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.

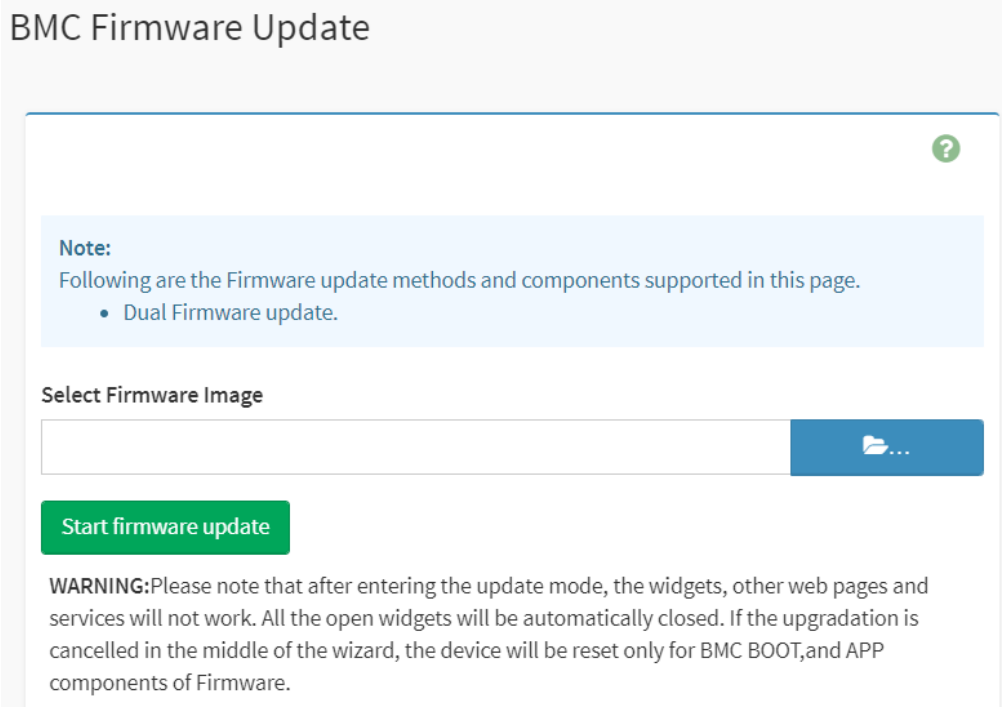
Warning: Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

> **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 into Update Mode and choose to cancel the firmware flash operation, the card must be reset. This means that you must close the Internet browser and log back onto the card before you can perform any other types of operations.
>
> Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern if Enable IPMI Command handling during flashing support is disabled in project configuration.

This feature enables the user to perform all Firmware Update operations such as Firmware Update and Dual Firmware Update.

To configure, choose '**Firmware Image Location**' under **Maintenance**.

To perform Firmware Update page, click **Maintenance** → **BMC Firmware Update** from the menu bar. A sample screenshot is displayed below.



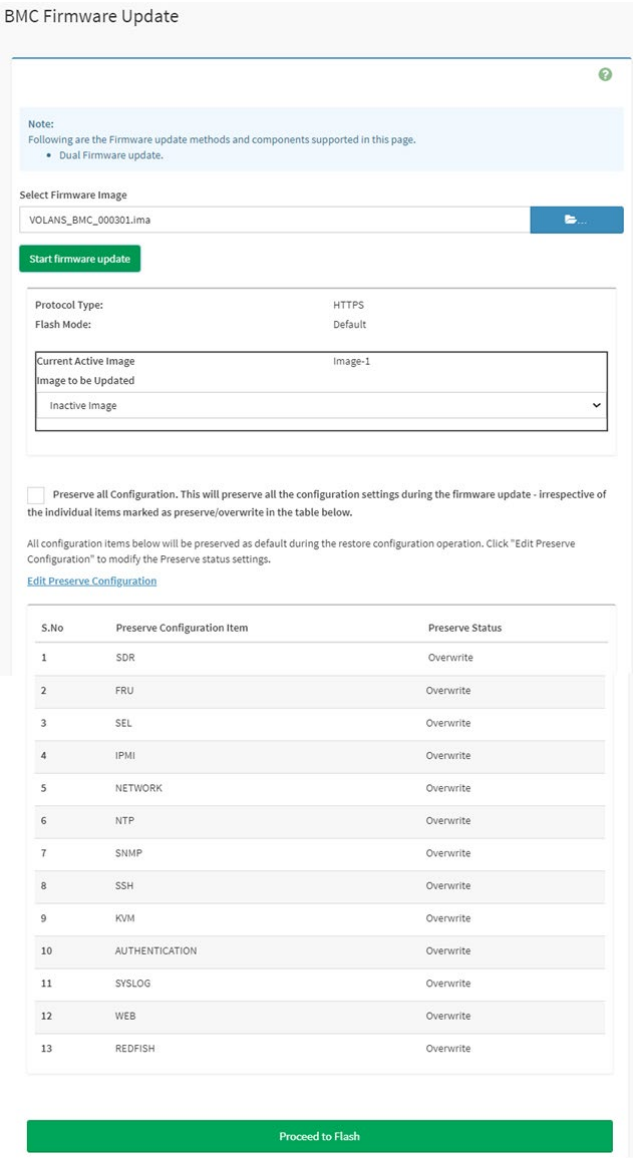
Procedure

1. Click 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 upload.

2. Click **Start firmware update** to load the Firmware Update information. A sample screenshot is displayed below.

> **NOTE**
> SignImage Public Key is feature based option. If encrypted Signimage feature is enabled, then support to Upload a public.pem key info option will be available.
>
> Firmware update methods and components supported in this page displayed based on the feature of configured/flashed image. So the content displayed in below screenshot as part of Note will differ across different image configurations.



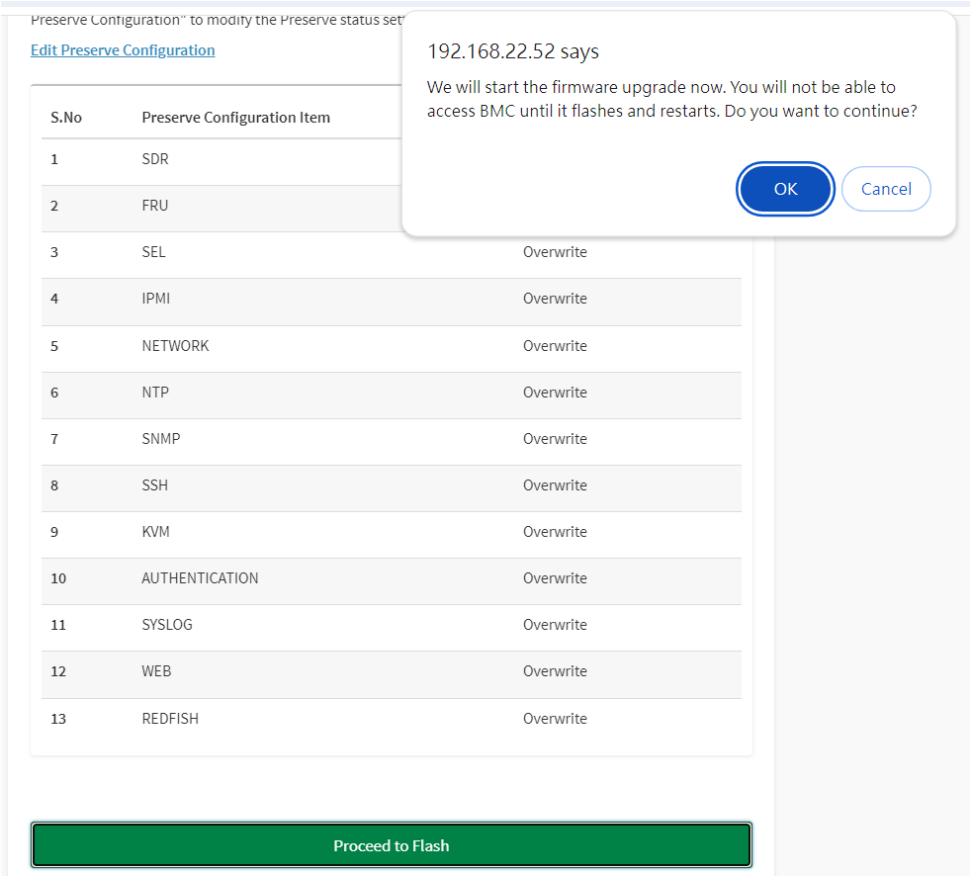
Firmware Update Page

3. If you want to preserve the configuration, select the option:
   - **Preserve all Configuration**: To preserve all configuration.
   - **Edit Preserve Configuration**: To modify the Preserve status settings.

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

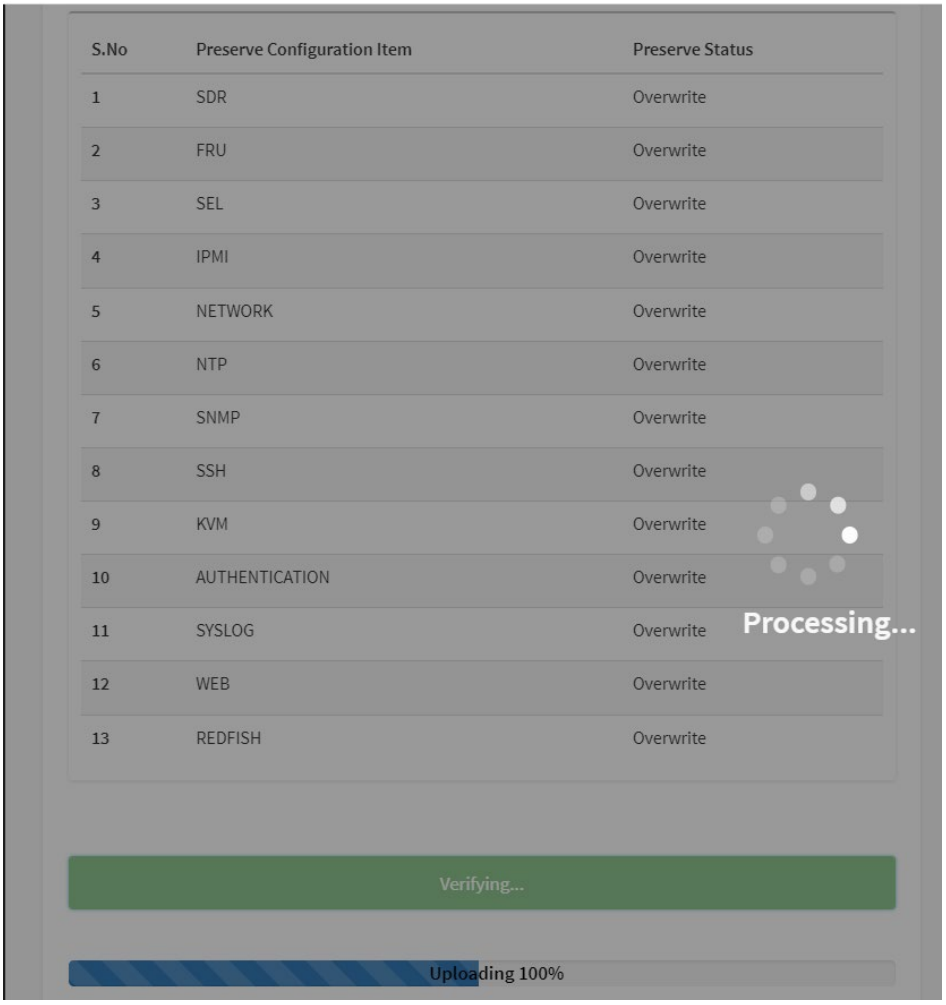
> **NOTE**
> All configuration items will be preserved/overwrite as default during the restore configuration operation.

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 Device for Firmware Upgrade
   C. Uploading Firmware Image.

   A sample screenshot is shown as below.



S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	KVM	Overwrite
10	AUTHENTICATION	Overwrite
11	SYSLOG	Overwrite
12	WEB	Overwrite
13	REDFISH	Overwrite

D. Verifying Firmware Image

In Section Based Firmware Update, you can configure the firmware image for section based flashing.

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

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

If only 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 flash operation, you are advised to verify the compatibility between image sections.

BMC Firmware Update

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

Select Firmware Image

VOLANS_BMC_000301.ima

Start firmware update

Protocol Type:	HTTPS
Flash Mode:	Default
Current Active Image	Image-1
Image to be Updated	
Inactive Image	

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

Edit Preserve Configuration

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	KVM	Overwrite
10	AUTHENTICATION	Overwrite
11	SYSLOG	Overwrite
12	WEB	Overwrite
13	REDFISH	Overwrite

Section Based Firmware Update

The following section is used to allow the user to configure the firmware image for section based flashing.

Full Flash

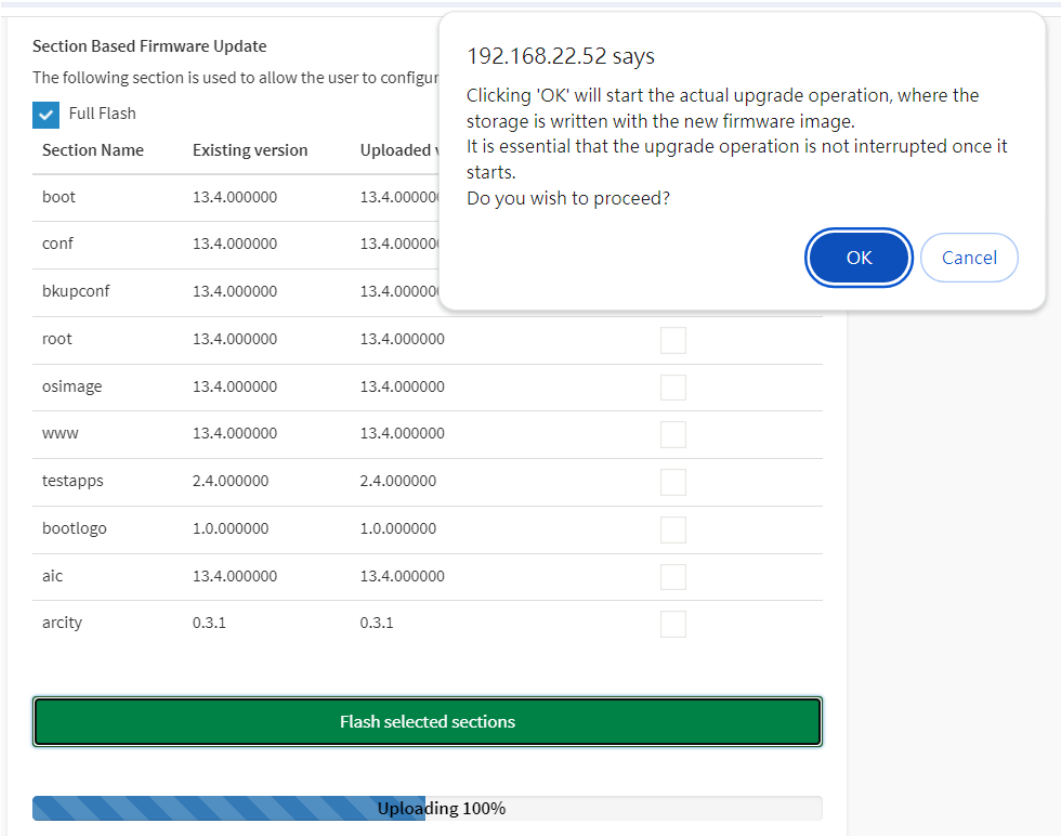
Section Name	Existing version	Uploaded version	Upgradable/Non-Upgradable
boot	13.4.000000	13.4.000000	
conf	13.4.000000	13.4.000000	
bkupconf	13.4.000000	13.4.000000	
root	13.4.000000	13.4.000000	
osimage	13.4.000000	13.4.000000	
www	13.4.000000	13.4.000000	
testapps	2.4.000000	2.4.000000	
bootlogo	1.0.000000	1.0.000000	
aic	13.4.000000	13.4.000000	
arcity	0.3.1	0.3.1	

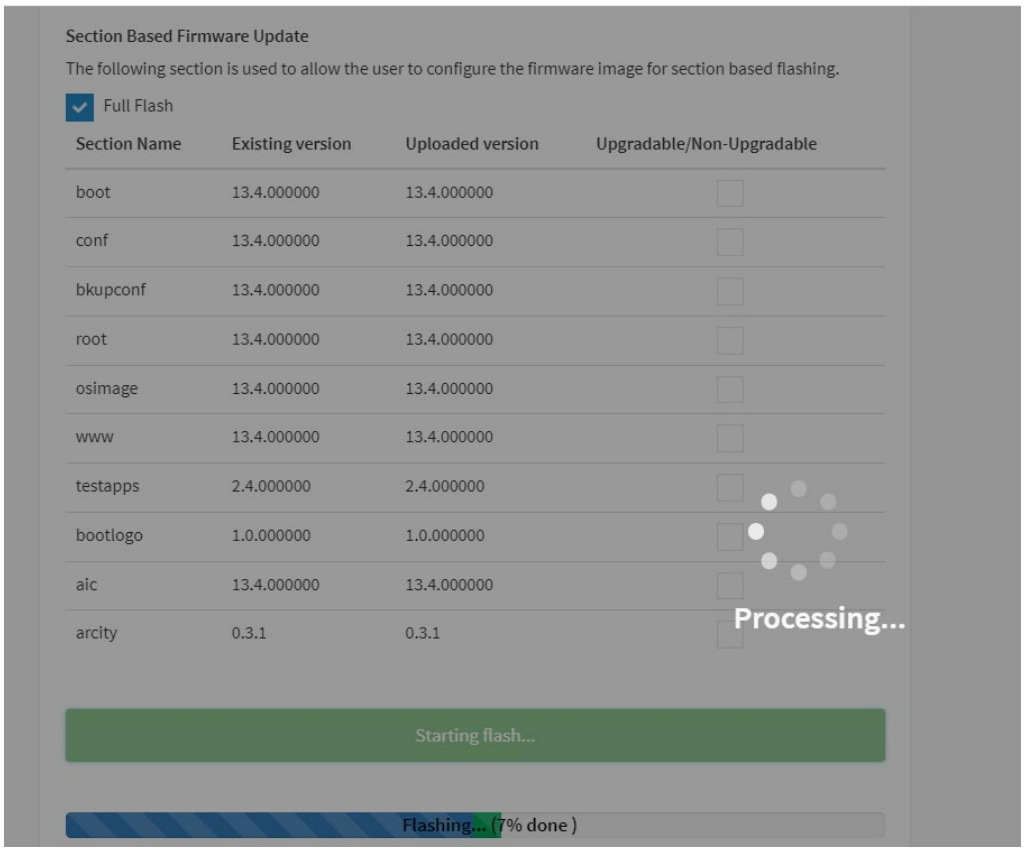
Flash selected sections

Uploading 100%

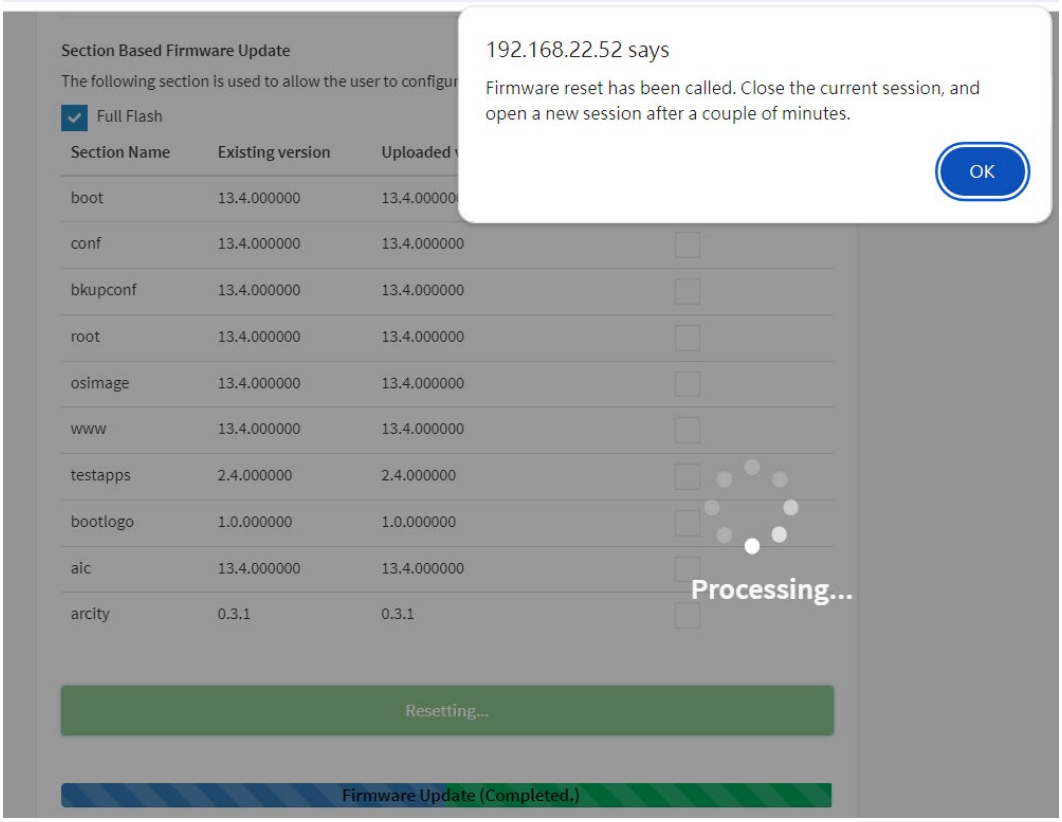
E. Click **Flash selected sections** to flashing the BMC firmware image. It will prompt you with the warning message. Click **Ok** to start the firmware update.

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





F. After the firmware update is completed, the device needs to be reset. It will prompt you with the message. Click **OK** to complete the process.



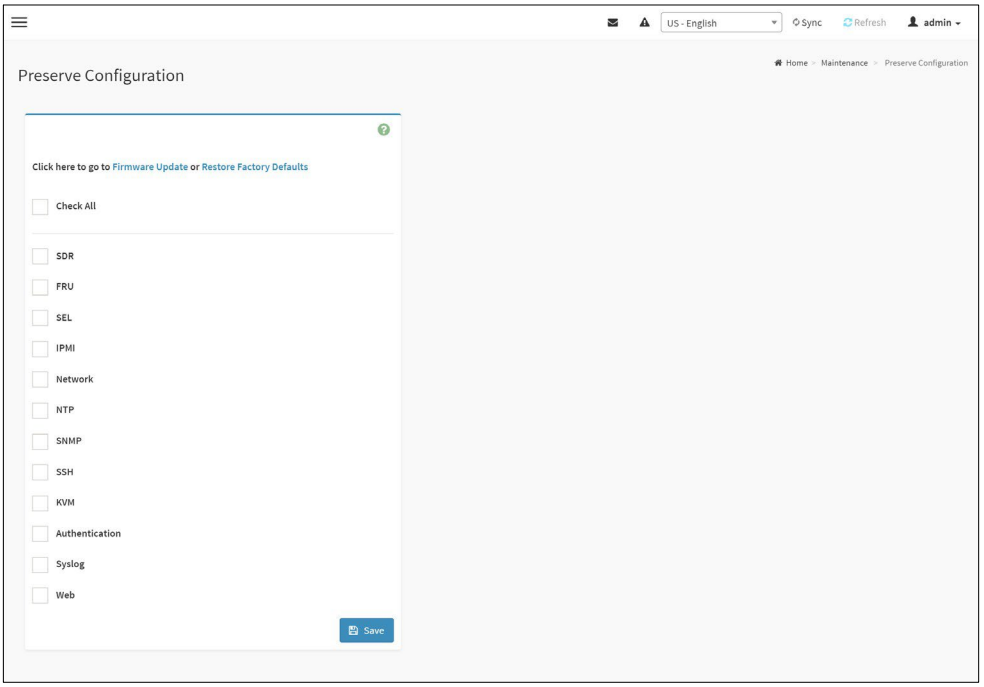
NOTE

The Firmware Update page will be disabled and you will not be able to perform any other tasks until 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 update is canceled. The device will also reset upon successful completion of firmware update.

16.5 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 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.

The various fields of Preserve Configuration are as follows.

Click here to go to Firmware Update or Restore Factory Defaults: This link will redirect to the Firmware Update or Restore Factory Defaults 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 Restore Factory Defaults process.

[Files Preserved]

SDR

Following files will be preserved.

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

Dependency Configurations – NIL

FRU

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

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.

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

Select "IPMI" will automatically select another option "Network" and it's vice versa. 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 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 – Network

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), selecting “IPMI” will automatically select the another option “**Network**” and it’s vice versa. After restore configuration, the Network Configuration will be preserved successfully. Following files will also be preserved.

dhcp.conf: This file is to configure the host name in the FQDN format.

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 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 has permission to access the system

hosts.deny : This file contains the list of host that does not allow accessing the system

resolv.conf: This file is used to store the name server 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, 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.

ncml.conf: This file contains service configuration details.

Dependency Configurations – IPMI

NTP

Following files will be preserved.

ntp.conf: This file contains the NTP dameon 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 local time or to the correct time zone in the system timezone directly.

Dependency Configurations - IPMI

SNMP

Following files will be preserved.

snmp_users.conf: This file contains the SNMP user configurations such as user name and password encryption mechanism for the specific users.

snmpcfg.conf: This file contains the SNMP users privilege levels such as ro user and rw user.

Dependency Configurations - NIL

SSH

Following files will be preserved.

sshd_config: This file contains the keyword argument pairs of configurations such as Address family, Accept Env, Allow, users, authorized key files etc.

ssh_host_dsa_key , ssh_host_rsa_key: These files contain the private parts of the host keys.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub: These files contain the public parts of the host keys.

Dependency Configurations - NIL

KVM & Media

Following files will be preserved.

vmedia.conf: This file contains the modes of media such as cd, hd and enable and disable flags for lmedia, rmedia and sd servers.

adviserd.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 file, the maximum time length of video record file and information about the remote machine path if it is enabled in the MDS project configuration.

stunnel.conf: This file contains the information about the stunnel configuration. It will also contain advisor and media server’s secure port if secure connection is enabled.

rmedia.conf: This file contains the image name and the remote machine information like IP address, user name, password, domain name and share type.

Dependency Configurations - NIL

Authentication

Following files will be preserved.

activedir.conf: This file contains the configurations such as sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such as name domain and privileges.

openLdapGroup.conf: This file contains the oprnm 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, 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 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 Preserve configuration

Procedure

1. Click **Firmware Update** or **Restore Configuration** link to view 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.

16.6 Restore Configuration

This page allows you to restore the configuration files from the client system to the BMC. To open Restore Configuration page, click **Maintenance** → **Restore Configuration** from the menu bar. A sample screenshot of Restore Configuration page is shown below.

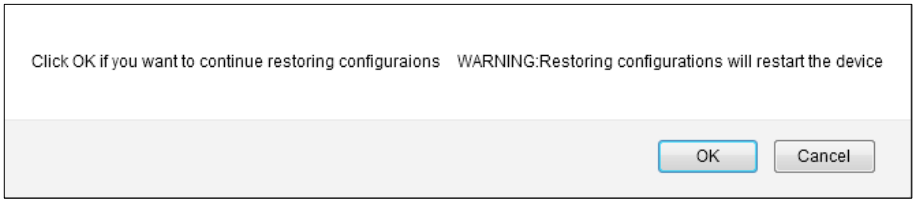
The various fields Restore Configuration page are given below.

Config File - This option is used to select the file which was backup earlier.

Upload - To 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 backup 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.



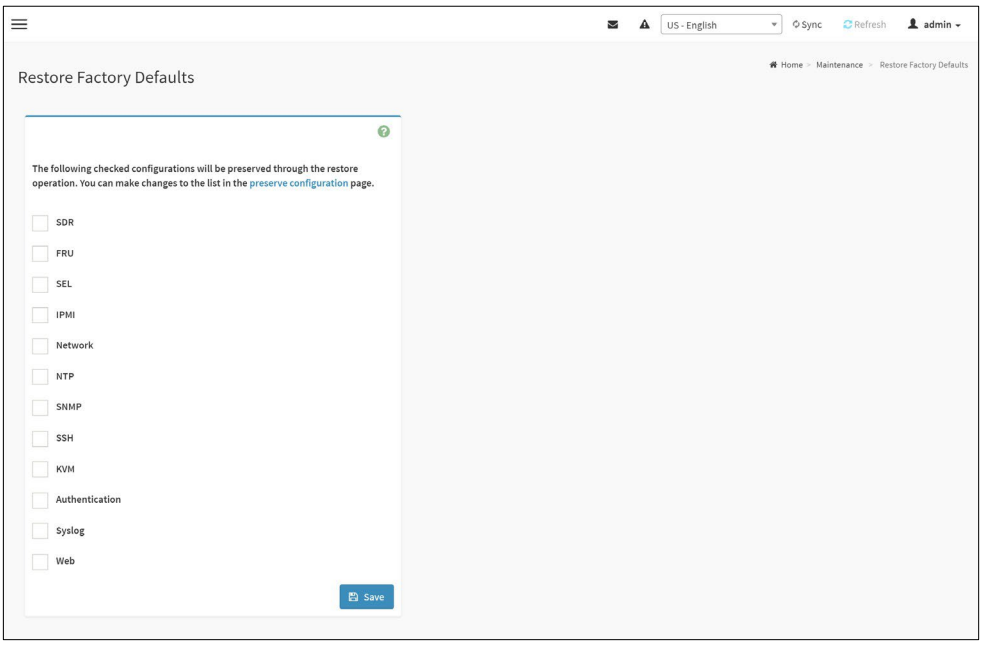
3. Click **OK** to upload the new configuration file and restore.

16.7 Restore Factory Default

This option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during 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 few minutes.

To open Restore Factory Defaults page, click **Maintenance** → **Restore Factory Defaults** from the menu bar. A sample screenshot of Restore Factory Defaults page is shown below.



Procedure

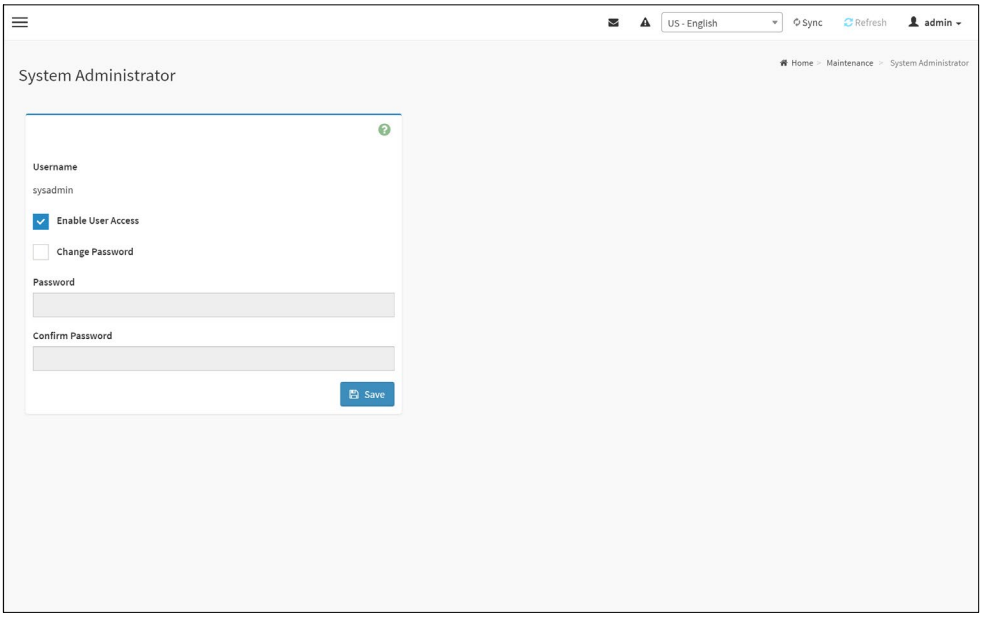
1. Click **Preserve Configuration** to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click **Restore Factory Defaults** to restore the factory defaults of the device firmware.

> **NOTE**
> When Restore Factory Defaults action is performed, there might be some log events present after performing restore operation. Those events might be newly generated which can be verified using its timestamp.

16.8 System Administrator

This page is used to configure the System Administrator settings.

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



The various fields of System Administrator page are given below.

Username: Username of System Administrator is a read only field.

Enable User Access: To enable user access for 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.

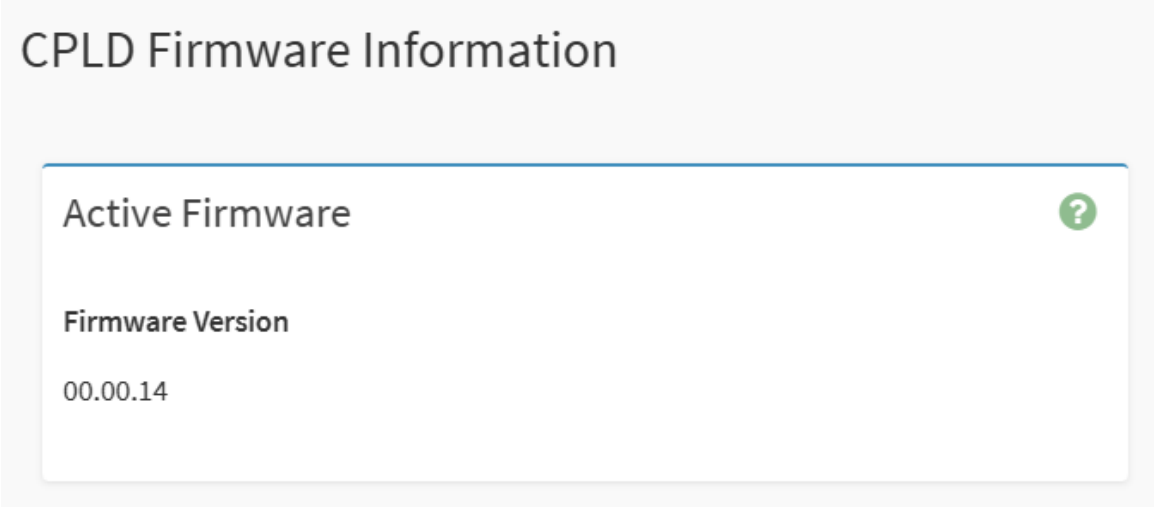
Save: To save the new configuration for system administrator.

Procedure:

1. Check **Enable User Access** to enable user access for 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.

16.9 CPLD Firmware Information

To perform CPLD Firmware Information operation, click **Maintenance** → **CPLD Firmware Information** from the menu bar. A sample screenshot is displayed below.

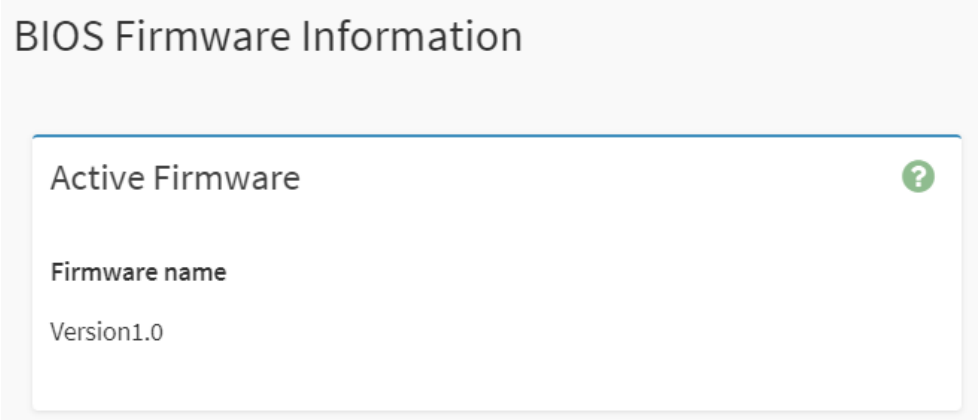


The various fields of CPLD Firmware Information page are given below.

Firmware Version: Describes the Firmware version of the CPLD image.

16.10 BIOS Firmware Information

To perform BIOS Firmware Information operation, click **Maintenance** → **BIOS Firmware Information** from the menu bar. A sample screenshot is displayed below.



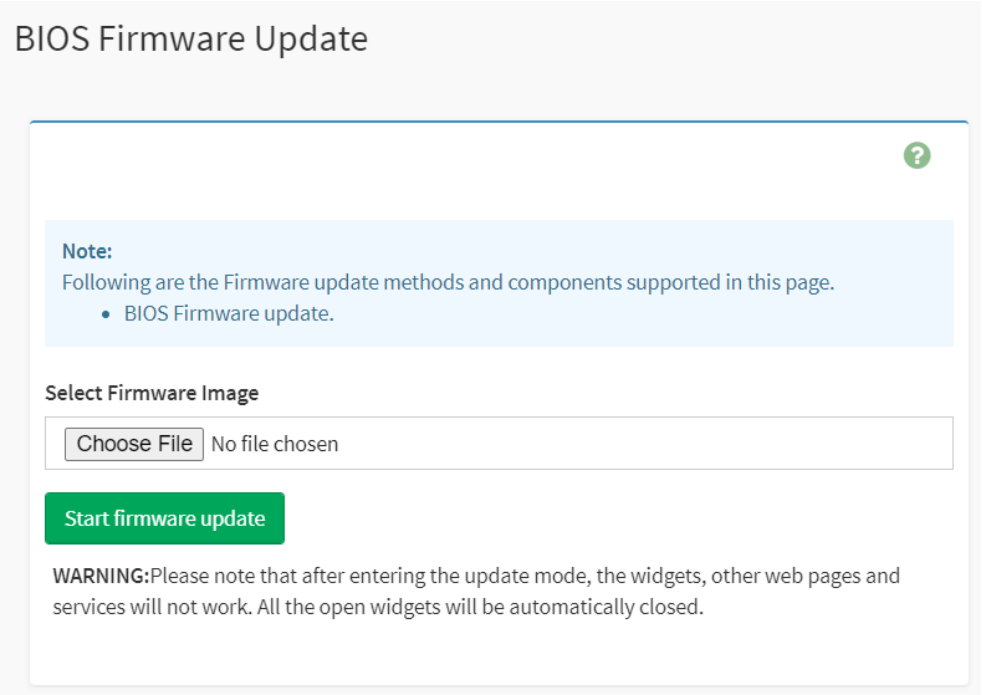
The various fields of BIOS Firmware Information page are given below.

Firmware name: Describes the Firmware name of the BIOS image.

.

16.11 BIOS Firmware Update

To perform BIOS Firmware Update operation, click **Maintenance** → **BIOS Firmware Update** from the menu bar. A sample screenshot is displayed below.



BIOS Firmware Update

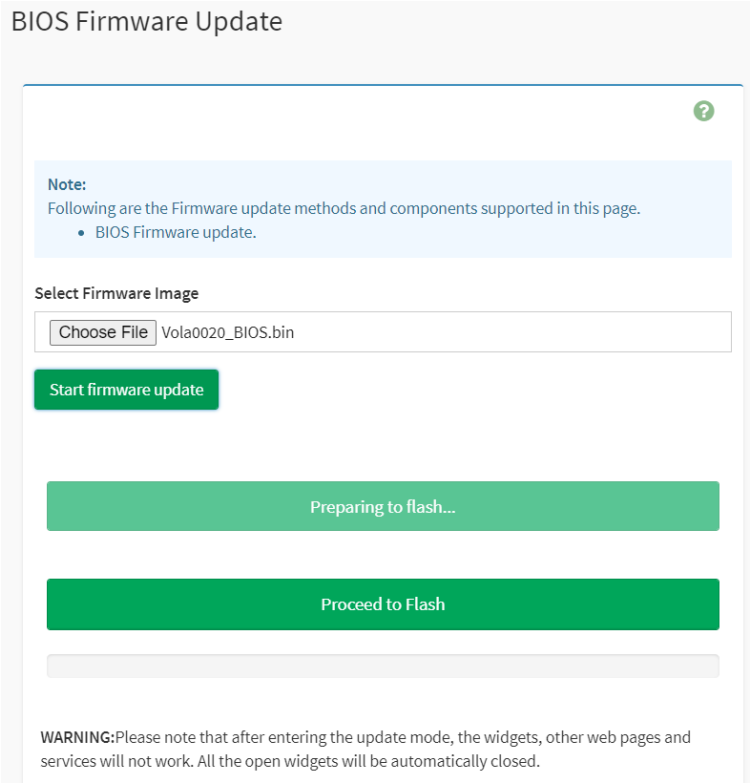
Procedure

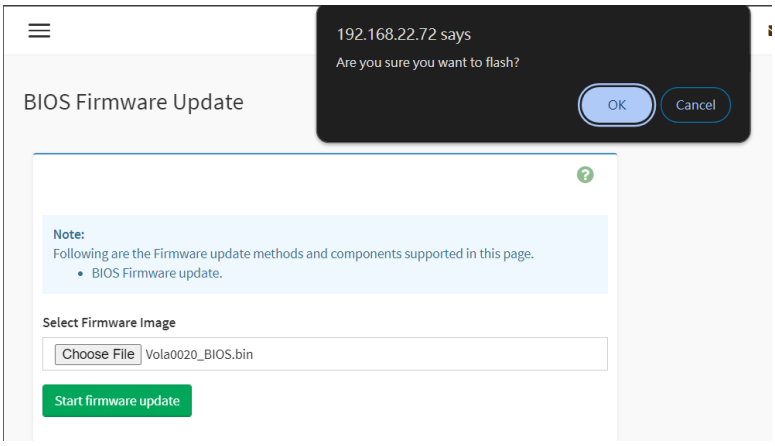
1. Click **Choose File** to select BIOS Firmware image.

> **NOTE**
> Firmware update wizard will detect .bin extension as BIOS firmware image.

2. Click **Start firmware update => Proceed to Flash** to load the BIOS firmware image information. It will prompt you with the warning message. Click **Ok** to start the firmware update. A sample screenshot is displayed below.

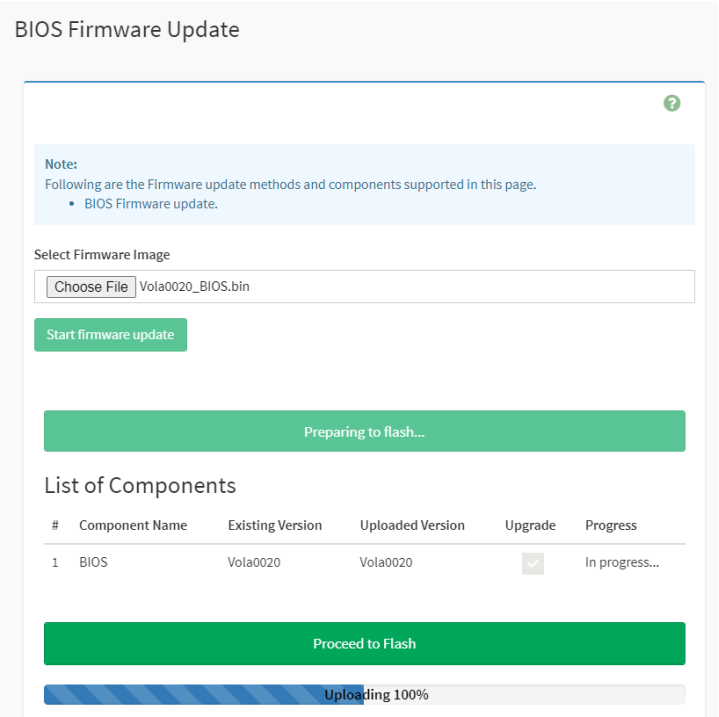
> **NOTE**
> Once you enter Firmware update page, an alert message will pop up if the system is on. The wizard will activate the update process after the user powers off the system.



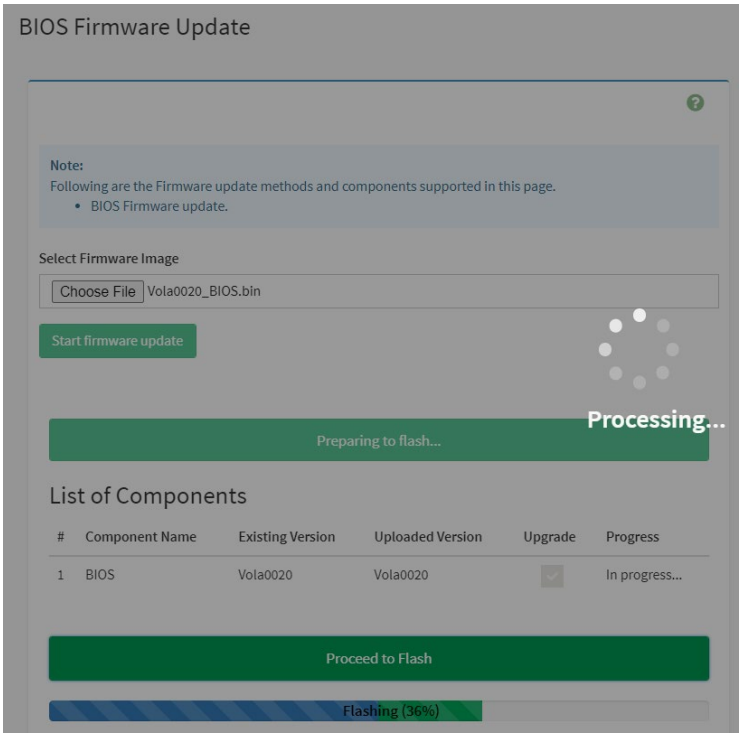


Start BIOS Firmware Update

3. Click **Proceed to Flash** to flashing the BIOS firmware image.



Uploading BIOS Firmware Image

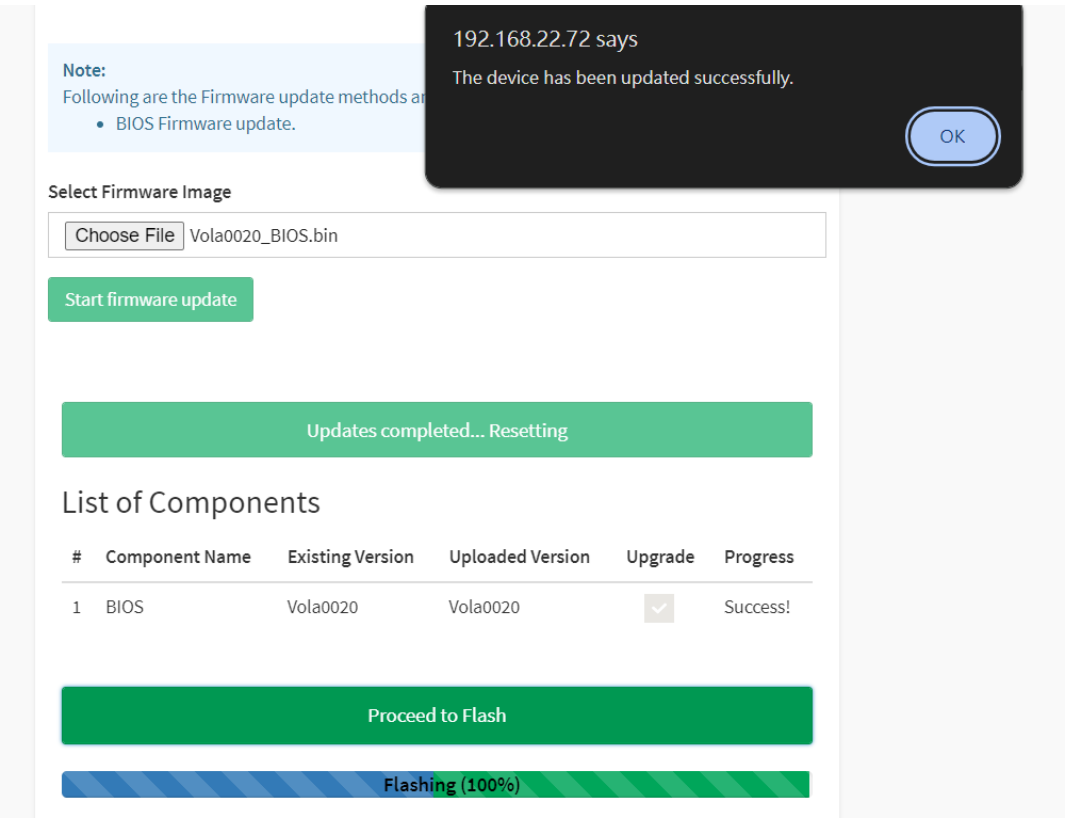


Flashing BIOS Firmware Image

NOTE

The BIOS Firmware Update page will be disabled and this action will not allow the user to perform any other tasks until firmware upgrade is completed.

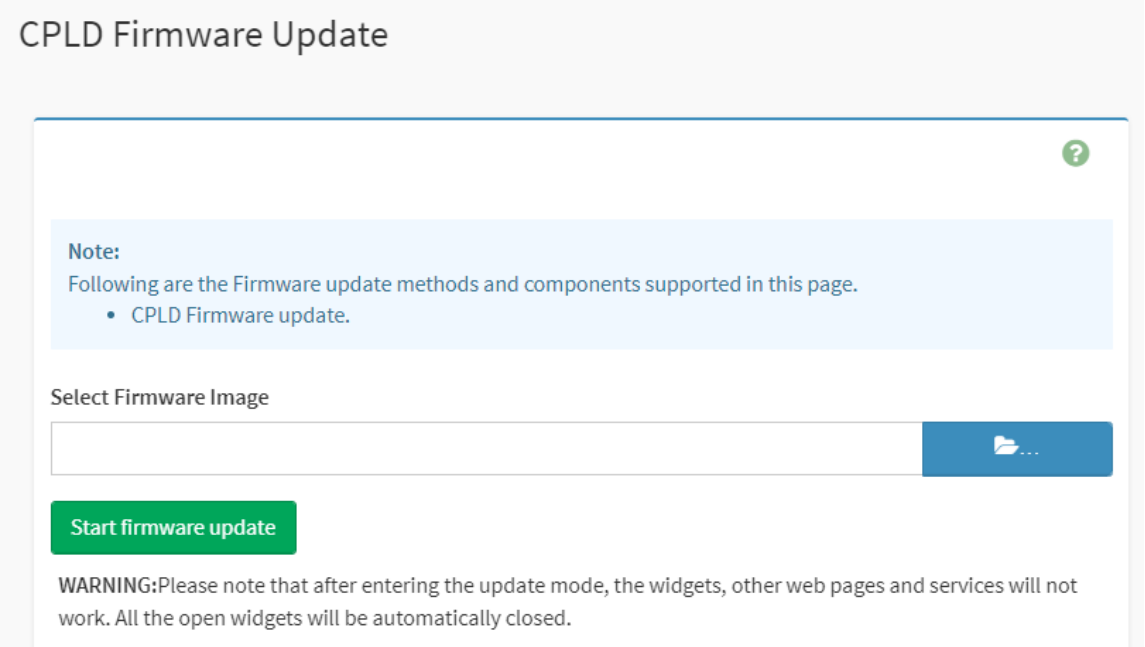
4. Once the BIOS firmware update is completed, it will prompt you with the success message. Click **OK** to complete the process. A sample screenshot is displayed below.



BIOS Firmware Update Success Message

16.12 CPLD Firmware Update

To perform CPLD Firmware Update operation, click **Maintenance** → **CPLD Firmware Update** from the menu bar. A sample screenshot is displayed below.

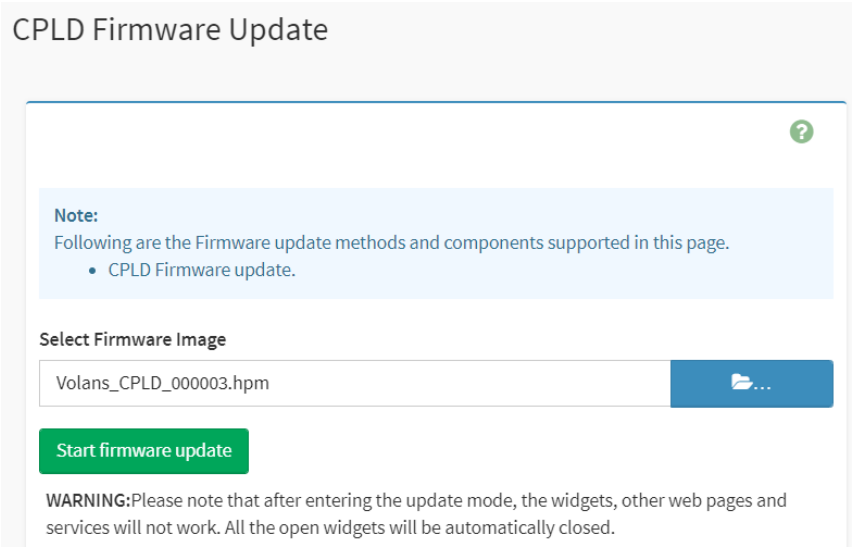


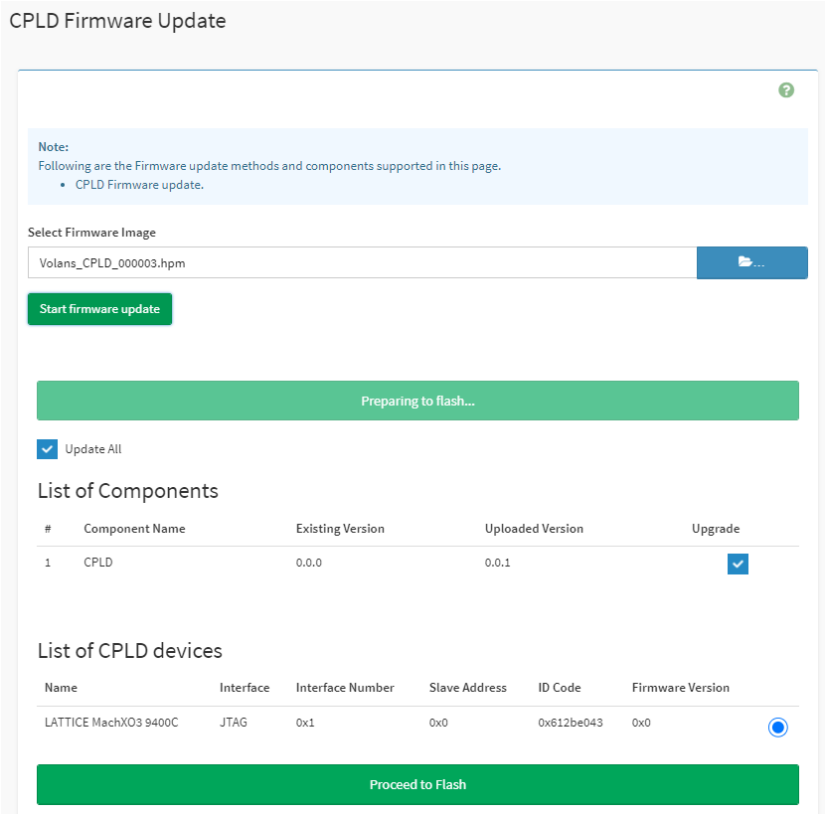
CPLD Firmware Update

Procedure

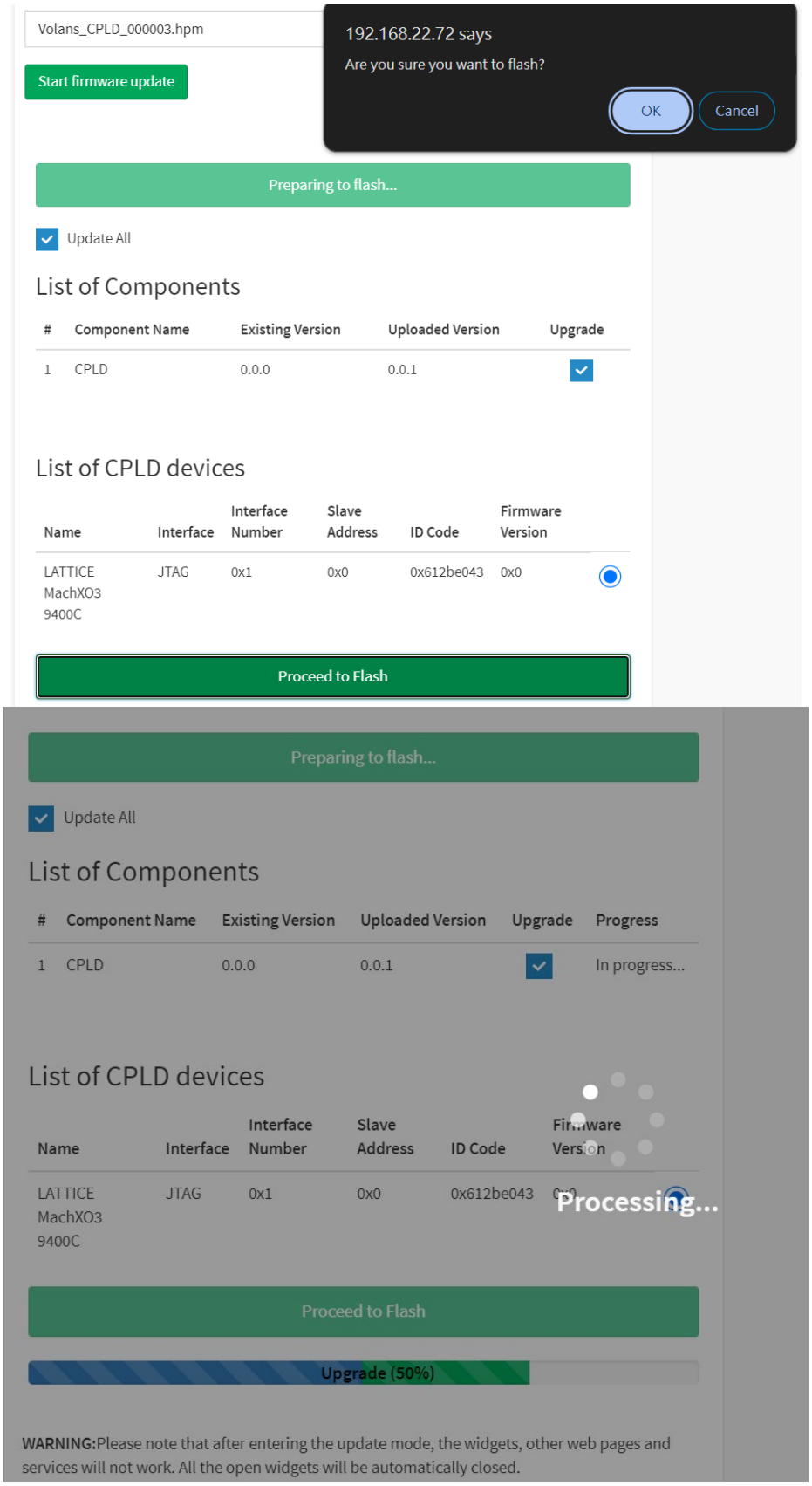
1. Click to select CPLD Firmware image.
2. Click **Start firmware update** to load the CPLD firmware image information. A sample screenshot is displayed below.

> **NOTE**
> Once you enter Firmware update page, an alert message will pop up if the system is on. The wizard will activate the update process after the user powers off the system.



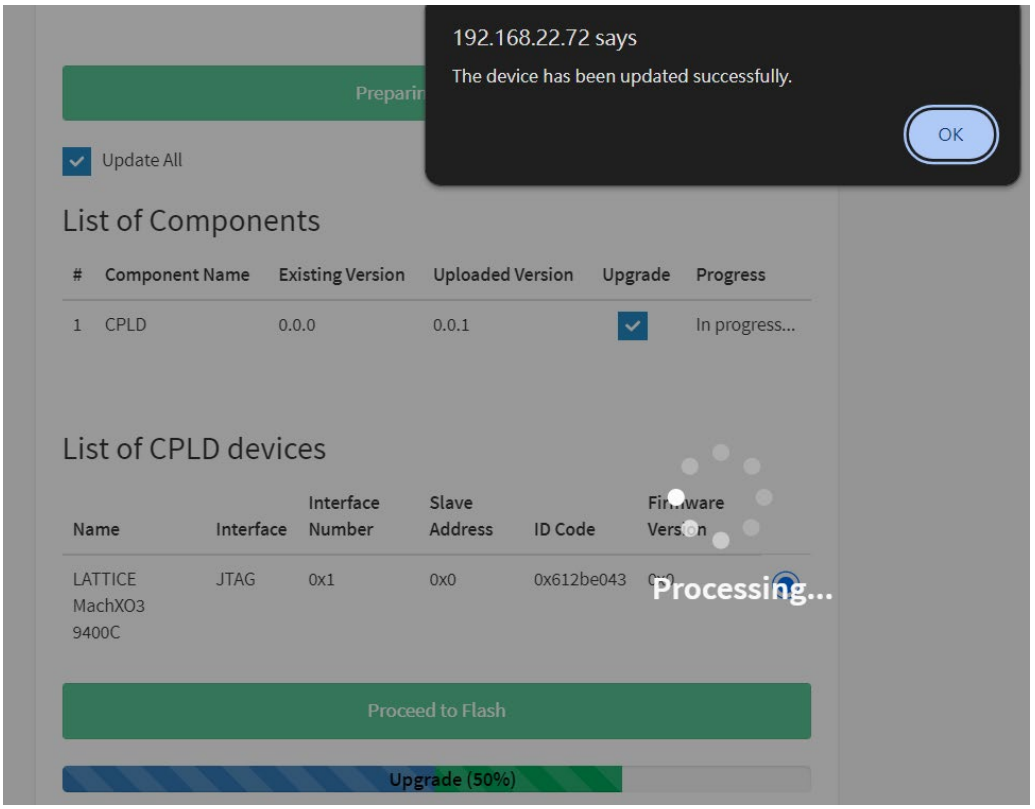


3. Click **Proceed to Flash** to flashing the CPLD firmware image. It will prompt you with the warning message. Click **Ok** to start the firmware update.



Flashing CPLD Firmware Image

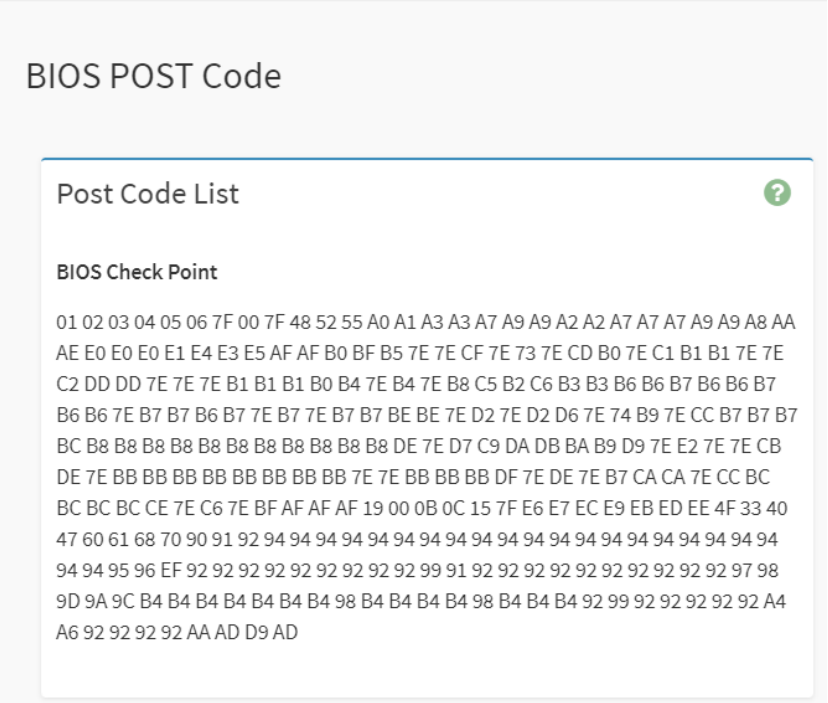
4. Once the CPLD firmware update is completed, it will prompt you with the success message. Click **OK** to complete the process.



16.13 Post Code

This page is used to get the system POST code.

To open POST Code page, click **Maintenance** → **POST Code** from the menu bar. A sample screenshot of POST Code page is shown below.



16.14 BMC Reset

This page is used to reset the BMC firmware.

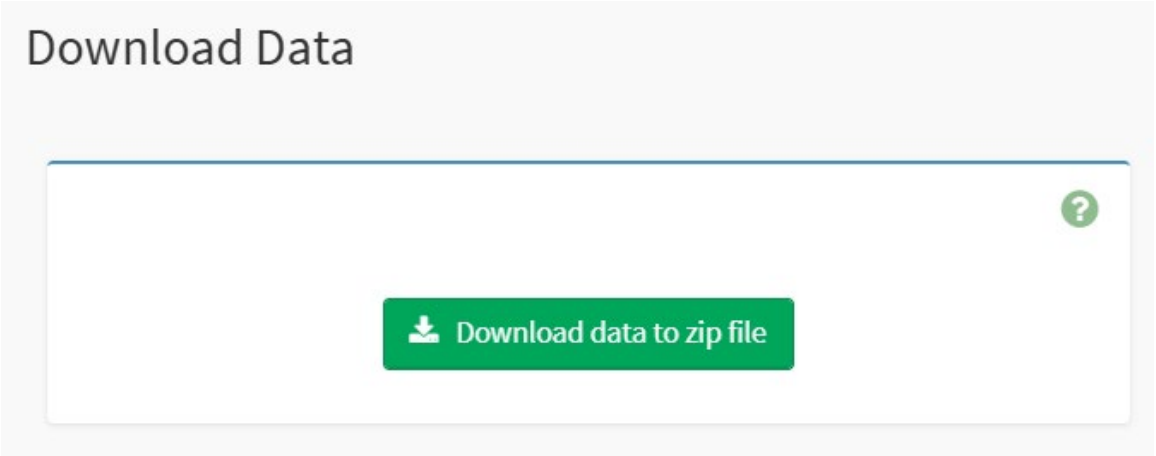
To open BMC Rest page, click **Maintenance** → **BMC Reset** from the menu bar. A sample screenshot of BMC Rest page is shown below.

Click **Reset** button to reset BMC firmware.

16.15 Download Data

This page is used to dump system information, like Firmware Info, Fru Info, Host Invnetory Info, Audit Log, Event Log, System Log, Sensor Info, Network Setting and Sensor Modification Setting.

To open Download Data page, click **Maintenance** → **Download Data** from the menu bar. A sample screenshot of Download Data page is shown below.



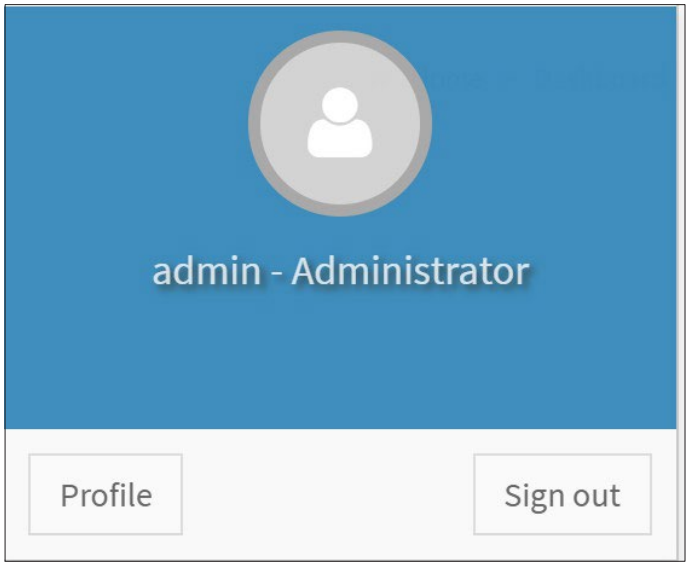
Click D**ownload data to zip** file button to dump system infomation.

data.zip file will be downloaded, and the system informations are in the zip file as below.

名稱	類型	壓縮大小	受密碼保護	大小	壓縮比	修改日期
firmware-info.json	JSON 來源檔案	1 KB	否	1 KB	0%	2025/2/25 上午 08:20
fru.json	JSON 來源檔案	2 KB	否	2 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_ba...	JSON 來源檔案	2 KB	否	2 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_m...	JSON 來源檔案	6 KB	否	6 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_pc...	JSON 來源檔案	10 KB	否	10 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_po...	JSON 來源檔案	9 KB	否	9 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_pr...	JSON 來源檔案	1 KB	否	1 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_st...	JSON 來源檔案	2 KB	否	2 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_sy...	JSON 來源檔案	1 KB	否	1 KB	0%	2025/2/25 上午 08:20
host_inventory_host_interface_th...	JSON 來源檔案	16 KB	否	16 KB	0%	2025/2/25 上午 08:20
logs_audit.json	JSON 來源檔案	9 KB	否	9 KB	0%	2025/2/25 上午 08:20
logs_event.json	JSON 來源檔案	12 KB	否	12 KB	0%	2025/2/25 上午 08:20
logs_save-interpreted-event-file.t...	TXT 檔案	3 KB	否	3 KB	0%	2025/2/25 上午 08:20
logs_system.json	JSON 來源檔案	1 KB	否	1 KB	0%	2025/2/25 上午 08:20
psu.json	JSON 來源檔案	2 KB	否	2 KB	0%	2025/2/25 上午 08:20
sensors.json	JSON 來源檔案	34 KB	否	34 KB	0%	2025/2/25 上午 08:20
settings_network.json	JSON 來源檔案	1 KB	否	1 KB	0%	2025/2/25 上午 08:20

Chapter 17. Sign Out

To log out from, 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. A Warning message will be prompted you to proceed further, click **OK** to log out or **Cancel** to retain the interface.

Chapter 18. Utility & Tool

18.1 Flash Tools

The Flash Tools are command line utility programs used to upgrade the firmware using different medium like KCS, USB, and LAN. There are three tools, which are being used **YAFUFlash**.

18.1.1 YAFUFlash

Yet Another Firmware Upgrade Flash (64 bit) is a tool used for flashing the BMC. This utility is used for flashing in both Linux and Windows environment. There are three types of mediums used to flash the BMC. They are,

- Network
- USB
- KCS

All the three mediums are applicable for Windows and Linux environment. But only KCS medium can be used in FreeDOS 1.2. The medium can be selected as per your requirement.

NOTE

YAFU based firmware update using Signed Hashed image is only possible if enough RAM is available to upload the full firmware image before the update starts.

In YAFU firmware upgrade, only YAFU command set is allowed if **Enable IPMI Command handling during flashing** support is disabled in project configuration.

YAFU flashing process has the following timeout values:

LAN interface: 3600 seconds

USB interface: 1800 seconds

KCS interface: 5400 seconds

If Secure Boot Support is enabled in the PRJ, YAFUFlash options for Section Based Flashing or Interactive mode will not be used. Hence any feature or options that rely on Section Based Flashing or Interactive mode cannot be used when Secure Boot Support is enabled.

18.1.2 Installation in Windows

1. Open the command prompt in administrator mode and enter YafuFlash\Windows path.
2. This contains two files, **Yafuflash.exe** and **LIBIPMI.dll**.
3. Format: **Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]**, where Perform BMC Flash Update
   - -? Displays the utility usage
   - -h Displays the utility usage

- -V Displays the version of the tool
- -e List outs a few examples of the tool

[OPTIONS]

- info	Displays information about existing FW and new FW.
-msi, -img-section-info	Displays information about current FW Sections.
-mi, -img-info	Displays information about current FW Versions.
- fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
- pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
- i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade.
- ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi,-ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.
-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore-reselect-image	Option skips reselecting the active image.
-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.

-mse, -img-select	Option to specify the Image to be updated 0- Inactive Image 1 - Image 1 2 - Image 2 3 - Both Images
-rp, -replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-sameimage','-ignore- module-location'&'-ignoreboot-version' options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask to confirm that those configuration is to be preserved.
-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp,-split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check
-d	Option to specify the peripheral(Only for Dual Image Support) <bit0> - BMC <bit1> - BIOS <bit2> - CPLD <BIT4> - ME
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-nr, -no-reboot	Option to skip the reboot. With online-flash support, if conf/extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method

-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw, **-ip,** **-u,** **-p,** **-host,** **_p**	Option to use Network Medium: '-ip' Option to enter IP, when using Network Medium '-host' Option to enter host name, when using Network Medium. '-u' Option to enter UserName, when using Network Medium. '-p' Option to enter Password, when using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.
-serial	Option to use serial interface.
-term	Option to use serial command, e.g. /dev/ttyS0.
-baudrate	Option to use baudrate of the serial terminal, e.g. 115200.

[FW_IMAGE_FILE] ***Firmware image file name [rom.ima].***

-pe, **-preserve-extlog**	Option to preserve extlog configuration during firmware flash.

NOTE
'-preserve-config' and '-force-boot' option not be used in interactive upgrade.

Examples for Network Medium

Eg1:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both existing firmware and new firmware.

Eg2:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -force-boot

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -preserve-config

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with preserve config params.

Eg5:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -force-boot -preserve-config

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg6:

- ./Yafuflash -nw -host spxbmc -force-boot -preserve-config rom.ima

Description: This command works with network medium using the host name spxbmc, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg7:

- ./Yafuflash -nw -ip 2000::2005 -force-boot rom.ima

Description: This command works with network medium using the ipv6 address 2000::2005, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg8:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -i

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima using interactive upgrade mode and user will be prompt to select the Number of modules and module names to upgrade.

Eg9:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-section-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg10:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of existing firmware Version.

Eg11:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin public.pem -replace-publickey

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in firmware.

Eg12 :

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-sdr

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg13 :

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-snmp -preserve-ntp

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg14 :

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -ignore-existing-overrides

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg15:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -preserve-snmp -ignore-existingoverrides

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg16:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg17:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-non-preserveconfig

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg18:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 0 rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg19:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 1 rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg20:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 2 rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg21:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 3 rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg22:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -quite

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima with minimum progress details.

Eg23:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -split-img boot.ima

Description: This command works with network medium to flash the boot split image.

Eg24:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin -split-img root.ima

Description: This command works with network medium to flash the root split image.

Eg25:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin rom.ima -flash-root -flash-conf

Description: This command works with network medium to flash root and conf section from rom. ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg26:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin boot.ima -split-img -flash-boot

Description: This command works with network medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg27:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -split-img -flash-www -flash-osimage

Description: This command works with network medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg28:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin rom.ima -preserve-extlog

Description: This command works with network medium to preserve extended log configuration.

Eg29:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -split-img -preserve-extlog

Description: This command works with network medium to preserve extended log configuration from split image.

Eg30:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -d 1 rom.ima

Description: This command works with network medium to flash the image on specific peripheral device.

Eg31:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -d 1 root.ima -split-img

Description: This command works with network medium to flash the split image on specific peripheral device.

Eg32:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin -bu root.ima

Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Eg 33:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -netfn 0x36

Description: This command works with network medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for USB Medium

Eg1:

- ./Yafuflash -cd rom.ima -info

Description: This command works with USB medium which displays the details of both Existing Firmware and new firmware.

Eg2:

- ./Yafuflash -cd rom.ima

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -cd rom.ima -force-boot

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4: ./Yafuflash -cd rom.ima -preserve-config

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

- ./Yafuflash -cd rom.ima -force-boot -preserve-config

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

- ./Yafuflash -cd rom.ima -i

Description: This command works with USB medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the number of modules and module names to upgrade.

Eg7:

- ./Yafuflash -cd -img-section-info

Description: This command works with USB medium which displays the details of Existing Firmware.

Eg8:

- ./Yafuflash -cd -img-info

Description: This command works with USB medium which displays the details of Existing Firmware Version.

Eg9:

- ./Yafuflash -cd public.pem -replace-publickey

Description: This command works with USB medium which replaces the public key in Existing Firmware.

Eg10:

- ./Yafuflash -cd rom.ima -preserve-sel -preserve-ipmi

Description: This command works with USB medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

- ./Yafuflash -cd rom.ima -preserve-sel -ignore-existing-overrides

Description: This command works with USB medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

- ./Yafuflash -cd rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

- ./Yafuflash -cd rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

- ./Yafuflash -cd -img-select 0 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

- ./Yafuflash -cd -img-select 1 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

- ./Yafuflash -cd -img-select 2 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

- ./Yafuflash -cd -img-select 3 rom.ima

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting both the images to be flashed.

Eg18:

- ./Yafuflash -cd rom.ima -quite

Description: This command works with USB medium, which start to flash the new rom.ima with minimum progress details.

Eg19:

- ./Yafuflash -cd -split-img boot.ima

Description: This command works with USB medium to flash the boot split image.

Eg20:

- ./Yafuflash -cd -split-img root.ima

Description: This command works with USB medium to flash the root split image.

Eg21:

- ./Yafuflash -cd rom.ima -flash-root -flash-conf

Description: This command works with USB medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg22:

- ./Yafuflash -cd boot.ima -split-img -flash-boot

Description: This command works with USB medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg23:

- ./Yafuflash -cd root.ima -split-img -flash-www -flash-osimage

Description: This command works with USB medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg24:

- ./Yafuflash -cd rom.ima -preserve-extlog

Description: This command works with USB medium to preserve extended log configuration.

Eg25:

- ./Yafuflash -cd root.ima -split-img -preserve-extlog

Description: This command works with USB medium to preserve extended log configuration from split image.

Eg26:

- ./Yafuflash -cd root.ima -d 1 rom.ima

Description: This command works with USB medium to flash the image on specific peripheral device.

Eg27:

- ./Yafuflash -cd root.ima -d 1 root.ima -split-img

Description: This command works with USB medium to flash the split image on specific peripheral device.

Eg28:

- ./Yafuflash -cd rom.ima -netfn 0x36

Description: This command works with USB medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for KCS Medium

Eg1:

- ./Yafuflash -kcs rom.ima -info

Description: This command works with KCS medium which displays the details of both Existing Firmware and new firmware.

Eg2:

- ./Yafuflash -kcs rom.ima

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -kcs rom.ima -force-boot

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

- ./Yafuflash -kcs rom.ima -preserve-config

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

- ./Yafuflash -kcs rom.ima -force-boot -preserve-config

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

- ./Yafuflash -kcs rom.ima -i

Description: This command works with KCS medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7:

- ./Yafuflash -kcs -img-section-info

Description: This command works with KCS medium which displays the details of Existing Firmware.

Eg8:

- ./Yafuflash -kcs -img-info

Description: This command works with KCS medium which displays the details of Existing Firmware Version.

Eg9:

- ./Yafuflash -kcs public.pem -replace-publickey

Description: This command works with KCS medium which replaces the public key in Existing Firmware.

Eg10:

- ./Yafuflash -kcs rom.ima -preserve-sel -preserve-ipmi

Description: This command works with KCS medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

- ./Yafuflash -kcs rom.ima -preserve-sel -ignore-existing-overrides

Description: This command works with KCS medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

- ./Yafuflash -kcs rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

- ./Yafuflash -kcs rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

- ./Yafuflash -kcs -img-select 0 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

- ./Yafuflash -kcs -img-select 1 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

- ./Yafuflash -kcs -img-select 2 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

- ./Yafuflash -kcs -img-select 3 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg18:

- ./Yafuflash -kcs rom.ima -quite

Description: This command works with KCS medium, which start to flash the new rom.ima with minimum progress details.

Eg19:

- ./Yafuflash -kcs -split-img boot.ima

Description: This command works with KCS medium to flash the boot split image.

Eg20:

- ./Yafuflash -kcs -split-img root.ima

Description: This command works with KCS medium to flash the root split image.

Eg21:

- ./Yafuflash -kcs rom.ima -flash-root -flash-conf

Description: This command works with KCS medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg22:

- ./Yafuflash -kcs boot.ima -split-img -flash-boot

Description: This command works with KCS medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg23:

- ./Yafuflash -kcs root.ima -split-img -flash-www -flash-osimage

Description: This command works with KCS medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg24:

- ./Yafuflash -kcs rom.ima -preserve-extlog

Description: This command works with KCS medium to preserve extended log configuration.

Eg25:

- ./Yafuflash -kcs root.ima -split-img -preserve-extlog

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg26:

- ./Yafuflash -kcs root.ima -d 1 rom.ima

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg27:

- ./Yafuflash -kcs root.ima -d 1 root.ima -split-img

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg28:

- ./Yafuflash -kcs rom.ima -netfn 0x36

Description: This command works with KCS medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

18.1.3 Installation in Linux

1. OpenSSL is pre-requisite for YafuFlash.
2. Open Terminal and go to **YafuFlash/Linux** path.
3. This contains Yafuflash tool.
4. Run **./Yafuflash** in the terminal.
5. Format: **Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]**, where Perform BMC Flash Update
   - -? Displays the utility usage
   - -h Displays the utility usage
   - -V Displays the version of the tool
   - -e List outs a few examples of the tool

[OPTIONS]

-info	Displays information about existing FW and new FW.
-msi, -img-section-info	Displays information about current FW Sections.
-mi, -img-info	Displays information about current FW Versions.
-fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
-pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
-i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade
-ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi, -ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.

-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore-reselect-image	Option skips reselecting the active image.
-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.
-mse, -img-select	Option to specify the Image to be updated 0 - Inactive Image 1 - Image 1 2 - Image 2 3 - Both Images
-rp, -replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-same-image','- ignore-module-location'&'- ignore- boot-version' options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask for the other configuration to be preserved.
-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp, -split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check

-d	Option to specify the peripheral(Only for Dual Image Support) <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-nr, -no-reboot	Option to skip the reboot With online-flash support, If conf/extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method
-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw, **-ip,** **-u,** **-p,** **-host,** **_p**	Option to use Network Medium: '-ip' Option to enter IP, when using Network Medium. '-host' Option to enter host name, When using Network Medium. '-u' Option to enter UserName, When using Network Medium. '-p' Option to enter Password, When using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.
-serial	Option to use serial interface.
-term	Option to use serial command, e.g. /dev/ttyS0.
-baudrate	Option to use baudrate of the serial terminal, e.g. 115200.

[FW_IMAGE_FILE] ***Firmware image file name [rom.ima].***

-pe, -preserve-extlog	Option to preserve extlog configuration during firmware flash.

NOTE

- '-preserve-config' and '-force-boot' option not be used in interactive upgrade
- IPv6 Support is added after the tool version 2.7. IPv6 Support can be used with latest Yafu tool and firmware, older version of yafu (and/or) firmware will not work.
- Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if it is built with Enable/Disable Interactive Upgrade YafuFlash option selected in Project Configuration file (*.PRJ) using MDS.

Examples for Network Medium

Eg1:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both existing firmware and new firmware.

Eg2:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -force-boot

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -preserve-config

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with preserve config params.

Eg5:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -force-boot -preserve-config

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg6:

- ./Yafuflash -nw -host spxbmc -force-boot -preserve-config rom.ima

Description: This command works with network medium using the host name spxbmc, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg7:

- ./Yafuflash -nw -ip 2000::2005 -force-boot rom.ima

Description: This command works with network medium using the ipv6 address 2000::2005, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg8:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -i

Description: This command works with network medium using the ip 155.166.132.12,

which start to flash the new rom.ima using interactive upgrade mode and user will be prompt to select the Number of modules and module names to upgrade.

Eg9:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-section-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg10:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of existing firmware Version.

Eg11:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin public.pem -replace-publickey

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in firmware.

Eg12:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-sdr

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurationswhich are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg13:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-snmp-preserve-ntp

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg14:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -ignore-existing-overrides

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg15:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -preserve-snmp -ignore-existing-overrides

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg16:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg17:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg18:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 0 rom.ima

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg19:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 1 rom.ima

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg20:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 2 rom.ima

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg21:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-select 3 rom.ima

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg22:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -quite

Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima with minimum progress details.

Eg23:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -split-img boot.ima

Description: This command works with network medium to flash the boot split image.

Eg24:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin -split-img root.ima

Description: This command works with network medium to flash the root split image.

Eg25:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin rom.ima -flash-root -flash-conf

Description: This command works with network medium to flash root and conf section from rom. ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg26:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin boot.ima -split-img -flash-boot

Description: This command works with network medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg27:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -split-img -flash-www -flash-osimage

Description: This command works with network medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg28:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin rom.ima -preserve-extlog

Description: This command works with network medium to preserve extended log configuration.

Eg29:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -split-img -preserve-extlog

Description: This command works with network medium to preserve extended log configuration from split image.

Eg30:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -d 1 rom.ima

Description: This command works with network medium to flash the image on specific peripheral device.

Eg31:

- ./Yafuflash -nw-ip 155.166.132.12 -u admin -p admin root.ima -d 1 root.ima -split-img

Description: This command works with network medium to flash the split image on specific peripheral device.

Eg32:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -netfn 0x36

Description: This command works with network medium to flash the image using 0x36

as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

```
root@localhost:/home/megarac/SP/6April/winbond/development/proprietary/software/YafuFlash/linux_86
You have new mail in /var/spool/mail/root
[root@localhost linux_86]# ./Yafuflash -nw -ip 10.0.0.120 -u root -p superuser .
./romP.ima
-----------------------------------------------
YAFUFlash - Firmware Upgrade Utility (Version 2.1)
-----------------------------------------------
(C)Copyright 2008, American Megatrends Inc.

Creating IPMI session via network with address 10.0.0.120...Done
===============================================================================
                              Firmware Details
===============================================================================
    RomImage                    ExistingImage from Flash

    ModuleName   Description   Version     ModuleName   Description   Version
1.  boot         BootLoader    9.19         boot         BootLoader    9.19
2.  params       ConfigParams  9.19         params       ConfigParams  9.19
3.  root         Root          9.19         root         Root          9.19
4.  osimage      Linux OS      9.19         osimage      Linux OS      9.19
5.  www          Web Pages     9.19         www          Web Pages     9.19
6.  cim                        9.19         cim                        9.19
7.  aviator                    9.19         aviator                    9.19

Existing Image and Current Image are Same
So,Type (Y/y) to do Full Firmware Upgrade or (N/n) to exit
Enter your Option : Y
*******************************************************************************
 WARNING!
        FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
        PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*******************************************************************************
Uploading Firmware Image : 100%... done
Flashing  Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Resetting the firmware.........
```

Screen: If Existing and current images are same

```
root@localhost:/home/megarac/SP/6April/winbond/development/proprietary/software/YafuFlash/linux_86
[root@localhost linux_86]# ./Yafuflash -nw -ip 10.0.0.120 -u root -p superuser ../romP.ima -force-boot
-----------------------------------------------
YAFUFlash - Firmware Upgrade Utility (Version 2.1)
-----------------------------------------------
(C)Copyright 2008, American Megatrends Inc.

Creating IPMI session via network with address 10.0.0.120...Done
*******************************************************************************
 WARNING!
        FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
        PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*******************************************************************************
Preserving Env Variables...        done
Setting Env variables ...          done
Upgrading Firmware Image : 100%... done
Resetting the firmware.........
[root@localhost linux_86]#
```

Existing and current are different

```
[root@muthu Linux_x86_32]# ./Yafuflash -nw -ip 10.0.3.5 -u admin -p admin rom.ima -i
-----------------------------------------------
YAFUFlash - Firmware Upgrade Utility (Version 2.11)
-----------------------------------------------
(C)Copyright 2008, American Megatrends Inc.

Creating IPMI session via network with address 10.0.3.5...Done
===============================================================================
                              Firmware Details
===============================================================================
    RomImage                    ExistingImage from Flash

    ModuleName   Description   Version     ModuleName   Description   Version
1.  boot         BootLoader    1.4.00       boot         BootLoader    1.4.00
2.  conf         ConfigParams  1.4.00       conf         ConfigParams  1.4.00
3.  bkupconf                   1.4.00       bkupconf                   1.4.00
4.  root         Root          1.4.00       root         Root          1.4.00
5.  osimage      Linux OS      1.4.00       osimage      Linux OS      1.4.00
6.  www          Web Pages     1.4.00       www          Web Pages     1.4.00
7.  lmedia                     1.4.00       lmedia                     1.4.00
8.  hornet                     1.4.00       hornet                     1.4.00

For Full Firmware upgrade,Please  type (0)  alone
For Module Upgrade enter the total no. of Modules to Upgrade
Enter your choice : 4
Enter the Module Name to Update : boot
```

Interactive Upgrade Mode

Eg33:

- ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin -bu root.ima

Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Examples for USB Medium

Eg1:

- ./Yafuflash -cd rom.ima -info

Description: This command works with USB medium which displays the details of both Existing Firmware and new firmware.

Eg2:

- ./Yafuflash -cd rom.ima

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -cd rom.ima -force-boot

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4:

- ./Yafuflash -cd rom.ima -preserve-config

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

- ./Yafuflash -cd rom.ima -force-boot -preserve-config

Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6:

- ./Yafuflash -cd rom.ima -i

Description: This command works with USB medium, which start to flash the new rom. ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7:

- ./Yafuflash -cd -img-section-info

Description: This command works with USB medium which displays the details of Existing Firmware.

Eg8:

- ./Yafuflash -cd -img-info

Description: This command works with USB medium which displays the details of Existing Firmware Version.

Eg9:

- ./Yafuflash -cd public.pem -replace-publickey

Description: This command works with USB medium which replaces the public key in Existing Firmare.

Eg10:

- ./Yafuflash-cd rom.ima -preserve-sel -preserve-ipmi

Description: This command works with USB medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

- ./Yafuflash -cd rom.ima -preserve-sel -ignore-existing-overrides

Description: This command works with USB medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

- ./Yafuflash -cd rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

- ./Yafuflash -cd rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

- ./Yafuflash -cd -img-select 0 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

- ./Yafuflash -cd -img-select 1 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

- ./Yafuflash -cd -img-select 2 rom.ima

Description: This command works with USB medium, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

- ./Yafuflash -cd -img-select 3 rom.ima

Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting both the images to be flashed.

Eg18:

- ./Yafuflash -cd rom.ima -quite

Description: This command works with USB medium, which start to flash the new rom.ima with minimum progress details.

Eg19:

- ./Yafuflash -cd -split-img boot.ima

Description: This command works with USB medium to flash the boot split image.

Eg20:

- ./Yafuflash -cd -split-img root.ima

Description: This command works with USB medium to flash the root split image.

Eg21:

- ./Yafuflash -cd -split-img root.ima

Description: This command works with USB medium to flash the root split image.

Eg22:

- ./Yafuflash -cd rom.ima -flash-root -flash-conf

Description: This command works with USB medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg23:

- ./Yafuflash -cd boot.ima -split-img -flash-boot

Description: This command works with USB medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg24:

- ./Yafuflash -cd root.ima -split-img -flash-www -flash-osimage

Description: This command works with USB medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg25:

- ./Yafuflash -cd rom.ima -preserve-extlog

Description: This command works with USB medium to preserve extended log configuration.

Eg26:

- ./Yafuflash -cd root.ima -split-img -preserve-extlog

Description: This command works with USB medium to preserve extended log configuration from split image.

Eg27:

- ./Yafuflash -cd root.ima -d 1 rom.ima

Description: This command works with USB medium to flash the image on specific peripheral device.

Eg28:

- ./Yafuflash -cd root.ima -d 1 root.ima -split-img

Description: This command works with USB medium to flash the split image on specific peripheral device.

Eg 29:

- ./Yafuflash -cd rom.ima -netfn 0x36

Description: This command works with USB medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

Examples for KCS Medium

Eg1:

- ./Yafuflash -kcs rom.ima -info

Description: This command works with KCS medium which displays the details of both Existing Firmware and new firmware.

Eg2:

- ./Yafuflash -kcs rom.ima

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware.

Eg3:

- ./Yafuflash -kcs rom.ima -force-boot

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader upgrade.

Eg4:

- ./Yafuflash -kcs rom.ima -preserve-config

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

- ./Yafuflash -kcs rom.ima -force-boot -preserve-config

Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader upgrade and preserving config params.

Eg6:

- ./Yafuflash -kcs rom.ima -i

Description: This command works with KCS medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7:

- ./Yafuflash -kcs -img-section-info

Description: This command works with KCS medium which displays the details of Existing Firmware.

Eg8:

- ./Yafuflash -kcs -img-info

Description: This command works with KCS medium which displays the details of Existing Firmware Version.

Eg9:

- ./Yafuflash -kcs public.pem -replace-publickey

Description: This command works with KCS medium which replaces the public key in Existing Firmware.

Eg10:

- ./Yafuflash -kcs rom.ima -preserve-sel -preserve-ipmi

Description: This command works with KCS medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11:

- ./Yafuflash -kcs rom.ima -preserve-sel -ignore-existing-overrides

Description: This command works with KCS medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg12:

- ./Yafuflash -kcs rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13:

- ./Yafuflash -kcs rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14:

- ./Yafuflash -kcs -img-select 0 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

- ./Yafuflash -kcs -img-select 1 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-section-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg17:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin -img-info

Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware Version.

Eg18:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin public.pem -replace-publickey

Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in Existing Firmware.

Eg19:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-sdr

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg20:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-snmp -preserve-ntp

Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg21:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -ignore-existing-overrides

Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg22:

- ./Yafuflash -nw -ip 155.166.132.12 rom.ima -preserve-fru -preserve-snmp -ignore-existing -overrides

Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg23:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-reselect-image

Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg24:

- ./Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -ignore-non-preserve-config

Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg25:

- ./Yafuflash -kcs -img-select 2 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg26:

- ./Yafuflash -kcs -img-select 3 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg27:

- ./Yafuflash -kcs rom.ima -quite

Description: This command works with KCS medium, which start to flash the new rom.ima with minimum progress details.

Eg28:

- ./Yafuflash -kcs -split-img boot.ima

Description: This command works with KCS medium to flash the boot split image.

Eg29:

- ./Yafuflash -kcs -split-img root.ima

Description: This command works with KCS medium to flash the root split image.

Eg30:

- ./Yafuflash -kcs rom.ima -flash-root -flash-conf

Description: This command works with KCS medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg31:

- ./Yafuflash -kcs boot.ima -split-img -flash-boot

Description: This command works with KCS medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg32:

- ./Yafuflash -kcs root.ima -split-img -flash-www -flash-osimage

Description: This command works with KCS medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg33:

- ./Yafuflash -kcs rom.ima -preserve-extlog

Description: This command works with KCS medium to preserve extended log configuration.

Eg34:

- ./Yafuflash -kcs root.ima -split-img -preserve-extlog

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg35:

- ./Yafuflash -kcs root.ima -d 1 rom.ima

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg36:

- ./Yafuflash -kcs root.ima -d 1 root.ima -split-img

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg 37:

- ./Yafuflash -kcs rom.ima -netfn 0x36

Description: This command works with KCS medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32.

18.1.4 YAFUFlash OS Compatibility

KCS/USB	LAN
Windows Server 2012	Ubuntu 16.04
Windows Server 2008	Windows 8.1
Windows Server 2016 Standard (Exclude Nano Server)	Ubuntu 14.04
Ubuntu Server 16.04	Windows 10
Ubuntu Server 14.04	Fedora 24
RHEL 7.2	
RHEL 6.5	
SLES Server 12.1	
SLES Server 11.4	

18.1.5 Installation in DOS

1. Copy **Yafuflash.exe** into DOS machine.
2. Run **Yafuflash** utility.
3. Format: **Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]** where, Perform BMC Flash Update.
    - -? Displays the utility usage
    - -h Displays the utility usage
    - -V Displays the version of the tool
    - -e List outs a few examples of the tool

[OPTIONS]

-info	Displays information about existing FW and new FW.
-msi, -img-section-info	Displays information about current FW Sections.
-mi, -img-info	Displays information about current FW Versions.
-fb, -force-boot	Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.
-pc, -preserve-config	Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.
-q, -quite	Use the option to show the minimum flash progress details.
-i	Option to interactive upgrade (Upgrade only required modules)**
-f, -full	Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade
-ipc, -ignore-platform-check	If this image is for a different platform, this option skips user interaction and continues update process.
-idi, -ignore-diff-image	If this image differs from the currently programmed image, this option skips user interaction and continues update process.
-isi, -ignore-same-image	If this image is same as the currently programmed image, this option skips user interaction and continues update process.
-iml, -ignore-module-location	If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.
-ibv, -ignore-boot-version	If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.
-iri, -ignore-reselect-image	Option skips reselecting the active image.
-inc, -ignore-non-preserve-config	Option skips the restore to default factor setting if the image shares the same configuration area.
-mse, -img-select	Option to specify the Image to be updated 0 - Inactive Image 1 - Image 1 2 - Image 2 3 - Both Images

-rp, -replace-publickey	Option to replace the Signed Image Key in Existing Firmware.
-vcf, -version-cmp-flash	Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.
-non-interactive	This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-same-image','- ignore-module-location'&'- ignore- boot-version' options.
-pXXX, -preserve-XXX	Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask for the other configuration to be preserved.
-ieo, -ignore-existing-overrides	Clears the existing overrides and preserves only the overrides given in command line if any.
-msp, -split-img	Option to flash the split image.
-f -XXX, -flash-XXX	Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.
-sc, -skip-crc	Option to skip the CRC check
-sf, -skip-fmh	Option to skip the FMH check
-d	Option to specify the peripheral(Only for Dual Image Support) <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-a, -activate	Option to activate peripheral devices <BIT0> - BMC <BIT1> - BIOS <BIT2> - CPLD
-nr, -no-reboot	Option to skip the reboot With online-flash support, If conf/extlog is not preserved, BMC will still reboot.
-bu, -block-upgrade	Option to Flash using Block by Block method
-netfn <NETFN>	Option to specify AMI OEM Net Function (default 0x32)

[MEDIUM]

-cd	Option to use USB Medium
-nw, **-ip,** **-u,** **-p,** **-host,** **_p**	Option to use Network Medium: '-ip' Option to enter IP, when using Network Medium. '-host' Option to enter host name, When using Network Medium. '-u' Option to enter UserName, When using Network Medium. '-p' Option to enter Password, When using Network Medium. '_p' Option to enter Port Number.
-kcs	Option to use KCS medium.

[FW_IMAGE_FILE]	**Firmware image file name [rom.ima].**
-pe, -preserve-extlog	Option to preserve extlog configuration during firmware flash.

Firmware image file name [rom.ima].

**Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if it is built with Enable/Disable Interactive Upgrade YafuFlash option selected in Project Configuration file (*.PRJ) using MDS.

Examples

Eg1:

- Yafuflash -kcs -info rom.ima

Description: Displays the details of both Existing Firmware and new firmware.

Eg2:

- Yafuflash -kcs rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware.

Eg3:

- Yafuflash -kcs -force-boot rom.ima

Description: This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

Eg4:

- Yafuflash -kcs -preserve-config rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware with preserving config params.

Eg5:

- Yafuflash -kcs -force-boot -preserve-config rom.ima

Description: This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade and preserving config params.

Eg6:

- Yafuflash -kcs -i rom.ima

Description: This command starts to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the number of modules and module names to upgrade.

Eg7:

- Yafuflash -kcs -img-section-info

Description: Displays the details of Existing Firmware.

Eg8:

- Yafuflash -kcs -img-info

Description: Displays the details of Existing Firmware Version.

Eg9:

- Yafuflash -kcs public.pem -replace-publickey

Description: Replaces the public key in Existing Firmware.

Eg10:

- Yafuflash -kcs rom.ima -preserve-sdr

Description: This command will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg11:

- Yafuflash -kcs rom.ima -preserve-snmp -preserve-ntp

Description: This command will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg12:

- Yafuflash -kcs rom.ima -preserve-fru -ignore-existing-overrides

Description: This command starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg13:

- Yafuflash -kcs rom.ima -preserve-fru -preserve-snmp -ignore-existing-overrides

Description: This command starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg14:

- Yafuflash -kcs -img-select 0 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15:

- Yafuflash -kcs -img-select 1 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16:

- Yafuflash -kcs -img-select 2 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg17:

- Yafuflash -kcs -img-select 3 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg18:

- Yafuflash -kcs -split-img boot.ima

Description: This command works with KCS medium to flash the boot split image.

Eg19:

- Yafuflash -ksc -split-img root.ima

Description: This command works with KCS medium to flash the root split image.

Eg20:

- Yafuflash -ksc rom.ima -flash-root -flash-conf

Description: This command works with KCS medium to flash the root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom. ima.

Eg21:

- Yafuflash -ksc boot.ima -split-img -flash-boot

Description: This command works with KCS medium to flash the root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg22:

- Yafuflash -ksc root.ima -split-img -flash-www -flash-osimage

Description: This command works with KCS medium to flash www and osimage from root. ima split image. --flash-<xxx>, where xxx specifies the modules in root.ima.

Eg23:

- Yafuflash -ksc rom.ima -preserve-exlog

Description: This command works with KCS medium to preserve extended log configuration.

Eg24:

- Yafuflash -ksc root.ima -split-img -preserve-exlog

Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg25:

- Yafuflash -ksc root.ima -d 1 rom.ima

Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg26:

- Yafuflash -ksc root.ima -d 1 root.ima -split-img

Description: This command works with KCS medium to flash the split image on specific peripheral device.

Eg27:

- Yafuflash -nw-ip 155.166.132.12 -u admin -p admin -bu root.ima

Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Eg 28:

- Yafuflash -nw -ip 155.166.132.12 -u admin -p admin rom.ima -netfn 0x36

Description: This command works with network medium to flash the image using 0x36 as AMI OEM Net Function instead of default AMI OEM Netfn 0x32

18.2 VMCLI Tool

VMCLI (Virtual Media Command Line Interface)

The Virtual Media Command Line Interface (VMCLI) utility is a scriptable command-line interface that provides virtual media features from the management station to the Host.

VMCLI is used to redirect the virtual media (Hard Disk, Floppy, CD drive, USB..) from the management station to the host.

> **NOTE**
> VMCLI Tool uses wget tool to communicate with webserver which runs inside BMC in order to fetch media server related configurations.
> Wget windows tool supports IPv6 link local ip too but Wget Linux tool doesn't support.

Features

- Removable media devices or image files that are consistent with the Virtual Media plug-ins.
- Automatic termination when the host firmware boot once option is enabled.
- Secure communication to the host using Secure Sockets Layer (SSL).
- VMCLI utility can run as a service as well as application.

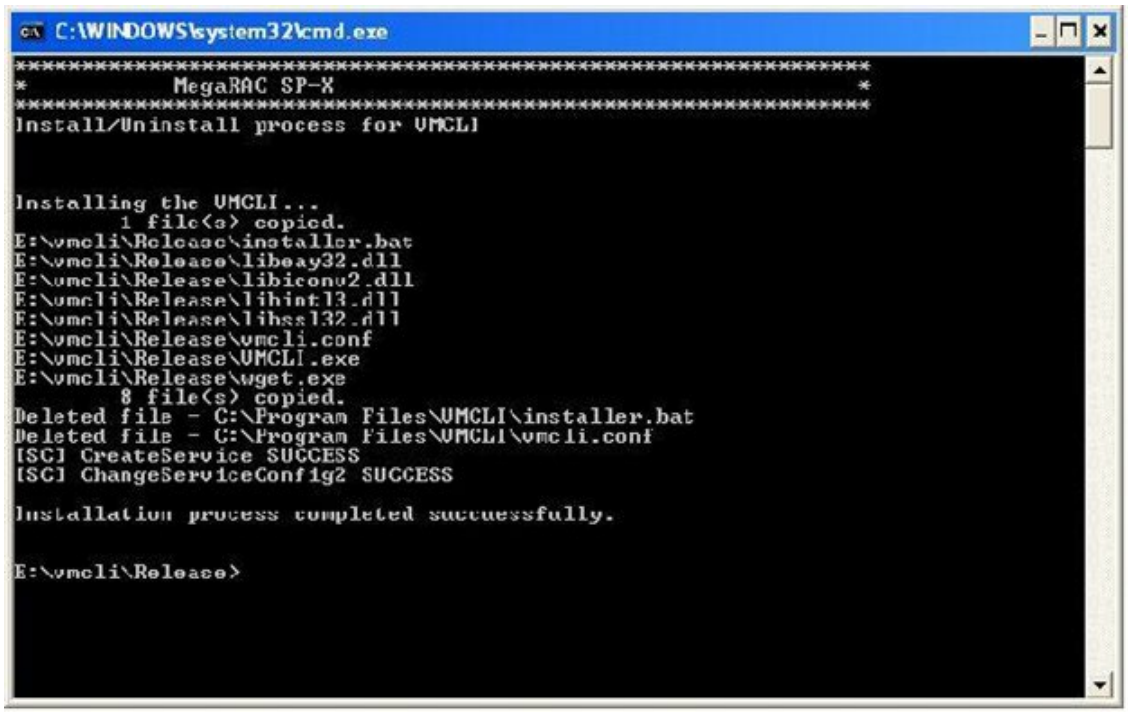
18.2.1 Installation in Windows

> **NOTE**
> Windows VMCLI requires "**Microsoft Visual C++ Redistributable Package**" to be installed in windows client.

1. VMCLI can be installed in windows using batch file, **installer.bat** in VMCLI folder.

> **NOTE**
> You must keep **wget** inside the VMCLI Folder, which is the support Tool for VMCLI.

2. Go to VMCLI folder and execute the installer script to install the VMCLI service.
   - Installer. bat -i



3. Installer script will add the VMCLI as windows service and user can start and stop the service using **sc command**.
4. To start VMCLI utility as service.

A. To start VMCLI utility as service using command line argument

Format:

- sc start VMCLI [-r][IP : Web-SSLPort] [-u][USER] [-p] [PASSWORD] [MEDIA TYPE] [MEDIA][-e]

B. To start as an application using command line argument

Format:

- VMCLI.exe [-r][IP : Web-SSLPort] [-u][USER] [-p] [PASSWORD] [MEDIA TYPE] [MEDIA][-e]

C. To start VMCLI using a configuration file

VMCLI Configuration fields to start CD redirection.

 # In vmcli.conf file
[config]
ipaddr = **[IP]**
username = **[USER]**
password = **[PASSWORD]**
port = **[Web-SSLPort]**
encryption = **[1/0]**
cdredirect = **[MEDIA]**
hdredirect =

VMCLI configuration fields to start HD redirection

 # In vmcli.conf
[config]
ipaddr = **[IP]**
username = **[USER]**
password = **[PASSWORD]**
port = **[Web-SSLPort]**
encryption = **[1/0]**
cdredirect =
hdredirect = **[MEDIA]**

D. To start as service

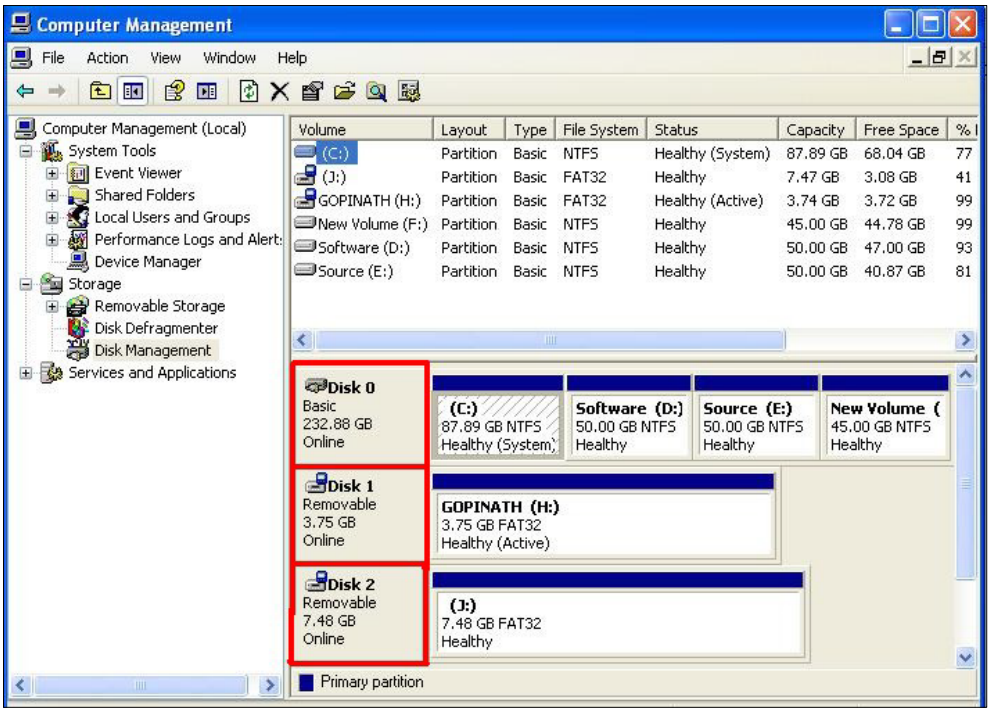
Format:

- sc start VMCLI

E. To start as application

Format:

- VMCLI.exe



Screen: Media Drive

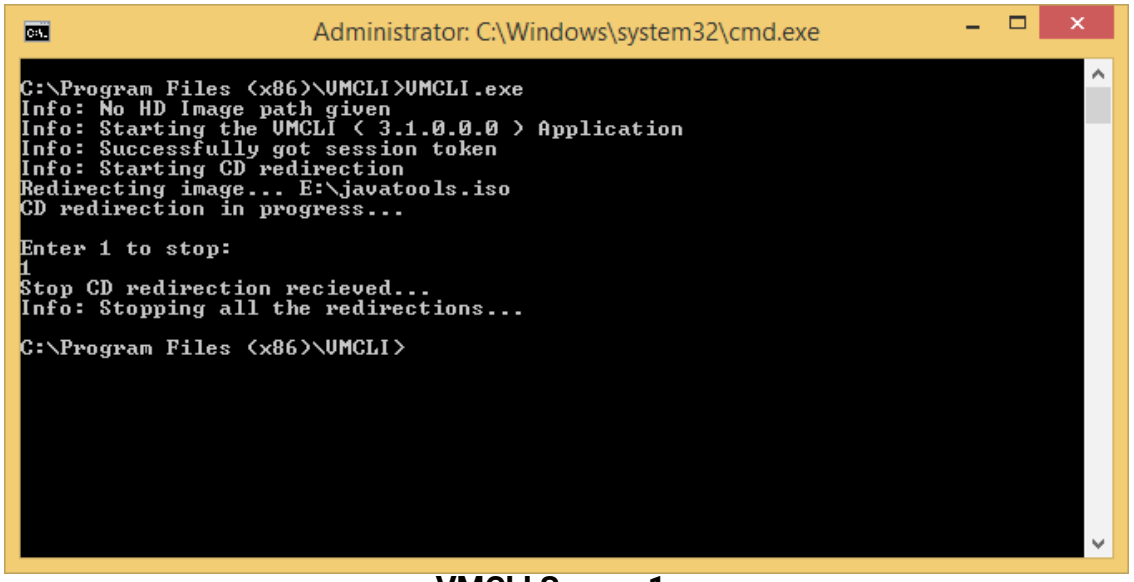
5. **To Stop the VMCLI service**

Format:

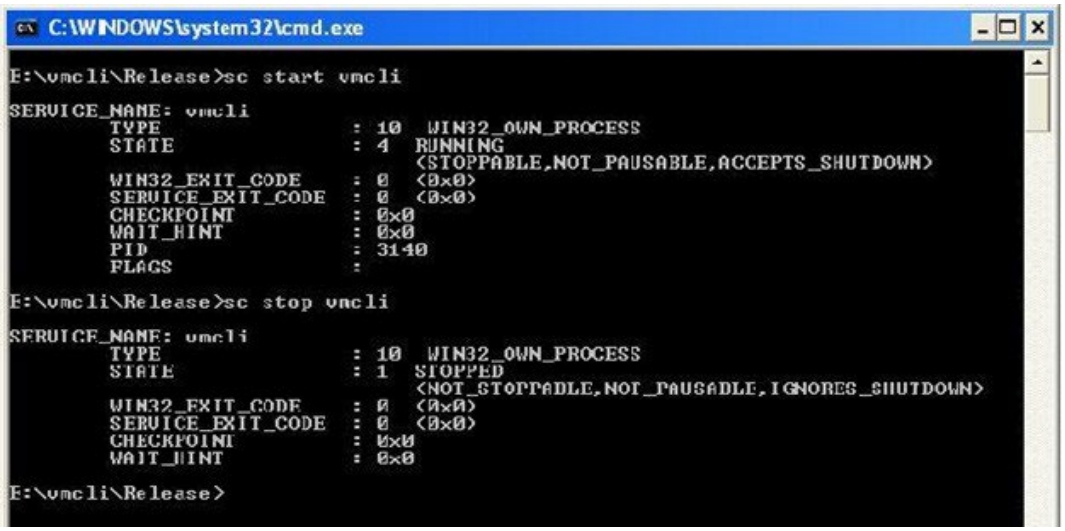
- sc stop VMCLI

To stop the VMCLI application

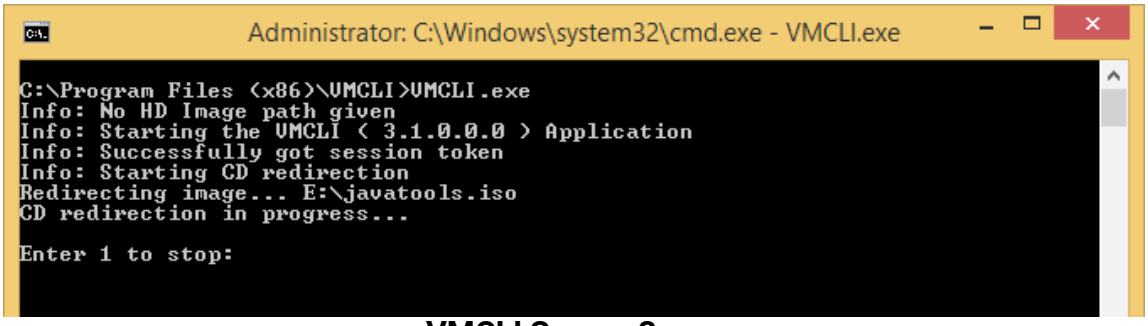
Format: Press 1 and enter to stop the application. (Reference VMCLI Screen 1)



VMCLI Screen 1



VMCLI Screen 2



VMCLI Screen 3

The above **VMCLI Screen 2** starts VMCLI service without command line argument, i.e, configuration will be read from conf file.

The above **VMCLI Screen 3** starts VMCLI application without command line argument, i.e, configuration will be read from conf file.

NOTE

If you would like to surround an argument by double quotation marks ("), please notice that a double quotation mark proceeded by a backslash, \", is interpreted as a literal double quotation mark. You have to use a pair of backslash (\\) followed by a double quotation mark, \\", let the double quotation mark interpreted as a string delimiter.

https://msdn.microsoft.com/en-us/library/a1y7w461.aspx

i.e.:

sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -c "E:\" ⇨ incorrect (X)

sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -c "E:\\" ⇨ correct (O)

Examples of CD-ROM Media redirection

Eg1:

VMCLI as service

IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -c E:\

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -c E:\

VMCLI as application

IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -c E:\

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c E:\

Description: This command is to redirect the CD/DVD drive from the management station to the host.

Eg2:

VMCLI as service

IPv4: sc start VMCLI r 10.0.6.8:443 -u admin -p admin -c E:\ -e

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -c E:\ -e

VMCLI as application

IPv4: VMCLI.exe r 10.0.6.8:443 -u admin -p admin -c E:\ -e

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c E:\ -e

Description: This command is to redirect the CD/DVD drive from the management station to the host. Data will be transfer through ssl.

Eg3:

VMCLI as service

IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -c “/home/cdrom.iso”

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -c “/home/cdrom.iso”

VMCLI as application

IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -c “/home/cdrom.iso”

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c “/home/cdrom.iso”

Description: This command is to redirect the CD image from the management station to the host. The image file path is full system path.

Eg4:

- sc stop VMCLI

Description: This command is used to stop the VMCLI service to stop the redirection.

NOTE

If you would like to surround an argument by double quotation marks ("), please notice that a double quotation mark proceeded by a backslash, \", is interpreted as a literal double quotation mark. You have to use a pair of backslash (\\) followed by a double quotation mark, \\", let the double quotation mark interpreted as a string delimiter.

https://msdn.microsoft.com/en-us/library/a1y7w461.aspx

i.e.:

sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\" ⇨ incorrect (X)

sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\\" ⇨ correct (O)

Examples of Hard Disk Drive Media redirection

Eg1:

VMCLI as service

IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd D:/

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd D:/

VMCLI as application

IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd D:/

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd D:/

Description: This command is to redirect the Hard disk drive from the management station to the host.

Eg2:

VMCLI as service

IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd D:/ -e

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd D:/ -e

VMCLI as application

IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd D:/ -e

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd D:/ -e

Description: This command is to redirect the Hard disk drive from the management station to the host. Data will be transfer through ssl/

Eg3:

VMCLI as service

IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”

IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd “/home/hd.img”

VMCLI as application

IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”

IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd “/home/hd.img”

Description: This command is to redirect the HD/USB image from the management station to the host. The image file path is full system path.

Eg4:

- sc stop VMCLI

Description: This command is used to stop the VMCLI service to stop the redirection.

18.2.2 Installation in Linux

> **NOTE**
> VMCLI uses TLSv1.2 so it needs **openssl1.0.0** (or above) and **wget1.16** (or above) to work properly.

The following steps are mentioned for openssl1.0.0 package. If anyother version is installed the steps will vary.

For example if openssl1.0.1 is installed then the libssl.so will have libssl.so.1.0.1 and libcryto file name will also be libcrypto.so.1.0.1 etc.

1. Search libssl.so.1.0.0 and libcrypto.so.1.0.0 locate at /usr/lib (if it's not available in /usr/lib, try searching in /usr/lib64) or not. If not, do yum install openssl libssl or rpm -ivh openssl.rpm and rpm -ivh libssl.rpm:
   - ls -l /usr/lib/libssl*
   - ls -l /usr/lib/libcrypto*

> **NOTE**
> For Ubuntu look in the path /lib/x86_64-linux-gnu or /lib/i386-linux-gnu

2. Create a force link as libssl.so.1.0.0 to libssl.so.10:
   - ln -sf libssl.so.1.0.0 libssl.so.10
3. Create a force link as libcrypto.so.1.0.0 to libcrypto.so.10:
   - ln -sf libcrypto.so.1.0.0 libcrypto.so.10
4. Open Terminal and go to **VMCLI folder**
5. Install the VMCLI service in Linux system using installer script
   - sudo bash ./installer.sh -i
6. To start VMCLI utility using command line arguments.

A. To start as service

Format:

- service vmcli start [-r] [IP:Web-SSLPort] [-u] [USER] [-p][PASSWORD] [MEDIATYPE] [MEDIA] [-e].

B. To start as application

Format:

- VMCLI.EXE [-r] [IP:Web-SSLPort] [-u] [USER] [-p][PASSWORD] [MEDIA TYPE] [MEDIA] [-e].

C. To start VMCLI using a configuration file

VMCLI Configuration fields to start CD redirection.

 # In vmcli.conf file
[config]
ipaddr = **[IP]**
username = **[USER]**

password = **[PASSWORD]**
port = **[Web-SSLPort]**
encryption = **[1/0]**
cdredirect = **[MEDIA]**
hdredirect =

VMCLI configuration fields to start HD redirection

 # In vmcli.conf
[config]
ipaddr = **[IP]**
username = **[USER]**
password = **[PASSWORD]**
port = **[Web-SSLPort]**
encryption = **[1/0]**
cdredirect =
hdredirect = **[MEDIA]**

D. To start as service

Format:

- service VMCLI start

E. To start as application

Format:

- VMCLI.exe

7. **To stop the VMCLI service**

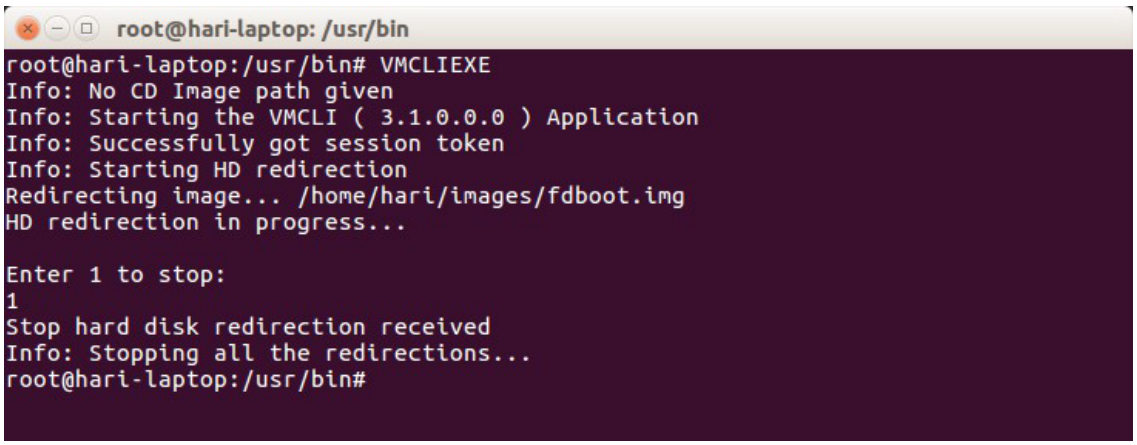
Format:

- service stop vmcli

To stop the VMCLI application

Format:

- Press 1 and enter to stop the application. (Reference VMCLI Screen 4)



VMCLI Screen 4

```
root@sengud-vpn:/home/gopi/Linux_x86_32
[root@sengud-vpn Linux_x86_32]# service vmcli start
Starting the VMCLI Service
[root@sengud-vpn Linux_x86_32]# service vmcli stop
Stopping the VMCLI Service
[root@sengud-vpn Linux_x86_32]#
```

VMCLI Screen 5

```
root@hari-laptop: /usr/bin
root@hari-laptop:/usr/bin# VMCLIEXE
Info: No CD Image path given
Info: Starting the VMCLI ( 3.1.0.0.0 ) Application
Info: Successfully got session token
Info: Starting HD redirection
Redirecting image... /home/hari/images/fdboot.img
HD redirection in progress...

Enter 1 to stop:
```

VMCLI Screen 6

The above VMCLI Screen 5 starts VMCLI service without command line argument, i.e, configuration will be read from conf file.

The above VMCLI Screen 6 starts VMCLI application without command line argument, i.e, configuration will be read from conf file.

Examples of CD-ROM Media redirection

Eg1:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8:443 -u admin -p admin -c /dev/sdc

IPv6 : service vmcli start -r [2004::2000] :443 -u admin -p admin -c /dev/sdc

VMCLI as application

IPv4 :VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -c /dev/sdc

IPv6 :VMCLIEXE -r [2004::2000] :443 -u admin -p admin -c /dev/sdc

Description: This command is to redirect the CD/DVD drive from the management station to the host.

Eg2:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8:443 -u admin -p admin -c“/home/cdrom.iso”

IPv6 : service vmcli start -r [2004::2000] :443 -u admin -p admin -c “/home/cdrom.iso”

VMCLI as application

IPv4 :VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -c“/home/cdrom.iso”

IPv6 :VMCLIEXE -r [2004::2000] :443 -u admin -p admin -c “/home/cdrom.iso”

Description: This command is to redirect the CD/DVD image from the management station to the host. The image file path is full system path.

Eg3:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8 :443 -u admin -p admin -c CD-RomImage.iso -e

IPv6 :service vmcli start -r [2004::2000] :443 -u admin -p admin -c CD-RomImage.iso -e

VMCLI as application

IPv4 : VMCLIEXE -r 10.0.6.8 :443 -u admin -p admin -c CD-RomImage.iso -e

IPv6 :VMCLIEXE -r [2004::2000] :443 -u admin -p admin -c CD-RomImage.iso -e

Description: This command is to redirect the CD/DVD image from the management station to the host. Data will be transfer through ssl.

Eg4:

service vmcli stop

Description: This command is used to stop the vmcli service to stop the redirection.

Examples of Hard Disk Drive Media redirection

Eg1:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8:443 -u admin -p admin -hd /dev/sda

IPv6 : service vmcli start -r [2004::2000] :443 -u admin -p admin -hd /dev/sda

VMCLI as application

IPv4 : VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -hd /dev/sda

IPv6 : VMCLIEXE -r [2004::2000] :443 -u admin -p admin -hd /dev/sda

Description: This command is to redirect the Hard disk drive from the management station to the host.

Eg2:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”

IPv6: service vmcli start - r [2004::2000] :443 -u admin -p admin -hd “/home/hd.img”

VMCLI as application

IPv4 : VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”

IPv6: VMCLIEXE - r [2004::2000] :443 -u admin -p admin -hd “/home/hd.img”

Description: This command is to redirect the HD/USB image from the management station to the host. The image file path is full system path.

Eg3:

VMCLI as service

IPv4 : service vmcli start -r 10.0.6.8 :443 -u admin -p admin -hd /dev/sda -e

IPv6 : service vmcli start -r [2004::2000] :443 -u admin -p admin -hd /dev/sda -e

VMCLI as application

IPv4 : VMCLIEXE -r 10.0.6.8 :443 -u admin -p admin -hd /dev/sda -e

IPv6 : VMCLIEXE -r [2004::2000] :443 -u admin -p admin -hd /dev/sda -e

Description: This command is to redirect the Hard disk drive from the management station to the host. Data will be transfer through ssl.

Eg4:

service vmcli stop

Description: This command is used to stop the vmcli service to stop the redirection.

Configuration File Support

VMCLI service is started with no command VMCLI supports the configuration file to pass the argument to the VMCLI service. The VMCLI service will read the configurations from the file, if the VMCLI service is started with no command line argument.

Example:

Service

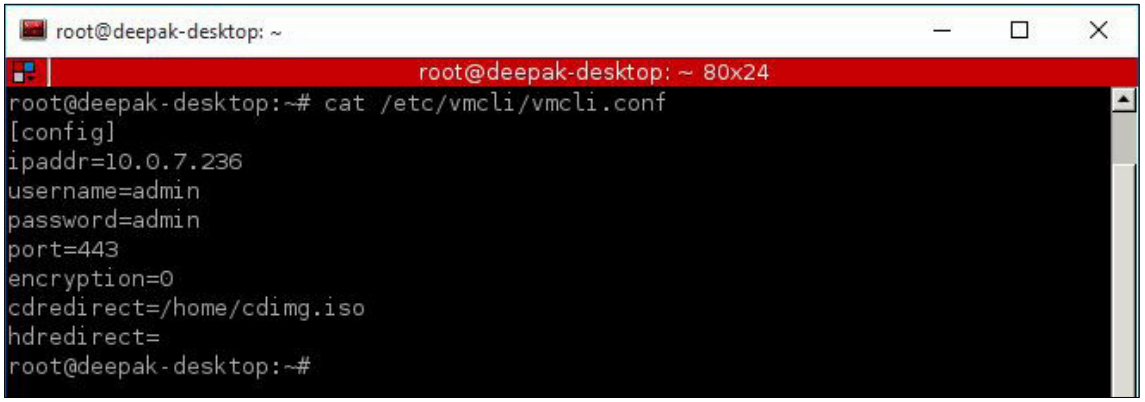
- service vmcli start [Linux] – filename is /etc/vmcli/vmcli.conf
- sc start vmcli [Windows] – filename is C:\WINDOWS\vmcli.conf

Application

- VMCLIEXE [Linux] – filename is <same path as vmcli binary>\vmcli.conf
- VMCLI.exe [Windows] – filename is <same path as vmcli binary>\vmcli.conf

Log file support is added to VMCLI service. The VMLCI service's start and stop information can be logged into this file (/var/log/vmcli or C:\WINDOWS\vmcli).

> **NOTE**
> VMCLI service will not be started if the command line arguments or configuration file are not configured properly.
> In Latest versions of Linux, the system in it system requires a service unit file to manage the services and it doesn't accept arguments. Hence configuration file is necessary to pass the arguments to the VMCLI service. It is mandatory for the user to fill the required arguments in the configuration file.



List of Supported OS

Kindly refer Client OS (64-bit) section in ***Chapter 21 KVM OS and Browser Compatibility***.

Chapter 19. LINUX OS Installation with nomodeset

LINUX OS Installation Post CVE 2019-6260 Mitigation Fix on AST SOC

After the CVE 2019-6260 fix in Aspeed SOC, Linux OS installation fails frequently. While booting into the installation media when the kernel tries to load the video driver module, the video driver crashes leading to kernel dump. Thus, the installation process fails.

As a work around for this issue, Aspeed suggested to use the nomodeset option in the GRUB, before booting into the installation medium for the new installation.

A few of the supported Linux operating systems for which we tried this option and the procedure is explained in this document.

Before proceeding with the OS installation, make sure the VBIOS version is v.1.09 or later.

19.1 SLES 12.x

To install OS using nomodeset, please follow the below steps.

1. On the Installation screen, click “e” to enter GRUB mode.
2. Add “nomodeset” before “splash=silent” in the line that starts with linuxefi. Adding the nomodeset parameter instructs the kernel to not load video drivers and use BIOS modes instead until X is loaded.
3. Clicking “e” key enables the user to edit a menu entry. This will bring up an openSUSE Leap GRUB screen as displayed in the below screenshot.

openSUSE Leap GRUB Screen

4. Use the arrow keys to navigate when screen editing is required. Navigate to the line on this screen that starts with linuxefi.

5. Replace splash=silent by nomodeset splash=silent. This change is only temporary — it will just be used once and GRUB won't remember it in the future.

6. Press Ctrl+X or F10 to boot with the nomodeset option which was added. If you make a mistake, press Esc to go back to the previous screen.

7. To make the change permanent, the user needs to add it to the /etc/default/grub file. Append nomodeset inside the quotes of the line GRUB_CMDLINE_LINUX_DEFAULT="...". Then update the GRUB settings with sudo update-grub.

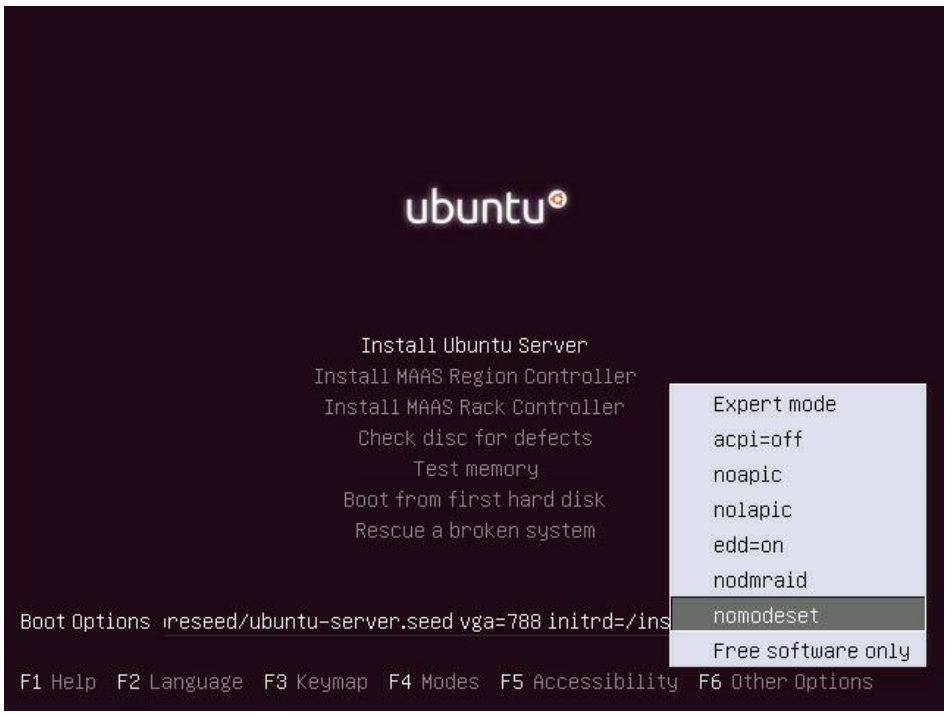
19.2 Ubuntu 14.04.x and Ubuntu 16.04.x

To install OS using nomodeset, please follow the below steps.

1. To perform installation, Boot into the installation media.
2. From the start Installation screen, click “F6” for Other Options.

Ubuntu Installation Screen

3. Select nomodeset option from the list. A sample screenshot is displayed below.



4. Click Enter to make the selection as displayed in the screenshot as below.

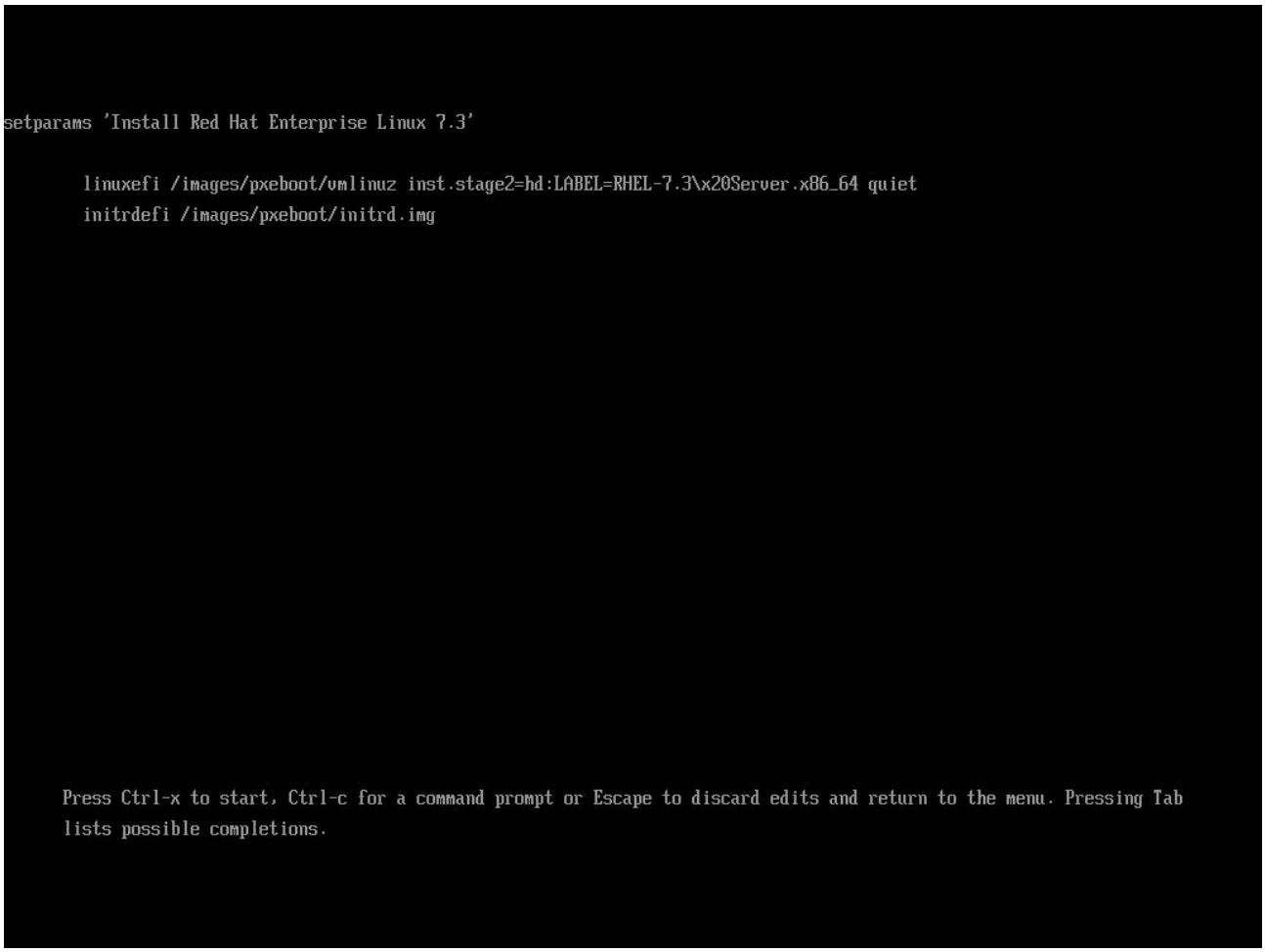
Ubuntu Installation Screen

5. And then it continues with the installation.

19.3 RHEL 6.9 and 7.3

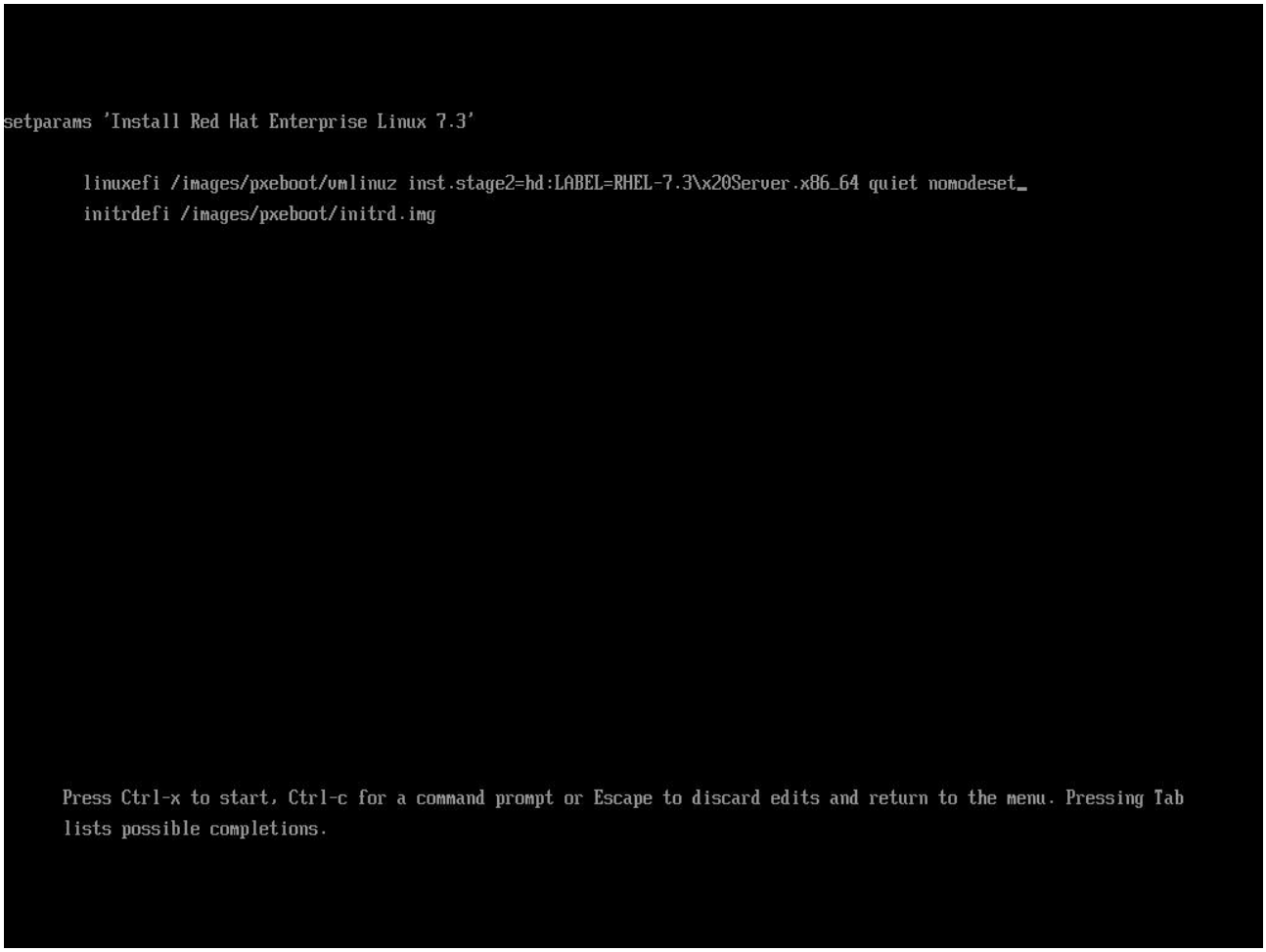
To install OS using nomodeset, please follow the below steps.

1. Click “E” while booting to the installation media.
2. This action displays the setparams option in the screen to edit bootparams. A sample screenshot is displayed below.



RHEL GRUB Screen

3. Include nomodeset in the first line of the screen as shown in the below screenshot. For RHEL 6.9 installation, options “xdriver=vesa brokenmodules=ast” should be added in addition to “nomodeset”. So if installation doesn’t work with “nomodeset” option, add “xdriver=vesa brokenmodules=ast” along with “nomodeset” and try installation.



RHEL with nomodeset

4. And then it continues with the installation.

Chapter 20. SOL (Serial Over LAN)

One of the powerful tools in IPMI is Serial Over LAN (SOL) which provides serial line access over the management LAN. The baseboard management controller (BMC) microcontroller embedded on the server motherboard does this by redirecting information destined for the serial port over to the LAN. With SOL console redirection system administrators can remotely view the text-based console on their remote servers from anywhere and perform any task that doesn't require a GUI.

Transporting serial data over IP networks using telnet, serial over IP, SOL and the likes is the way forward for server serial communications. Just as the KVM functions in embedded service processors is displacing the need for external KVM appliances, so the SOL capability of BMCs and console redirection in service processors is reducing the need for serial console servers for server console management.

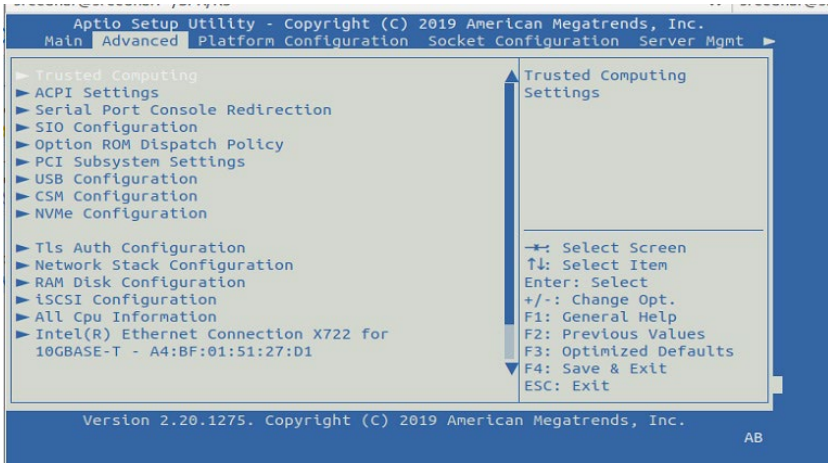
One other feature to capture SOL data over SSH connection other than the IPMI tool is SOLSSH.

SOLSSH: It is an application that enables to capture the host logs of the server over the SSH/TELNET connection. The functionality of the SOLSSH is the same as SOL except it redirects data over SSH/TELNET session. it will read the data from the serial port configured and redirects to the user session.

To launch the SOLSSH session follow the below-mentioned steps.

1. Create a new user under **Settings** → **User Management** in UI, because the fixed users are configured to launch fixed services.
2. Log in to BMC over SSH with the new user using command 'ssh <username>@<BMC IP>'
3. Enter the password when prompts.
4. A session will be created and will be provided to the user through this a user can control the server remotely.

Example: setting the BIOS settings of the server over SOLSSH service.



BIOS Screen

Chapter 21. KVM OS and Browser Compatibility

This section lists out the supported KVM OS and Browsers Compatibility.

H5Viewer OS & Browser Compatibility	
Host OS (Server Edition 64-bit)	• Ubuntu Server LTS 20.04.6, 22.04.1 • Windows Server 2019, 2022 • RHEL Server 8.8, 9.2 • Cento OS Stream 8 (22.11.2022), 9 (23.11.2022) • SLES 15 SP4, SLES 12 SP5
Host VGA Driver	• Windows - v1.15.01 • Linux - v1.14.2
VBIOS	• v1.13.01
Client OS (64-bit)	• Ubuntu LTS 20.04, 22.04 • macOS 10.13.6 • Windows 10, 11 • Fedora 38
Web Browser (64-bit)	Chromium Edge • Windows – v121.0.2277.83 Chrome • Windows – v119.0.6045.159 • Linux – v119.0.6045.105, v121.0.6167.85 Firefox • Linux – v116.0.2, v122.0 Safari • MacOS - v13.1.2

- On Pilot IV with Linux host, some performance issues might happen if valid PilotIV video driver not installed. Please make sure kernel update has been executed to avoid such issues.
- Suggests users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode.

NOTE

- It is mandatory to use server edition as HOST OS. If Client OS version is used as HOST OS then KVM will not work as expected.
- ASPEED VGA driver should be installed in HOST OS. Please download and install the appropriate ASPEED driver from *https://www.aspeedtech.com/support_driver/* website.
- If there is continuous full screen update in the host, the video shown in KVM client will not be in proper sync with host video.

H5Viewer Browser Limitations

All Browser Limitations:

- To use secure H5Viewer session adding SSL certifificate to the browser is mandatory.
- H5Viewer video record length (Client-side video recording length set by the user) will diffffer from downloaded video fifile duration. ThThe recorded video duration depends on the browser, and the amount of host video update.
- Keyboard LED sync will not work, when the host is Linux text console.
- Clearing H5Viewer session will take some time when user abruptly closes the H5Viewer window.
- If any dialog (like File Choose, Confifirmation dialog, etc) in H5Viewer is kept open and not closed, then the background functionalities of threads might get affffected leading to H5Viewer reconnect or connection close.
- ThThe H5Viewer video may flflicker occasionally when there is fading animation in the Host video. ThThis can result in the H5Viewer video output becoming unsynchronized with the host video.
- Browsers use optimization techniques to save resources when a tab is not in use. ThThis helps improve the performance of the system by reducing the amount of memory and CPU power used. However, these optimizations can sometimes cause a KVM timeout, especially if the browser thinks that the KVM tab is not being used. Disabling these options in the browser could help with KVM timeout.
    - Ex: For edge browser disable “Save resources with sleeping tabs”
    - For Chrome disable “Probabilistic Memory Saver Mode” and “Memory Saver”.
    - For Firefox disable “Tab Unloading”.

Google Chrome:

- On launching H5Viewer window won’t resize to the client resolution.

Firefox:

- Only Japanese QWERTY input method will work, Japanese hiragana or katakana input method will not work.

Safari:

- Keyboard LED sync will not work.
- To use secure H5Viewer session adding SSL certifificate to the browser is mandatory.

Chapter 22. OTP (One Time Password)

OTP Support for Password Reset

OTP mechanism is used to generate temporary password. Forgot Password option in Log-in Page Web UI can be used to generate OTP which will be sent to already configured e-mail ID. This generated temporary password will be valid for only 5 minutes.

Initial access of Web UI prompts you to enter the User Name and Password.

A sample screenshot of the login screen is given below.

Login Page

The fields are explained as follows:

Username: Enter your username in this field.

Password: Enter your password in this field.

Language Selection: Language selection drop-down will be populated based on supported languages in Web UI as a part of multi language support feature. Drop-down option value will be selected based on the browser language. For example, if browser language is configured with Simplified Chinese language (ZH-CN), then option value will be auto selected as China - 中文 (简体).

Default language will be selected as US-English if the browser configured language not supported by Web UI. Entire Web UI pages language strings will be displayed based on selected language from drop-down.

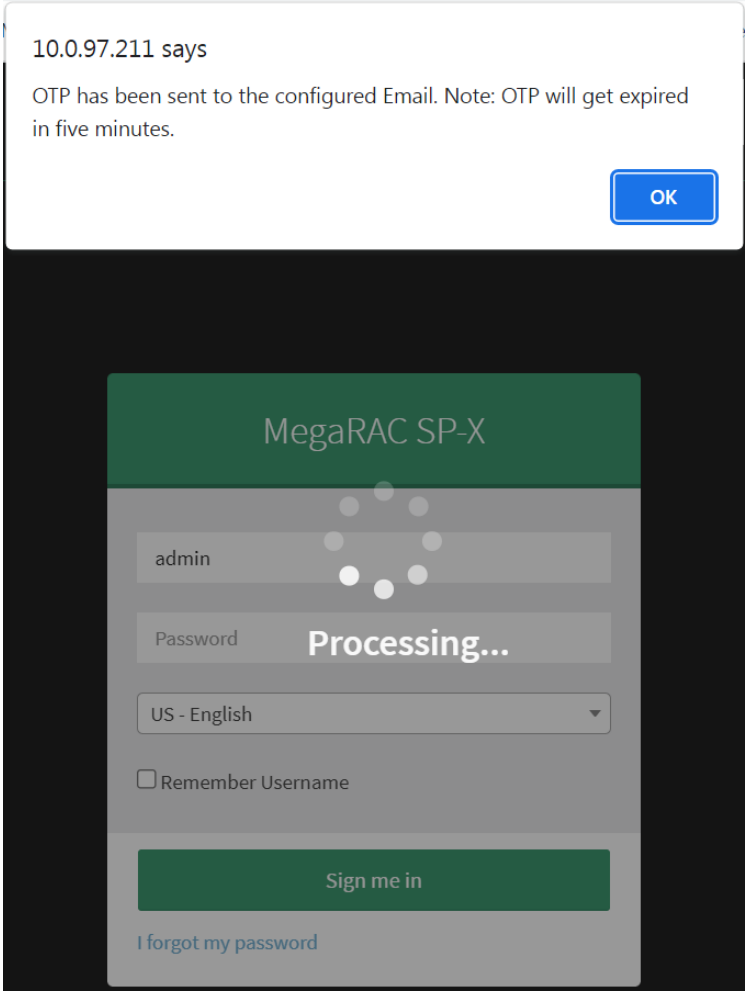
Remember Username: Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.

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 password using this link.

Procedure to Reset Password

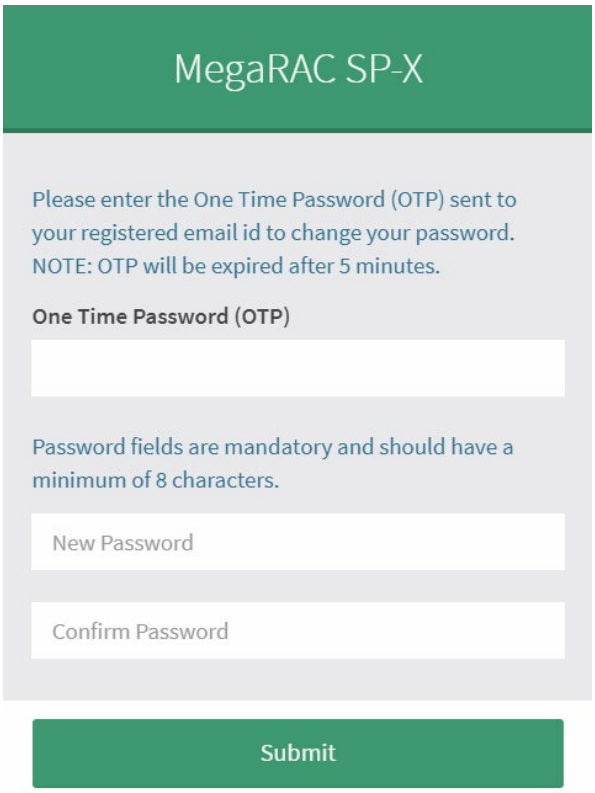
1. Enter the **Username**, and click on **Forgot Password** link. A pop-up message will prompt you to proceed further, click **OK** to proceed. A sample screenshot is given below.



Login Page - Forgot Password

2. Enter **One Time Password (OTP)** sent to your registered Email-ID for changing the password, and also enter a password in the **New Password** and **Confirm Password** fields. And then click **Submit**. A sample screenshot is given below.

> **NOTE**
> OTP will be expired after 5 minutes.



Login Page - OTP

3. Once all the above steps are success, your password will be reset.

NOTE

- Default password should contain minimum of 8 and maximum of 16 alphanumeric characters.
- White space is not allowed.

Chapter 23. Thermal Management Support

The thermal Management module resides in BMC, which ensures that appropriate temperature/heat level and airflow is maintained in the server. The thermal management module by default provides efficient “Range Based thermal algorithm”.

It uses a pre-configured zones and fan speed profiles. A zone is a logical grouping of the temperature sensor and fans. This grouping is to say which all fans will be controlled based on the particular temperature sensors values.

For Example, we have the following pre-configured zones:

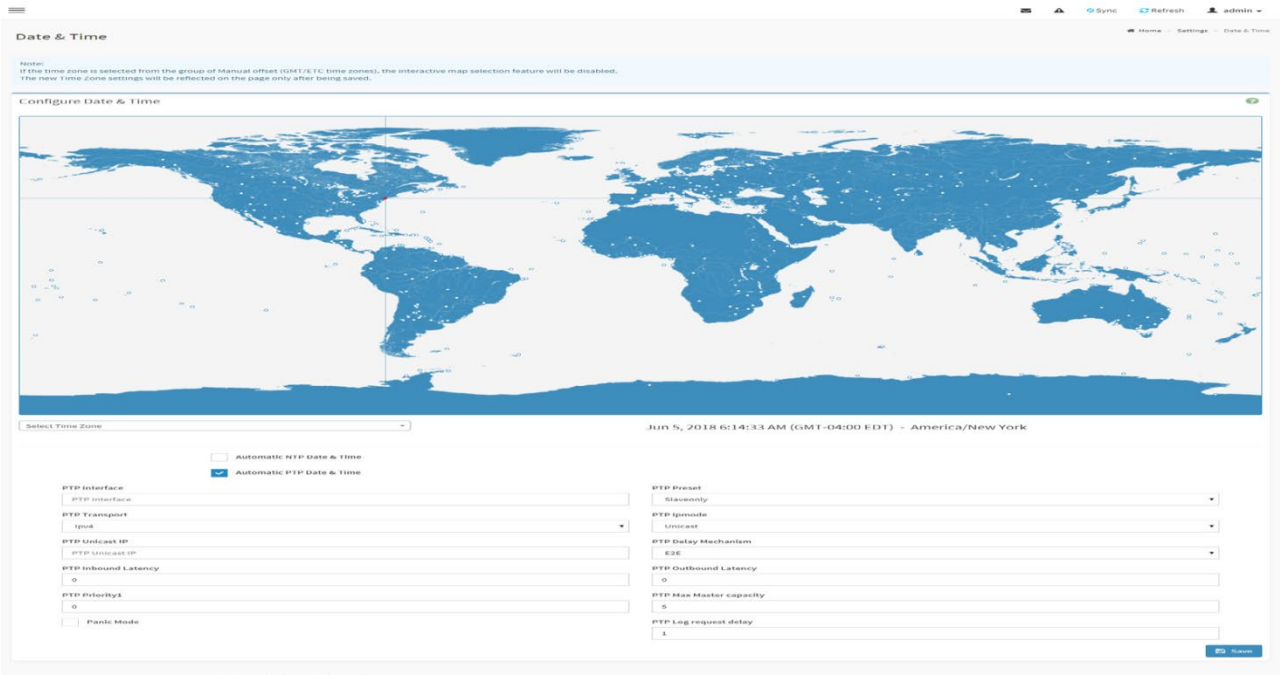
Now based on the maximum temperature in a particular zone, the equivalent fan duty cycle will be calculated using the fan speed profile configurations and applied to the Fans present in that zone.

Whenever there is a change in the maximum temperature in a particular zone, the corresponding Fan speeds also gets varied.

Chapter 24. PTP IEEE 1588 support

Using PTP (IEEE 1588) daemon to sync the time with Master time server. This field is used to set the date and time on the BMC.

A sample screenshot of **Automatic PTP** Date & Time is shown as below.



Date&Time - Automatic PTP Date & Time

The Date & Time section consists of the following fields.

Configure Date & Time: Displays Timezone 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 PTP Date & Time: To enable/disable the use of PTP servers to automatically set the date and time.

- **PTP Interface**: To confifigure a PTP server interface to use when automatically setting the date and time.
- **PTP Preset**: To confifigure a PTP Preset type to use when automatically setting the date and time.
- **PTP Transport**: To confifigure a PTP Transport type to use when automatically setting the date and time.
- **PTP Ipmode**: To confifigure a PTP Ipmode type to use when automatically setting the date and time.
- **PTP Unicast IP**: To confifigure a Unicast ip when ipmode is unicast and server to use when automatically setting the date and time.

- **PTP Delay Mechanism**: To confifigure a PTP Delay Mechanism type to use when automatically setting the date and time.
- **PTP Inbound Latency**: To confifigure a Inbound latency of the server to use when automatically setting the date and time.
- **PTP Outbound Latency**: To confifigure a PTP outbound latency server to use when automatically setting the date and time.
- **PTP Priority1**: To confifigure a priority of PTP clock to use when automatically setting the date and time.
- **PTP Max Master capacity**: To confifigure a max master capacity of the PTP clock to use when automatically setting the date and time.
- **Panic Mode**: To confifigure a PTP clock to not reset if jump is more then 1 second, use when automatically setting the date and time.
- **PTP Log request delay**: To confifigure a PTP log request delay,use when automatically setting the date and time.

Save: To save the settings.

> **NOTE**
> If the timezone is selected as Manual Offset, the map selection will be disabled. The Time-Zone settings will be reflected only after saving the settings.

Procedure

1. Select the **Timezone** location either using drop down or Map.
2. Enable **Automatic PTP Date & Time** to enable/disable the use of PTP servers to automatically set the date and time.
   A. Enter the Interface, Preset, Transport, Ipmode, Unicast IP, Delay Mechanism, Inbound Latency, Outbound Latency, Priority1, Max Master capacity and Log request delay details in their corresponding fields.
   B. Enable/Disable **Panic Mode** to not reset if jump is more then 1 second, use when automatically setting the date and time.
3. Click **Save** button to save the settings.

Chapter 25. Web Privileges

Each page of the web exposes IPMI commands in a UI format. The underlying IPMI commands the minimum requirements for that page or it will not show. Some of the pages require a higher privilege for modification of the contents on the page, so they will appear read-only to a user of insufficient privileges. Other pages are read-only to all users because they are informational only and do not contain any user-modifiable content.

A = Administrator only
O = Operator or higher
U = User or higher
N/A = read-only page.

S.No	Main Menu	Sub Menu	View	Change
1	Dashboard	Dashboard	U	N/A
2	Sensors	Sensor Reading > Sensor detail	U	O
3	Sensors	Sensor Detal > Sensor Thresholds	O	O
4	FRU	FRU	U	N/A
5	Logs & Reports	Logs & Reports > IPMI Event Log	U	O
6	Logs & Reports	Logs & Reports > System Log	U	N/A
7	Logs & Reports	Logs & Reports > Audit Log	U	N/A
8	Logs & Reports	Logs & Reports > Video Log	U	O
9	Settings	Settings > Captured BSOD	U	N/A
10	Settings	Settings > Date & Time	U	A
11	Settings	Settings > External User Services	U	U
12	Settings	Setings > External User Services > LDAP/E-	U	U
13	Settings	Settings > External User Services > LDAP/E-Directory Settings > General LDAP Settings	U	A
14	Settings	Settings > External User Services > LDAP/ E-Directory Settings > Role Groups	U	A
15	Settings	Settings > External User Services > Active directory Settings	U	A
16	Settings	Settings > External User Services > Active directory Settings > General Active Directory	U	A
17	Settings	Settings > External User Services > Active directory Settings > Role Groups	U	A
18	Settings	Settings > External User Services > RADIUS Settings	U	A
19	Settings	Settings > External User Services > RADIUS Settings > General RADIUS Settings	U	A
20	Settings	Settings > External User Services > RADIUS Settings > Advanced RADIUS Settings	U	A
21	Settings	Settings > KVM Mouse Setting	U	A

22	Settings	Settings > Log Settings	U	A
23	Settings	Settings > Log Settings > SEL Log Settings	U	A
24	Settings	Settings > Log Settings > Advanced Log Settings	U	A
25	Settings	Settings > Media Redirection	U	A
26	Settings	Settings > Media Redirection > General	U	A
27	Settings	Settings > Media Redirection > VMedia Instance Settings	U	A
28	Settings	Settings > Media Redirection > Remote Session	U	A
29	Settings	Settings > Media Redirection > Active Redirections	U	N/A
30	Settings	Settings > Network Settings	U	A
31	Settings	Settings > Network > Network IP Settings	O	A
32	Settings	Settings > Network > Network Bond Configuration	O	A
33	Settings	Settings > Network > Network Link Configuration	O	A
34	Settings	Settings > Network Settings > DNS Configuration	O	A
35	Settings	Settings > PAM Order	U	A
36	Settings	Settings > Platform Event Filters	U	A
37	Settings	Settings > Platform Event Filters > Event Filters	O	A
38	Settings	Settings > Platform Event Filters > Alert Policies	O	A
39	Settings	Settings > Platform Event Filters > LAN Destinations	O	A
40	Settings	Settings > Services	U	A
41	Services	Services > Service Sessions	U	A
42	Services	Services > Service Configuration	A	A
43	Settings	Settings > SMTP Settings	O	A
44	Settings	Settings > SSL Settings	U	A
45	Settings	Settings > SSL Settings > View SSL Certificate	U	N/A
46	Settings	Settings > SSL Settings > Generate SSL Certificate	U	A
47	Settings	Settings > SSL Settings > Upload SSL Certificate	U	A
48	Settings	Settings > System Firewall	U	A
49	Settings	Settings > Firewall > General Firewall Settings	U	A

50	Settings	Settings > Firewall > General Firewall Settings > Existing Firewall Settings	U	A
51	Settings	Settings > Firewall > General Firewall Settings > Add Firewall Settings	U	A
52	Settings	Settings > Firewall > IP Firewall Rules	U	A
53	Settings	Settings > Firewall > IP Oriented Firewall Rules > Existing IP Rules	U	A
54	Settings	Settings > Firewall > IP Oriented Firewall Rules > Add IP Rule	U	A
55	Settings	Settings > Firewall > Port Firewall Rules	U	A
56	Settings	Settings > Firewall > Port Oriented Firewall Rules > Existing Port Rules	U	A
57	Settings	Settings > Firewall > Port Oriented Firewall Rules > Add Port Rule	U	A
58	Settings	Settings > User Management	O	A
59	Settings	Settings > User Management > User Management Configuration	U	A
60	Settings	Settings > Video Recording	U	A
61	Settings	Settings > Video > Auto Video Settings	U	A
62	Settings	Settings > Video > Auto settings > Video Trigger Settings	U	A
63	Settings	Settings > Video > Auto settings > Video Remote Storage	U	A
64	Settings	Settings > Video > Auto settings > Pre-Event Video Recordings	U	A
65	Settings	Settings > Video > Sol Settings	U	A
66	Settings	Settings > Video > Sol > SOL Configurations	U	A
67	Settings	Settings > IPMI Interfaces	A	A
68	Remote Control	Remote Control	U	U
69	Image Redirection	Image Redirection	U	A
70	Image Redirection	Image Redirection > Local Media	U	A
71	Image Redirection	Image Redirection > Remote Media	U	A
72	Power Control	Power Control	U	O
73	Maintenance	Maintenance > Backup Configuration	U	A
74	Maintenance	Maintenance > BMC Recovery	A	A
75	Maintenance	Maintenance > Firmware Image Location	A	A
76	Maintenance	Maintenance > Firmware Information	U	N/A

77	Maintenance	Maintenance > Firmware Update	A	A
78	Maintenance	Maintenance > Preserve Configuration	U	A
79	Maintenance	Maintenance > Restore Configuration	U	A
80	Maintenance	Maintenance > Restore Factory Defaults	A	A
81	Maintenance	Maintenance > System Administrator	O	A

Chapter 26. Technical Support

www.aicipc.com

Taiwan, Global Headquarters

Address: No. 152, Section 4, Linghang N. Rd, Dayuan District, Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China

Address: Room 215, Building 4, No.471 Guiping Road, Xuhui District, Shanghai City, 200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia

Address: No. 500, 5th Floor, 5th Entrance, 32A, Khoroshevskoye Shosse, Moscow, 123007
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

Address: 48531 Warm Springs Boulvard Suite 404 Fremont, CA 94539, United States Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States

Address: 21808 Garcia Lane City of Industry, CA 91789, United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: +1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States

Address: 322 Route 46 West Suite 100 Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands

Address: Peppelkade 58, 3992AK, Houten, The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com

For additional technical support or questions about trouble shooting, please contact the AIC® representative nearest to you or visit our AIC® website for more information.
AIC® website: **https://www.aicipc.com/en/faq**.

Appendix

Ports Usage

Port #	Owner Module	Usage
80	Web server(lighttpd)	Listening for network connections on HTTP://
443	Web server(lighttpd)	Listening for secured network connections on HTTPS://
22	Secure Shell (sshd)	Secure SMASH-Lite session
23	Telnet	Telnet session
7578	KVM server (adviser)	To accept regular KVM redirection connections
623	IPMI	LAN interface
1900	uPnP discovery	Used for uPnP based BMC discovery
49153	uPnP discovery	Used for uPnP based BMC discovery
50000	uPnP discovery	Used for uPnP based BMC discovery
427	SLPD	Service Locater
123	NTP	Network Time Protocol (NTP) - used for time synchronization (UDP Connection)
161	SNMP	SNMP listens on this port for incoming SNMP requests. (UDP)
199	SNMP	SNMP listens on this port for incoming connect requests (from the SMUX peers and various other TCP end-points connected to SMUX peers to exchange SMUX PDUs)
546	DHCPv6	DHCPv6 clients listen for DHCP messages on this port (UDP)
5120	CD media server	To accept regular CD media redirection connections
5123	HD media server	To accept regular HD media redirection connections
5125	Intel ASD	Used for ASD server
2371	H5SOL Server(solagent)	To accept secure (SSL based) SOL redirection connections
514	syslog	Syslog is sent to the server through the default port

Mouse Mode

Host OS	Mouse Mode
Windows Server 2019 / 2016	Absolute
RHEL/CENTOS 8.0-8.2 / 7.6-7.8	Absolute
SLES 15 SP2 / 12 SP5	Absolute
Ubuntu Server 20.04 / 18.04	Absolute

NOTE
AIC suggests users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode. Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

KVM Sharing Scenario

KVM Client	KVM	Keyboard and Mouse	H5Viewer
Client 1 (Full Privilege)	Connected	Allowed	Allowed
Client 2 (Partial Privilege)	Connected	Not Allowed	Not Allowed

VMedia Sharing Scenario

NOTE
If MULTIPLE_USER_VMEDIA feature is disabled, then only one VMedia client can redirect media at a time. In the following table, KVM represents the video and H5Viewer represents the media redirection from the H5Viewer client.

Default IPMI Channel Numbers

Interface	Channel Number
Primary LAN Channel	0x01
Secondary LAN Channel	0x08
Serial Channel	0x02
Primary IPMB Channel	0x00
Secondary IPMB Channel	0x06
Third IPMB Channel	0x0a
System Interface	0x0f
SMM Interface	0x05
SSIF Channel	0x04
USB0 Channel	0x7
USB1 Channel	0x9

Secured Communication

- AD, LDAP, RADIUS based user authentication support
- Local IPMI user based authentication support
- Role/Privilege based authentication for each user for extra security
- Encrypted password support for AD/LDAP server authentication
- Single port access support for web/KVM/vMedia for enhanced security
- IPMI – Cipher suites support
- System Firewall support for IP/port level or IP/port range based blocking
- IPMI command/sub-command level firewall support
- TSIG authentication support for DNS
- OpenSSL based encryption – Latest OpenSSL 1.0.1 supported
- Key based Feature licensing/access support
- Secured handshaking support across concurrent KVM client sessions for controlled/seured access to the server
- SMTP-AUTH support

Service listings

Service	User Authentication	Encryption
Web	Yes	Openssl
KVM	Yes	Openssl
vMedia	Yes	Openssl
Standalone KVM Client	Yes	Openssl
SMASH	Yes	Openssl
SSL based SOL	Yes	Openssl
SNMP (v3)	Yes	SHA256, SHA384, SHA512, AES, DES
SSH	Yes	Openssl
IPMI	Yes	Please refer list of supported cipher suites
YAFUFLASH (Out of band)	Yes	Please refer list of supported cipher suites

NOTE
Currently only SHA256, SHA384 and SHA512 is supported. SHA and MD5 protocols are deprecated and can be used only if previously configured and preserved user has this protocol enabled.

Limitation of NCSI transfer

On the intel report we found that if the link speed was 1Gbps up to 5% of the packets were being retransmitted, but if the external link speed was 100Mbps transmit will be smooth. At network transmit, retransmits will much affect performance, because a packet is only retransmitted after a timeout occurs.

Hence when remote console tries to stream data at a physical link speed rate (1Gbps or 10Gbps) over an NC-SI interface capable of only 100Mbps. It will resulting in dropped packets and poor performance. Therefore, we have limitation at physical link of 1G/10G bps doesn't fit into a 100Mbps NC-SI connection.

Reference Document :

https://www.intel.com/content/www/us/en/embedded/products/networking/nc-si-overview-andperformance-notes.html

List of supported cipher suites in IPMI

ID	Authentication Algorithm	Integrity Algorithm	Confidentiality Algorithm
0	RAKP – NONE	NONE	NONE
1	RAKP-HMAC- SHA1	NONE	NONE
2	RAKP-HMAC- SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC- SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC- MD5	NONE	NONE
7	RAKP-HMAC- MD5	HMAC-MD5-128	NONE
8	RAKP-HMAC- MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC- MD5	MD5-128	NONE
12	RAKP-HMAC- MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_ SHA256	NONE	NONE
16	RAKP_HMAC_ SHA256	HMAC-SHA256-128	NONE
17	RAKP_HMAC_ SHA256	HMAC-SHA256-128	AES-CBC-128