BMC

J4024-04-35X_BMC
User's Manual

UM_J4024-04-35X_BMC_v1.1_022223

Table of Contents

Preface i
Chapter 1. Login Information 1
1.1 User Name and Password 1
1.2 Menu Bar 2
1.3 Quick Button and Logged-in User 3
Chapter 2. Dashboard 4
Chapter 3. Sensor 5
Chapter 4. FRU Information 7
Chapter 5. PSU Information 8
Chapter 6. Logs & Reports 9
6.1 IPMI Event Log 10
6.2 Audit Log 11
Chapter 7. Settings 12
7.1 Date and Time 13
7.2 Log Settings 14
7.2.1 SEL Log Setting Policy 14
7.2.2 Advanced Log Settings 15
7.3 Network Settings 17
7.3.1 Network IP Settings 17
7.3.2 Network Link Configuration 19
7.3.3 DNS Configuration 20
7.4 Platform Event Filter 23
7.4.1 Event Filters 23
7.4.2 Alert Policies 27
7.4.3 LAN Destinations 29
7.5 Service 31
7.6 SMTP Settings 34
7.7 System Firewall 36
7.7.1 General Firewall Settings 36
7.7.2 IP Address Firewall Rules 39
7.7.3 Port Firewall Rules 41
7.8 User Management 44
7.9 Power Restore Policy 49
Chapter 8. Remote Control 50

Chapter 9. Chassis Identify 51
Chapter 10. HDD Management 52
Chapter 11. Power Control 53
Chapter 12. Maintenance Group 54
12.1 Backup Configuration 55
12.2 Firmware Information 56
12.3 BMC Firmware Information 57
12.4 BMC Firmware Update 58
12.5 Preserve Configuration 65
12.6 Restore Configuration 67
12.7 Restore Factory Default 68
12.8 Expander Update 69
12.9 CPLD Firmware Update 70
12.10 BMC Reset 71
Chapter 13. Sign Out 72
Chapter 14. Technical Support 73

Document Release History

Release Date	Version	Update Content
June, 2021	1	Manual release to public.
February, 2023	1.1	Update the content of Chapter 12. / Image update.

Preface

Copyright

Trademarks

Changes

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

Warning

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

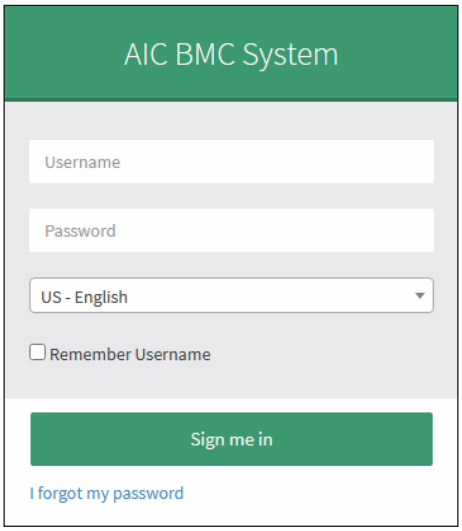
Disclaimer

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

Chapter 1. Login Information

1.1 User Name and Password

Initial access 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. Default language will be selected as US-English if the browser configured language not supported by Web UI. Entire Web UI pages language strings will be displayed based on selected language from drop-down.

Remember Username: Check this option to remember your login Username. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill Username for you.

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

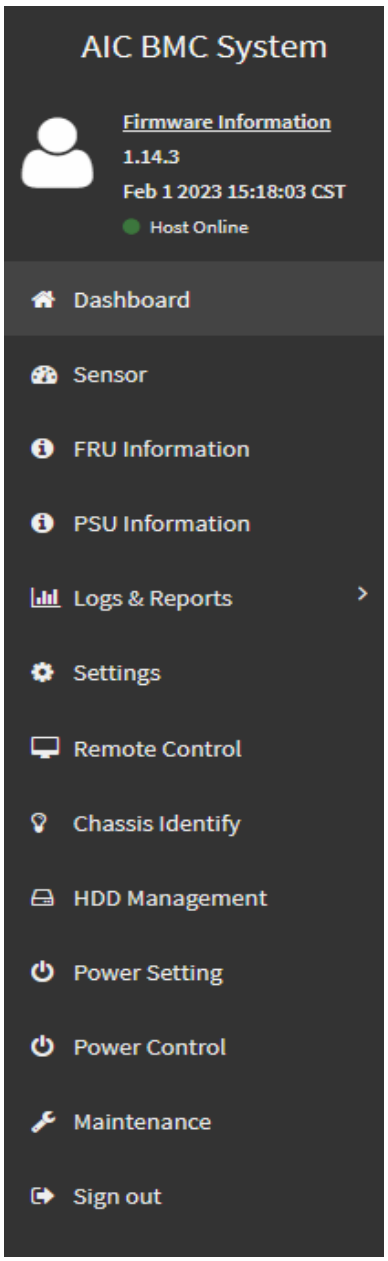
I Forgot my Password: If you forget your password, you can generate a new password using this link.

1.2 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
- PSU Information
- Logs & Report
- Settings
- Chassis Identify
- HDD Management
- Power Control
- Maintenance
- Sign out

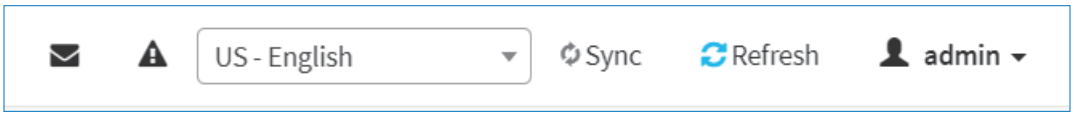


Menu Bar

1.3 Quick Button and Logged-in User

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

User Information
The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions.



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

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

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

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

Signout: Click the Sign out icon to log out.

Notification: Click to view the notification received.

Quick Search: Quick Search is a short-cut for the available menu and sub-menu pages. It displays available search queries. Click US - English (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.

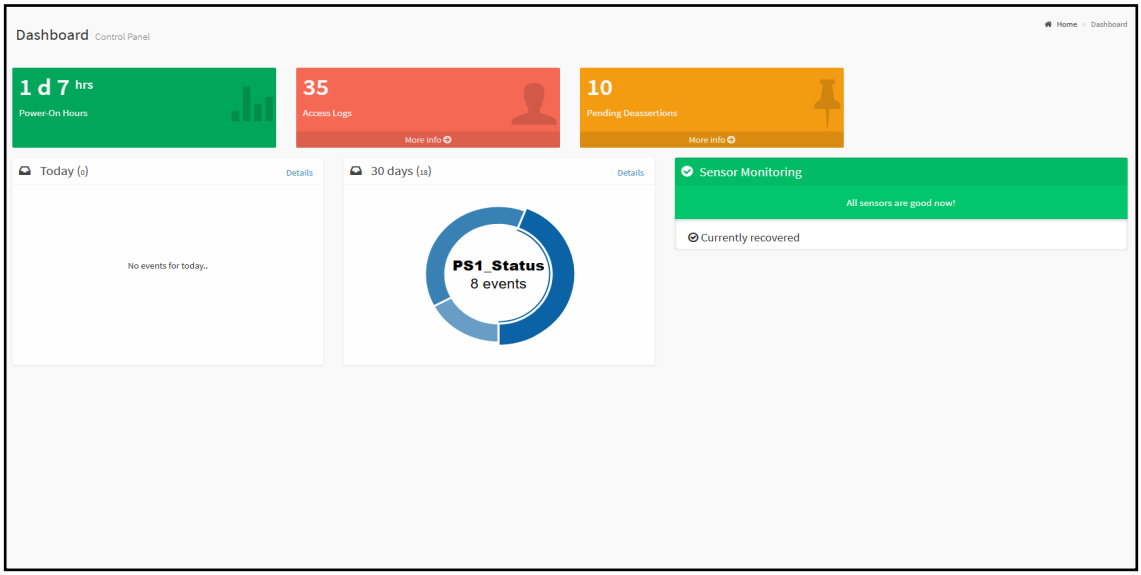
Help

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

Chapter 2. Dashboard

The Dashboard page gives the overall information about the status of a device.

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



Dashboard page

A brief description of the Dashboard page is given below.

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

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

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

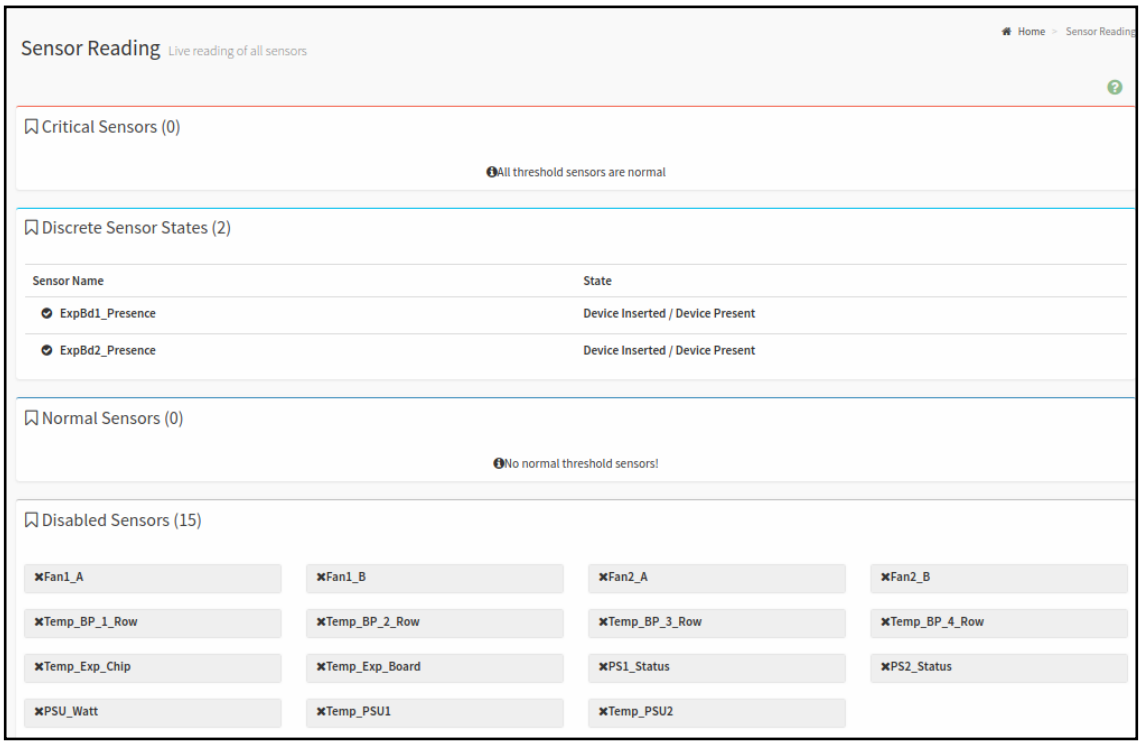
Today & 30 Days (Event Logs)
This page displays the list of event logs occurred by the different sensors on this device. Click Details link on Today and 30 days to view the event logs for Today and 30 days respectively.

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

Chapter 3. Sensor

The Sensor Reading page displays all the sensor related information.

To open the Sensor Reading page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Reading page is given below.

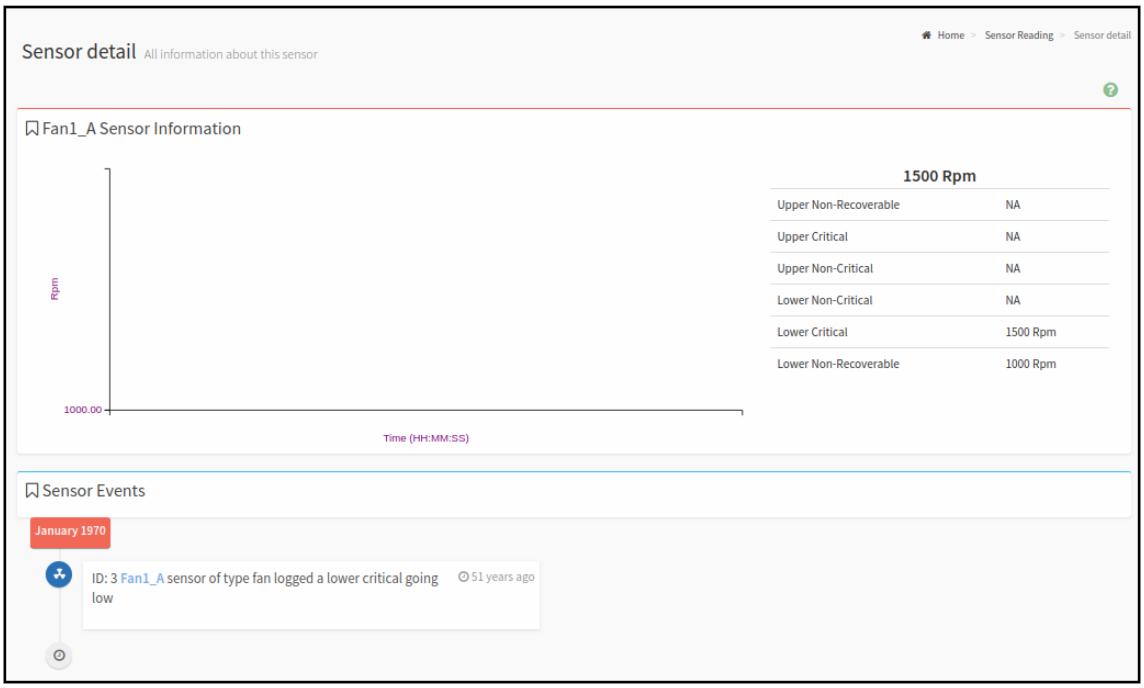


Sensor page

The Sensor Reading page contains the following information.
In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behaviour 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.

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



Sensor detail page

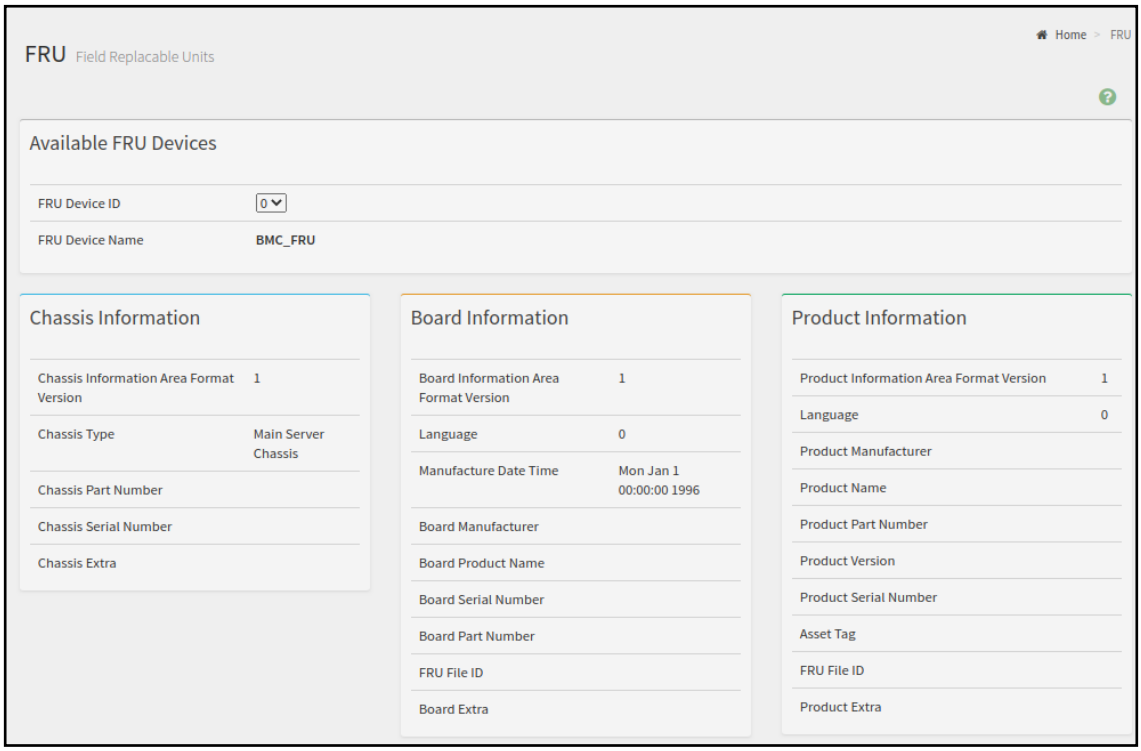
NOTE
Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live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

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

Chapter 4. FRU Information

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

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



FRU Information page

The following fields are displayed here for selected device.

Available FRU Devices

- FRU device ID - Select the device ID from the drop down list
- FRU Device Name - The device name of the selected FRU device.

Chassis Information

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

Board Information

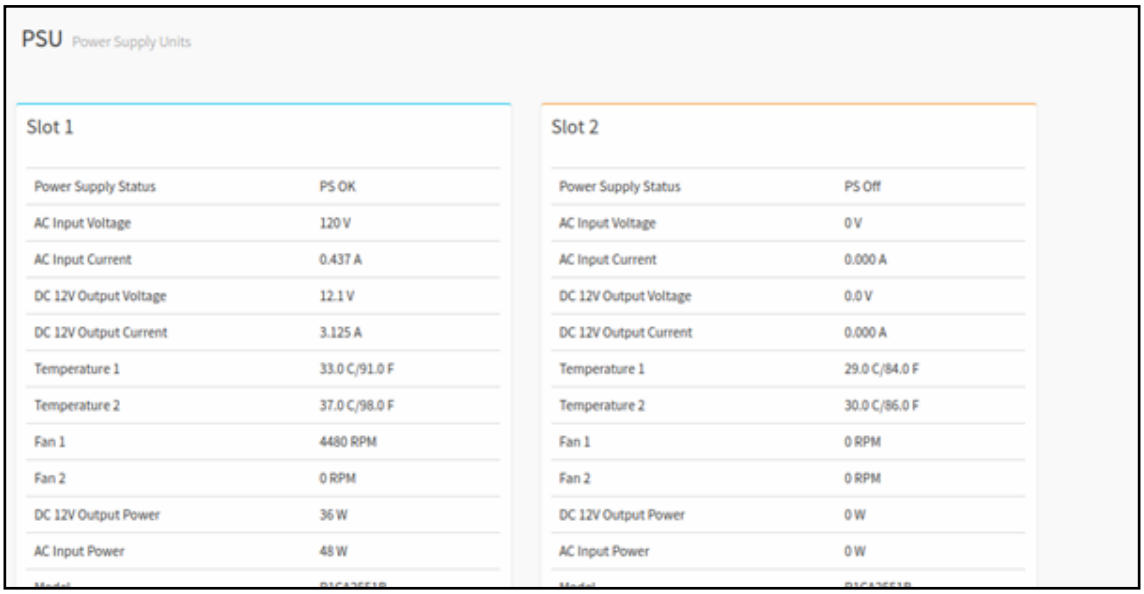
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

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

Chapter 5. PSU Information

PSU Information page displays the PSU information. This page shows information like Status, Sensor Reading and Model Details of the PSU. A screenshot of PSU Information page is given below.



FRU Information Page

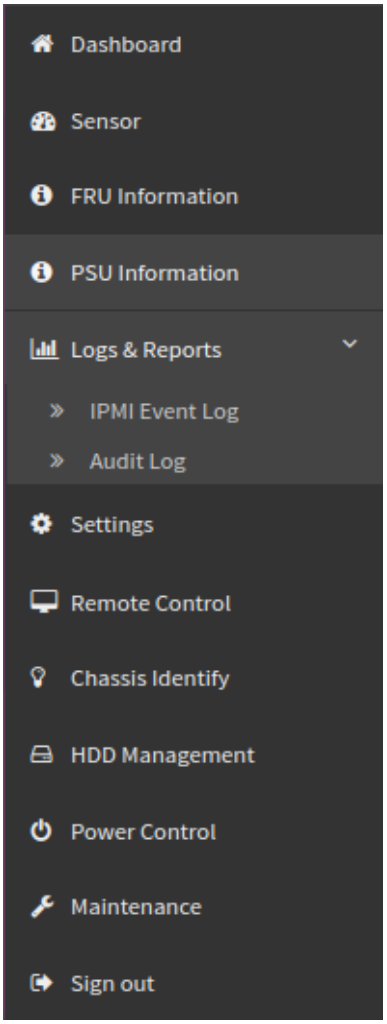
NOTE
If the device is not detected successfully, please turn on the power or reinstall the device.

Chapter 6. Logs & Reports

The Logs & Reports page displays the following information.

- IPMI Event Log
- Audit Log

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

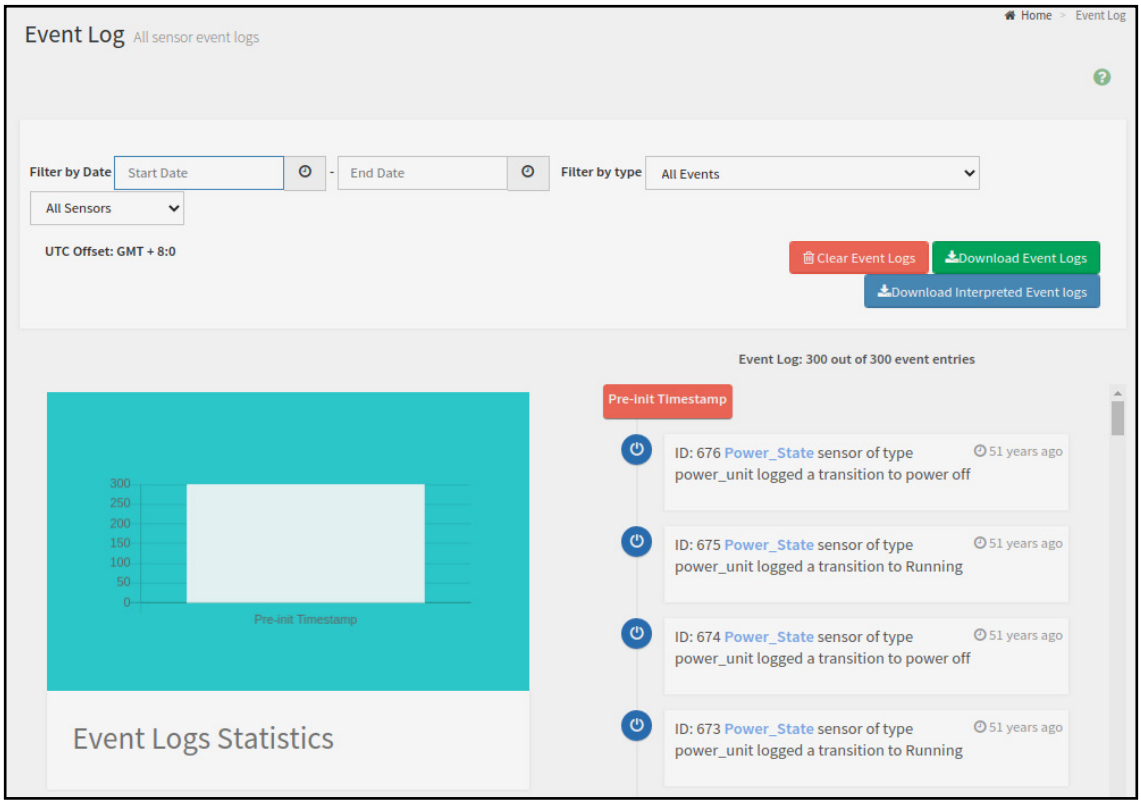


Logs and Reports Menu

6.1 IPMI Event Log

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

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



Event Log page

The Event Log page consists of the following Fields.

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

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.

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.

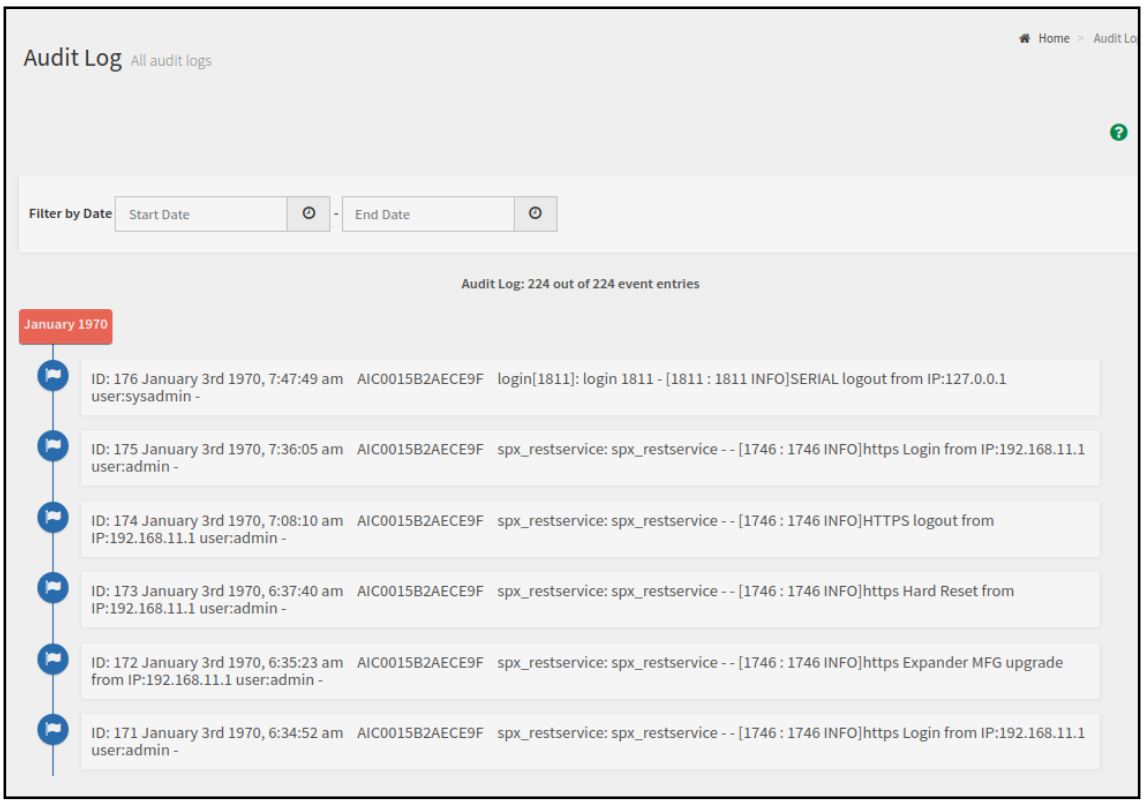
Download Event Logs: To download the event logs.

6.2 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.

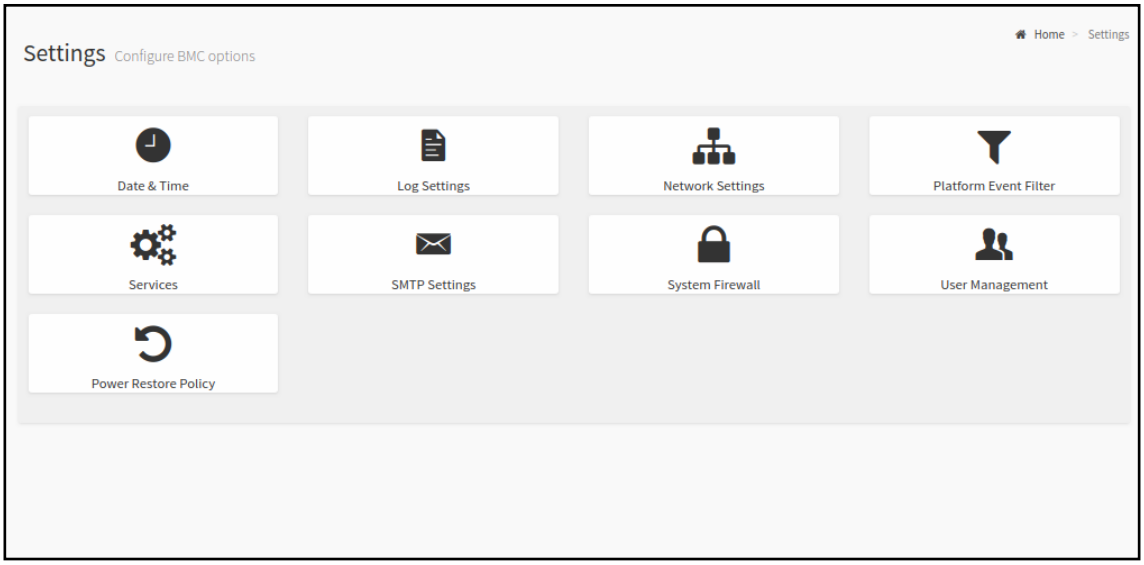
To open the Event Log page, click Logs & Reports → Audit Log from the menu bar. A sample screenshot of Audit Log page is shown below.



Audit Log page

Chapter 7. Settings

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

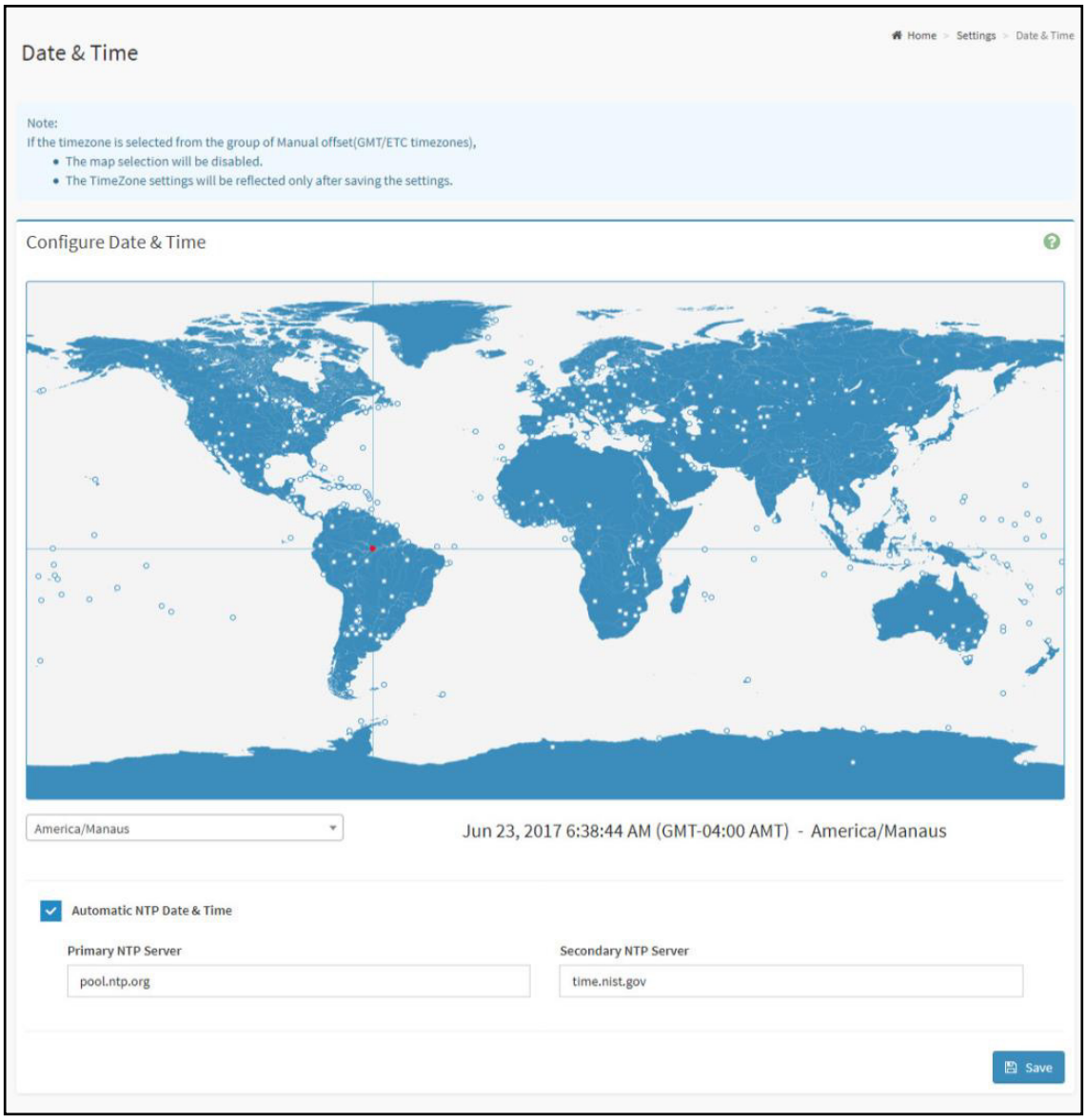


Configuration Group Menu page

A detailed description of the Configuration menu is given below.

7.1 Date and Time

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



Date & Time Automatic Date & Time page

The Date & Time section consists of the following fields.

Configure Date & Time: Displays Time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.

Select Time Zone: This field is used to set the date and time on the BMC.

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

Save: To save the settings.

> **NOTE**
> If the time zone is selected as Manual Offset, the map selection will be disabled. The Time Zone settings will be reflected only after saving the settings.

7.2 Log Settings

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

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

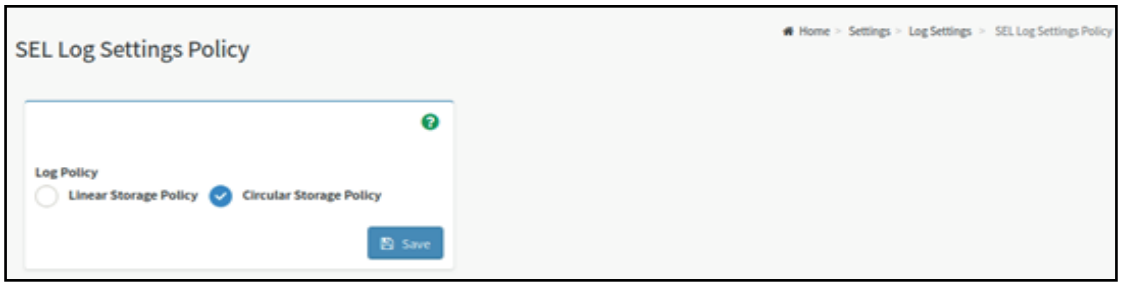
Log Settings page

System and Audit Log Settings
The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

7.2.1 SEL Log Setting Policy

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



SEL Log Settings Policy page

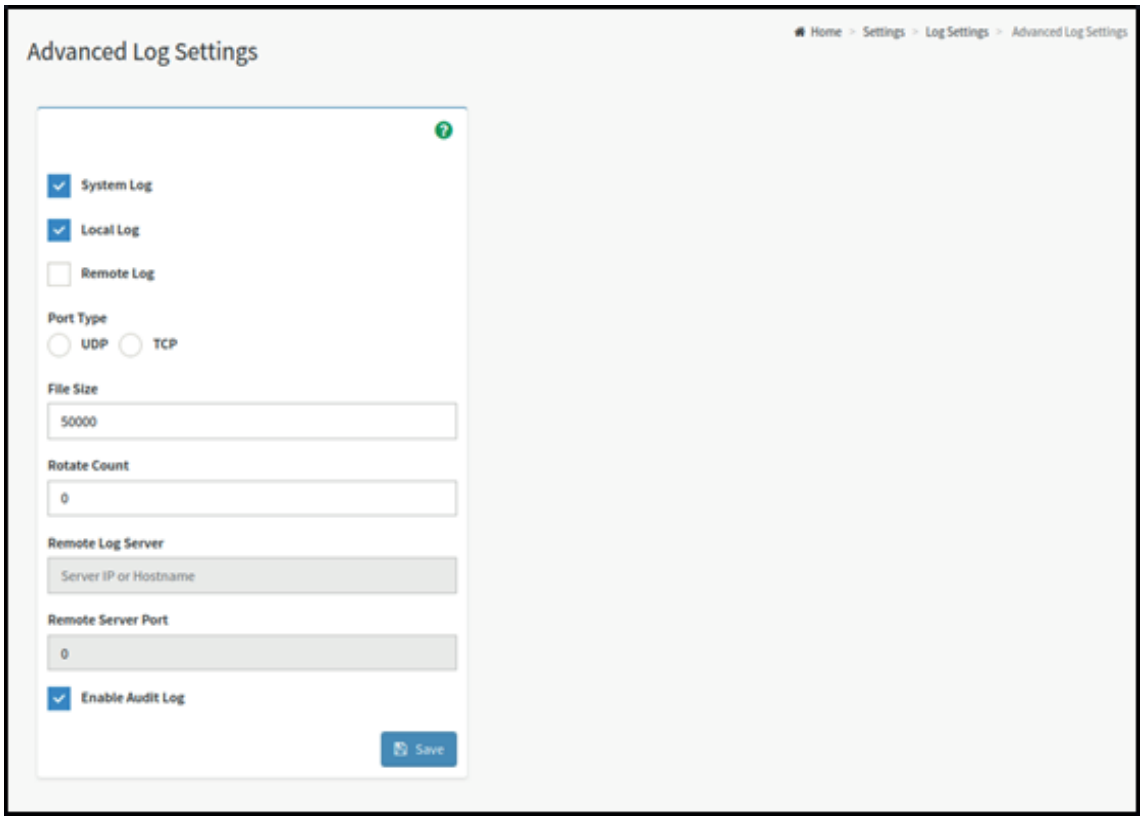
This page is used to configure the log policy for the event log. The fields are as followed.

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

Save: To save the configured settings.

7.2.2 Advanced Log Settings

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



Advanced Log Settings page

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 selection 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.

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.

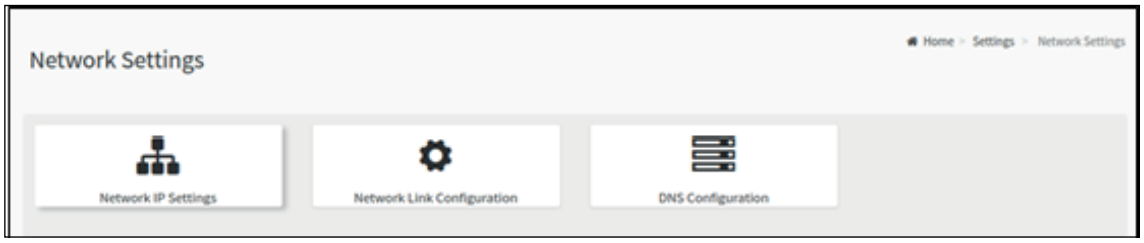
> **NOTE**
> Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

Enable Audit Log: To enable or disable the audit log.

Save: To save the changes.

7.3 Network Settings

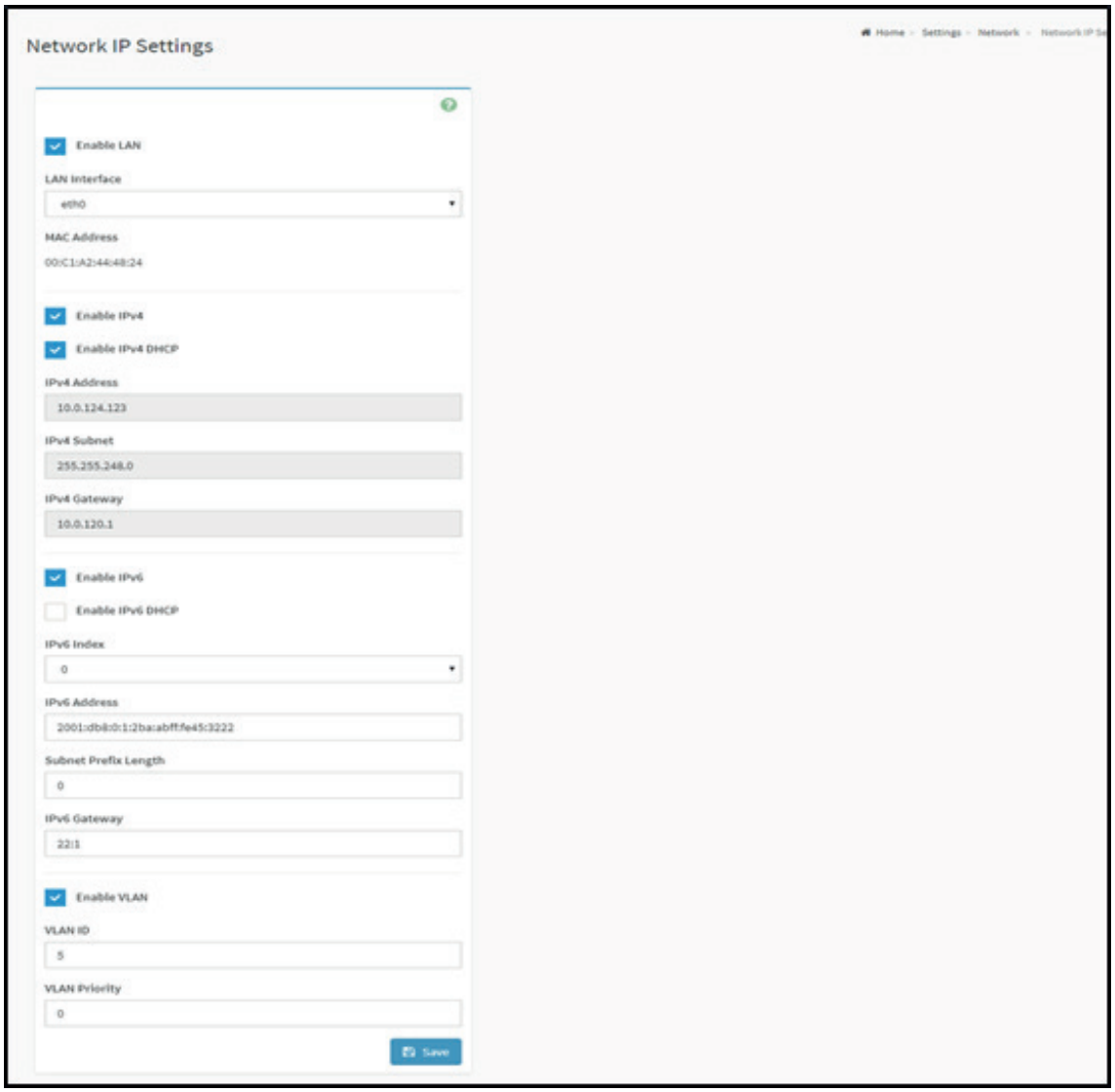
The Network Settings Page is used to configure the network settings for the available LAN channels. A sample screenshot of Network Settings page is shown below.



Network Settings page

7.3.1 Network IP Settings

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



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 IPv 4: This option is to enable/disable the IPv4 settings in the device.

Enable IPv4 DHCP: This option is to enable IPv4 DHCP support for the selected interface.

IPv4 Address, IPv4 Subnet Mask , and IPv4 Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.

> **NOTE**
> - IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
> - Each Number ranges from 0 to 255.
> - First Number must not be 0.

Enable IPv6: To Enable/Disable the IPv6 configuration settings.

Enable IPv6 DHCP: To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).

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

IPv6 Index: To specify a static IPv6 Index to be configured to the device. Eg: 0

IPv6 Address: To specify a static IPv6 address to be configured to the device. Eg: 2004::2010

Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.

> **NOTE**
> Value ranges from 0 to 128.

IPv6 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.

Enable VLAN: To enable/disable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.

> **NOTE**
> Value ranges from 2 to 4094.

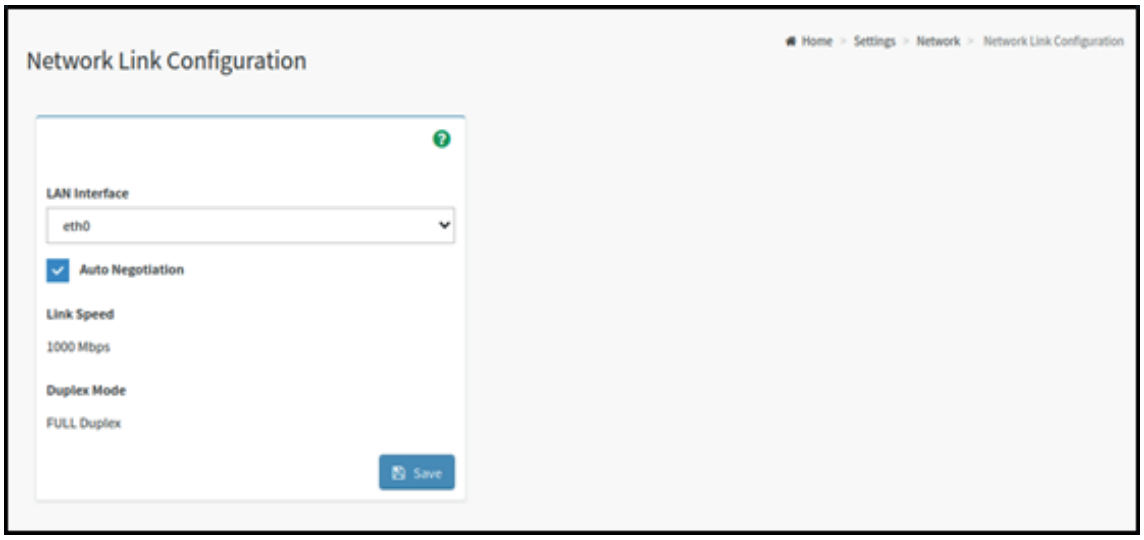
VLAN Priority: The priority for VLAN configuration.

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

7.3.2 Network Link Configuration

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

To open Network Link page, click Settings → Network Settings → Network Link 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.

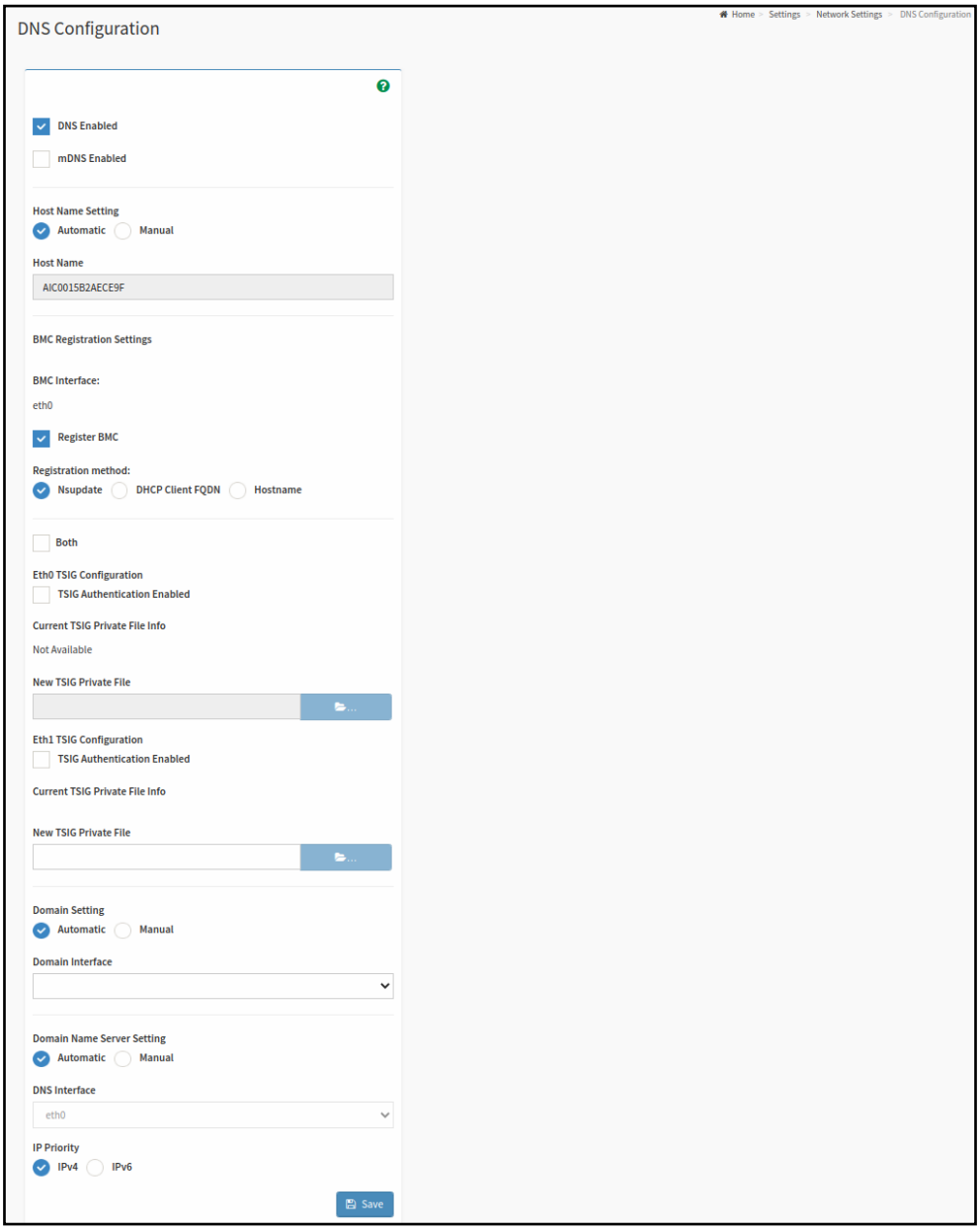
Save: To save the settings.

7.3.3 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 characters '-'(hyphen) and '_'(underscore) are allowed.
> - It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_) character.

BMC Registration Settings

BMC Interface: Options to register the BMC are through an Interface.

Register BMC: To register BMC through registration method.

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

TSIG Configuration:
Both: Check this option to modify TSIG authentication for both interfaces.
Eth 0&1:

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

> **NOTE**
> TSIG file should be of private type.

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

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

> **NOTE**
> If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name".

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

Domain Name Server Setting

Automatic: If you select Automatic “DNS Interface” option should be explained.
Manual: Specify the DNS (Domain Name System) server address to be configured for the BMC.

IP Priority:

- If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
- If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.

> **NOTE**
> This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

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

> **NOTE**
> - IPv4 Addresses should be given in dotted decimal representation.
> - IPv6 Addresses are supported and must be global unicast addresses.

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Save: To save the entered changes.

7.4 Platform Event Filter

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

The PEF Management is used to configure the following

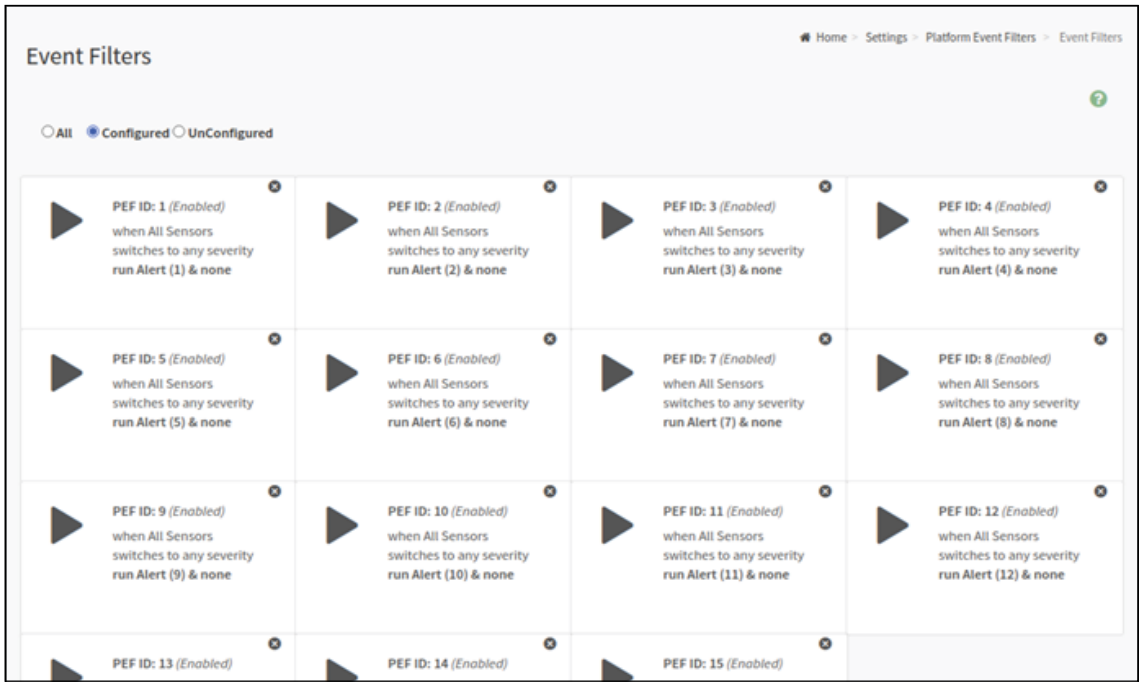
- Event Filters
- Alert Policies
- LAN Destinations

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

Platform Event Filters page

7.4.1 Event Filters

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

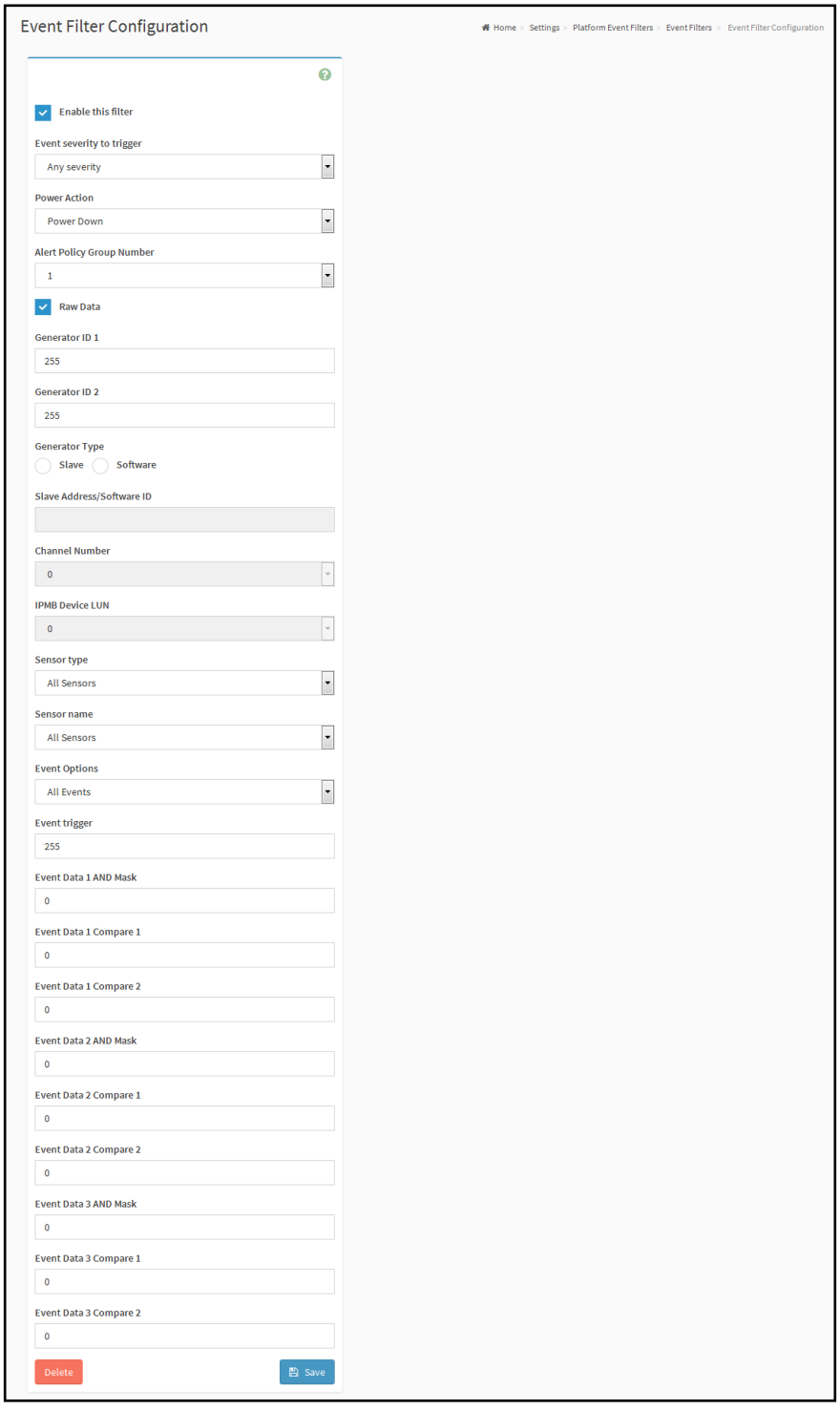


Event Filters page

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 Filters Configuration page

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 Al l 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 wild carded or compared bits.

> **NOTE**
> Value ranges from 1 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.

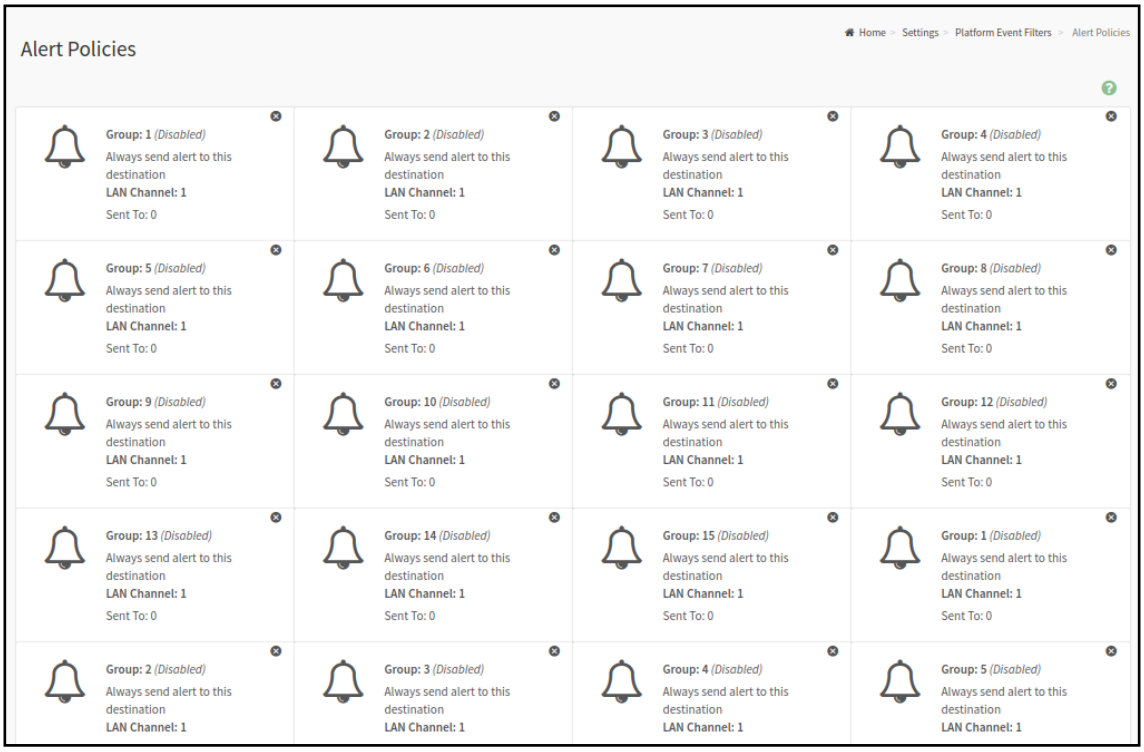
> **NOTE**
> Value ranges from 1 to 255.

- Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
- Event Da ta 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.

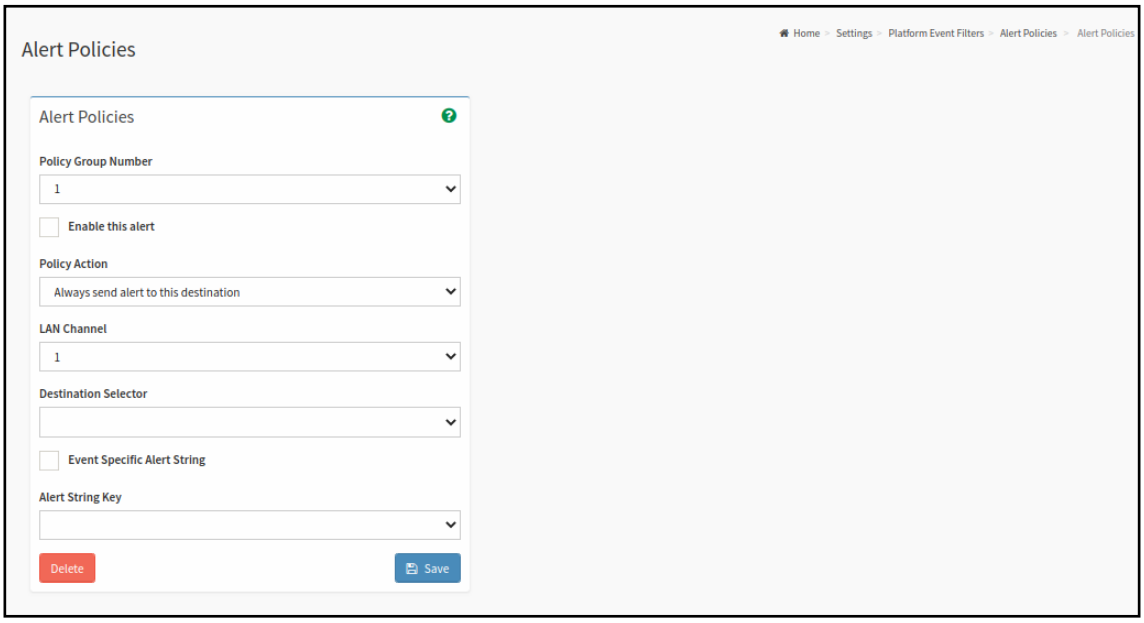
7.4.2 Alert Policies

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



Platform Event Filters - Alert Policies page

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

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.

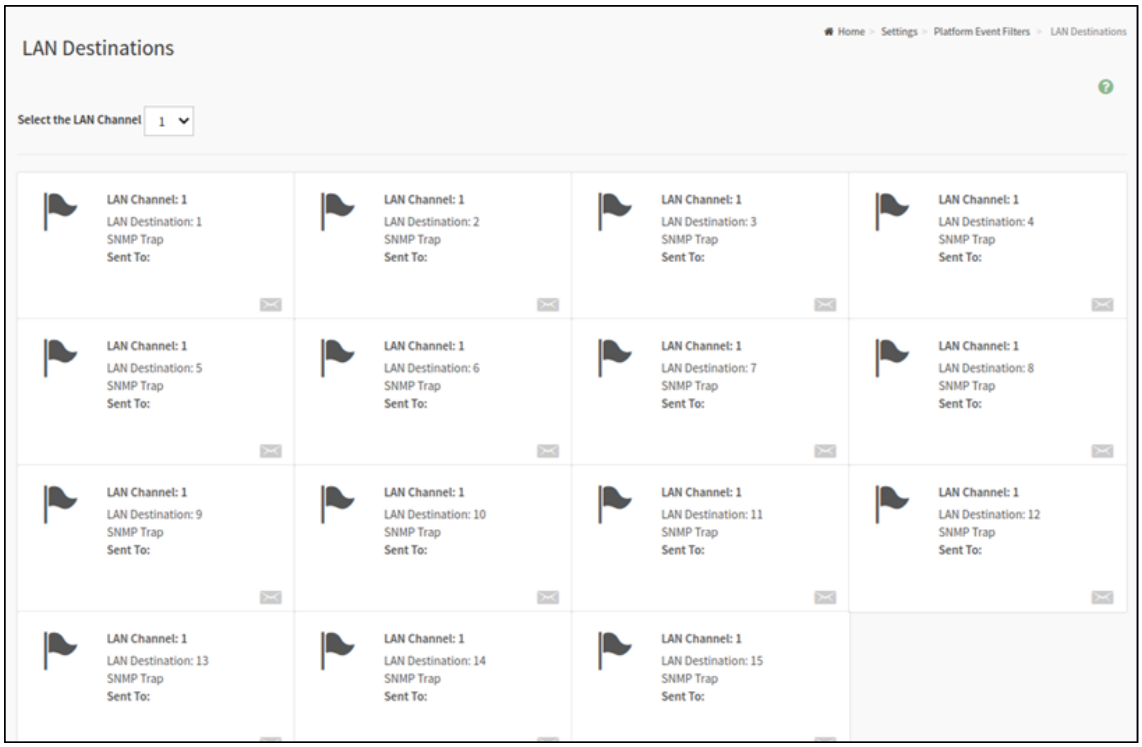
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

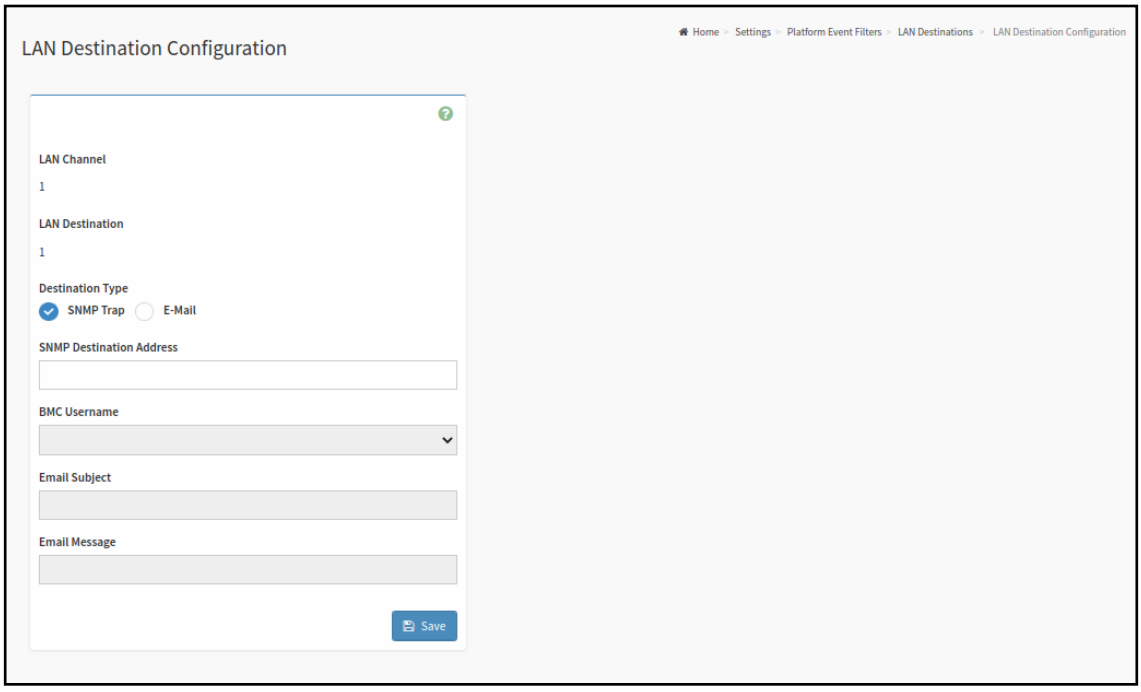
7.4.3 LAN Destinations

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



Platform Event Filters LAN Destinations

Select the slot and click on the empty slot to open the
LAN Destination Configuration page as shown in the screenshot below.



Add LAN Destination entry Page

The fields of Platform Event Filters – LAN Destinations are explained below.

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 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.

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.

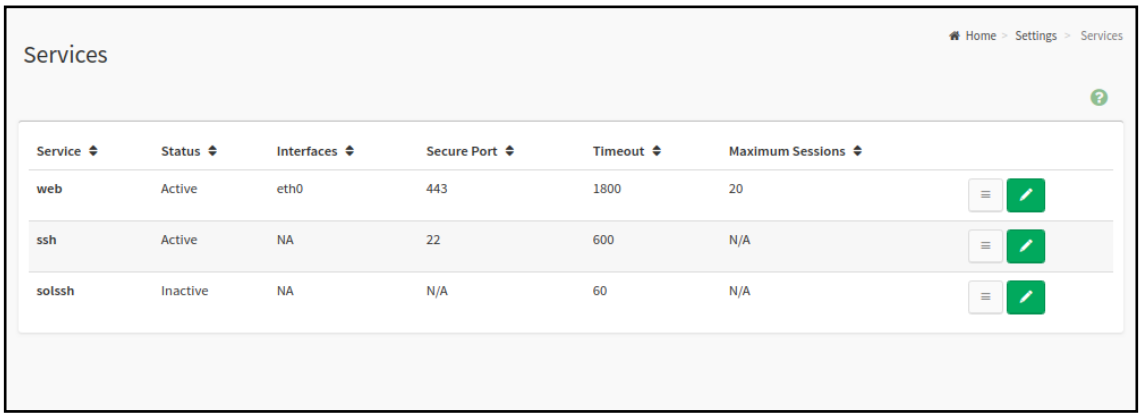
Click Message icon ( ) to send sample alert to configured destination.

> **NOTE**
> Test alert can be sent only with enabled SMTP configuration. SMTP support can be enabled under Settings→SMTP Settings.

7.5 Service

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

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



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

- Web default port is 443
- SSH default port is 22

> **NOTE**
> SOLSSH will not support secure port.

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.
> - SSH timeout value ranges from 60 to 1800 seconds.

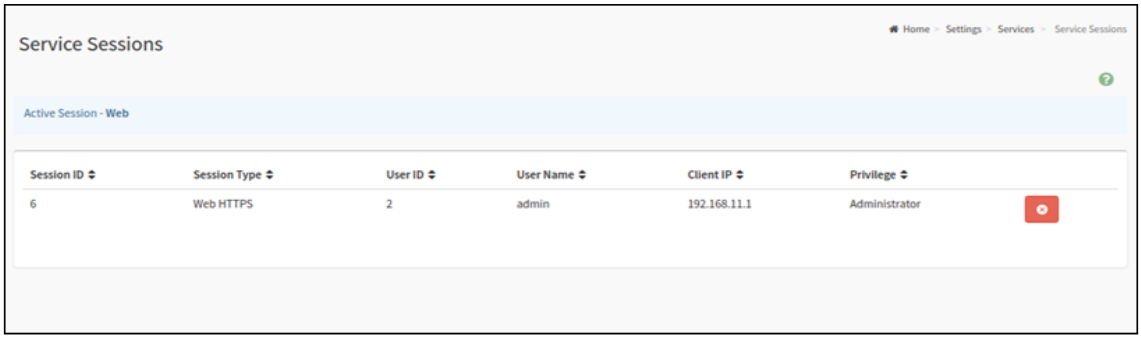
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

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

To view the Active Sessions:

Procedure:

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



Service Session page

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

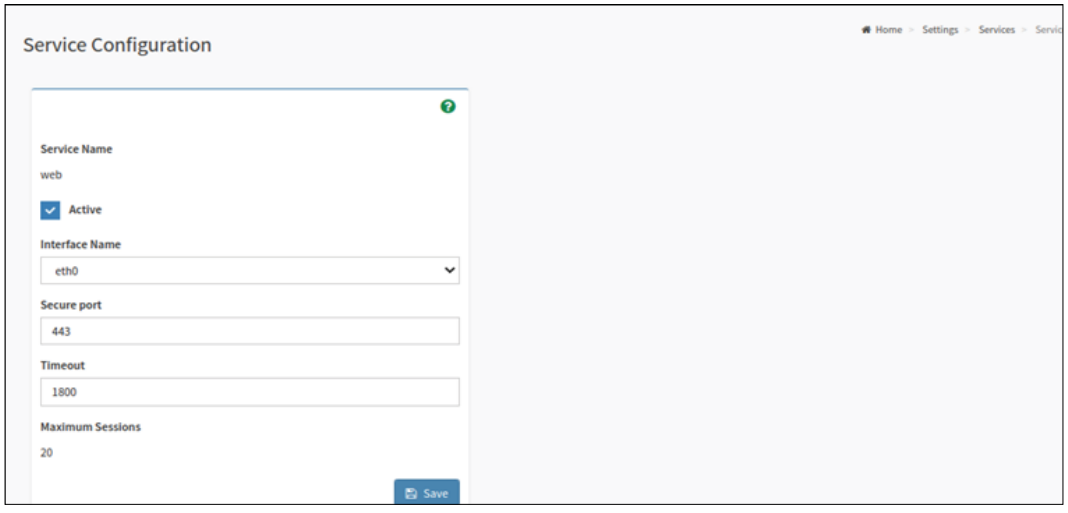
To modify the existing services:

Procedure

1. Select a slot and click Edit icon ( ) to modify the configuration of the service.

> **NOTE**
> Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the Service Configuration screen as shown in the screenshot below.



3.. Service Name is a read only field.

4. Activate the Current State by enabling the Active check box.

> **NOTE**
> Interfaces, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Choose any one of the available interfaces from the Interface Name drop-down list.

6. Enter the Secure Port Number in the Secure Port field.

7. Enter the timeout value in the Timeout field.

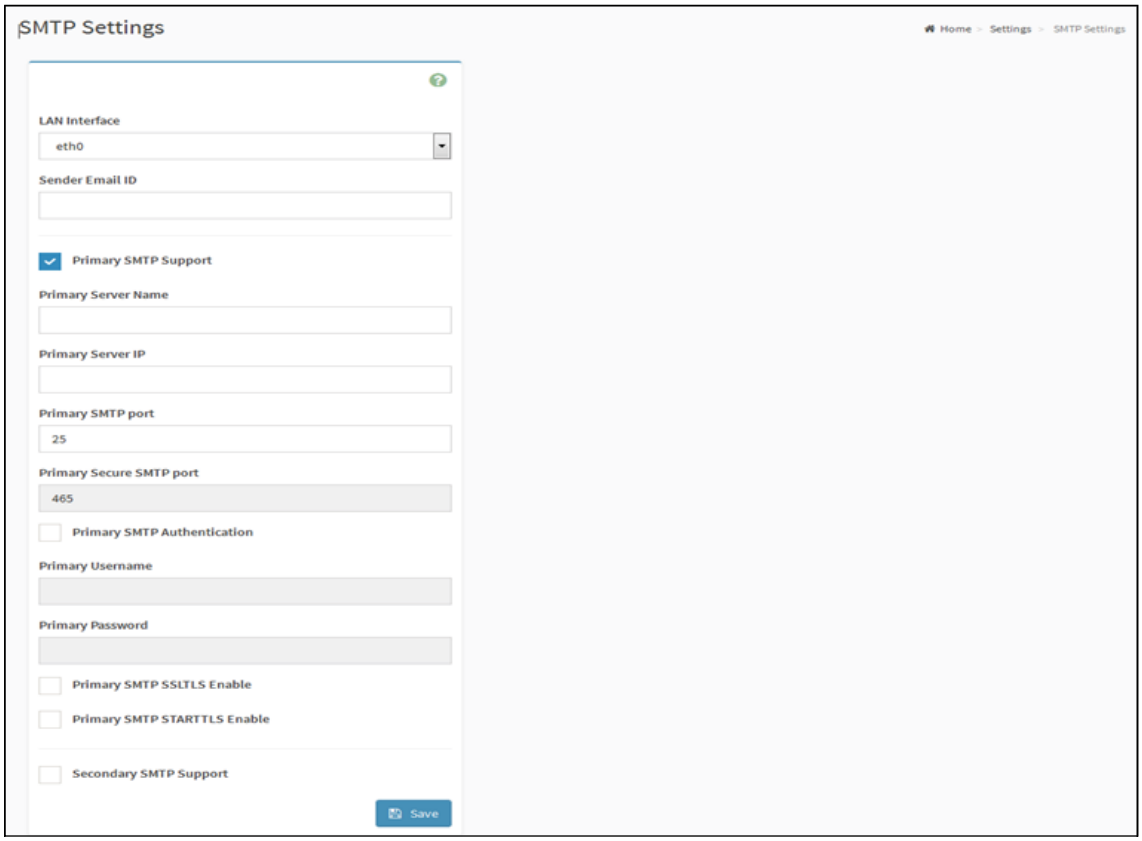
> **NOTE**
> The values in the Maximum Sessions field cannot be modified.

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

7.6 SMTP Settings

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

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



SMTP Settings page

The fields of SMTP Settings page are explained below.

LAN Interface: Displays the list of LAN channels available

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

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

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

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

Primary SMTP Port: To specify the SMTP Normal Port.

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

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

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

NOTE
- IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports IPv4 Address format and IPv6 Address format.

Primary SMTP Authentication: To enable/disable SMTP Authentication.

NOTE
SMTP Server Authentication Types supported are:
- CRAM-MD5
- LOGIN
- PLAIN

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

Primary Username: Enter username to access SMTP Accounts.

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

Primary Password: Enter password for the SMTP User Account.

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

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

- **Upload SMTP CA Certificate File**: File that contains the certificate of the trusted CA certs. CACERT key file should be of pem type.
- **Upload SMTP Certificate File**: Client certificate filename. CERT key file should be of pem type.
- **Upload SMTP Private Key**: Client private key filename. SMTP key file should be of pem type.

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

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

NOTE
Options of Secondary SMTP Support are same as Primary SMTP Support.

Save: To save the new SMTP server configuration.

7.7 System Firewall

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

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

System Firewall page

7.7.1 General Firewall Settings

Click Settings → Firewall → General Firewall Settings from the menu bar. A sample screenshot of General Firewall Settings page is shown below.

General Firewall Settings page

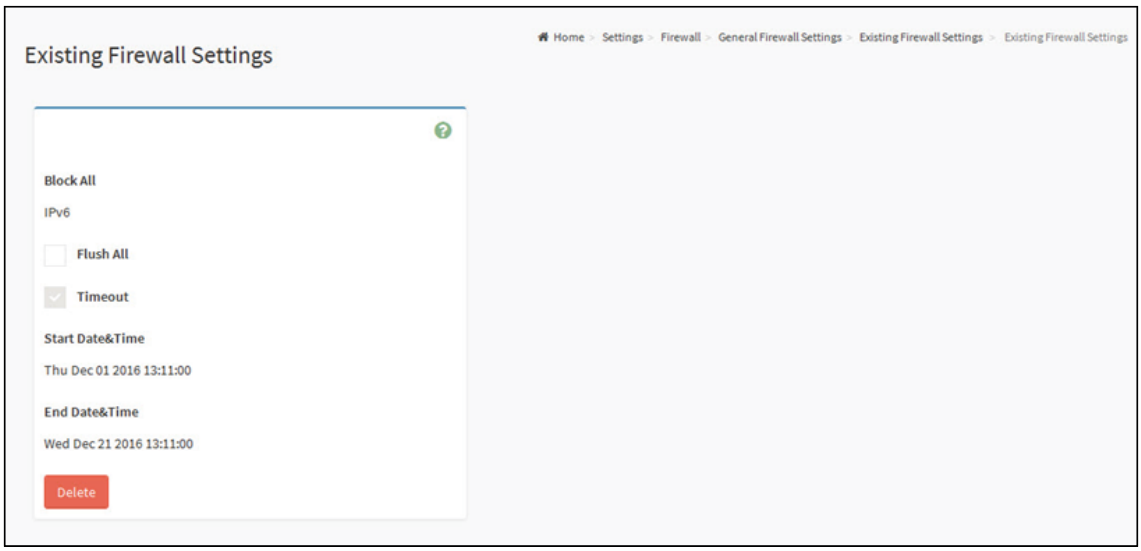
The fields of Firewall Settings tab are explained below.

Existing Firewall Settings

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

Procedure to Add Firewall settings

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

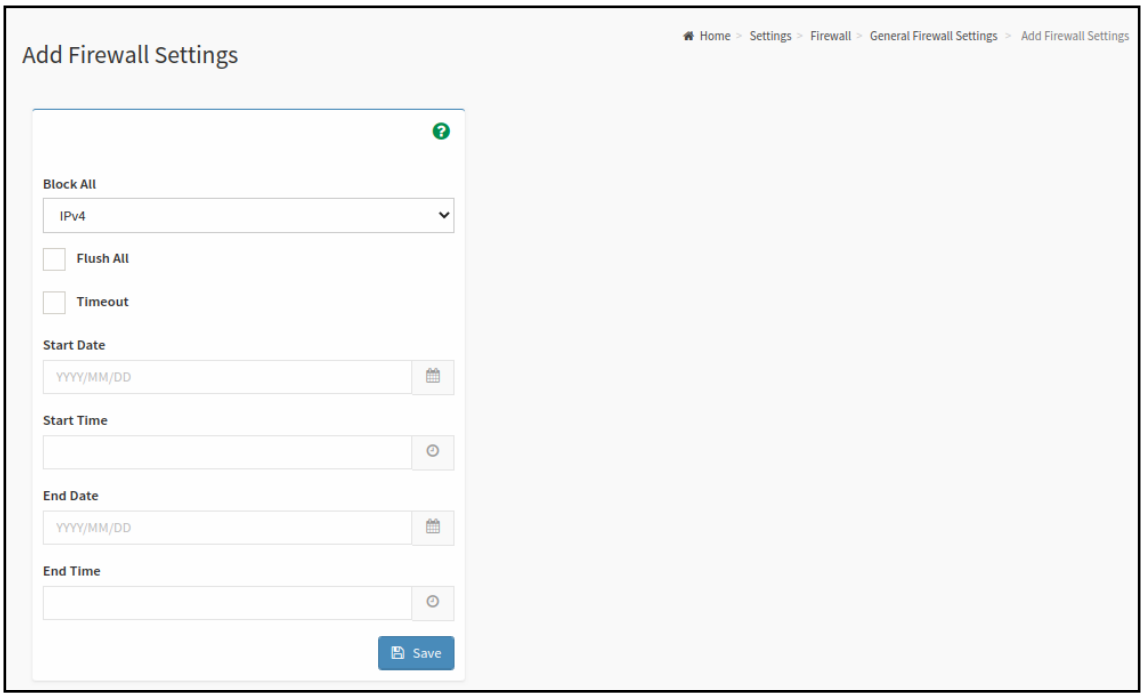


Existing Firewall Settings page

- **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 page

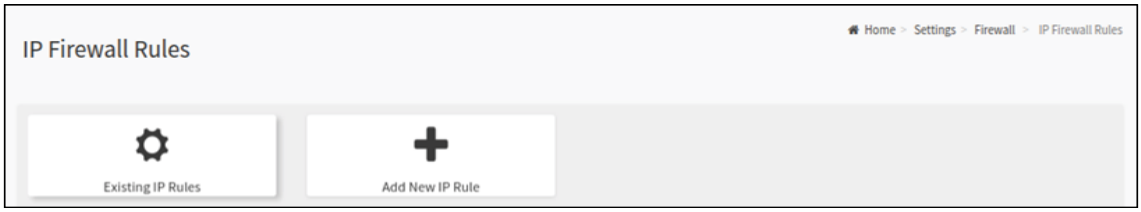
2. Select Block All to block all the incoming IP's and Port's.
3. Select Flush All to flush all the system firewall rules.
4. Select Timeout to enable or disable firewall rules with timeout.
5. Enter Start Time to start the respective firewall rule effect from this time.
6. Enter End Time to end the respective firewall rule effect from this time.

> **NOTE**
> The time should be in the dd-mm-yy:hh-mm formart.

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

7.7.2 IP Address Firewall Rules

Click Settings → Firewall → IP Address Firewall Rules from the menu bar. A sample screenshot of IP Address Firewall Rules page is shown below.

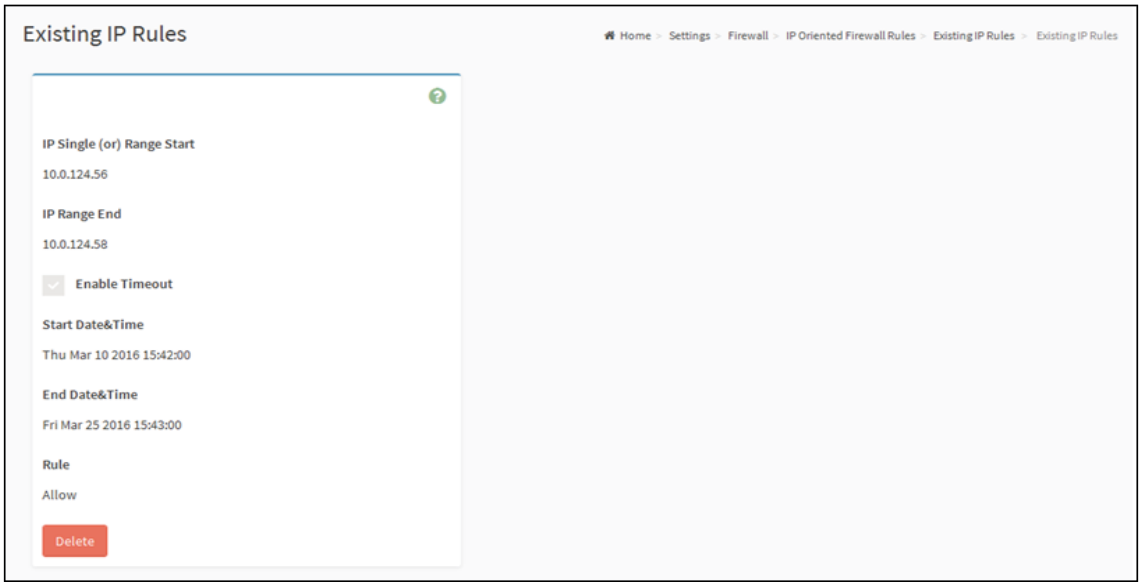


IP Firewall Rules page

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.



Existing IP Rules page

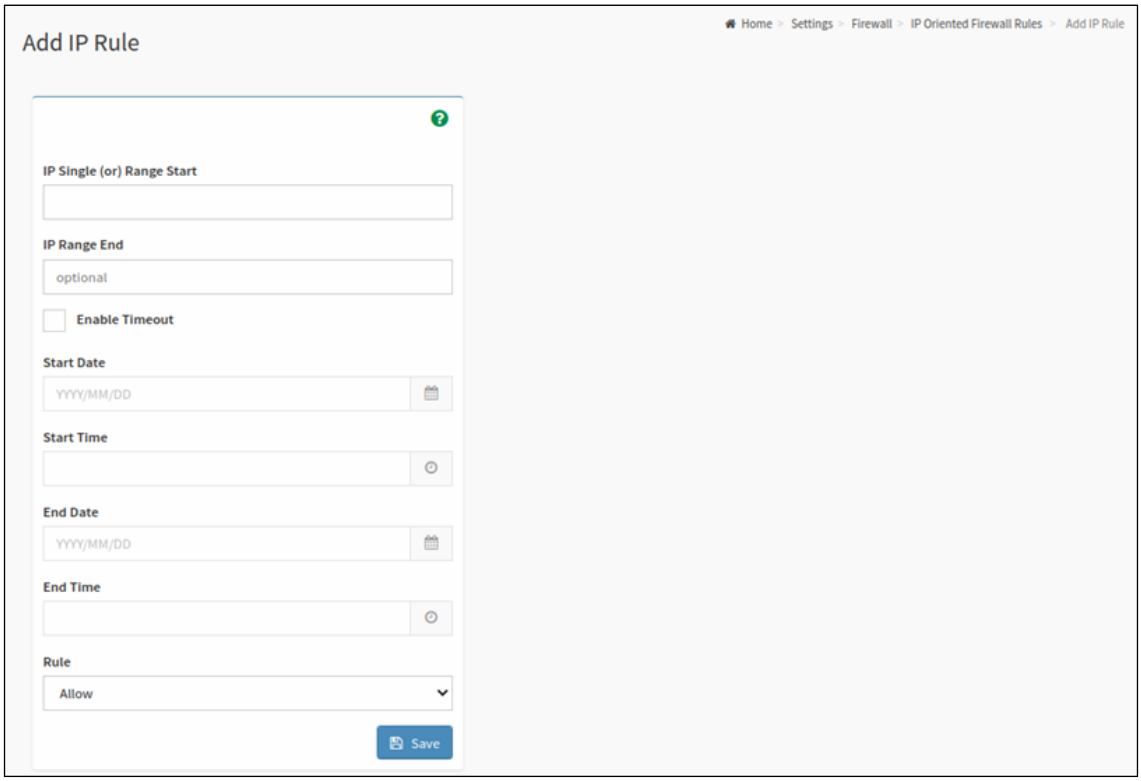
IP Single (or) Range Start: To show the configured Port Address or Range of Ports.
IP Range End: To show the configured Port Address or Range of Ports.
Enable Timeout: To enable/disable Timeout.
Start Date: The respective firewall rule effect will start from this date.
Start Time: The respective firewall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

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

Delete: To delete the selected slot.

Procedure To add an IP address or range of IP addresses,

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



Add IP Rule

2. In the Add new rule for IP page, Enter the IP address and a range of IP addresses in the IP Single or IP Range Start field.

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

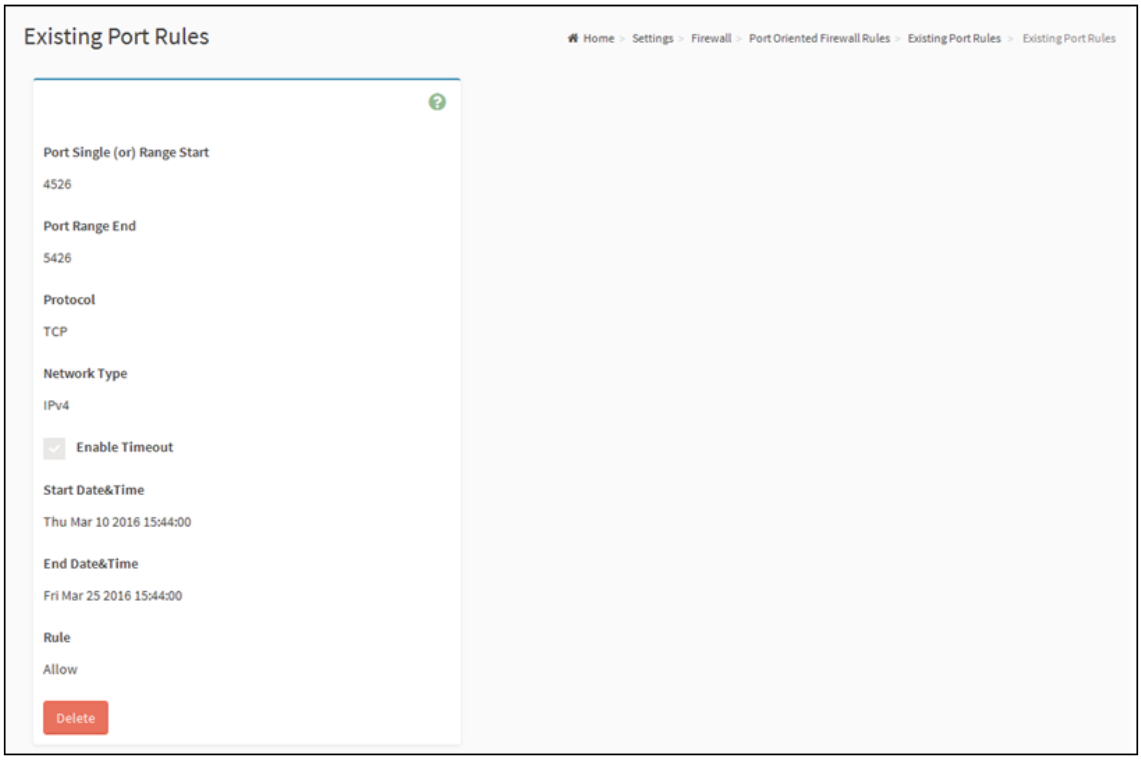
7.7.3 Port Firewall Rules

Click Settings → Firewall → Port Firewall Rules from the menu bar. A sample screenshot of Port Firewall Rules page is shown below.

Port Firewall Rules page

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.



Existing Port Rules page

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

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

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

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

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

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

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

Start Time: The respective firewall rule will start from this time. End Date - The respective firewall rule effect will end on this date. End Time - The respective firewall rule will end at this time.

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

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

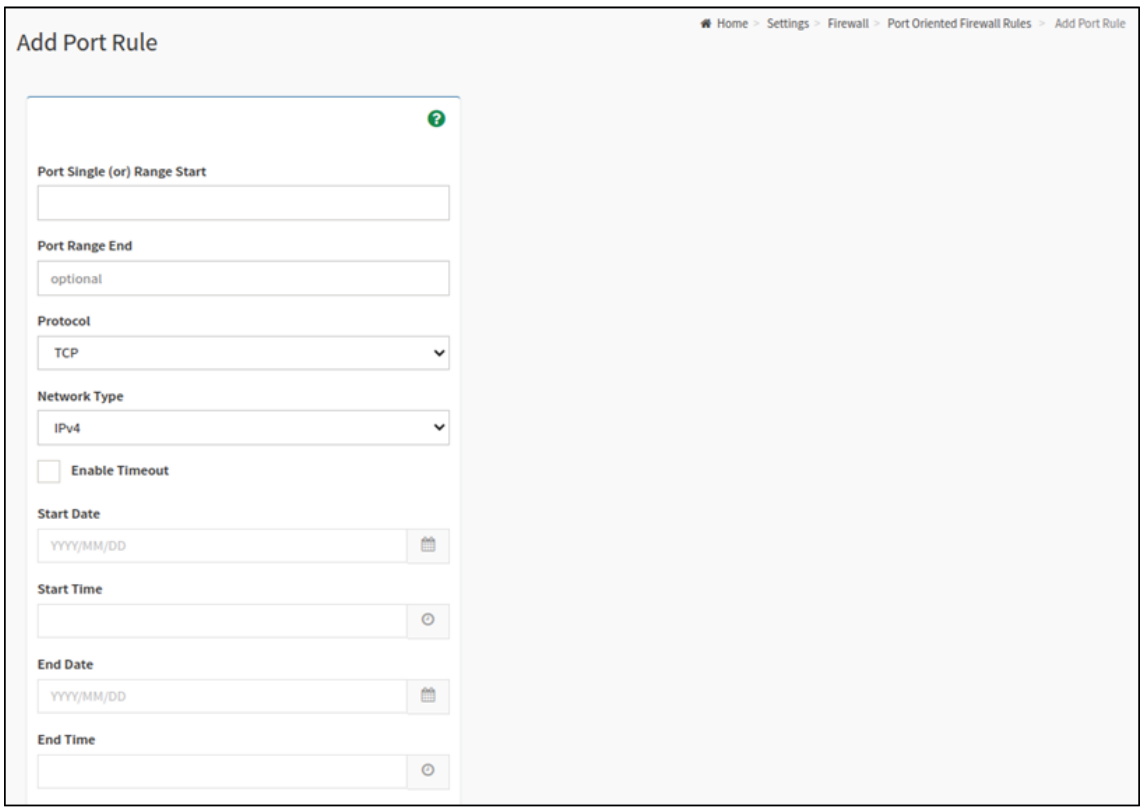
Rule: To indicate Allow or Block status.

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 page

2. In the Add new rule for Port window, enter the port number or a range of port numbers in the Port Single (or) Range Start field.

> **NOTE**
> Port value ranges from 1 to 65535.

3. Enter the end value in the Port Range End field.
4. Select the Protocol to be either TCP or UDP or Bot.
5. Select the Network Type. It may be IPv4 or IPv6 or Both.
6. Select Timeout to enable or disable firewall rules with timeout.
7. Enter Start Time to start the respective firewall rule effect from this time.
8. Enter Start Date to start the respective firewall rule effect from this date.
9. Enter End Date to end the respective firewall rule effect on this date.
10. Enter End Time to end the respective firewall rule effect at this time.

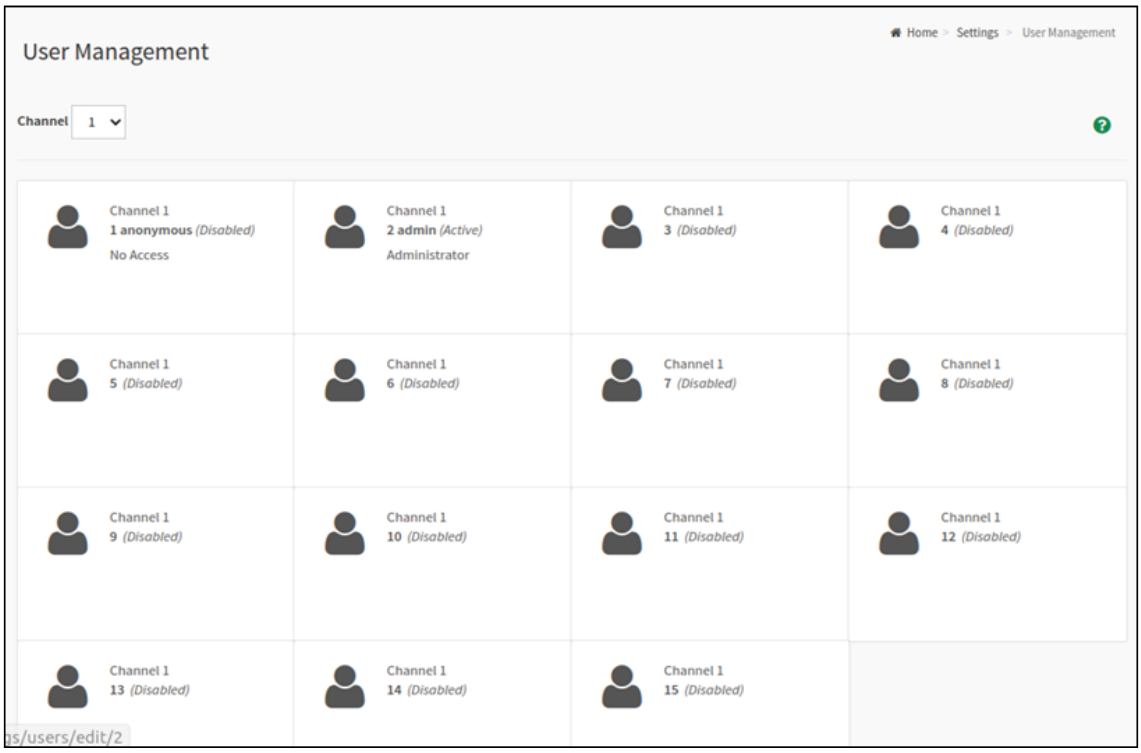
> **NOTE**
> The time should be in the YYYY/MM/DD:hh-mm format.

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

7.8 User Management

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

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



User Management page

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

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

> **NOTE**
> The Free slots are shown as “Disabled” in all columns for the slot.

The fields of User Management page are explained below.

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

User ID: Displays the ID number of the user.

> **NOTE**
> The list contains a maximum of ten users only.

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.

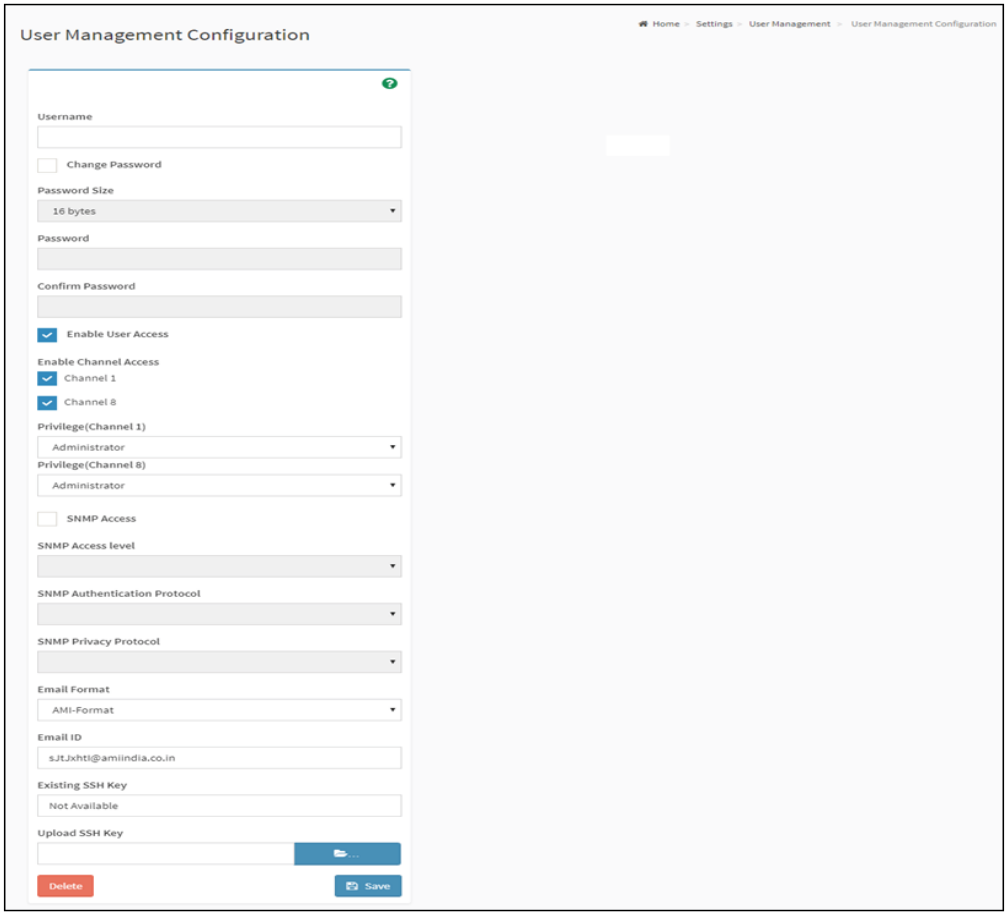
E-mail ID: Displays e-mail address of the user.

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 Management Configuration.



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) 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
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)
04	EOT (end of transmission)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal tab)
0A	LF '\n' (new line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	DC2 (device control 2)
13	DC3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
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.
8. Check the SNMP Access check box to enable SNMP access for the user.
9. 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.
10. 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.

11. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.
12. In the Email ID field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

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

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

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

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

To Modify User

1. To modify the existing user, click on the active user tab.
2. Check Change Password, if you wish to change the existing Password.
3. Follow the steps (3 to 15) of Procedure to add a new User.
4. Click Save to save the changes and return to the users list.
5. Click Save to save the changes and return to the users list.

IMPORTANT NOTE

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

- sysadmin
- daemon
- sshd
- ntp
- root

7.9 Power Restore Policy

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

Power Restore Policy page

After an unexpected power failure, the state of the system power supply when the power supply is restored.

Always off: Keep power off.

Previous: Restore to the previous state

Always on: Keep power on.

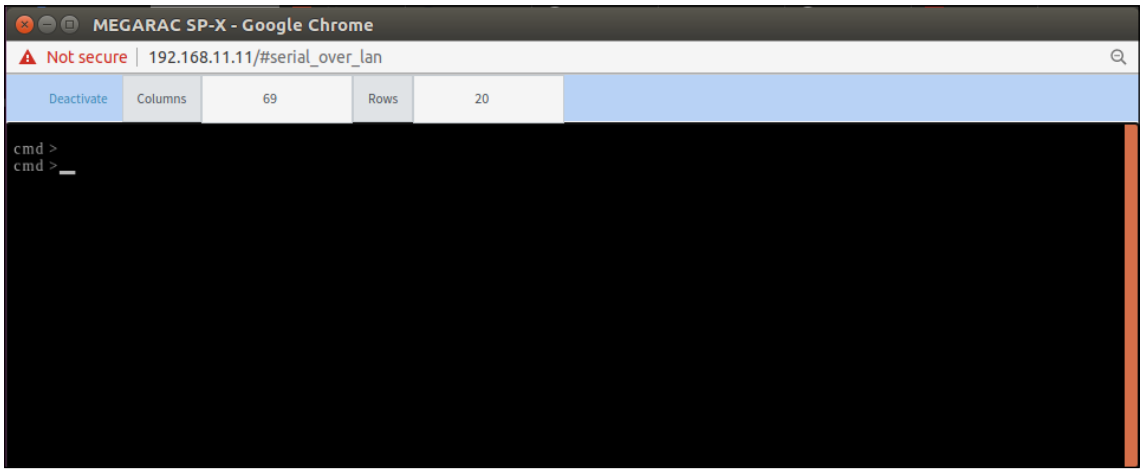
Chapter 8. Remote Control

The Remote Control page consists of the following options. A sample screenshot is displayed below.

Remote Control page

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

Open the Remote Control page, click Activate. A sample screenshot of the Remote serial over lan page is shown below.



Serial over lan page

Chapter 9. Chassis Identify

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

Chassis Identify page

The various options of Chassis Identify LED Control are given below.

Chassis Identify Off: Turn off the chassis identify LED.

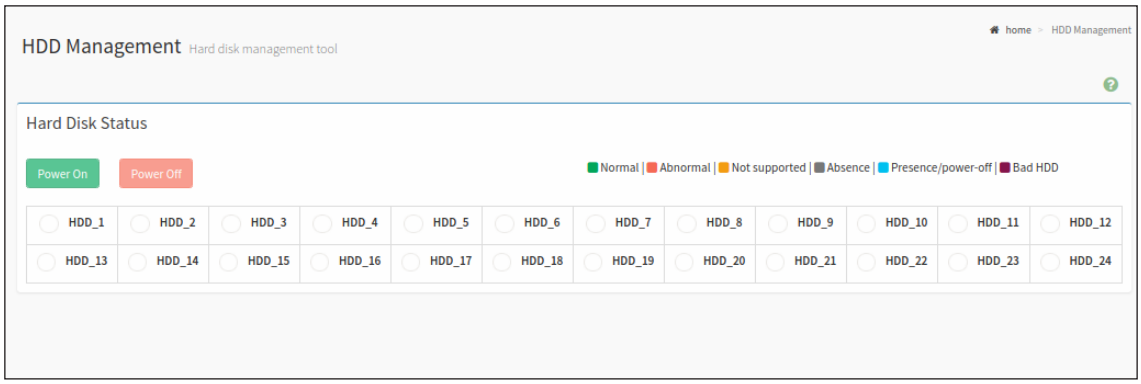
Chassis Identify On: Turn on the chassis identify LED.

Chapter 10. HDD Management

This page allows you to view and control the hard disk drivers .

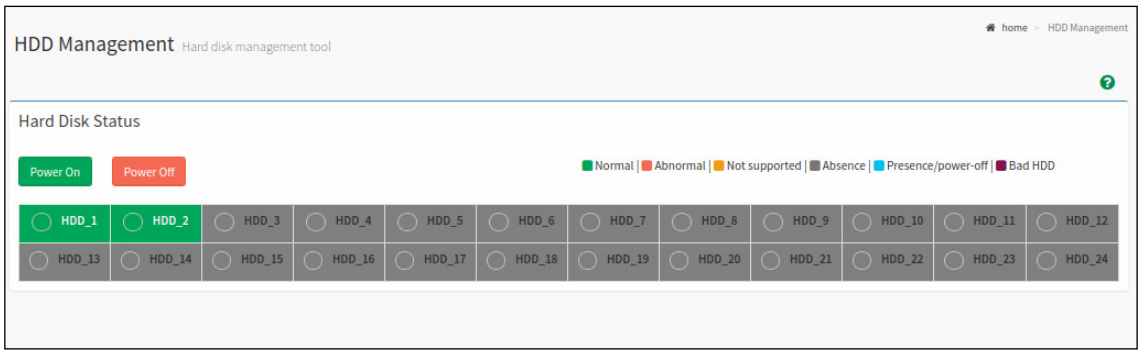
To open HDD Management, click HDD Management from the menu bar. A sample screenshot of HDD Management page is shown below.

When host is currently off



HDD Management page

When host is currently on



HDD Management page

Each hard disk driver will display a different color, each color represents a different st ate including normal, abnormal and absence, etc.

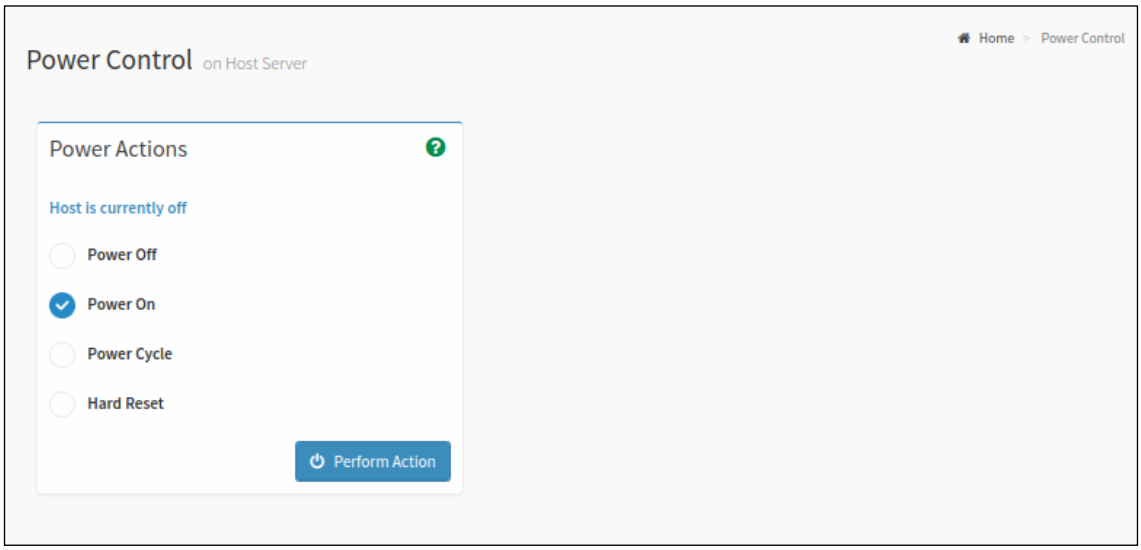
Power on: To power on the hard disk driver.

Power off: To power off the hard disk driver.

Chapter 11. 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 page

The various options of Power Control are given below.

Power Off: To immediately power off the server.

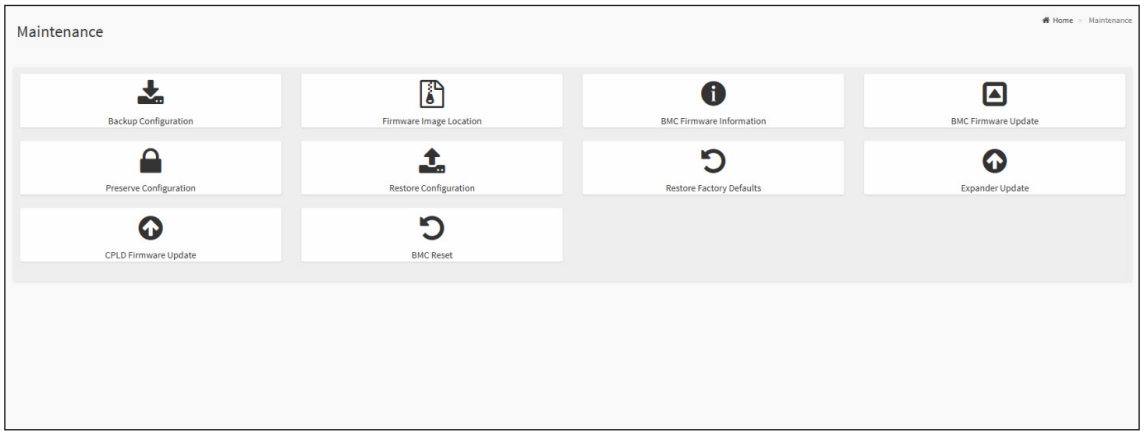
Power On: To power on the server.

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).

Chapter 12. Maintenance Group

To open Power Control, click Maintenance from the menu bar. A sample screenshot of Maintenance page is displayed below.



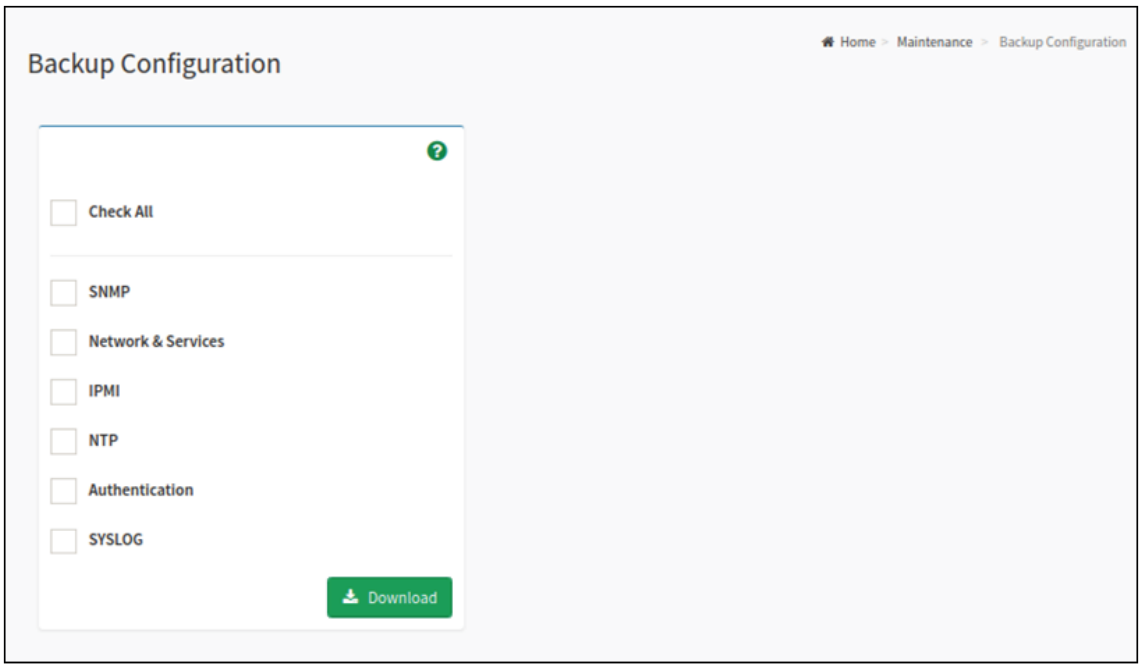
Maintenance page

A detailed description is given below.

12.1 Backup Configuration

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 page

The various fields of Backup Configuration page are given below.

Check All: To select all the configuration list.

Download: 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. User has to set password again after restoring configuration by using default user in case of login failure.

Procedure for Backup Configuration:

1. Click Check All to 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.

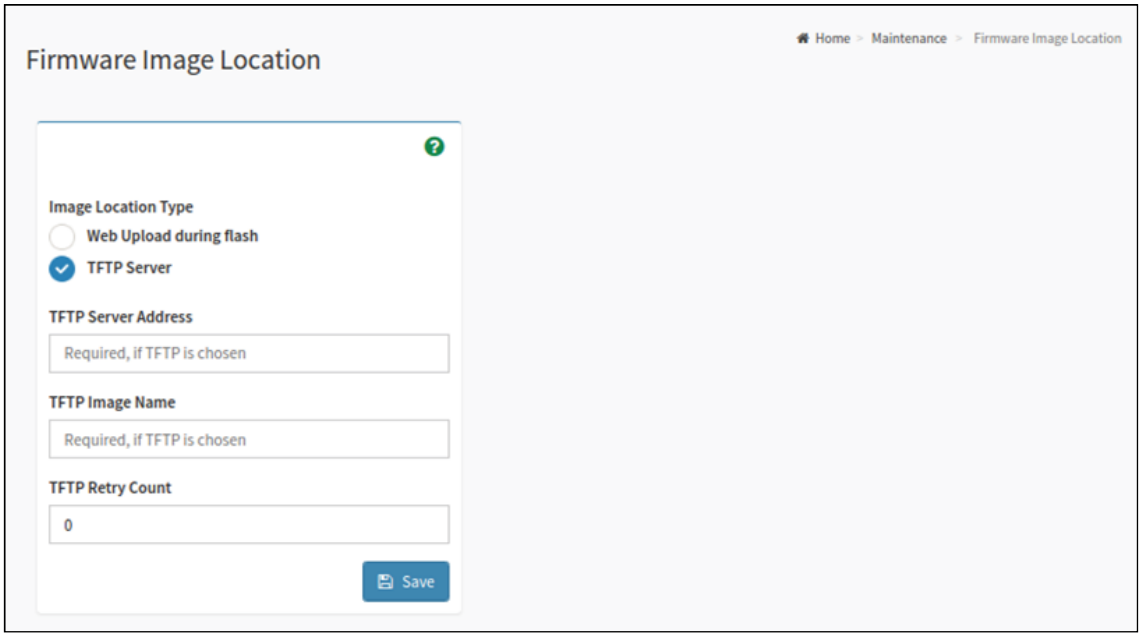
> **NOTE**
> Network configurations are inter-related to IPMI, and hence by default IPMI configurations will be selected automatically when you select “Network and Services” to be backed up.

2. Click Download Config to save the backup file to the client system.

12.2 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.

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

TFTP 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 Image Name: Full Source path with filename of the firmware image is stored on TFTP Server.

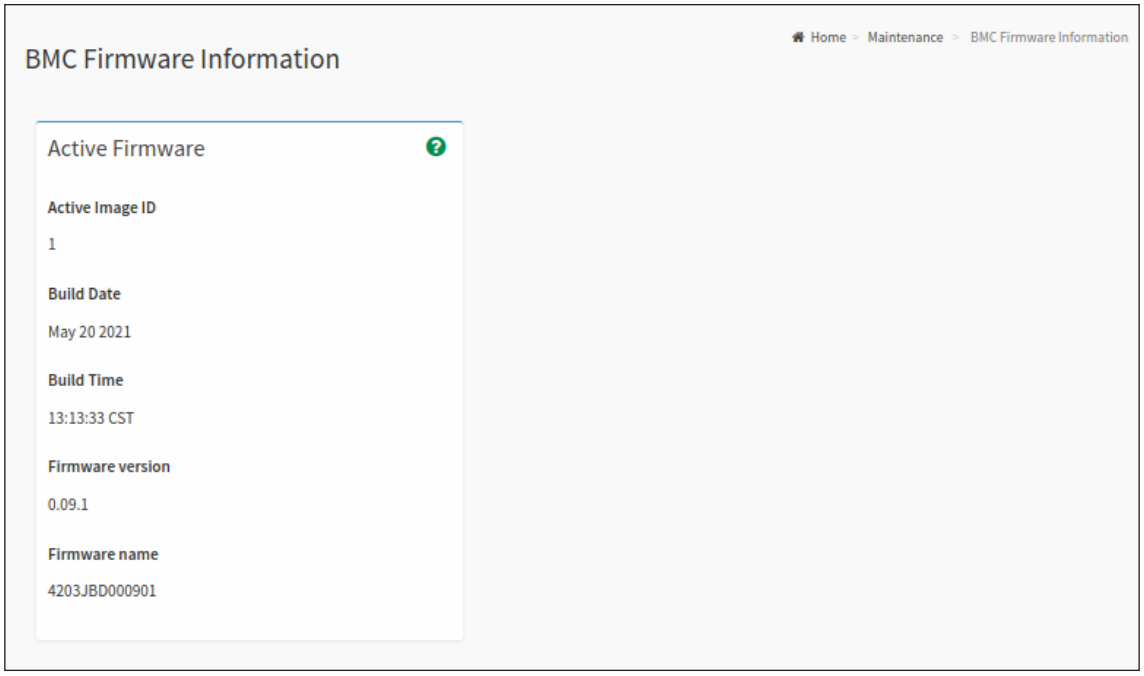
TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

12.3 BMC Firmware Information

This page shows the BMC Firmware Information.

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



BMC Firmware Information page

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

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

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

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

Firmware version: Describes the Firmware version of the active BMC

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

12.4 BMC Firmware Update

This wizard takes you through the process of BMC 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.

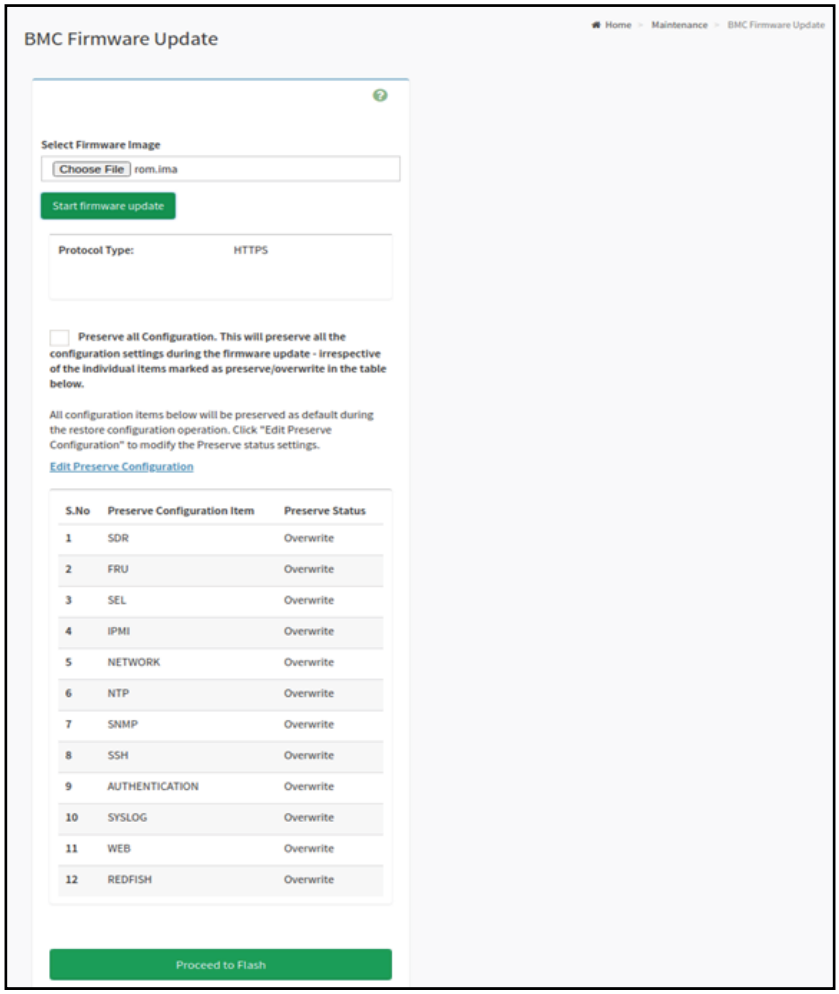
NOTE
Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

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 BMC must be reset. This means that you must close the Internet browser and log back onto the BMC 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. To configure, choose 'Firmware Image Location' under Maintenance. To open Firmware Update page, click Maintenance → BMC Firmware Update from the menu bar. A sample screenshot of BMC Firmware Update Page is shown below.



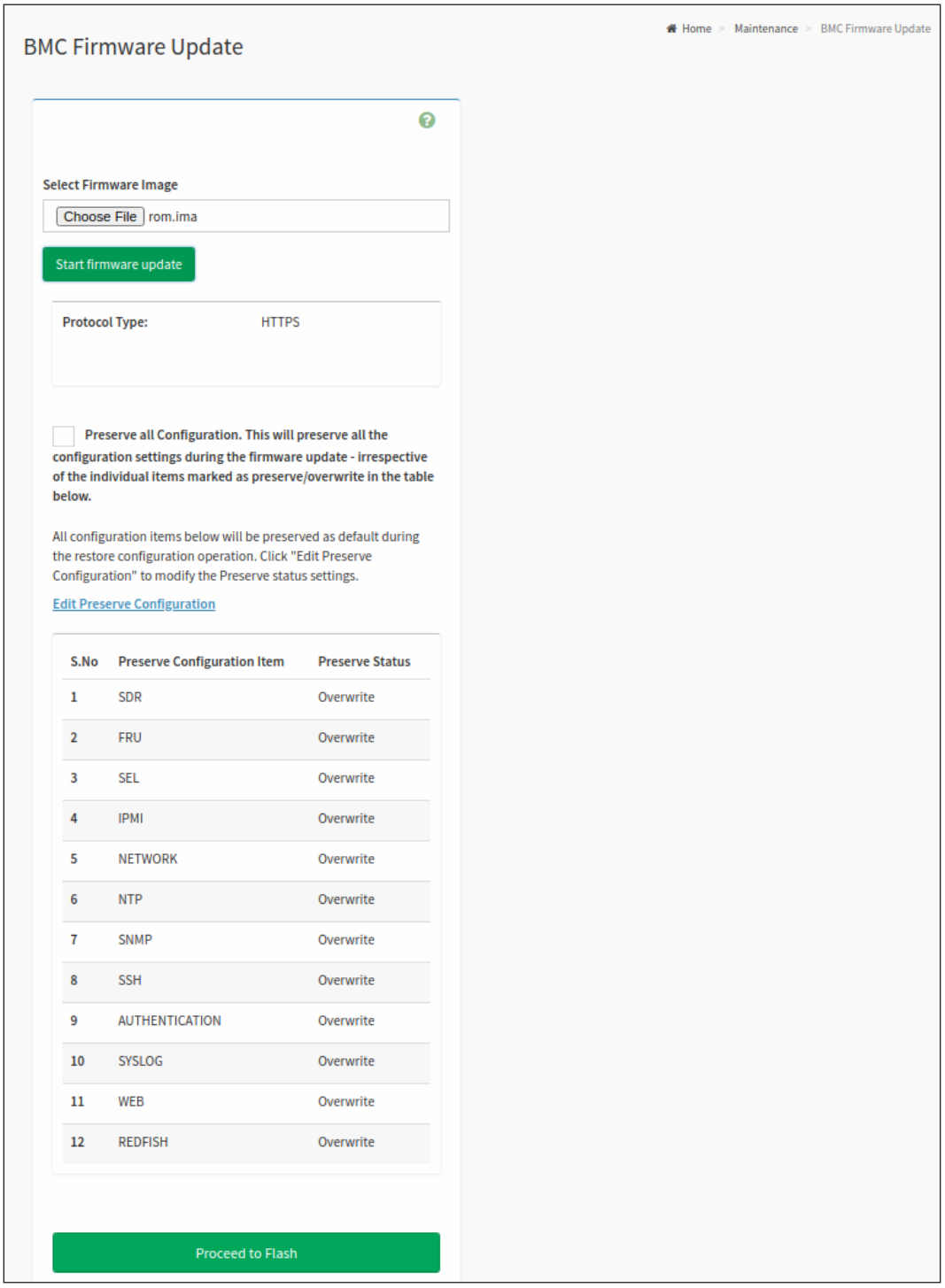
BMC Firmware Update page

Procedure

1. Click Choose File 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. to load the Firmware Update information. A sample screenshot is displayed below.

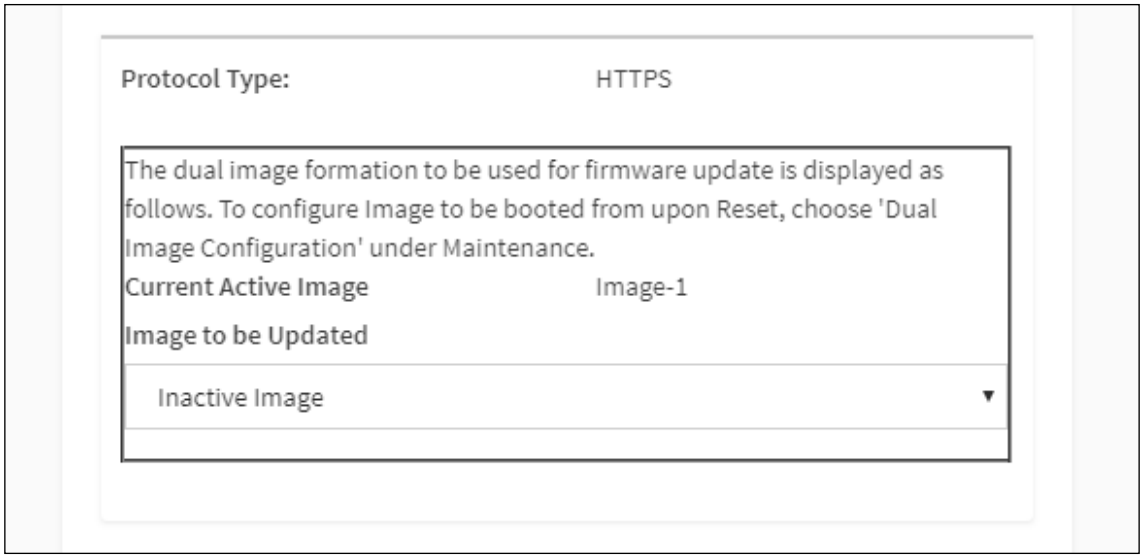


BMC Firmware Update page

NOTE
Sign Image Public Key is feature based option. If encrypted Signimage feature is enabled, then support to Upload a public.pem key info option will be available.

NOTE
Dual Firmware Update
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.



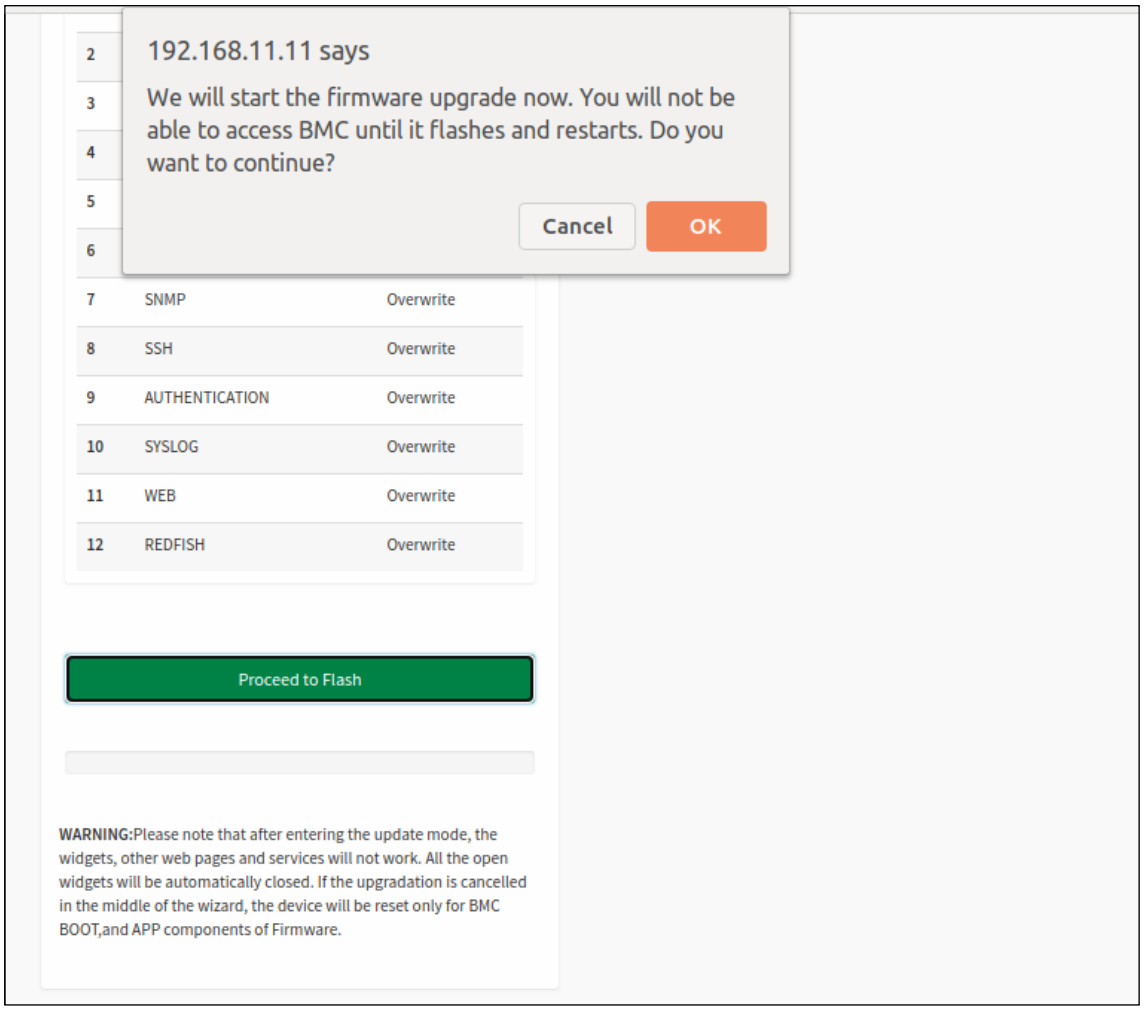
Dual Image Selected page

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

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.

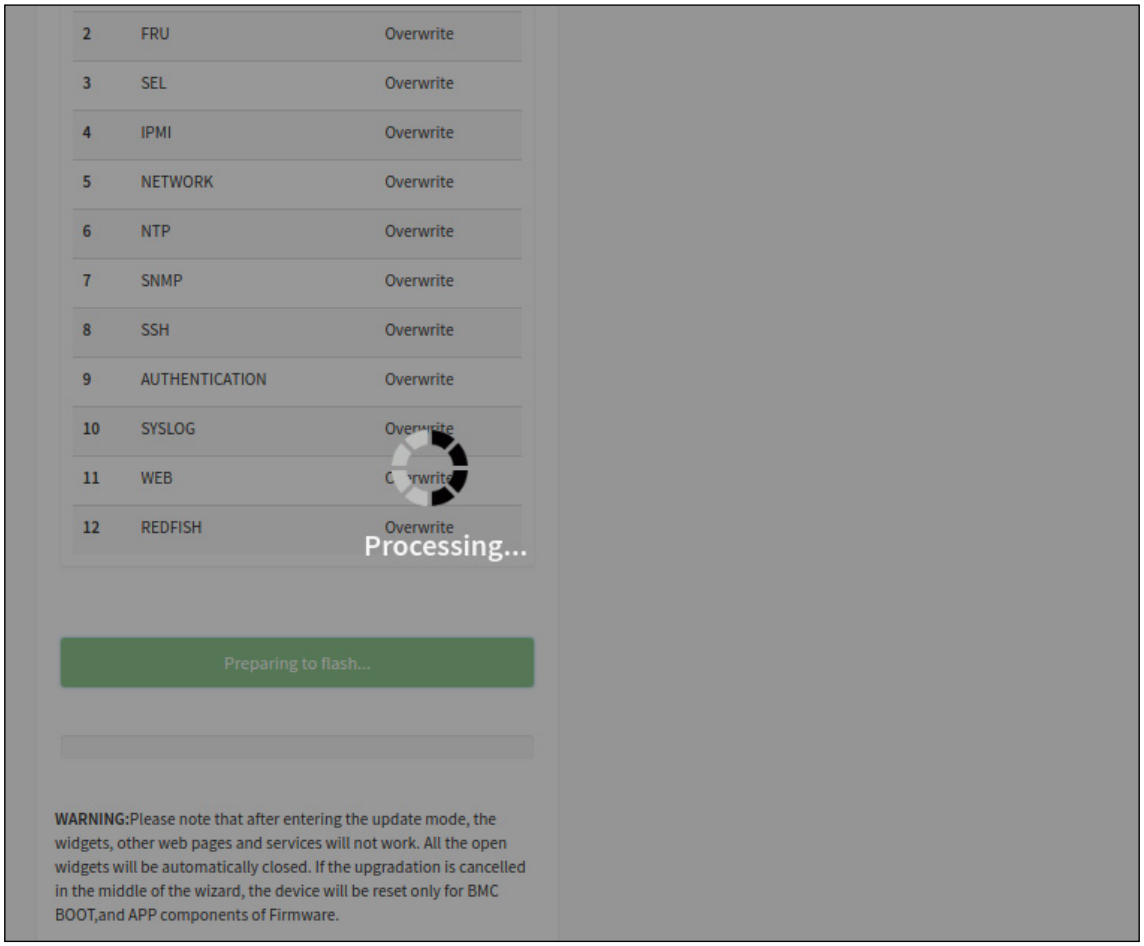
4. Click Proceed to Flash, it will prompt you with the warning message. Click Ok to start the Firmware update.



Firmware Update page

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 page

   d. Verifying Firmware Image

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

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

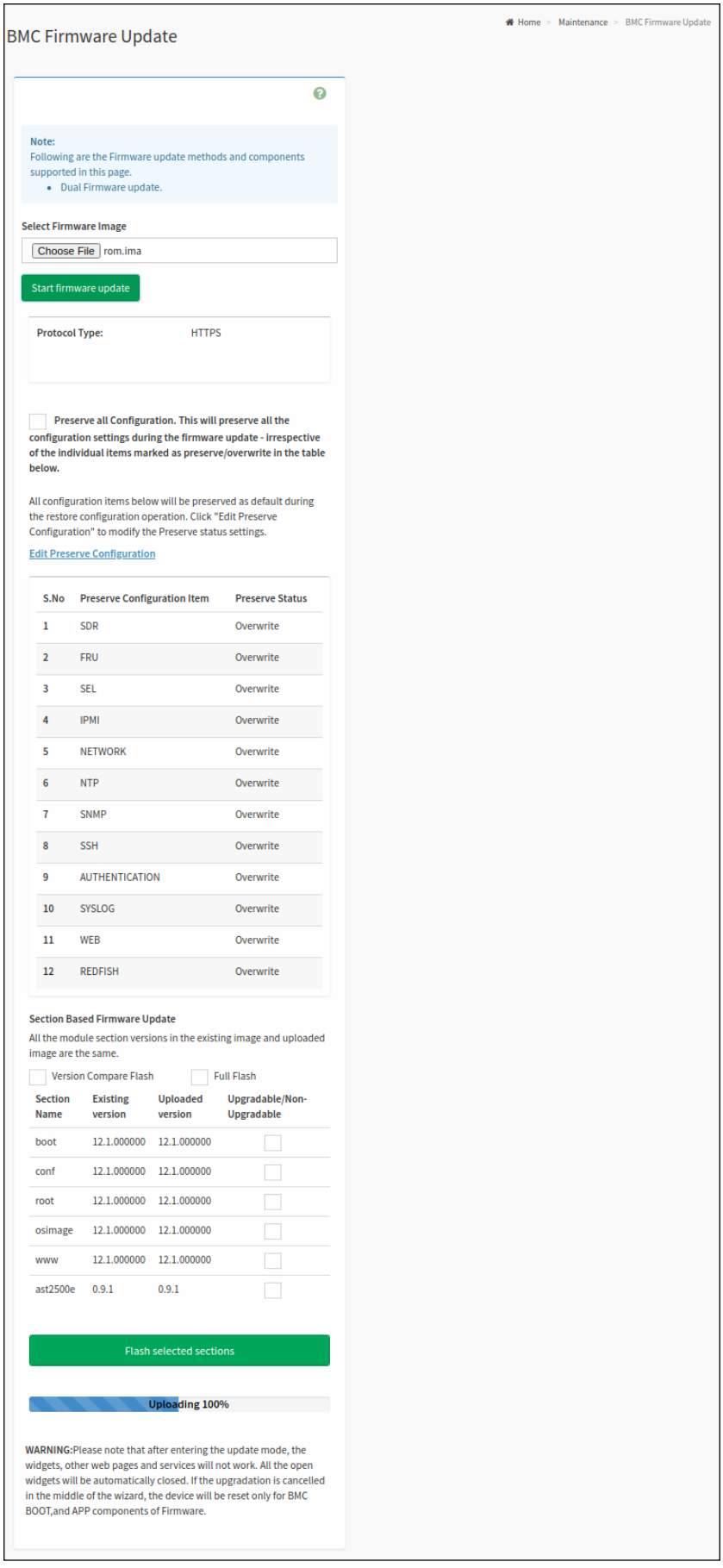
      If you select Version Compare Flash option from web, the current and uploaded module versions, FMHlocation, size will be compared.

      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 differing, those modules will be flashed.

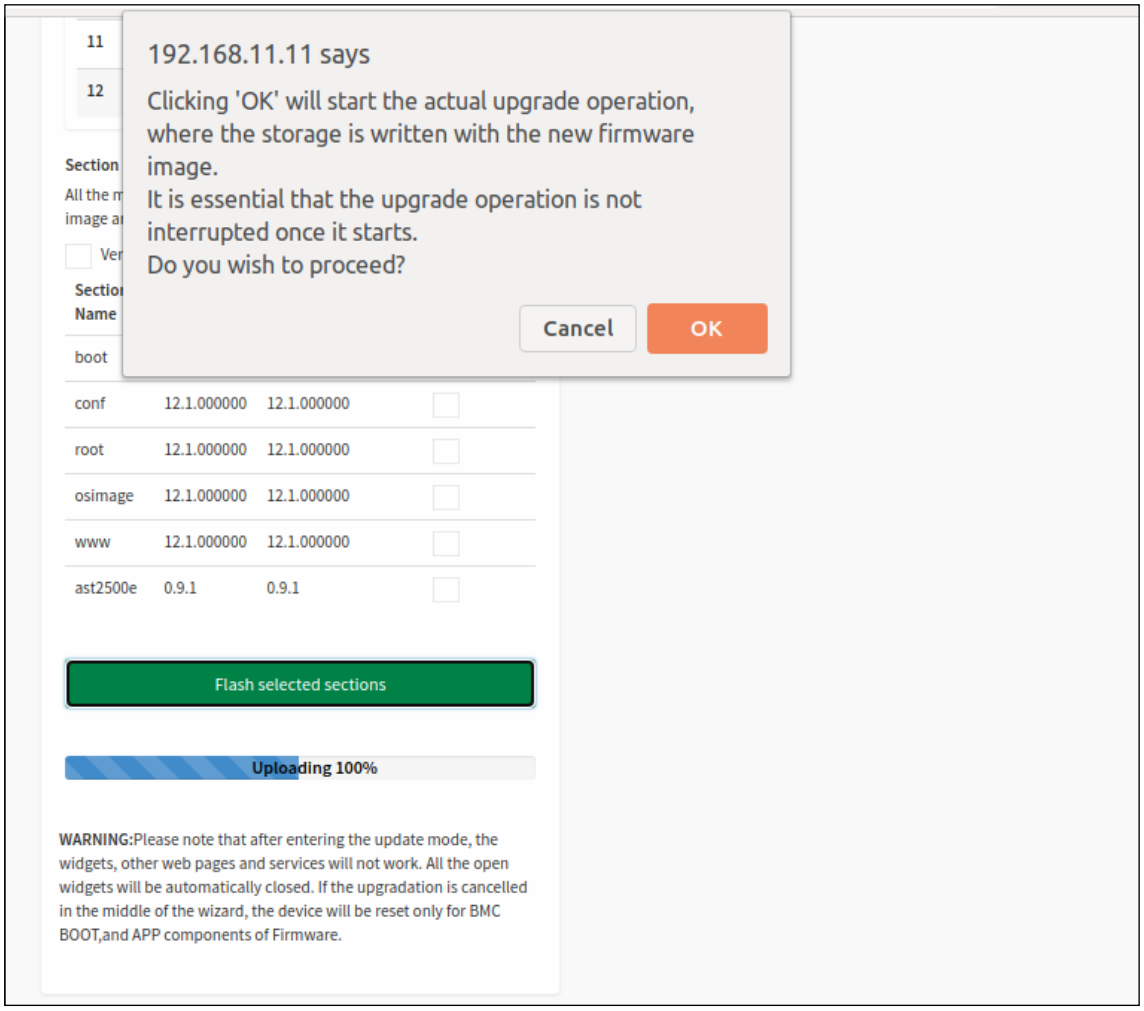
NOTE
Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.



Section Based Firmware Flashing page

e. Flashing Firmware Image

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



Firmware Update page

NOTE

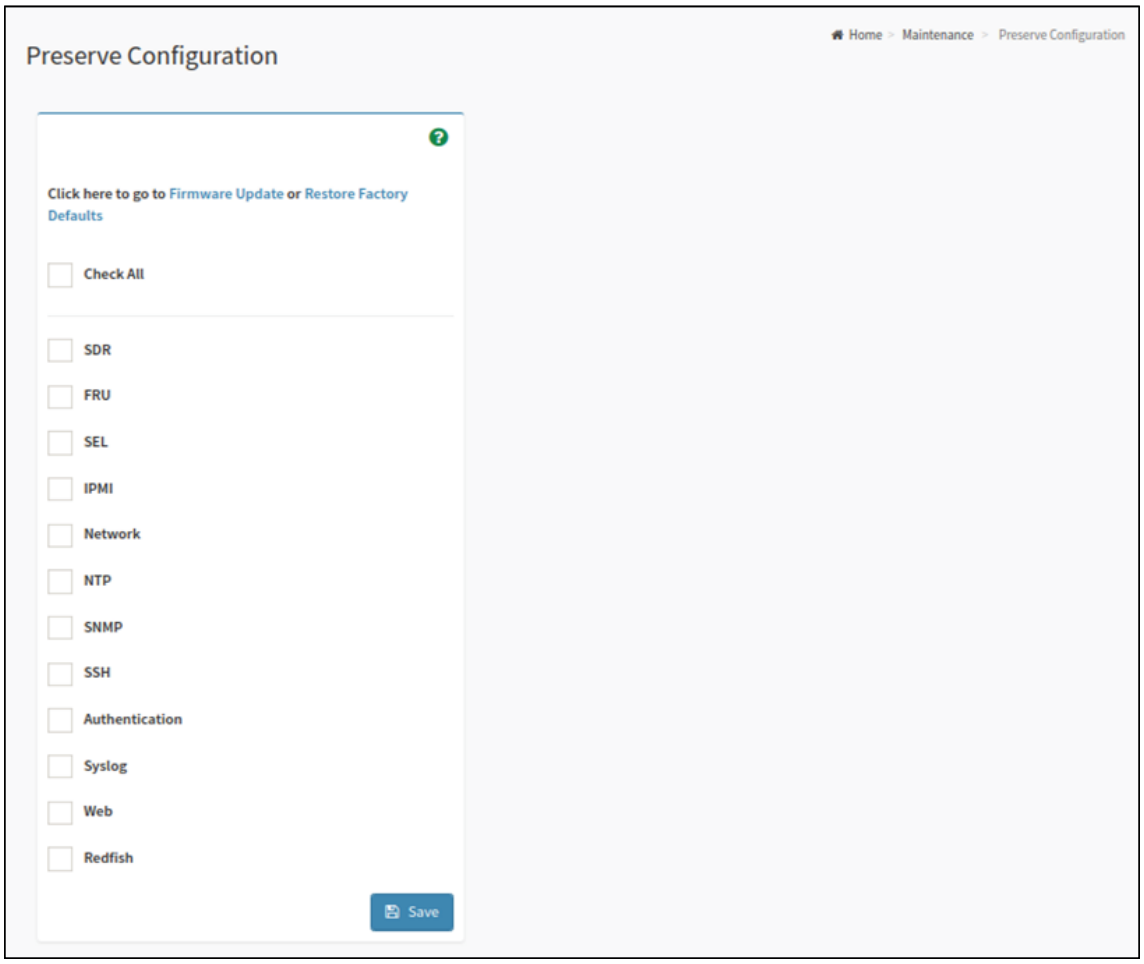
The Firmware Update pa ge will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update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

12.5 Preserve Configuration

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

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

> **NOTE**
> You can navigate to the Firmware Update page and Restore Factory Defaults by clicking the respective links.



Preserve Configuration page

The various fields of Preserve Configuration are as follows.

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

Check All: To check the entire configuration list.

Save: To save any changes made.

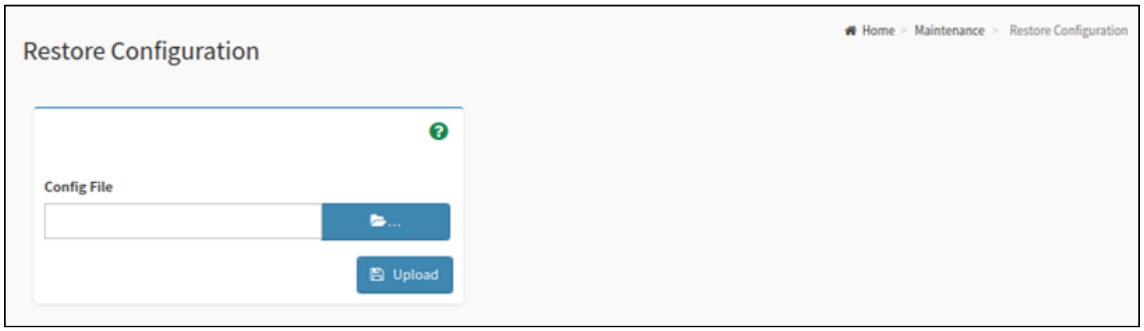
> **NOTE**
> This configuration is used by Restore Factory Defaults process.

- **SDR**: The sensor data record information will be preserved.
- **FRU**: The fru data will be preserved.
- **SEL**: The system event logs that are being logged by the IPMI will be preserved.
- **IPMI**: Preserve the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.
- **Network**: To save network settings related with IPMI (LAN IP or DHCP configuration), selecting “IPMI” will automatically select the another option “Network” and it’s vice versa.
  After restore configuration, the Network Configuration will be preserved successfully.
- **NTP**: Automatic or manual network type protocol and time settings will be preserved.
- **SNMP**: The SNMP user configurations and the SNMP users privilege levels will be preserved.
- **SSH**: SSH configuration will be preserved.
- **Authentication**: Authentication related documents and settings will be preserved.
- **Syslog**: The system log configuration details will be preserved.
- **Web**: The firmware image location details will be preserved.
- **Redfish**: Redfish's files and settings will be preserved.

12.6 Restore Configuration

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

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



Restore Configuration page

The various fields Restore Configuration page are given below.

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

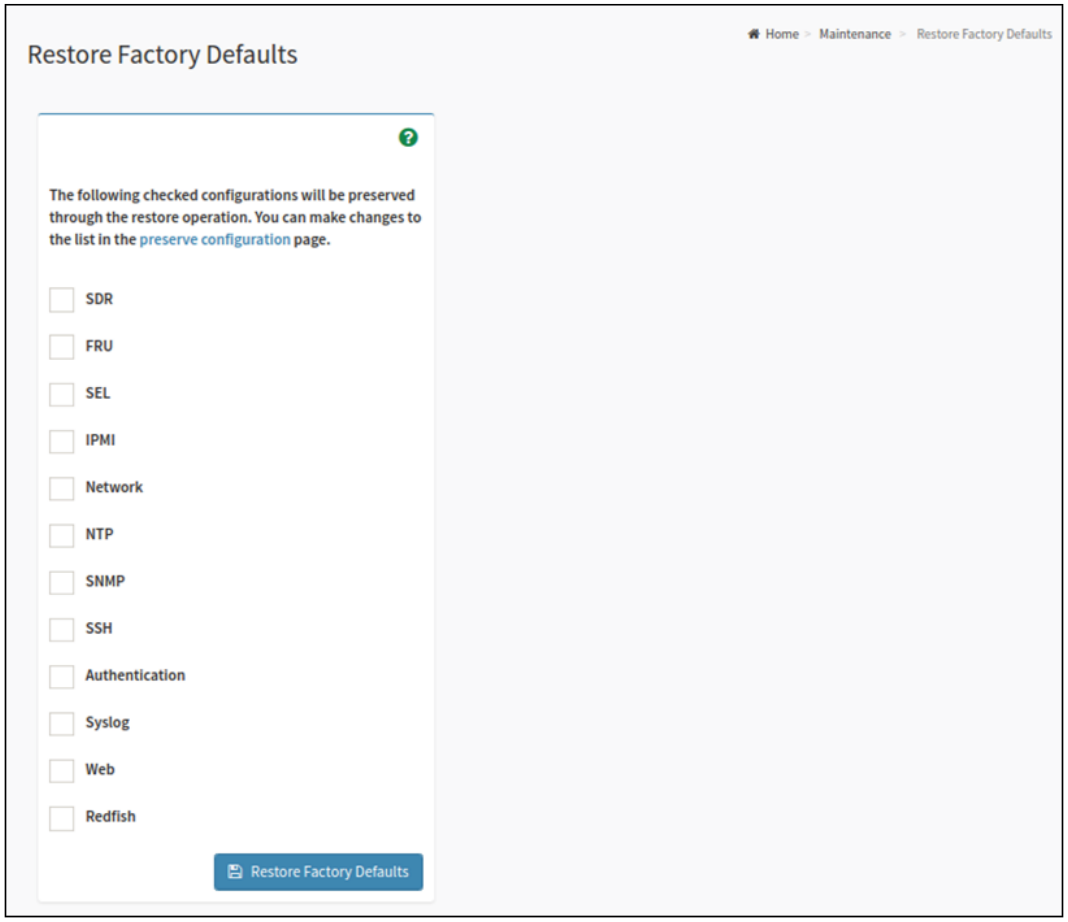
Upload: To upload the backup file to restore the backup files.

12.7 Restore Factory Default

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

> **NOTE**
> *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 page

Procedure

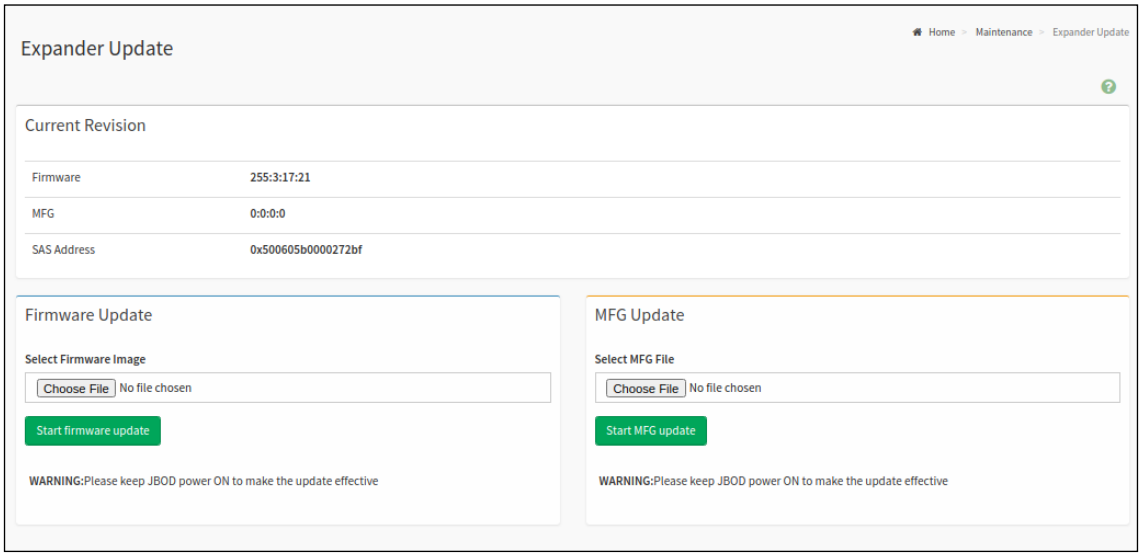
1. Click Preserve Configuration to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Factory Defaults to restore the factory defaults of the device firmware.

> **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.

12.8 Expander Update

This page is used to update expander.

To open Expander Update page, click Maintenance → Expander Update from the menu bar. A sample screenshot of Expander Update page is shown below.



Expander Update page

Current Revision: current expander information includes expander firmware vrsion, MFG version and SAS Address

Firmware Update:

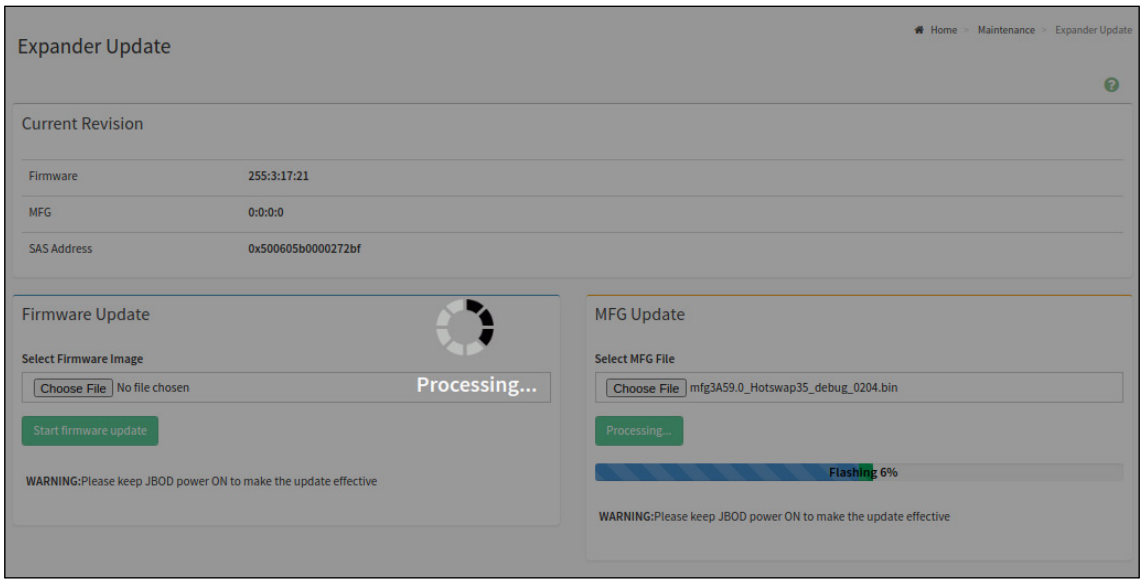
a. Click Choose File to select firmware image.

b. Click Start firmware update to update Expander Firmware

MFG Update:

a. Click Choose File to select firmware image.

b. Click Start firmware update to update MFG Firmware Resetting the image. The sample screenshot of Firmware update is as shown below.

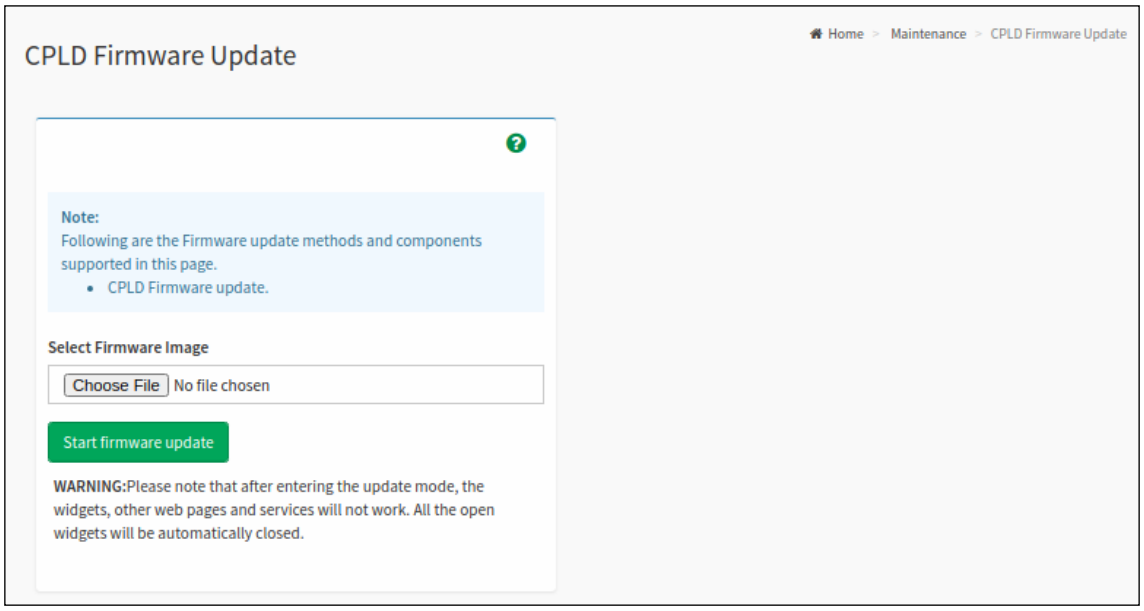


Firmware Update page

12.9 CPLD Firmware Update

This page is used to update CPLD firmware.

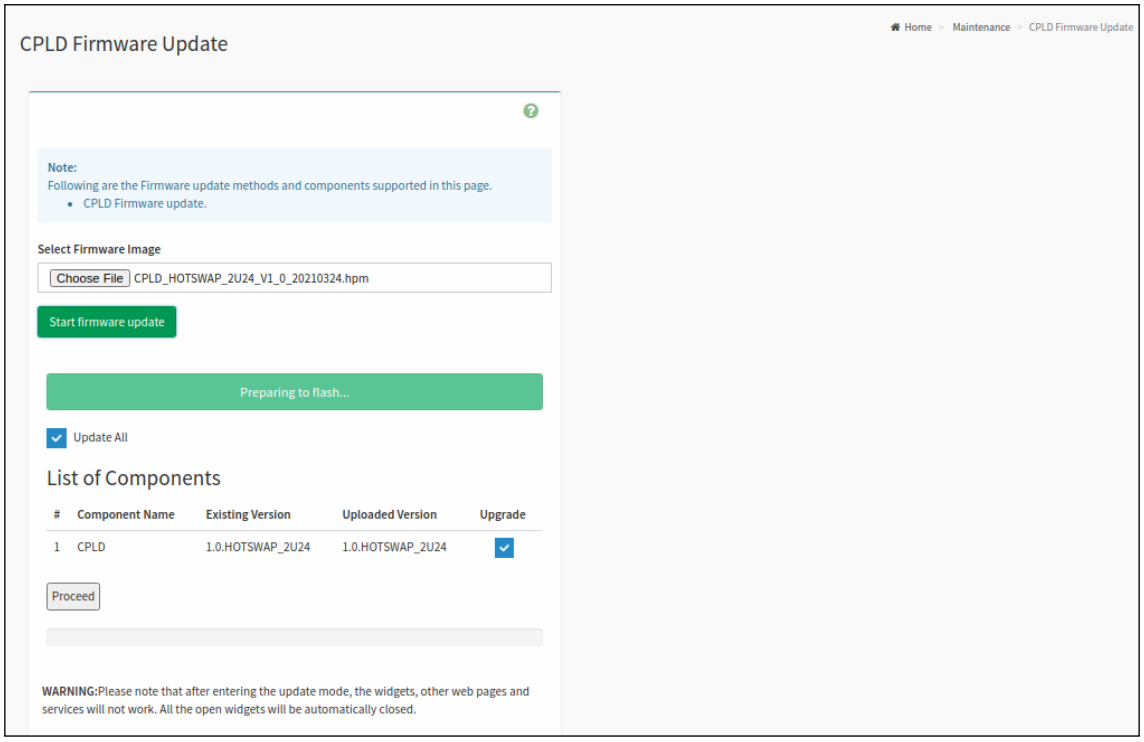
To open CPLD Firmware Update page, click Maintenance → CPLD Firmware Update from the menu bar. A sample screenshot of CPLD Firmware Update page is shown below.



CPLD Firmware Update page

Procedure for CPLD Firmware Update

a. Click Choose File to select firmware image.
b. Click Start firmware update to load the Firmware Update information.



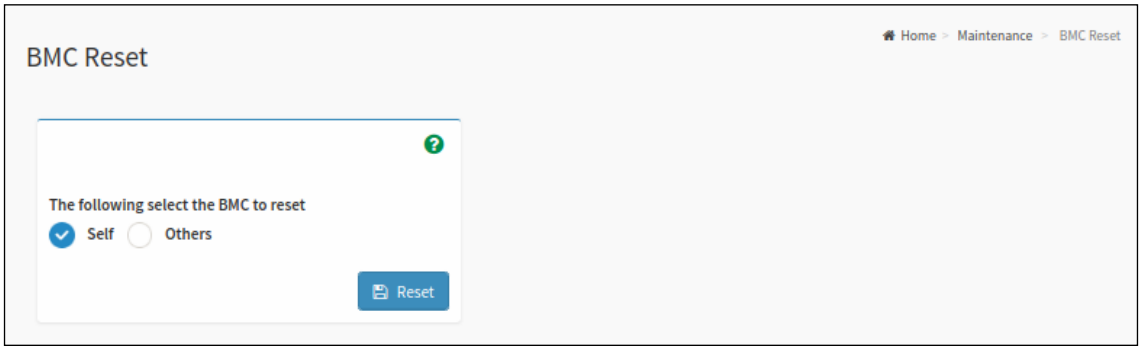
Firmware Update page

c. Check the correctness of the firmware version and c lick Proceed to update CPLD Firmware.

12.10 BMC Reset

This page is used to reset BMC.

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

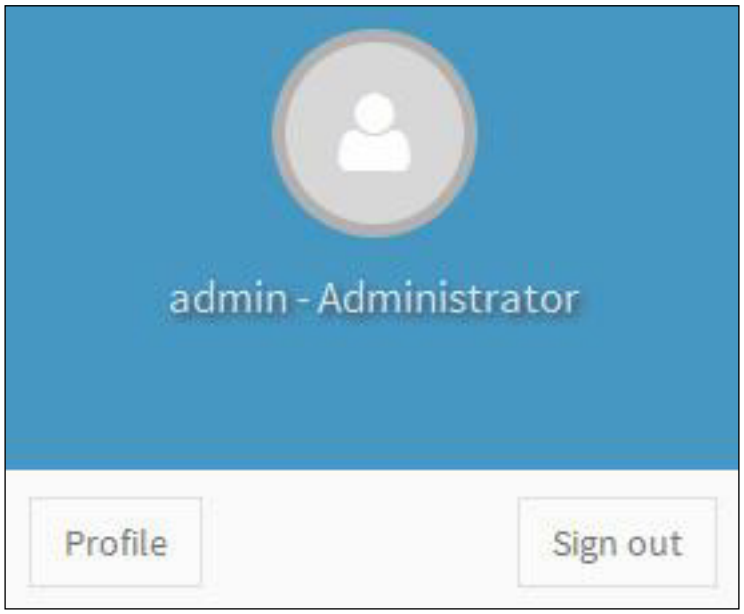


BMC Reset page

Self: Activate BMC.
Others: Other BMC.

Chapter 13. Sign Out

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



Sign Out page

Click Sign Out to perform log out. A Warning message will be prompted you to proceed further, click OK to log out or Cancel to retain the interface.

Chapter 14. Technical Support

www.aicipc.com

Taiwan, Global Headquarters

Address: No. 152, Section 4, Linghang N. Rd, Dayuan District, Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China

Address: Room 215, Building 4, No.471 Guiping Road, Xuhui District, Shanghai City, 200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia

Address: No. 500, 5th Floor, 5th Entrance, 32A, Khoroshevskoye Shosse, Moscow, 123007
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

Address: 48531 Warm Springs Boulvard Suite 404 Fremont, CA 94539, United States
Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States

Address: 21808 Garcia Lane City of Industry, CA 91789, United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: +1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States

Address: 322 Route 46 West Suite 100 Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands

Address: Peppelkade 58, 3992AK, Houten, The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com