S5063/ S3063/ S6053

SP-X Firmware
BMC User Guide

MSI Enterprise Platform Solutions

CONTENTS

1 INTRODUCTION 5

Notes 5
Overview 5
Supported SoC and Hardware platforms 6

2 SP-X FEATURES 7

IPMI Message Interface Support 7
IPMI 2.0 based management 7
Event Log and Alerting 7
Sophisticated User Management 7
LDAP support 7
Remote Server Power Control 7
Media Redirection 8
SSH based SOL 8
Web based configuration 8
KVM/Media Redirection Support 8
KVM/Media Redirection H5Viewer Support 9
Security Support 9
Multiple Language Support for Web and KVM 9
Dual Image Support 9
SW eMMC Boot Support 9
Miscellaneous 9

3 SP-X HTML5 WEB GUI 10

SP-X GUI Overview 10

4 USER NAME AND PASSWORD 11

5 USING MSI SP-X 14

Menu Bar 14
Quick Button and Logged-in User 15
Logged-in user and its privilege level 16
Help 16

6 DASHBOARD 17

7 SENSOR 19

Sensor Detail 20

8 SYSTEM INVENTORY 22

System 23
Processor 23
Memory Controller 24
BaseBoard 25
Power 26
Thermal 27
PCIE Device 28
PCIE Function 29
Storage 30

9 FRU INFORMATION (FIELD REPLACEABLE UNITS) 31

10 LOGS & REPORTS 33

IPMI Event Log (All Sensor Event Logs) 34

System Log (All System Event Logs) 36
Audit Log 37
Video Log 38

11 SETTINGS 39

Captured BSOD 40
Date & Time 41
External User Services 44
LDAP/E-Directory Settings 44
Active Directory Settings 49
Role Groups 52
RADIUS Settings 54
KVM Mouse Settings 58
Log Settings 59
SEL Log Setting Policy 60
Advanced Log Settings 61
Media Redirection Settings 63
General Settings 63
VMedia Instance Settings 67
Remote Session 69
Active Redirections 71
Network Settings 72
Network IP Settings 73
Network Bond Configuration 76
Network Link Configuration 78
DNS Configuration 79
BMC Registration Settings 81
Registration Method 81
TSIG Configuration 81
Domain Name Server Setting 82
DOH DNS URL 84
NC-SI Configuration 86
PAM Order Settings 87
Platform Event Filter 89
Event Filters 89
Alert Policies 92
LAN Destinations 94
Services 97
To view the Active Sessions: 99
To modify the existing services: 100
SMTP Settings 101
SSL Settings 104
System Firewall 109
General Firewall Settings 109
IP Address Firewall Rules 112
Port Firewall Rules 114
User Management 117
Video Recording 123
Auto Video Settings 124
Video Trigger Settings 125
Video Remote Storage 127
Pre-Event 128
Post-Event 128
SOL Settings 129
SOL Configurations 130
IPMI Interfaces 131
ID LED Control 132

12 REMOTE CONTROL 133

Launch H5Viewer 133
Media Redirection 135
Video 136
Mouse 136
Options 136
Keyboard 137
Send Keys 138
Video Record 139
Power 140
Active Users 140
Help 140
Quick Buttons 141
Keyboard LED Sync 142
Control keys 142
KVM Sharing 142
Quick Buttons 144
Keyboard LED Sync 145

13 IMAGE REDIRECTION 146

Remote Media 147

14 POWER CONTROL 150

15 MAINTENANCE GROUP 151

Backup Configuration 152
TFTP Server Configuration 154
SFTP Server Configuration 156
Firmware Image Location 157
Firmware Information 159
Firmware Update 160
Dual Firmware Update 164
ME Firmware Component Update 167
Parallel Firmware Update 167
BIOS Firmware Update 168
Preserve Configuration 170
Files Preserved 171
Restore Configuration 177
Restore Factory Defaults 178
System Administrator 179
Fail Safe Booting Configuration 180

16 SIGN OUT 181

Copyright and Trademarks Notice

Copyright © Micro-Star Int'l Co., Ltd. All rights reserved. The MSI logo used is a registered trademark of Micro-Star Int'l Co., Ltd. All other marks and names mentioned may be trademarks of their respective owners. No warranty as to accuracy or completeness is expressed or implied. MSI reserves the right to make changes to this document without prior notice.

Technical Support

If a problem arises with your product and no solution can be obtained from the user's manual, please contact your place of purchase or local distributor. Alternatively, please visit https://eps.msi.com/support for further guidance.

Revision History

Version 1.0, 2026/07, First release.

1 Introduction

Notes

This document describes the operation of generic SP-X firmware. This document, until and unless specified, confirms the functionality on all the SoC platforms listed in this document.

Generic SP-X core refers to the new core of SP firmware running on various SoC platforms.

SP and **Service Processor** terms are used interchangeably throughout this document to refer to generic SP solution.

SP-X, SP, SP-X Core and **Generic SP** terms are used interchangeably throughout this document to refer to MSI's service processor firmware solution.

SMASH-Lite functionality mentioned in this document may or may not be available in all versions of Generic SP. Please refer to the release notes of your firmware version for more details.

Although this document explains the new features etc. of the new SP core, it also includes specific details about the existing core (core 2.0), whenever necessary. The sections where core 2.0 is mentioned are: supported SoC platforms and schedule/release milestones.

Overview

Generic SP is a powerful software stack combining the functionality of a Service Processor and of a Baseboard Management Controller (BMC). The software implements IPMI 2.0 and KVM/IP based on the service processor. It performs all the BMC management tasks defined by IPMI 2.0 and, as a Service Processor, allows for video redirection and remote monitoring using KVM over LAN or Serial over LAN. For remote access, MSI-SP runs an embedded web- server, provides a command line interface according to the DMTF SMASH specification. SP also provides Secure-Shell (SSH) based SOL to provide remote access. SP is also available for all the advanced System-On-Chips (SoC) on the market today.

SP can be completely customized and enriched with DS, an Integrated Development Environment (IDE), for server management designed as a set of Eclipse Plug-ins (www.eclipse.org).

The new core (SP-X) of firmware provides higher level of modularity in the stack, ability to easily configure the complete stack by selecting/deselecting features which are now available in the packages form. There are various other improvements like new Linux kernel base, new set of automated test tools, and easy portability/customization using supplied tools. DS has been extended to include the ability to customize the stack, build and debug at the same time.

Supported SoC and Hardware platforms

This section lists out the supported SoC platforms by MSI SP-X core.

SoC vendor	SoC/EVB	SP-X Core
ASPEED	AST2600	Yes

The hardware platform used to validate MSI SP stack typically is:

The SoC EVB plugged-in to MSI's x86 motherboard or any other motherboard, required by the SoC EVB.

In addition, an I2C board and another BMC are used to validate I2C related functionality of MSI SP core. This setup is being added to ensure that generic releases of MSI SP core includes actual, real-time sensors/server health management, FRU, and multi-master functionality. Please refer to the later sections of this document for more details on this I2C setup.

2 SP-X Features

IPMI Message Interface Support

- KCS (System Interface Support)
- IPMB
- LAN
- BT (System Interface Support)
- Serial Interface (Basic & Terminal Mode) Support

Note: Needed to disable UART Mirror log feature in order to support Serial Interface feature, as a multiplexer is utilized for communication in both features.

IPMI 2.0 based management

- BMC stack with a full IPMI 2.0 implementation
- Customizable sensor management
- IPMI threads management
- Support for reusing the space upon a SEL entry deletion
- LAN channel mapping via MDS. Support for Setting Override using PDK hook

Event Log and Alerting

- Read Log events
- Sensor readings
- SNMP traps
- E-mail alerts

Sophisticated User Management

- IPMI based user management
- Added security with SSL (HTTPS)
- Multiple user permission level
- Multiple user profiles

LDAP support

- Direct LDAP support from the device
- Open LDAP (Generic LDAP) supported

Remote Server Power Control

- Server's power status report
- Support for remotely power-cycle, power-down, power-up and reset the server

Media Redirection

- Simultaneous CD or DVD redirection.
- Efficient USB 2.0 based CD/DVD redirection speed at the max around 20XCD *. Speed varies depends on the method of communication (SSL/Non-SSL). Refer media performance analysis matrix for further information.
- Completely secured (Authenticated or Encrypted) remote KVM or vMedia.

SSH based SOL

- Power control of the server
- Support for all DMTF Profiles
- Complete command support
- Customizable parser for easy update to future modifications in grammar
- Dynamic target discovery
- Firmware update
- Role based authentication and authorization
- Output filtering
- OEM command and target

Web based configuration

- Full configuration using web UI
- Fail-safe firmware upgrade

KVM/Media Redirection Support

- Auto video recording based on the event trigger
- Auto video recording prior to critical events (crash/reset) triggers
- Auto Recorded Video saved in the Remote share support
- Standalone Java client support for recorded video playback
- Auto resizing of KVM/JViewer window to fit the client resolution (Via Standalone Java client)
- Privilege support for KVM
- IPMI Raw command support (Via Standalone Java client)
- Single JAR for Standalone app
- Keyboard mapping in KVM to send the correct codes as per host
- KVM localization using menu option in the client at runtime (Via Standalone Java client)
- Recorded videos to be downloaded & playable in AVI format
- BSOD capture/view support
- HID Sharing support to allow more than two concurrent sessions
- RMedia configuration using IPMI commands
- Power Save Mode Support

KVM/Media Redirection H5Viewer Support

- Keyboard mapping in KVM to send the correct codes as per host.
- Recorded videos to be downloaded & playable in AVI format.
- HID Sharing support to allow more than two concurrent sessions.

Security Support

- Encrypted password support for AD/LDAP server authentication.
- KVM/Media Redirection works through Web Port.

Multiple Language Support for Web and KVM

- Web pages are loaded based on the browser language settings and user can change the language at runtime based on supported languages appeared on Web.
- H5Viewer GUI Language Settings can be loaded based on the language selected in Web UI pages (English, Chinese and Simplified Chinese).
- JViewer GUI Language Settings can be loaded based on the language selected in Web UI pages (English, Chinese and Simplified Chinese).

Dual Image Support

- Backup Image
- Boot of images at any instant
- Updates Firmware Image as per user request
- Online Firmware Update
- Configuration migration

SW eMMC Boot Support

- SW eMMC Boot can be enabled based on PRJ selection.
- SW eMMC enabled Image need to be used
- Image upgrade can be done via, WEBUI, IPMITOOL, and YAFUFLASH
- EMMC partition Need to be taken care.

Miscellaneous

- Memory test support in u-boot
- Section based flashing support via Web
- Support for auto reboot in case of abrupt cancellation during YAFU based firmware update.

3 SP-X HTML5 Web GUI

SP-X GUI Overview

The SP-X on SoC has a generic, user-friendly Graphics User Interface (GUI) called the SP-X GUI. It is designed for easy usage. It has a low learning curve because it uses standard Internet browsers.

This chapter allows you to become familiar with the SP-X GUI's various functions. Each function is described in detail.

Following are the list of latest version browsers are recommended to launch the Web UI.

- Google Chrome
- Firefox
- Microsoft Chromium-based Edge
- Safari (On Mac only)

Following list of browsers are **NOT** recommended to launch the Web UI. As Microsoft stop supporting following browsers hence, we are not recommended to use the same.

- Microsoft Edge Legacy
- IE11

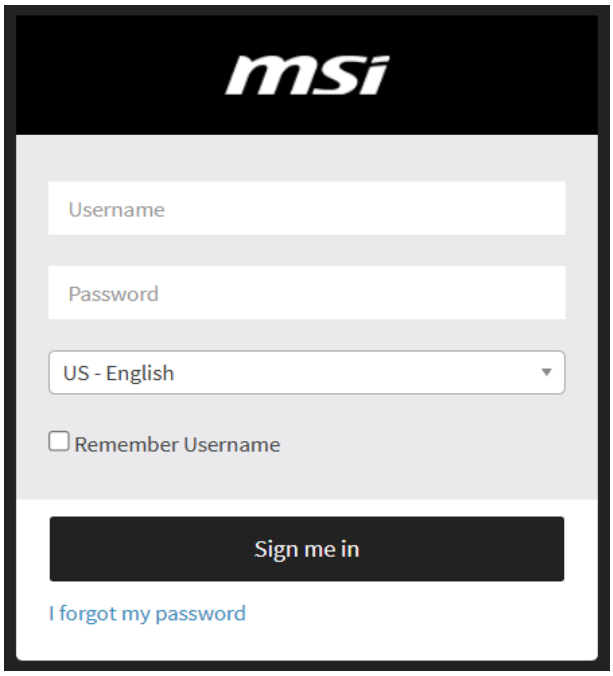
***Note**:*

- *There won't be any debug support if any issues occurring in browsers which are not recommended.*
- *When the Chrome browser is in private mode, the session will be copied to manage the web UI in another private tab. The same case will not be applicable for the rest of other browser's private windows.*
- *For security reasons, input data with special characters like "" , : / ../ # and $, data with HTML tags like "test<123>456", combination of <> characters etc...will be blocked from Web UI/REST API .*

Your SP-X GUI may not exactly match this document.

4 User Name and Password

Initial access of MSI SP-X 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.

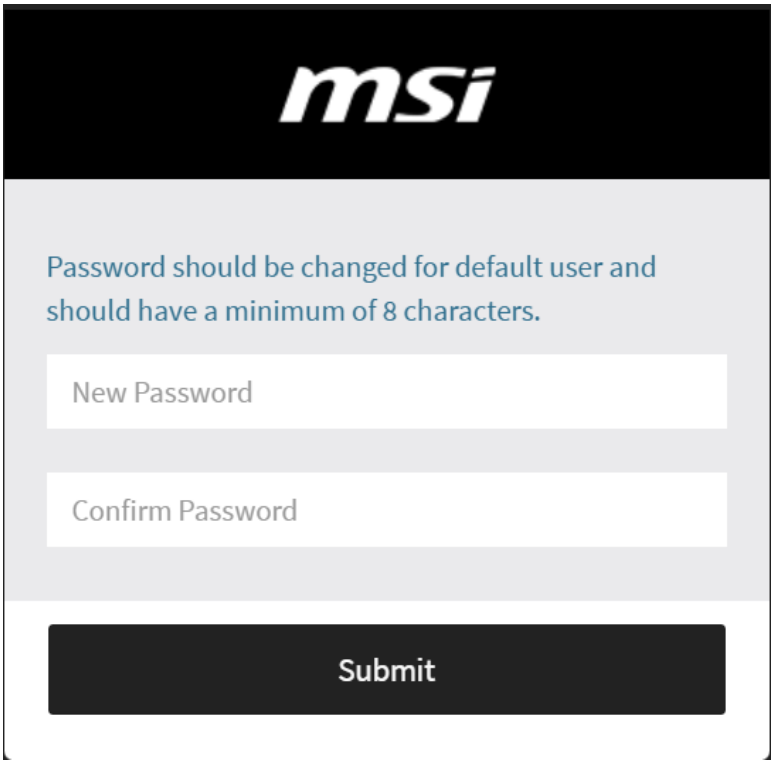
Sign me in: After entering the required credentials, click the Sign me in to login to MSI GUI.

I Forgot my Password: If you forget your password, you can generate a new password using this link.

Need for Password Change

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 WebUI 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.



Password Change

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

- IPMI Tool
- WebUI
- Redfish (If Redfish Support is enabled)

***Note**: The last password used cannot be used to reset the password.*

Password Change Required Case

- When the BMC boots with factory firmware, user needs to change the default password on first boot.
- When user upgrades the BMC firmware without preserve configuration, default password needs to be changed on first boot.
- When user does a factory restore and reboot BMC, default password needs to be changed on reboot.
- 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.

***Note**: Since Password Change at first login is made as PRJ configurable and if this feature is disabled then it is not mandatory to change the default password at first login.*

Required Browser Settings:

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

Default User Name and Password

Username: admin

Password: admin

***Note**:*

Password should be changed for default user and should have a minimum of 8 characters and maximum of 16 characters.

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, RADIUS or IPMI since the privilege of one Authentication method is overwritten by another authentication method when login and hence the correct privilege cannot 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*

5 Using MSI SP-X

The MSI GUI consists of various menu items.

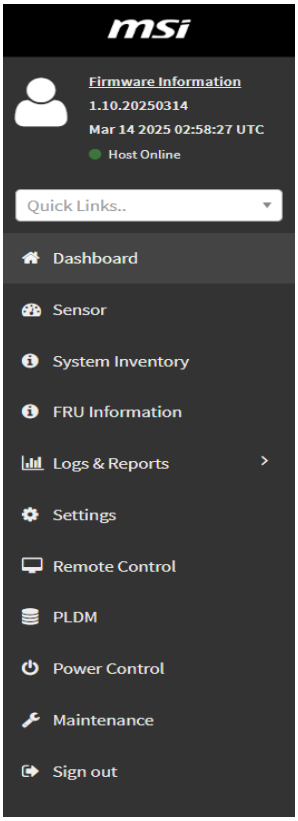
Menu Bar

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 Online link.

- Dashboard
- Sensor
- FRU Information
- Logs & Reports
- Settings
- Remote Control
- Power Control
- Maintenance
- Sign out

A screenshot of the menu bar is shown below.



Menu Bar

Quick Button and Logged-in User

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



User Information

The logged-in user information shows the logged-in user, his/her privilege and the 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.

BIOS: BIOS WebUI can be accessed via the BIOS icon as depicted in the below screenshot.



BIOS Quick Button

This page is displayed only when Redfish is enabled in the BMC image. It also requires Redfish enabled BIOS to view and modify/apply the BIOS settings remotely by the user and this page is maintained by MSI BIOS counterpart.

BIOS WebUI can be launched/accessed independent of BMC WebUI with the following URI also: https://{{ip}}/bios/Index.html

Redfish Credentials to use for Login to this webpage.

> ***Note:*** *If Unified User is enabled, BMC WebUI/IPMI credentials can also be used to login to this web page.*

Please refer MSI BIOS counterpart for any further details.

2FA: To enable or disable Two Factor Authentication (2FA) for the current user in this channel. It will show the QR code and backup codes on the pop-up window after the user clicks the '2FA' switch button. The user needs to download the mobile App 'Authenticator' to scan the QR code, the

application will generate a six-digit one-time password which users must enter to their usual login details. In addition, please save the backup codes for emergency use, and a backup code will become invalid once the code is used.

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

Refresh: Click the  icon to reload the current page.

Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There is 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.

Signout: Click the  icon to log out of the GUI.

Quick Search: Quick Search is a short-cut for the available menu and sub-menu pages. It displays available search queries. Click  (Quick Search) field, and type search terms of the lists in the menu bar. As you type, the suggestions will be displayed in a drop-down list below the Quick Search field as a navigational links of the menu and sub-menu. On selecting your search term from the drop-down list, it will directly go to the specific page which you have searched.

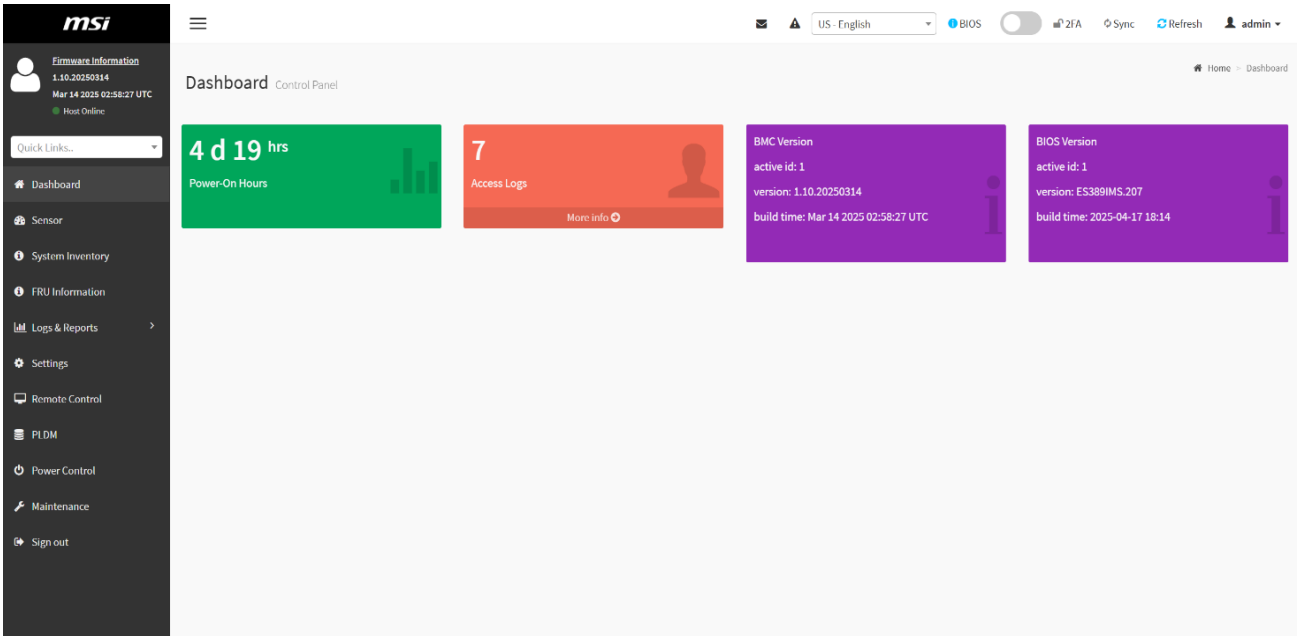
Help

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

6 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.



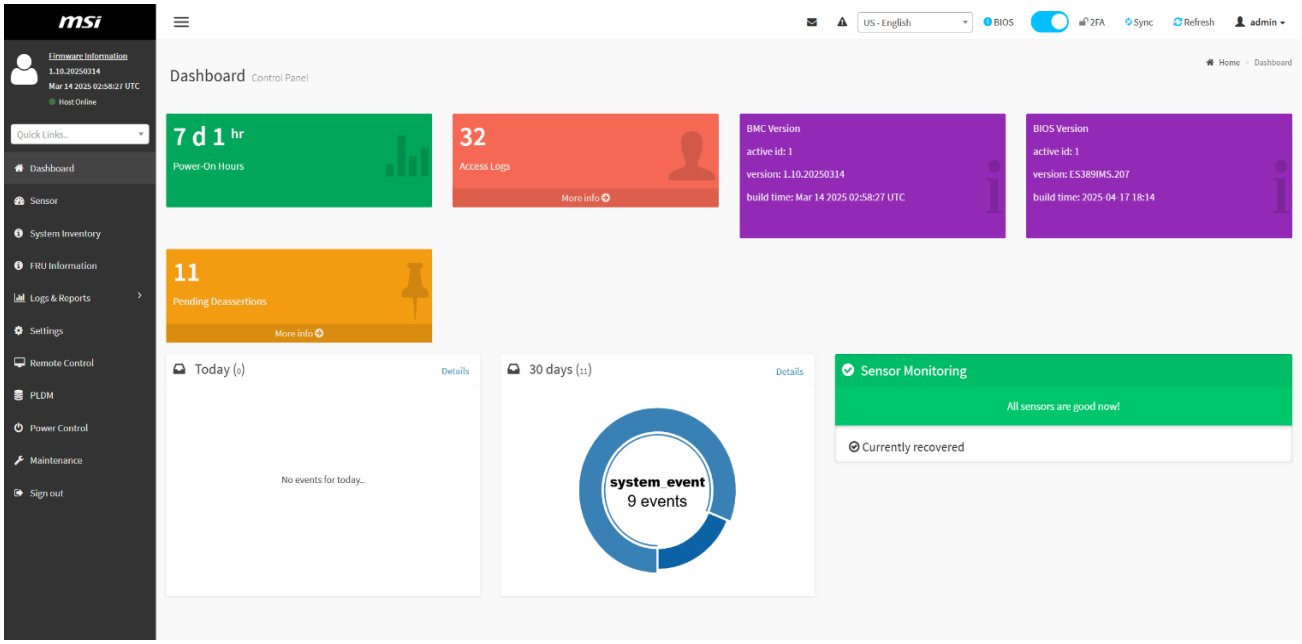
Dashboard

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.*



Dashboard

Language Selection

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

Power-On Hours

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

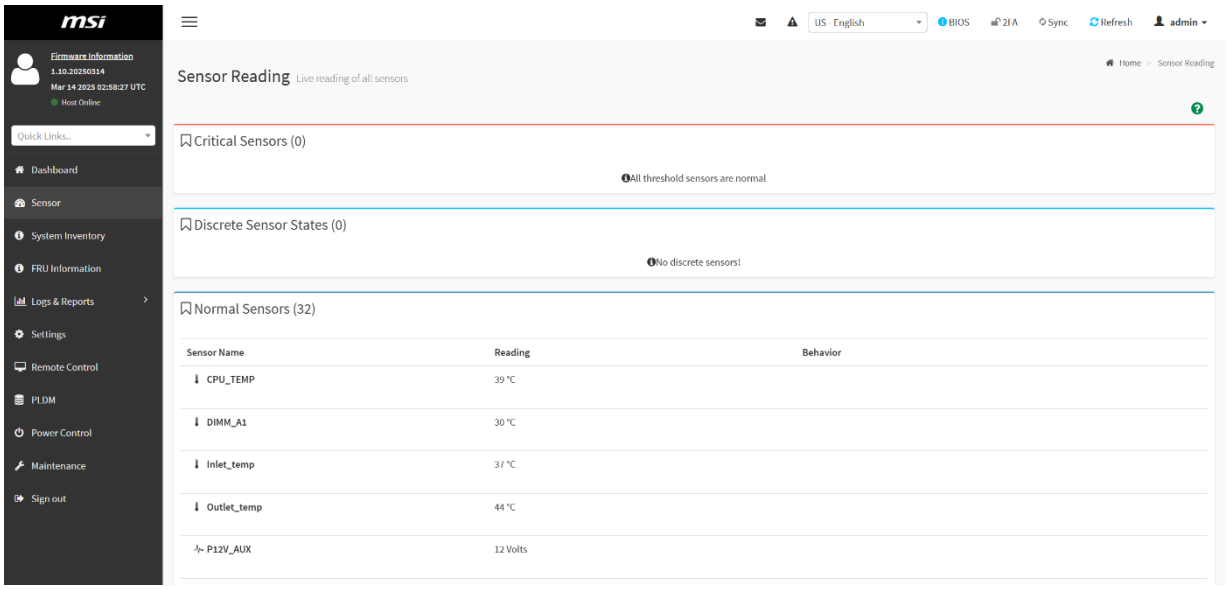
It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

7 Sensor

The Sensor Readings page displays all the sensor related information.

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

A screenshot of Sensor Readings page is given below.



Sensor Readings Page

The Sensor Readings page contains the following information.

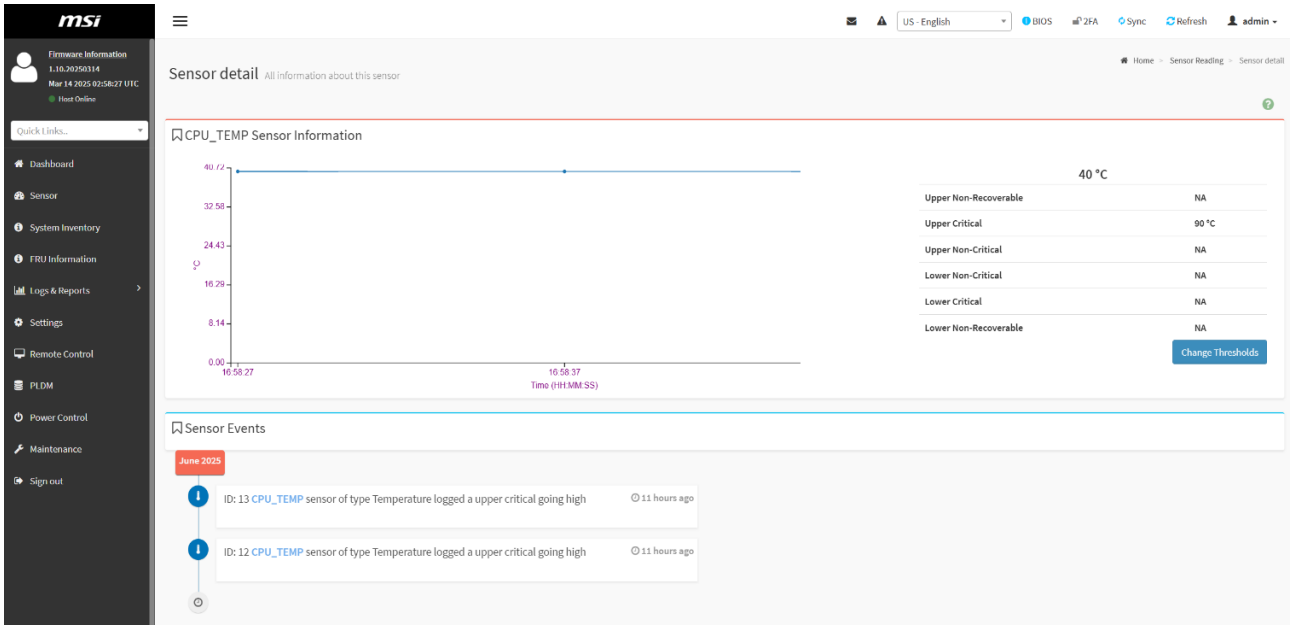
In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior will be appeared, else you can choose the sensor type that you want to display from the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.

Sensor Detail

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

> ***Note**: Change Thresholds is a feature enabled option, to enable this feature refer specific PRJ (Refer MDS Guide).*

For Illustrative Purpose, a sample screenshot of Sensor detail page with Change Thresholds option is shown and explained 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 get 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)

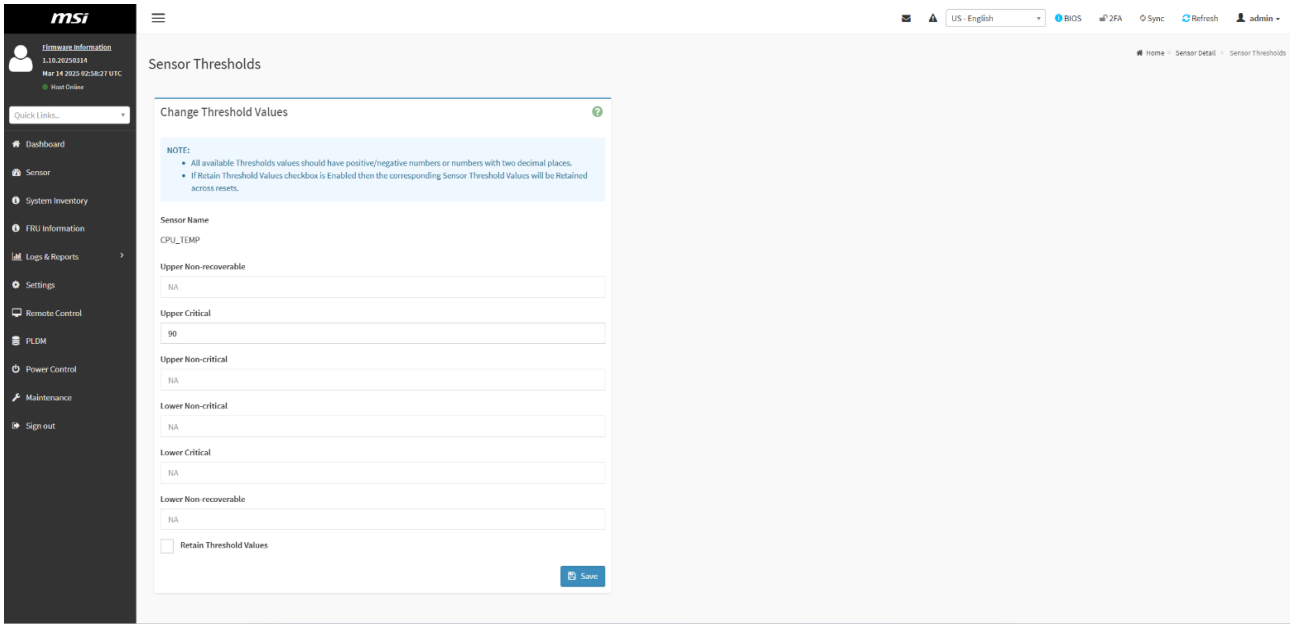
The threshold states could be Lower Non-critical - going low, Lower Non-critical - going high, Lower Critical - going low, Lower Critical - going high, Lower Non-recoverable - going low, Lower Non-

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.

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

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.

   ***Note**:*

   To display/hide the Retain Threshold values option in Sensor Thresholds page, based on feature "CONFIG_SPX_FEATURE_SENSORTHRESHOLDACROSSRESETS_SUPPORT" is enabled/disabled respectively.

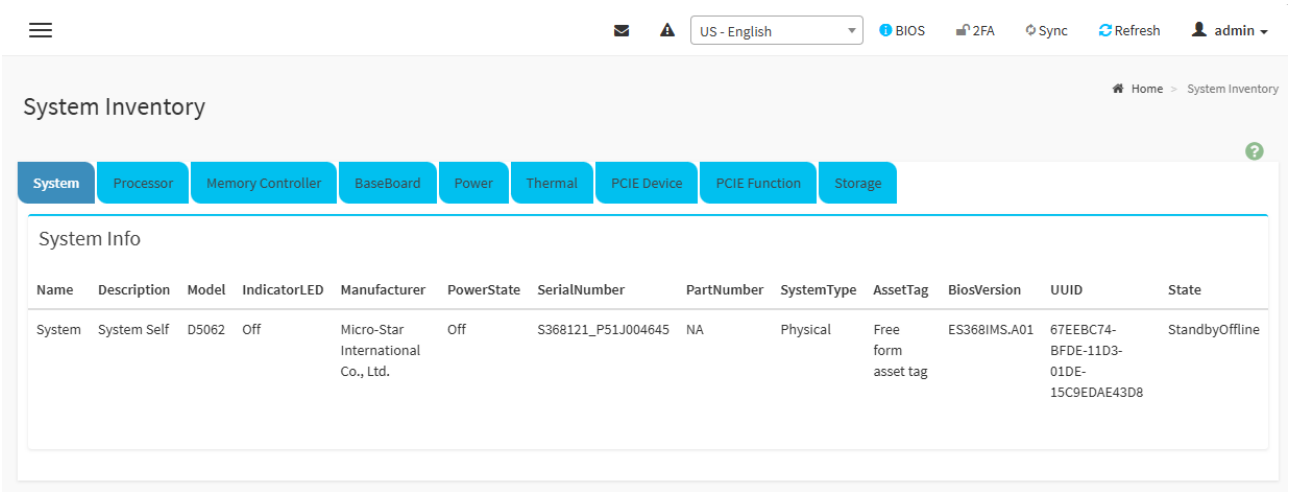
4. Click **Save** to configure the threshold values.

8 System Inventory

System Inventory page displays the following information

- System
- Processor
- Memory Controller
- BaseBoard
- Power
- Thermal
- PCIE Device
- PCIE Function
- Storage

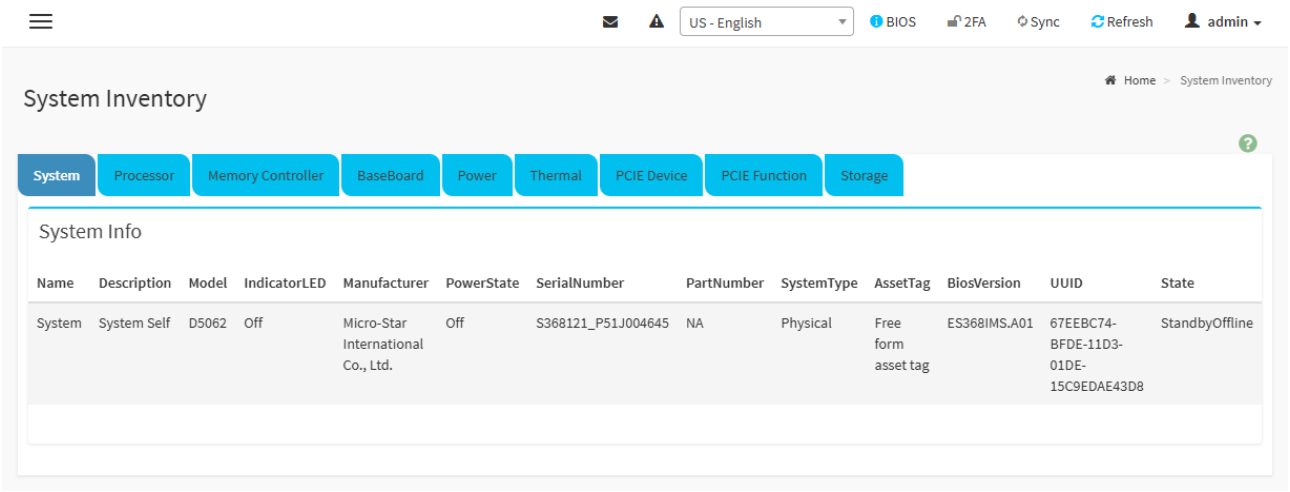
To open the System Inventory page, click **System Inventory** from the menu bar. A sample screenshot of the System Inventory page is shown below.



System Inventory

System

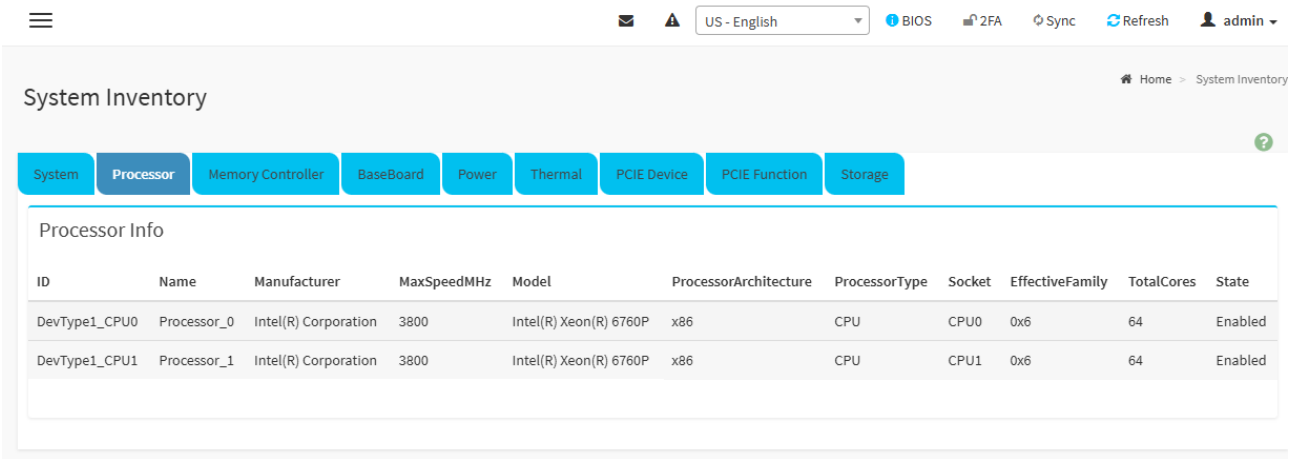
This page provides an overview of the system information for this device. A sample screenshot of the System Info page is shown below.



System Info

Processor

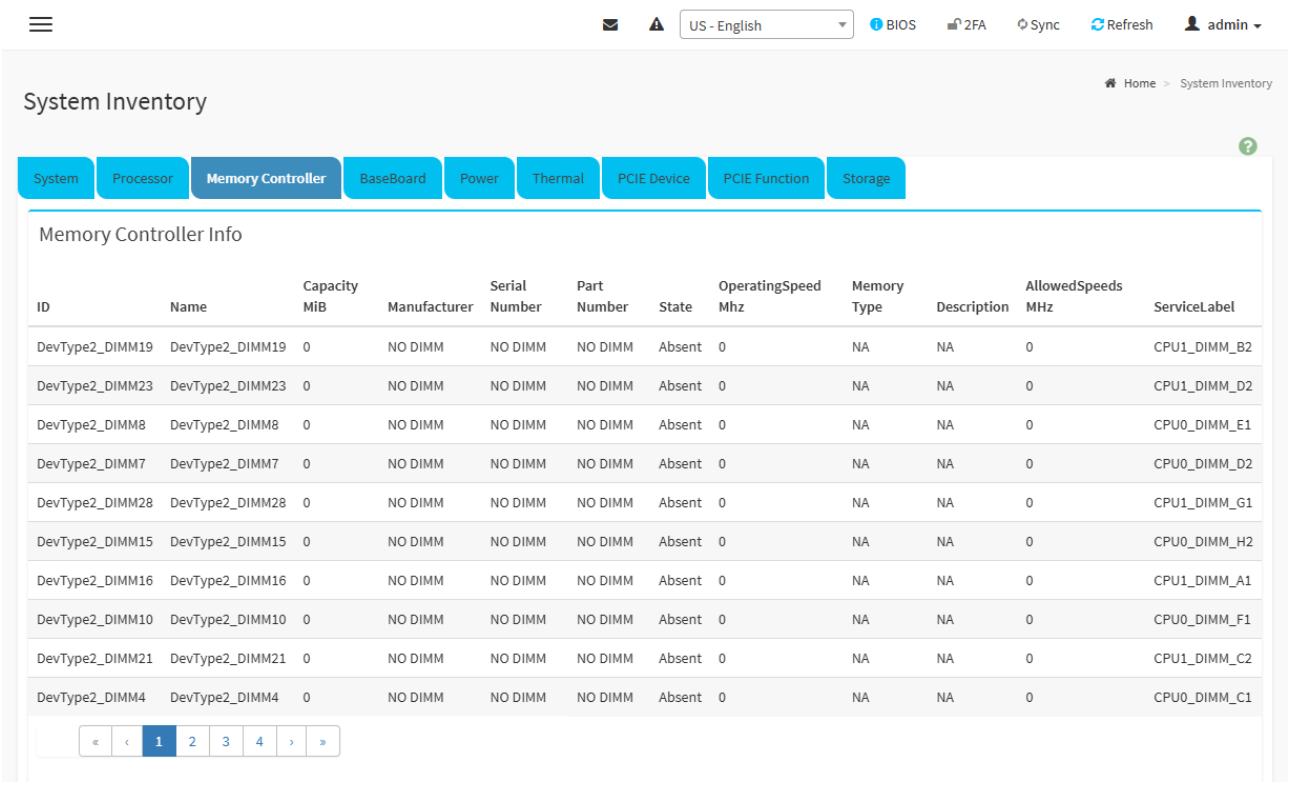
This page displays all detected CPUs on this device. A sample screenshot of the Processor Info page is shown below.



Processor Info

Memory Controller

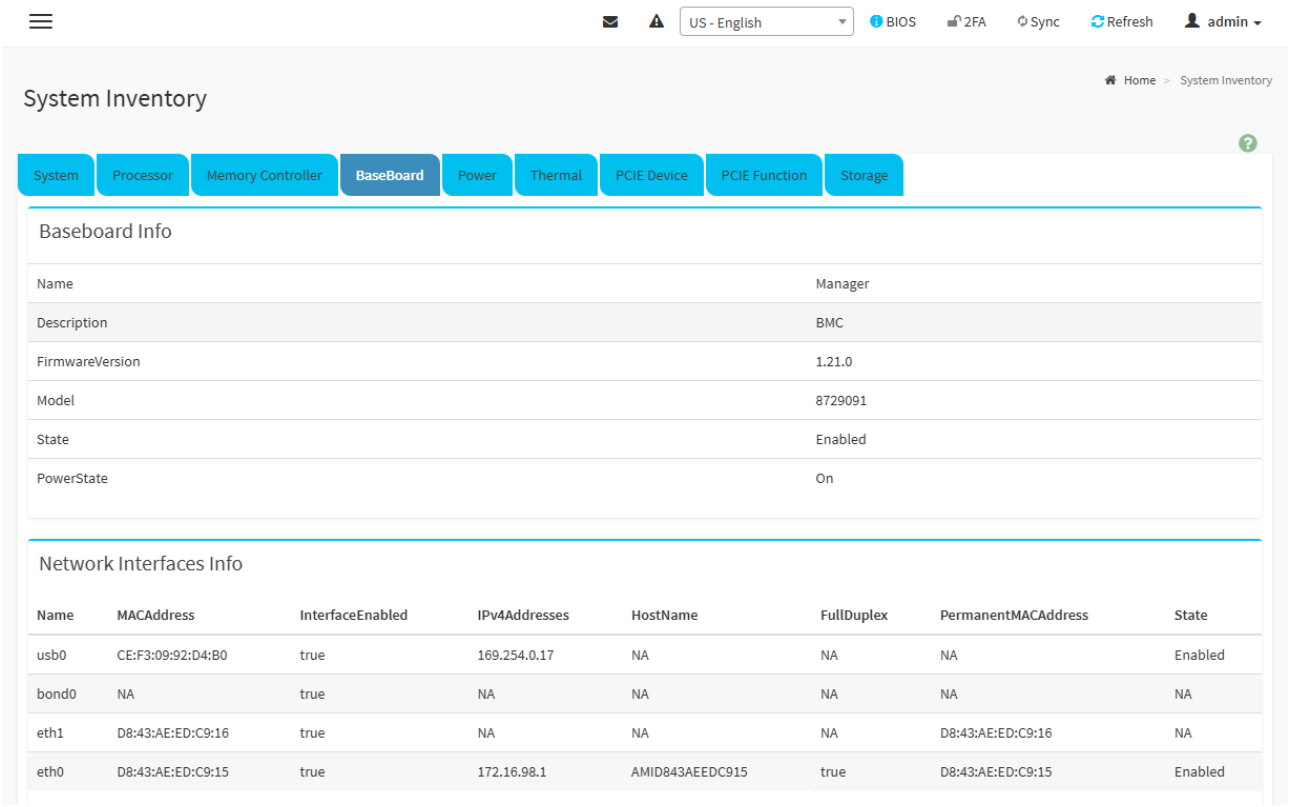
This page displays all detected DIMMs on this device. A sample screenshot of the Memory Controller Info page is shown below.



Memory Controller Info

BaseBoard

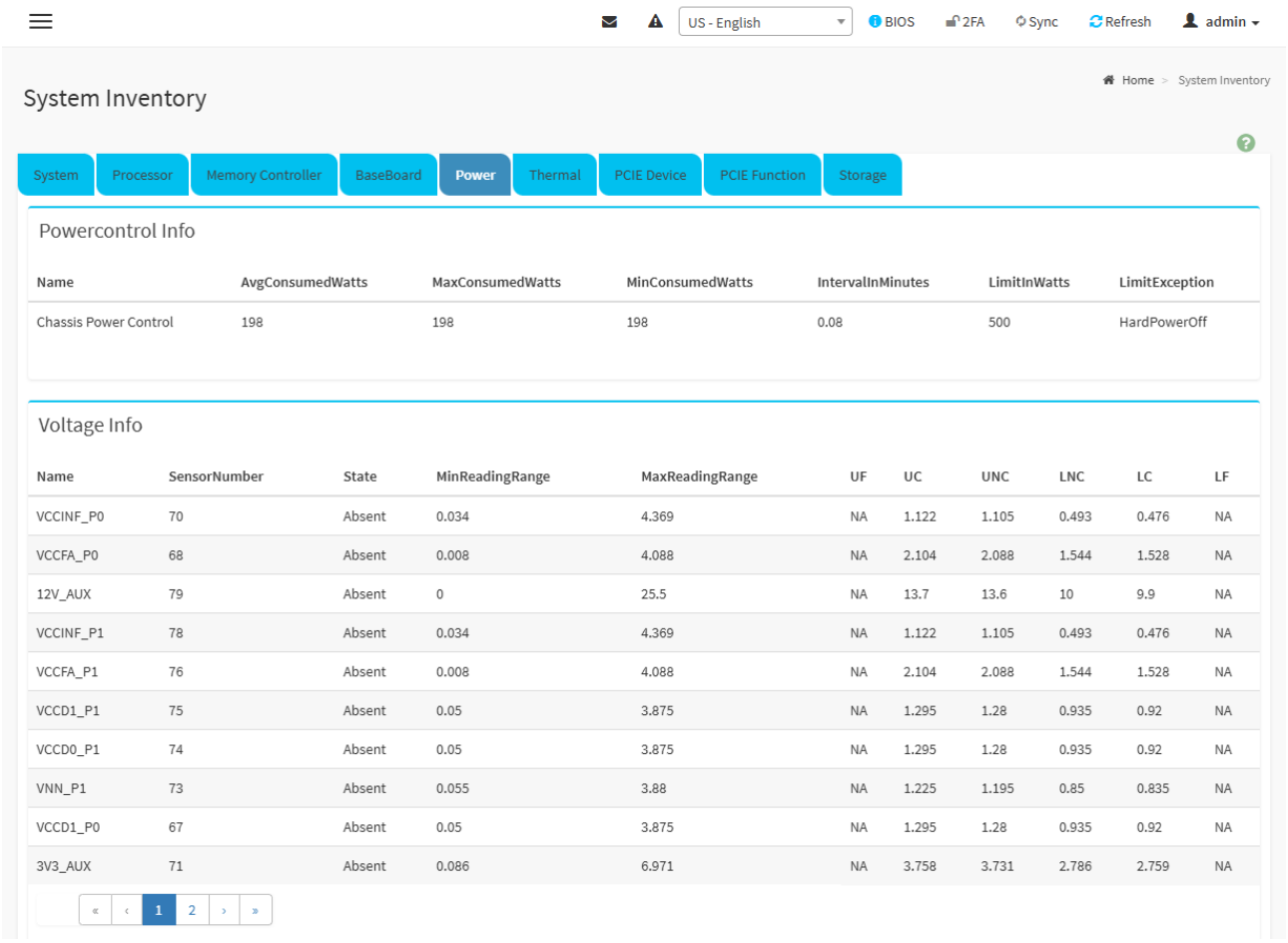
This page displays base board and network interfaces information of this device. A sample screenshot of the BaseBoard Info page is shown below.



BaseBoard and Network Interfaces Info

Power

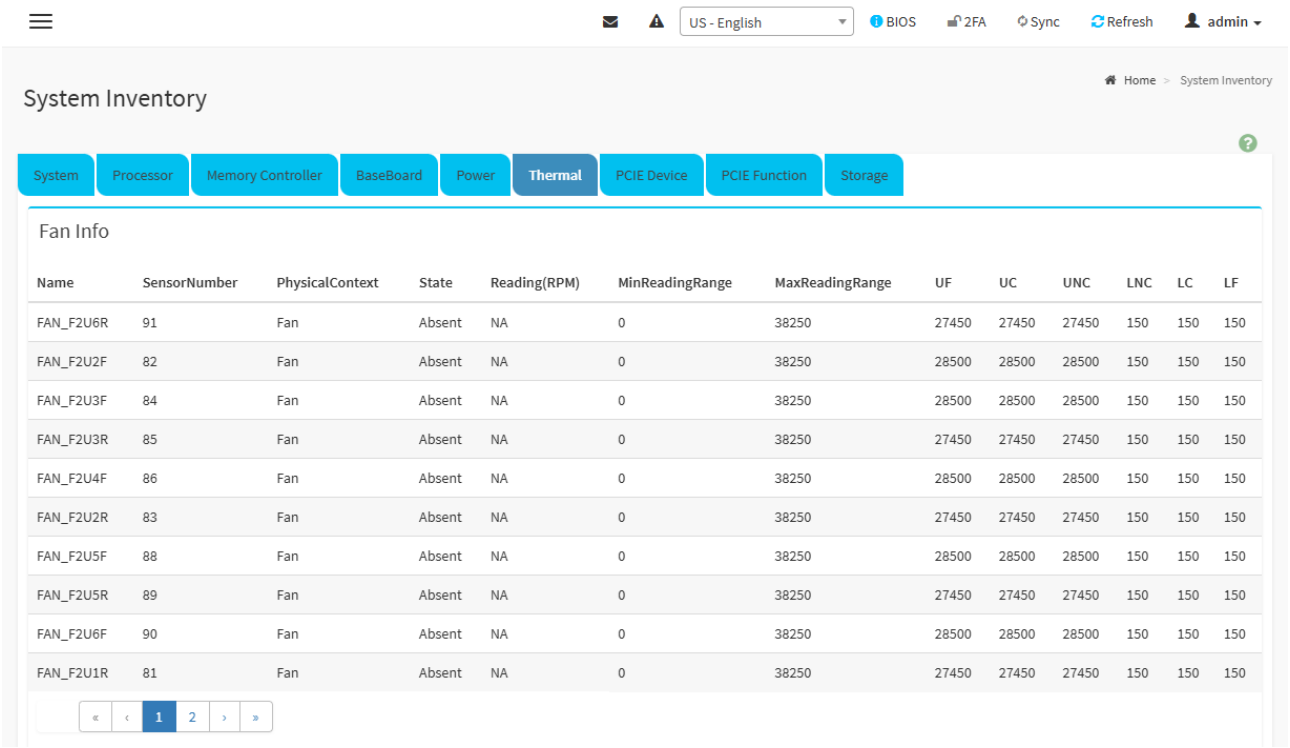
This page displays power control and voltage information of this device. A sample screenshot of the Power Info page is shown below.



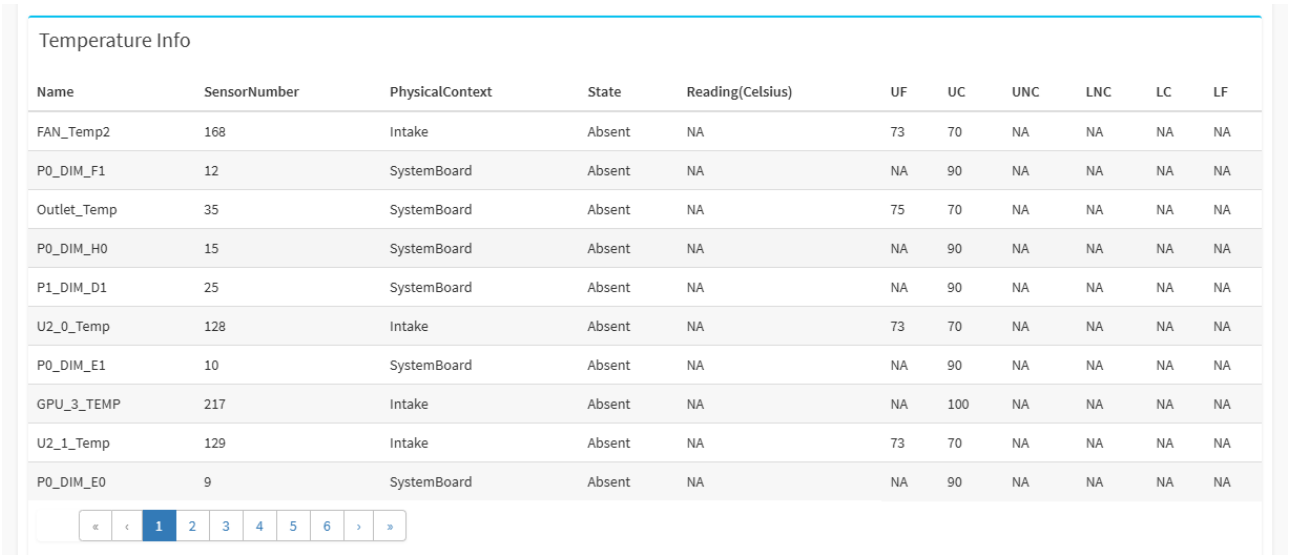
Powercontrol and Voltage Info

Thermal

This page displays fan and temperature information of this device. A sample screenshot of the Thermal Info page is shown below.



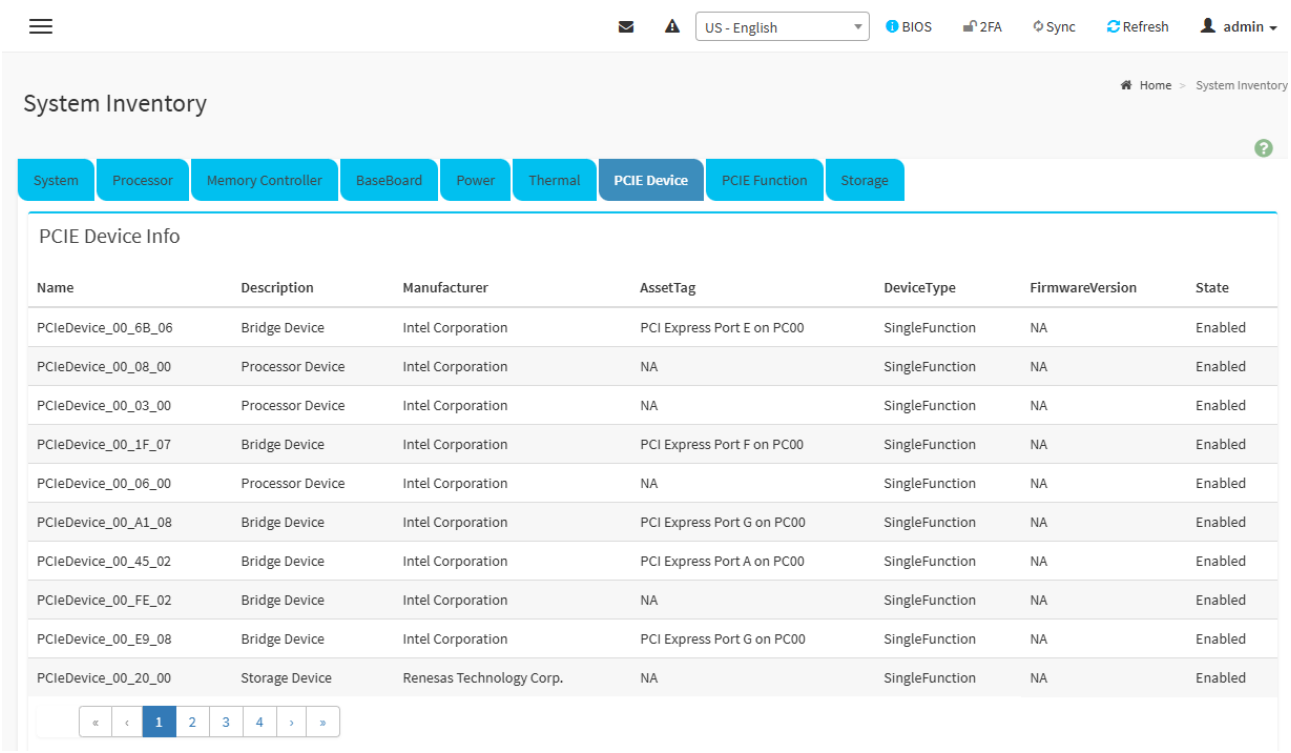
Fan Info



Temperature Info

PCIE Device

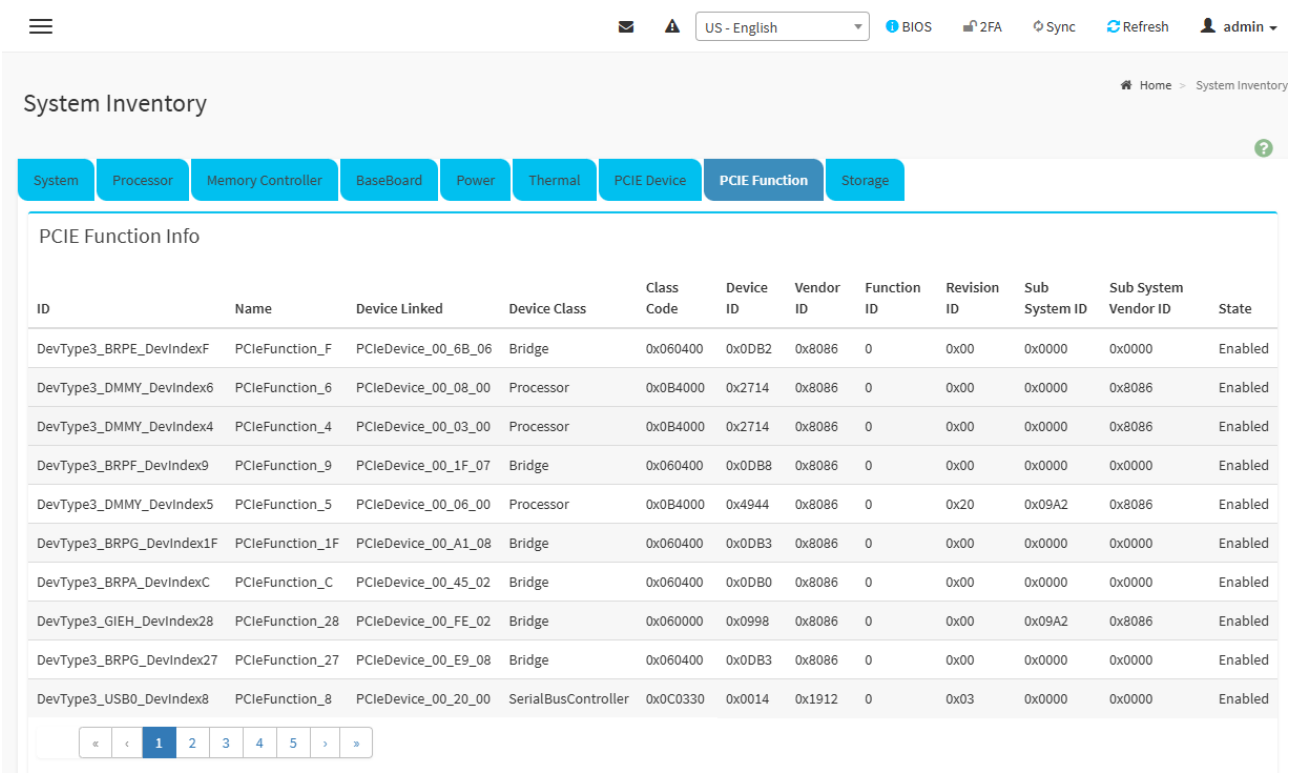
This page displays all detected PCIE devices information on this device. A sample screenshot of the PCIE Device Info page is shown below.



PCIE Device Info

PCIE Function

This page displays all detected PCIE functions information on this device. A sample screenshot of the PCIE Function Info page is shown below.



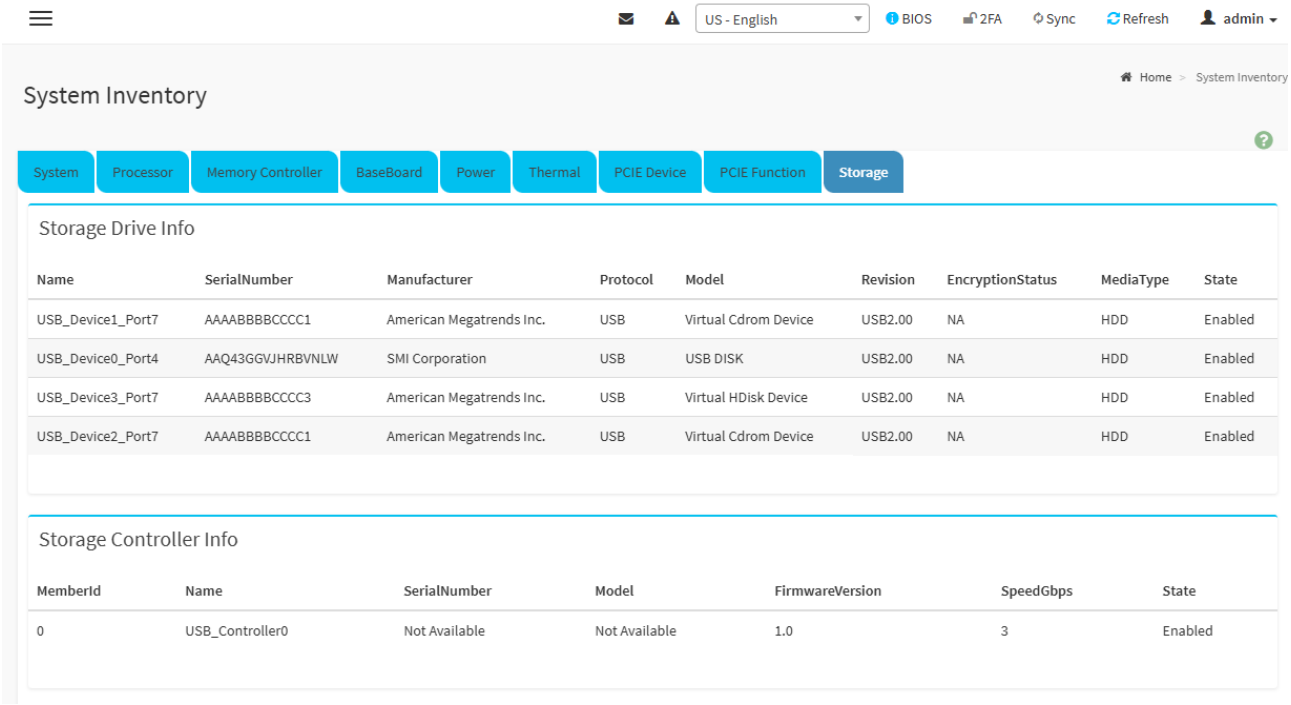
ID	Name	Device Linked	Device Class	Class Code	Device ID	Vendor ID	Function ID	Revision ID	Sub System ID	Sub System Vendor ID	State
DevType3_BRPE_DevIndexF	PCIeFunction_F	PCIeDevice_00_6B_06	Bridge	0x060400	0x0DB2	0x8086	0	0x00	0x0000	0x0000	Enabled
DevType3_DMMY_DevIndex6	PCIeFunction_6	PCIeDevice_00_08_00	Processor	0x0B4000	0x2714	0x8086	0	0x00	0x0000	0x8086	Enabled
DevType3_DMMY_DevIndex4	PCIeFunction_4	PCIeDevice_00_03_00	Processor	0x0B4000	0x2714	0x8086	0	0x00	0x0000	0x8086	Enabled
DevType3_BRPF_DevIndex9	PCIeFunction_9	PCIeDevice_00_1F_07	Bridge	0x060400	0x0DB8	0x8086	0	0x00	0x0000	0x0000	Enabled
DevType3_DMMY_DevIndex5	PCIeFunction_5	PCIeDevice_00_06_00	Processor	0x0B4000	0x4944	0x8086	0	0x20	0x09A2	0x8086	Enabled
DevType3_BRPG_DevIndex1F	PCIeFunction_1F	PCIeDevice_00_A1_08	Bridge	0x060400	0x0DB3	0x8086	0	0x00	0x0000	0x0000	Enabled
DevType3_BRPA_DevIndexC	PCIeFunction_C	PCIeDevice_00_45_02	Bridge	0x060400	0x0DB0	0x8086	0	0x00	0x0000	0x0000	Enabled
DevType3_GIEH_DevIndex28	PCIeFunction_28	PCIeDevice_00_FE_02	Bridge	0x060000	0x0998	0x8086	0	0x00	0x09A2	0x8086	Enabled
DevType3_BRPG_DevIndex27	PCIeFunction_27	PCIeDevice_00_E9_08	Bridge	0x060400	0x0DB3	0x8086	0	0x00	0x0000	0x0000	Enabled
DevType3_USB0_DevIndex8	PCIeFunction_8	PCIeDevice_00_20_00	SerialBusController	0x0C0330	0x0014	0x1912	0	0x03	0x0000	0x0000	Enabled

« ‹ 1 2 3 4 5 › »

PCIE Function Info

Storage

This page displays all detected storage drive and controller information on this device. A sample screenshot of the Storage Info page is shown below.

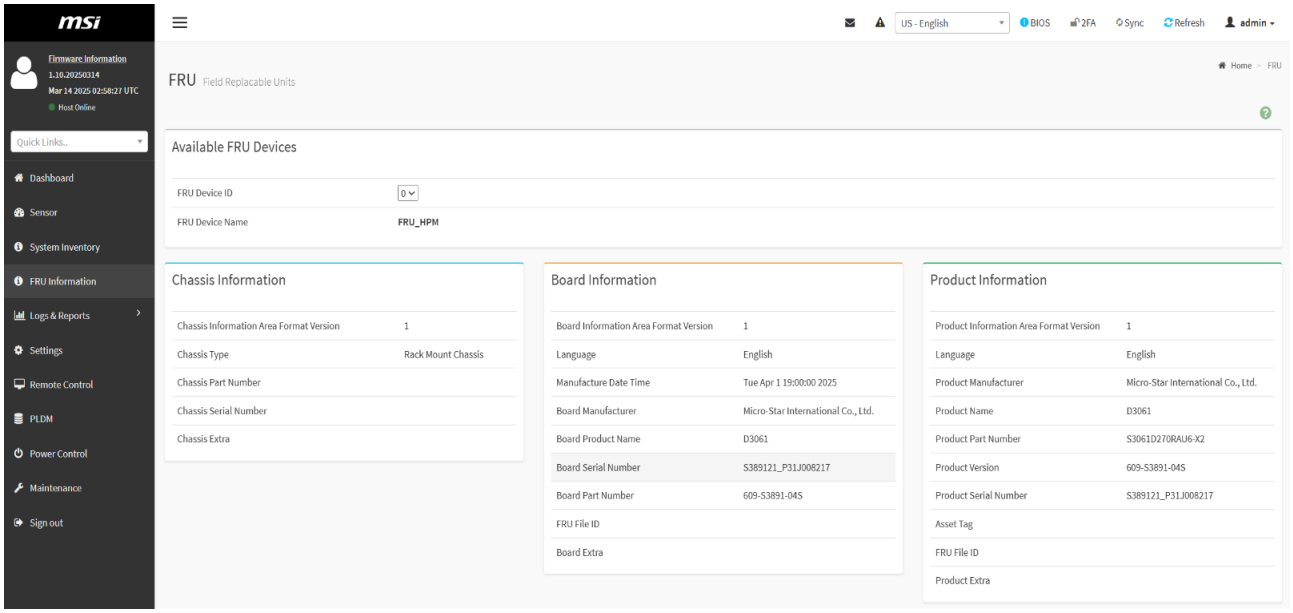


Storage Drive and Controller Info

9 FRU Information (Field Replaceable Units)

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 the 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

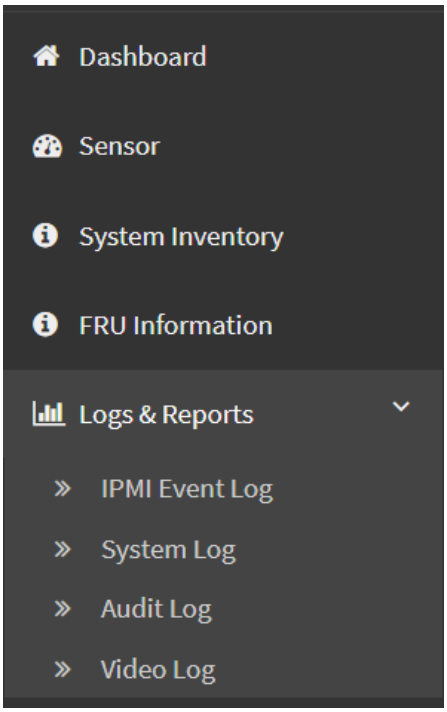
- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

10 Logs & Reports

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.



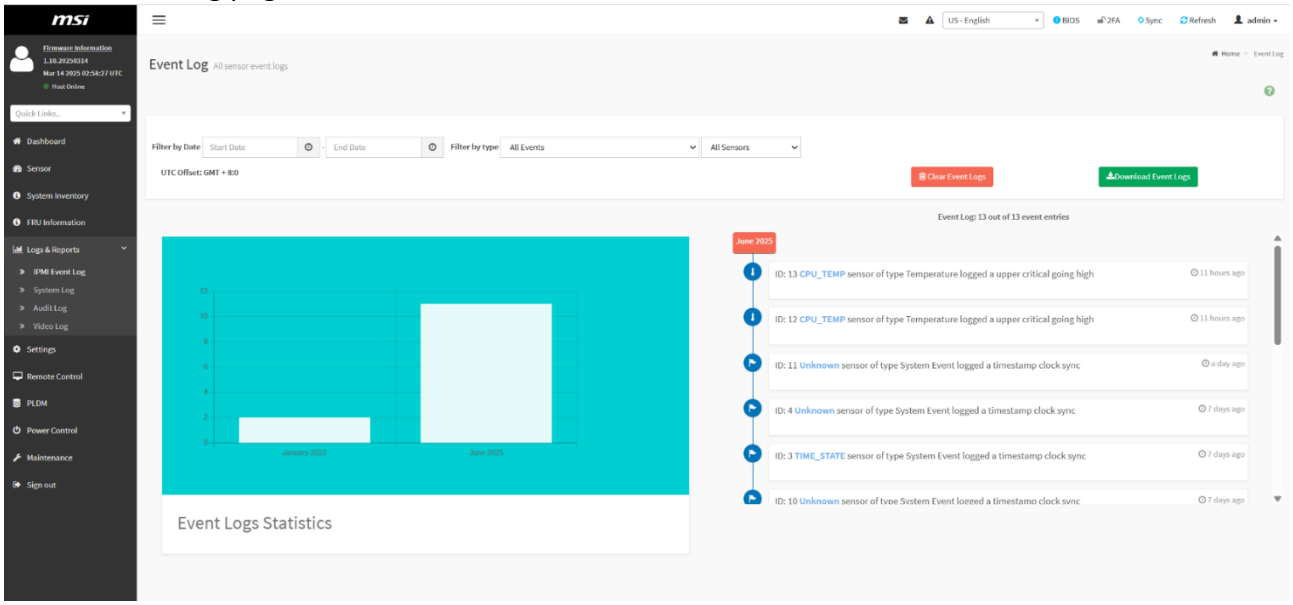
Logs & Reports – Menu

A detailed description of Logs & Reports is given below.

IPMI Event Log (All Sensor Event Logs)

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. All the events will be sorted based on the timestamp value.

To open the Event Log page, click **Home > IPMI Event Log** from the menu bar. A sample screenshot of IPMI 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 Calendar.

***Note**: Date should be in MM/DD/YYYY format.*

By default, all log time will be displayed in BMC time zone.

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

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

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 timestamp.*

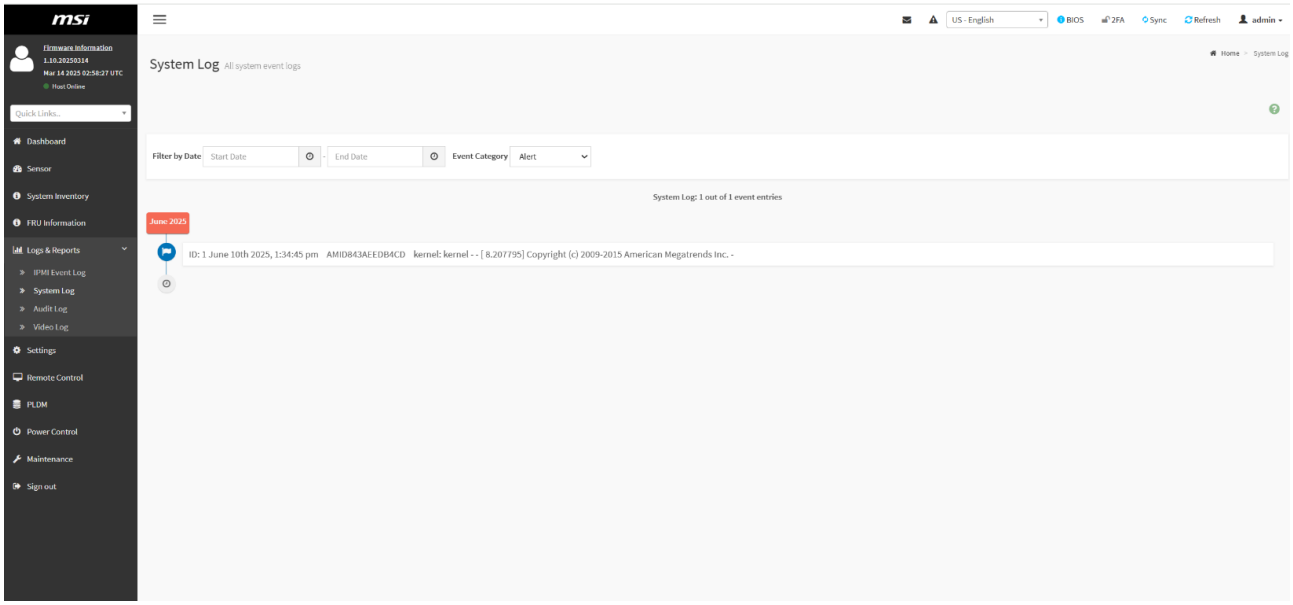
System Log (All System Event Logs)

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.



System Log

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.

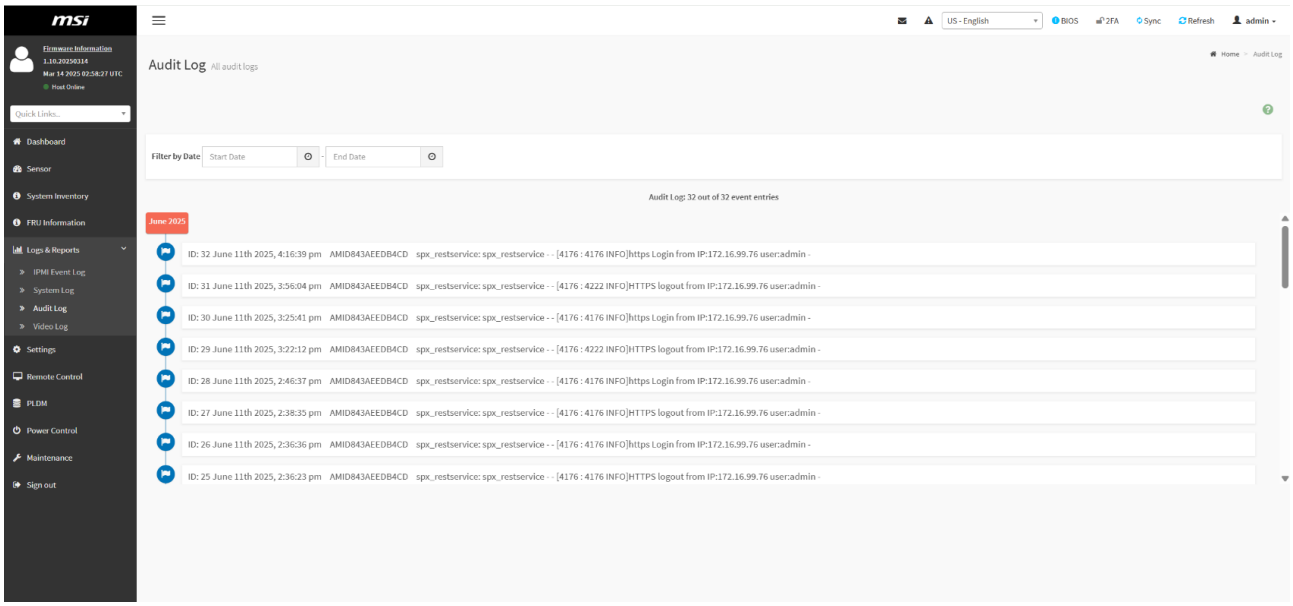
Audit Log

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.



Audit Log

Procedure

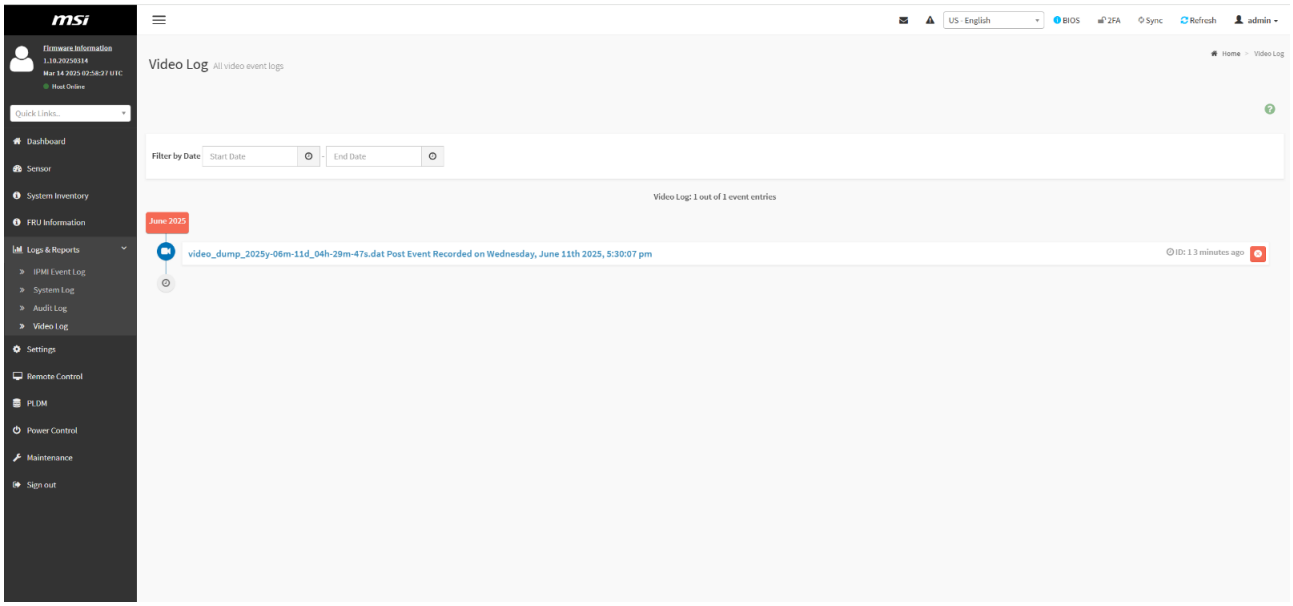
To view **Audit Log**, click the Audit Log tab to view all audit events for this device.

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**:*

- *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.*
- *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

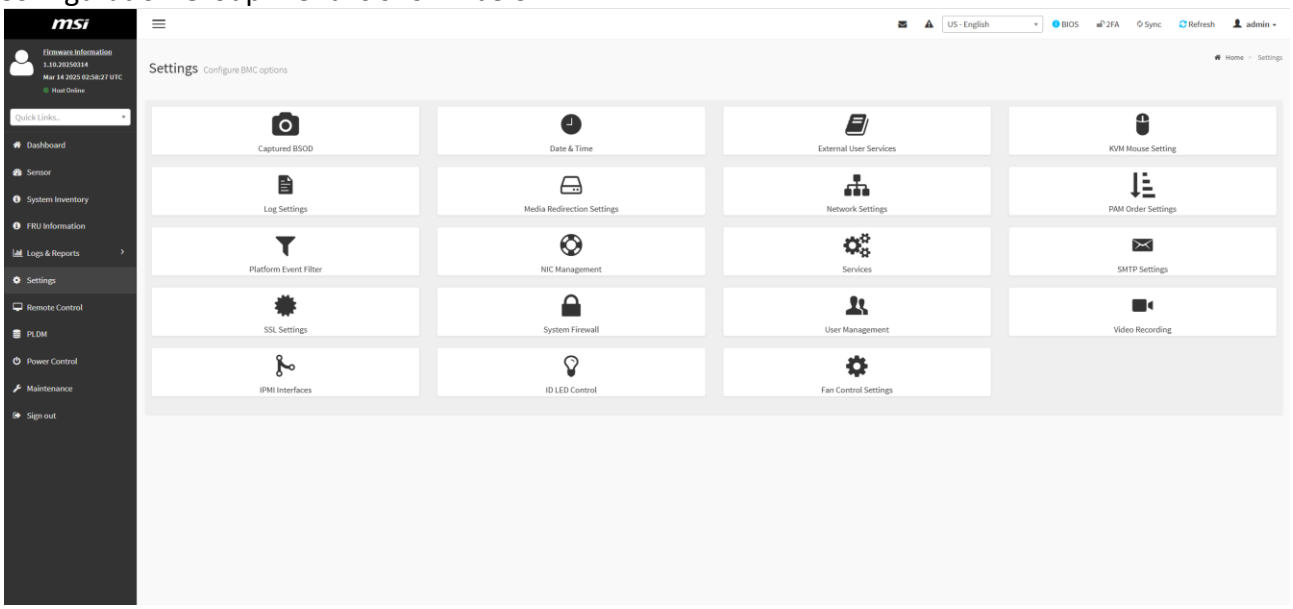
You can Download ( ), Play/Pause ( ) and Delete ( ) the video by clicking the respective icons.

***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.*

11 Settings

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



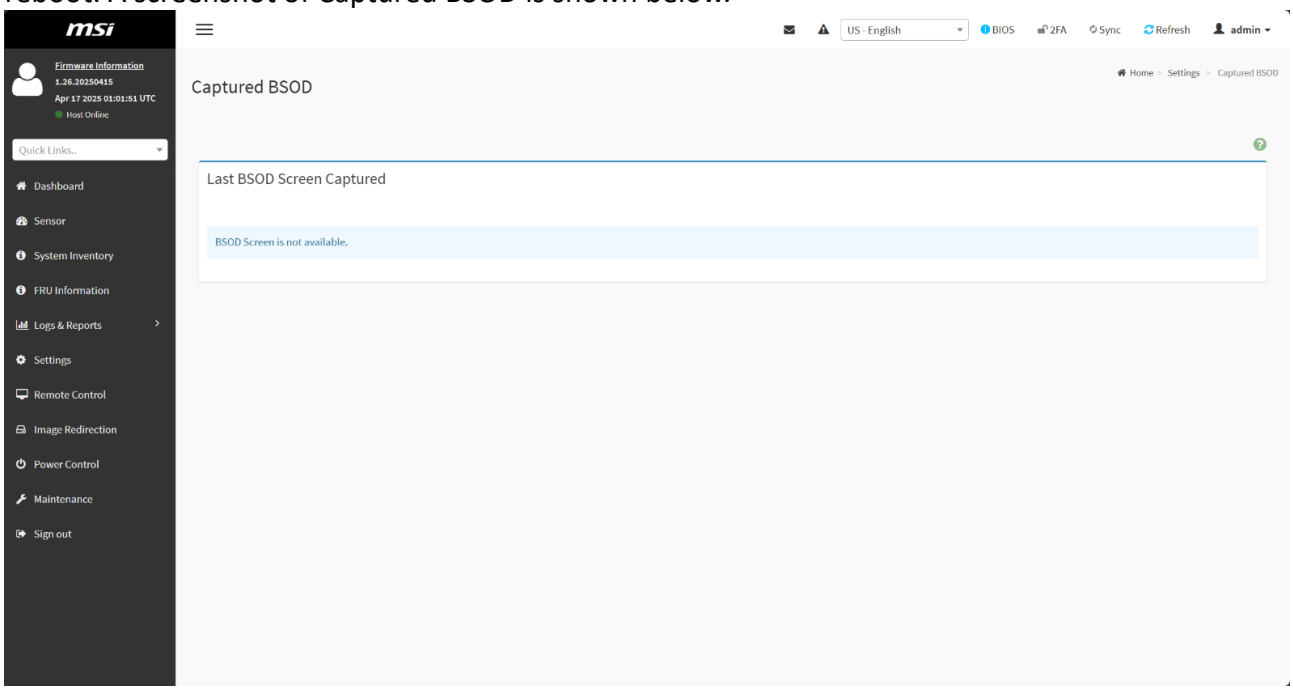
Configuration Group Menu

A detailed description of the Configuration menu is given below.

Note: All configuration sub menus will be displayed based on the features which are enabled in PRJ.

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.

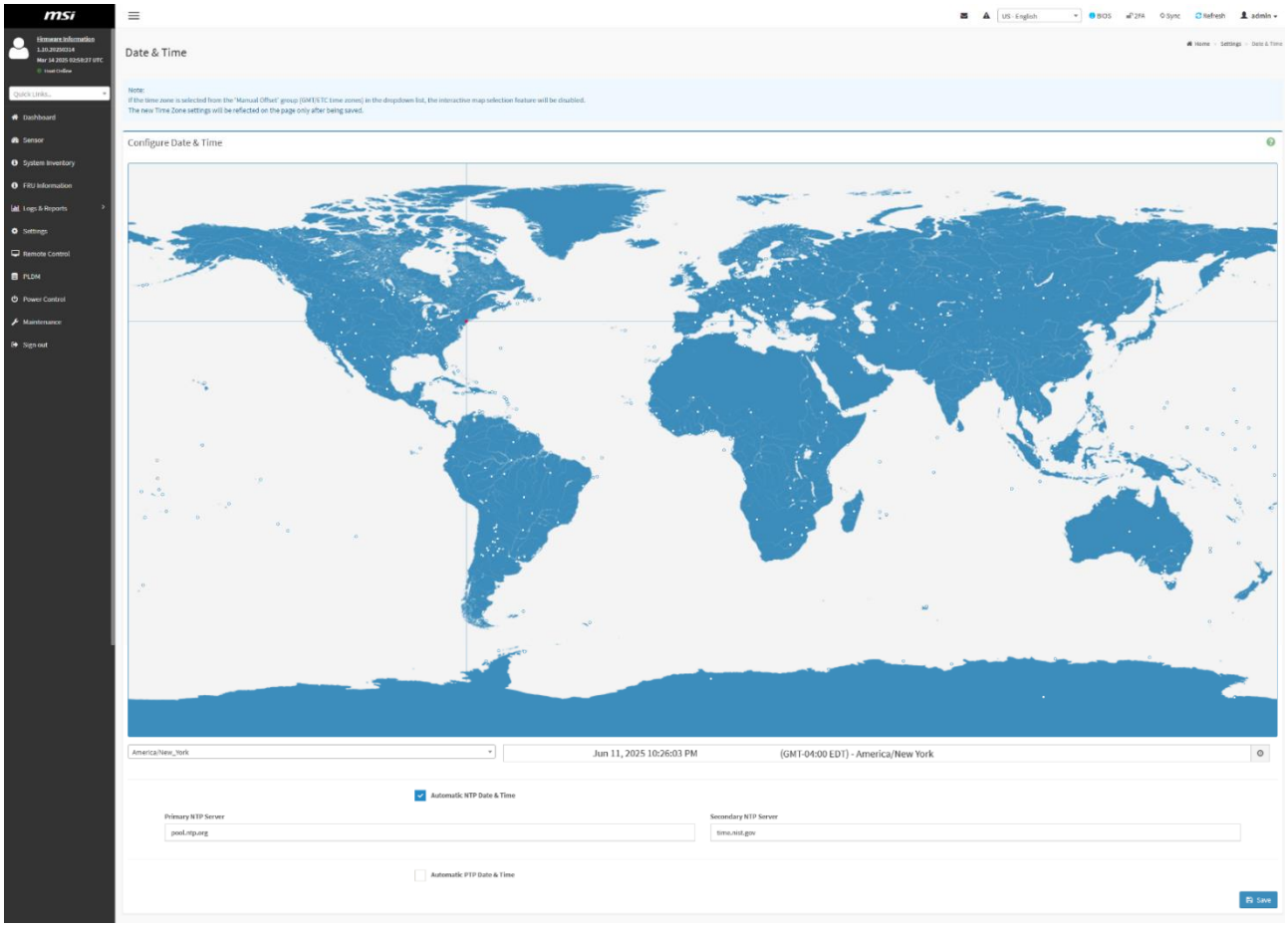


Captured BSOD

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

Date & Time

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



Date & Time - 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 NTP 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 set- ting 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 configure a PTP server interface to use when automatically setting the date and time.
- **PTP Preset**: To configure a PTP Preset type to use when automatically setting the date and time.
- **PTP Transport**: To configure a PTP Transport type to use when automatically setting the date and time.
- **PTP Ipmode**: To configure a PTP Ipmode type to use when automatically setting the date and time.
- **PTP Unicast IP**: To configure a Unicast ip when ipmode is unicast and server to use when au- tomatically setting the date and time.
- **PTP Delay Mechanism**: To configure a PTP Delay Mechanism type to use when automatically setting the date and time.
- **PTP Inbound Latency**: To configure a Inbound latency of the server to use when automatically setting the date and time.
- **PTP Outbound Latency**: To configure a PTP outbound latency server to use when automatically setting the date and time.
- **PTP Priority1**: To configure a priority of PTP clock to use when automatically setting the date and time.
- **PTP Max Master capacity**: To configure a max master capacity of the PTP clock to use when automatically setting the date and time.
- **Panic Mode**: To configure a PTP clock to not reset if jump is more than 1 second, use when automatically setting the date and time.
- **PTP Log request delay**: To configure 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 than 1 second, use when automatically setting the date and time.
4. Click **Save** button to save the settings.

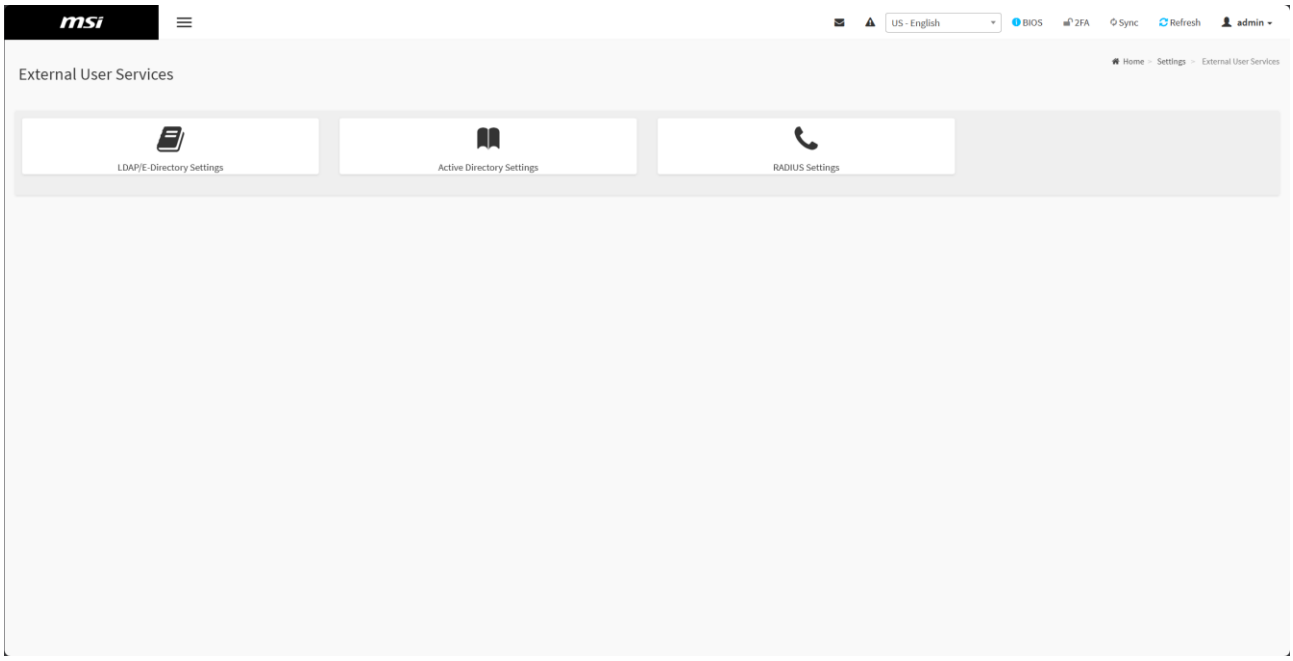
External User Services

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 MSI GUI, LDAP is an Internet protocol that 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 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 MSI 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.

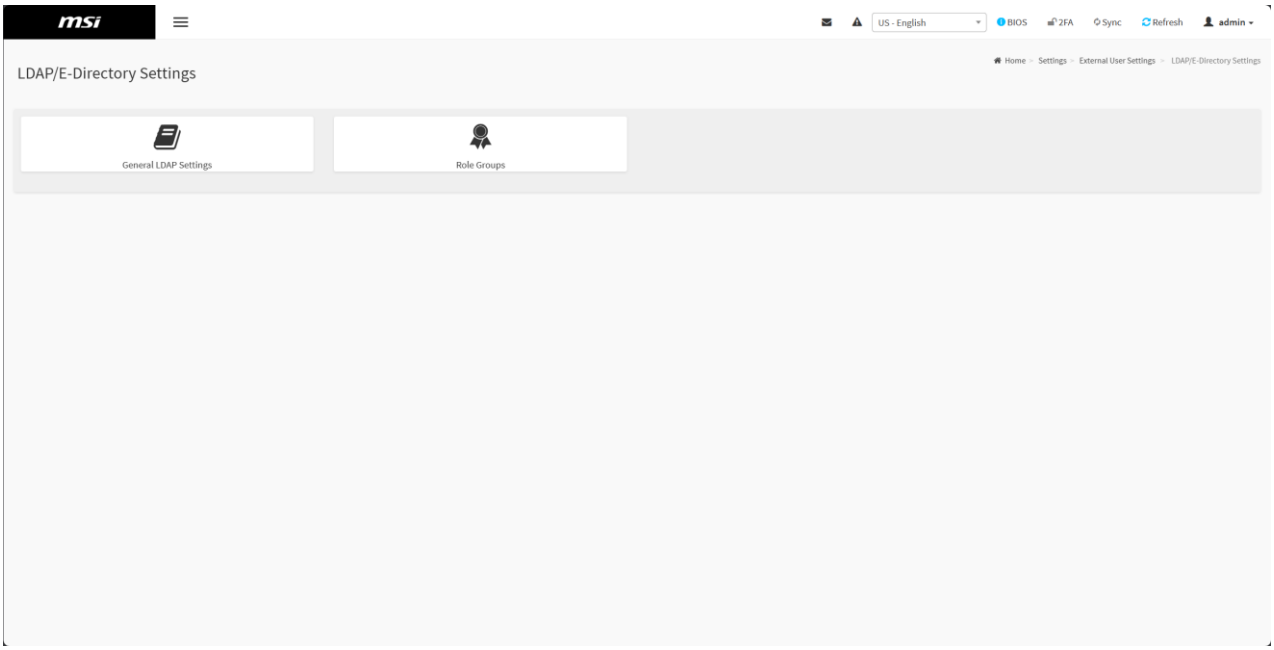
To open External User Services page, click **Settings >External User Services** from the menu bar. A sample screenshot of External User Services page is shown below.



External User Services Page

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.



LDAP/E-Directory Settings page

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

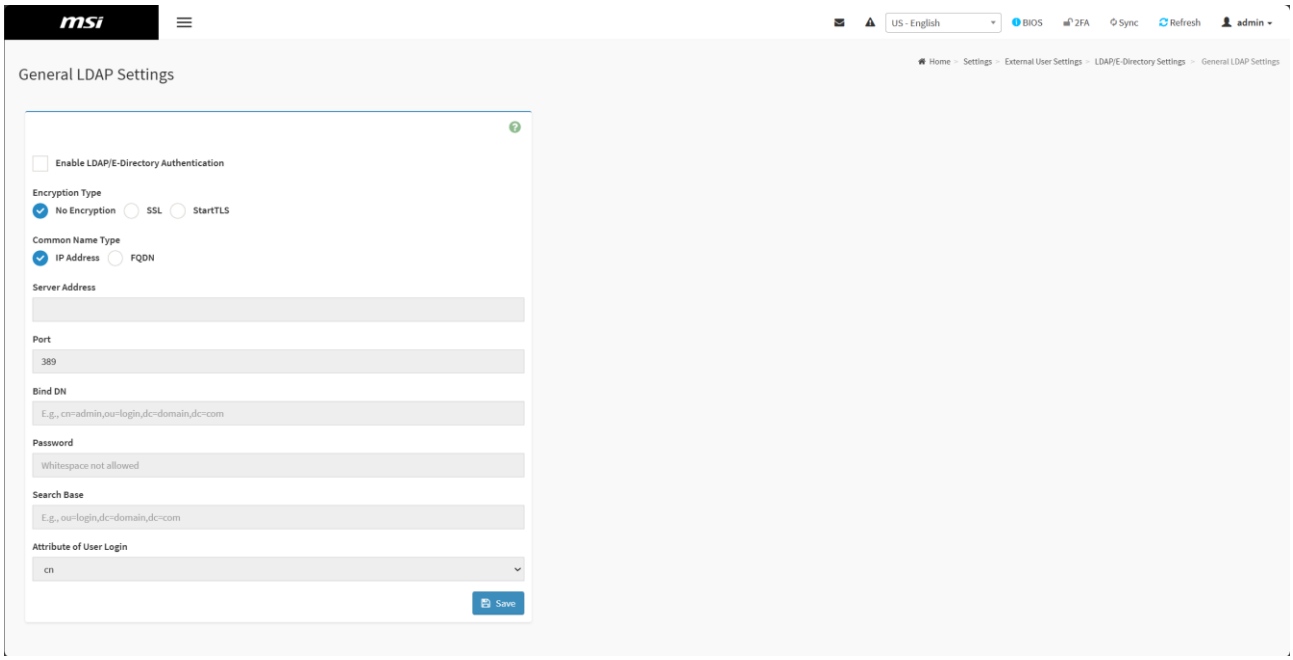
General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port and Search base.

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.



General LDAP/E-Directory Settings

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 FQDN address, when using StartTLS with FQDN.*

6. Specify the LDAP Port in the **Port** field.

   ***Note**: Default Port is 389. For SSL connections, default port is 636. The Port value ranges from 1 to 65535.*

7. Specify the **Bind DN** that is used during bind operation, which authenticates the client to the server.

   ***Note**:*

   Bind DN is a string of 4 to 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 allow more than 48 characters.*

9. Enter the **Search Base**. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory.

   ***Note**: Search base is a string of 4 to 253 alpha-numeric characters. It must start with an alphabetical character. Special Symbols like dot(.), command (,), 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 SSL or StartTLS is enabled.*

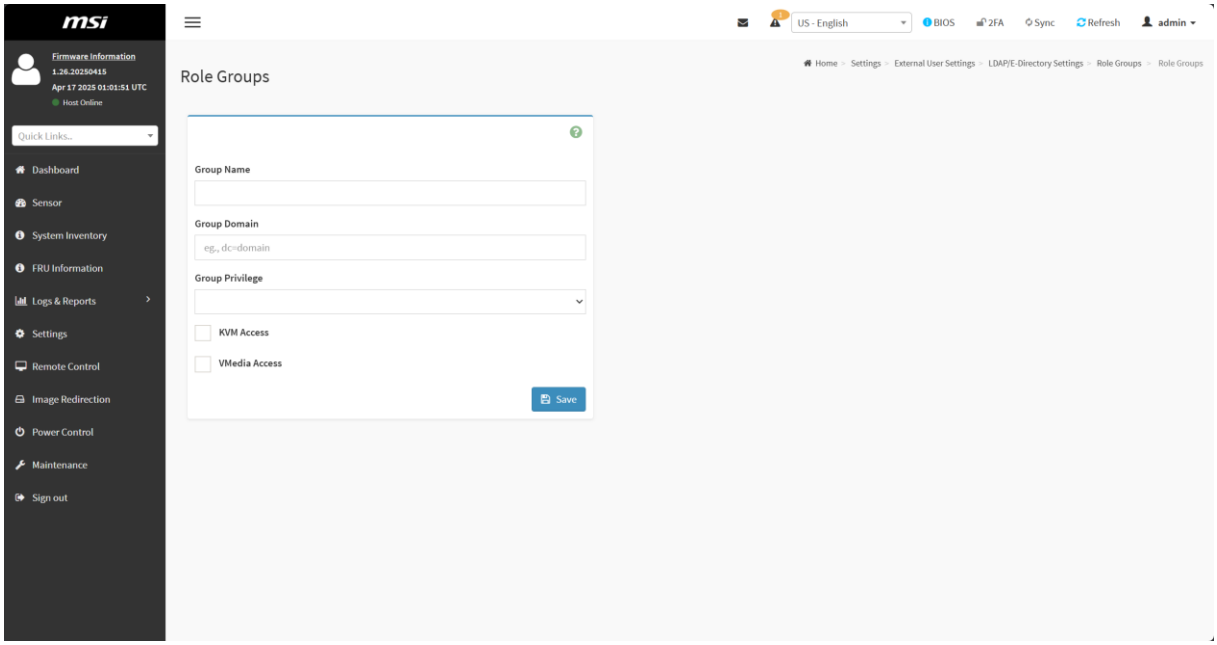
14. Click **Save** to save the settings.

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.



Add Role group Page

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

   ***Note**: VMedia privilege is not applicable for LMedia and RMedia clients.*

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

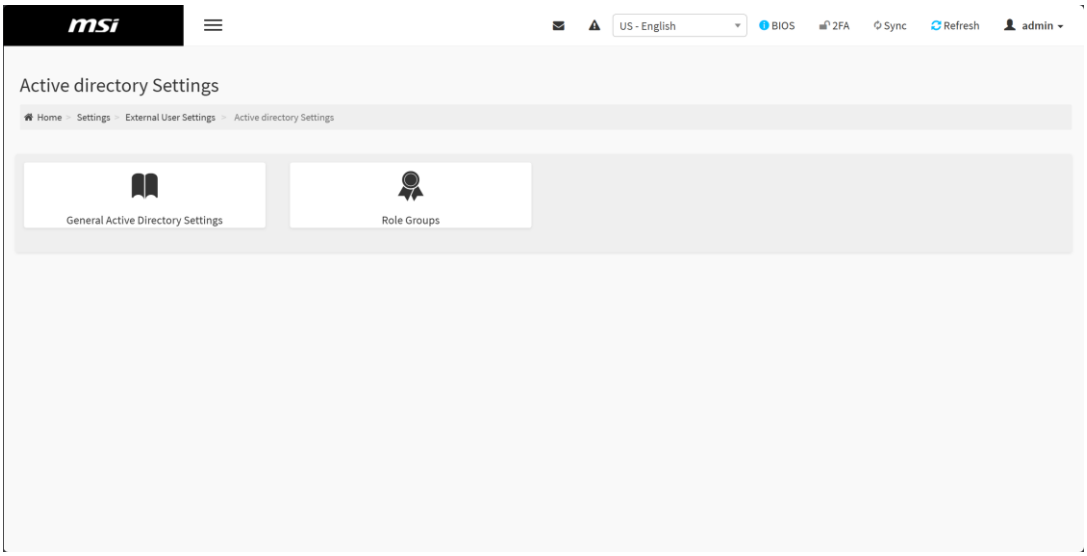
Active Directory Settings

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

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

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

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



Active Directory Settings Page

The fields of Active Directory page are explained below.

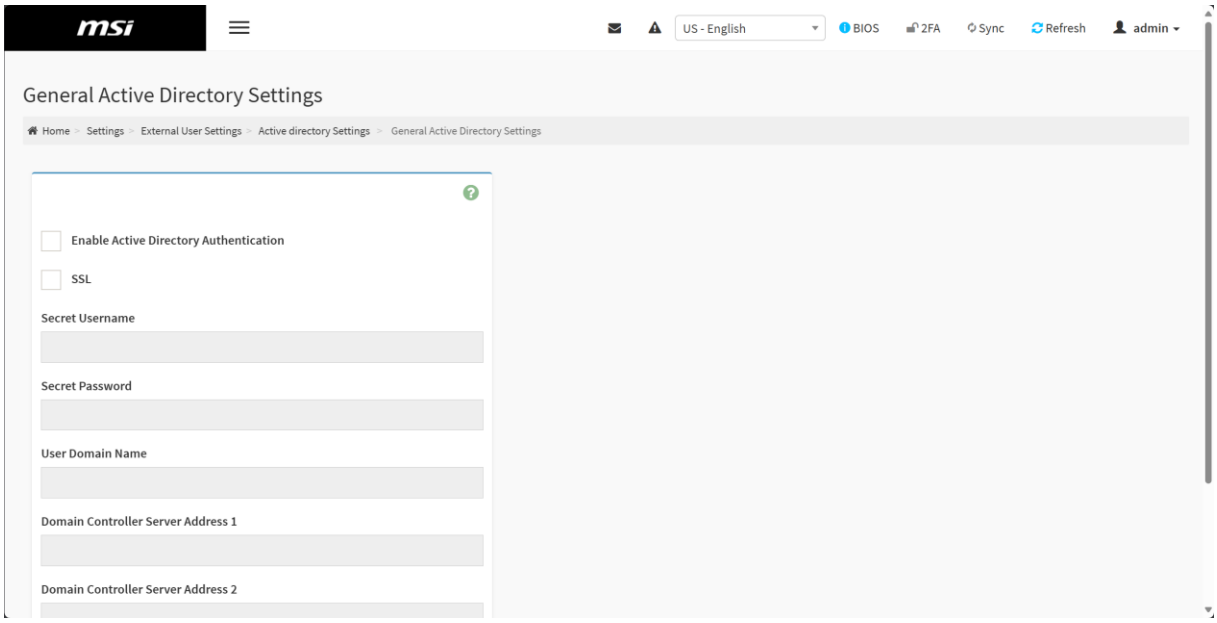
General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.

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.



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 character long and will not allow more than 127 characters.*
   - *White space is not allowed.*

5. Specify the Domain Name for the user in the **User Domain Name** field. E.g., MyDomain.com
   - Domain Name is a string of 255 alpha-numeric characters.

- Special symbols like hyphen, underscore and dot are allowed.

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**:*

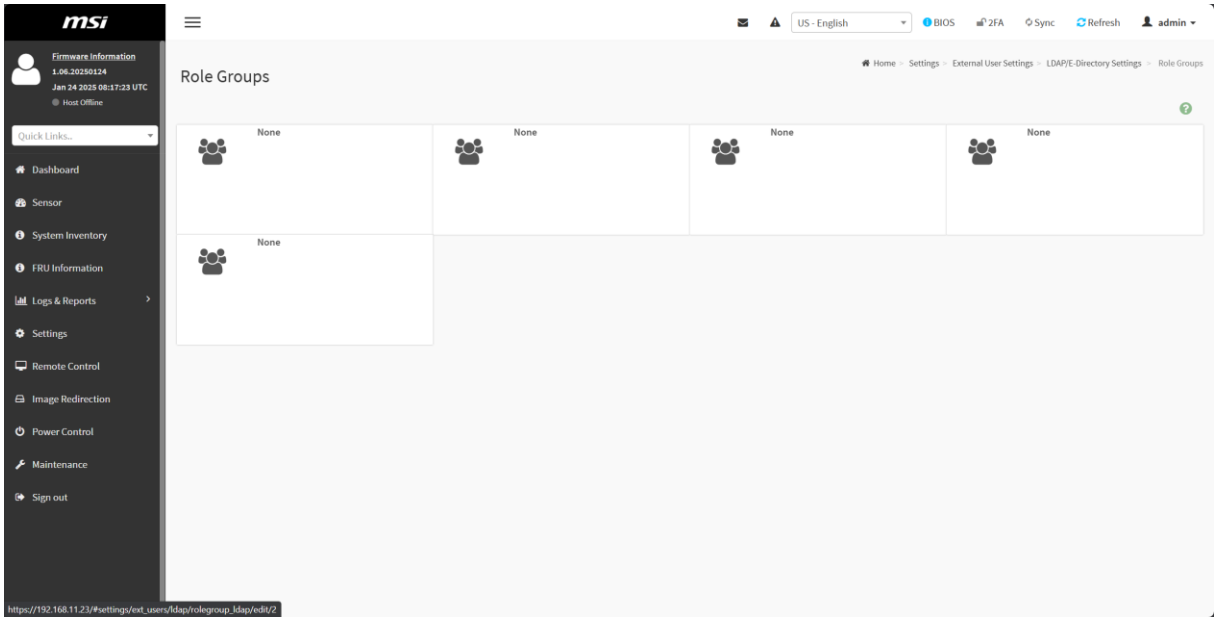
   IP address of Active Directory server: At least one Domain Controller Server Address must be configured. The following address formats are supported. They are IPv4 Address format, IPv6 Address format and FQDN (Fully Qualified Domain Name) format.

   - *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 support 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.



Role Groups

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.

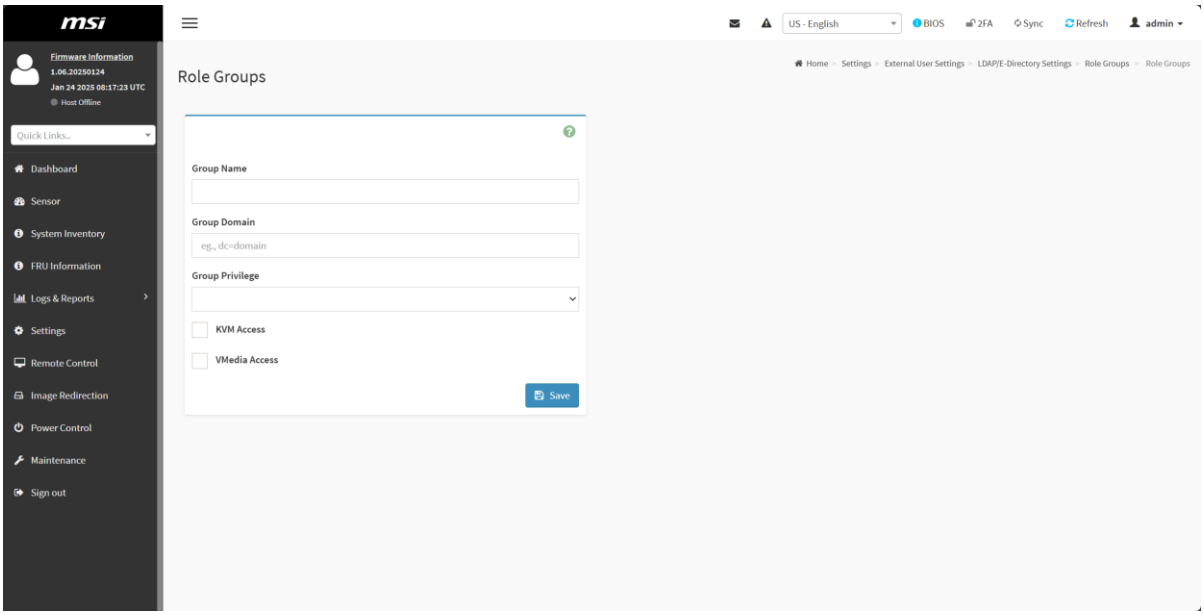
KVM Access: To provide access to KVM for AD authenticated role group user.

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.*



Role Groups Page

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

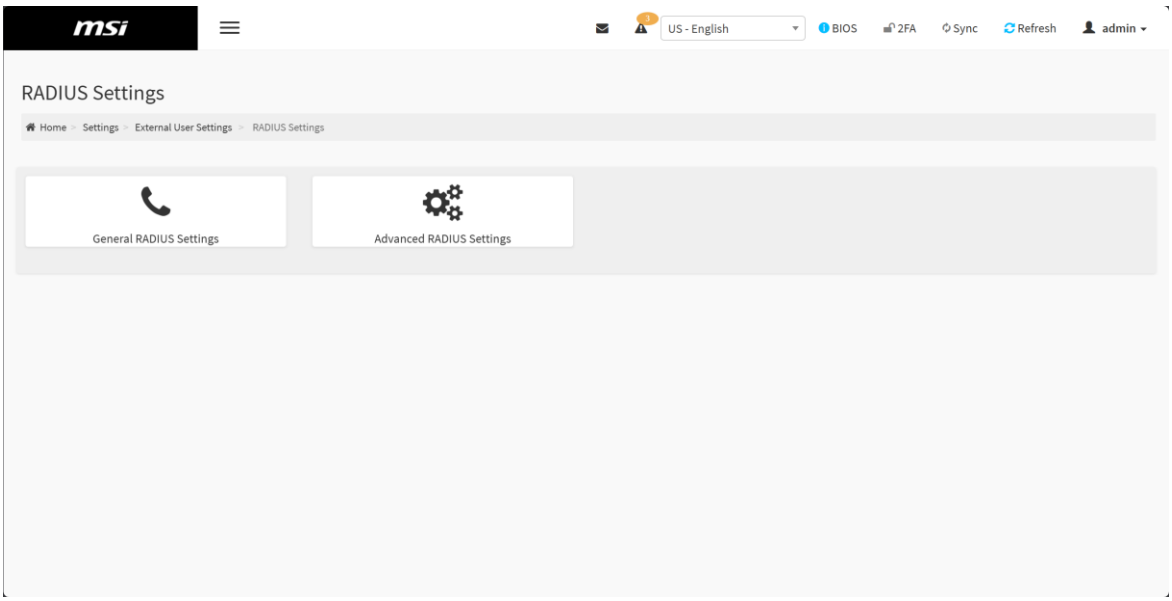
1. In the **Role Groups** Page, select the row that you wish to delete.
2. Click Delete Role Group.

RADIUS Settings

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

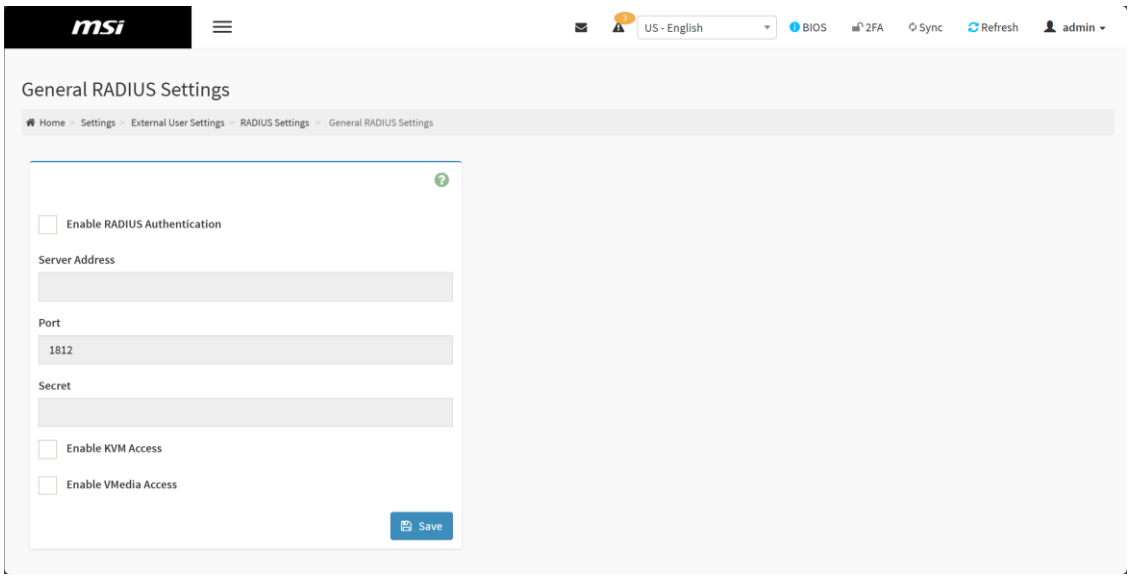
In MSI GUI, this page is used to set the RADIUS Authentication.

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.



RADIUS Settings

General RADIUS Settings



General Radius Settings Page

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.*
- *Port 80 is blocked for TCP/UDP protocols.*

Secret: The Authentication Secret for RADIUS server.

***Note**:*

- *This field will not allow more than 32 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

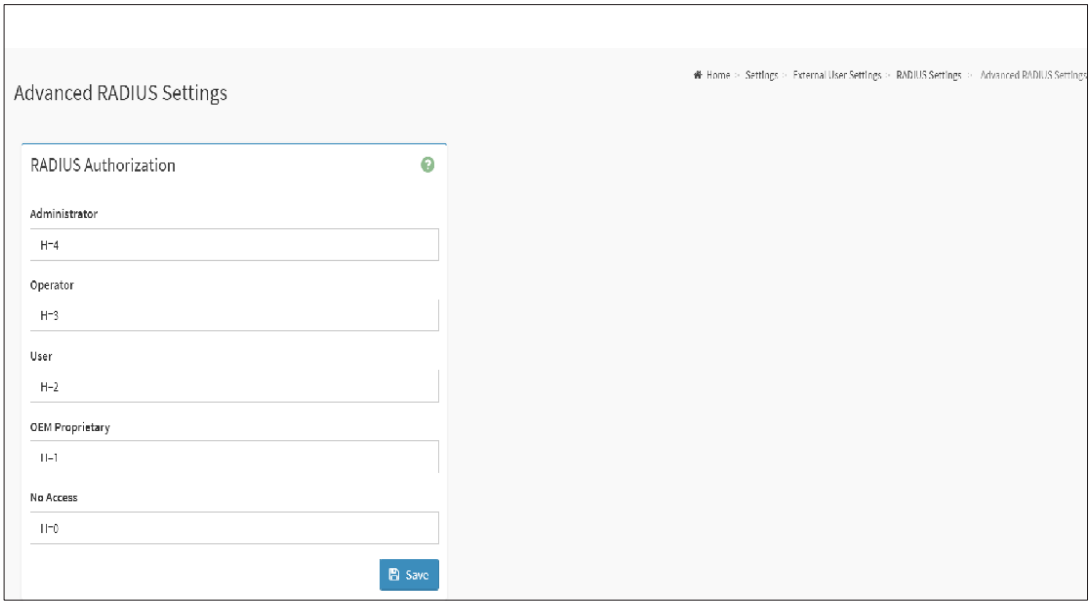
1. Enable the **RADIUS Authentication** check box to authenticate the RADIUS.

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.



Radius Authorization Page

- For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.

Example

- Add Vendor-Specific attribute

cd /usr/share/freeradius

vim dictionary.adtest (Add content below) #dictionary.adtest

VENDOR ADTest 58

Standard attribute BEGIN-VENDOR ADTest

ATTRIBUTE ADTest-group 1 string END-VENDOR ADTest

vim dictionary (Add this line)

SINCLUDE dictionary.adtest

- Add users:

vim users

(Add below content)

"RadiusTest1" Cleartext-Password := "000000"

Service-Type = Administrative-User,

Auth-Type := System,

ADTest-group := “H=4”

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

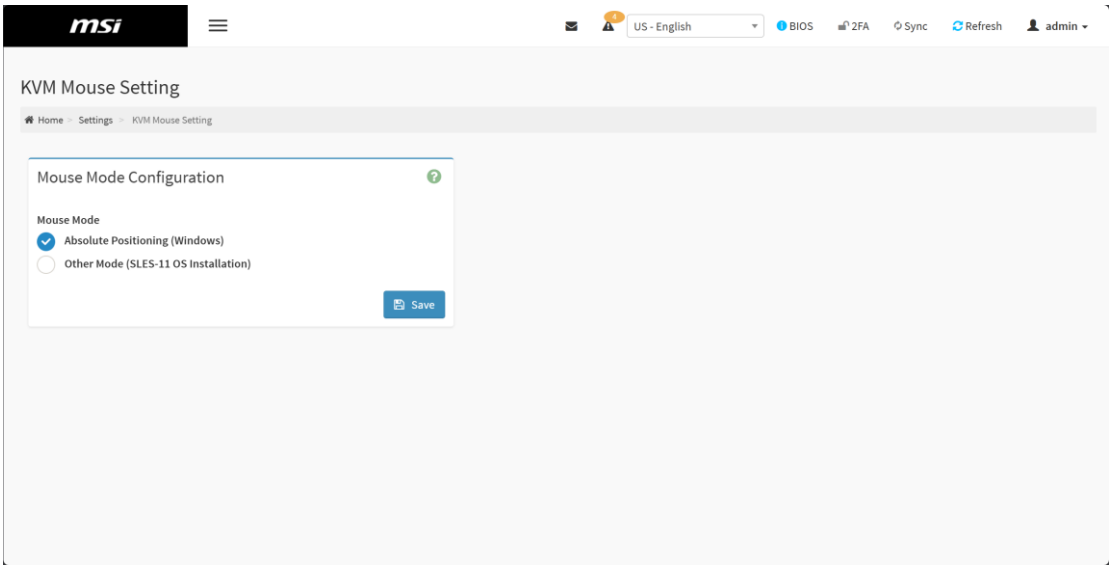
***Note**: These fields will not allow more than 127 characters. ‘;’ and ‘#’ are not allowed.*

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

KVM Mouse Settings

In MSI GUI, Redirection Console handles mouse emulation from local window to remote screen in either of three methods. User has to be an Administrator to configure this option. To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.

To open KVM Mouse setting page, click **Settings >KVM Mouse Setting** from the menu bar. A sample screenshot of KVM Mouse Settings Page is shown below.



Mouse Mode Settings Page

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

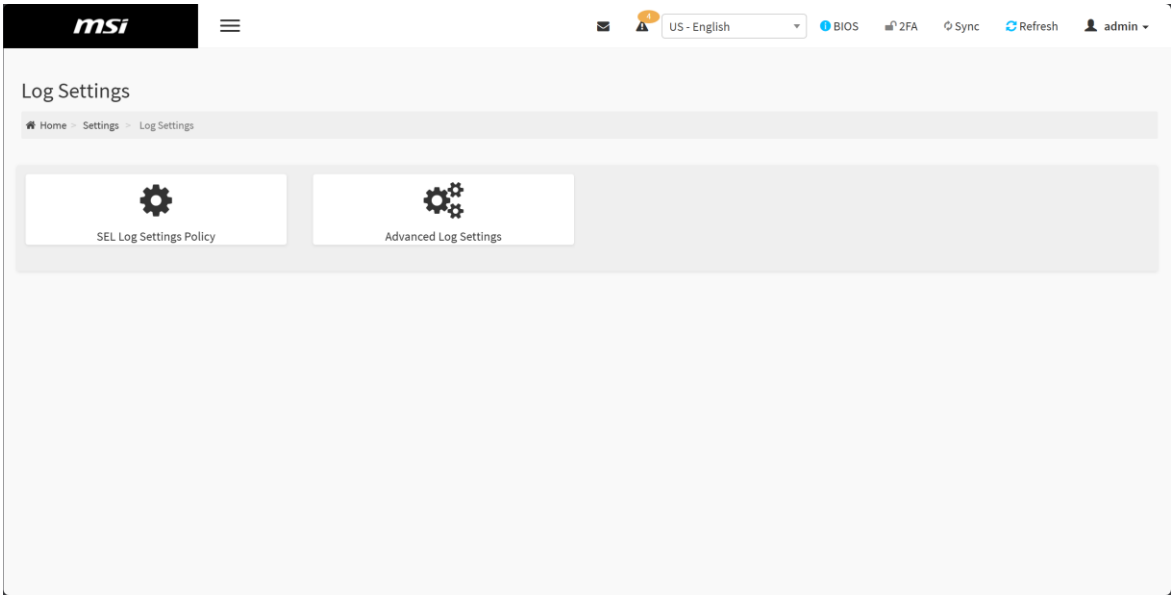
   ***Note**: Recommended for SLES-11 OS Installation*
2. Click **Save** button to save the changes made.

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

Log Settings

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

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



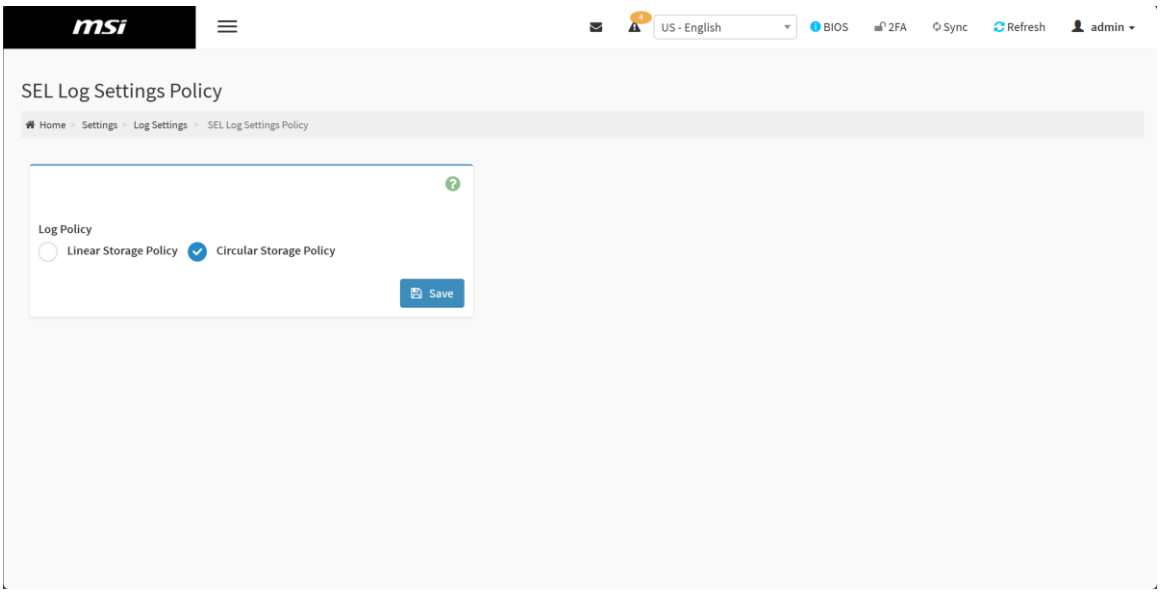
System and Audit Log Settings

The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

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 SEL Log Settings Policy page is shown below.



SEL Log Settings Policy

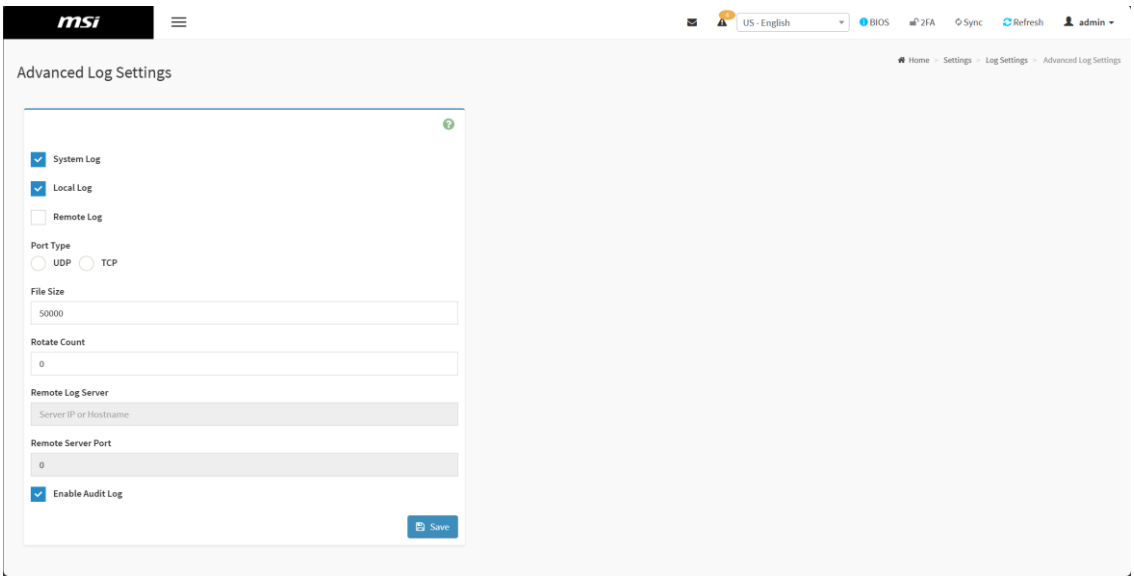
This page is used to configure the log policy for the event log. The fields are as followed.

Log Policy: This field is to enable or disable the Linear Storage Policy or Circular Storage Policy.

Save: To save the configured settings.

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.



Advanced Log Settings

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).

Remote Log: Select Remote Log to save the logs in a remote machine.

***Note**: - You can select either **Local Log/Remote Log** or both Logs as per the requirement.*

- *Either one of the Log selections is mandatory.*
- *Local file resides at /var/log/*

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.*

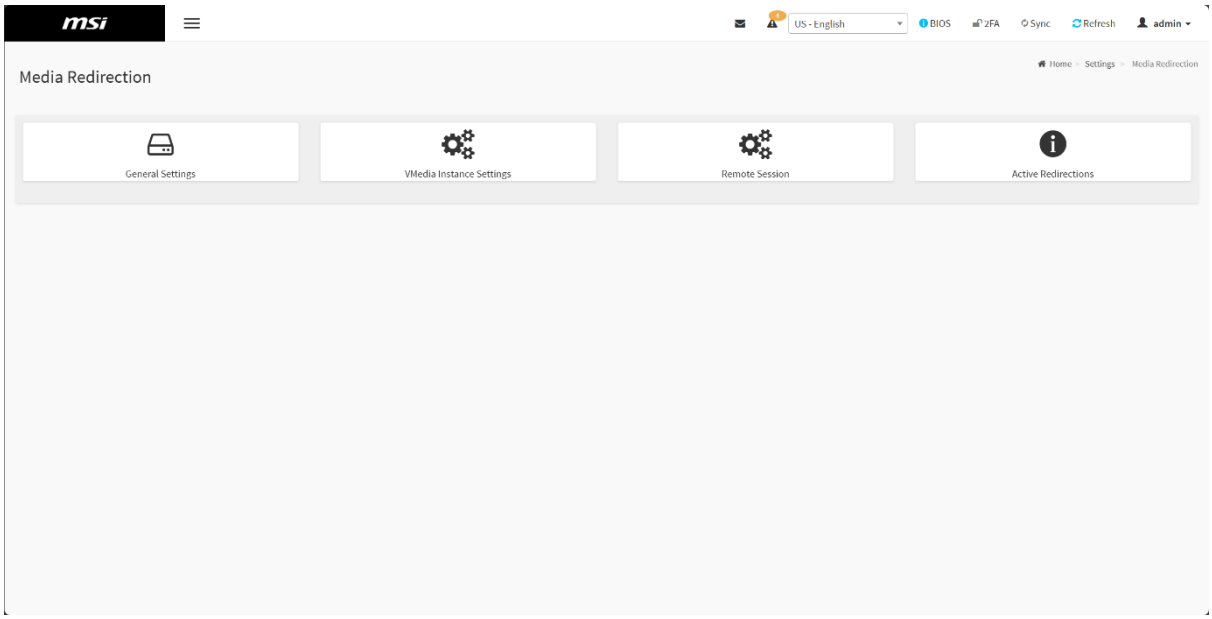
On FC machine, disable the following lines for UDP in /etc/rsyslog.conf.

- MODLOAD imudp
- UDPSERVER 514

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.



Media Redirection

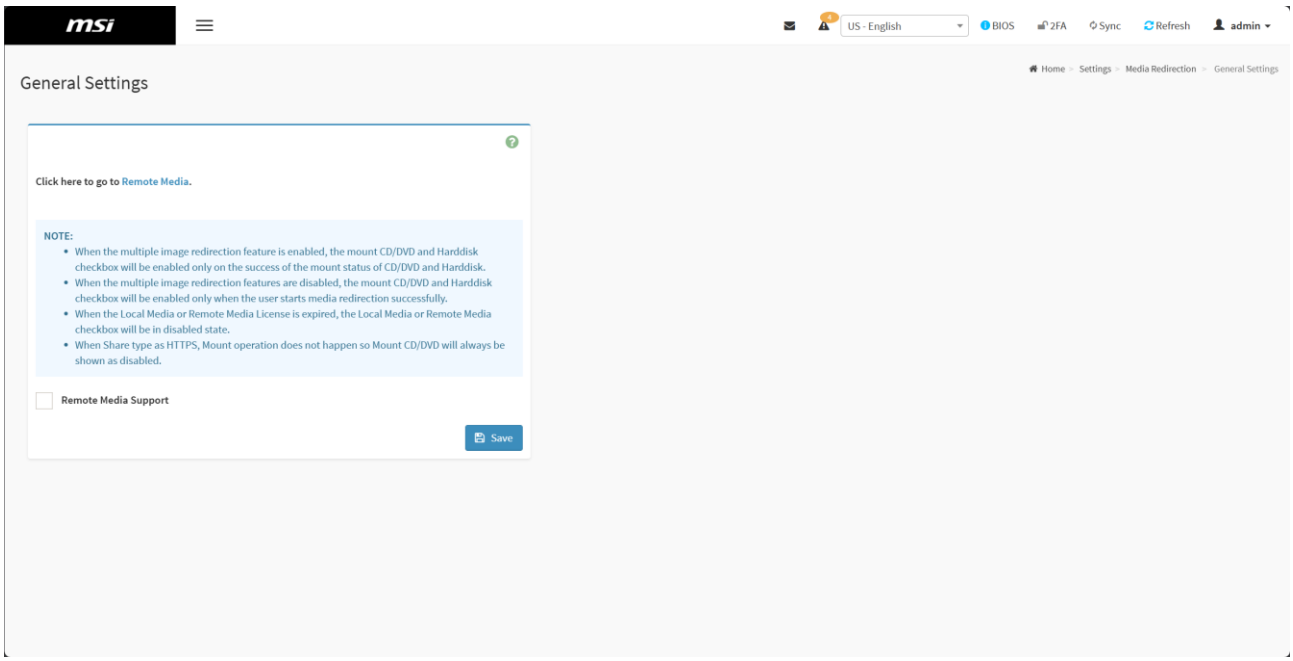
The fields of Media Redirection page are explained below.

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

General Settings

This option is used to configure General Media Settings.

To open General Media Settings section, click **Settings > Media Redirection Settings > General Settings**. Click **LocalMedia** or **Remote Media** for navigating to the appropriate page.



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.*

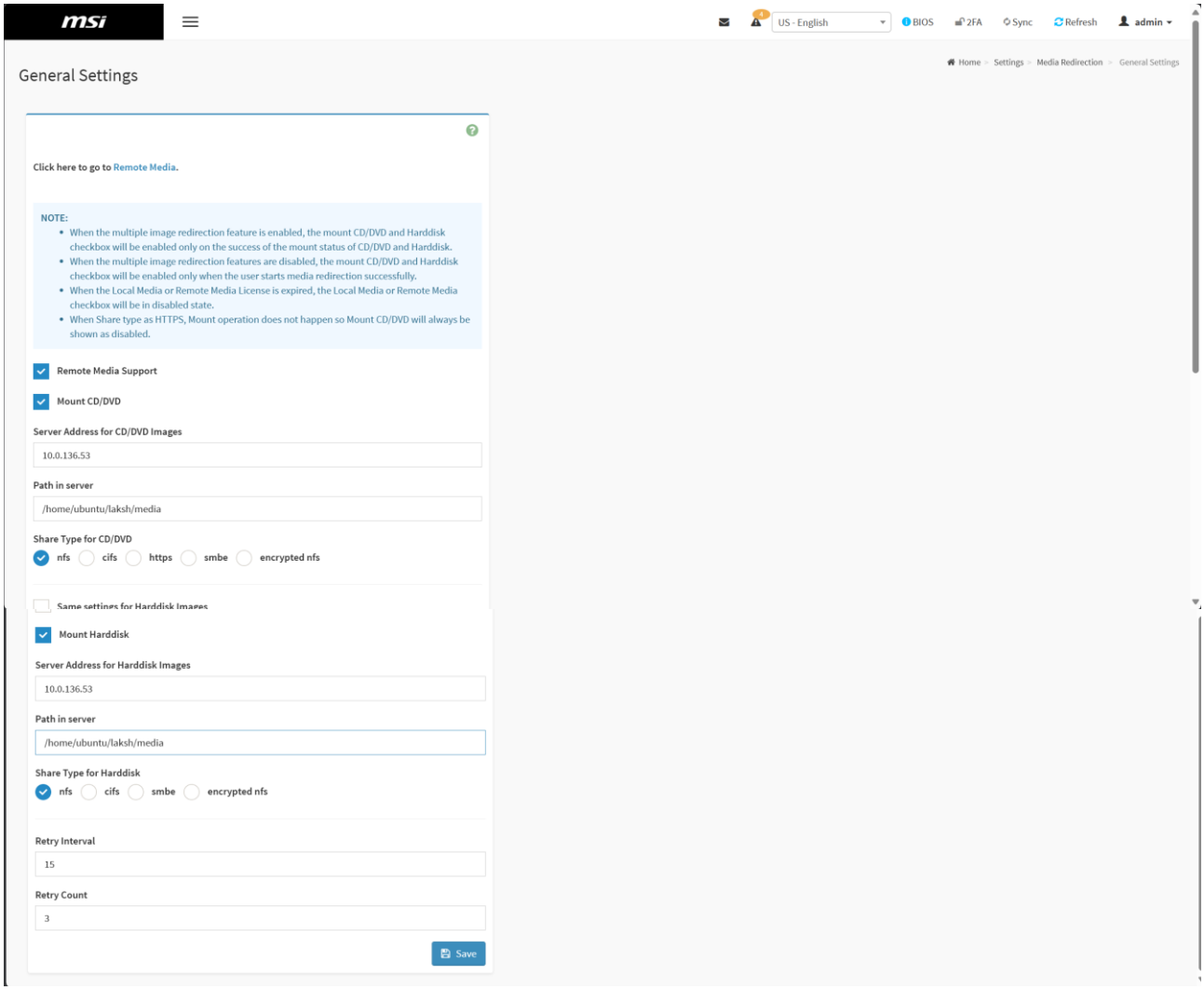
Local Media Support: To enable or disable Local Media support, check/uncheck the '**Enable**' check box.

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 Hard disk

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.



General Settings

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.

***Note**: To display/hide the SMBE option in Media Redirection General Settings page, based on feature "CONFIG_SPX_FEATURE_RMEDIA_CIFS_ENC" is enabled/disabled respectively.*

- **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 en- crypted 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.*

– *To display/hide the HTTPS option in Media Redirection General Settings page, based on feature "CONFIG_SPX_FEATURE_RMEDIA_HTTPS_IMAGE_REDIR" is enabled/disabled respectively.*

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.

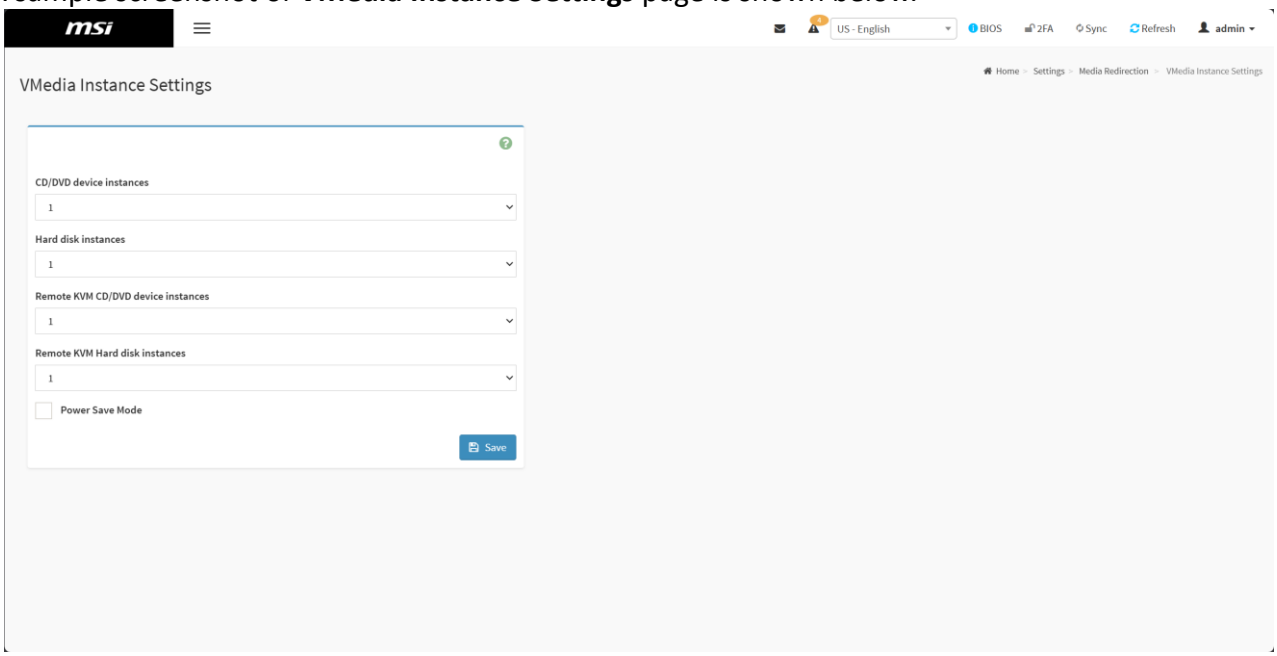
***Note**: For RMedia share types, we support the following NFS, CIFS, HTTPS, SMBE and encrypted NFS mount protocols, for mounting remote image share paths to the BMC.*

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

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.



VMedia Instance Settings

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 hard disk devices supported for Virtual Media redirection.

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

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

Power Save Mode: To enable or disable the virtual USB devices visibility in the host. If this option is enabled, Virtual media devices will be connected to the Host machine only at the instance launching KVM session. If this option is disabled, Virtual media devices will remain connected to the host machine all the time irrespective of KVM session status. If media is redirected from a kvm/media client and the client application is closed then the respective media session will be disconnected.

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, Hard disk 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 Hard disk drives.*

2. Check the **Power Save Mode** option to enable/disable the Virtual USB devices visibility in the host.
3. Click **Save** to save the changes made else click Reset to reset the previously saved values.

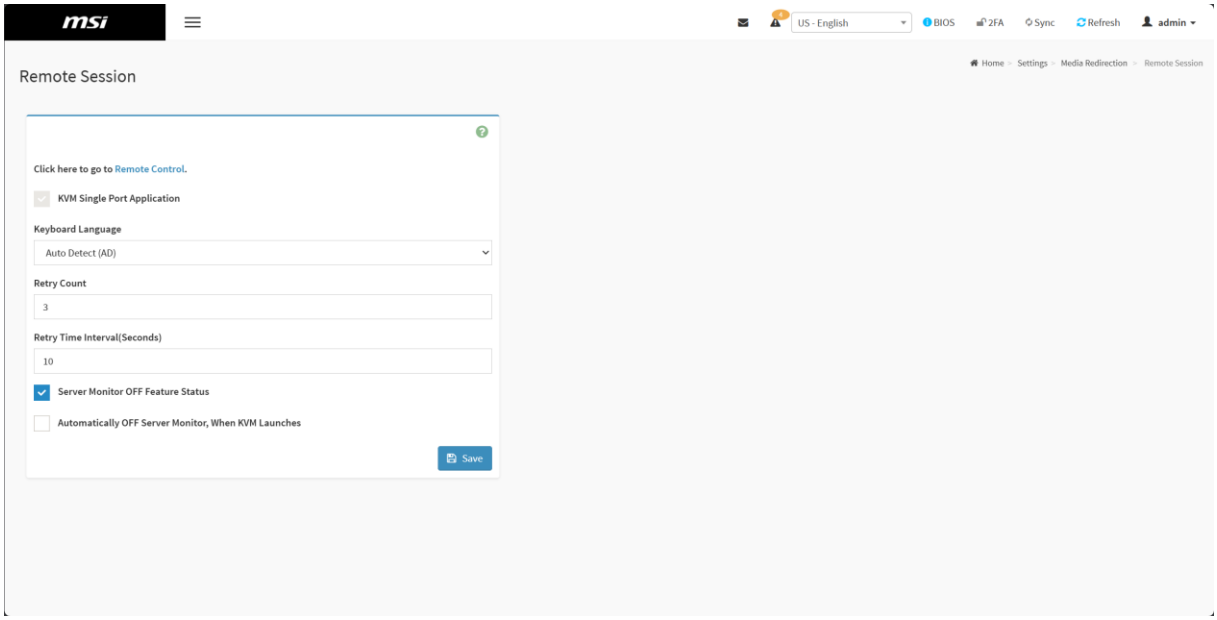
   ***Note**: When KVM is launched from Standalone Application, If there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.*

   Unmounting device will make the driver disconnect device when using Auto Attach. Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected.

Remote Session

In MSI SP, 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 > 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.



Remote Session

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.

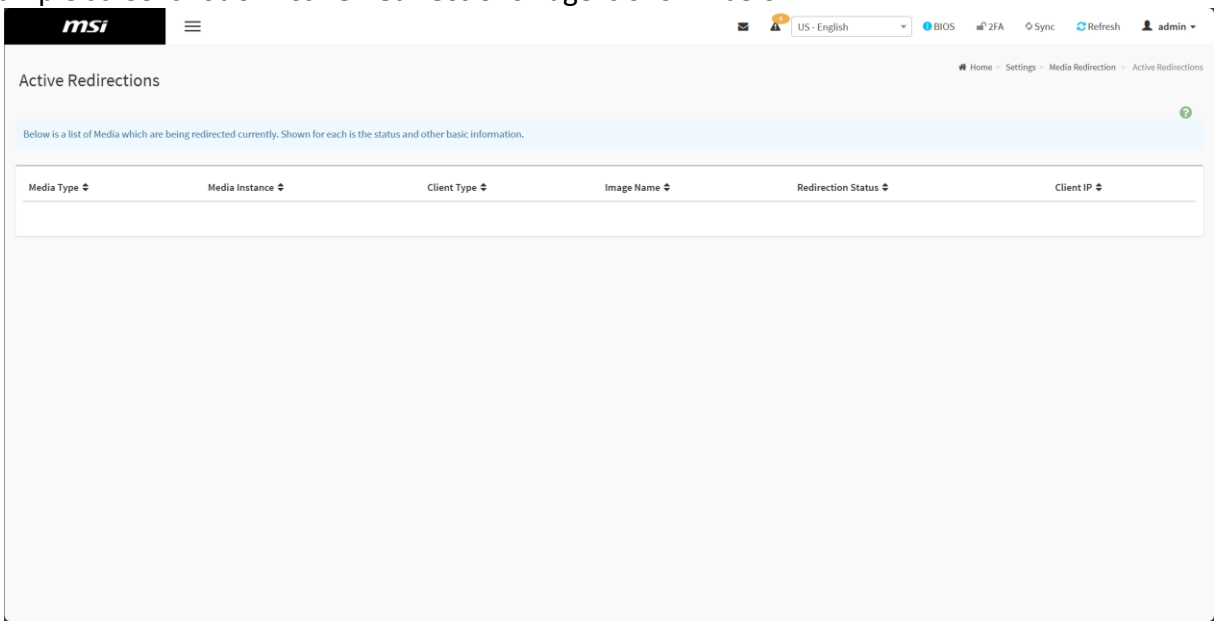
Procedure

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 attempt.
4. Check the **Server Monitor OFF Feature Status** check box to enable Local Monitor ON/OFF command during runtime.
5. Check the **Automatically OFF Server Monitor, When KVM Launches** check box to automatically Lock the local monitor during H5Viewer launch.
6. Click **Save** to save the current changes.

Active Redirections

This page is used to display the active redirected media, which are redirected via JViewer/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.



Active Redirections

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 (JViewer/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.

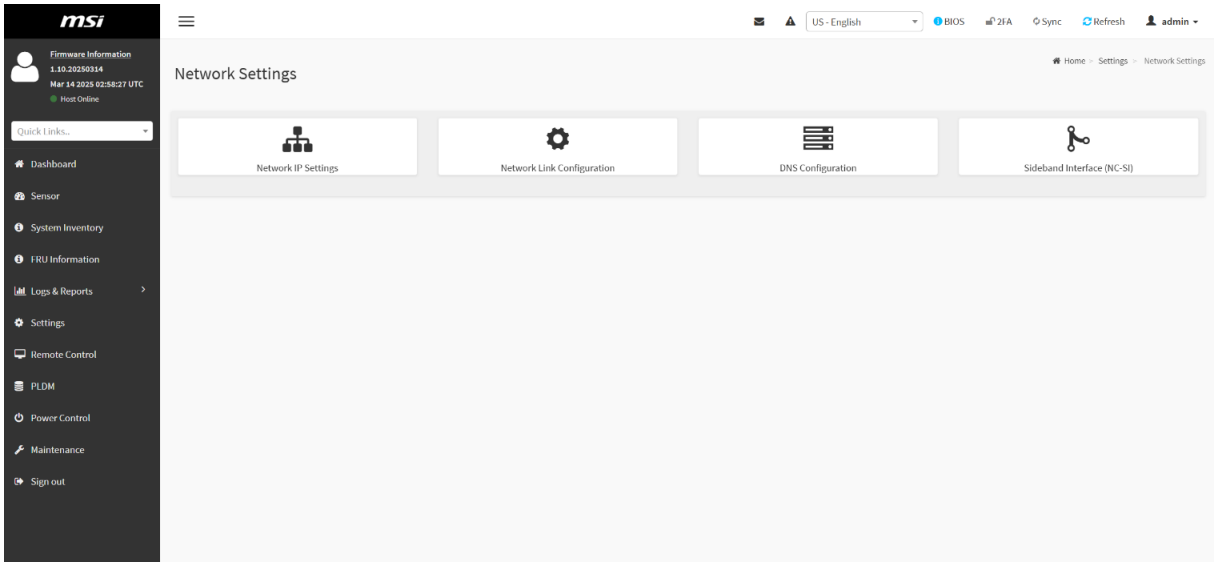
Client IP: The IP of the connected Media devices (CD/DVD) supported for Active Redirections.

> ***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.*

Network Settings

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

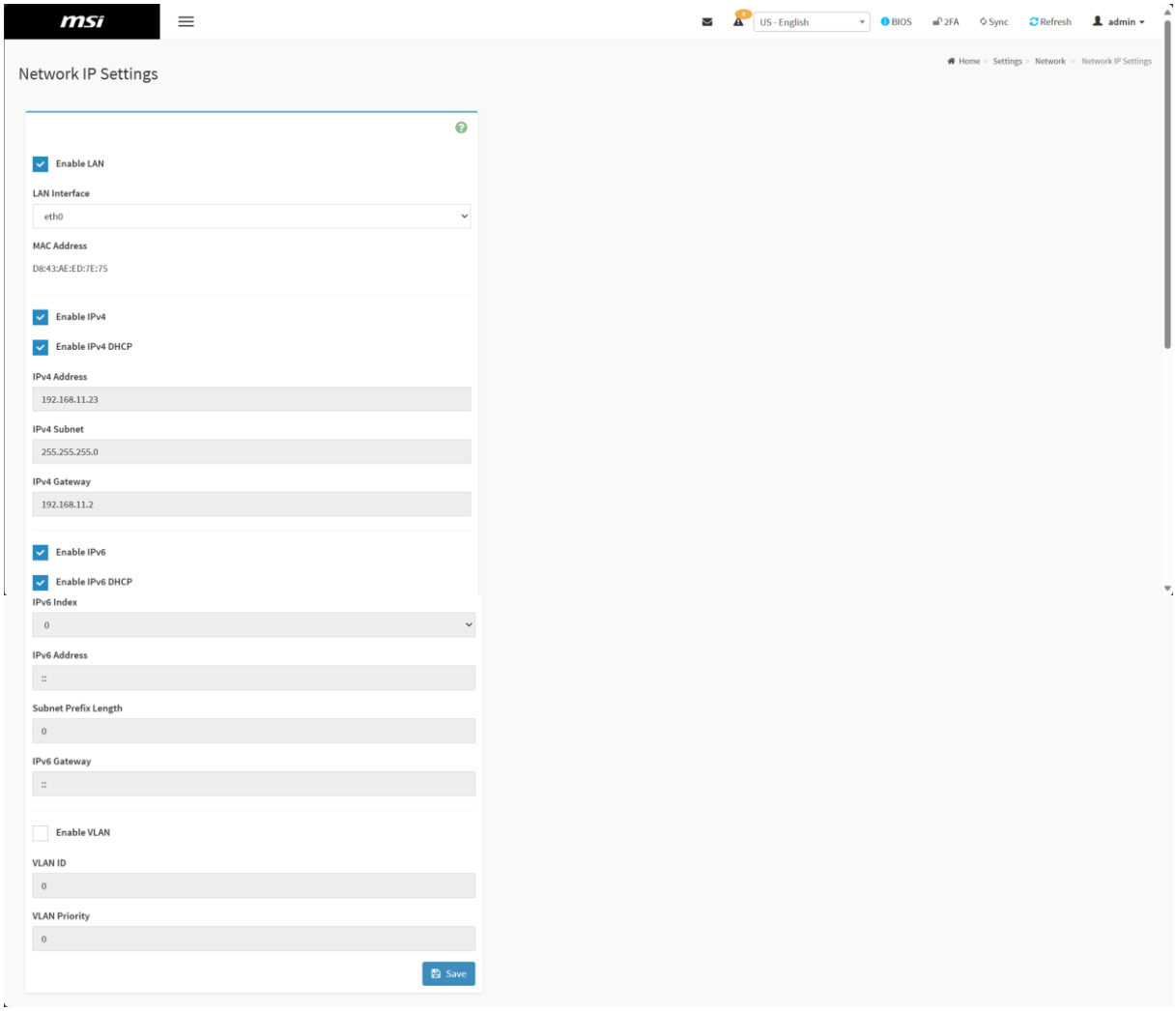
A sample screenshot of **Network Settings** page is shown below.



Network Settings Page

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. A sample screenshot of **Network Settings** page is shown below.



Network IP Settings Page

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 for the selected interface 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 for the selected interface in the device.

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. E.g.: 0

IPv6 Address: To specify a static IPv6 address to be configured to the device. E.g.: 2004::2010. User can mention

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 cannot 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:

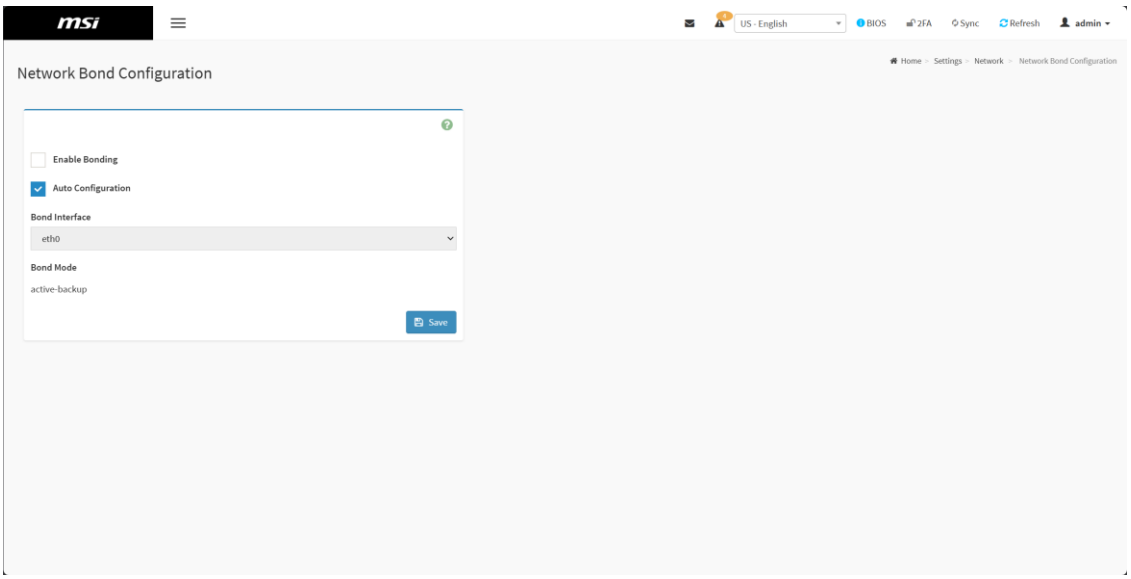
1. Check **Enable LAN** to enable LAN support for the selected interface.
2. elect the **LAN Interface** to be configured.
3. Check Enable IPv4 to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled,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

Network Bond Configuration

In MSI GUI, 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 Bond Configuration** page is shown below.



Network Bond Configuration Page

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 cannot 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 behavior 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.

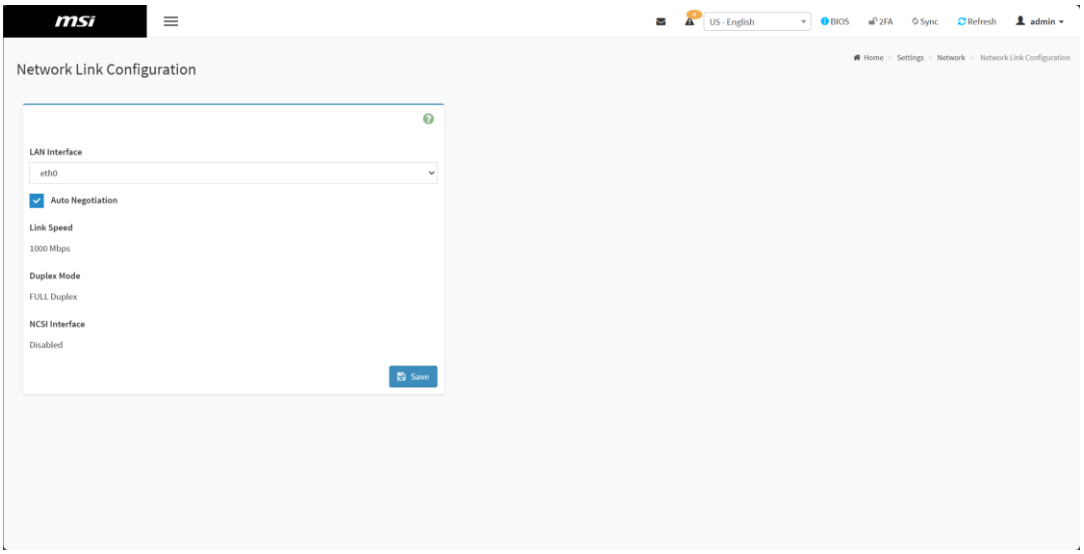
Case 2 : When Bond Interface Channel IP source is Static

Bond interface will be assigned a static IP address and other LAN Parameter as per Channel 1.

Network Link Configuration

In MSI GUI, 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 Configuration** from the menu bar. A sample screenshot of **Network Link Configuration** page is shown below.



Network Link Configuration Page

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.*

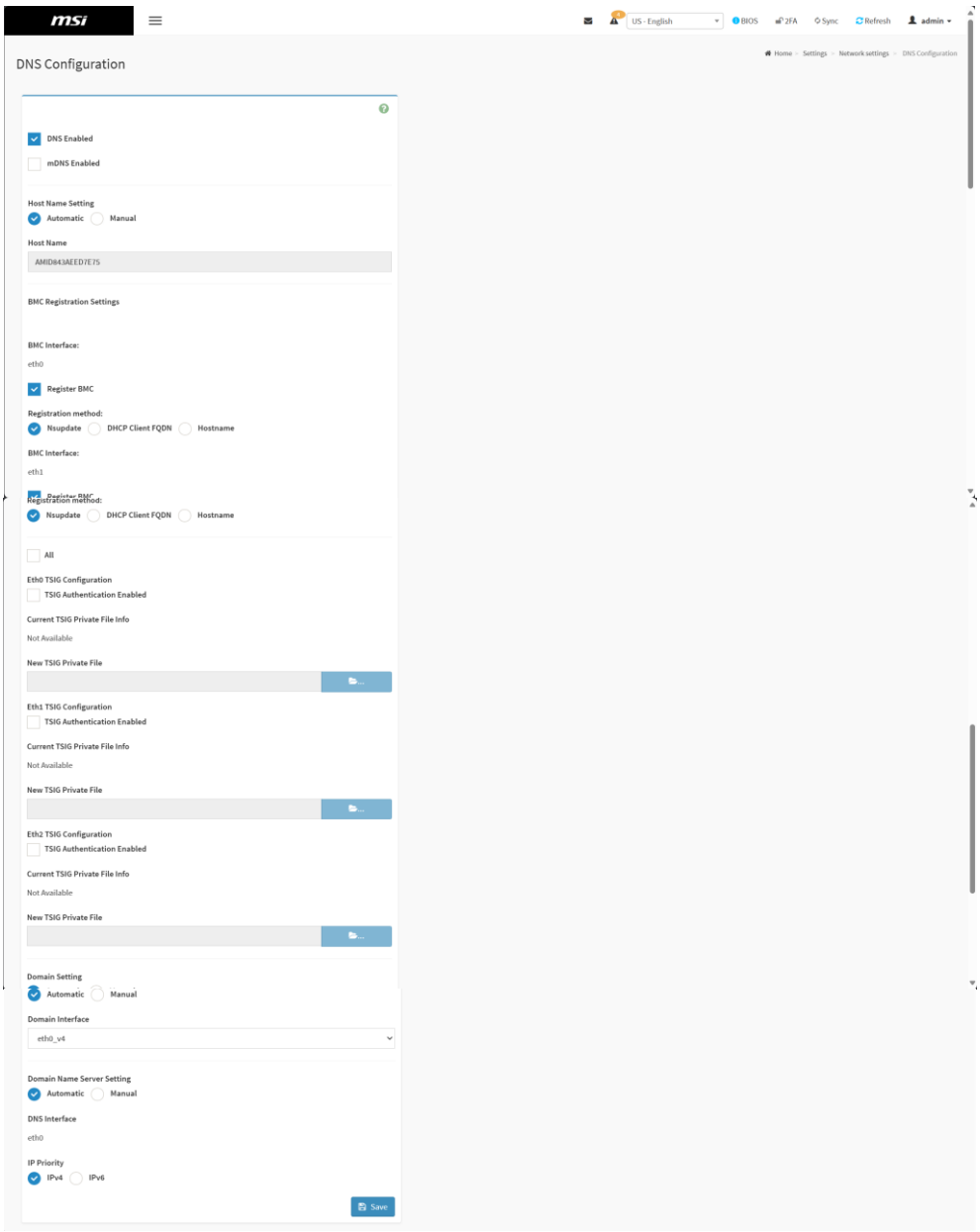
3. Select the **Link Speed** from the drop-down list.
4. Select the **Duplex Mode** either Full duplex or Half duplex.
5. Click **Save** to save the configuration.

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.



DNS Configuration Page

The fields of DNS Configuration page are explained below.

Domain Name Service Configuration

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

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

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 is not a legal character for use in host names.*

BMC Registration Settings

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

Register BMC: To register BMC through registration method.

Registration Method

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

TSIG Configuration

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

Eth 0&1:

- **TSIG Authentication Enabled**: Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
- **Current TSIG Private File**: The information of Current TSIG private file along with its uploaded date/time will be displayed (read-only).
- **New TSIG Private File**: Browse and navigate to the TSIG private file.

***Note**: TSIG file should be of private type.*

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

- **Automatic** - If you Select Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** - If the Domain setting is chosen as Manual, then specify the domain name of the device.

***Note**: If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name".*

- **Domain Name**: It displays the domain name of the device, 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 at least 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.

DNS over HTTPS Setting:

***Note**: if this feature enabled CONFIG_SPX_FEATURE_DNS_OVER_HTTPS_SUPPORT DNS over HTTPS Setting with following fields will be displayed.*

Mode: Select the DNS over HTTPS mode configuration with Disable or Automatic or Manual.

Disable - If you select Disable DNS over HTTPS will be disabled.

Automatic - If you select Automatic then DNS over HTTPS settings enabled - Automatic with auto server and service traffic should be configured for configured for the BMC.

- Server: Select the DNS over HTTPS auto server configuration with,
- Google
- Cloudflare
- OpenDNS
- Service Traffic: Select the DNS over HTTPS auto Service Traffic configuration with,
- IPv4
- IPv6
- Both

Manual - Specify the DOH DNS URL to be configured for the BMC.

DOH DNS Server 1, 2 & 3

To specify the DOH DNS Manual 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

DOH DNS URL

To specify the DOH DNS URL to be configured for the BMC.

- All valid URLs follow a specific pattern: protocol, domain name, and path.

Save: To save the entered changes.

Procedure:

1. In Domain Name Service Configuration, Enable DNS Service.
   - Check the option **DNS Enabled** to enable all the DNS Service Configurations.
2. Choose the **Host Name Setting** either Automatic or Manual

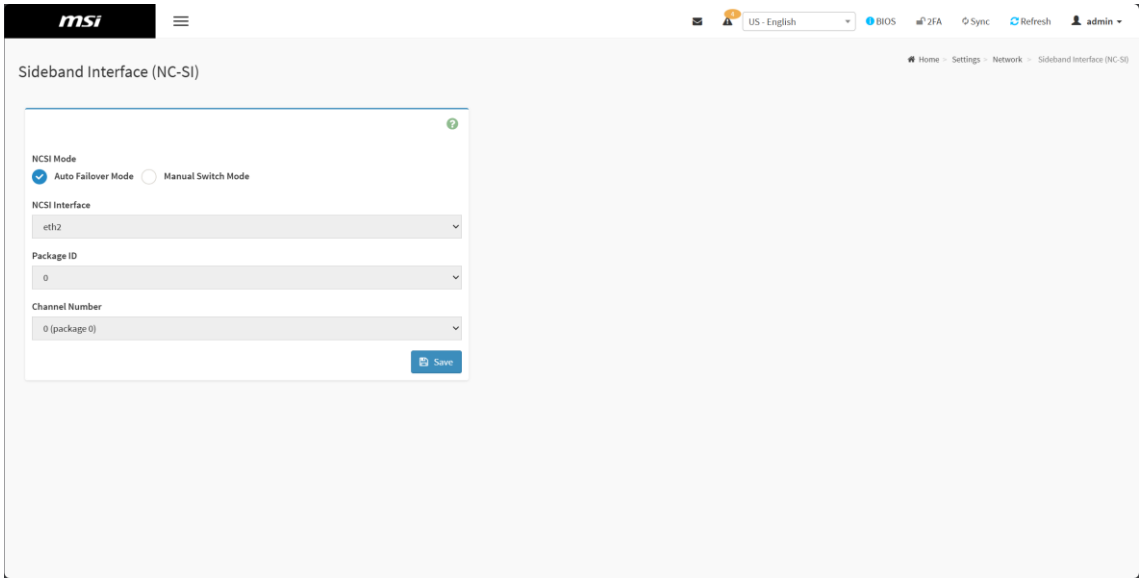
   Note*: If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.*

3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC's network port to register with DNS settings.
   - Check **Register BMC** option to register with DNS settings.
   - **Nsupdate** - Choose **Nsupdate** option to register with DNS server using nsupdate application.
   - **DHCP Client FQDN** - Choose **DHCP Client FQDN** option to register with DNS Server using DHCP option 81.
   - **Hostname** - Choose **Hostname** option to register with DNS server using DHCP option 12.

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

5. Check **Both** options 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.



NC-SI Configuration

The following fields are displayed in this page.

NCSI Mode: To Select the NCSI Mode either Auto Failover Mode or Manual Switch mode.

NCSI Interface: It lists the interface name in list box.

Channel Number: Lists the channel number of the selected interface.

Package ID: Lists the package id of the selected interface.

Save: To save the current changes.

Procedure

- Select **NCSI Mode** type either Auto Failover Mode or Manual Switch Mode.

***Note**:*

– *- If you select Auto Failover Mode, the NCSI Interface will be configured automatically as displayed below.*

10. In DNS over HTTPS Setting,

Select the Mode for DNS over HTTPS Setting with Disable or Automatic or Manual. If mode selected as Automatic then following fields should be configured.

- **Server**: Select the DNS over HTTPS auto server configuration with,
- Google
- Cloudflare
- OpenDNS
- **Service Traffic**: Select the DNS over HTTPS auto Service Traffic configuration with,
- IPv4
- IPv6
- Both

If mode selected as Manual then following fields should be configured.

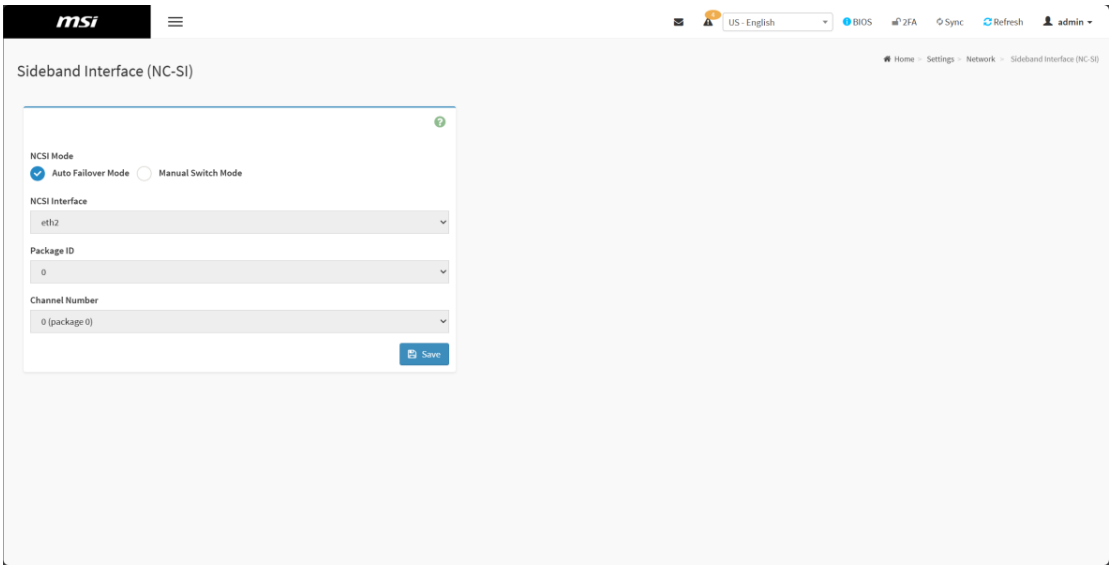
- DOH DNS Server 1, 2 & 3
- DOH DNS URL

11. lick **Save** to save the entries.

NC-SI Configuration

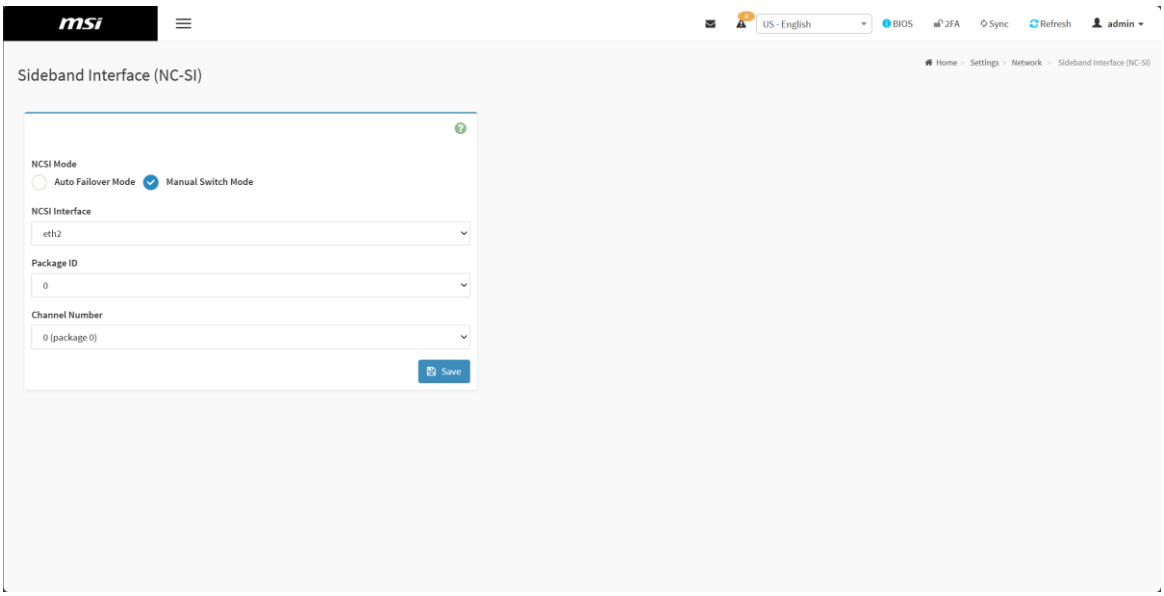
In MSI GUI, this page is used to configure Network Controller Sideband Interface (NCSI) configuration settings.

To open NC-SI page, click **Settings > Network Settings > Sideband Interface (NCSI)Configuration** from the menu bar. A sample screenshot of **Sideband Interface (NCSI)** Page is shown below.



Auto Failover Mode

- If you select Manual Switch Mode only you are allowed to configure NCSI Interface, Channel number and Package ID as displayed below.



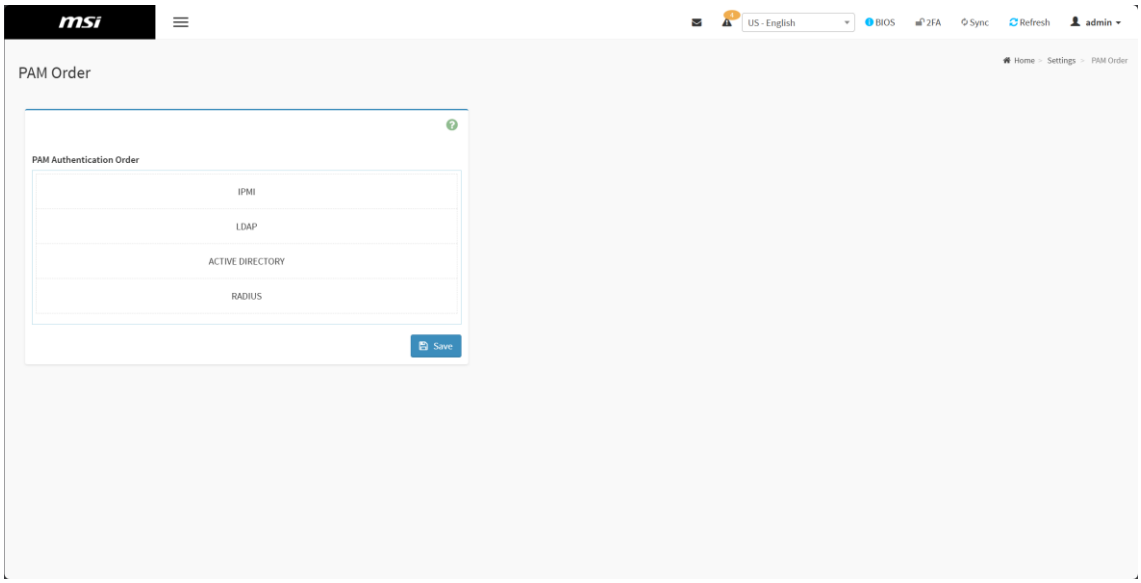
Manual Switch Mode

1. Choose the particular **NCSI Interface** to which you need to configure NCSI settings.
2. Choose the **Channel Number** to be configured for the selected Interface name.
3. Choose the **Package ID** to be configured for the selected Interface name.
4. Click **Save** to save the current changes.

PAM Order Settings

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

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



PAM Order Settings Page

The fields of **Settings > PAM Ordering** page are explained below.

PAM Module: It shows the list of available PAM modules supported in BMC.

***Note**:*

- *It is recommended to not to keep same username for different PAM modules.*
- *If Authentication fails, the reason of fail could be invalid User or Invalid Password.*
- *If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So, it is always treated as Invalid username error and PAM will try other Authentication Methods.*
- *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.*

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.

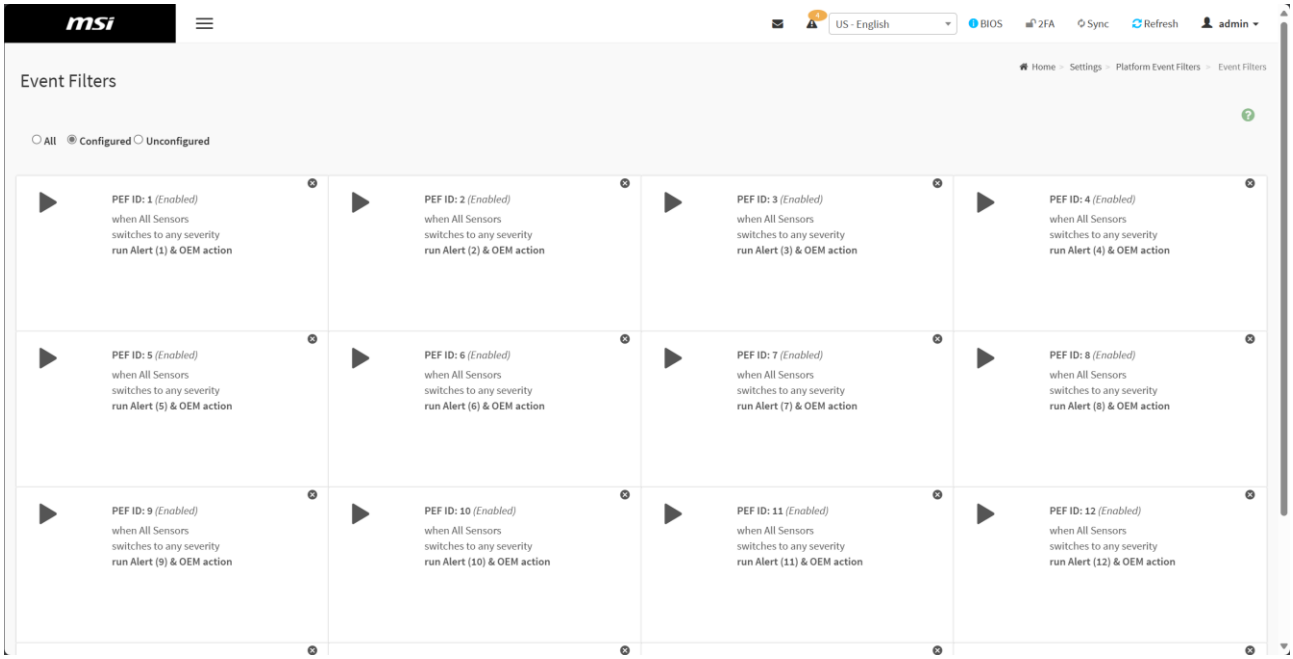
In MSI GUI, the PEF Management is used to configure the following

- Event Filters
- Alert Policies
- LAN Destinations

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

Event Filters

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



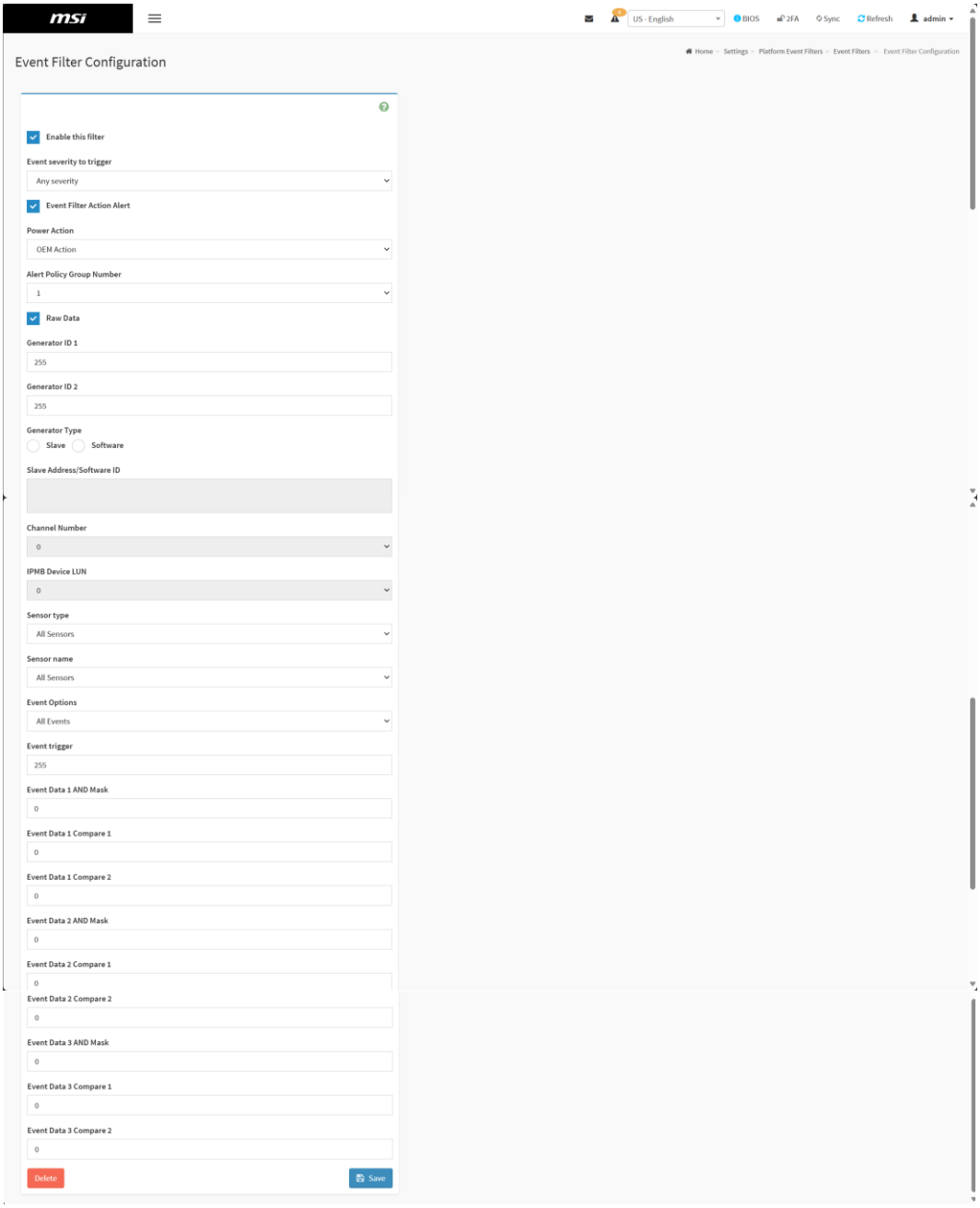
Event Filters

The fields of Platform Event Filters Tab are explained below.

This page contains pre-configured 40 Events with PEF IDs. Click **Delete** icon (**x**) 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 **SensorName** 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.

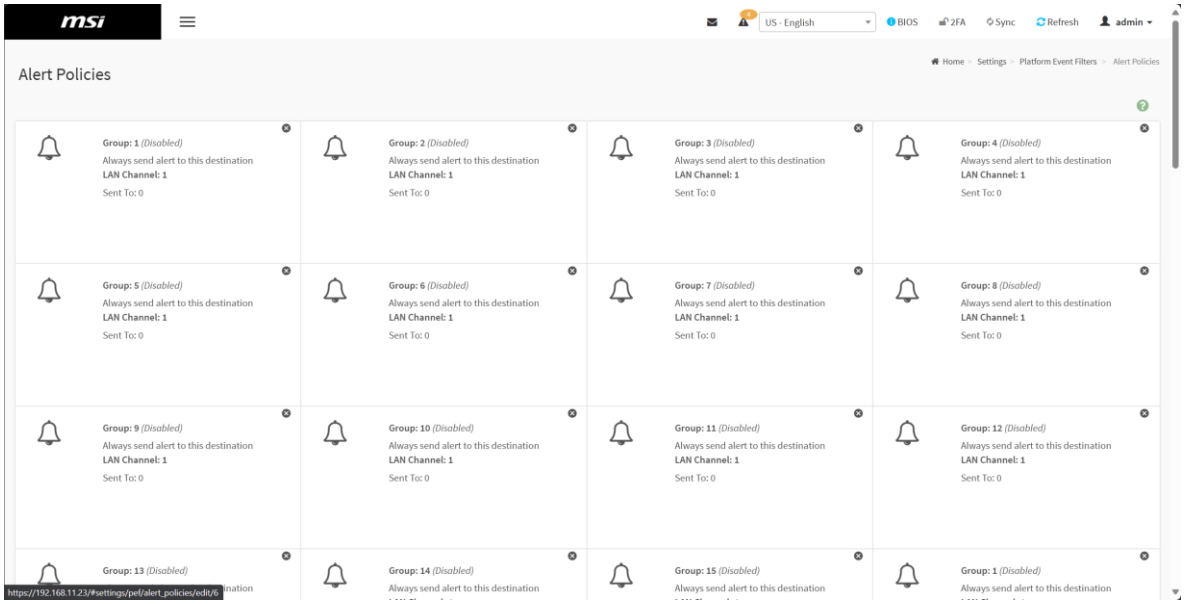
***Note**: Value ranges from 0 to 255.*

- **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.

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.

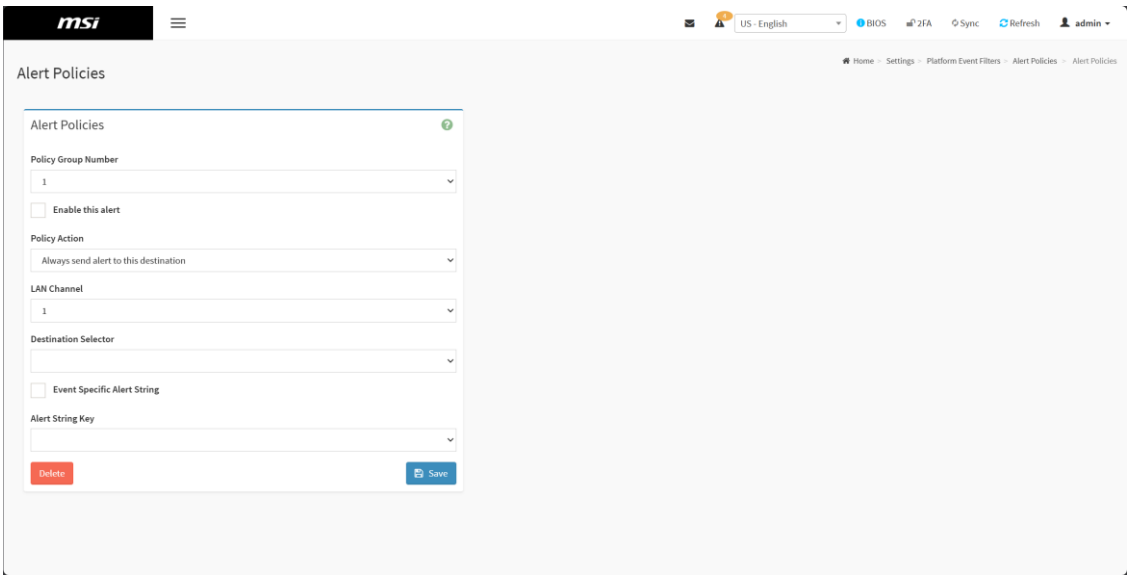
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

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.



Add Alert Policies Page

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 have to be configured using IPMI Command (Set PEF Config Parameter "Alert String").

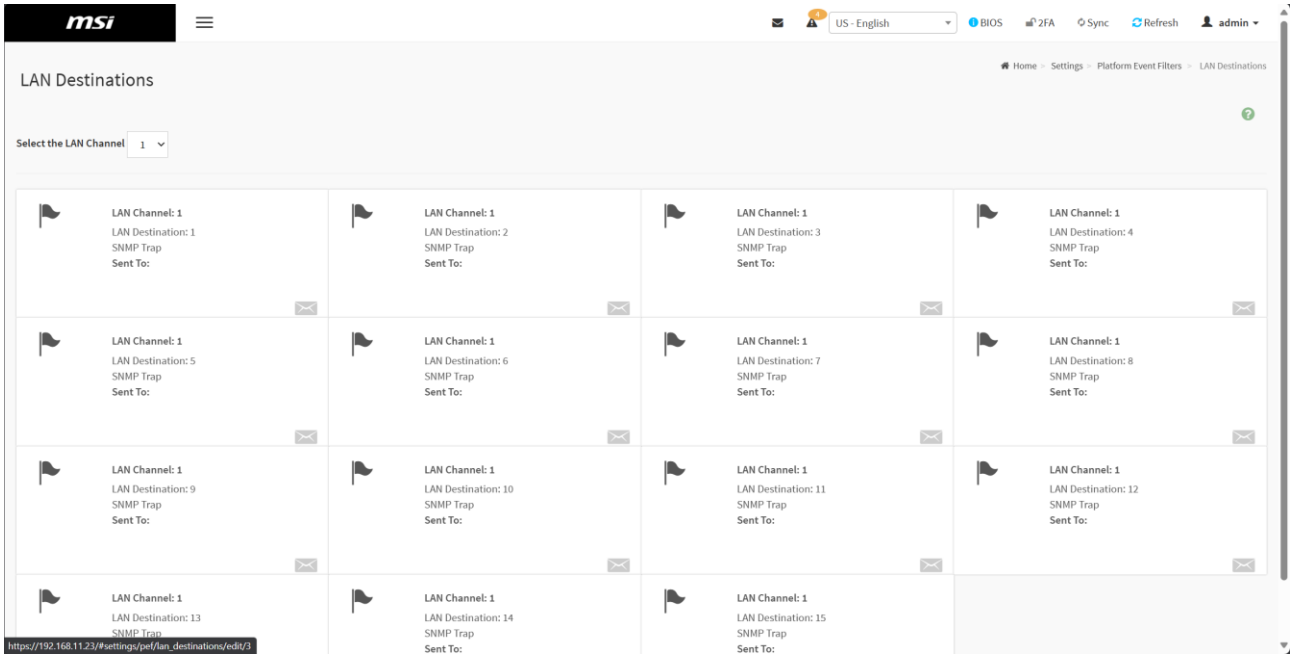
   # and ; symbols are not supported for PEF Alert string.

10. lick **Save** to save the new alert policy and return to Alert Policy list.

11. Click **Delete** to delete a configuration.

LAN Destinations

This page is used to configure the LAN destinations of PEF configuration. A sample screenshot of LAN Destinations 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 (read-only).

Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC 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 Qualified 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.

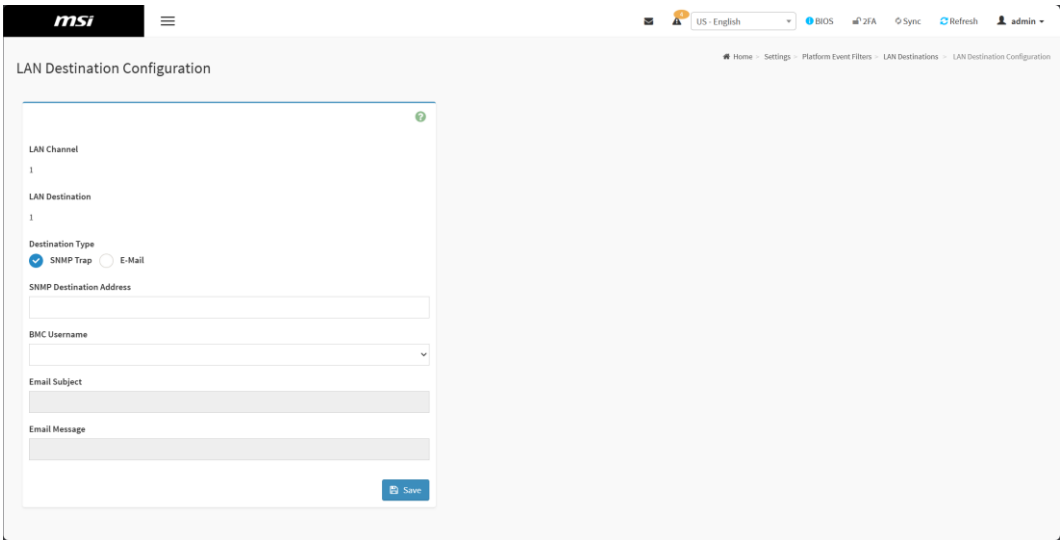
***Note**: User should be configured under Settings-->Users Management*

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 Configuration**.



LAN DestinationConfiguration

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 be 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.*

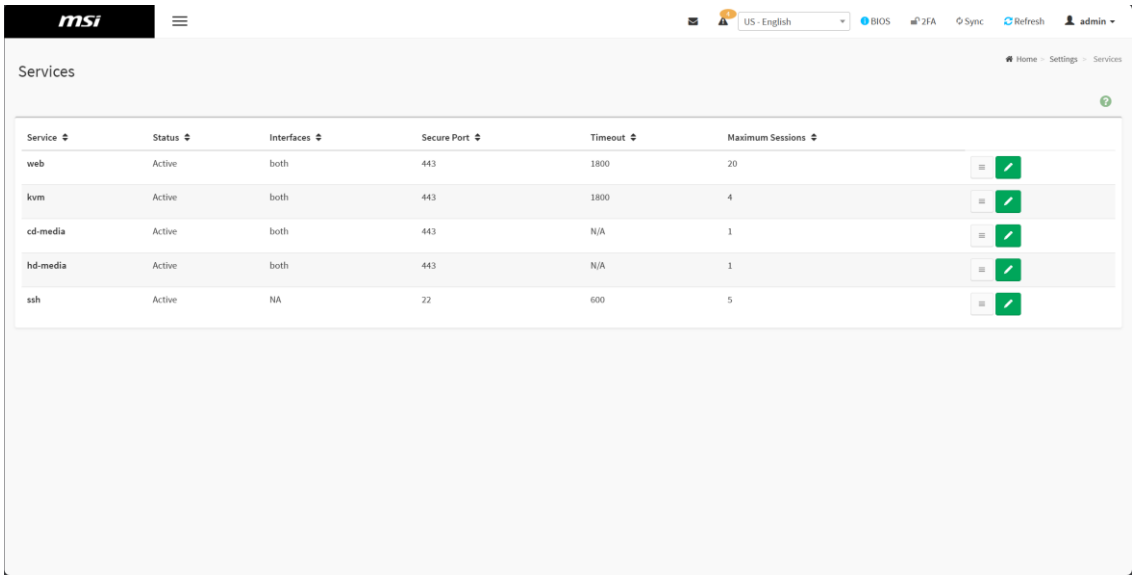
Services

This page displays the basic information about services running in the BMC. Also provided are the current status and other basic information about each. 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.

Click  icon to modify the services configuration.

Click icon to view or terminate the connected session for this service.



Services Page

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 port, and CD Media Port 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 port and Media Port 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, EO – Exposed Outside.*

The adviser will always be listening to loopback as well as KVM configured interface as mentioned in the above table. So that the H5Viewer client can connect to the video server.

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.
- 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.

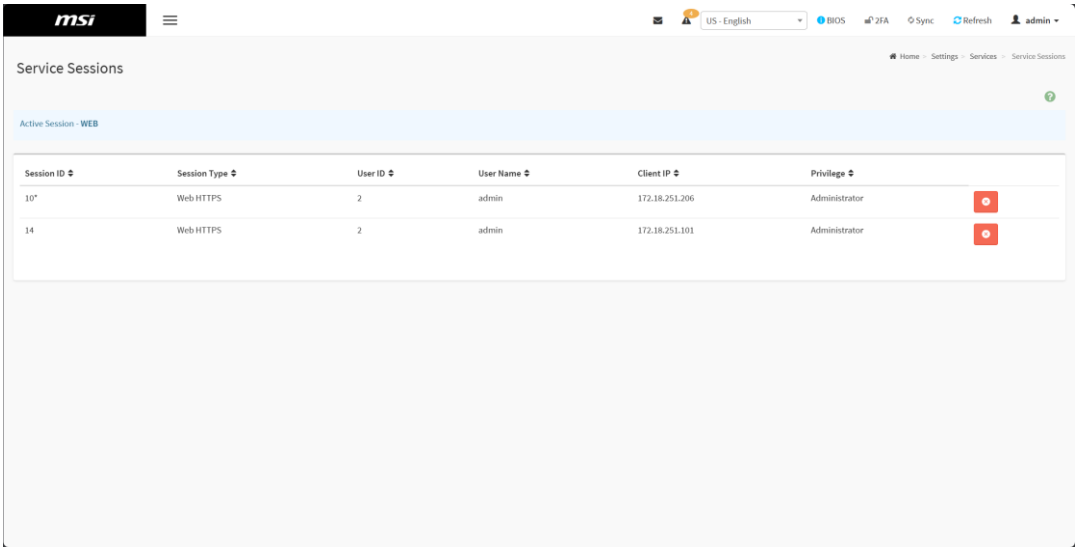
Active Sessions: To view the current active sessions for the service.

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.



Service Sessions

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.

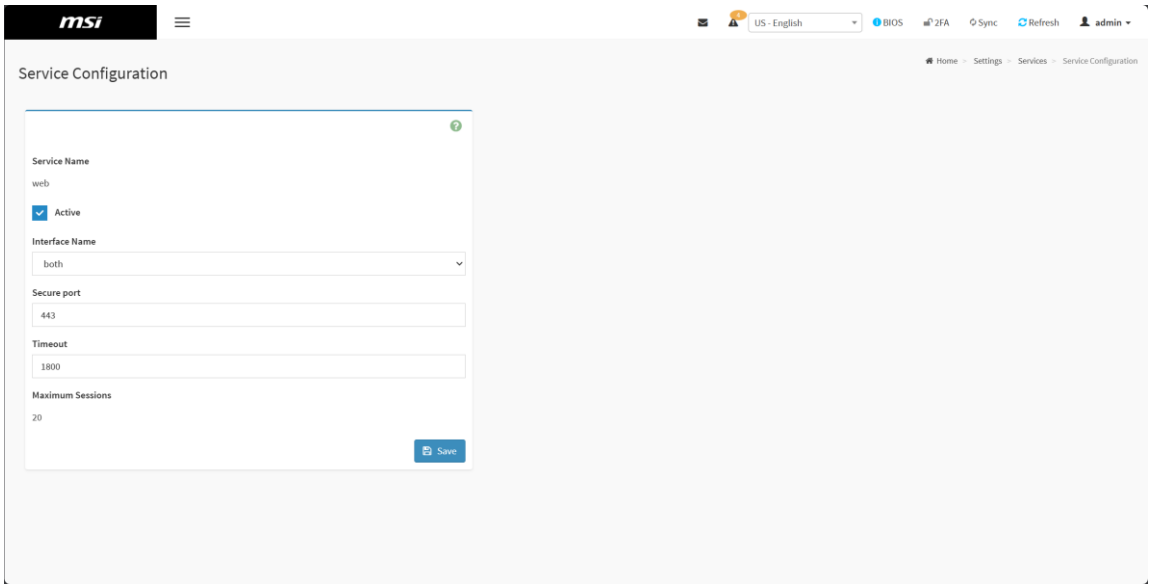
To modify the existing services:

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.



Service Configuration

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.

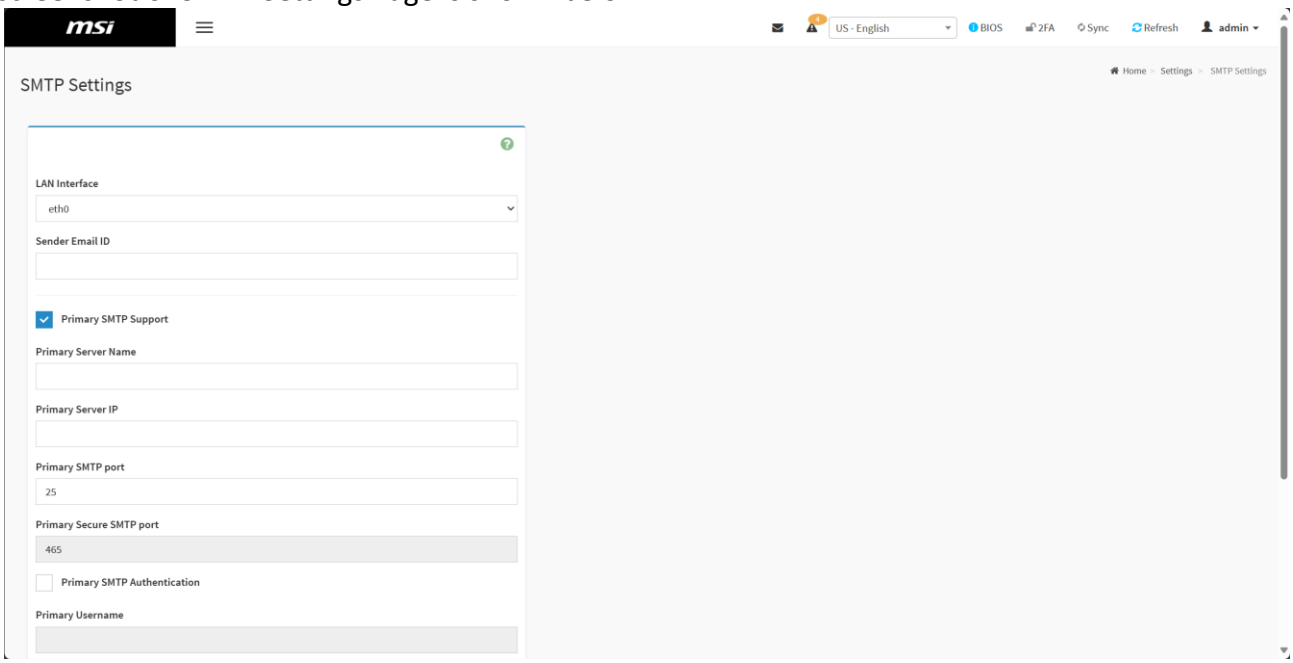
   ***Note**: Make sure that the SOLSSH service idle timeout should not be greater than the SSH idle timeout.*

SMTP Settings

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

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

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 Email ID' to indicate the BMC, whenever e-mail is sent. Maximum allowed size for Email ID is 64 bytes, which includes username and domain name. This field is for information purpose only.

Primary Server Name: The 'Machine Name' of the BMC, from where the e-mail is sent. This field is for information purpose only.

Note:

- *Machine Name is a string of maximum 25 alpha-numeric characters.*
- *Space, special characters are not allowed.*
- *Primary Server Name is mandatory if the primary SMTP SSLTLS or primary SMTP STARTTLS is enabled.*

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, IPv6 Address format and FQDN 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.

SSL Settings

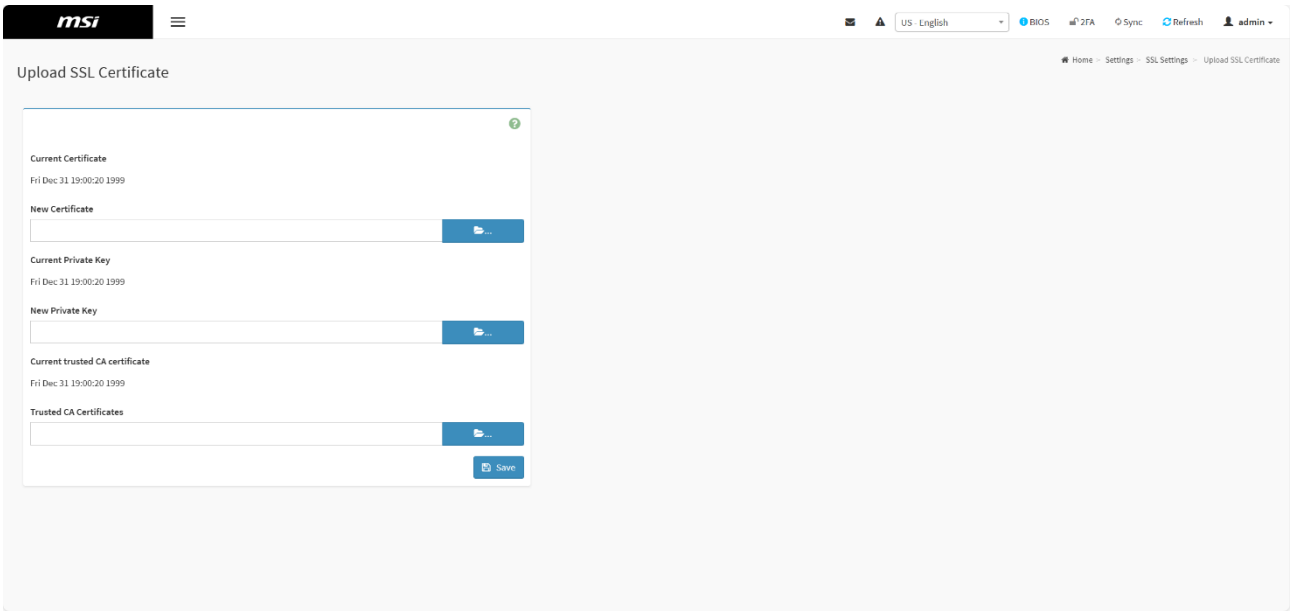
The **Secure Socket Layer** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Using MSI GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secure 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.

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

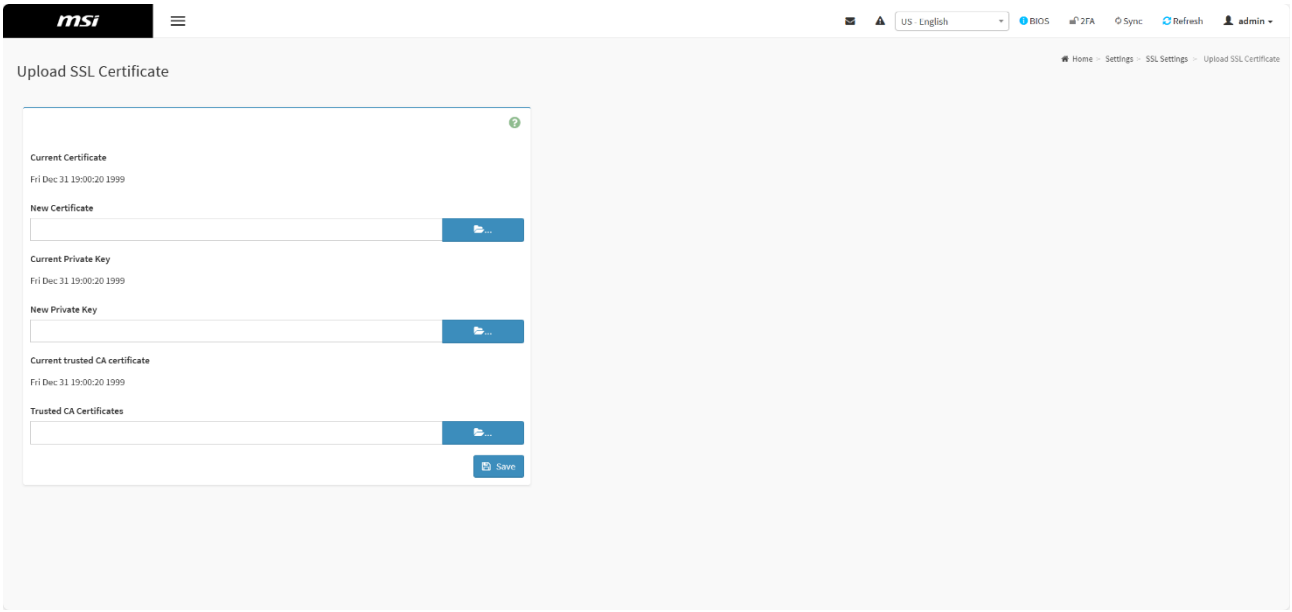
Current Private Key: Current Private key information will be displayed (read-only).

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 in our BMC, the Redfish feature has always been enabled by default.*

A sample screenshot is displayed below.



Trusted CA Certificates

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.

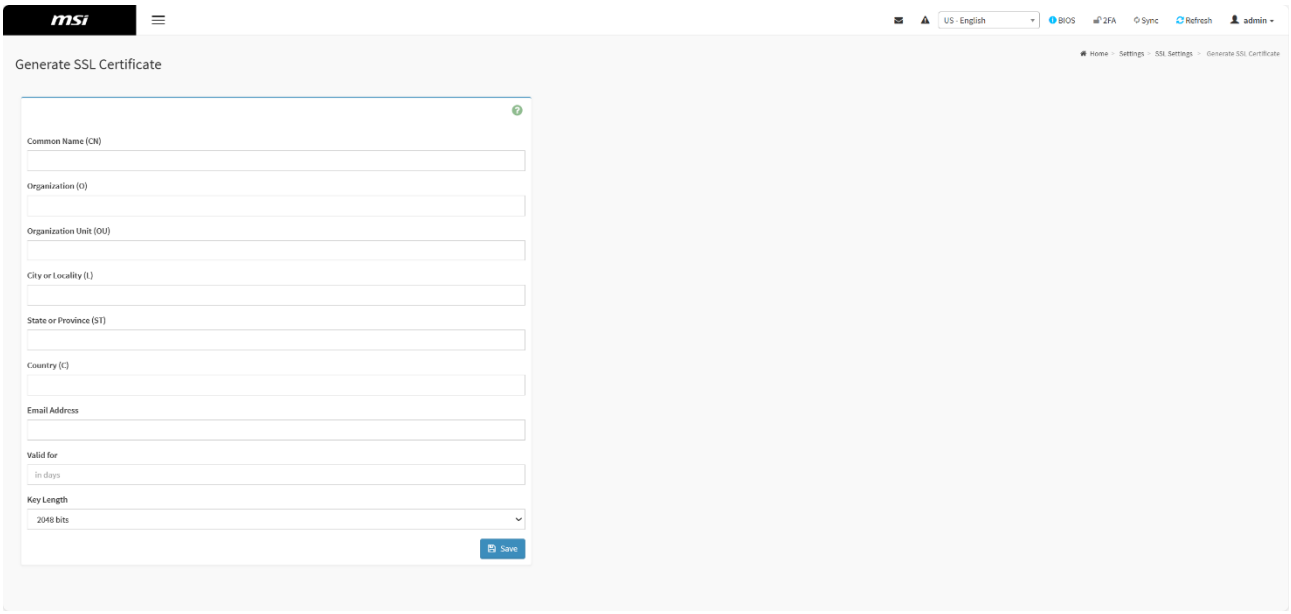
If the user uploaded New Certificate, New Private key & Intermediate key means in BMC concatenate all three files together and serve as server.pem

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 and Expiry date should not be more than 19 January 2038. After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.*
- *If the user gives Factory Restore Defaults, SSL certificate at the run-time will get vanish and it moves to the SSL certificate provided at the built-time.*



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).

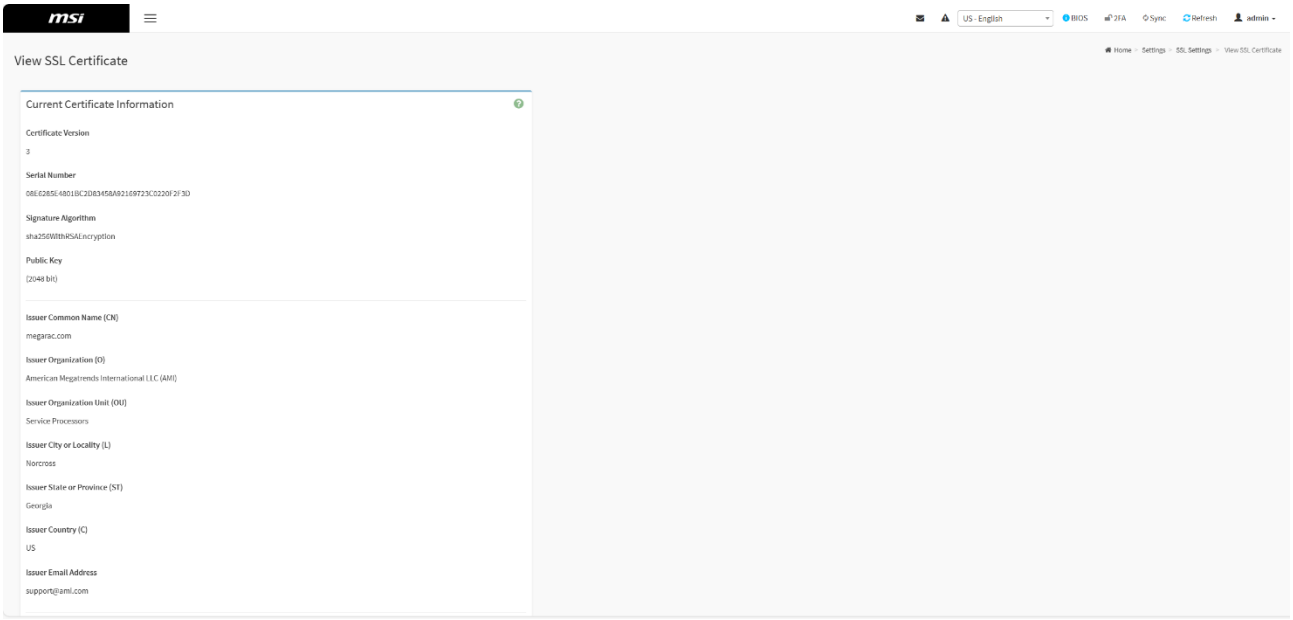
Valid for: Validity of the certificate.

- 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.*



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 Generic BMC securely using the following format in your IP Address field from your Internet browser: https://<you BMC's IP address here>*
– *For example, if your BMC's IP address is 192.168.0.30, enter the following: https://192.168.0.30*
– *Please note the <**s**> after <**http**>. You must accept the certificate before you are able to access your Generic BMC.*

System Firewall

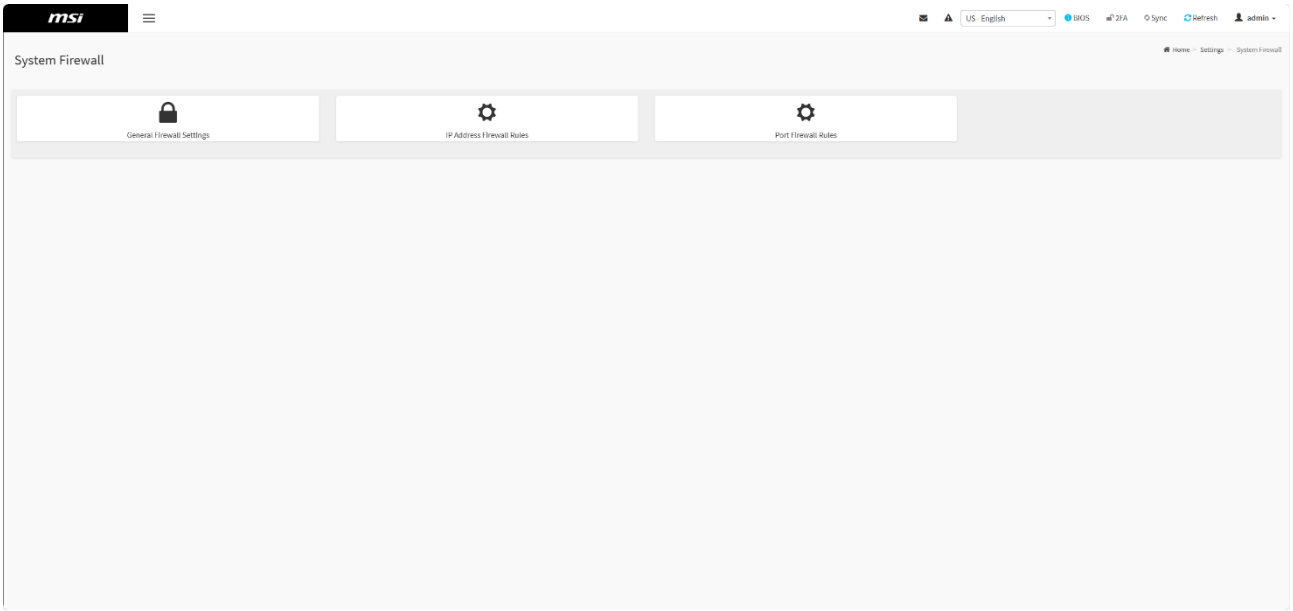
In MSI GUI, the System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

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

General Firewall Settings

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

Firewall Settings



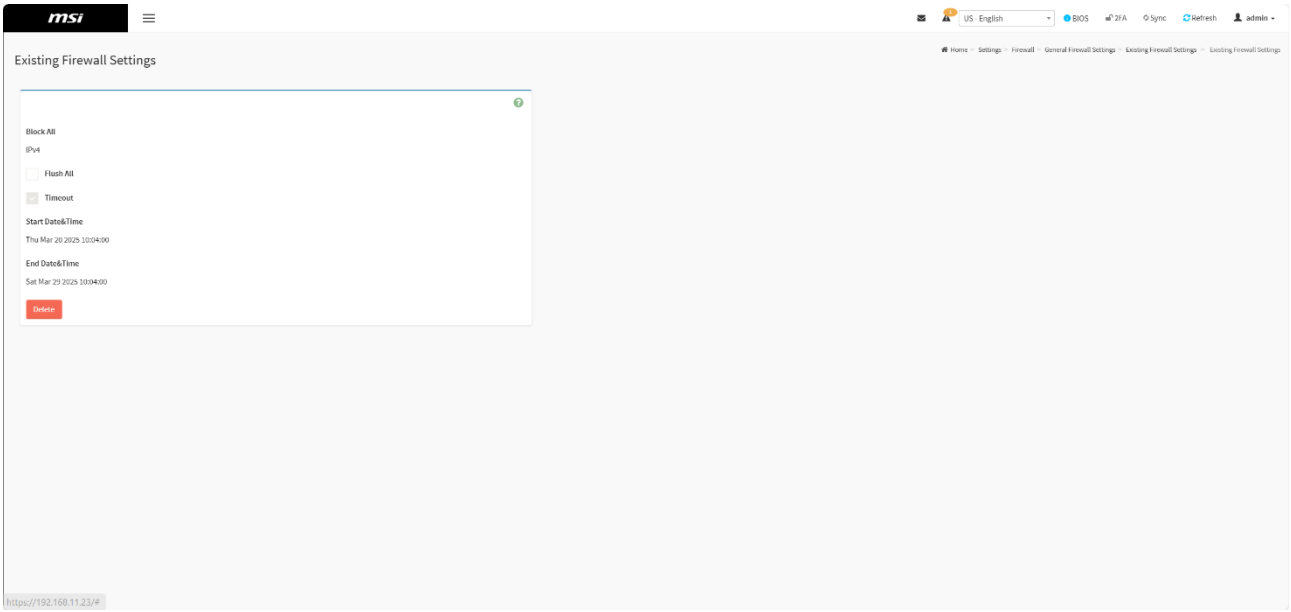
The fields of **Firewall Settings** tab are explained below.

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 setting by clicking link **Add Firewall Settings** page.

Procedure to Add Firewall settings

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

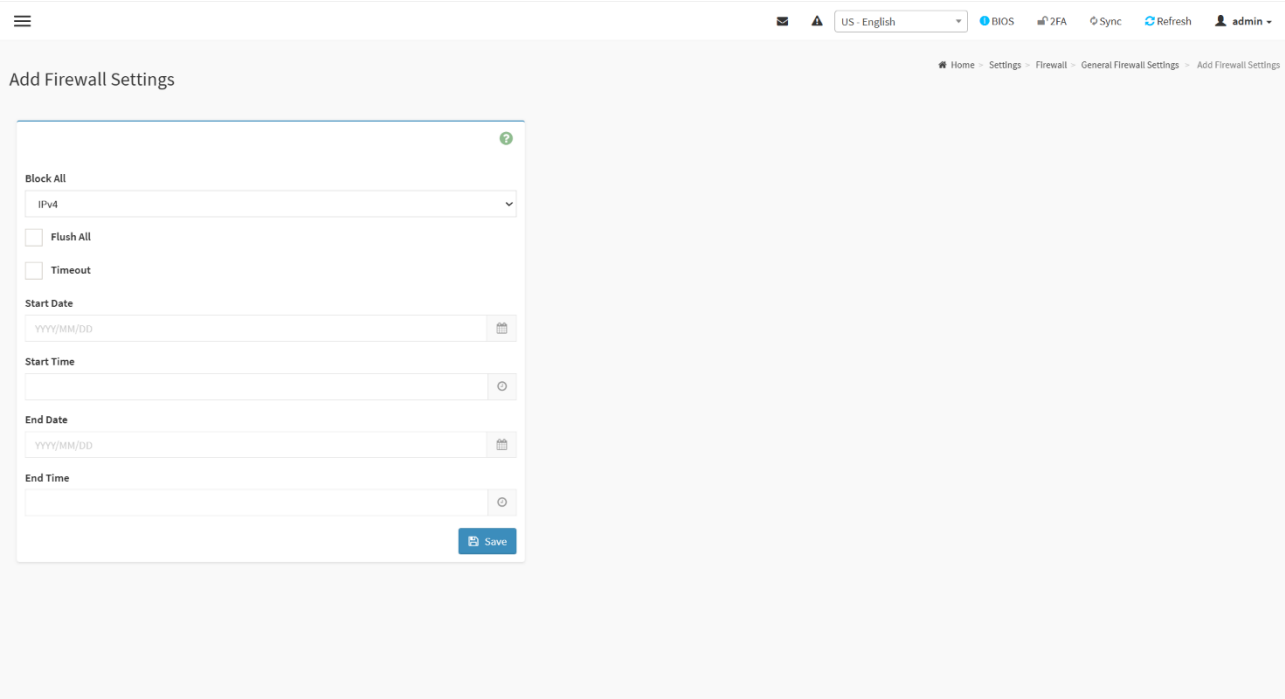


Existing Firewall Settings

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

Add Firewall Settings

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



Add Firewall Settings

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 Date** to start the respective firewall rule effect from this date. The firewall rule become effective from 1970-01-02 to 2038-01-18 only allowed.
6. Enter **Start Time** to start the respective firewall rule effect from this time.
7. Enter **End Date** to start the respective firewall rule effect from this date. The firewall rule become effective from 1970-01-02 to 2038-01-18 only allowed.
8. Enter **End Time** to end the respective firewall rule effect from this time.

   ***Note**:*

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

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

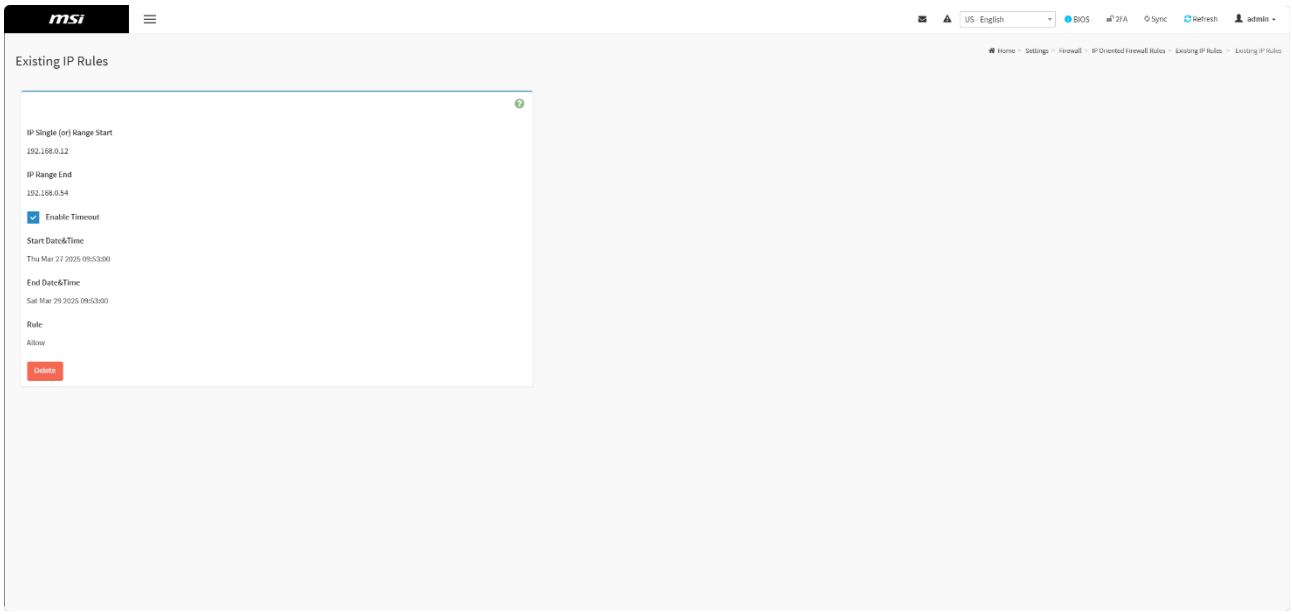
IP Address Firewall Rules

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

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

Procedure to Add IP Rule

1. Click **Settings** > **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.

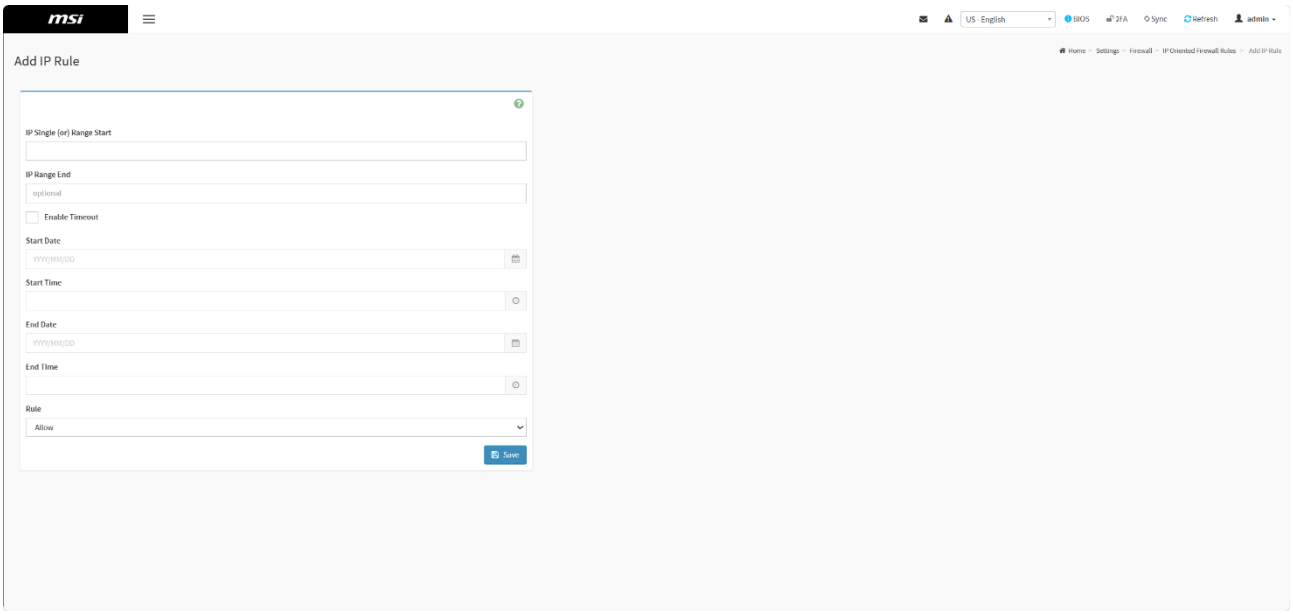
End Time - The respective firewall rule effect will end from this time.

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 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**:*

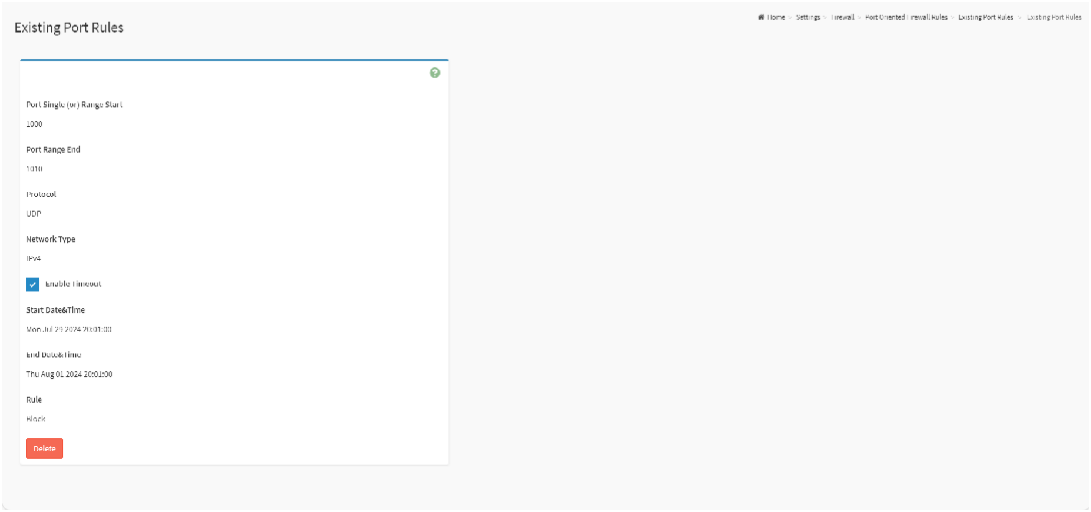
   - *IP Address will support IPv4 Address format only:*
   - *IPv4 Address made of 4 numbers separated by dots as in xxx.xxx.xxx.xxx.*
   - *Each number ranges from 0 to 255.*
   - *First number must not be 0.*
   - *IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in xxx x:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.*
3. Enter IP range end value in the **IP Range End** field.
4. Enable **Timeout** to enable firewall rules with timeout.
5. Enter **Start Date** to start the respective firewall rule effect from this date.
6. Enter **End Date** to end the respective firewall rule effect from this date.
7. Enter **Start Time** to start the respective firewall rule effect from this time.
8. Enter **End Time** to end the respective firewall rule effect from this time.

   ***Note**: The date and time should be in the YYYY/MM/DD and hh-mm format respectively.*
9. Determine the rule to block or accept.
10. Click **Save** to save the changes made.

Port Firewall Rules

To view Existing Port Rules

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 is 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.

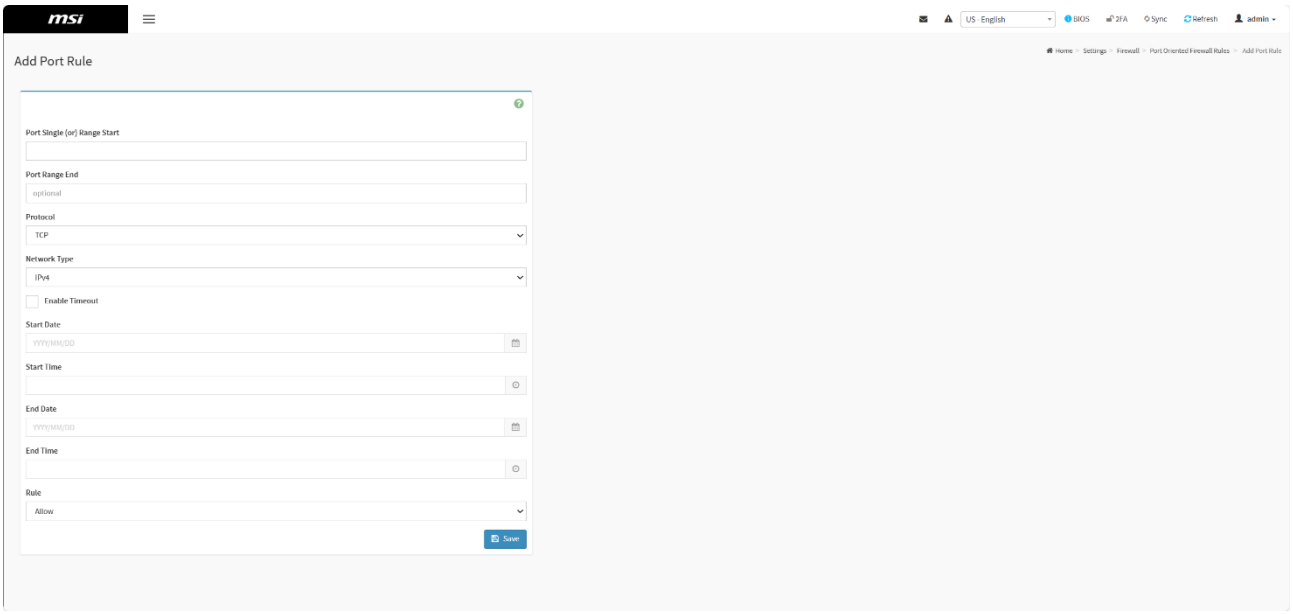
End Time - The respective firewall rule will end at this time.

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. Port 80 is blocked for TCP/UDP protocols.*

3. Enter the end value in the **Port Range End** field. This field is optional.
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 Date** to start the respective firewall rule effect from this date. The firewall rule will become effective from 1970-01-02 to 2038-01-18 only allowed.
8. Enter **Start Time** to start the respective firewall rule effect from this time.
9. Enter **End Date** to end the respective firewall rule effect on this date. The firewall rule will expire on this date from 1970-01-02 to 2038-01-18 only allowed.
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.*

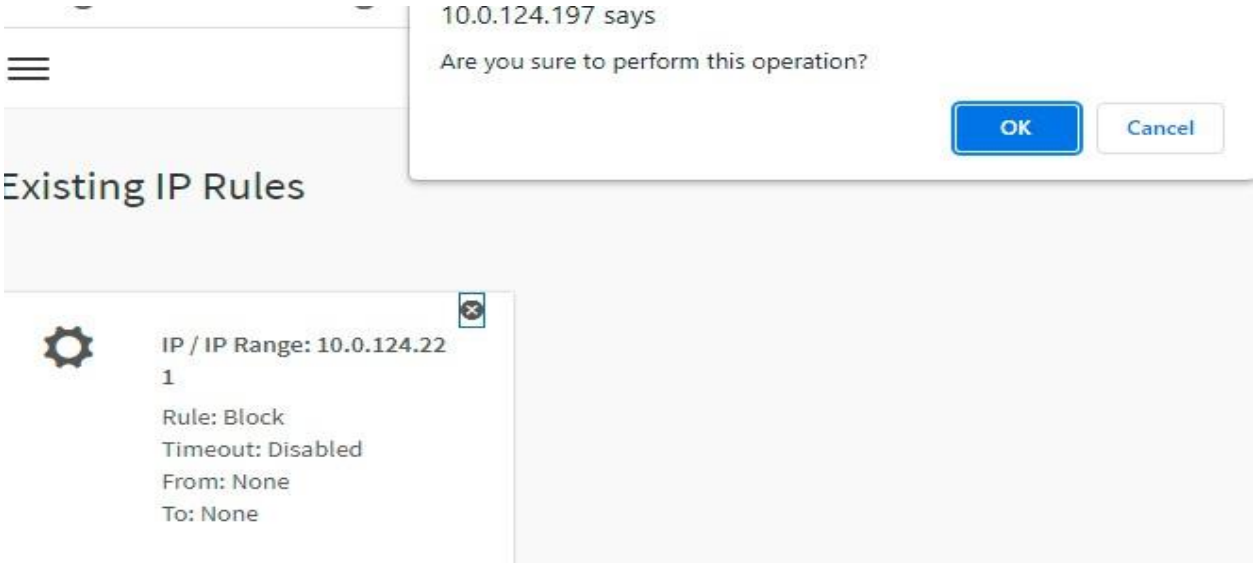
11. Select the **Rule** to determine the rule to **Block** or **Allow**.
12. Click **Save** to save the changes made.

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

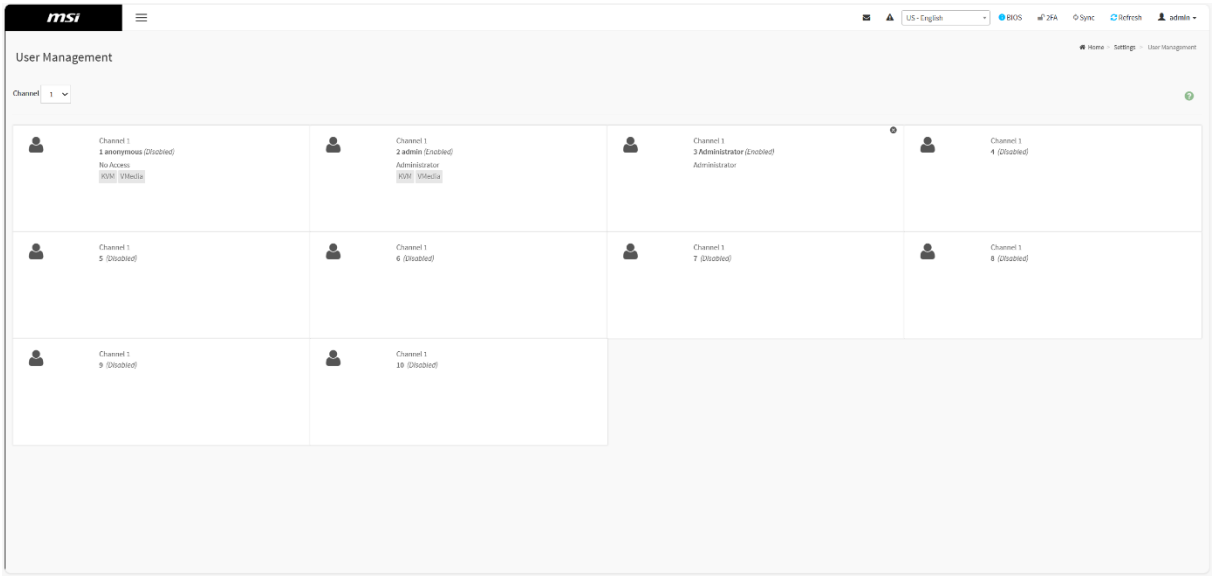


Existing Firewall Settings

User Management

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

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



User Management

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.

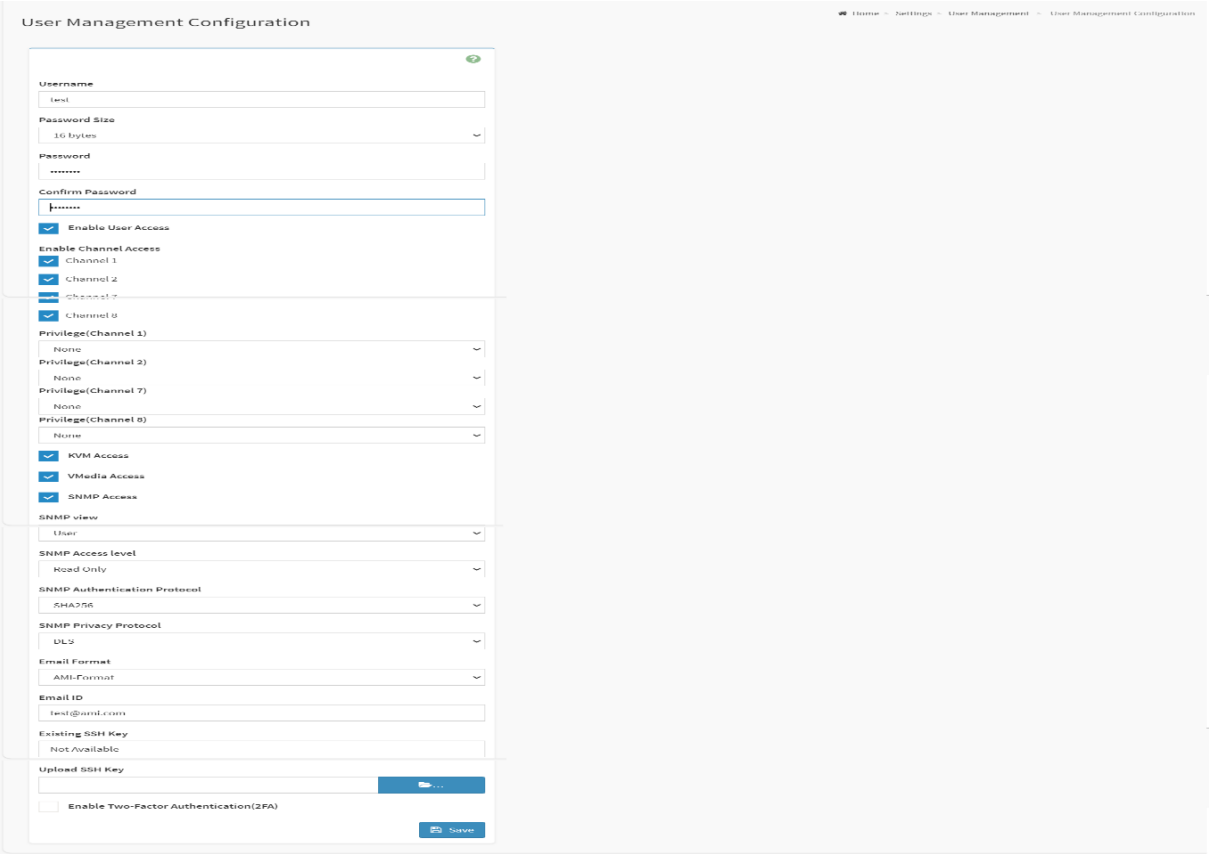
E-mail ID: Displays e-mail address of the user.

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 Page

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 it's 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, JViewer, 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** (SHA or MD5) drop-down list. Either it can be Read Only or Read Write.
13. Choose the **SNMP Authentication Protocol** (SHA or MD5) to use for SNMP settings from the drop-down list.

    ***Note**: Password field is mandatory, if Authentication protocol is changed.*

14. Choose the Encryption algorithm to use for SNMP settings from the **SNMP Privacy protocol** (AES or DES) 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.

    ***Note**: SMTP Server must be configured to send emails.*

    ***Email Format**: Two types of formats are available:*

    ***AMI-Format**: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.*

    ***Fixed-Subject Format**: This format displays the message according to user's setting. You must set the subject and message for email alert.*

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

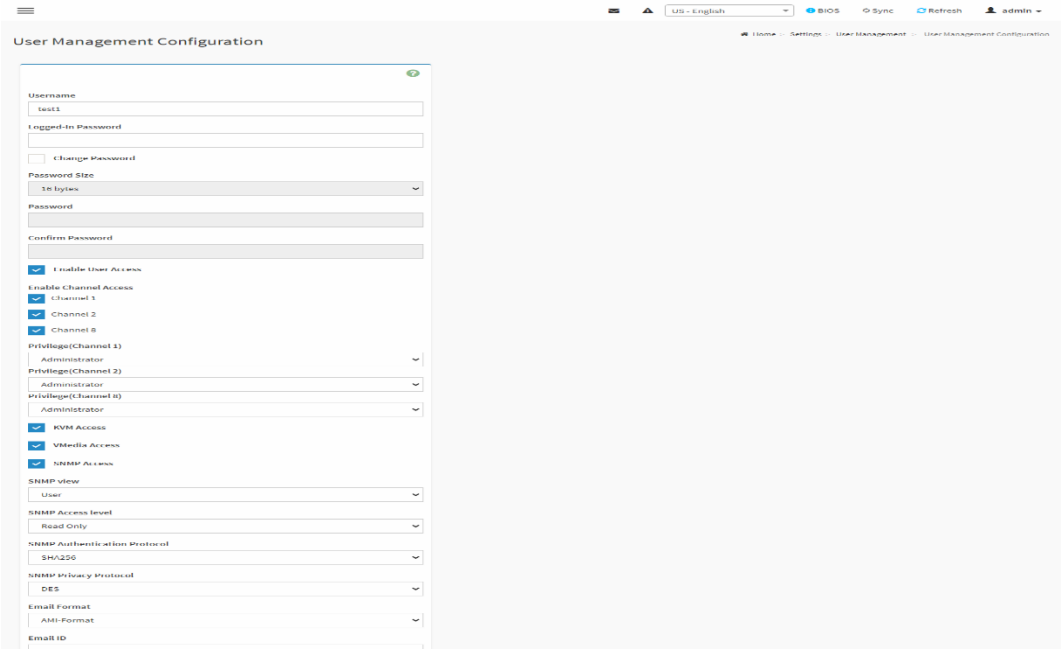
    ***Note**: SSH key file should be of pub type.*

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

Procedure: 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.



User Management Configuration Page

2. Enter the **Username** in the given field.
3. Mention the same password which is initially given to the login page in **Logged-In Password** field.

   ***Note**: User must enter the logged-in password again for confirmation. If it is successful only, user modifying operation can be done otherwise error message will pop-up.*

4. Check **Change Password**, if you wish to change the existing Password.

   ***Note**:- If user login with admin and testuser in two different Web-Browsers and change the pass- word for testuser account from admin account then the testuser account will automatically get logged-out from Web-Browser where the testuser is logged in.*

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

   ***Note**: There is a list of reserved users which cannot be added / modified as BMC users. Please Refer **BMC Platform Porting Guide** section **Changing the Configurations in PMC File-> User Configurations in PMC File** for the list of reserved users.*

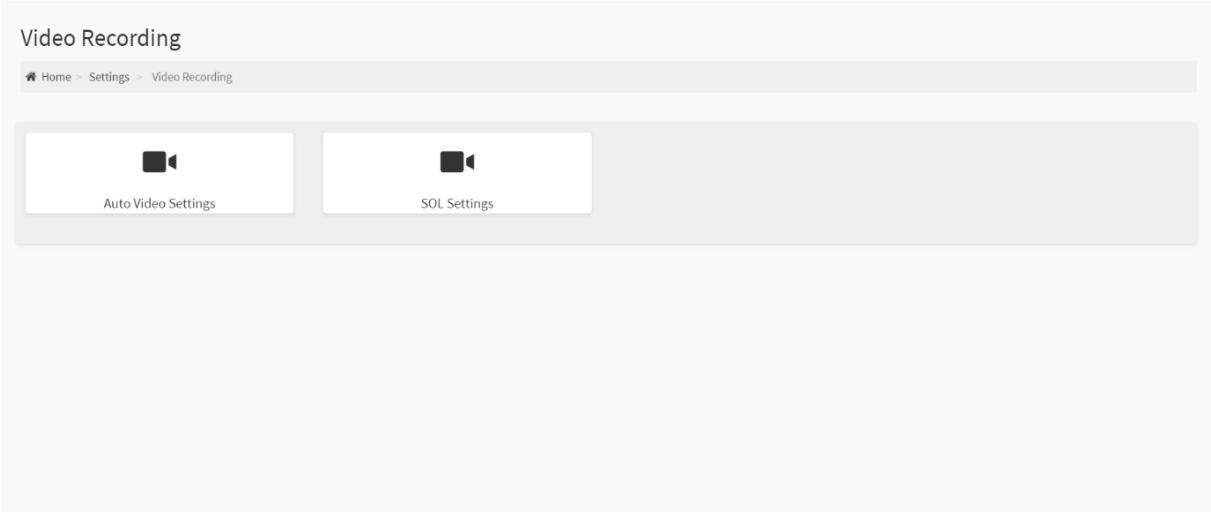
   ***Important**:*

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

- *sysadmin*
- *daemon*
- *sshd*
- *ntp*
- *root*

Video Recording

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



Video Recording

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

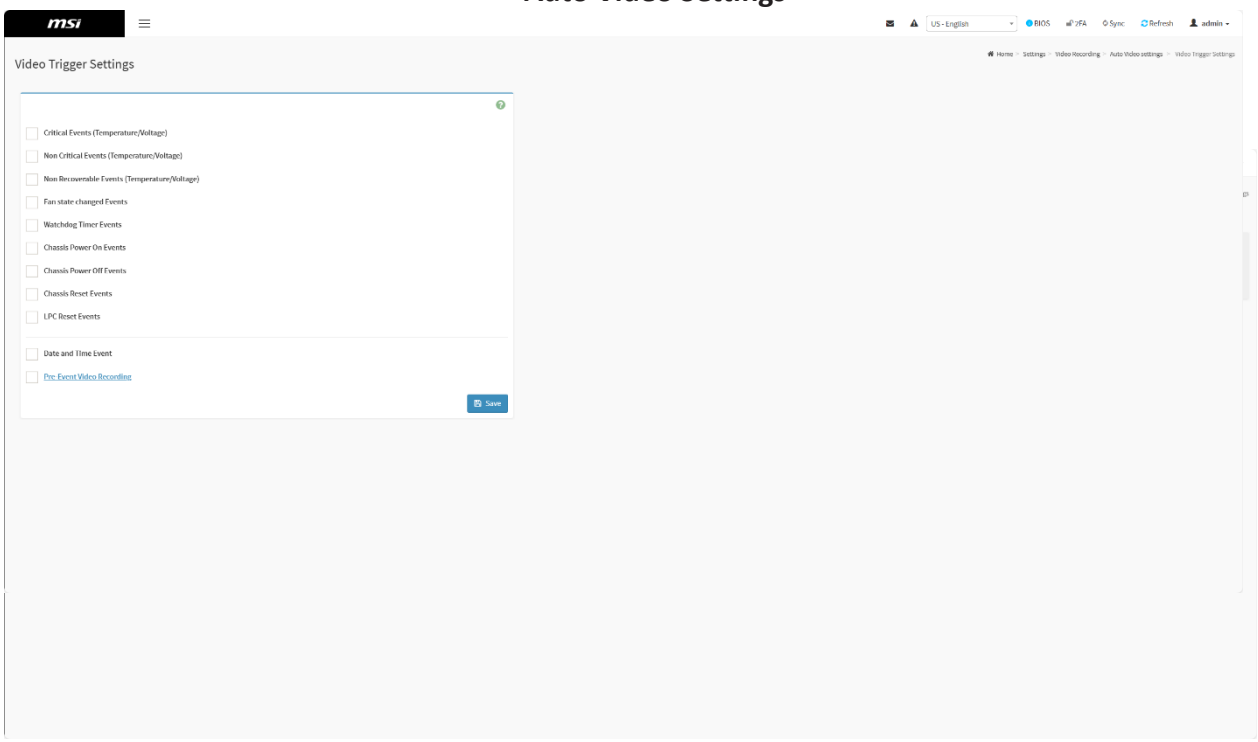
A detailed description of the menu items is given below.

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



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

Video Trigger Settings

Video Trigger Settings

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

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

Save: To save any changes made.

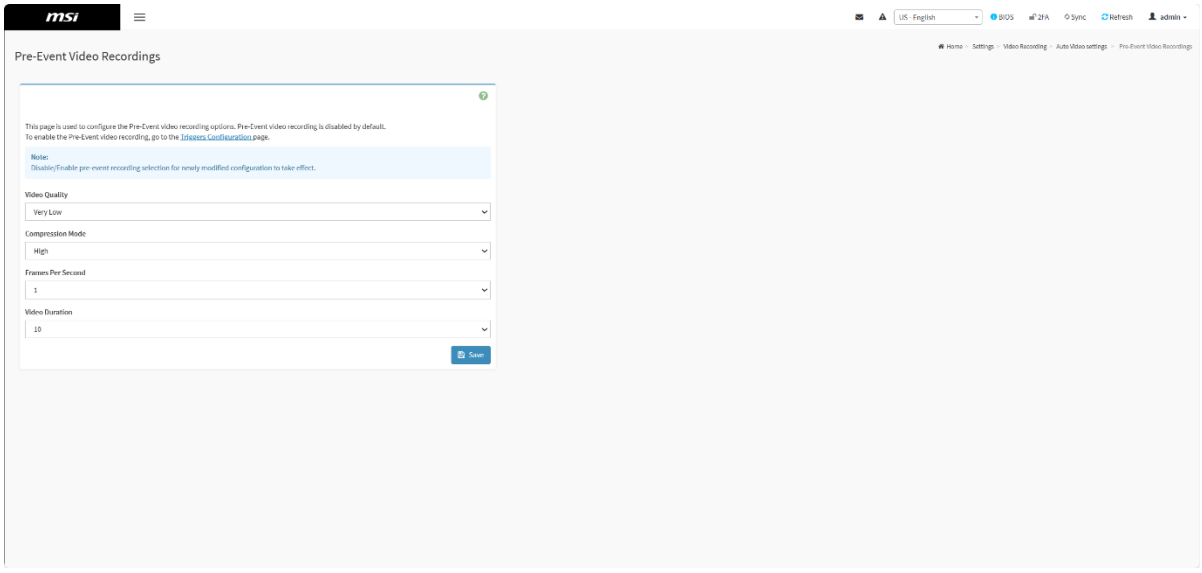
Procedure:

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.*



Pre-Event Video Recordings

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** drop- down 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.

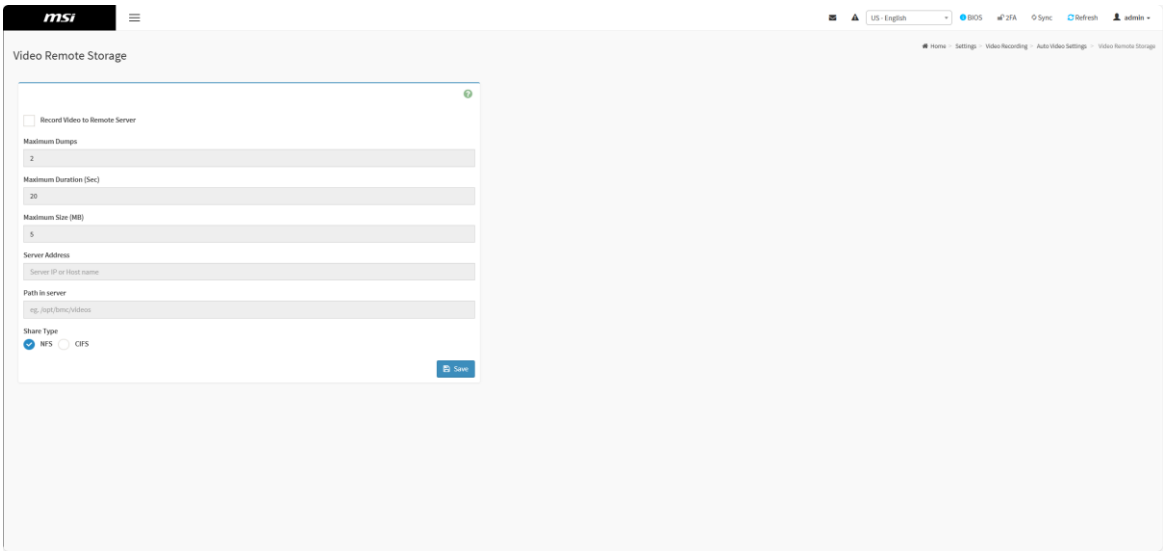
***Note**: -*

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.

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:

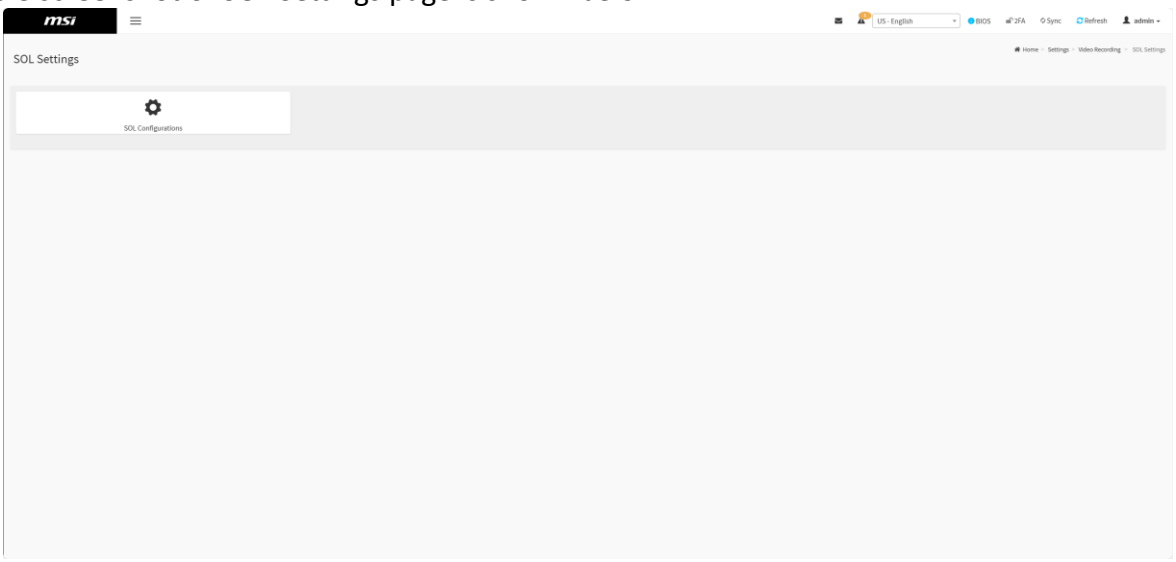
	Auto Video Recording (Post Event)	**Pre-Event Video Recording (only for Crash/reset event)**
Time Limits	20 seconds or 5.5MB video allowed if Local Storage.	Default-10sec, but can be configurable up to 60sec.
	3600 seconds or 500MB video recording allowed if Remote Storage (Remote Path).	
Video File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

***Note**:*

- *If video resolution change during auto-video recording then multiple video files will be down-loaded. 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 occur. This behavior difference between HTML video download option and Java video down- load 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 down-loaded /played.*

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.



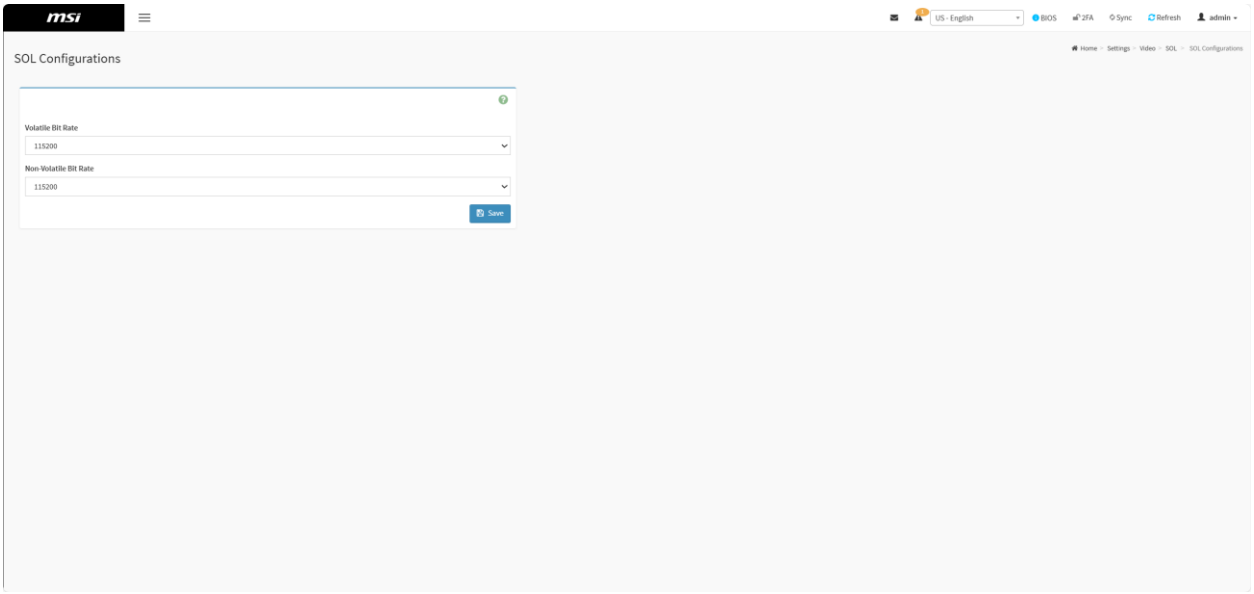
SOL Settings

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 as below.



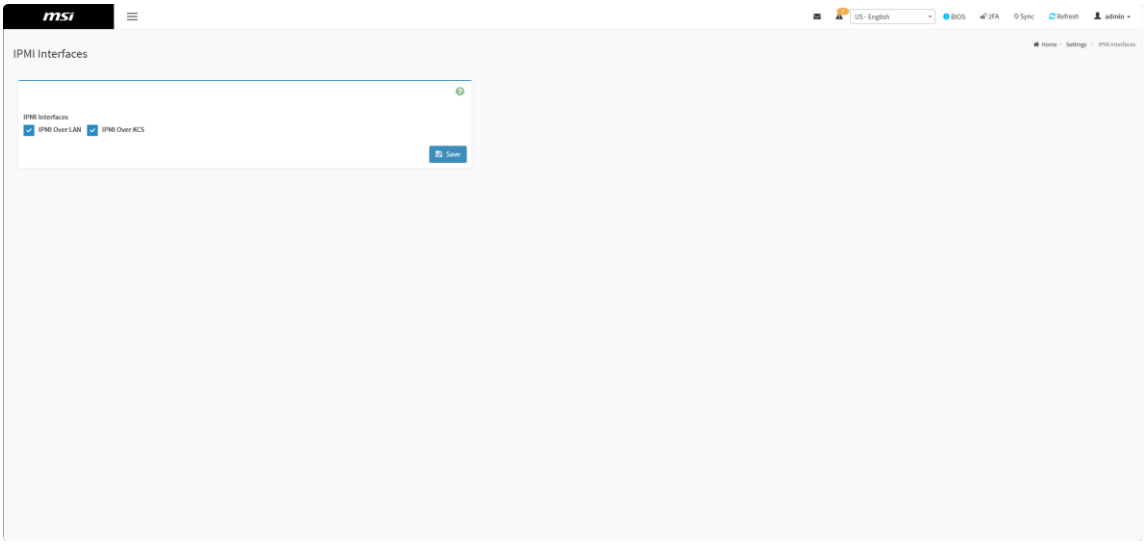
SOL Configurations

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.

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

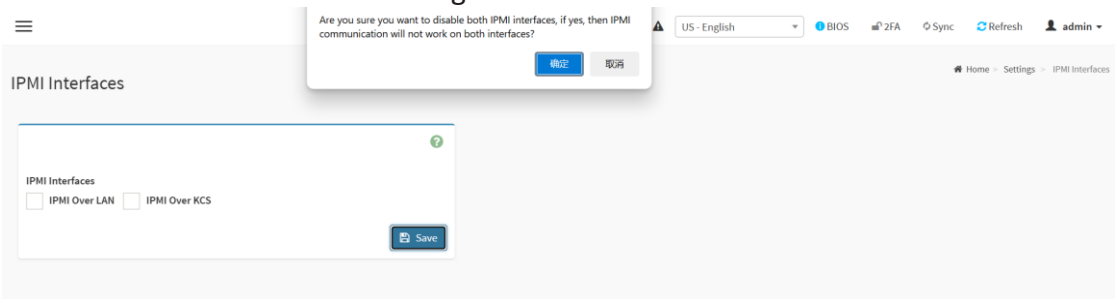
This page displays the following interfaces like **IPMI Over LAN** and **IPMI Over KCS**.

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.*

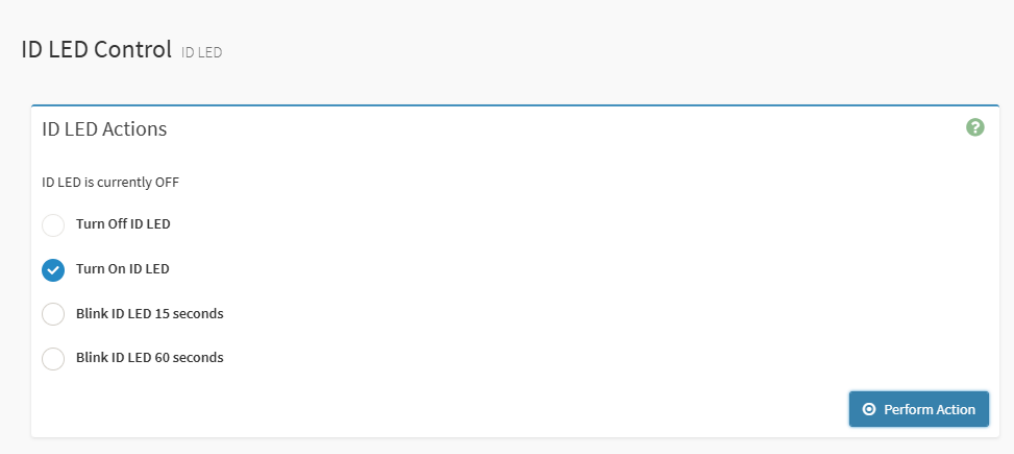
- **Save**: Click Save to save the configured interfaces.



IPMI Interfaces

ID LED Control

The ID LED Control page can show the status of the ID LED, and also allows you to control the ID LED for the server.



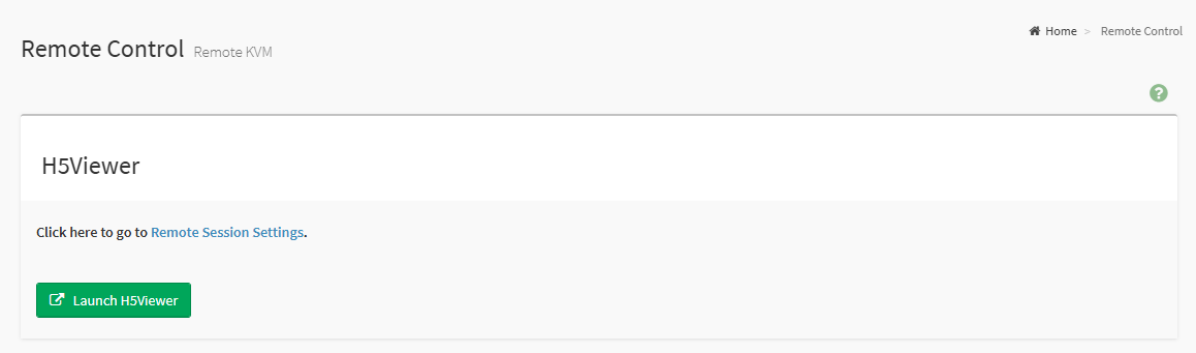
ID LED Control

Select the action and click **Perform Action** to take effect.

12 Remote Control

The Remote Control page consists of the following options. Click **Remote Session Settings** for navigating to that page. A sample screenshot is displayed below.

- Launch H5Viewer



Remote Control page

Launch H5Viewer

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

System Requirements

- Client machine with 8GB RAM
- If the client machine has 4GB RAM 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 MSI 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.

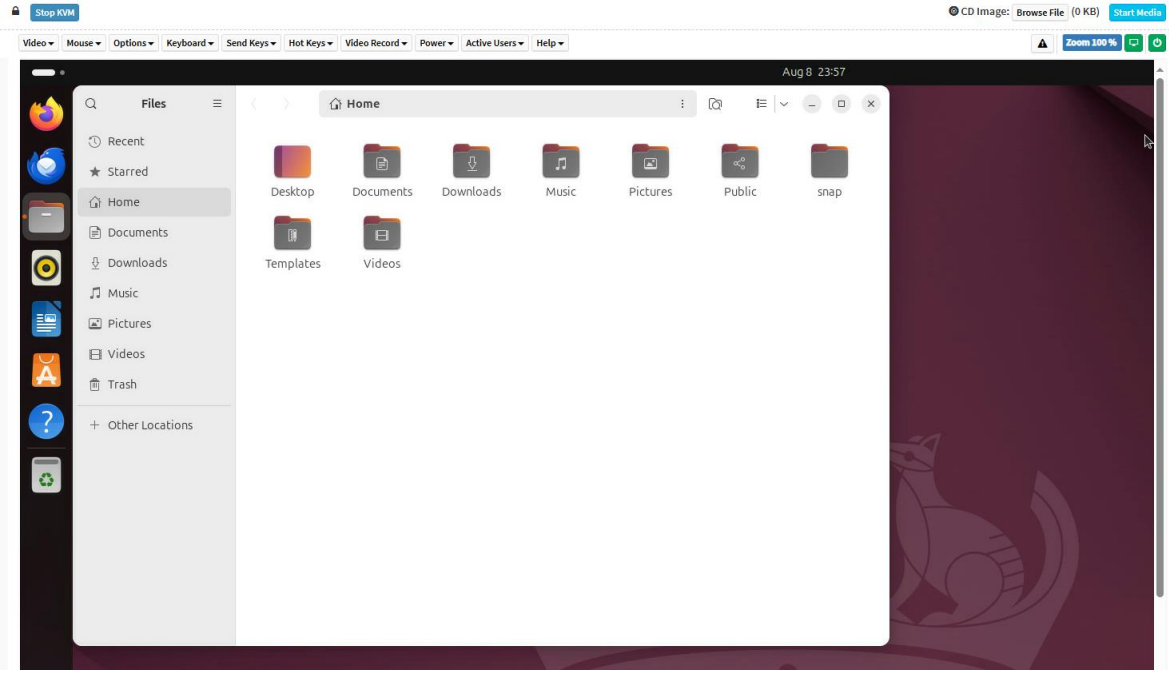
To open Remote Control page, click **Remote Control** from the menu bar.

A detailed description of the menu items is given below.

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

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.



Start KVM

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

Media Redirection

H5Viewer supports media redirection for 1 CD or up to 4 HDs simultaneously. The first instance can be a CD or HD, while the remaining three are HDs only, allowing for a combination of 1 CD/ HD and 3 HDs.

Procedure To Start / Stop Media

1. Click **Browse File** to select a CD/HD Image. After selecting the image, you can enable/disable the Media Boost option for CD/DVD.
2. Click **Start Media** to redirect the selected CD/HD image file to the Host.

***Note**:*

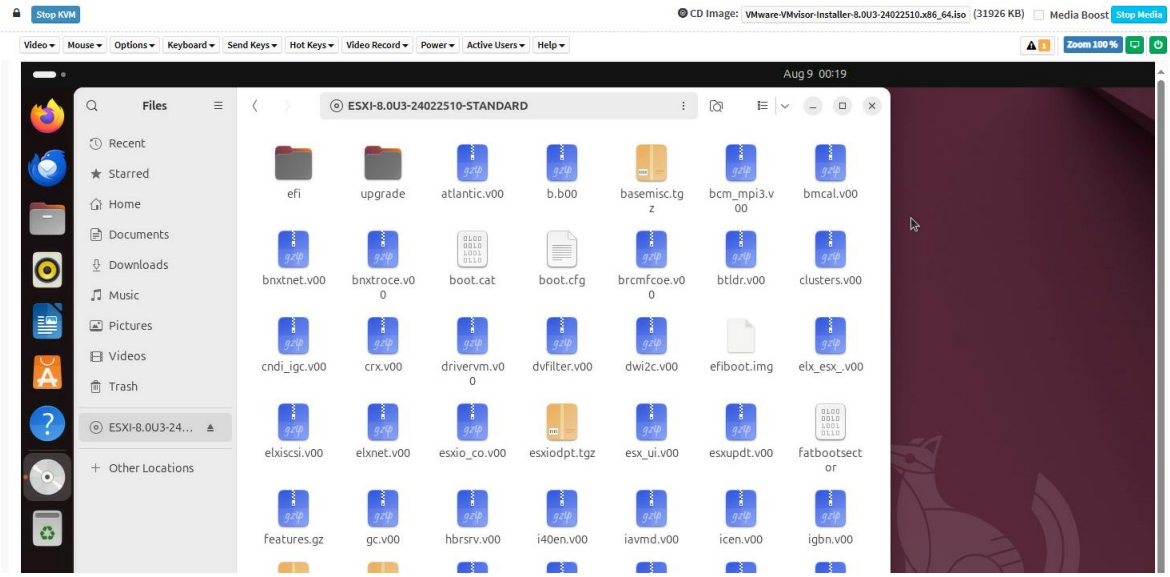
Users can redirect ISO/NRG file formats through the CD slot and IMG/IMA file formats through the HD slot.

Enabling Media Boost gives media redirection processes higher priority, enhancing performance but reducing CPU availability for other tasks.

Media Boost only applies to CD/DVD.

If you start a CD/DVD instance with Media Boost enabled, subsequent CD/DVD instances will start automatically without showing a pop-up.

HD image will be redirected only as READ-ONLY.



Start Media

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

A detailed description of menu items is 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.

- 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**: MSI SP-X 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.

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 has 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 SPX 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 behavior is caused due to H5Viewer HID event listener.*

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

- English US
- English UK
- Spanish
- French
- German
- Italian
- Korean
- Chinese Simplified
- 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.*
- *User 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 contain 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

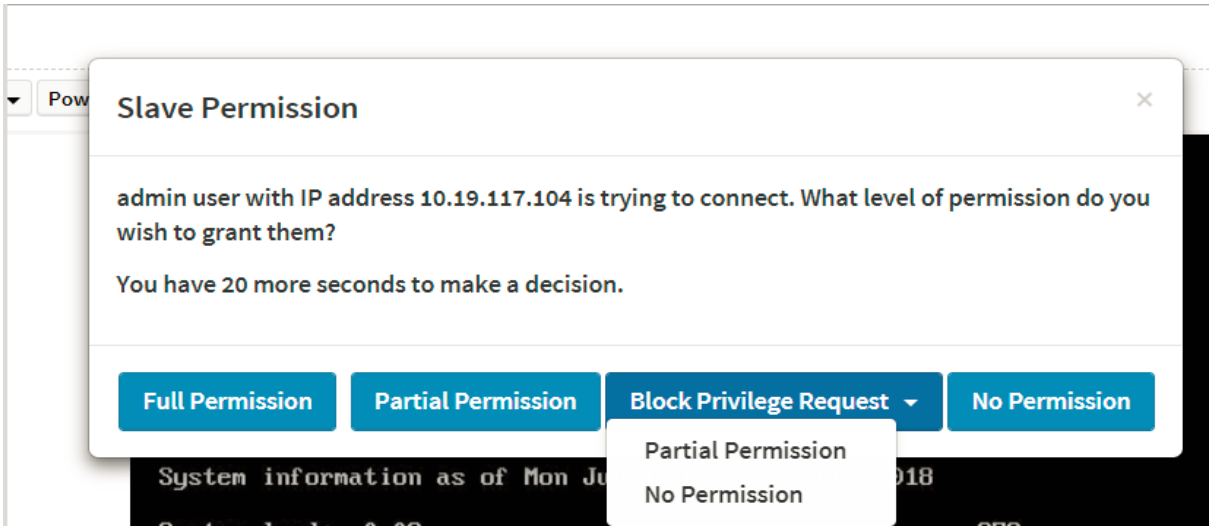
This option provides the same functionality of **Send Keys > Hold Down** menu item. Select any of the menu item, it will highlight the corresponding status bar button in green color. Similarly, by clicking the buttons will toggle the selection status of the corresponding menu item.

KVM Sharing

MSI SP-X stack supports "N" number of KVM Redirection sessions. Only one full permission JViewer/H5Viewer session at a time. With Full permission in JViewer/H5Viewer, the user can control the KVM redirection, and the other JViewer/H5Viewer users can only view the video redirected from the server without intervention.

When the First user launches JViewer/H5Viewer, the user will get full permission to control the host during KVM redirection. When another JViewer/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:



KVM Sharing

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.

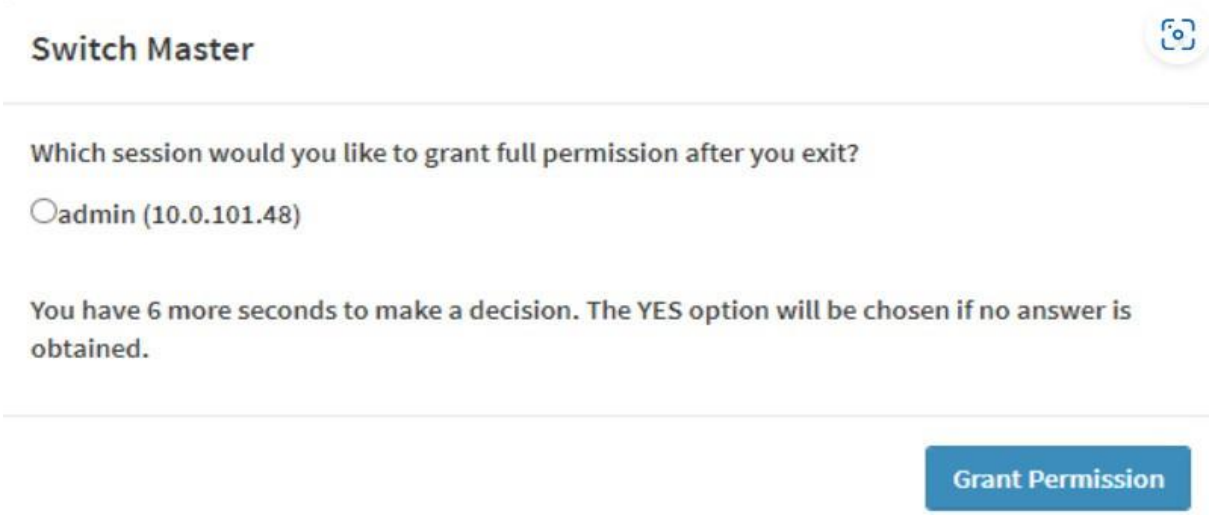
Partial Permission: When this button is clicked, the requesting session will receive partial permission and can only view server display (Video only).

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.



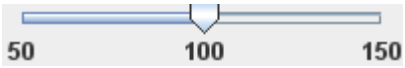
Switch Master

***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 help 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 quick buttons will pop up a virtual media where you can configure the media.

Keyboard LED Sync

When the JViewer is launched from a client machine, the keyboard locks status and LEDs denoting the lock status, in the host machine should be in sync with that in the client machine. That is if the Num/Caps/Scroll lock is enabled in the host, the same should be enabled in the client machine as well.

The host keyboard LED status will be synced with the client keyboard, the lock indicators in the JViewer status bar, and the JViewer Softkeyboard.

The client keyboard's LED status before launching JViewer, or before the JViewer gains focus, will be set back to the client when the focus is lost from the JViewer, or when the JViewer is closed.

***Note**:*

For Macintosh OS X clients, the client keyboard LED sync will not work as the OS does not allow user applications to alter the keyboard LED status. However, the keyboard lock indicators on the JViewer status bar, and the JViewer Softkeyboard lock status will sync with the host keyboard LED status.

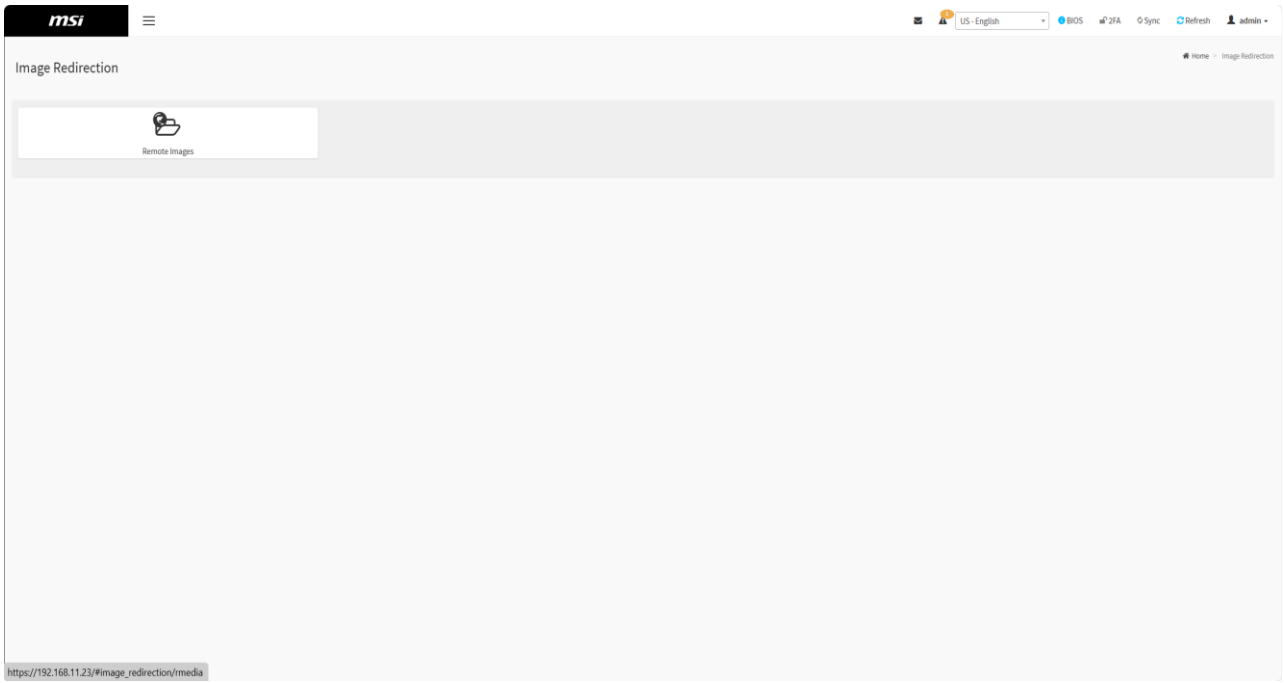
In the case of latest Linux distributions used as host, the keyboard LED sync will not work if the lock status is changed using the host physical keyboard directly. However, the synch will work if the LED status is changed using the onscreen keyboard available in the host OS.

Open a child dialog in JViewer will cause the focus shift out of JViewer. The client keyboard's LED status before launching JViewer, or the JViewer gains focus, will be set back to the client in this case.

13 Image 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.



Images Redirection

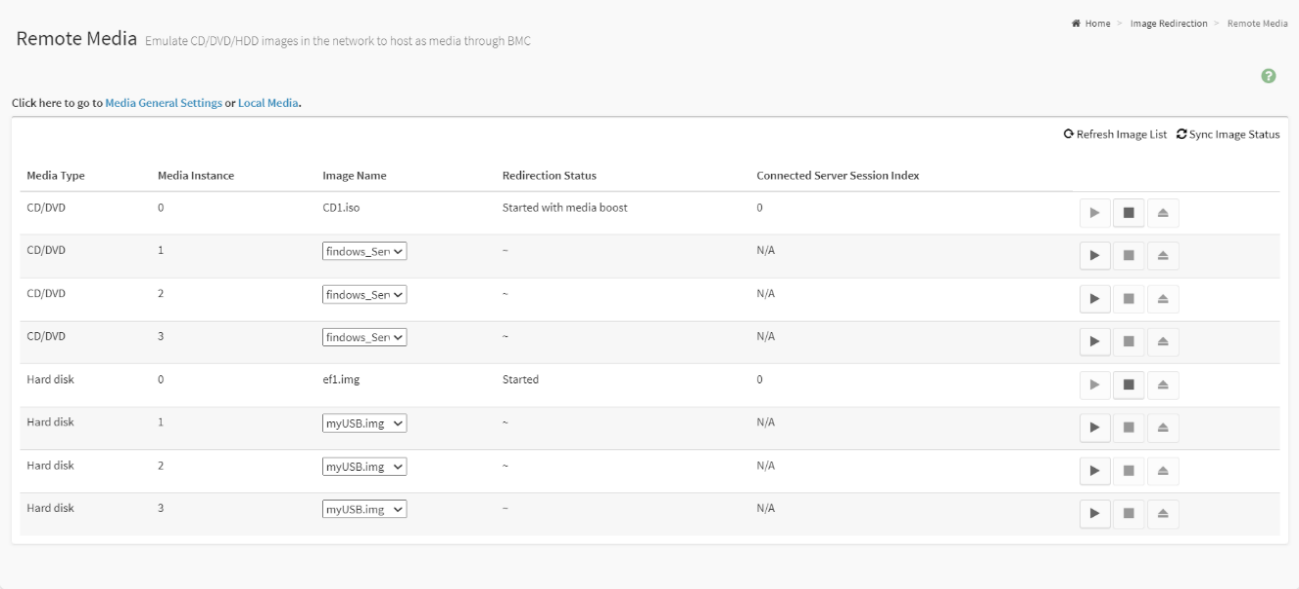
The fields of Images Redirection page is consist of Remote Images.

> ***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.*

Remote Media

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.



Remote Media - Multiple Images

***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

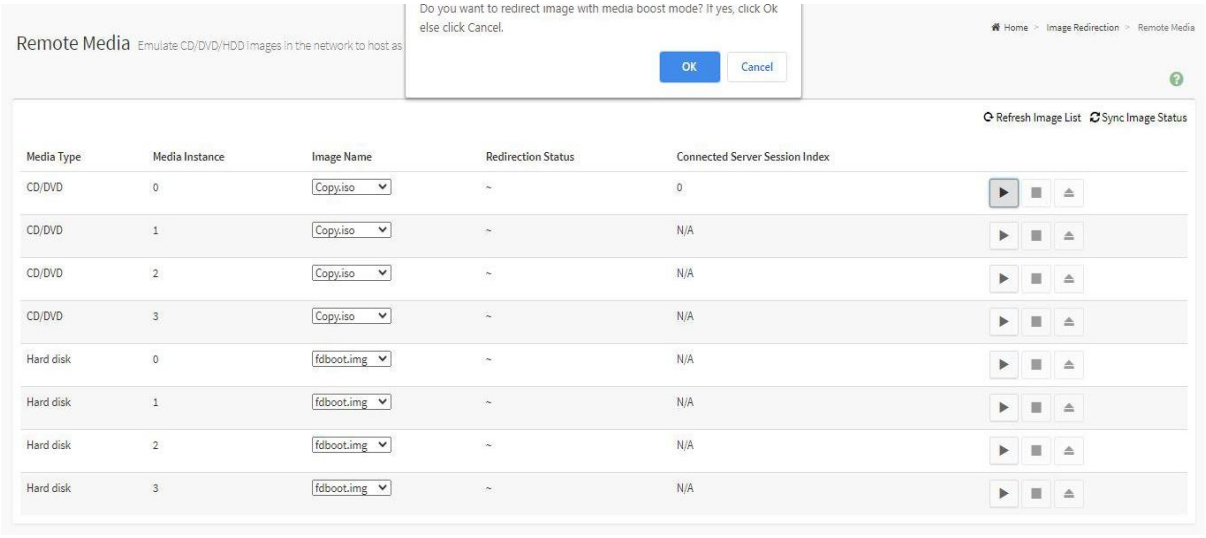
   {}()<>&`|=?;[]$-#~!\ ”%/\ \ :+,’*

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 Re-direction -> 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

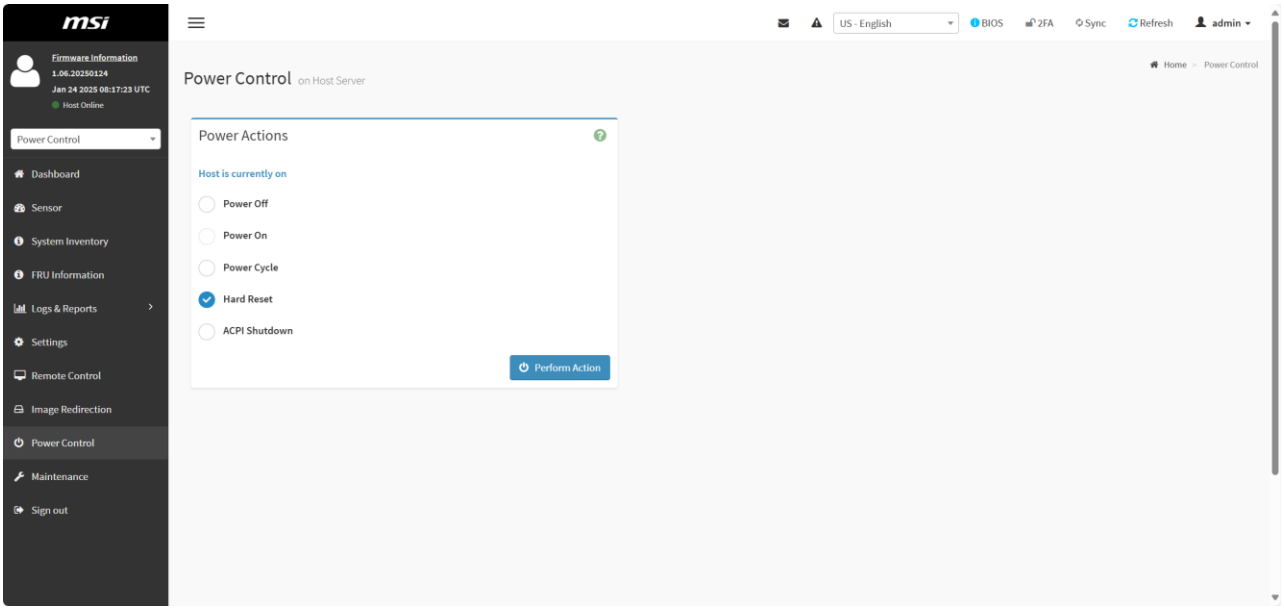
   {}()<>&`|=?;[]$-#~!\"%/\\:+,'*

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

14 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.



Power Control

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.

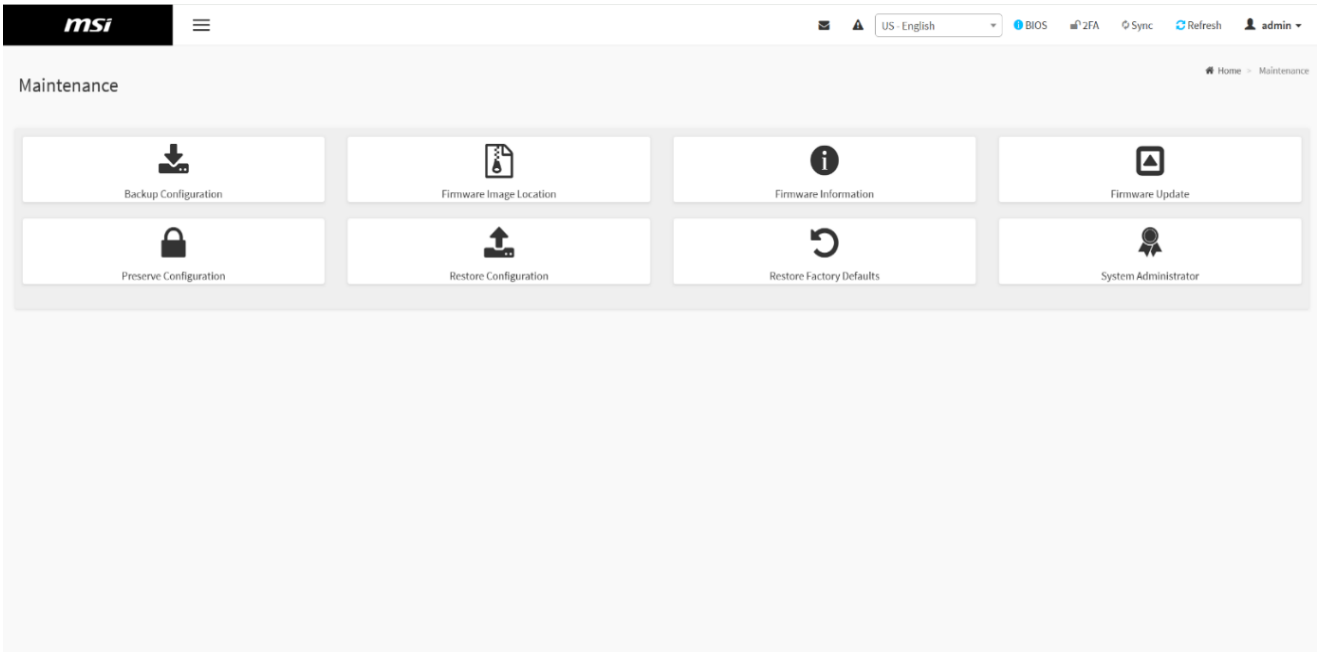
> ***Note**: During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.*

15 Maintenance Group

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

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

A sample screenshot of **Maintenance** page is displayed below.



Maintenance

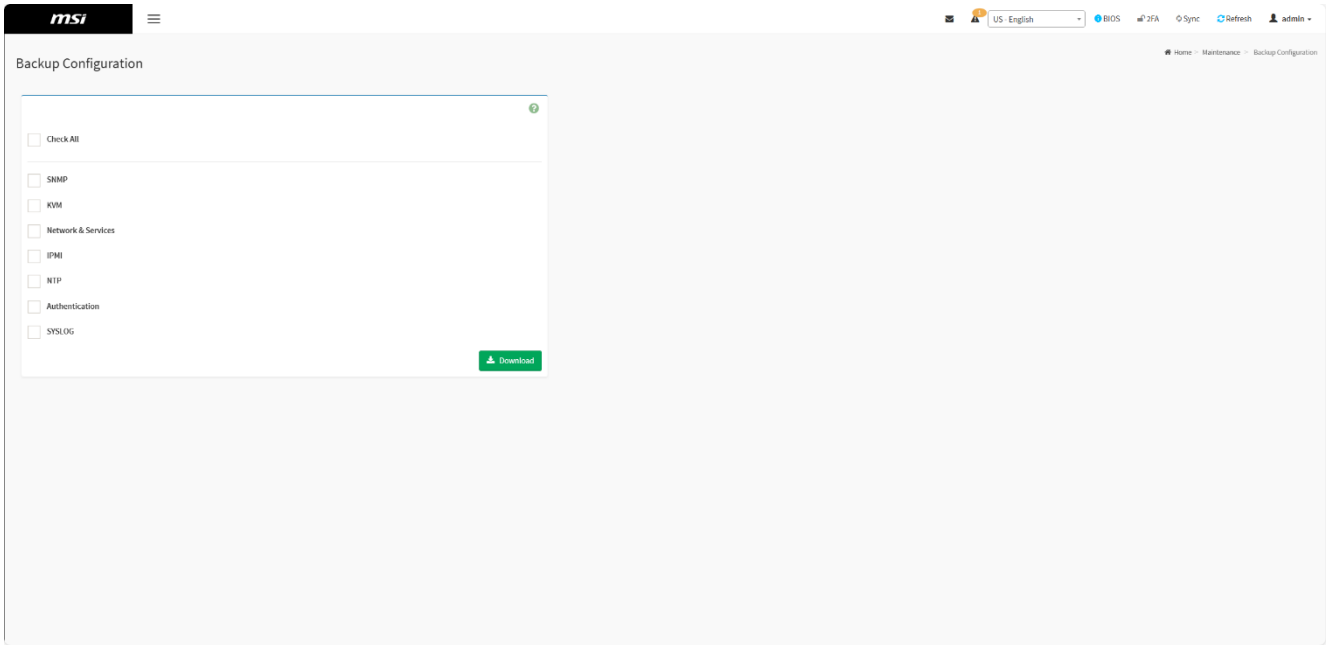
A detailed description is given below.

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.



Backup Configuration

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 user’s password be set to default password. User has to set password again after restoring configuration by using default user in case of login failure.*
>
> *The default password set for all users is fetched from macro “FEATURE_DEFAULT_PASSWD in PRJ“*

Procedure for Backup Configuration:

1. Click Check All to back up 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.

   >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.*

##

>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

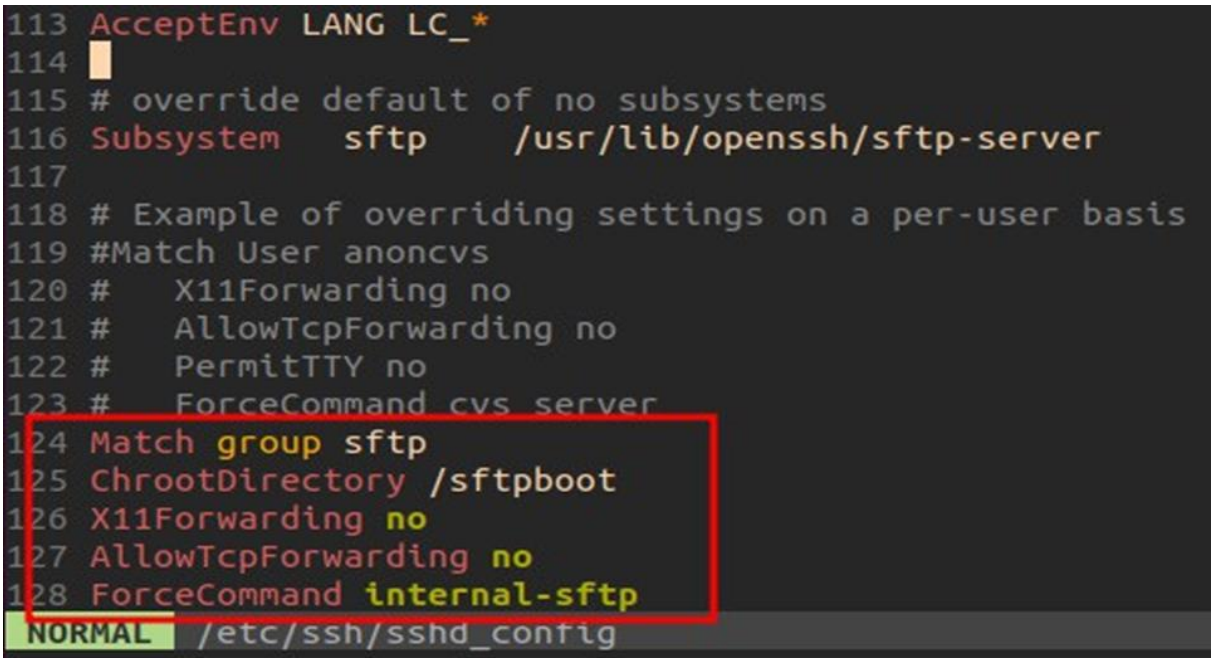
1. Install ssh if haven't installed.

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.



Firmware Image Location

4. Restart SSH services.

sudo systemctl restart ssh

5. Create sftp group 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:

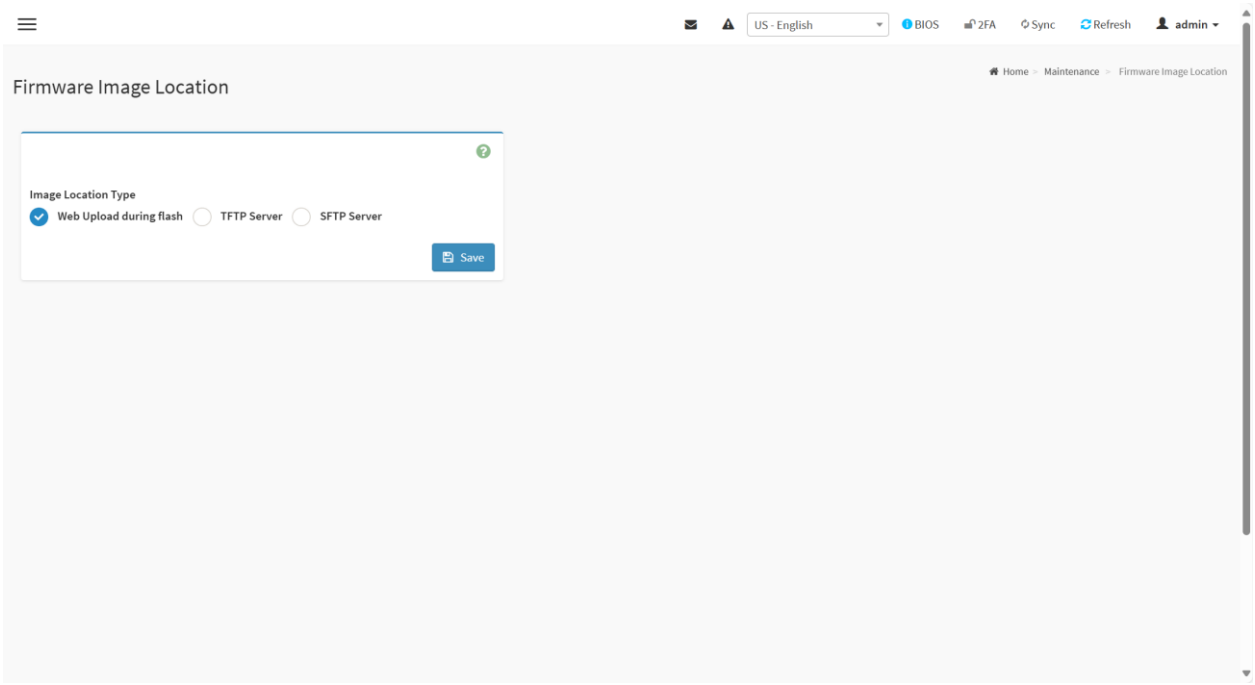
https://linuxhint.com/setup-sftp-server-ubuntu/

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

Firmware Image Location

This page is used to configure TFTP/SFTP location of BMC firmware image.

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



Firmware Image Location

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 filename 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.

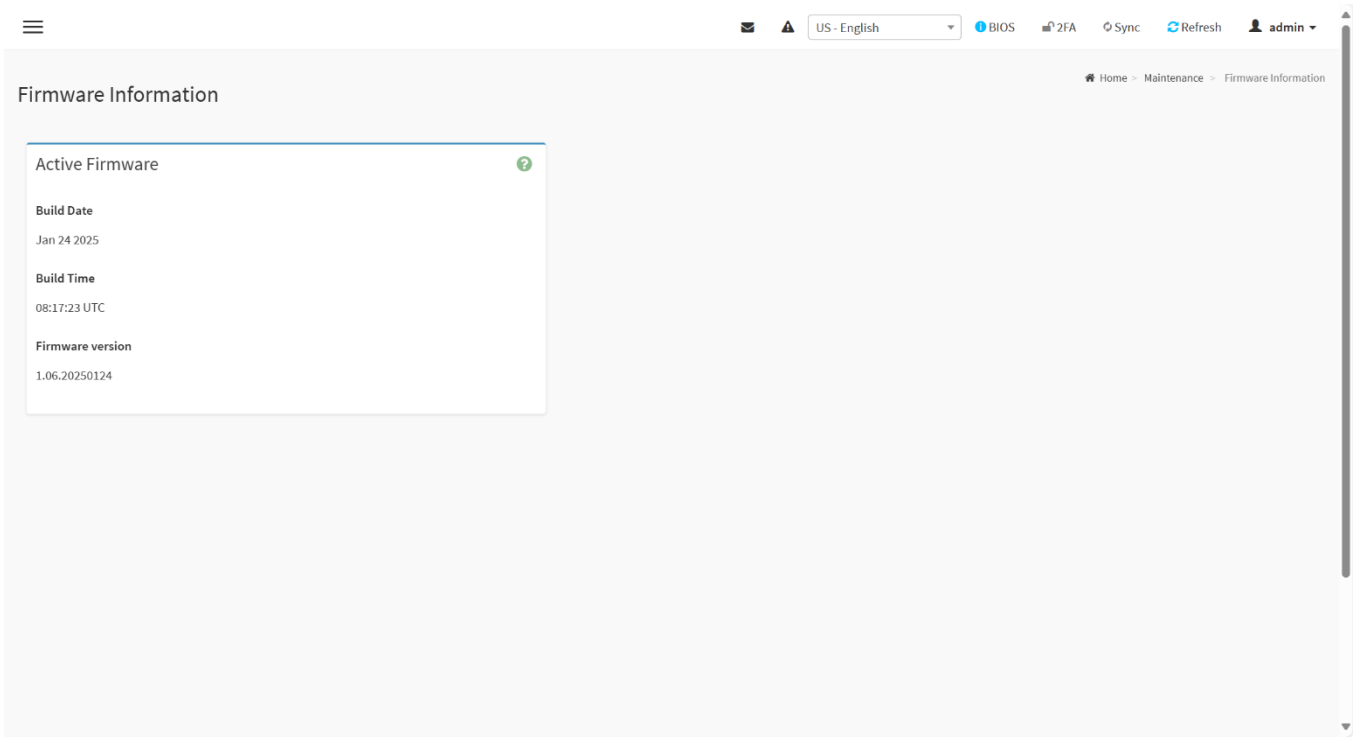
Procedure

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.

Firmware Information

This page is used to configure the Firmware Information settings.

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



Firmware Information

The various fields of Firmware Information page are given below.

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 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, HPM Firmware Update and Dual Firmware Update.

RSA PKCS1 PSS Padding: Enabling this support enables RSA-PSS algorithm Support. This support will be disabled by default and it can be enabled based on the customers requirement.

> ***Note**: Based on this feature "FEATURE_PKCS1_PSS_PADDING_SUPPORT" enabled/ disabled in PRJ, the option in imagesigning tool, pss padding has to be set Yes/No.*

To configure, choose '**Firmware Image Location**' under **Maintenance**. To open Firmware Update page, click **Maintenance** > **Firmware Update** from the menu bar.

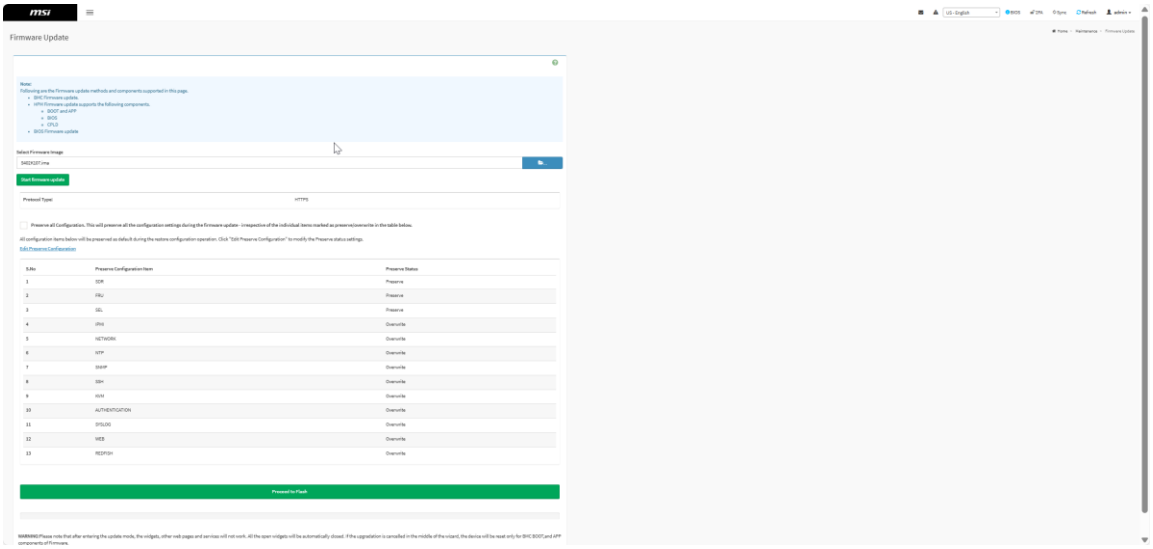
Procedure

1. Click **Browse** to select firmware image.

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

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

   ***Note**: 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.*



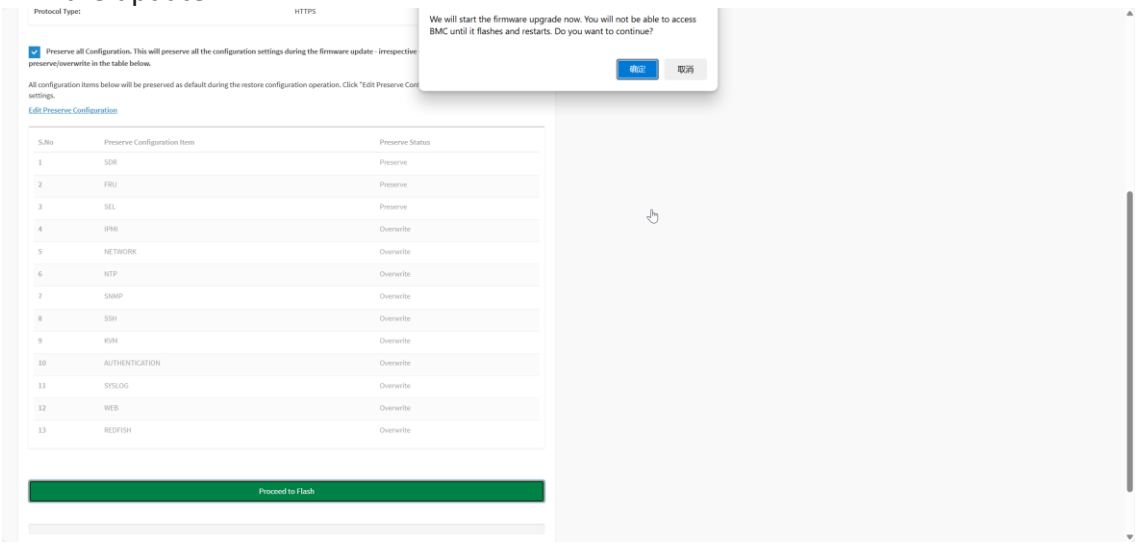
firmware Update Page

3. Click **Preserve all Configuration** to preserve all configuration.
   - **Preserve all Configuration**: To preserve all configuration.
   - **Edit Preserve Configuration**: To modify the Preserve status settings.

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

***Note**: All configuration items will be preserved/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.



Firmware Update

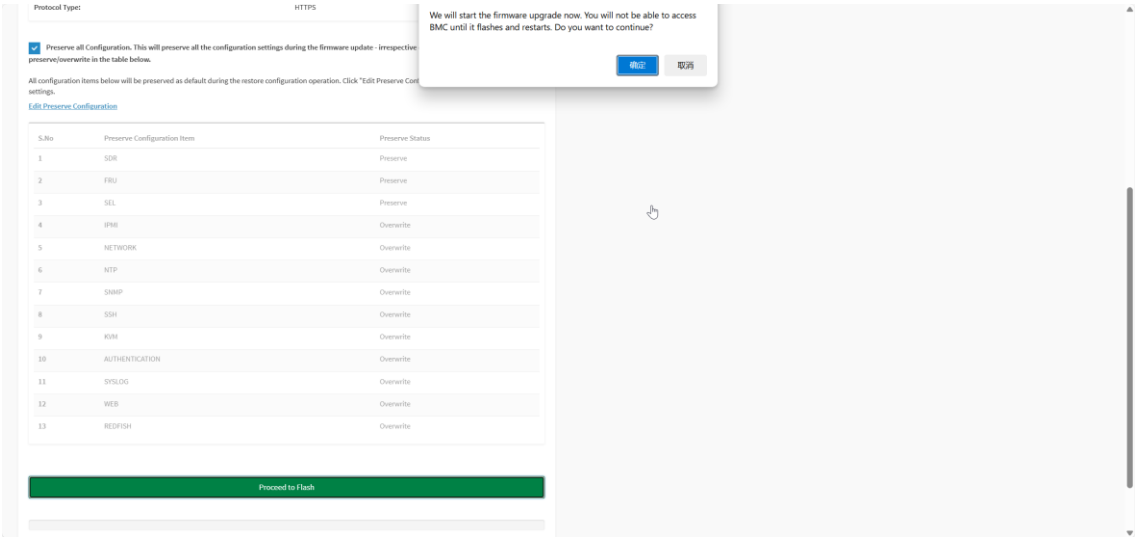
5. The Firmware update undergoes the following steps:

   a) Closing all active client requests

   b) Preparing Device for Firmware Upgrade

   c) Uploading Firmware Image.

A sample screenshot is shown as below.



Firmware Update - Image Upload Start

   d) Verifying Firmware Image

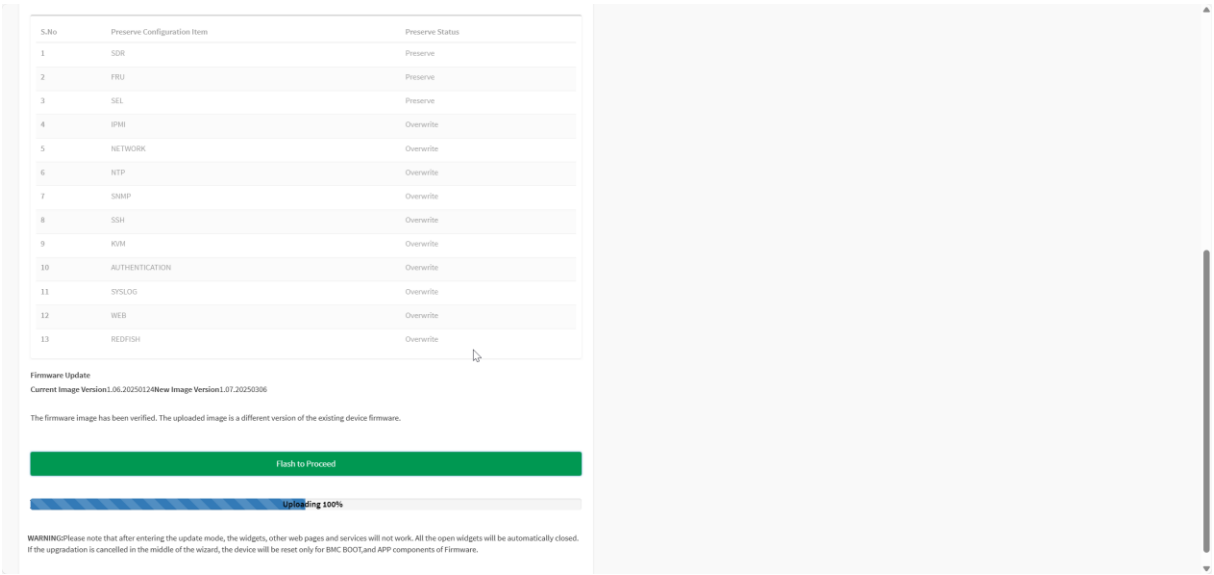
   In Section Based Firmware Update, you can configure the firmware image for section-based flashing. Check the required sections and click **Proceed** to update the firmware.

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

   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 differed, those modules will be flashed.

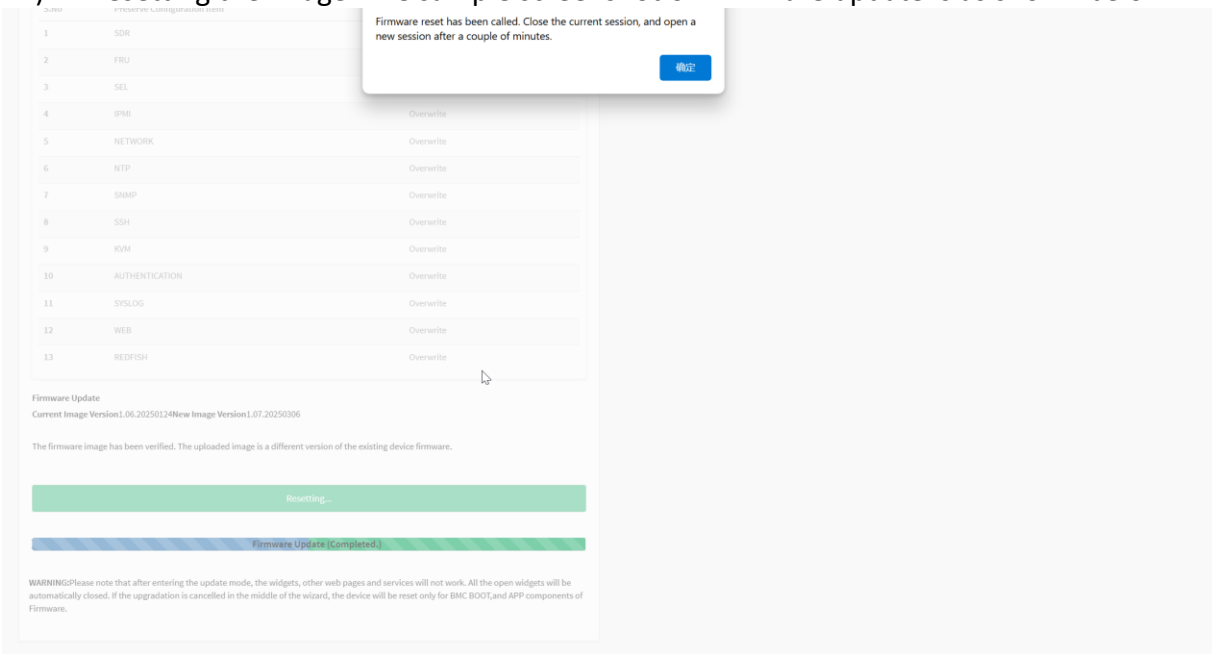
***Note**: Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.*



Section Based Firmware Flashing

e) Flashing Firmware Image

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



Firmware Update

***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.*

Dual Firmware Update

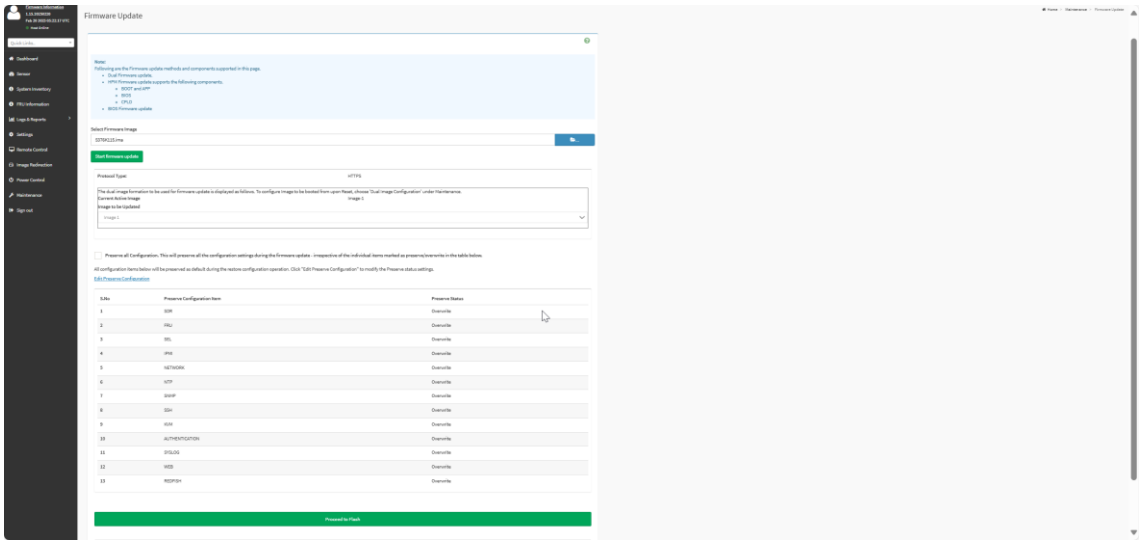
To perform Dual Firmware Update operation, click **Maintenance** > **Firmware Update** from the menu bar.

Procedure

1. Click **Browse** to select firmware image.

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

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



Dual Firmware Update Page

3. Select an Image (Inactive Image, Image 1, Image 2 or Both Image) from **Image to be Updated** drop-down list. The selected image will be getting flashed.
   - **Image to be Updated**: To update an Image (Inactive, Image 1, Image 2 or Both) to be flashed. If You select an Inactive image, the Inactive image will be flashed. If you select both images, then Both Image 1 and Image 2 will be flashed with uploaded image file.
   - **reboot the device after update**: This option is used to reboot the device after the firmware update.

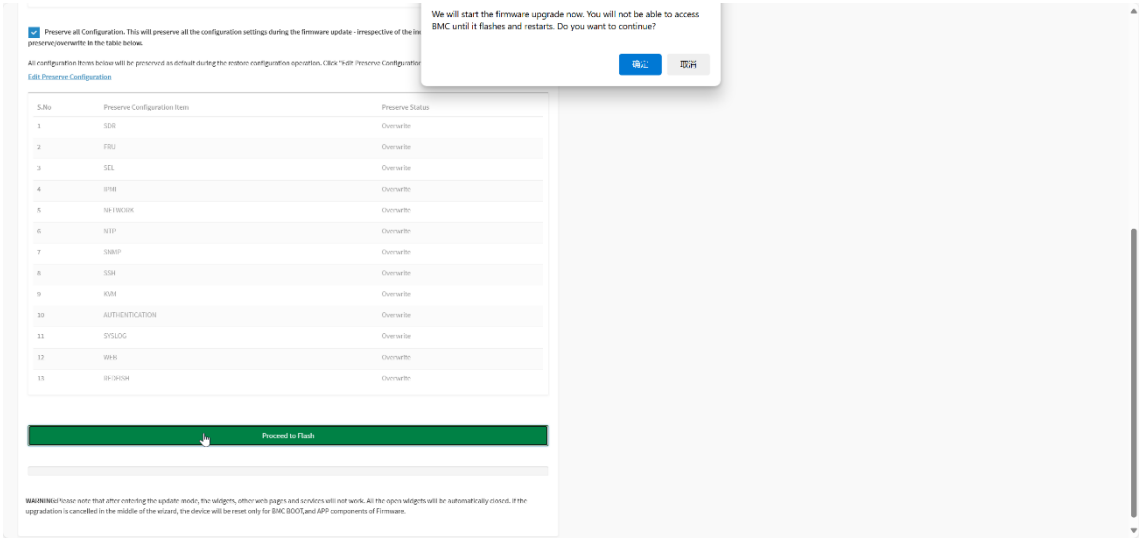
   ***Note**: To display/hide the reboot the device after update check box, based on feature "CON FIG_SPX_FEATURE_GLOBAL_ON_LINE_FLASHING_SUPPORT" is enable/disable in Dual Firmware Update.*

4. Click **Preserve all Configuration** to preserve all configuration.
   - **Preserve all Configuration**: To preserve all configuration.
   - **Edit Preserve Configuration**: To modify the Preserve status settings.

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

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

5. Click **Proceed to Flash**, it will prompt you with the warning message. Click **Ok** to start the Firmware update.



Firmware Update

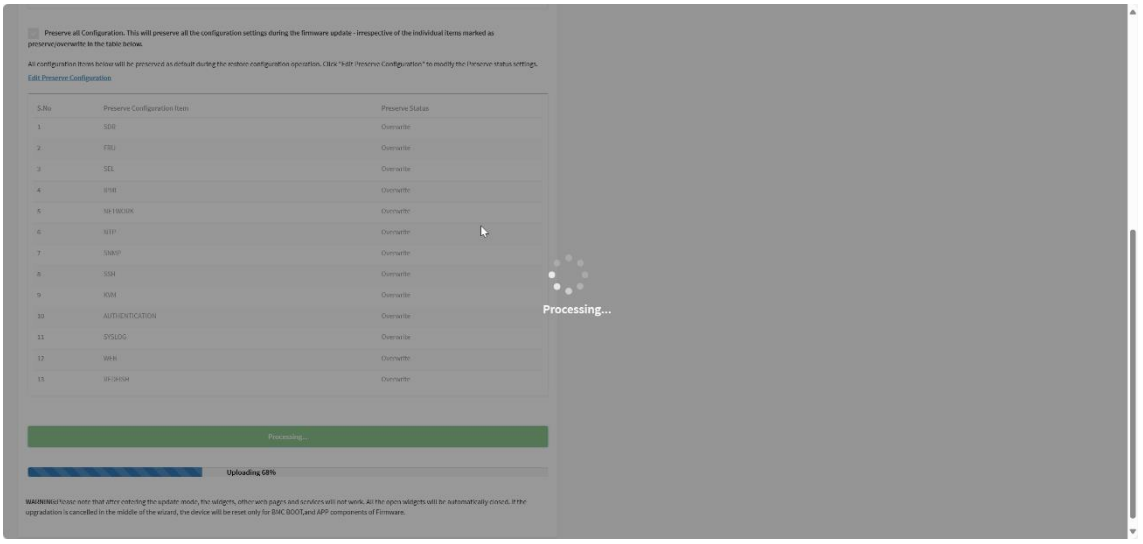
6. The Dual Firmware Update undergoes the following steps:

   a) Closing all active client requests

   b) Preparing Device for Firmware Upgrade

   c) Uploading Firmware Image

A sample screenshot is shown below.



Dual Firmware Update - Image Upload Start

   d) Verifying Firmware Image

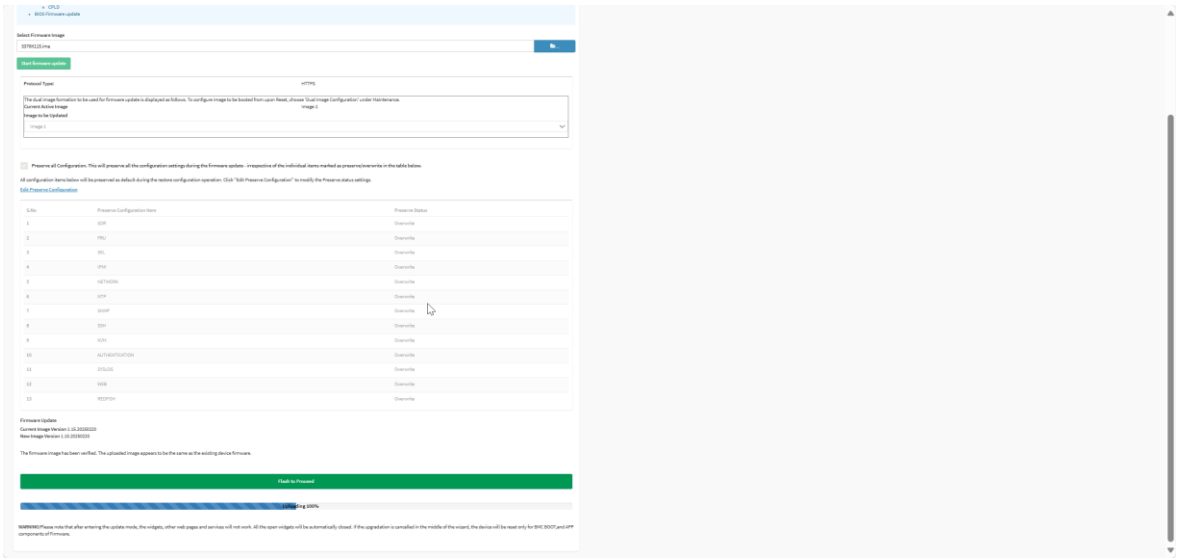
   In Section Based Firmware Update, you can configure the firmware image for section-based flashing. Check the required sections and click Proceed to update the firmware.

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

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 differed, those modules will be flashed.

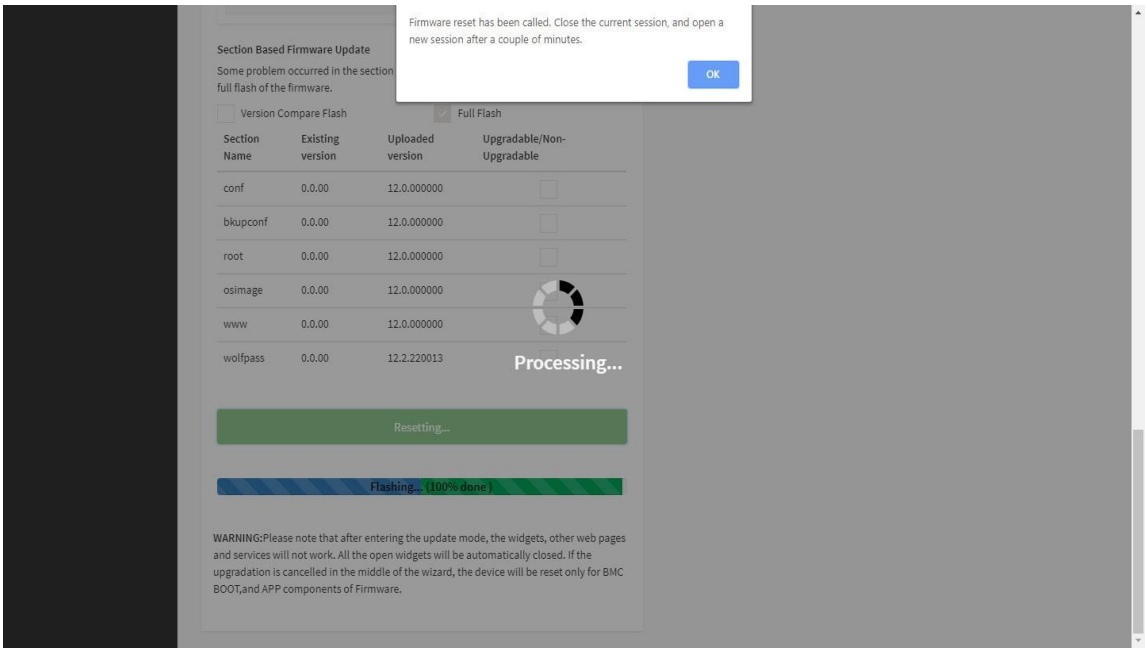
***Note**: Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.*



Section Based Firmware Flashing - - Image 1, Image 2 and Inactive Image

e) Flashing Firmware Image

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



Dual Firmware Update

***Note**: The Dual 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.*

ME Firmware Component Update

ME Firmware component update support is not available in the Eaglestream platform.

As per Node Manager 6.0 specification, Intel(R) has removed the IPMI commands that support the ME firmware update in the Eaglestream platform.

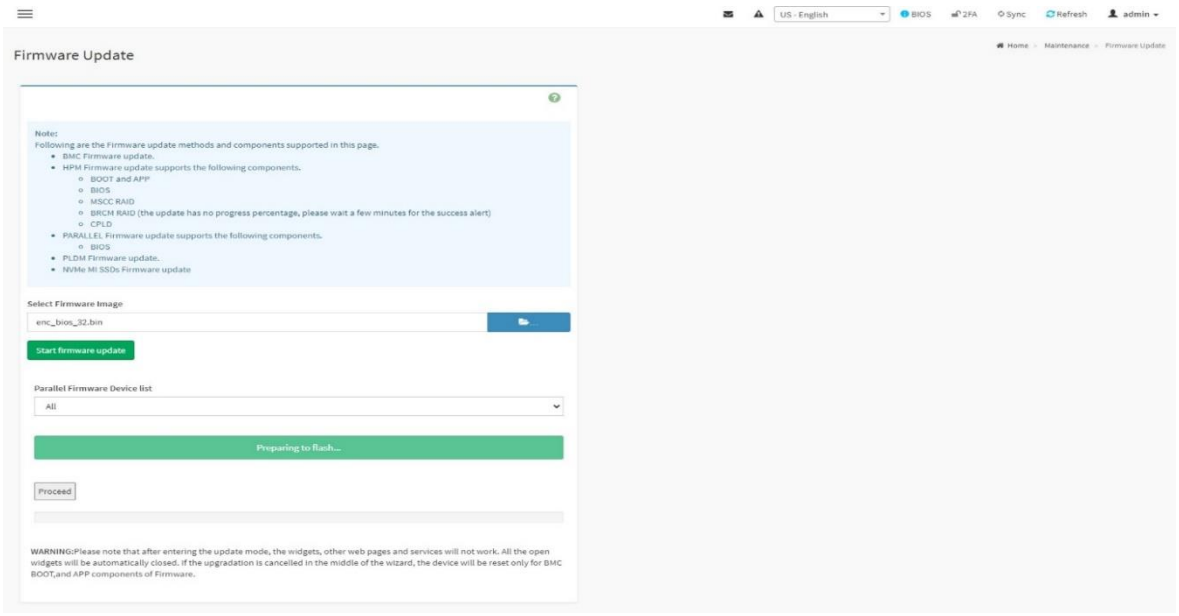
So, our BMC stack will not support ME firmware update (both binary and HPM format) through IPMI tool, WEB and Yafuflash in the Eaglestream platform.

Parallel Firmware Update

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

BIOS Firmware Update

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



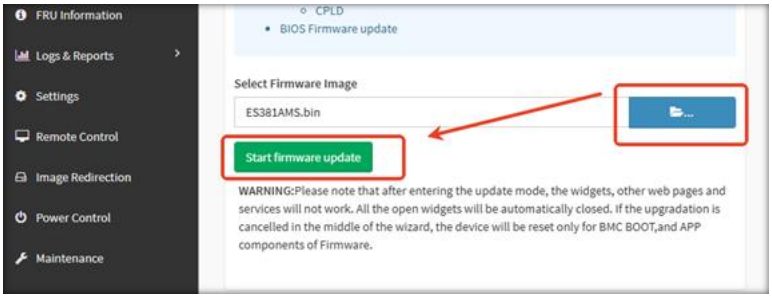
BIOS Firmware Update

Procedure

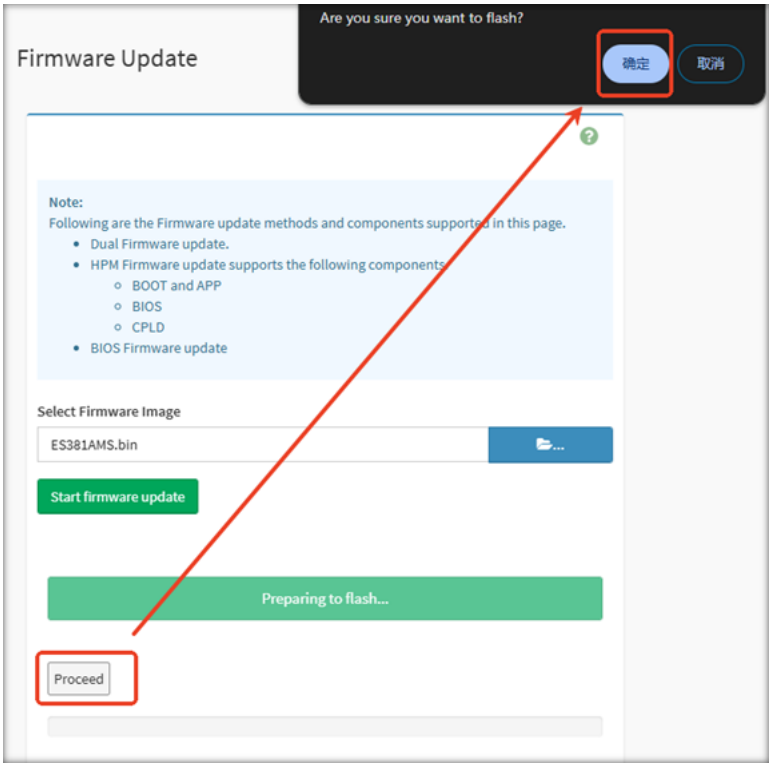
1. Click **Browse** to select BIOS Firmware image.

   ***Note**: Firmware update wizard will detect .bin and .bin_enc extensions, and validate as BIOS firmware image.*

2. Click **Start Firmware Update** to load the BIOS firmware image information. A sample screenshot is displayed below.
3. **Parallel Firmware Device List**: It will display the list of available BIOS spi devices.
   - User can select **All** or single available BIOS spi option from drop down list to perform the BIOS firmware update.
4. Click **Proceed**, it will prompt you with the warning message. Click **Ok** to start the firmware update. Sample screenshots are displayed below.



BIOS Firmware Update with All

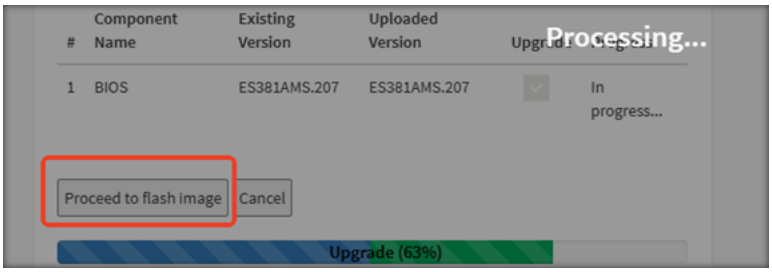


BIOS Firmware Update

5. The **BIOS Firmware Update** undergoes the below steps.
   a) Uploading Firmware Image
   b) Getting BIOS existing and uploaded versions (BIOS Tag)
   c) Flashing 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.*

6. Once the BIOS firmware update is completed, it will prompt you with the success message. Click **OK** to complete the process. Sample screenshots are displayed below.
7.



BIOS FW Update Success Message using single spi

***Note**: Like above, we can perform the HPM firmware update with the combination of components configured e.g. (APP, BOOT and BIOS), BIOS, etc.*

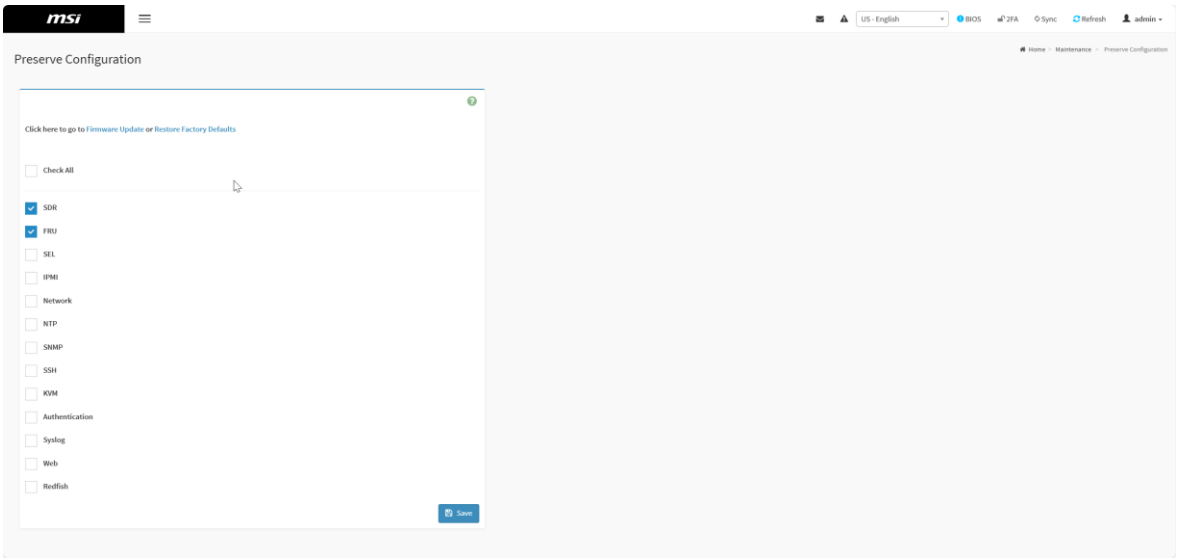
Preserve Configuration

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.*
- *When user performs Firmware update via WebUI, SSL certificates will be preserved, only if any "Preserve configuration" options are selected.*
- *When user performs Restore Factory Defaults via WebUI, SSL certificates will be pre- served, only if Authentication option is selected from "Preserve Configuration" page.*



Preserve Configuration

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 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.

shd_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.

usermacro.conf: This file saves the user defined macro from the JViewer.

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*

Redfish

Following files will be preserved.

redis-dump.rdb.gz: This gzip file contains compressed redis db data

RedisdbChecksum: This is the checksum value of redis-dump.rdb.gz file

redfish – This folder contains the multiple files of Redfish

bios - This folder contains the multiple files of bios

Dependency Configurations - NIL

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

Procedure

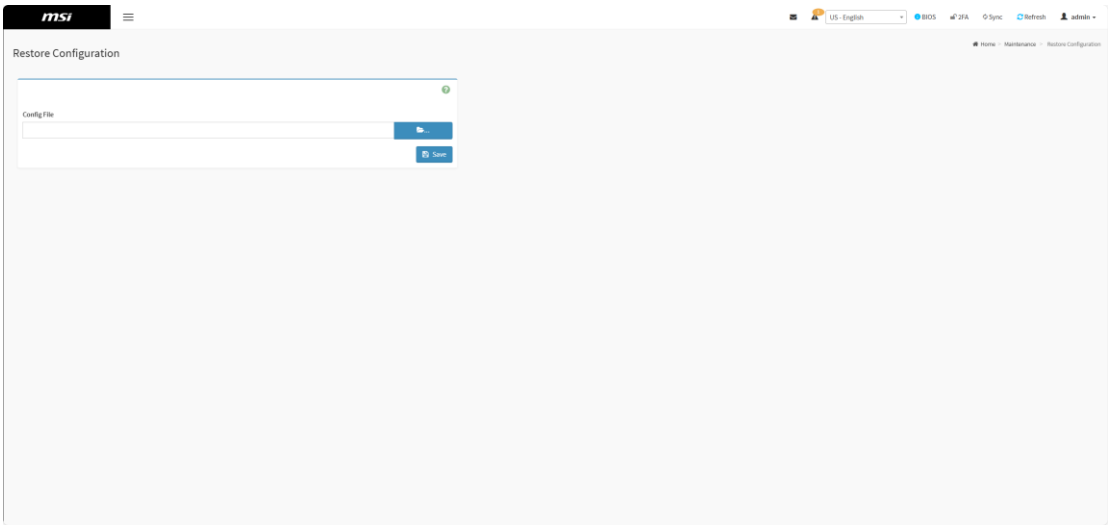
1. Click **Firmware Update** or **Restore Configuration** link to view Firmware Update or Restore Configuration page accordingly.

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.

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.



Restore Configuration

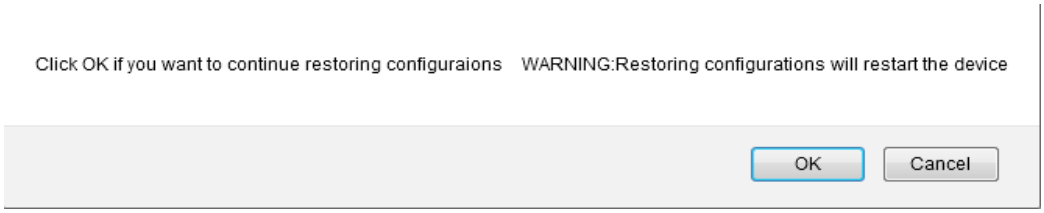
The various fields Restore Configuration page are given below.

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.



Restore Configuration

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

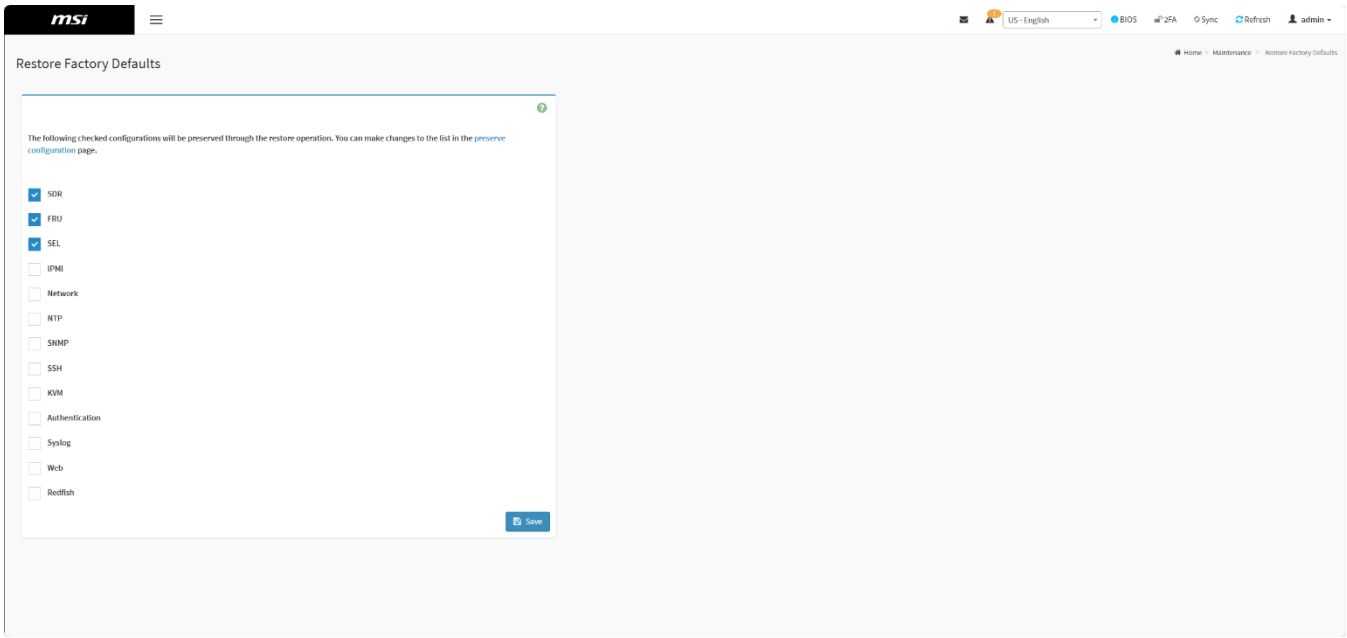
Restore Factory Defaults

In MSI GUI, this option is used to restore the factory defaults of the device firmware.

This section lists the configuration items that will be preserved during 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.



Restore Factory Defaults

Procedure

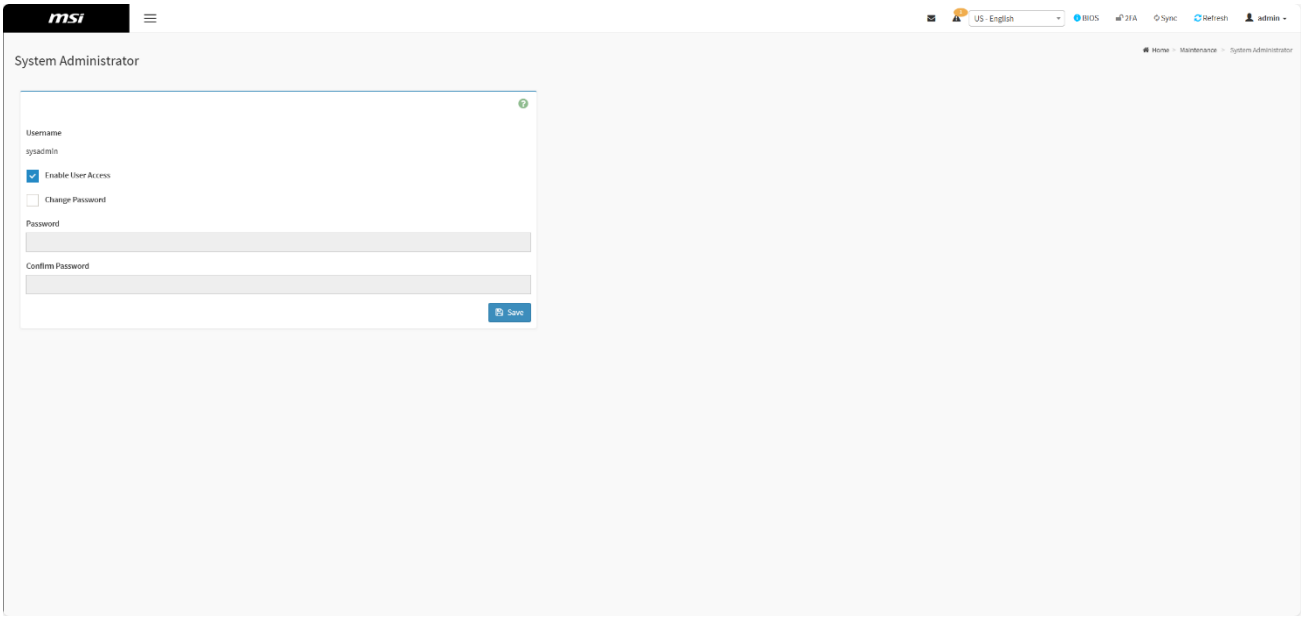
1. Click **Preserve Configuration** to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click **Restore Factory Defaults** to restore the factory defaults of the device firmware.

   ***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.*

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.



System Administrator

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.

Fail Safe Booting Configuration

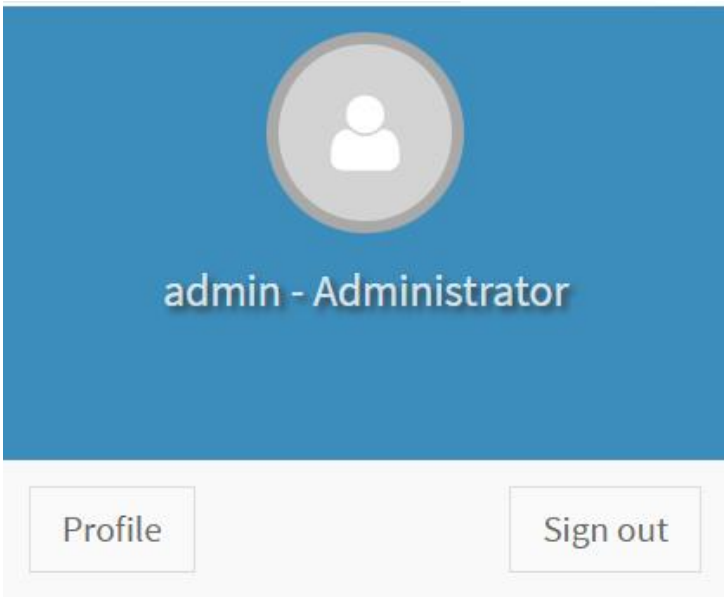
Hardware based fail safe boot support - This feature supports switching to secondary image as failsafe using hardware configurations. Using this feature, the user can boot into secondary image, even though primary uboot is crashed. Please verify whether SOC supports this feature.

Software Fail Safe Boot - Legacy dual image support. This feature uses common UBOOT which switches between 2 different images based on user requirement. This feature does not re- quires a special hardware support.

> ***Note**: To display/hide the Dual Image configuration page, based on feature "CONFIG_SPX_FEATURE_SW_FAILSAFE_BOOT" is enabled/disabled.*

16 Sign Out

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



admin – Sign out

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

MSI.COM

EPS.MSI.COM