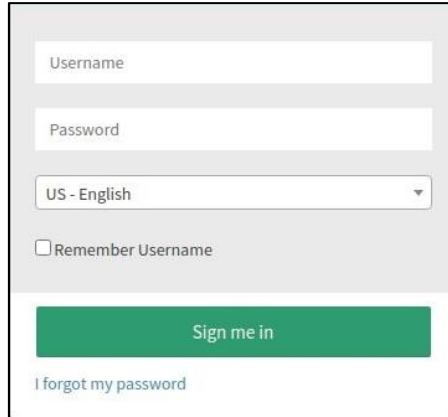


H3

PCIe Gen5 JBOX BMC User's Manual

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.

A screenshot of a login page form. It features a light gray background. At the top, there is a white input field labeled "Username". Below it is another white input field labeled "Password". Underneath the password field is a dropdown menu currently showing "US - English". Below the dropdown is a checkbox labeled "Remember Username". At the bottom of the form is a prominent green button with the text "Sign me in". Below the button, there is a link that says "I forgot my password".

Login Page

The fields are explained as follows

Username: Enter your username in this field.

Password: Enter your password in this field.

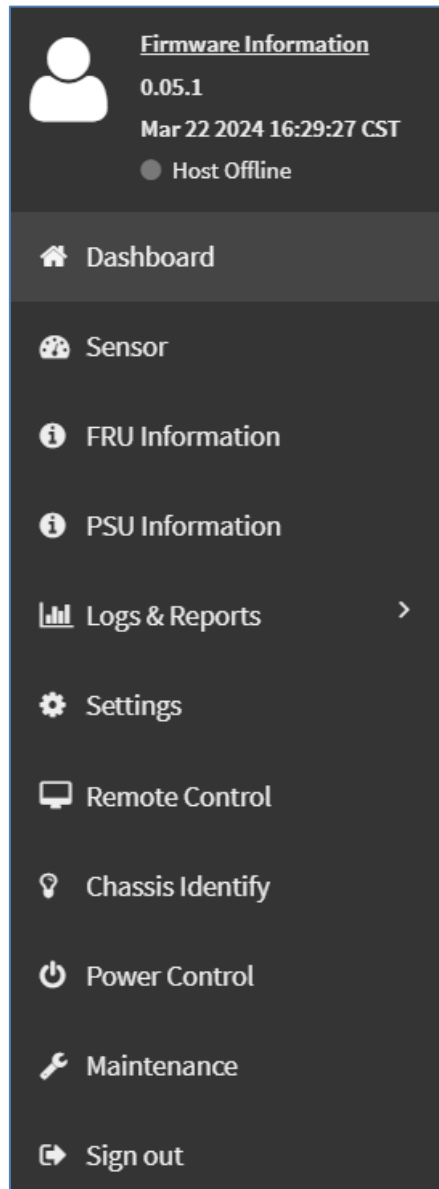
Language Selection: Language selection drop-down will be populated based on supported languages in Web UI as a part of multi language support feature. Drop-down option value will be selected based on the browser language. Default language will be selected as US-English if the browser configured language 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.

Menu Bar

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.

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. 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.

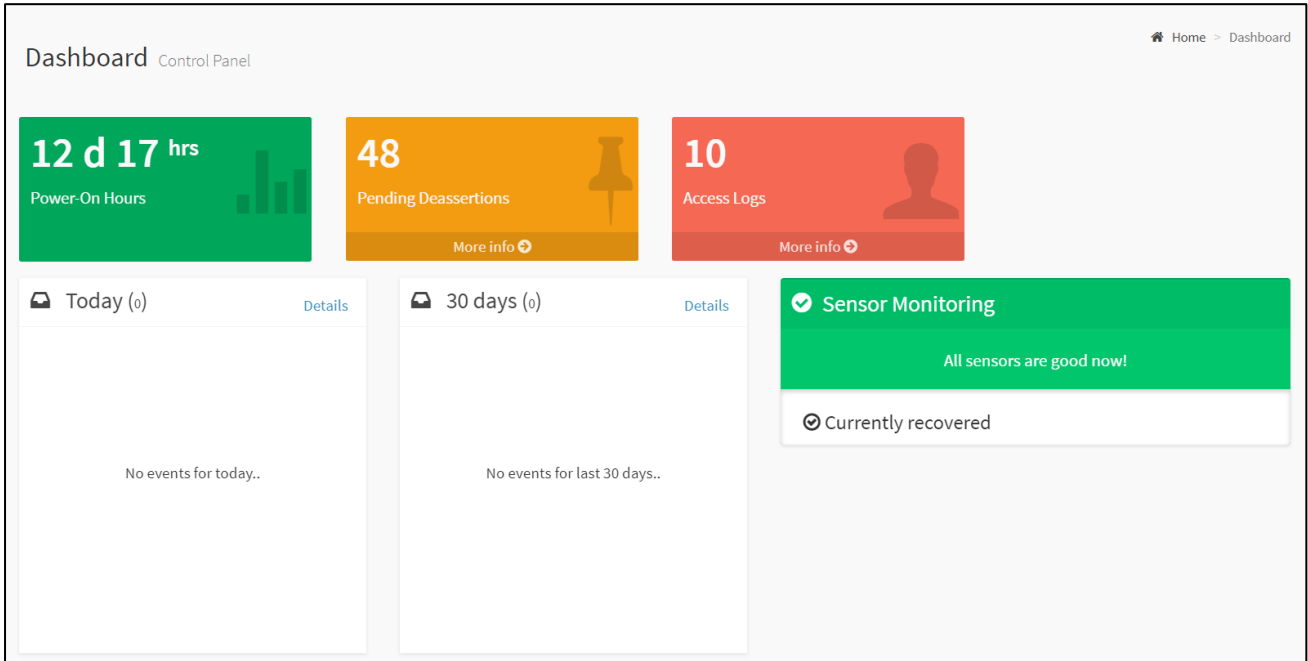
Signout: Click the  Sign out icon to log out.

Notification: Click  to view the notification received.

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

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

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)

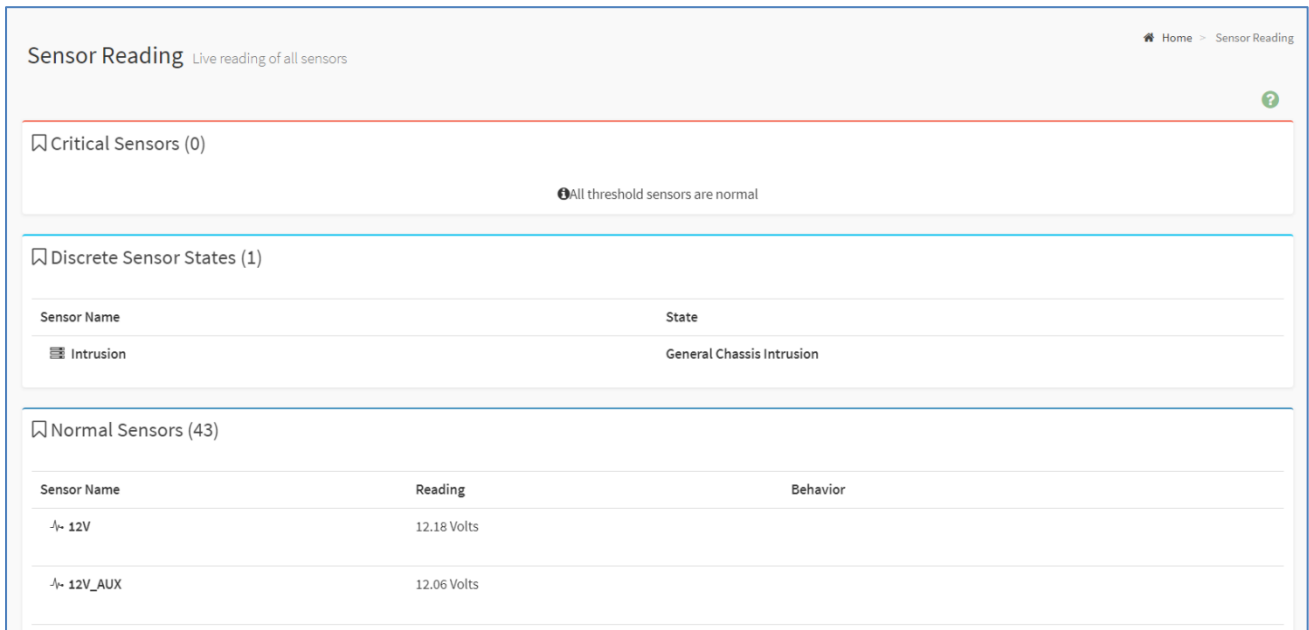
This page displays the list of event logs occurred by the different sensors on this device. Click **Details** link on Today and 30 days to view the event logs for Today and 30 days respectively.

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.

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.



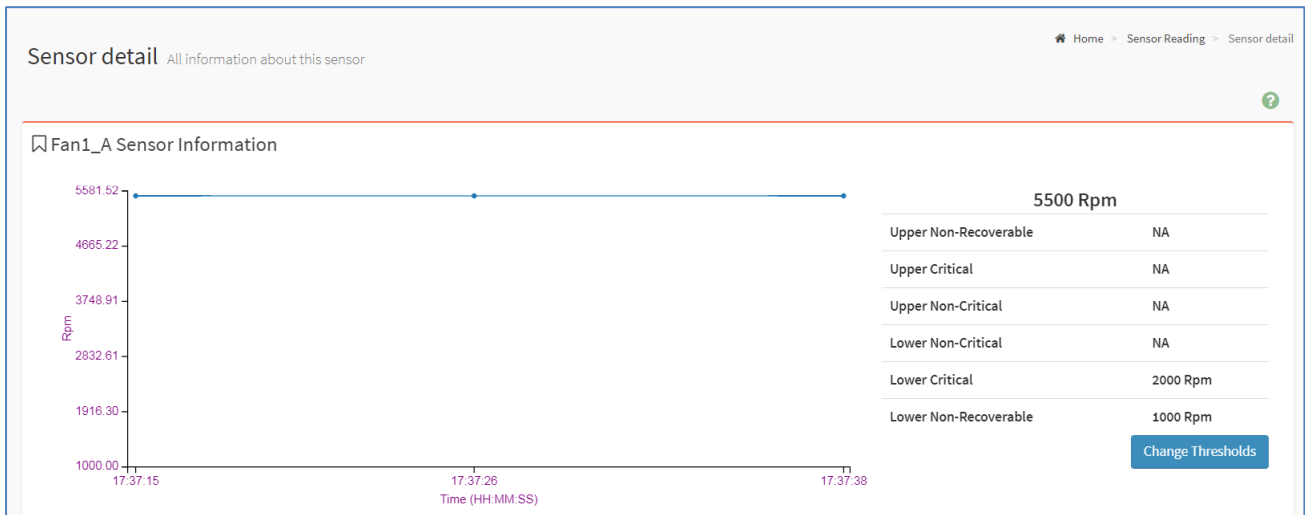
Sensor Readings Page

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 and Fan 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

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)

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.

The screenshot displays the FRU (Field Replacable Units) information page. At the top, the breadcrumb navigation shows 'Home > FRU'. Below the header, there is a section titled 'Available FRU Devices' with a search bar and a dropdown menu for 'FRU Device ID' set to '0'. The 'FRU Device Name' is listed as 'BMC_FRU'. The main content area is divided into three columns: 'Chassis Information', 'Board Information', and 'Product Information', each containing a table of device details.

Chassis Information	
Chassis Information Area Format Version	1
Chassis Type	Main Server Chassis
Chassis Part Number	
Chassis Serial Number	
Chassis Extra	

Board Information	
Board Information Area Format Version	1
Language	0
Manufacture Date Time	Mon Jan 1 00:00:00 1996
Board Manufacturer	AIC
Board Product Name	DB-BMC003-TY
Board Serial Number	505-20071400110003
Board Part Number	BDB-BMC0005A_B02
FRU File ID	
Board Extra	

Product Information	
Product Information Area Format Version	1
Language	0
Product Manufacturer	
Product Name	
Product Part Number	
Product Version	
Product Serial Number	
Asset Tag	
FRU File ID	
Product Extra	

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

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.

The screenshot displays the 'PSU Power Supply Units' page. It features a breadcrumb trail 'Home > PSU' and a help icon. The page is divided into four columns, each representing a different PSU slot. Each slot contains a table of key performance indicators and sensor data.

Slot 1	Slot 2	Slot 3	Slot 4
Power Supply Status: PS OK	Power Supply Status: PS Off	Power Supply Status: PS Off	Power Supply Status: PS OK
AC Input Voltage: 228 V	AC Input Voltage: 0 V	AC Input Voltage: 0 V	AC Input Voltage: 227 V
AC Input Current: 0.515 A	AC Input Current: 0.000 A	AC Input Current: 0.000 A	AC Input Current: 0.453 A
DC 12V Output Voltage: 12.0 V	DC 12V Output Voltage: 0.0 V	DC 12V Output Voltage: 0.0 V	DC 12V Output Voltage: 12.0 V
DC 12V Output Current: 6.000 A	DC 12V Output Current: 0.000 A	DC 12V Output Current: 0.000 A	DC 12V Output Current: 4.375 A
Temperature 1: 30.0 C/86.0 F	Temperature 1: 31.0 C/87.0 F	Temperature 1: 31.0 C/87.0 F	Temperature 1: 29.0 C/84.0 F
Temperature 2: 46.0 C/114.0 F	Temperature 2: 31.0 C/87.0 F	Temperature 2: 30.0 C/86.0 F	Temperature 2: 46.0 C/114.0 F
Fan 1: 11008 RPM	Fan 1: 0 RPM	Fan 1: 0 RPM	Fan 1: 11008 RPM
DC 12V Output Power: 90 W	DC 12V Output Power: 0 W	DC 12V Output Power: 0 W	DC 12V Output Power: 53 W
AC Input Power: 107 W	AC Input Power: 0 W	AC Input Power: 0 W	AC Input Power: 91 W
Model: R1CA2202A	Model: R1CA2202A	Model: R1CA2202A	Model: R1CA2202A
Serial Number: FSH0010S300AGB1 827000324	Serial Number: FSH001A0000AGB2 011000975	Serial Number: FSH0010S300AGB1 827000354	Serial Number: FSH001A0000AGB2 011000956
FW Rev: 07 01 08 02	FW Rev: 00 00 09 02	FW Rev: 00 00 08 02	FW Rev: 08 01 09 02

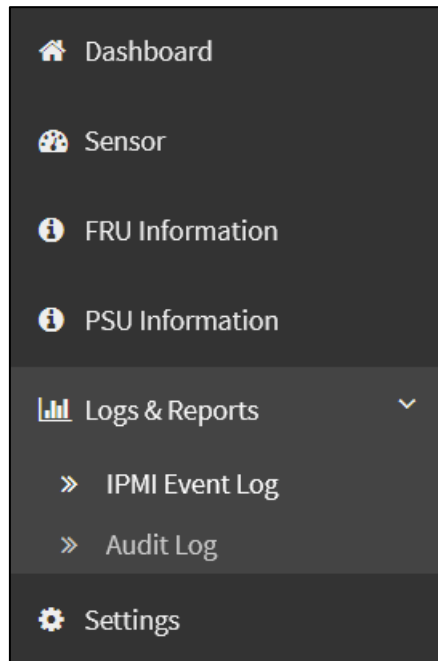
PSU Information

Logs & Reports

The Logs & Reports page displays the following information.

- IPMI Event Log
- Audit Log

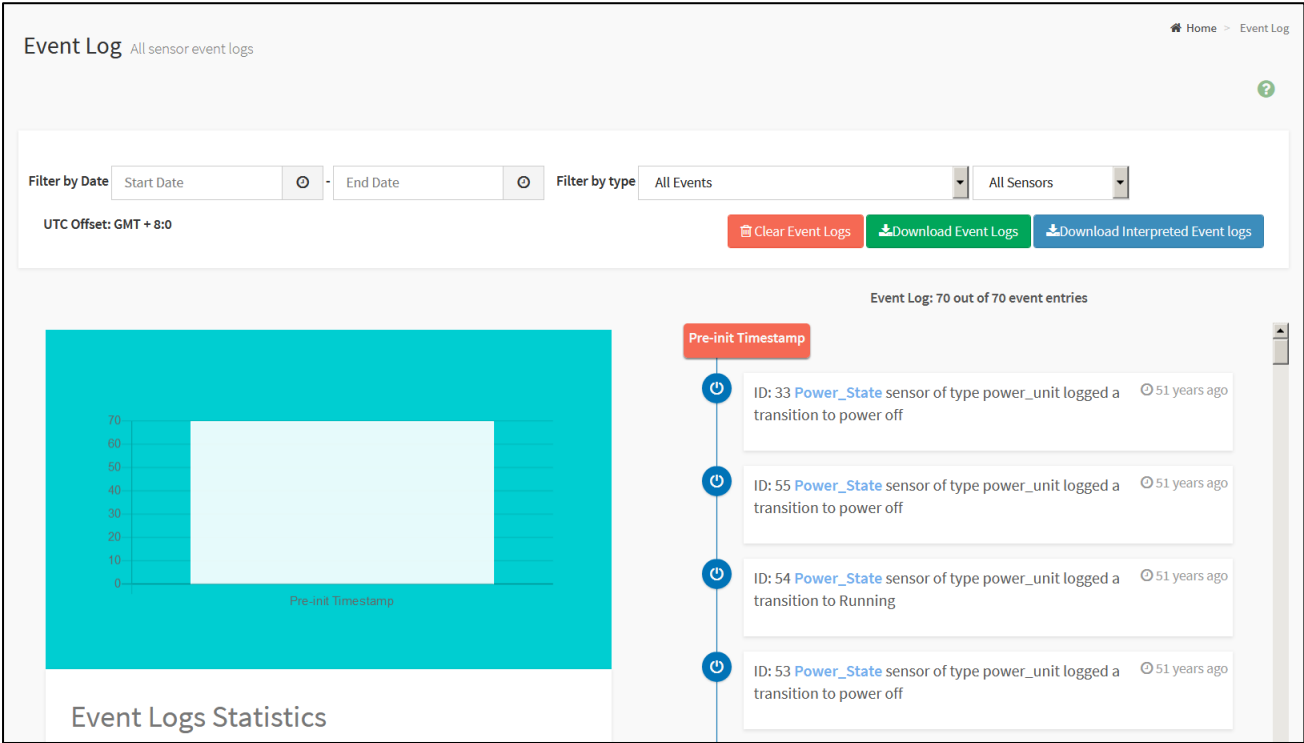
A screenshot displaying the menu items under Logs & Reports is shown below



Logs & Reports – Menu

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 **Calender**.

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.

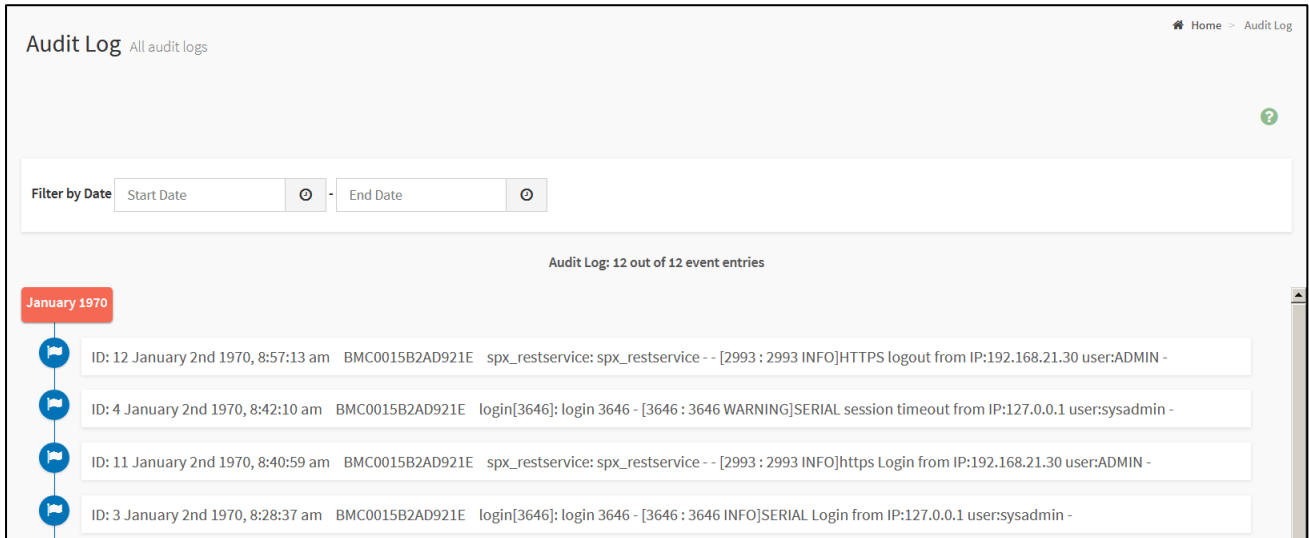
Audit Log

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.



The screenshot displays the Audit Log interface. At the top, it says "Audit Log" with a link to "All audit logs" and a breadcrumb "Home > Audit Log". Below this is a filter section with "Filter by Date" and two date input fields labeled "Start Date" and "End Date". A status message indicates "Audit Log: 12 out of 12 event entries". A date selector shows "January 1970". The main area contains a list of four event entries, each with a blue circular icon on the left and a text box on the right containing the event details.

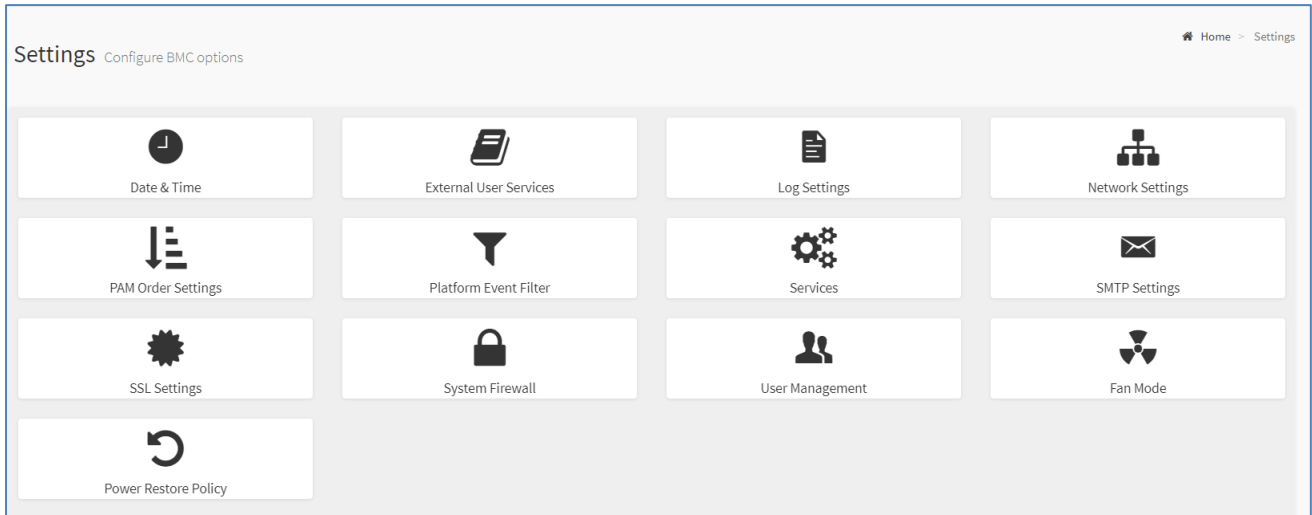
ID	Timestamp	Device ID	Event Description
12	January 2nd 1970, 8:57:13 am	BMC0015B2AD921E	spx_restservice: spx_restservice - - [2993 : 2993 INFO]HTTPS logout from IP:192.168.21.30 user:ADMIN -
4	January 2nd 1970, 8:42:10 am	BMC0015B2AD921E	login[3646]: login 3646 - [3646 : 3646 WARNING]SERIAL session timeout from IP:127.0.0.1 user:sysadmin -
11	January 2nd 1970, 8:40:59 am	BMC0015B2AD921E	spx_restservice: spx_restservice - - [2993 : 2993 INFO]https Login from IP:192.168.21.30 user:ADMIN -
3	January 2nd 1970, 8:28:37 am	BMC0015B2AD921E	login[3646]: login 3646 - [3646 : 3646 INFO]SERIAL Login from IP:127.0.0.1 user:sysadmin -

Audit Log

Settings

This group of pages allows you to access various configuration settings.

A screenshot of Configuration Group menu is shown below.

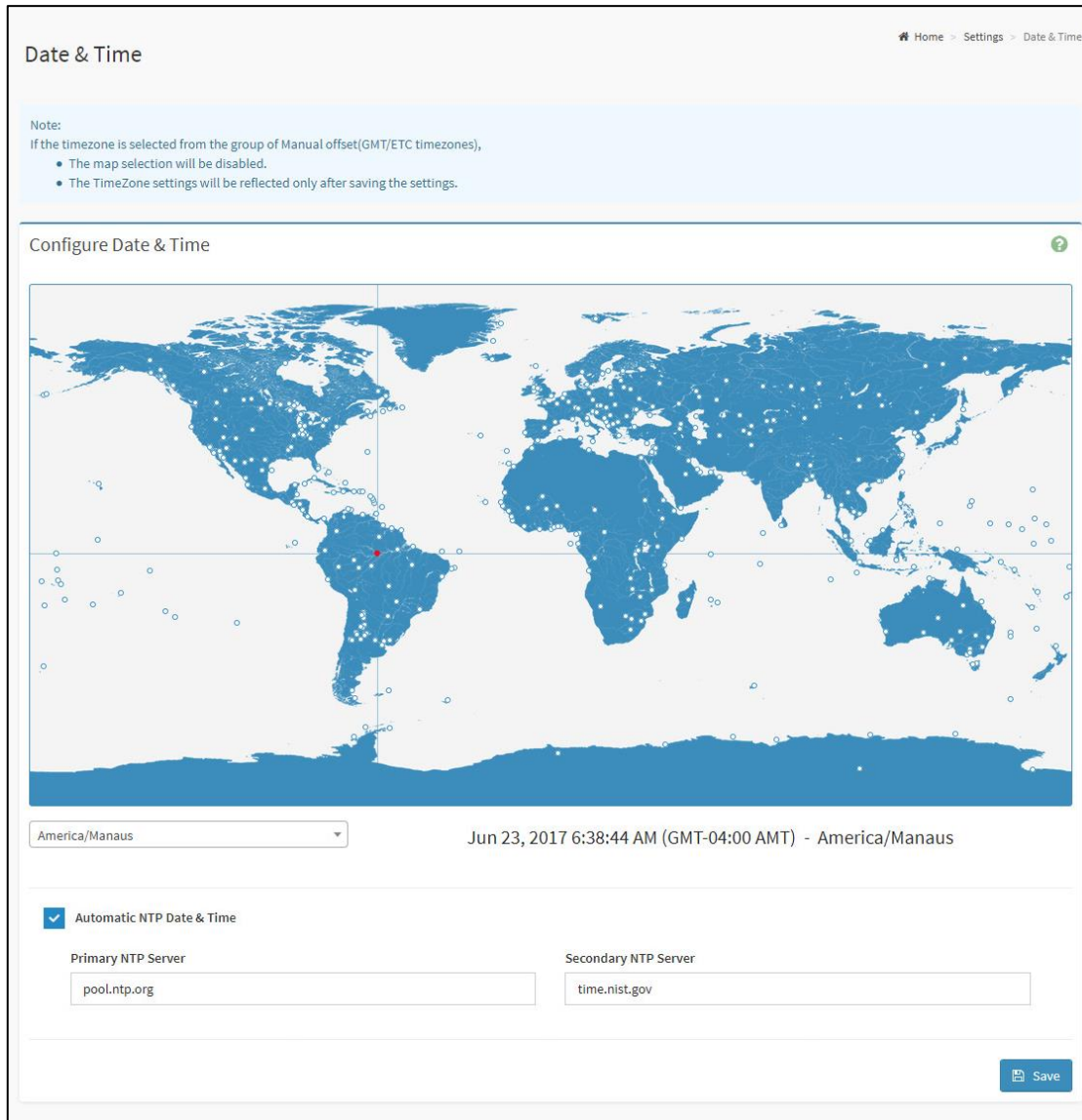


Configuration Group Menu

A detailed description of the Configuration menu is given below.

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 Timezone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.

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

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

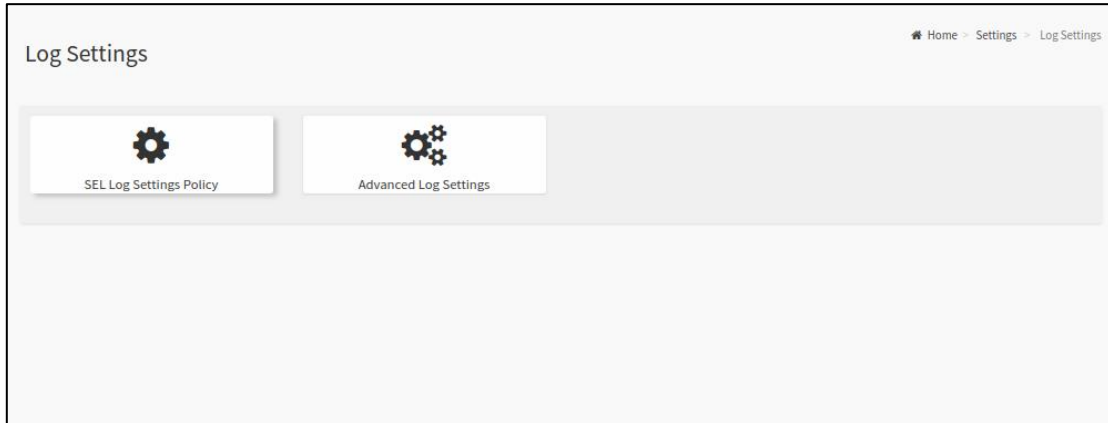
- **Primary NTP Server:** To configure a primary NTP server to use when automatically setting the date and time.
- **Secondary NTP Server:** To configure a secondary NTP server to use when automatically setting the date and time.

Save: To save the settings.

***Note:** If the timezone is selected as Manual Offset, the map selection will be disabled. The TimeZone settings will be reflected only after saving the settings.*

Log Settings

System and Audit log page displays a list of system logs and audit logs occurred in this device. To open Log Settings page, click **Settings > Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



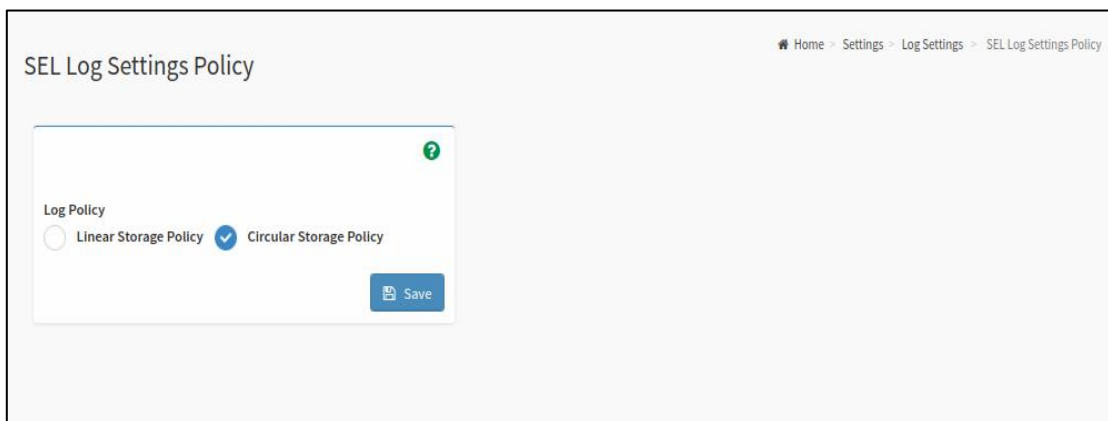
System and Audit Log Settings

The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

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.

The screenshot displays the 'Advanced Log Settings' configuration page. At the top right, a breadcrumb trail reads: Home > Settings > Log Settings > Advanced Log Settings. The main content area is a white box with a green help icon in the top right corner. It contains the following settings:

- System Log
- Local Log
- Remote Log
- Port Type: UDP TCP
- File Size:
- Rotate Count:
- Remote Log Server:
- Remote Server Port:
- Enable Audit Log

A blue 'Save' button with a floppy disk icon is located at the bottom right of the settings box.

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 selection is mandatory.

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.

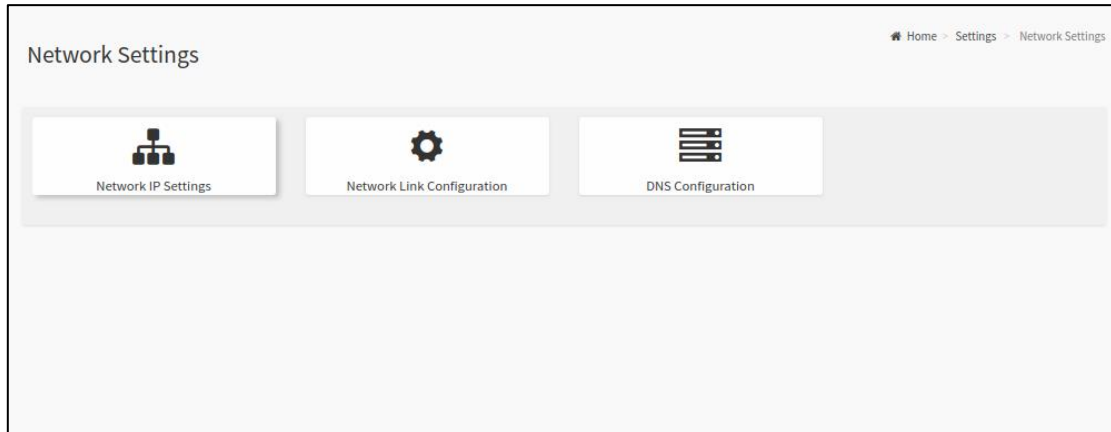
Note: Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

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

Save: To save the changes

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

Network IP Settings

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

The screenshot shows the 'Network IP Settings' page with a breadcrumb trail: Home > Settings > Network > Network IP Settings. The page contains several sections of configuration options:

- Enable LAN:** A checked checkbox.
- LAN Interface:** A dropdown menu with 'eth0' selected.
- MAC Address:** A text field containing '00:C1:A2:44:48:24'.
- Enable IPv4:** A checked checkbox.
- Enable IPv4 DHCP:** A checked checkbox.
- IPv4 Address:** A text field containing '10.0.124.123'.
- IPv4 Subnet:** A text field containing '255.255.248.0'.
- IPv4 Gateway:** A text field containing '10.0.120.1'.
- Enable IPv6:** A checked checkbox.
- Enable IPv6 DHCP:** An unchecked checkbox.
- IPv6 Index:** A dropdown menu with '0' selected.
- IPv6 Address:** A text field containing '2001:db8:0:1:2ba:abff:fe45:3222'.
- Subnet Prefix Length:** A text field containing '0'.
- IPv6 Gateway:** A text field containing '22:1'.
- Enable VLAN:** A checked checkbox.
- VLAN ID:** A text field containing '5'.
- VLAN Priority:** A text field containing '0'.

A 'Save' button is located at the bottom right of the form area.

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 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. E.g.: 0

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

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.

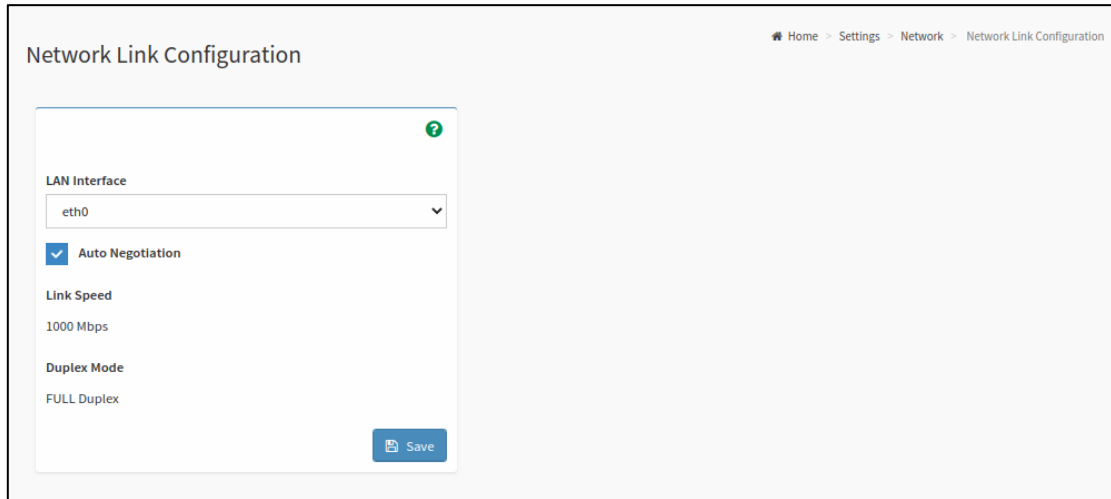
Note:

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

Save: To save the entries.

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.

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

DNS Enabled

mDNS Enabled

Host Name Setting

Automatic Manual

Host Name

AIC0015B2AECE9F

BMC Registration Settings

BMC Interface:

eth0

Register BMC

Registration method:

Nupdate DHCP Client FQDN Hostname

Both

Eth0 TSIG Configuration

TSIG Authentication Enabled

Current TSIG Private File Info

Not Available

New TSIG Private File

Eth1 TSIG Configuration

TSIG Authentication Enabled

Current TSIG Private File Info

New TSIG Private File

Domain Setting

Automatic Manual

Domain Interface

Domain Name Server Setting

Automatic Manual

DNS Interface

eth0

IP Priority

IPv4 IPv6

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 through the Interfaces (eth0ð1).

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 (readonly).
- **New TSIG Private File:** Browse and navigate to the TSIG private file.

Note: TSIG file should be of private type.

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

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

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

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

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.

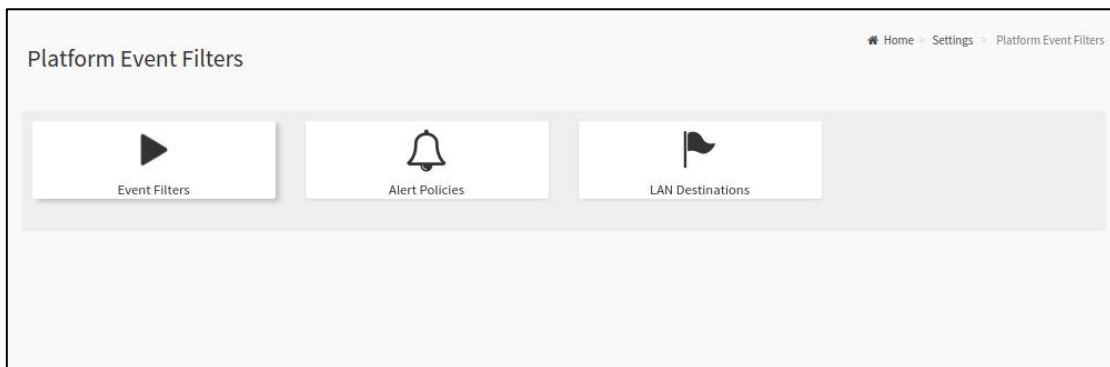
Platform Event Filter

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

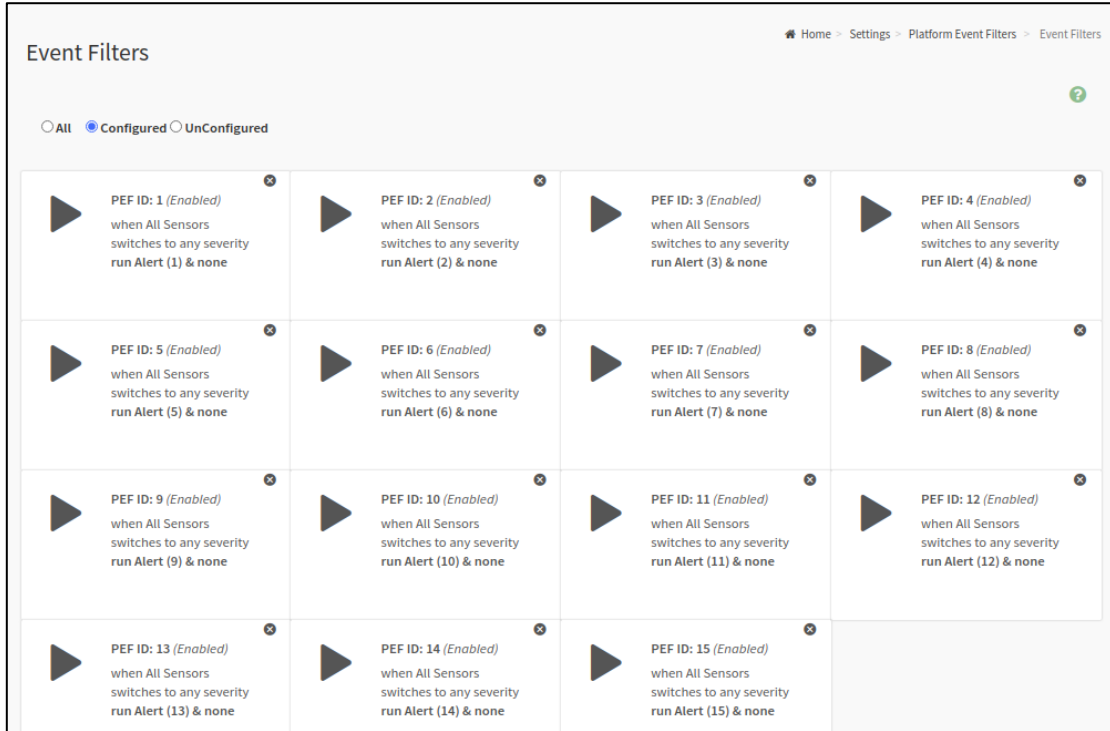
To open PEF Management Settings page, click **Settings > Platform Event Filter** from the menu bar. A sample screenshot of Platform Event Filter page is shown below.



Platform Event Filter Page

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.



Platform 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

Home > Settings > Platform Event Filters > Event Filters > Event Filter Configuration

Enable this filter

Event severity to trigger
Any severity

Power Action
Power Down

Alert Policy Group Number
1

Raw Data

Generator ID 1
255

Generator ID 2
255

Generator Type
 Slave Software

Slave Address/Software ID

Channel Number
0

IPMB Device LUN
0

Sensor type
All Sensors

Sensor name
All Sensors

Event Options
All Events

Event trigger
255

Event Data 1 AND Mask
0

Event Data 1 Compare 1
0

Event Data 1 Compare 2
0

Event Data 2 AND Mask
0

Event Data 2 Compare 1
0

Event Data 2 Compare 2
0

Event Data 3 AND Mask
0

Event Data 3 Compare 1
0

Event Data 3 Compare 2
0

Delete Save

Event Filter Configuration

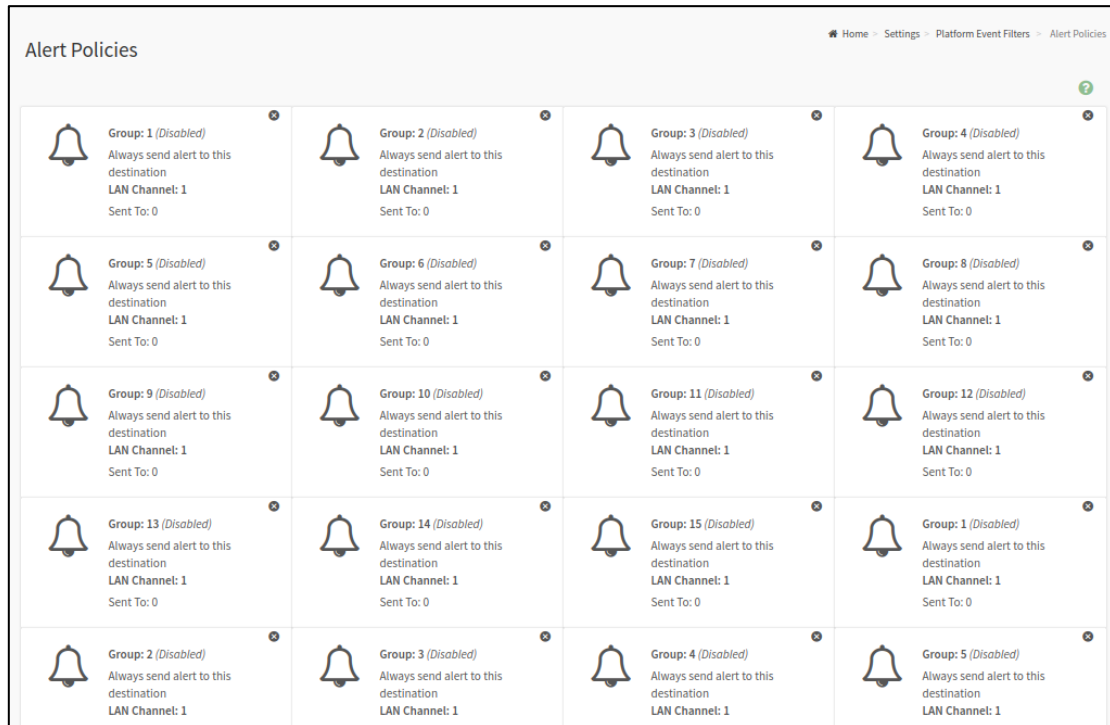
In the **Event Filter Configuration** section,

- 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 (readonly).
- 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

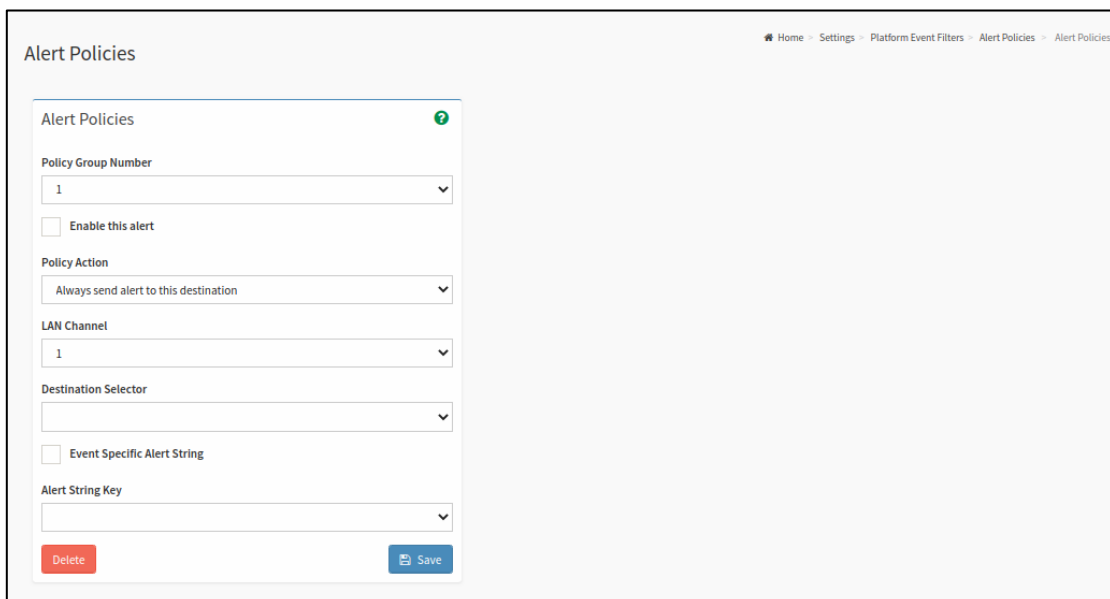
This page is used to configure the Alert Policy for the PEF configuration. You can add, delete or modify an entry in this page.



The screenshot shows the 'Alert Policies' page with a breadcrumb trail: Home > Settings > Platform Event Filters > Alert Policies. The page contains a grid of 20 alert policy entries, each in a disabled state. Each entry includes a bell icon, a group number (e.g., Group: 1), the text '(Disabled)', the action 'Always send alert to this destination', 'LAN Channel: 1', and 'Sent To: 0'. A small 'x' icon is present in the top right corner of each entry's box.

Platform Event Filters – Alert Policies

Select the slot and click on the empty slot to open the **Alert Policies** page as shown in the screenshot below.



The screenshot shows the 'Add Alert Policies' page. The breadcrumb trail is: Home > Settings > Platform Event Filters > Alert Policies > Alert Policies. A configuration form is displayed on the left side of the page. The form includes the following fields and options:

- Alert Policies** (with a help icon)
- Policy Group Number**: A dropdown menu with the value '1' selected.
- Enable this alert**
- Policy Action**: A dropdown menu with the value 'Always send alert to this destination' selected.
- LAN Channel**: A dropdown menu with the value '1' selected.
- Destination Selector**: A dropdown menu.
- Event Specific Alert String**
- Alert String Key**: A dropdown menu.
- Delete** button (red)
- Save** button (blue)

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.

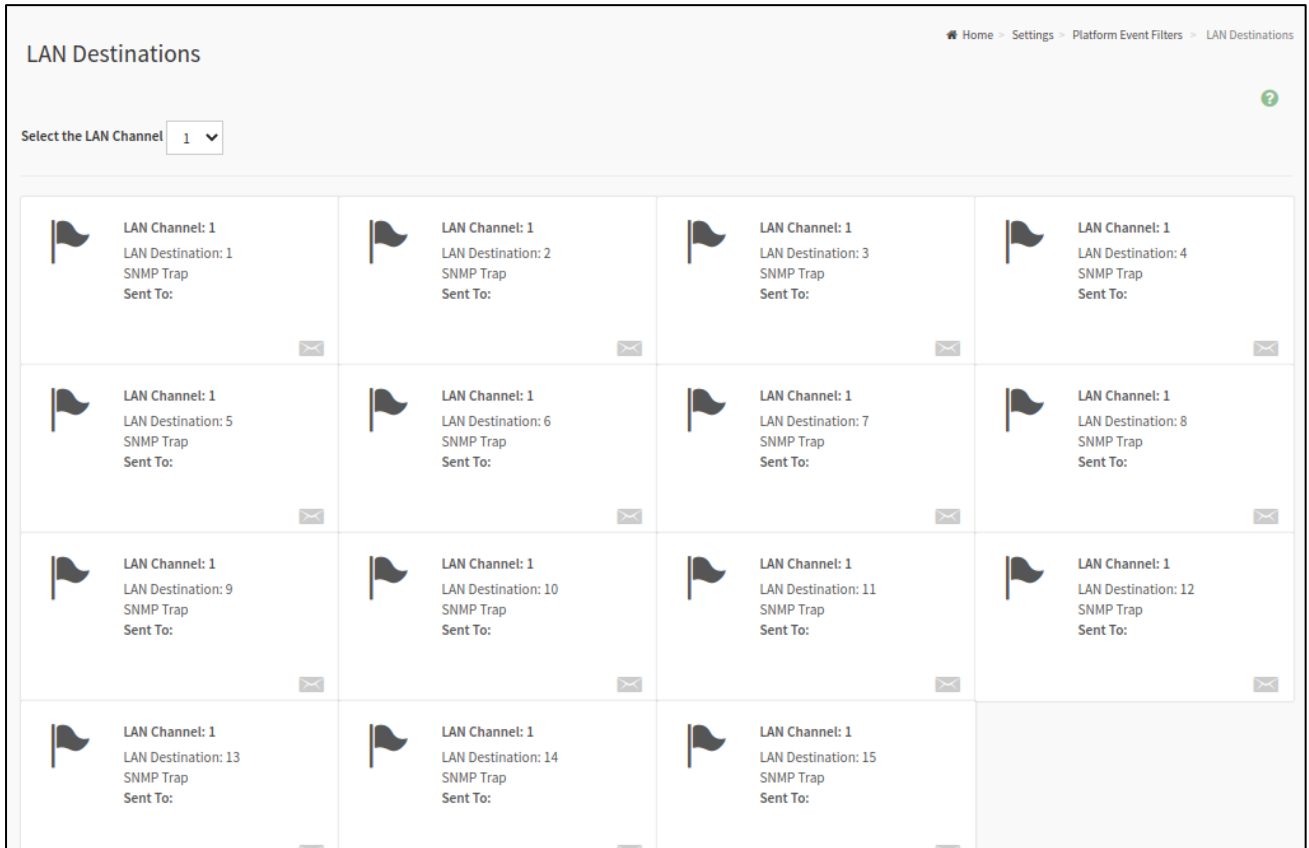
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

LAN Destinations

This page is used to configure the LAN destinations 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.

LAN Destination Configuration

Home > Settings > Platform Event Filters > LAN Destinations > LAN Destination Configuration

LAN Channel
1

LAN Destination
1

Destination Type
 SNMP Trap E-Mail

SNMP Destination Address

BMC Username

Email Subject

Email Message

Save

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 (readonly).

Destination Type: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under **Settings** ->**SMTP Settings**. For SNMP Trap, only the SNMP Destination Address has to be filled.

SNMP Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.
- IPv6 address format.


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.

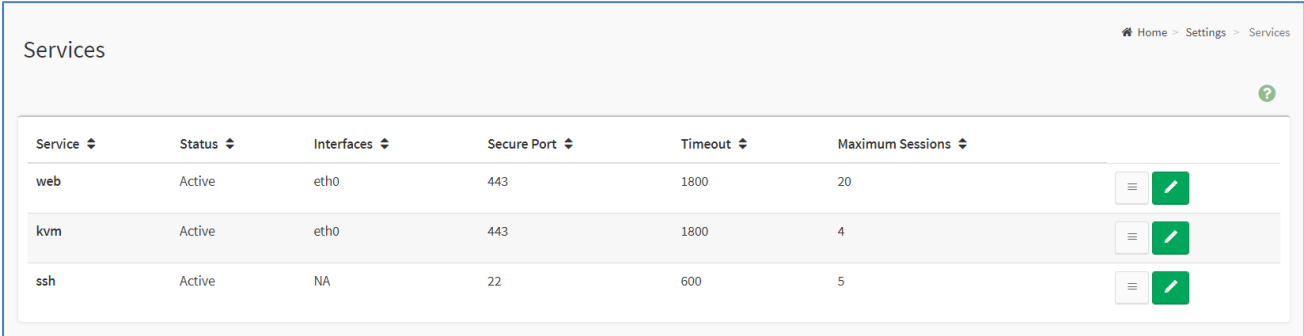
Delete: To delete the selected configured LAN Destination.







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**.*

Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service. To open Services page, click **Settings > Services** from the menu bar. A sample screenshot of Services Page is shown below.



Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions	
web	Active	eth0	443	1800	20	 
kvm	Active	eth0	443	1800	4	 
ssh	Active	NA	22	600	5	 

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.

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.

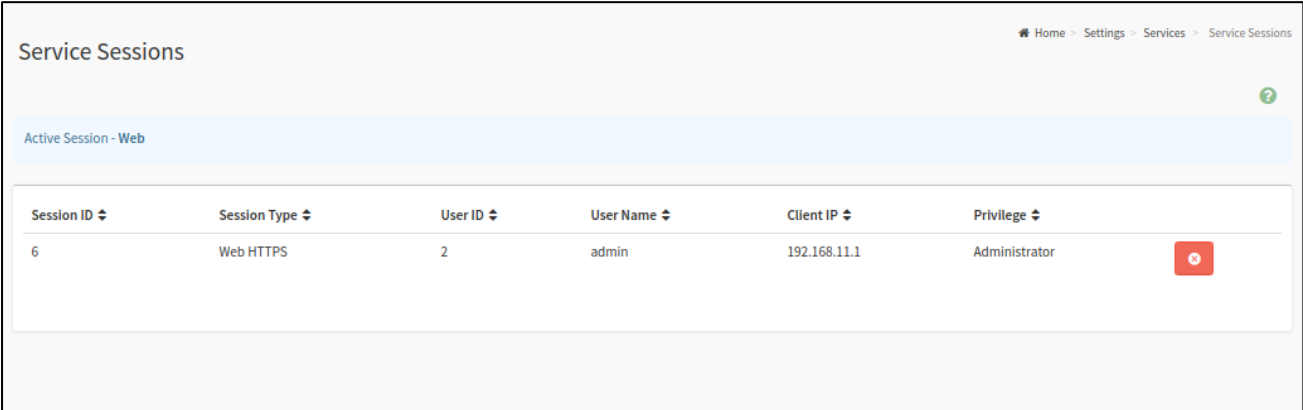
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

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 Sessions

Home > Settings > Services > Service Sessions

Active Session - Web

Session ID	Session Type	User ID	User Name	Client IP	Privilege
6	Web HTTPS	2	admin	192.168.11.1	Administrator

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.

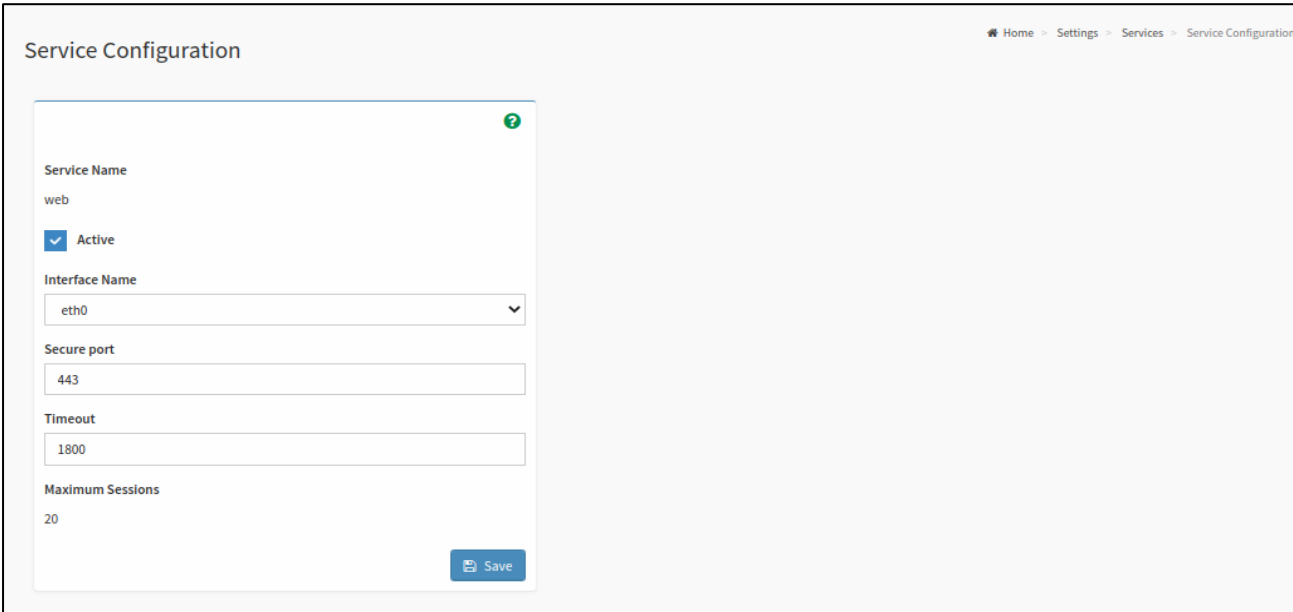
To modify the existing services:

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

Home > Settings > Services > Service Configuration

Service Name
web

Active

Interface Name
eth0

Secure port
443

Timeout
1800

Maximum Sessions
20

Save

Service Configuration

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.

SMTP Settings

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

The screenshot shows the SMTP Settings page with the following fields and options:

- LAN Interface:** eth0
- Sender Email ID:** (empty text field)
- Primary SMTP Support**
- Primary Server Name:** (empty text field)
- Primary Server IP:** (empty text field)
- Primary SMTP port:** 25
- Primary Secure SMTP port:** 465
- Primary SMTP Authentication**
- Primary Username:** (empty text field)
- Primary Password:** (empty text field)
- Primary SMTP SSLTLS Enable**
- Primary SMTP STARTTLS Enable**
- Secondary SMTP Support**

A **Save** button is located at the bottom right of the form.

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.

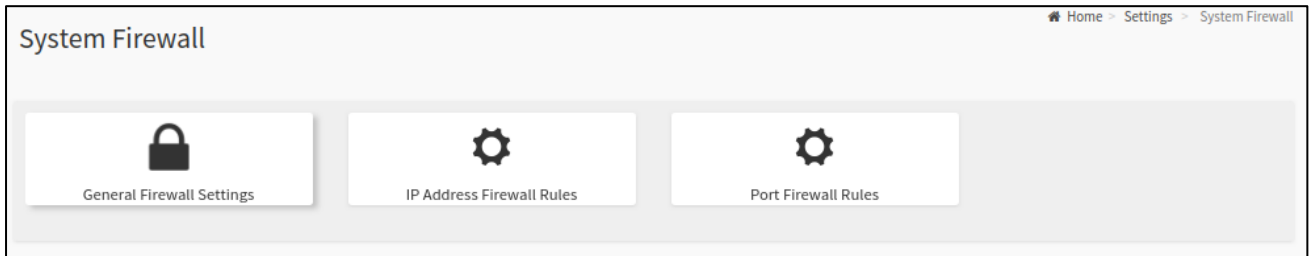
Secondary SMTP Support: It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it tries with Secondary SMTP Server configuration.

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

Save: To save the new SMTP server configuration.

System Firewall

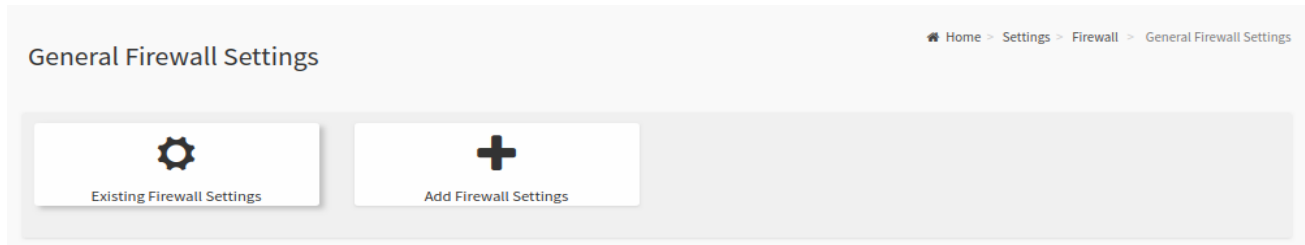
The System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall. To open System Firewall page, click **Settings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



Firewall Settings

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

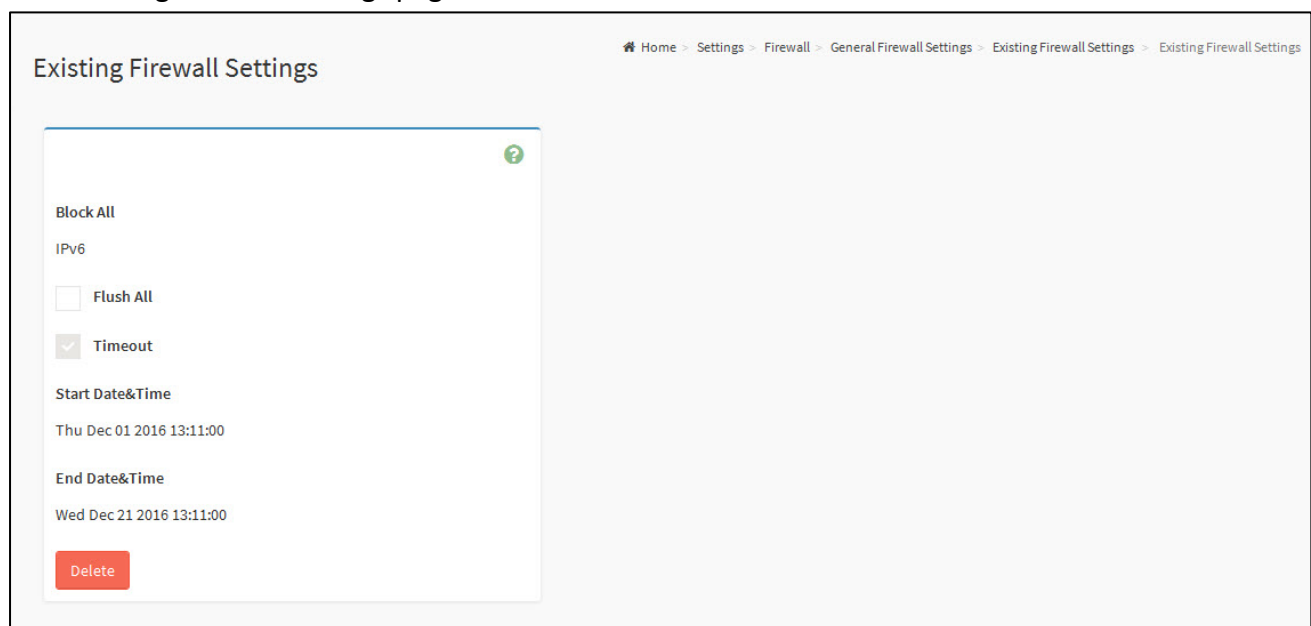
The fields of **Firewall Settings** tab are explained below.

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

- **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.

The screenshot shows the 'Add Firewall Settings' page. The breadcrumb trail at the top right is 'Home > Settings > Firewall > General Firewall Settings > Add Firewall Settings'. The main content area is a form with the following fields:

- Block All:** A dropdown menu with 'IPv4' selected.
- Flush All:** A checkbox.
- Timeout:** A checkbox.
- Start Date:** A date picker with the format 'YYYY/MM/DD'.
- Start Time:** A time picker.
- End Date:** A date picker with the format 'YYYY/MM/DD'.
- End Time:** A time picker.
- Save:** A blue button at the bottom right.

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.
5. Enter **Start Time** to start the respective firewall rule effect from this time.
6. Enter **End Time** to end the respective firewall rule effect from this time.
Note: The time should be in the *dd-mm-yy:hh-mm* format.
7. Click **Save** to save the changes made else click **Cancel** to go back to the previous screen.

IP Address Firewall Rules

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



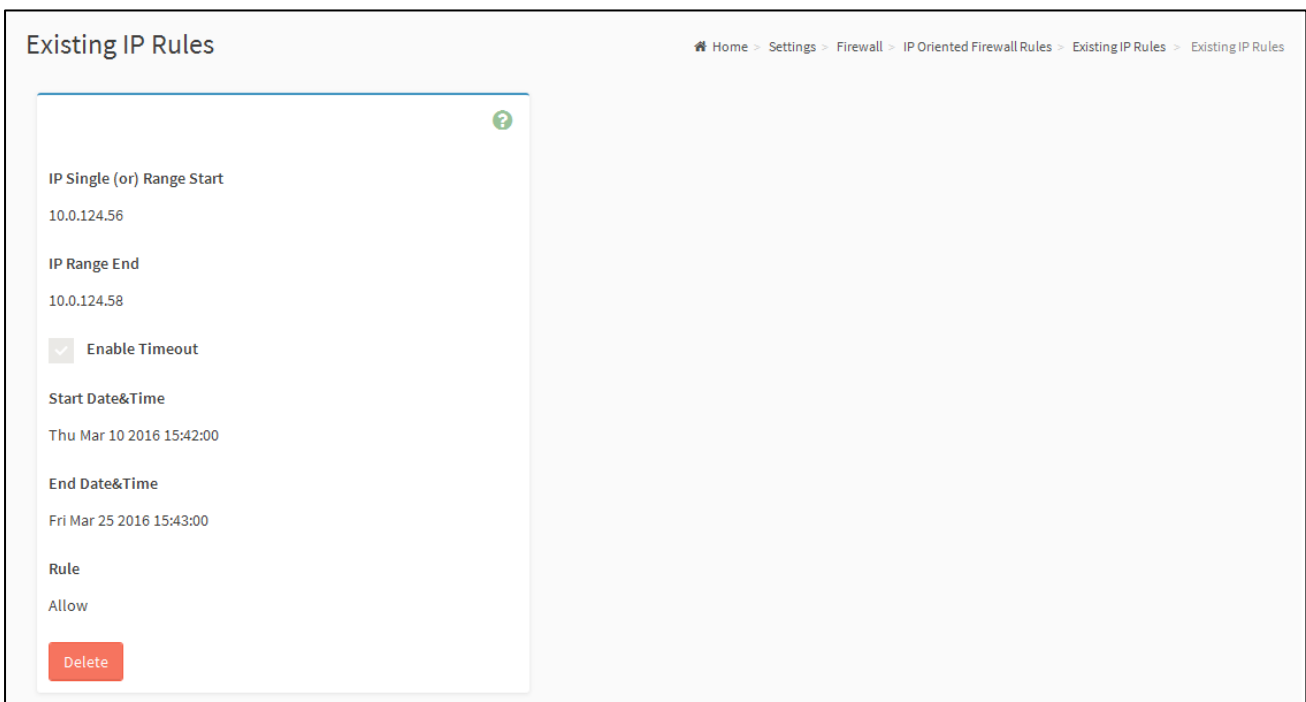
IP Address Firewall Rules

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

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

Procedure to Add IP Rule

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



System Firewall - Existing IP Rule

IP Single (or) Range Start - To show the configured Port Address or Range of Ports.

IP Range End - To show the configured Port Address or Range of Ports.

Enable Timeout - To enable/disable Timeout.

Start Date - The respective firewall rule effect will start from this date.

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

End Date - The respective firewall rule effect will end from this date.

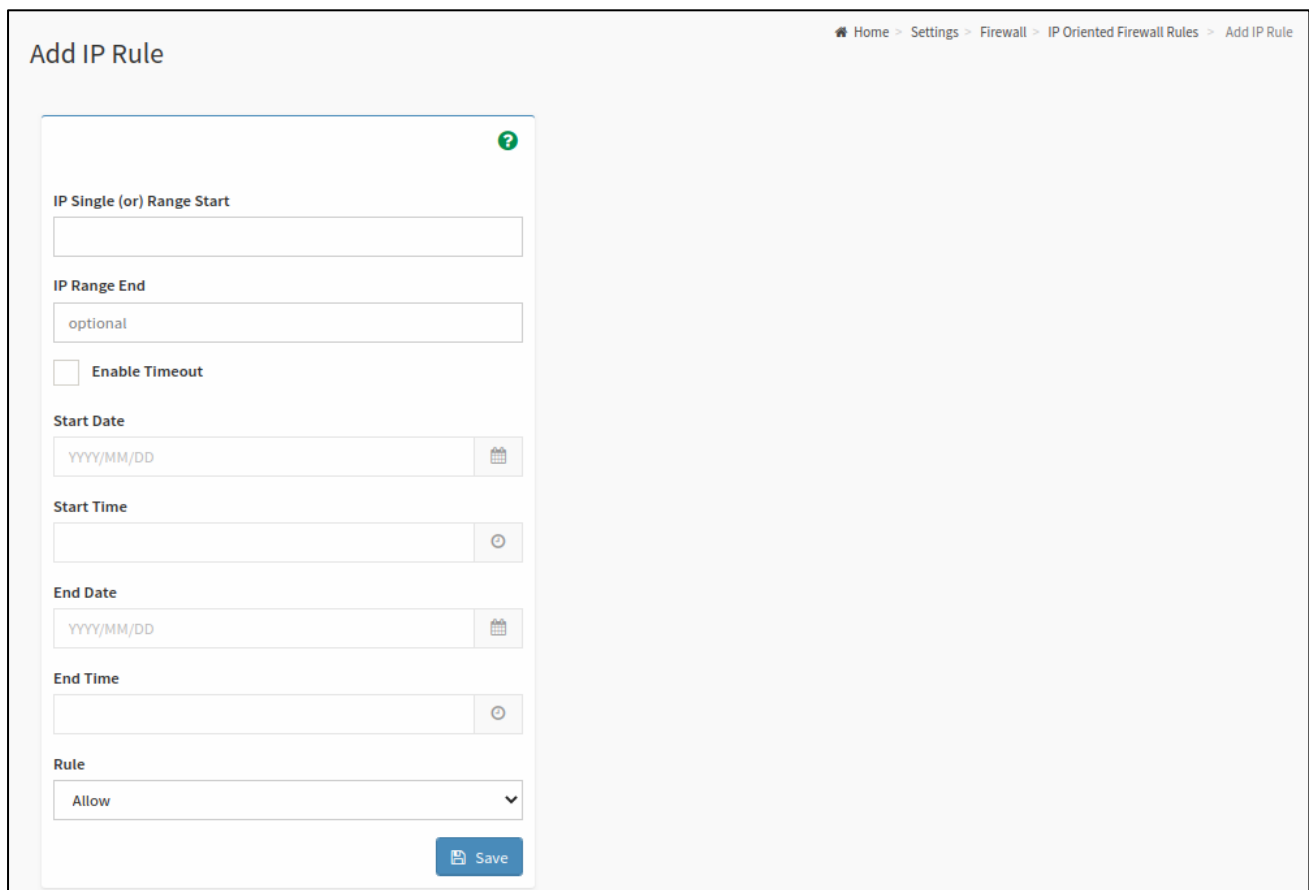
End Time - The respective firewall rule effect will end from this time.

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

Delete: To delete the selected slot.

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

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



The screenshot shows a web interface for adding a new IP rule. The page title is "Add IP Rule" and the breadcrumb navigation is "Home > Settings > Firewall > IP Oriented Firewall Rules > Add IP Rule". The form contains the following fields:

- IP Single (or) Range Start:** A text input field with a green question mark icon.
- IP Range End:** A text input field with the placeholder text "optional".
- Enable Timeout:** A checkbox.
- Start Date:** A date picker field with the placeholder "YYYY/MM/DD" and a calendar icon.
- Start Time:** A time picker field with a clock icon.
- End Date:** A date picker field with the placeholder "YYYY/MM/DD" and a calendar icon.
- End Time:** A time picker field with a clock icon.
- Rule:** A dropdown menu with "Allow" selected.

A blue "Save" button is located at the bottom right of the form.

Add IP rule

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

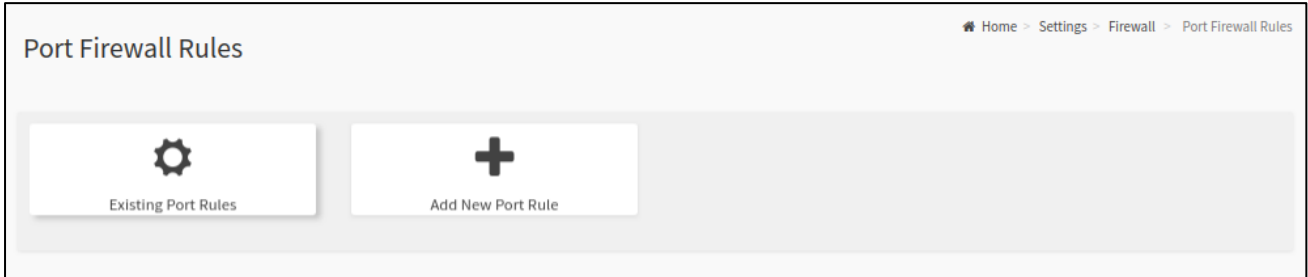
Note - IP Address will support IPv4 Address format only:

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

3. Enter IP range end value in the **IP Range End** field.
 4. Enable **Timeout** to enable firewall rules with timeout.
 5. Enter **Start Date** to start the respective firewall rule effect from this date.
 6. Enter **End Date** to end the respective firewall rule effect from this date.
 7. Enter **Start Time** to start the respective firewall rule effect from this time.
 8. Enter **End Time** to end the respective firewall rule effect from this time.
- Note:** The date and time should be in the YYYY/MM/DD and hh-mm format respectively.
9. Determine the rule to block or accept.
 10. Click **Save** to save the changes made.

Port Firewall Rules

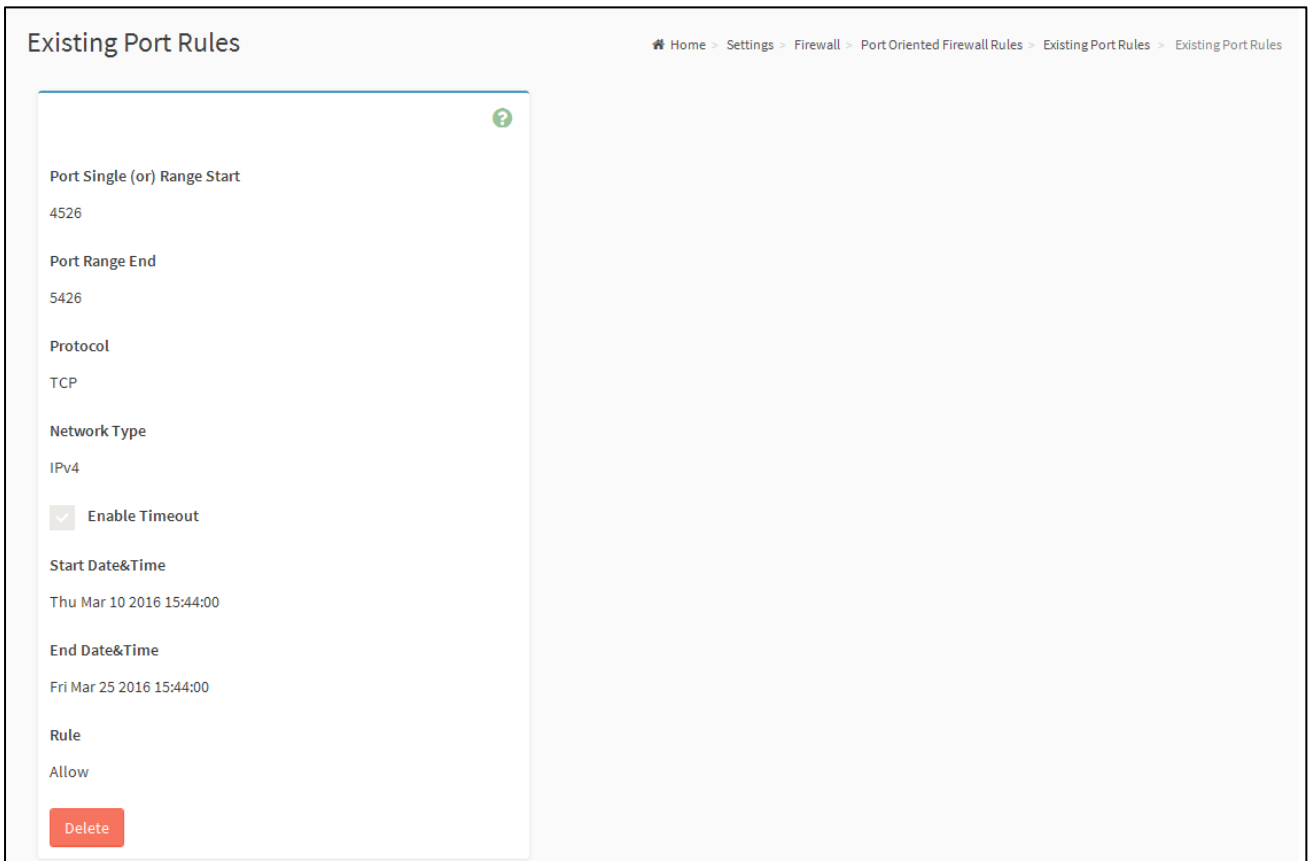
Click **Settings > Firewall > Port Firewall Rules** from the menu bar. A sample screenshot of Port Firewall Rules page is shown below.



Port Firewall Rules

To view Existing Port Rules

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



System Firewall - Existing Port Rules

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

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

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

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

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

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

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

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

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

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

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

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

To Add Port/Range of ports

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

Add Port Rule

Home > Settings > Firewall > Port Oriented Firewall Rules > Add Port Rule



Port Single (or) Range Start


Port Range End

Protocol


Network Type

Enable Timeout


Start Date


Start Time

End Date

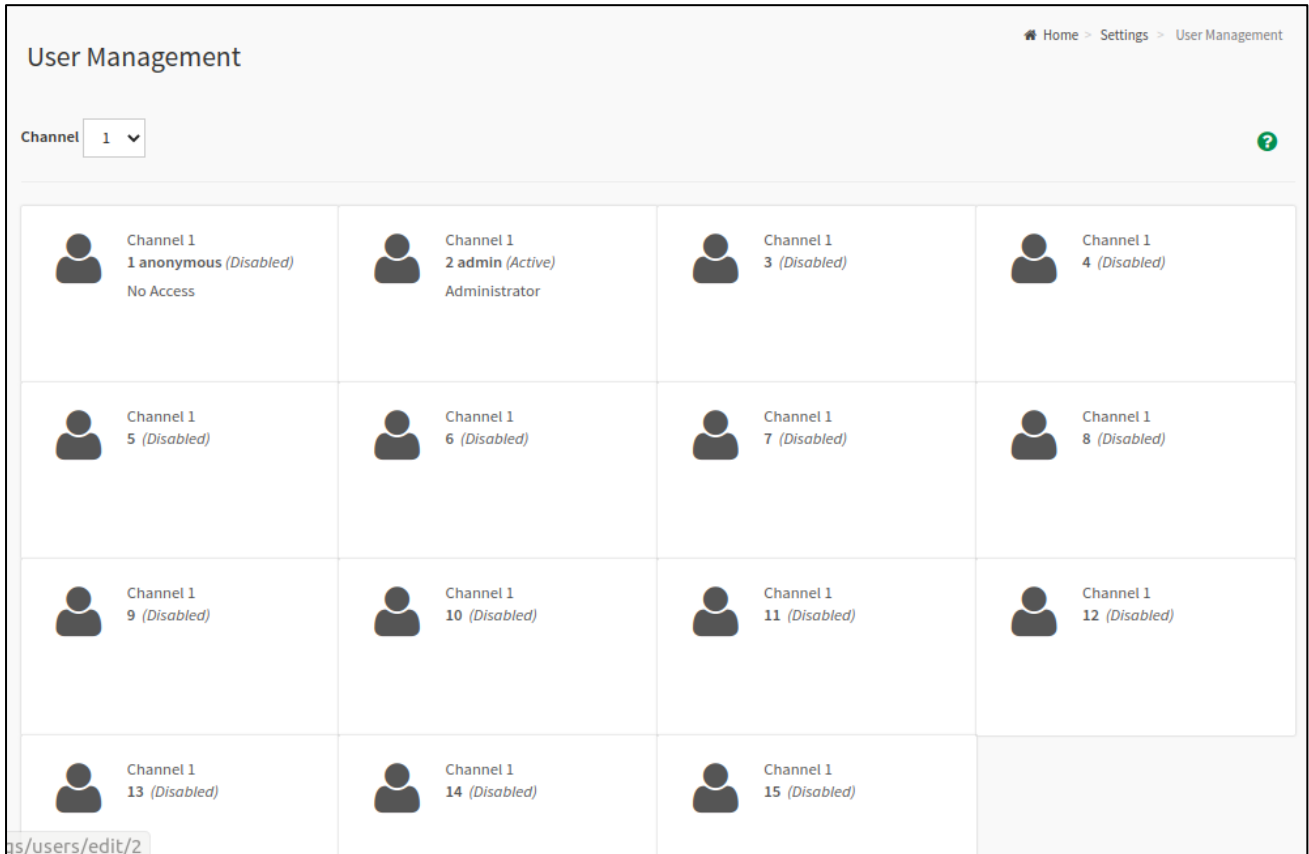
End Time


Add Port rule

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

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 Management Configuration.
2. Enter the name of the user in the **User Name** field.

Note:

- *User Name is a string of 1 to 16 alpha-numeric characters.*
- *It must start with an alphabetical character.*
- *It is case-sensitive.*
- *Special characters '-'(hyphen), '_'(underscore), '@'(at sign) 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".*

User Management Configuration

Change Password

Password Size
16 bytes

Enable User Access

Enable Channel Access

Channel 1

Channel 8

Privilege(Channel 1)
Administrator

Privilege(Channel 8)
Administrator

SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format
AMI-Format

Email ID
sJtJxhtl@amiindia.co.in

Existing SSH Key
Not Available

Upload SSH Key

User Management Configuration Page

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.
Note: *Password field is mandatory, if SNMP Status is enabled.*
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 13) of Procedure to add a new User.
4. Click **Save** to save the changes and return to the users list.
5. Click **Delete** to delete the user.

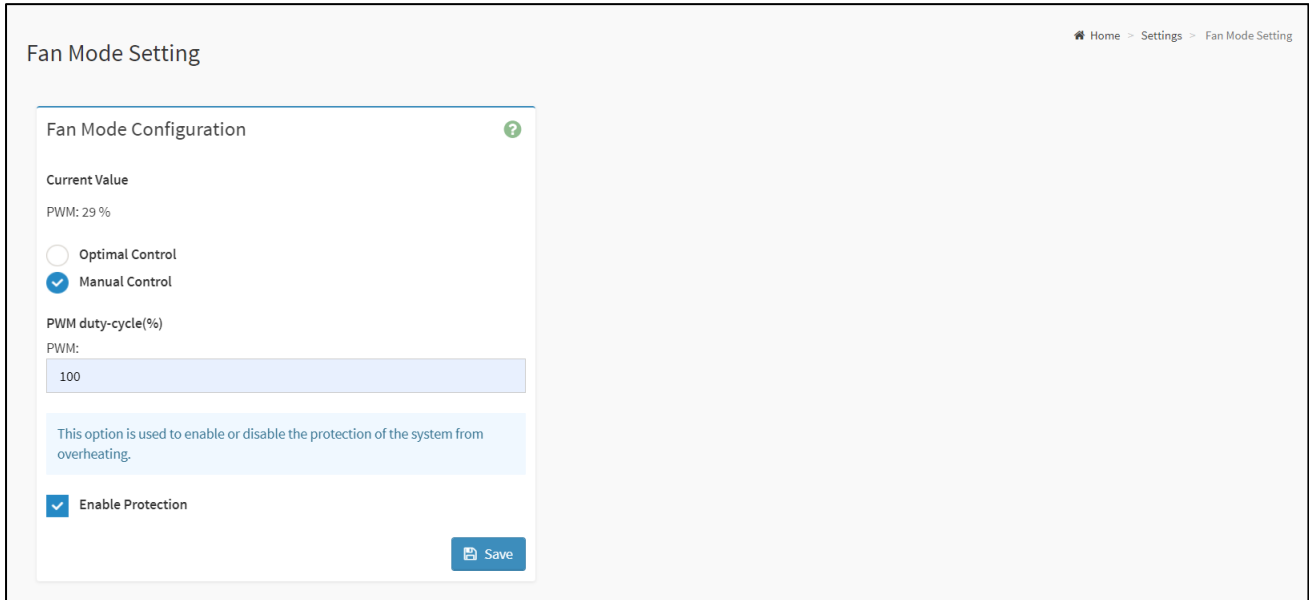
Important:

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

- sysadmin
- daemon
- sshd
- ntp
- root

Fan Mode

This field is used to set the Fan mode configuration on the BMC. To open Fan Mode page, click **Settings** > **Fan Mode** from the menu bar. A sample screenshot of Fan Mode is shown as below.



Fan Mode

The fields are as followed.

Current Value: Displays the current PWM duty-cycle of Fans.

Optimal Control: To automatically control Fan speed with the Smart Fan.

Manual Control: To manually control Fan speed (PWM duty-cycle) without the Smart Fan.

Note:

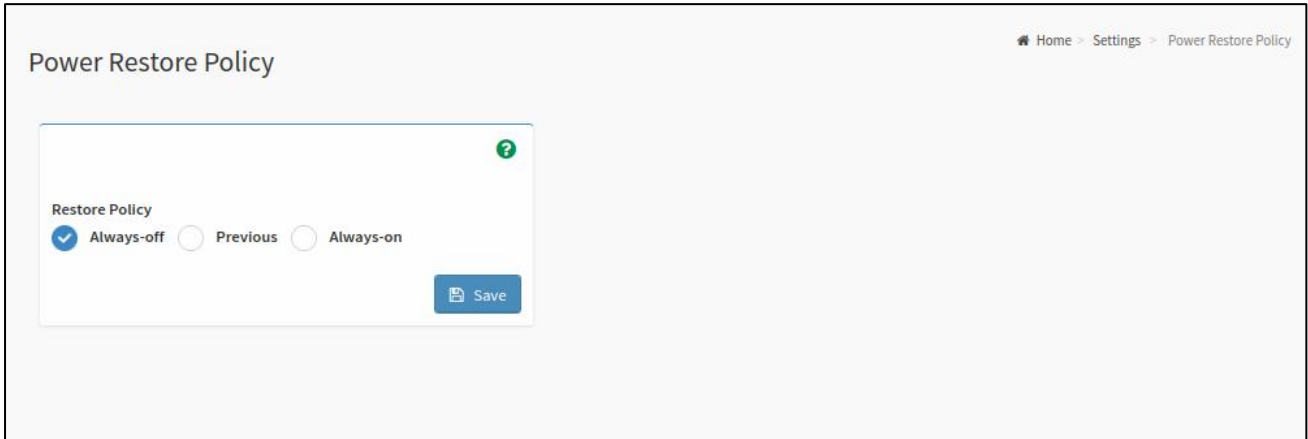
- Value range is 1 ~ 100 %.

Enable Protection: This option is used to enable or disable the protection of the system from overheating.

Save: To save the settings.

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

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

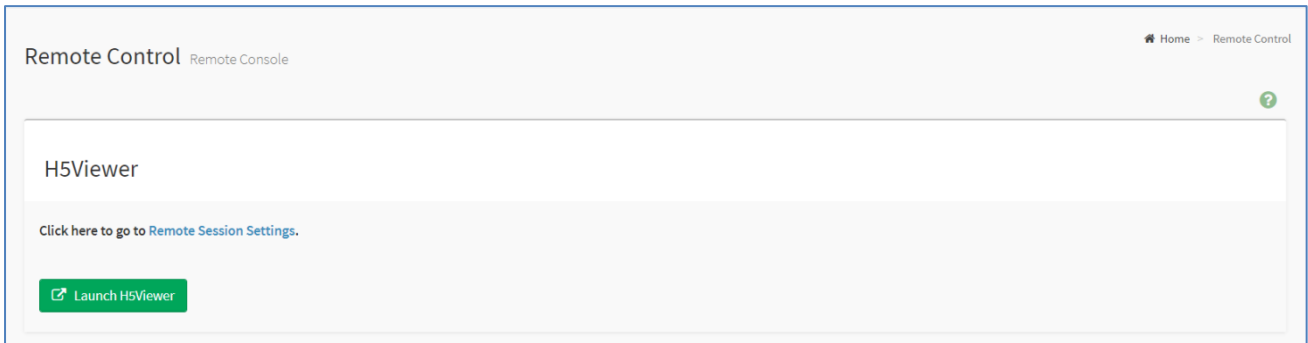
Always-off: Keep power off

Previous: Restore to the previous state

Always-on: Keep power on

Remote Control

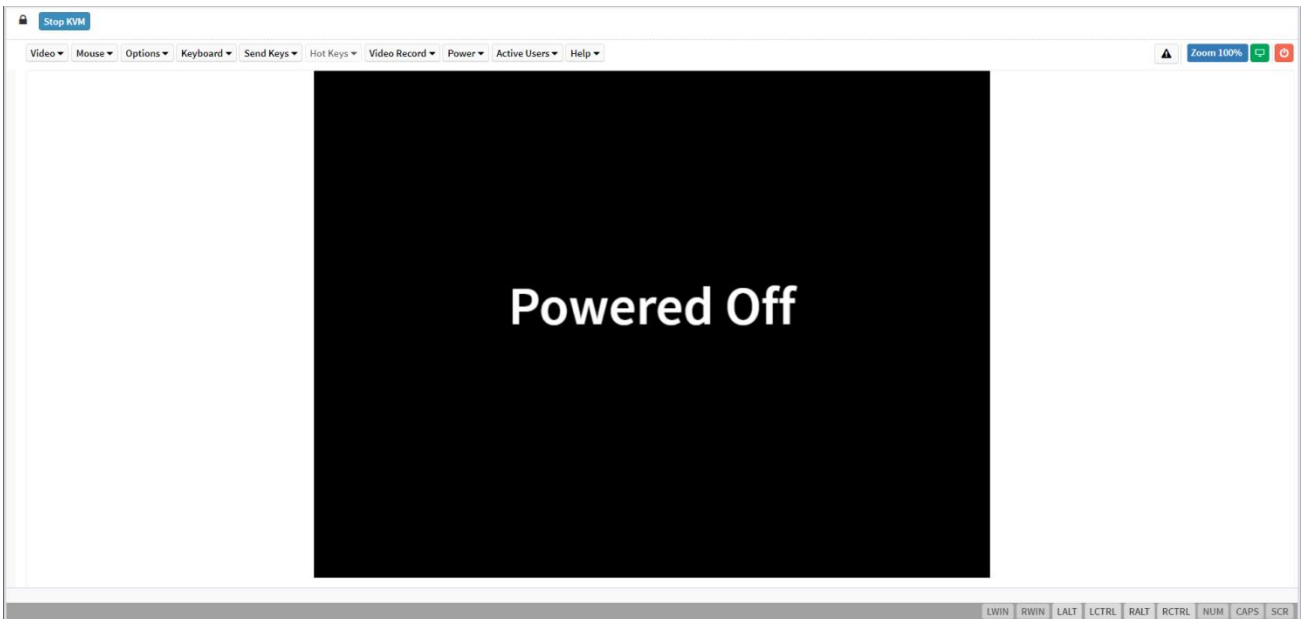
The Remote Control page consists of the following options. A sample screenshot is displayed below.



Remote Control page

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

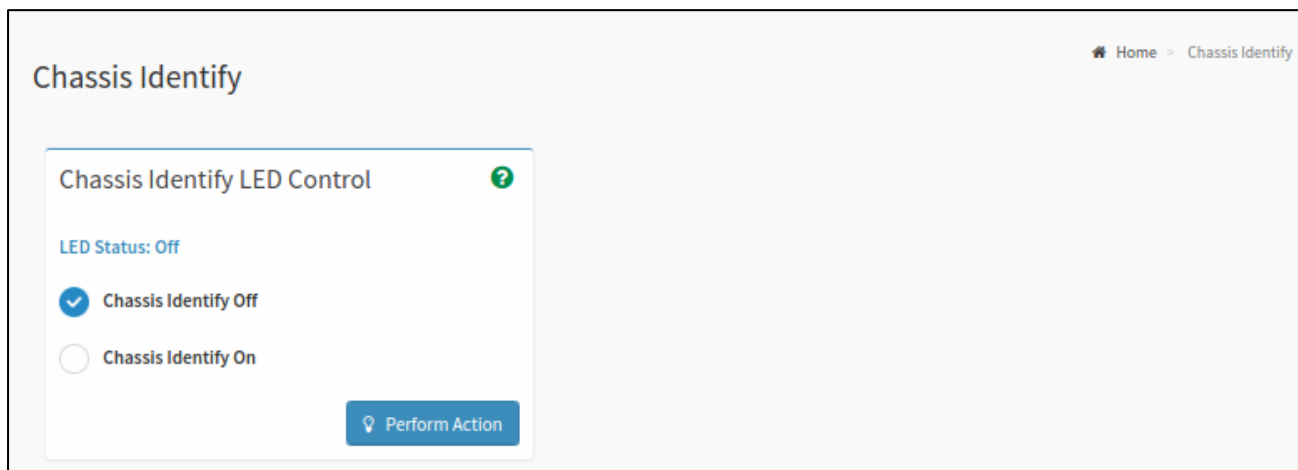
Open the Remote Control page, click **Launch KVM**. A sample screenshot of the Remote **KVM** page is shown below.



Remote KVM

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.

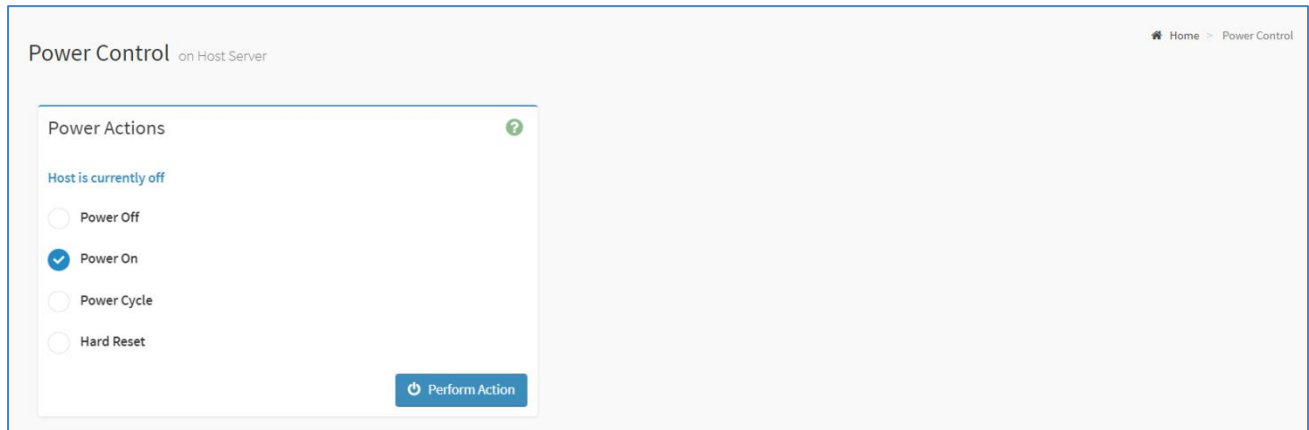
Chassis Identify Off: turn off the chassis identify LED

Chassis Identify On: turn on the chassis identify LED

Perform Action: Perform the selected action.

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.

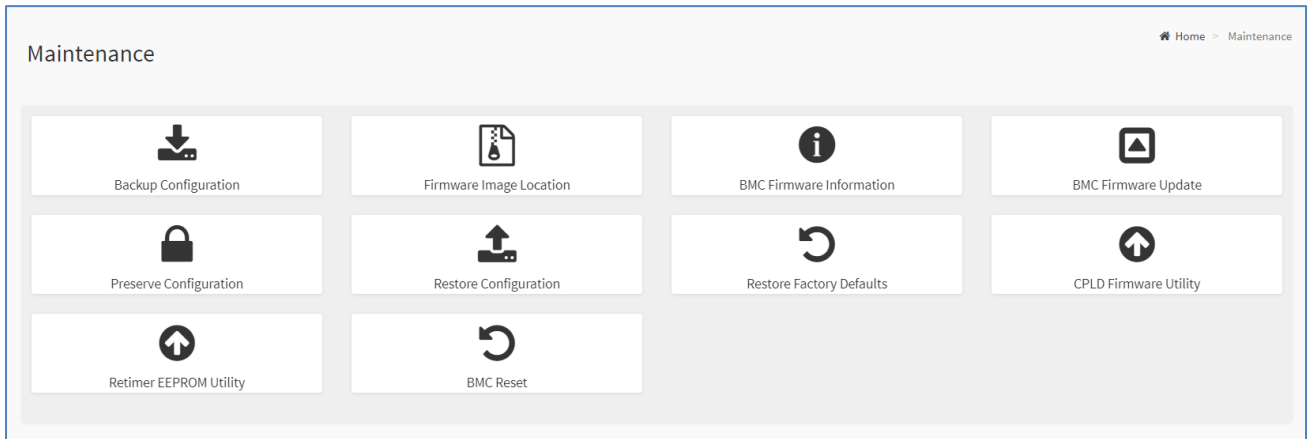
Power Cycle: This option will first power off, and then reboot the system (cold boot).

Hard Reset: This option will reboot the system without powering off (warm boot).

Perform Action: Perform the selected action.

Maintenance Group

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

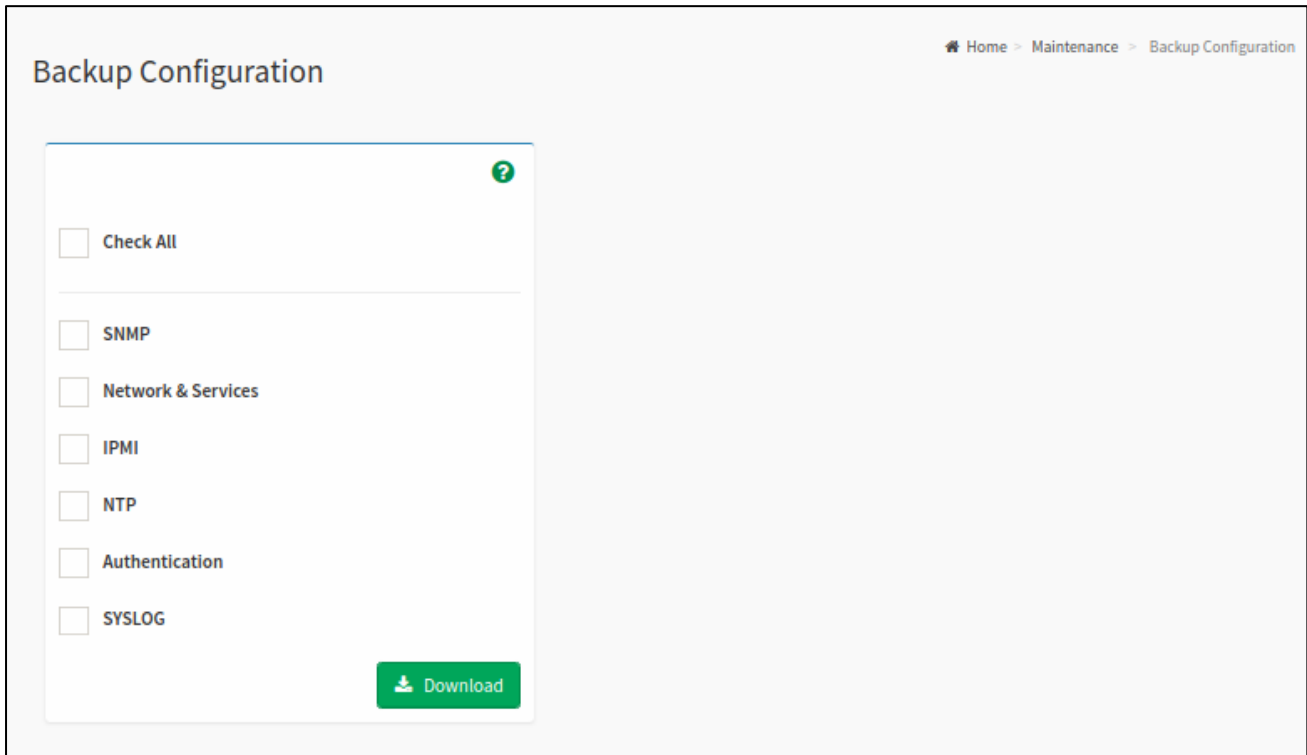


Maintenance

A detailed description is given below.

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

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:

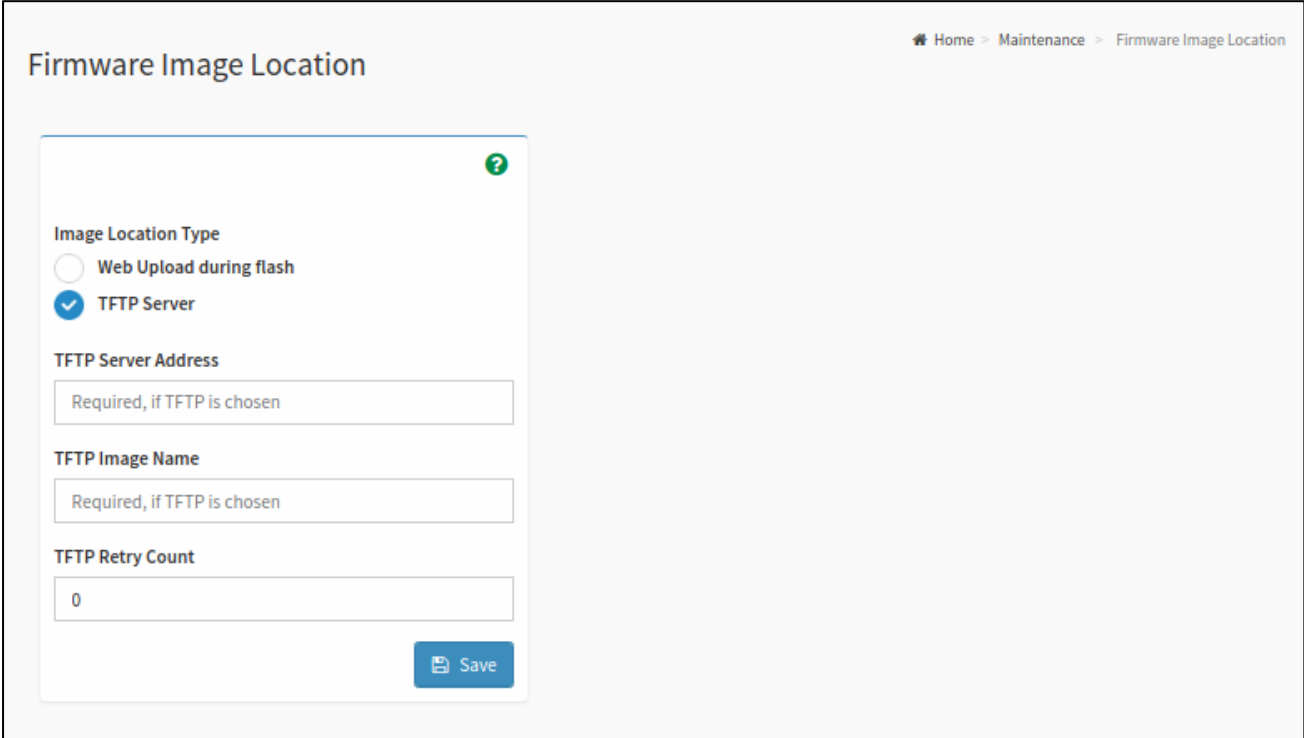
1. Click **Check All** to backup all the configuration items or check the configuration that needs to be backup. The Backup Configuration page will appear as shown in the above screenshot.

***Note:** Network configurations are interrelated to IPMI, and hence by default IPMI configurations will be selected automatically when you select “Network and Services” to be backed up.*

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

Firmware Image Location

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



The screenshot shows the 'Firmware Image Location' configuration page. At the top right, there is a breadcrumb: Home > Maintenance > Firmware Image Location. The main heading is 'Firmware Image Location'. Below it is a form with a green question mark icon in the top right corner. The form has four sections: 1. 'Image Location Type' with two radio buttons: 'Web Upload during flash' (unselected) and 'TFTP Server' (selected). 2. 'TFTP Server Address' with a text input field containing the placeholder text 'Required, if TFTP is chosen'. 3. 'TFTP Image Name' with a text input field containing the placeholder text 'Required, if TFTP is chosen'. 4. 'TFTP Retry Count' with a text input field containing the value '0'. At the bottom right of the form is a blue 'Save' button with a floppy disk icon.

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 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.

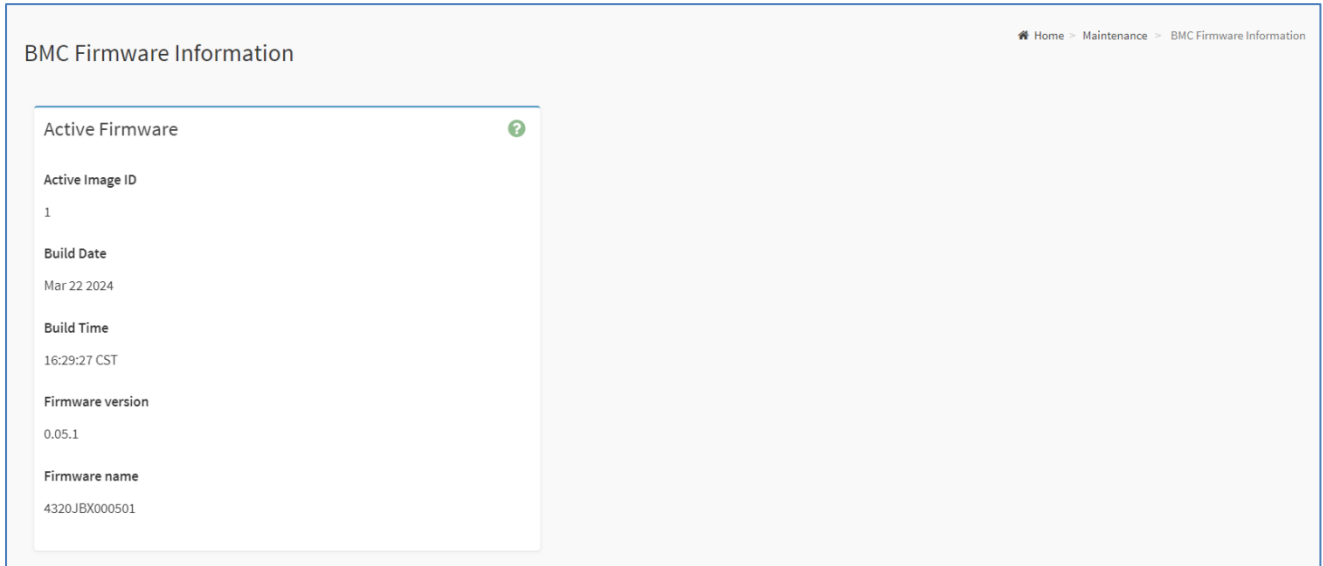
TFTP Image Name: Full Source path with filename of the firmware image is stored on TFTP Server.

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.

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

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 image.

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

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.

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 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.

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.

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.

Home > Maintenance > BMC Firmware Update

BMC Firmware Update

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

Select Firmware Image

Start firmware update

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

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

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

[Edit Preserve Configuration](#)

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

Proceed to Flash

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

BMC Firmware Update Page

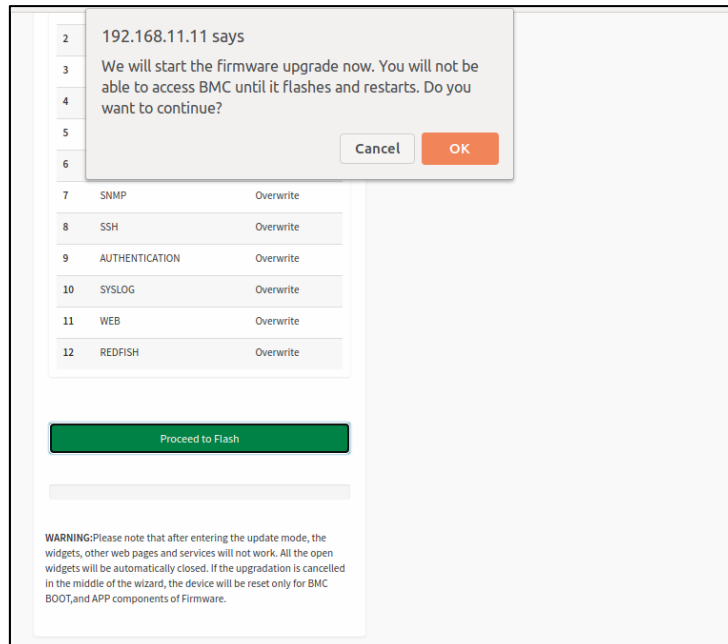
3. Click **Preserve all Configuration** to preserve all configuration.

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

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.*

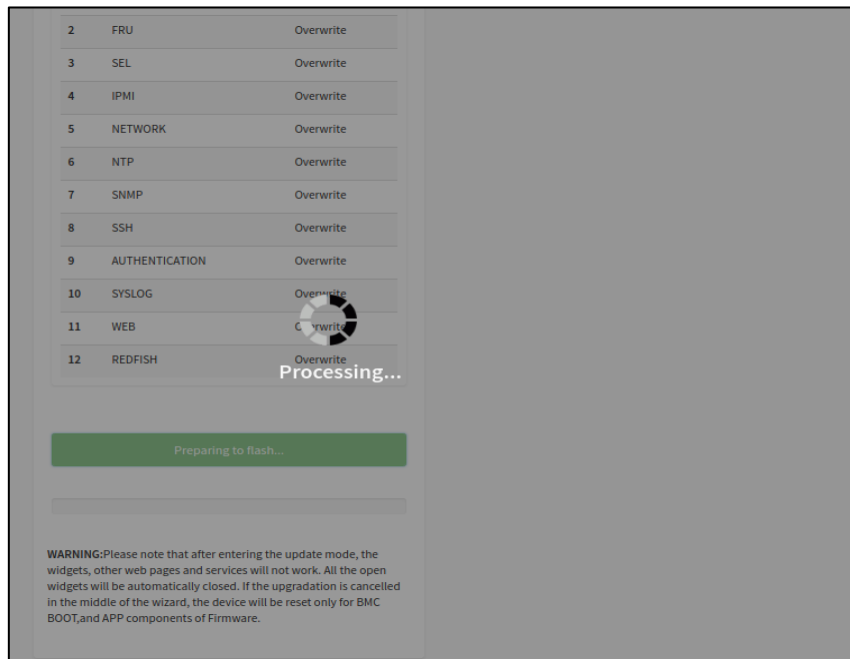
4. Click **Proceed to Flash**, it will prompt you with the warning message. Click **Ok** to start the Firmware update.



BMC 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.

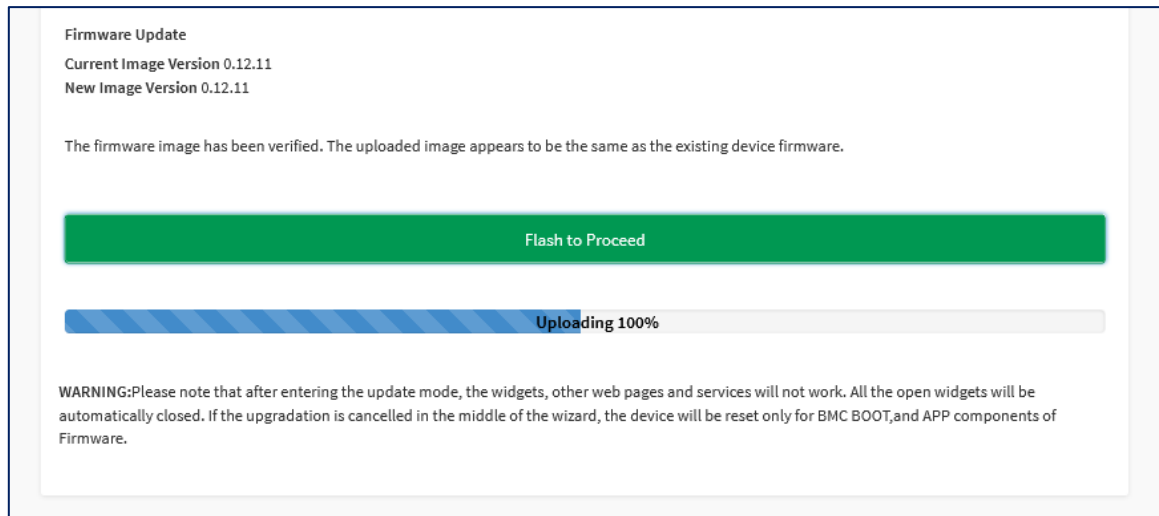
A sample screenshot is shown as below.



BMC Firmware Update - Image Upload Start

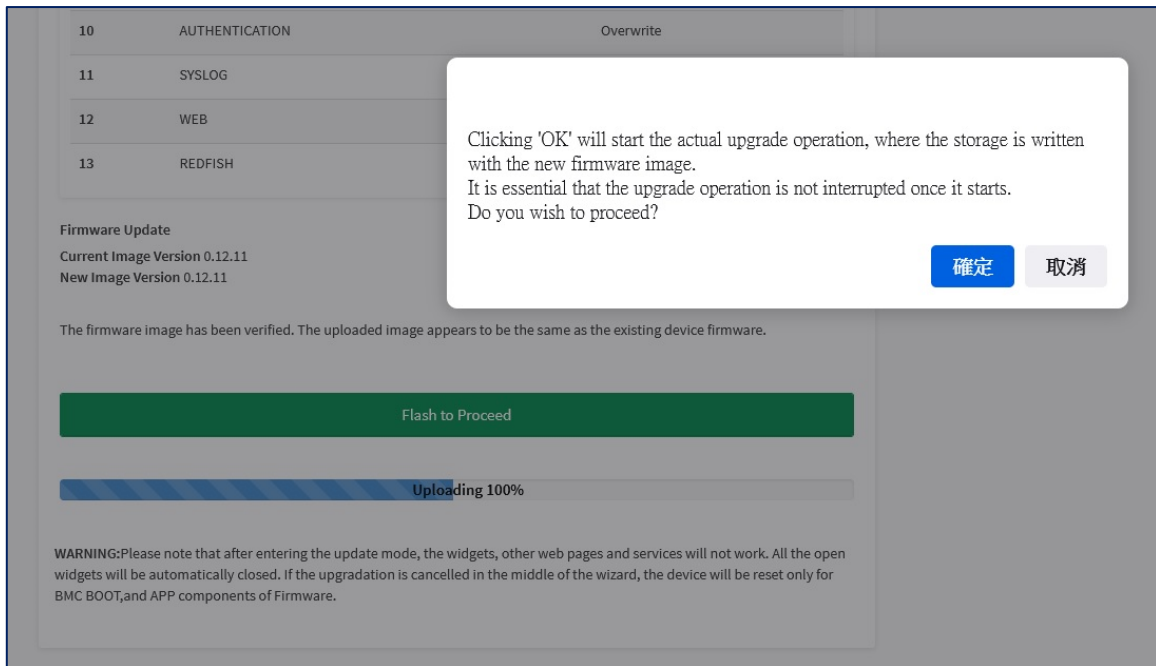
d. Verifying Firmware Image

The firmware update will compare image version. Flashing is Full Flash mode, click **Proceed** to update the firmware.



e. Flashing Firmware Image

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



BMC Firmware Update

Note: The BMC 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 BMC firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

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

Home > Maintenance > Preserve Configuration

Click here to go to [Firmware Update](#) or [Restore Factory Defaults](#)

Check All

SDR

FRU

SEL

IPMI

Network

NTP

SNMP

SSH

Authentication

Syslog

Web

Redfish

Save

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.

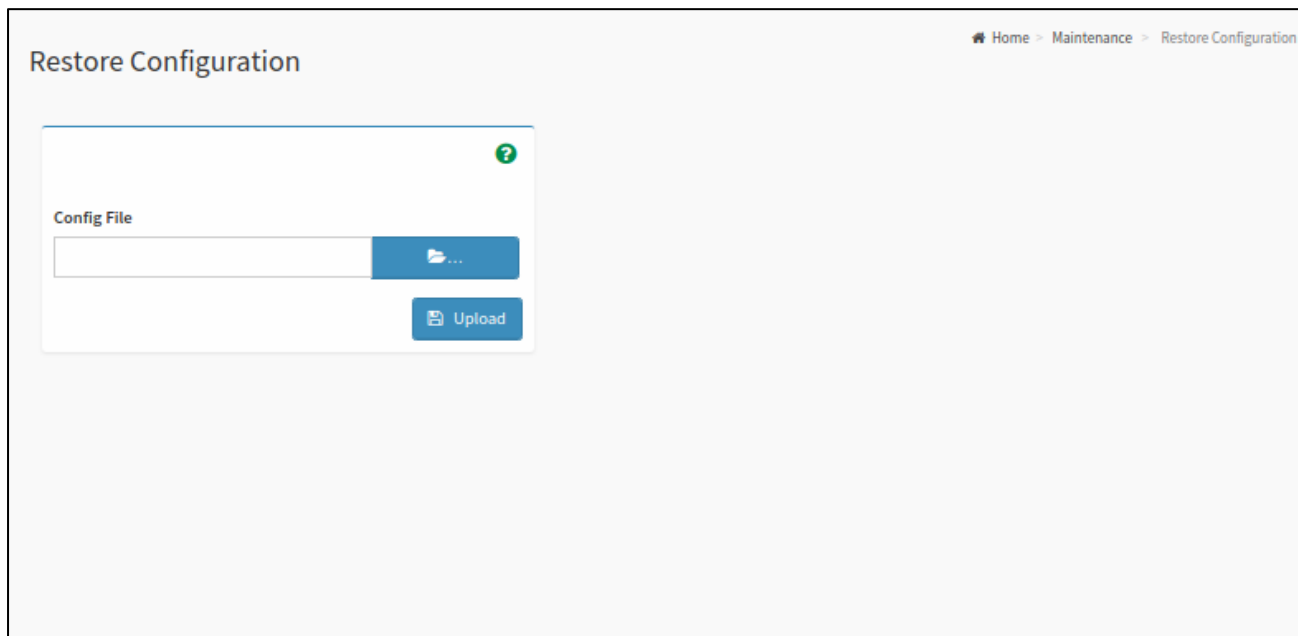
Save: To save any changes made.

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

- **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.

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.

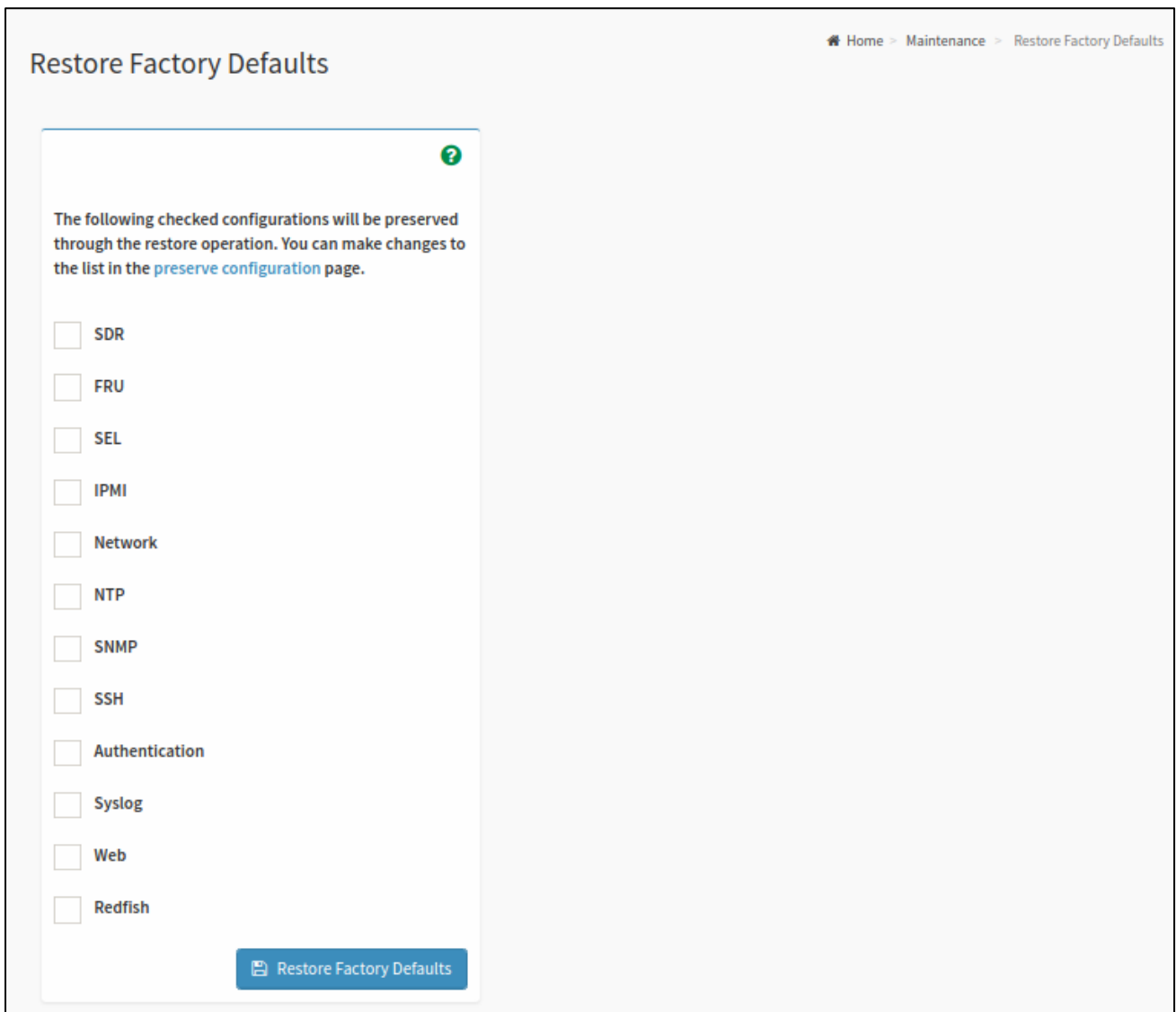
Upload - To upload the backup file to restore the backup files.

Restore Factory Defaults

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

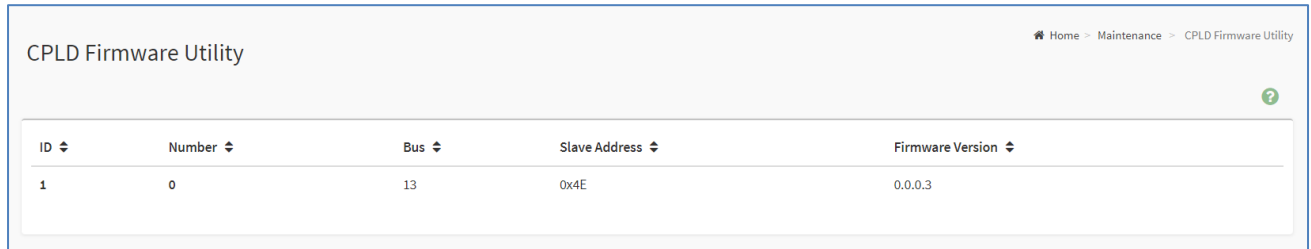
Procedure

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.*

CPLD Firmware Utility

This page shows information like Firmware Version and ID of the CPLD. To open CPLD Firmware Utility page, click **Maintenance > CPLD Firmware Utility** from the menu bar. A screenshot of CPLD Firmware Utility page is given below.



The screenshot shows a web page titled "CPLD Firmware Utility". In the top right corner, there is a breadcrumb trail: "Home > Maintenance > CPLD Firmware Utility". Below the title, there is a table with five columns: "ID", "Number", "Bus", "Slave Address", and "Firmware Version". The table contains one row of data with the following values: ID: 1, Number: 0, Bus: 13, Slave Address: 0x4E, and Firmware Version: 0.0.0.3. A green question mark icon is visible in the top right corner of the table area.

ID	Number	Bus	Slave Address	Firmware Version
1	0	13	0x4E	0.0.0.3

CPLD Firmware Utility

Retimer EEPROM Utility

This page shows information like Firmware Version of the CPLD and update Retimer EEPROM (Configuration). To open Retimer EEPROM Utility page, click **Maintenance > Retimer EEPROM Utility** from the menu bar. A screenshot of Retimer EEPROM Utility page is given below.

Retimer EEPROM Utility Home > Maintenance > Retimer EEPROM Utility

?

ID	Number	Bus	Slave Address	EEPROM Version
6	0	1	0x40	1.03_CV01(0x04)
13	0	1	0x40	1.03_CV01(0x04)
14	1	1	0x40	1.03_CV01(0x04)
15	0	1	0x40	1.03_CV01(0x04)
16	1	1	0x40	1.03_CV01(0x04)

Select Retimer ID

6 - 0 - 1 - 0x40 - 1.03_CV01(0x04)

Select Retimer EEPROM file

選擇檔案 未選擇任何檔案

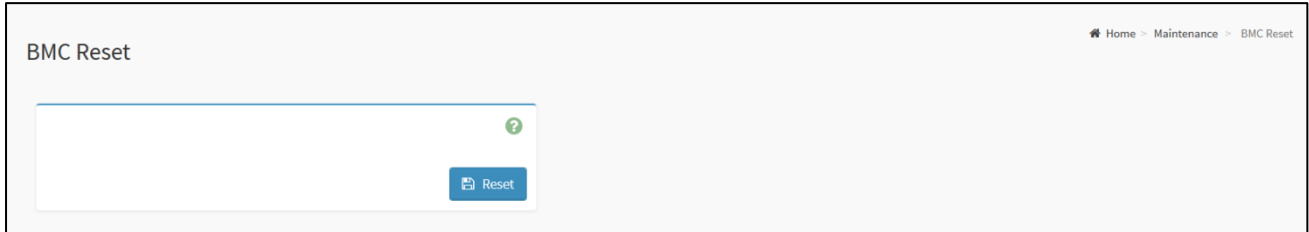
Start Update

Please Select Retimer ID and EEPROM file

Retimer EEPROM Utility

BMC Reset

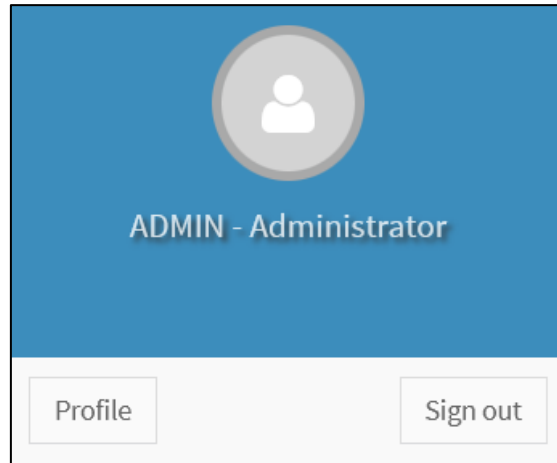
This page is used to reset BMC. To open BMC Reset page, click **Maintenance > BMC Reset** from the menu bar. A sample screenshot of BMC Reset page is shown below.



BMC Reset page

Sign Out

To log out the current user, click the **icon** (👤) on the top right corner of the screen. A sample screenshot is shown below.



Sign out

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