4U18N

Chassis Management Module

USER GUIDE

AST2500, Rev. 1.01

Contents

Figures

Revision History

Revision	Description	Date
1.00	• First Release	January 2023
1.01	• Removed the following feature descriptions due to these features are not supported in the CMM firmware. ▪ Connect to CMM WebUI service with HTTP protocol feature ▪ SSHSOL feature ▪ KCS feature ▪ Keep Share NIC Link Up feature	January 2023

1.0 Introduction

This user guide is written for system administrators and end-users who intend to configure the Intelligence Platform Management Interface (IPMI) settings supported by ASPEED AST2500 Baseboard Management Controller (BMC), which is integrated into the Chassis Management Module (CMM).

This document provides detailed information on configuring the CMM settings supported by the AST2500 controller.

Note: All screenshots in this document are provided for illustrative purposes only and may vary from the actual product.

2.0 CMM Web User Interface Service

The CMM firmware provides an embedded web server that allows users to configure the CMM settings through the Web User Interface (WebUI) service. The detailed information is listed in the following sections.

2.1 CMM WebUI Login URL

CMM WebUI service only supports login the service by URL with HyperText Transfer Protocol Secure (HTTPS) protocol. Users can use the browser that supports the HTTPS protocol to access the CMM WebUI service.

2.1.1 Default CMM URL Address

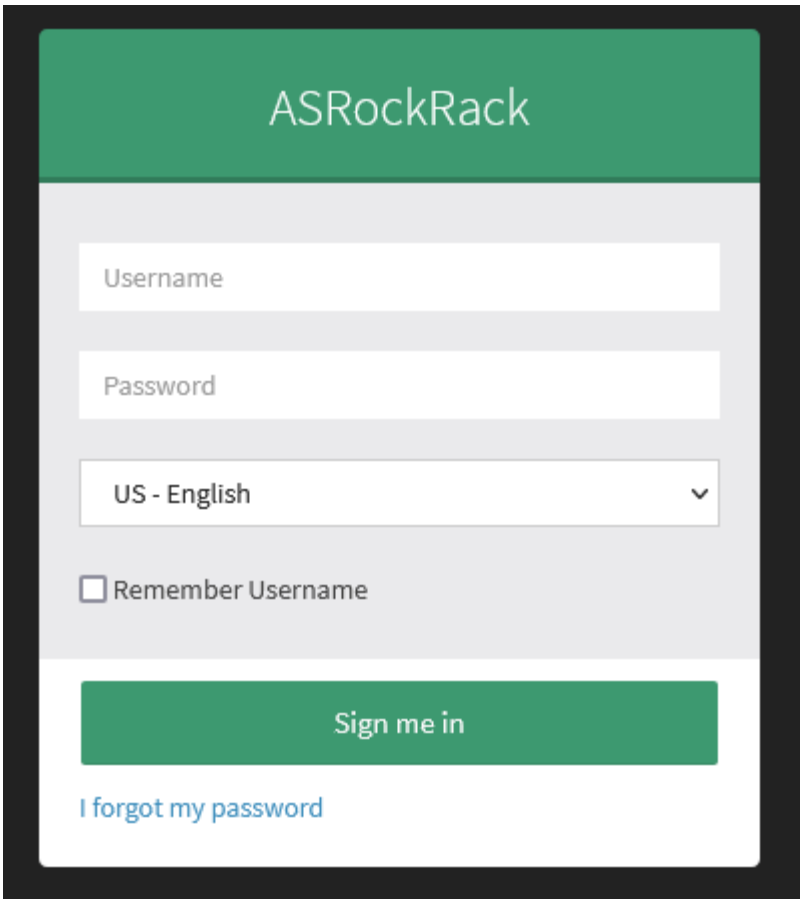
To access the CMM WebUI service by URL, users can use the default URL address as below:

Default URL Address: https://192.168.199.50

2.2 Username and Password

Once users connect to the CMM WebUI service through the browser, the CMM WebUI service login page will display on the browser.

Figure 1. Snapshot of CMM WebUI Service Login Page



The fields description is shown as follows:

- **Username:** Enter the user identifier (UID) of the account to who wants to log in.
- **Password:** Enter the password of the account to which wants to log in.
- **Language Menu:** Changes CMM WebUI supported language.
- **Remember Username:** Check the box if users want to keep the username in the browser settings.
- **Sign me in:** After entering the required credentials, click the **Sign me in** to log in to the CMM WebUI service.
- **I forgot my password:** The user can generate a new password using

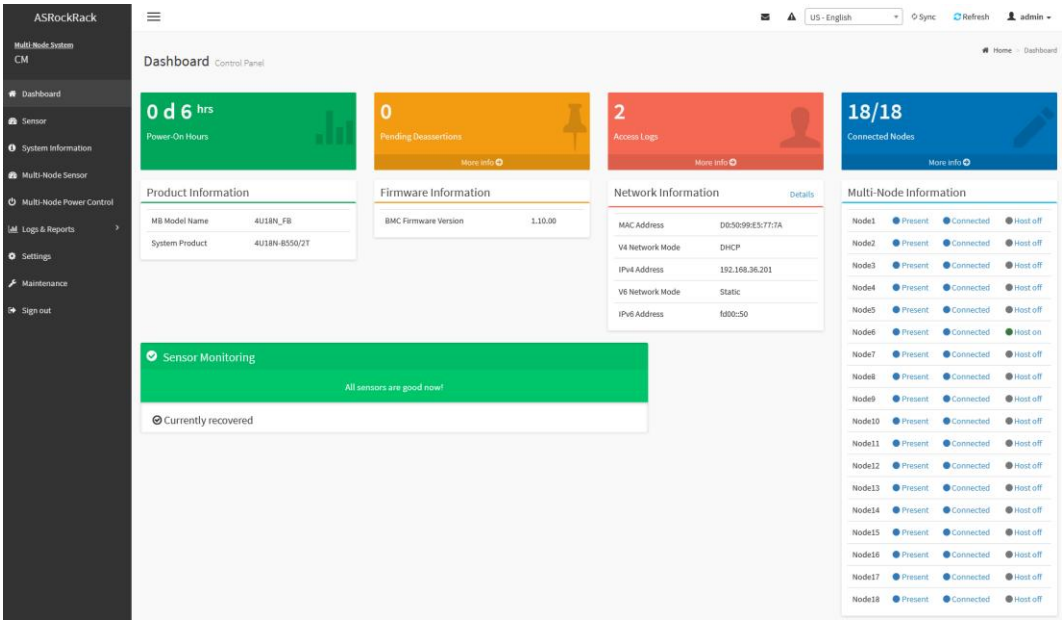
this link if the user forgot the password.

- **Default Username and Password:**
  - **Username:** admin
  - **Password:** admin

2.3 Accessing CMM WebUI Service

The CMM WebUI service consists of various items, including menu, graphics, table, options, and configuration. The detailed information is listed in the following subsections.

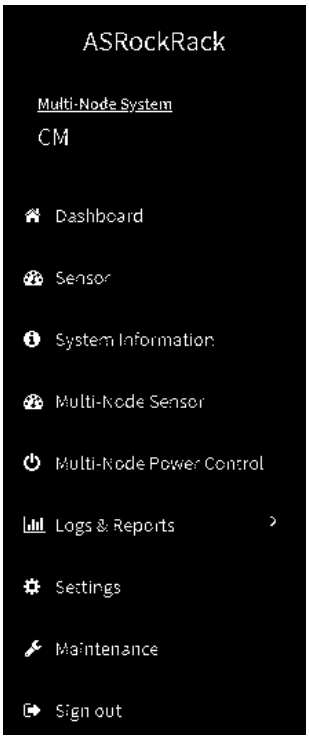
Figure 2. Snapshot of CMM WebUI Service Main Page



2.3.1 Menu Bar

The Menu Bar provides a group of functional feature tabs for users to configure the CMM configuration. The Menu Bar is located on the left side of CMM WebUI.

Figure 3. Snapshot of Menu Bar



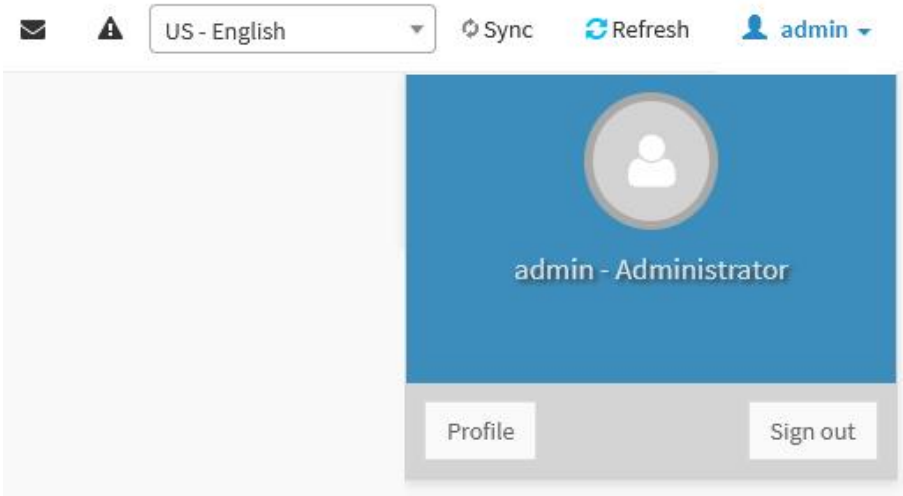
The supported feature tabs are listed in the following:

- **Dashboard**
- **Sensor**
- **System Information**
- **Multi-Node Sensor**
- **Logs and Reports**
  - **IPMI Event Log**
  - **Audit Log**
  - **Debug Log**
- **Settings**
- **Maintenance**
- **Sign Out**

2.3.2 Quick Link and User Information

The Quick Link and User Information are located in the upper right corner of CMM WebUI. It provides various functional feature links for users quickly view the information or change the specific configuration.

Figure 4. Snapshot of Quick Link and User Information



2.3.2.1 Quick Links

The supported Quick Links and their actions are listed in the following:

- **Message:** Click **Message** ( ) Quick Link to quickly view the received event logs or alert messages in the popup window. Click the message listed in the popup window, then navigates to the Logs and Reports page to view the details.
- **Notification:** Click **Notification** ( ) Quick Link to quickly view the received notification in the popup window.
- **Language Menu:** Click **Language Menu** (US - English) to change the supported CMM WebUI language.
- **Sync:** Click **Sync** (Sync) Quick Link to turn on/off the sync feature. Turn on this feature that syncs the latest Sensor and Event Log updates.
- **Refresh:** Click **Refresh** (Refresh) Quick Link to reload current page.

2.3.2.2 User Information

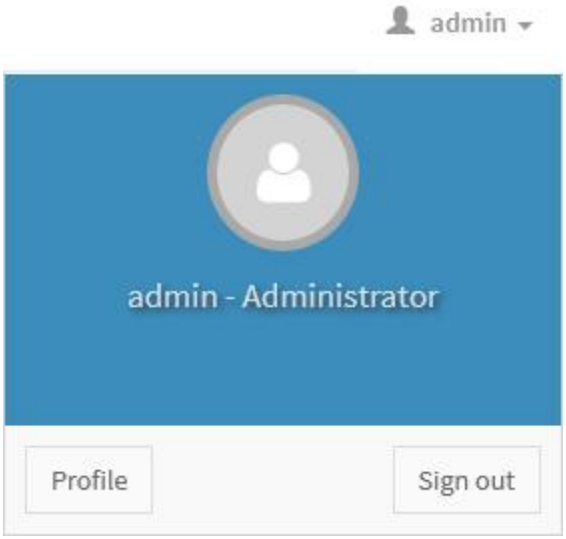
The User Information shows the logged-in user information.

Click **User Information** (admin) Quick Link to show more information on the currently logged-in user. The currently logged-in user's username will show on the Quick Link.

Click the **Profile** button in the popup window, then navigate to the User Management Configuration page of the currently logged-in user.

Click the **Sign out** button in the popup window, and sign out the current session.

Figure 5. Snapshot of User Information and Popup Window



2.3.2.3 User Privilege

CMM WebUI service provides five user privilege levels for the administrator to manage user account privilege. The details in the following:

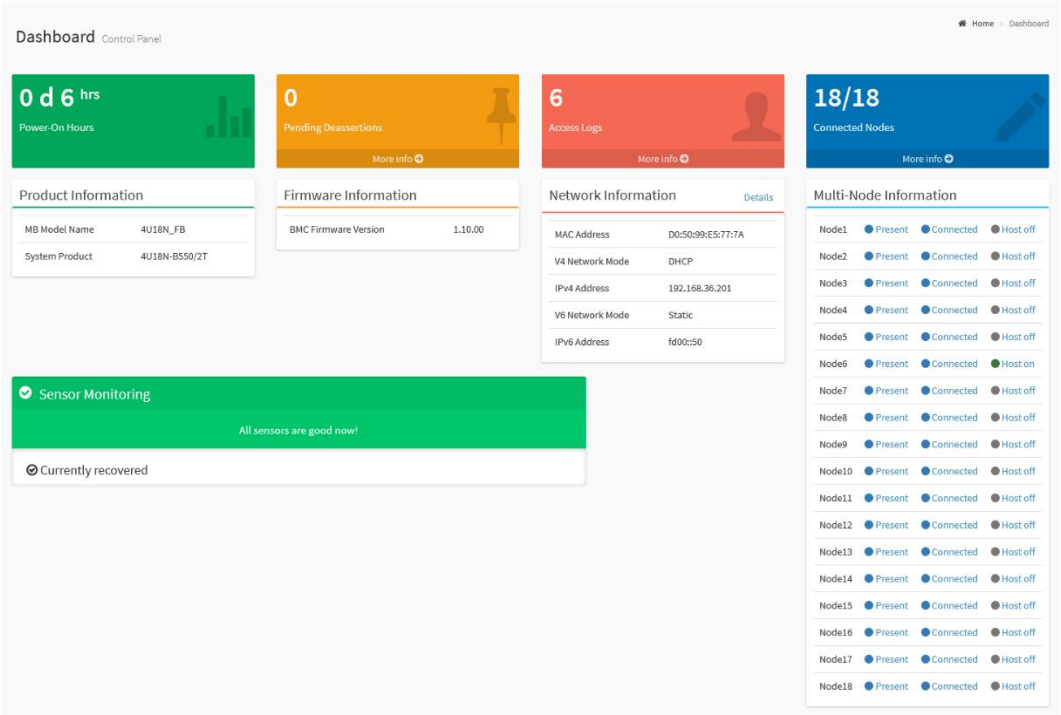
- **None:** Not allow login and access CMM WebUI Service.
- **User:** Only perform the allowed commands.
- **Operator:** All commands are allowed except configuration commands that can change the behavior of the out-of-band interfaces.
- **OEM:** All OEM commands are allowed.
- **Administrator:** All commands are allowed.

2.4 Dashboard

CMM Dashboard provides overall information on system status.

To view the Dashboard page, click the **Dashboard** tab from the menu bar.

Figure 6. Snapshot of Dashboard Page



The items on the Dashboard page are described in the following subsections.

2.4.1 Power-On Hours

It indicates the system power-on time and keeps on accumulating when the system is powered. After flashing a new CMM firmware image, the data of power-on time to be cleared to zero.

2.4.2 Pending Deassertions

It indicates the number of all pending events which are generated by various sensors and waiting for de-asserted.

Click the **More Info** link then navigate to the Event Log page to view all the event logs information.

2.4.3 Access Log

It indicates the number of Access Logs which are generated by users accessing the CMM WebUI.

Click the **More Info** link then navigate to the Audit Log page to view all of the access logs information.

2.4.4 Connected Nodes

It lists the number of current connected nodes.

Click the **More Info** link then navigate to the Multi-Node Information page to view the CMM and all of nodes information.

2.4.5 Product Information

It lists related components' names, such as CMM name, system name, etc.

2.4.6 Firmware Information

It lists the current CMM related firmware version.

2.4.7 Network Information

It lists related network configuration information such as CMM MAC address, IPv4/IPv6 address, IPv4/IPv6 network mode, etc.

Click the **Details** link then navigate to the **Network IP Settings** page to view more network configuration information or configure network settings.

2.4.8 Multi-Node Information

It lists the status of each node, including Present state, Connected state and Node Power state.

2.4.9 Sensor Monitoring

It lists all the critical sensors on the system.

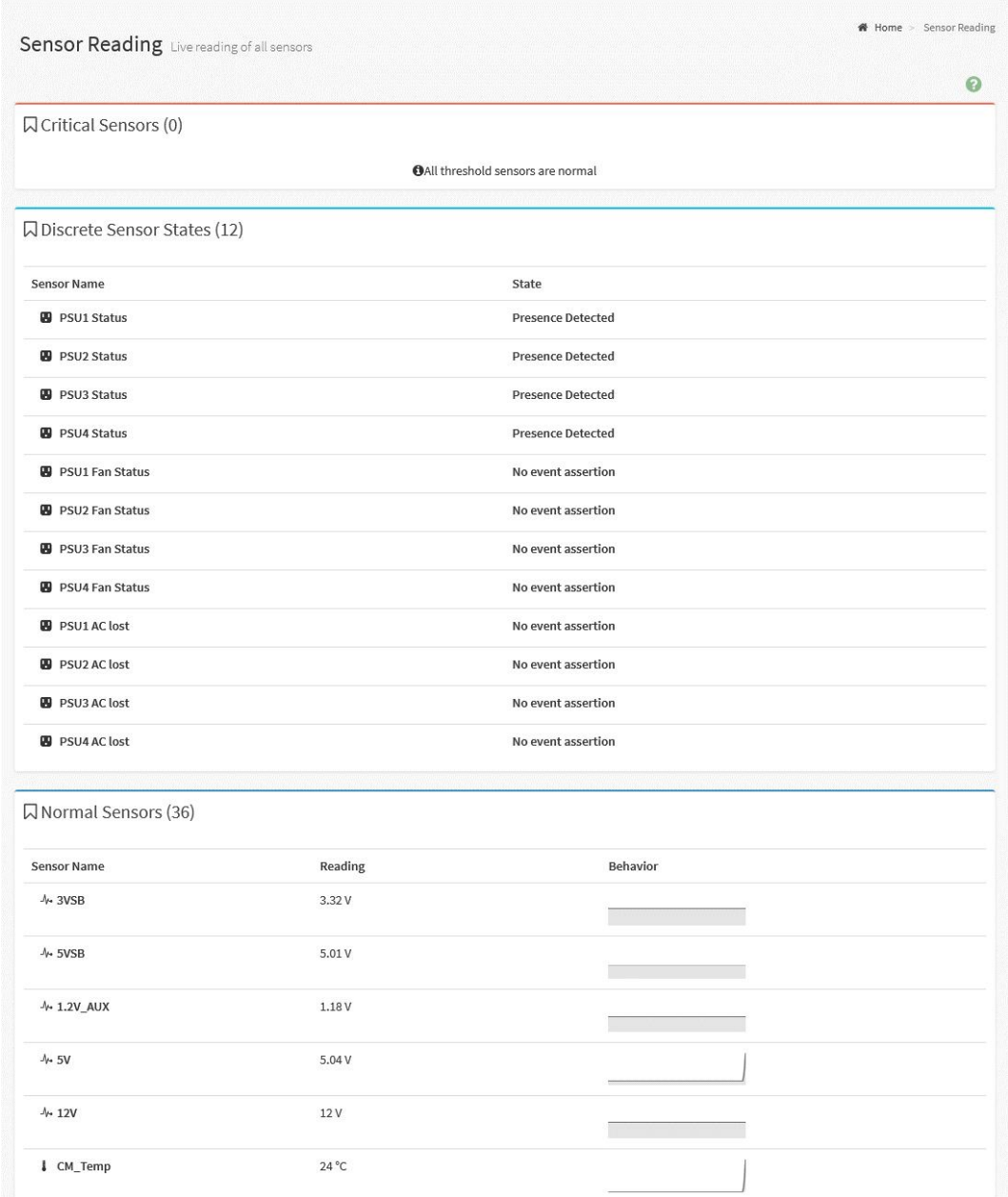
Click the listed critical sensor, then navigate to the Sensor detail page to view all information on the selected sensor.

2.5 Sensor

The Sensor Reading page provides related information on all sensors in the system.

To view the Sensor Reading page, click the **Sensor** tab from the menu bar.

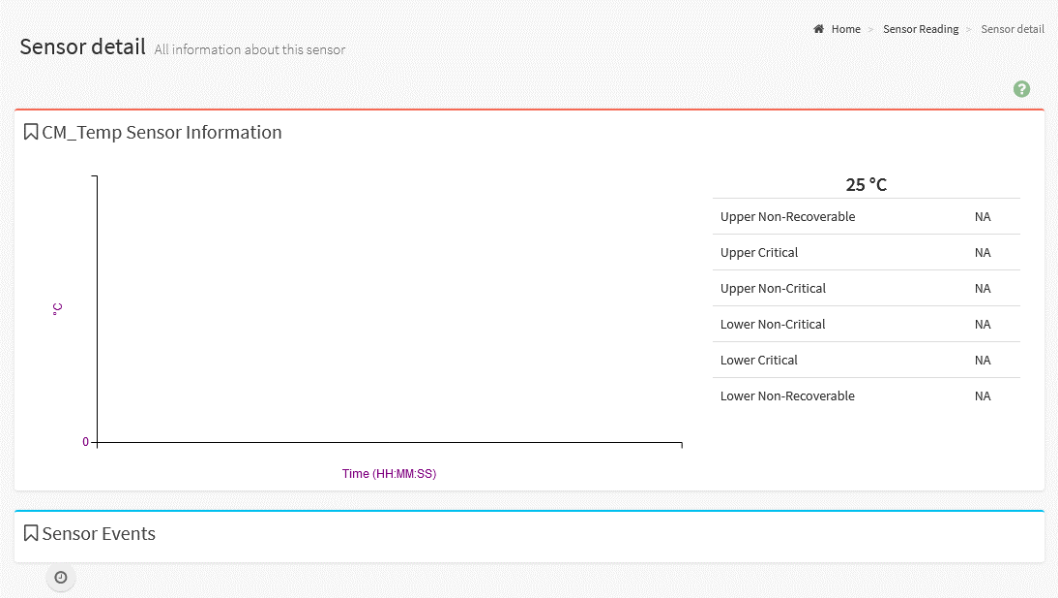
Figure 7. Snapshot of Sensor Reading Page



2.5.1 Sensor Detail

Click on the specific sensor from the Sensor Reading page then navigate to the Sensor detail page to view more information about the selected sensor, including sensor threshold values, events and graphical representation.

Figure 8. Snapshot of Sensor Detail Page



There are six types of threshold values are listed on the page:

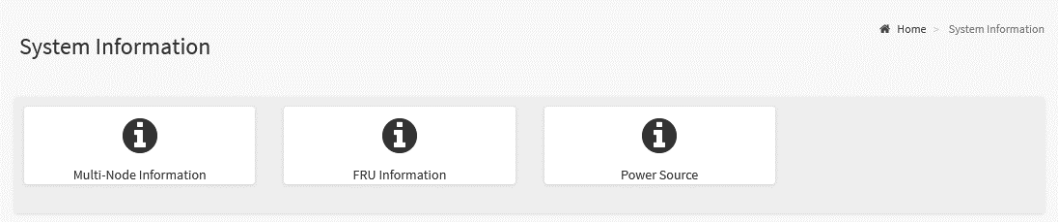
- **Upper Non-Recoverable (UNR)**
- **Upper Critical (UC)**
- **Upper Non-Critical (UNC)**
- **Lower Non-Critical (LNC)**
- **Lower Critical (LC)**
- **Lower Non-Recoverable (LNR)**

The event triggered by the selected sensor will be listed in the Sensor Events group.

2.6 System Information

System Information page provides devices information of the system, including Multi-Node Information, FRU Information and Power Source information.

Figure 9. Snapshot of System Information Page

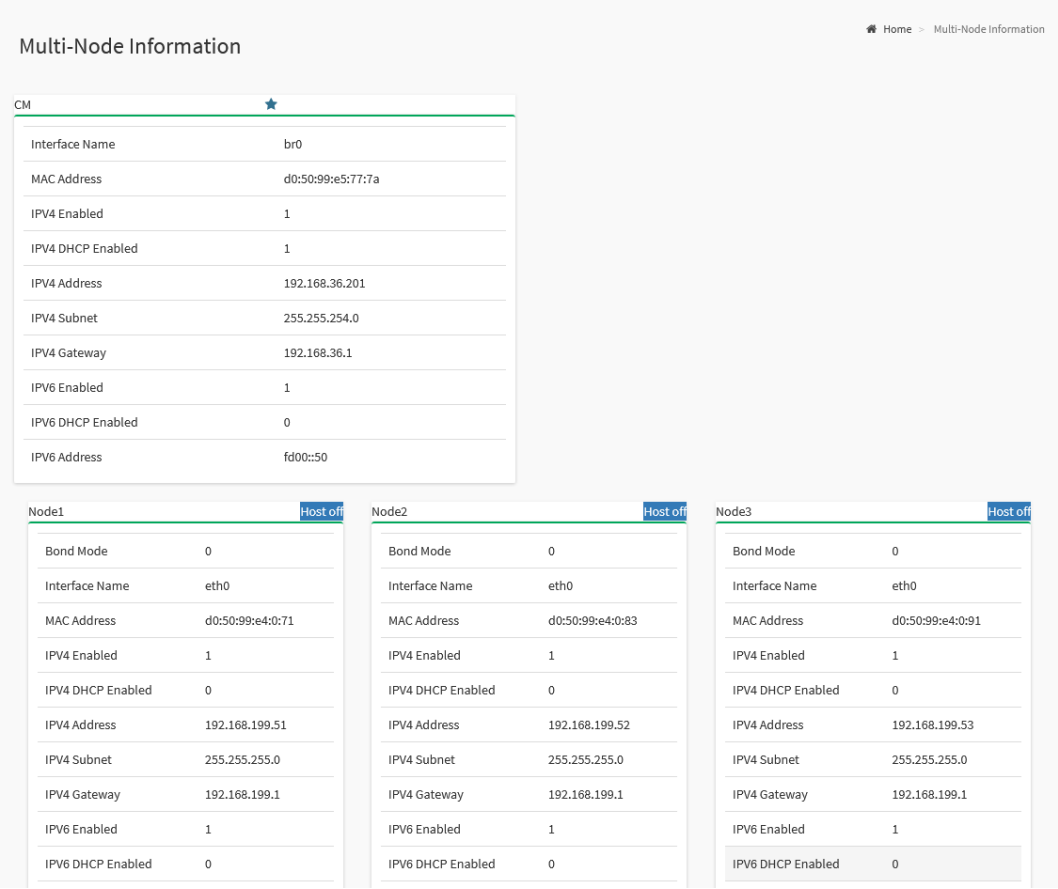


The details about each feature are listed in the following.

2.6.1 Multi-Node Information

Multi-Node Information page provides the information of CMM and each node includes

Figure 10. Snapshot of Multi-Node Information Page



The fields on the Multi-Node Information page includes

- **CM Information**
  - **Interface Name**
  - **MAC Address**
  - **IPV4 Enabled**
  - **IPV4 DHCP Enabled**
  - **IPV4 Address**
  - **IPV4 Subnet**
  - **IPV4 Gateway**
  - **IPV6 Enabled**

- **IPV6 DHCP Enabled**
- **IPV6 Address**

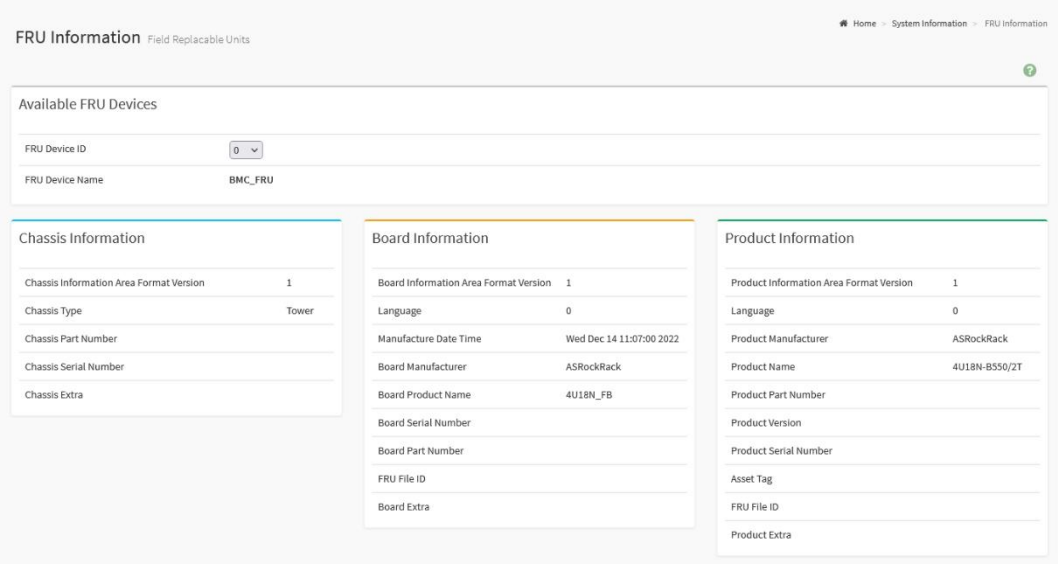
- **Node Information**
  - **Power State (Host off or Host on)**
  - **Bond Mode**
  - **Interface Name**
  - **MAC Address**
  - **IPV4 Enabled**
  - **IPV4 DHCP Enabled**
  - **IPV4 Address**
  - **IPV4 Subnet**
  - **IPV4 Gateway**
  - **IPV6 Enabled**
  - **IPV6 DHCP Enabled**
  - **IPV6 Address**

2.6.2 FRU Information

FRU Information page provides various information on CMM FRU devices. Three types of information are listed on the FRU Information page includes Chassis Information, Board Information, and Product Information.

To view the FRU Information page, click the **FRU Information** tab from the System Information page

Figure 11. Snapshot of FRU Information Page



The fields on the FRU Information page includes

- **Available FRU Devices**
  - **FRU Device ID**
  - **FRU Device Name**
- **Chassis Information**
- **Board Information**
- **Product Information**

2.6.2.1 Chassis Information

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

2.6.2.2 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**

2.6.2.3 Product Information

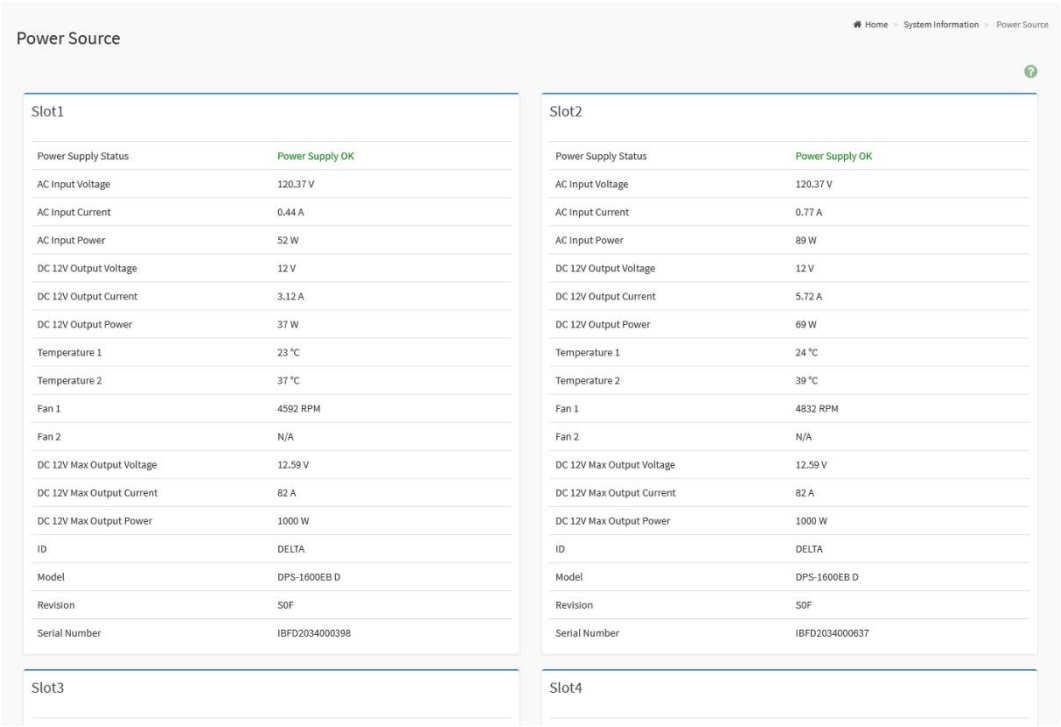
- **Product Information Area Format Version**
- **Language**
- **Product Manufacturer**
- **Product Name**
- **Product Part Number**
- **Product Version**
- **Product Serial Number**
- **Asset Tag**
- **FRU File ID**
- **Product Extra**

2.6.3 Power Source

Power Source page provides various information about each system Power Supply Unit (PSU) installed in the host.

To view the Power Source page, click the **Power Source** tab from the System Information page.

Figure 12. Snapshot of Power Source Page



The fields on the Power Source page includes

- **Power Supply Status**
- **AC Input Voltage**
- **AC Input Current**
- **AC Input Power**
- **DC 12V Output Voltage**
- **DC 12V Output Current**
- **DC 12V Output Power**
- **Temperature 1**
- **Temperature 2**

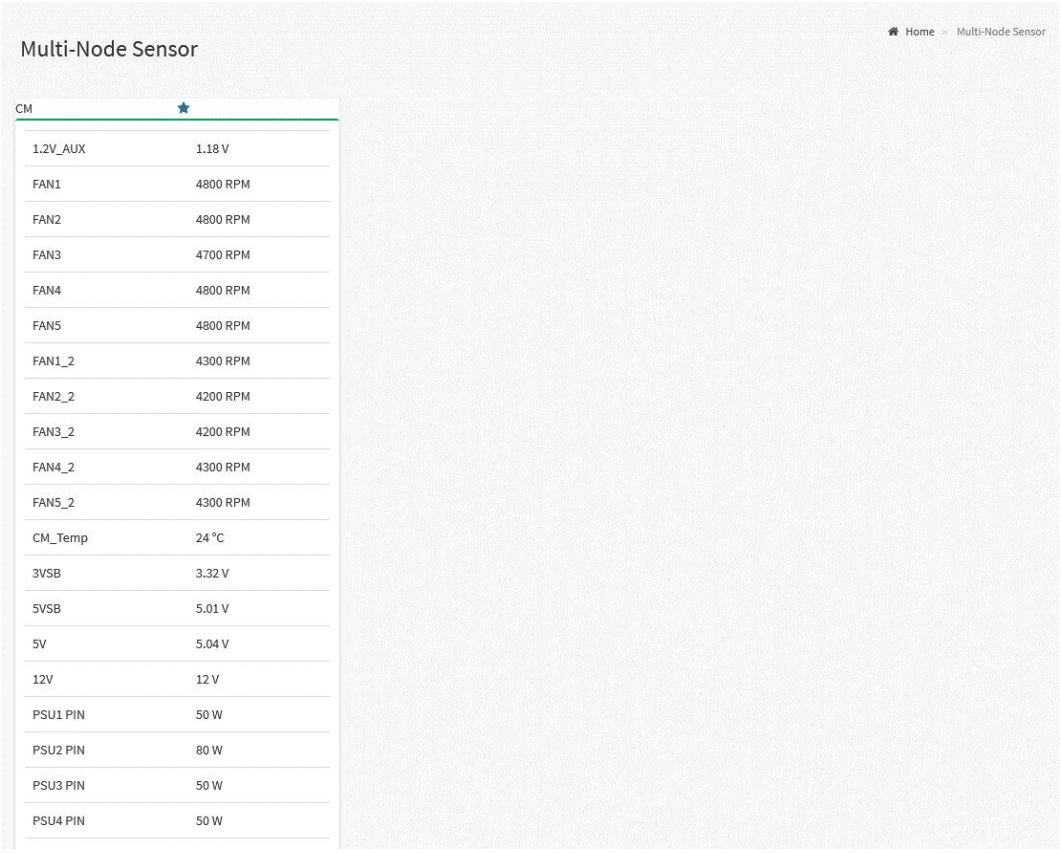
- **Fan 1**
- **Fan 2**
- **DC 12V Max Output Voltage**
- **DC 12V Max Output Current**
- **DC 12V Max Output Power**
- **ID**
- **Model**
- **Revision**
- **Serial Number**

2.7 Multi-Node Sensor

Multi-Node Sensor page provides various information about each sensor located on the CMM or the Node.

To view the Multi-Node Sensor page, click the **Multi-Node Sensor** tab from the menu bar.

Figure 13. Snapshot of Multi-Node Sensor Page



The fields on the Multi-Node Sensor page includes

- **CM Sensor**
  - **1.2V_AUX**
  - **FAN1**
  - **FAN2**
  - **FAN3**
  - **FAN4**
  - **FAN5**

- **FAN1_2**
- **FAN2_2**
- **FAN3_2**
- **FAN4_2**
- **FAN5_2**
- **CM_Temp**
- **3VSB**
- **5VSB**
- **5V**
- **12V**
- **PSU1 PIN**
- **PSU2 PIN**
- **PSU3 PIN**
- **PSU4 PIN**
- **PSU1 POUT**
- **PSU2 POUT**
- **PSU3 POUT**
- **PSU4 POUT**
- **PSU1 Temp**
- **PSU2 Temp**
- **PSU3 Temp**
- **PSU4 Temp**
- **PSU1 VIN**
- **PSU2 VIN**
- **PSU3 VIN**
- **PSU4 VIN**
- **PSU1 IOUT**
- **PSU2 IOUT**
- **PSU3 IOUT**
- **PSU4 IOUT**

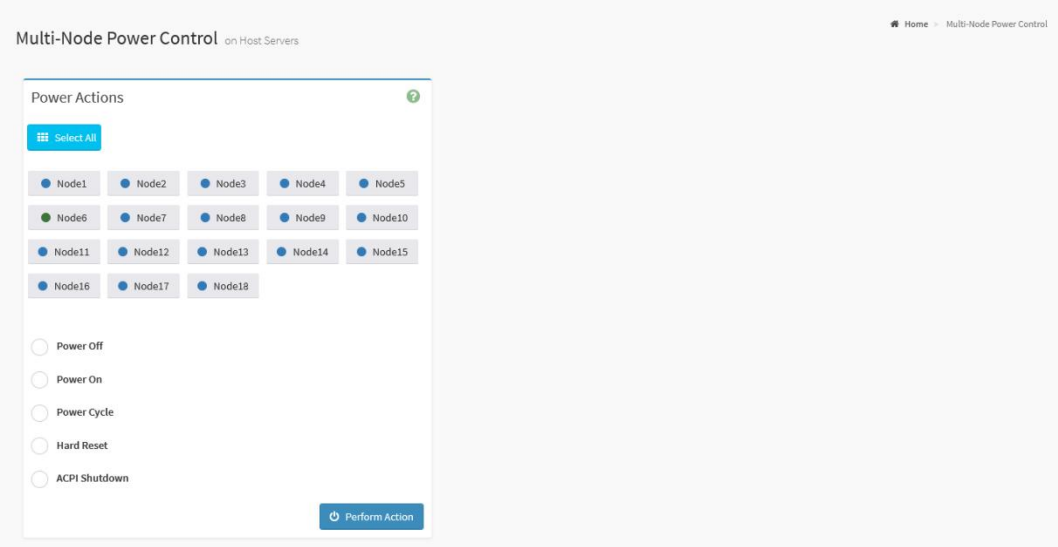
- **Node Sensor**
  - **Power State (Host off or Host on)**
  - **3VSB**
  - **5VSB**
  - **VCPU**

- **VSOC**
- **VCCM**
- **APU_VDDP**
- **1.05V_PROM_S5**
- **2.5V_PROM**
- **1.05V_PROM_RUN**
- **BAT**
- **3V**
- **5V**
- **12V**
- **MB Temp**
- **Card Side Temp**
- **CPU Temp**
- **DDR4_A1_Temp**
- **DDR4_A2_Temp**
- **DDR4_B1_Temp**
- **DDR4_B2_Temp**

2.8 Multi-Node Power Control

Multi-Node Power Control page provides the feature that users can control the power state of multi-node on the WebUI service.

Figure 14. Snapshot of Multi-Node Power Control Page



The fields on the Multi-Node Power Control page includes

- **Select All (Select All):** Click this button to select all nodes or deselected all nodes.
- **Node 1 ~ Node 18:** Indicates power state of the node.
  - **Node with blue indicator means the node is Power Off (Node1)**
  - **Node with green indicator means the node is Power On (Node6)**
- **Power Off:** Click this option to perform Power-Off on selected node.
- **Power On:** Click this option to perform Power-On on selected node.
- **Power Cycle:** Click this option to perform Power Cycle on selected node.
- **Hard Reset:** Click this option to perform Hard Reset on selected node.
- **ACPI Shutdown:** Click this option to perform ACPI Shutdown on selected node.
- **Perform Action (Perform Action):** Click this button to perform the power state action on selected node.

2.9 Logs & Reports

Logs & Reports provides various functional features for users to audit the logs triggered by multiple devices or conditions.

Supported features are listed in the following subsections including

- **IPMI Event Log**
- **Audit Log**
- **Debug Log**

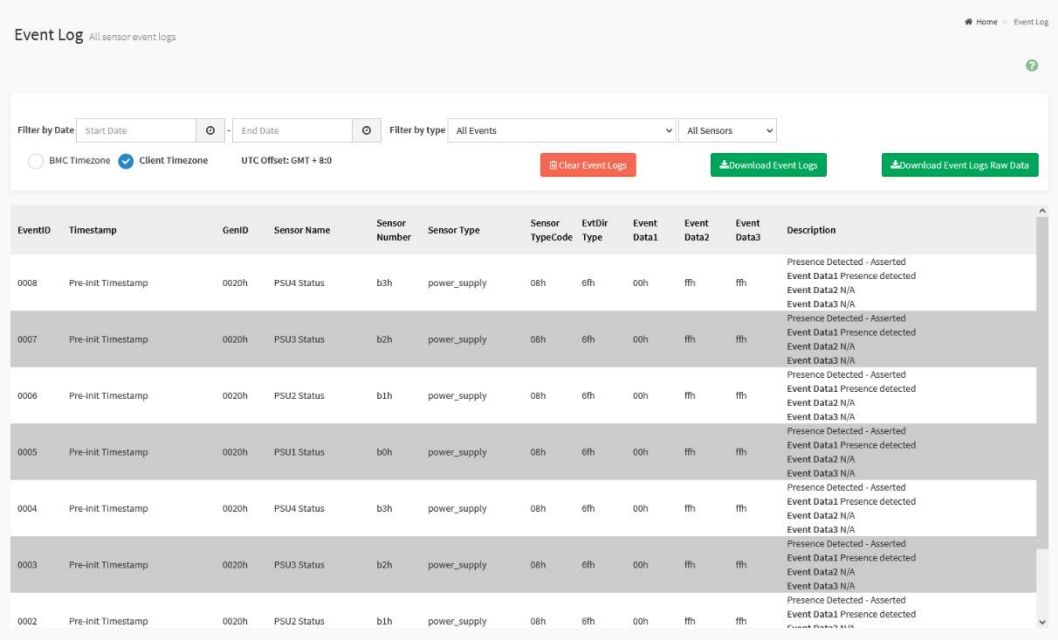
The **Logs & Reports** tab is located at the menu bar, click **Log & Reports** tab to expand all the supported features tabs.

2.9.1 IPMI Event Log

IPMI Event Log page provides various event logs information which is generated by different sensors for users to monitor system status.

To view the IPMI Event Log page, click **Logs & Reports** tab from the menu bar to expand the sub-menu bar, then click the **IPMI Event Log** tab from the sub-menu bar.

Figure 15. Snapshot of IPMI Event Log Page



The fields on the IPMI Event Log page include:

- **Filter by Date:** Filter the records by specific Start Date and End Date using Calendar.
- **Filter by Type:** Filter the records by specific Event Type and Sensor Type.
- **BMC and Client Time Zone:** Select either one to switch the current UTC offset value. The timestamp value will be updated when the option has been changed.
- **UTC Offset:** Display the current UTC Offset value.
- **Clear Event Logs:** Click the **Clear Event Logs** button to clear the records.

- **Download Event Logs:** Click the **Download Event Logs** button to download all records information with the specific data format.
- **Download Event Logs Raw Data:** Click the **Download Event Logs** button to download all records information in the raw data format.

The information listed on the page includes

- **EventID**
- **Timestamp**
- **Severity**
- **GenID**
- **Sensor Name**
- **Sensor Number**
- **Sensor Type**
- **Sensor TypeCode**
- **EvtDir Type**
- **Event Data1**
- **Event Data2**
- **Event Data3**
- **Description**

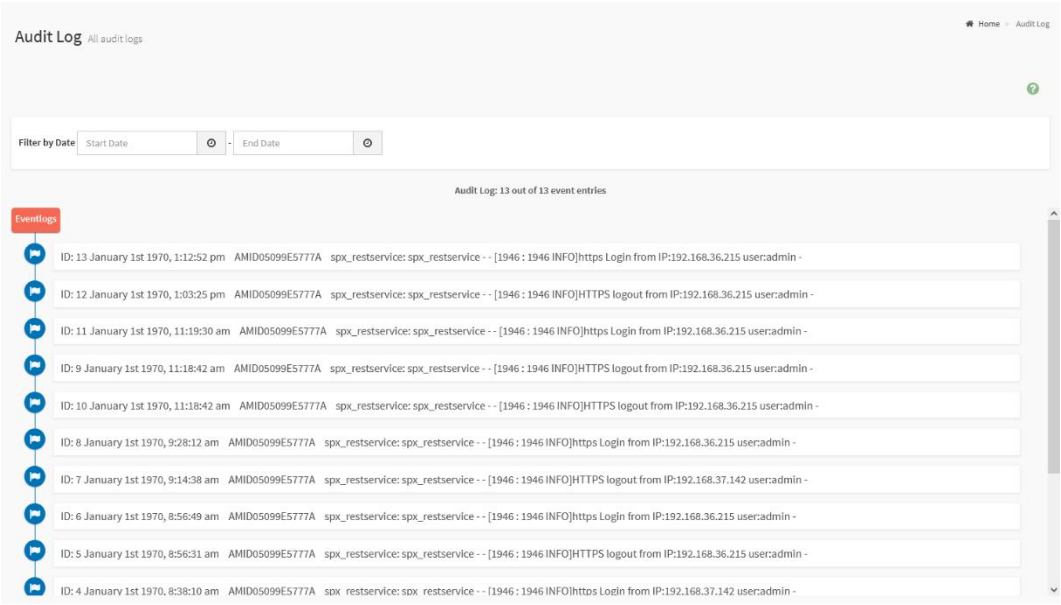
2.9.2 Audit Log

Audit Log page provides user login information log for users to monitor the CMM WebUI access.

To view the Audit Log page, click **Logs & Reports** tab from the menu bar to expand the sub-menu bar, then click the **Audit Log** tab from the sub-menu bar.

Note: To configure this feature, users can view the Advanced Log Settings page. Click the **Settings** -> **Log Settings** -> **Advanced Log Settings** tab from the menu bar

Figure 16. Snapshot of Audit Log Page



The fields on the Audit Log page include

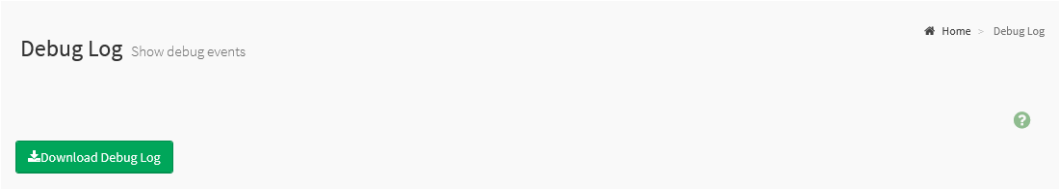
- **Filter by Date:** Filter the records by specific Start Date and End Date using Calendar.

2.9.3 Debug Log

Debug Log page provides the feature that downloads the debug log file, which for users to download all debug logs stored in the CMM system and diagnostics the CMM status.

To view the Debug Log page, click **Logs & Reports** tab from the menu bar to expand the sub-menu bar, then click the **Debug Log** tab from the sub-menu bar.

Figure 17. Snapshot of Debug Log Page



The fields on the Debug Log page include

- **Download Debug Log:** Click the **Download Debug Log** to save all CMM system debug logs.

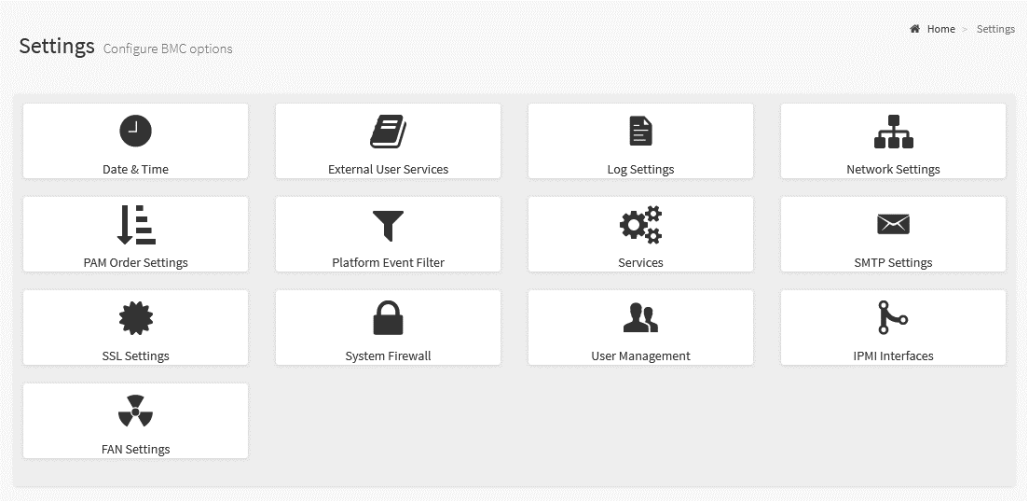
2.10 Settings

Settings page provides various functional features for users to configure all the CMM supports services, including

- **Date & Time**
- **External User Services**
- **Log Settings**
- **Network Settings**
- **PAM Order Settings**
- **Platform Event Filter**
- **Services**
- **SMTP Settings**
- **SSL Settings**
- **System Firewall**
- **User Management**
- **IPMI Interface**
- **FAN Settings**

To view the Settings page, click the **Settings** tab from the menu bar.

Figure 18. Snapshot of Settings Page



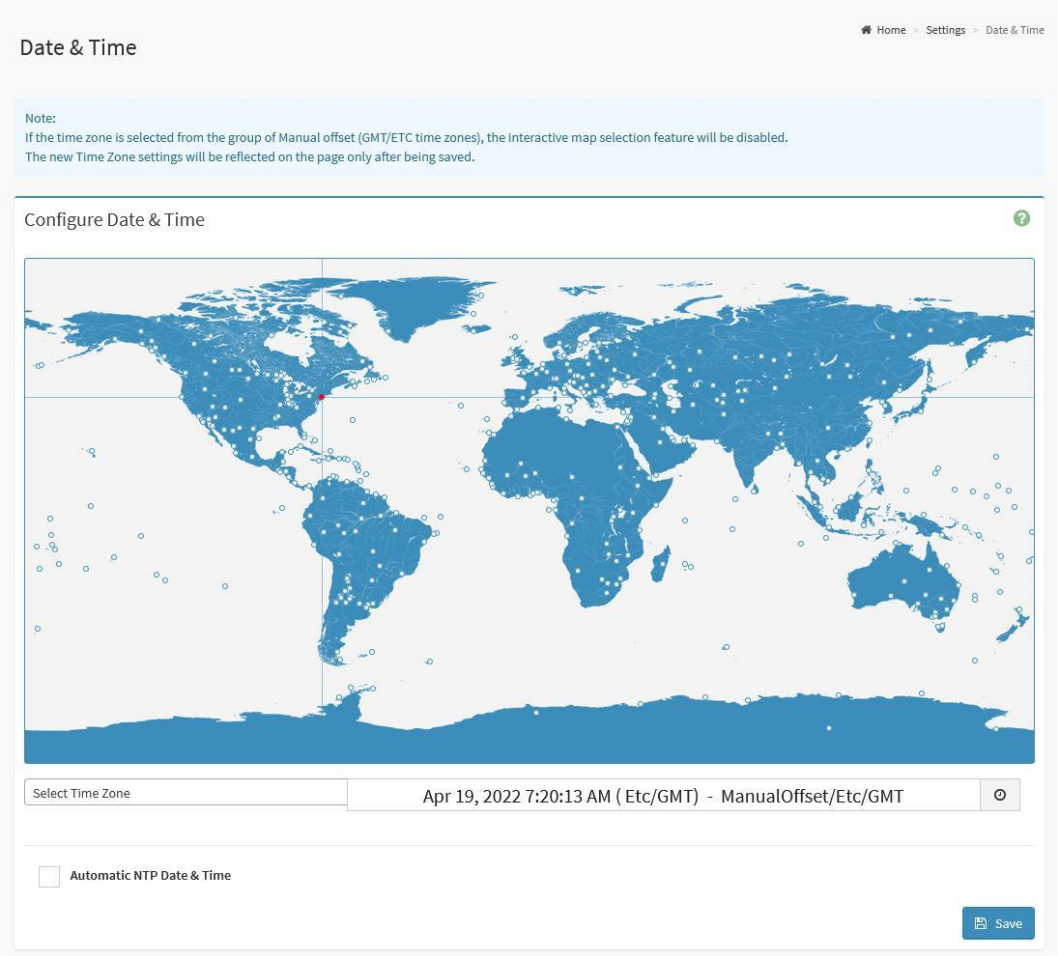
The details about each feature are listed in the following subsections.

2.10.1 Date & Time

Date & Time page provides the various configuration for users to configure the date and time on the CMM.

To view the Date & Time page, click the **Settings** -> **Date & Time** tab from the menu bar.

Figure 19. Snapshot of Date & Time Page



The fields on the Date & Time page include

- **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 CMM.

- **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.
- **Clock:** Click the **Clock** icon (⚙) to manually modify the Date and Time.
- **Save:** To save the configured 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.

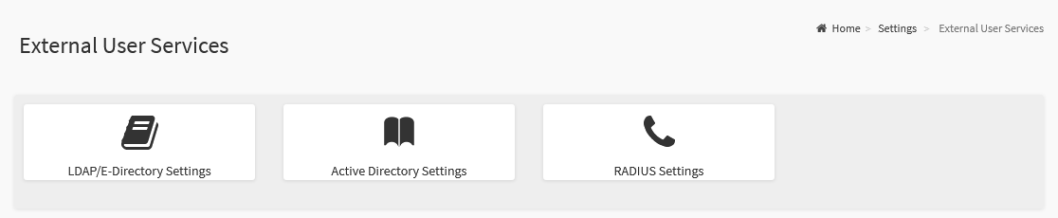
2.10.2 External User Services

External User Services page provides three functional feature tabs for users to configure the external user services, including

- **LDAP/E-Directory Settings**
- **Active Directory Settings**
- **RADIUS Settings**

To view the External User Services page, click the **Settings** -> **External User Services** tab from the menu bar.

Figure 20. Snapshot of External User Services Page



The details about each feature are listed in the following subsections.

2.10.2.1 LDAP/E-Directory Settings

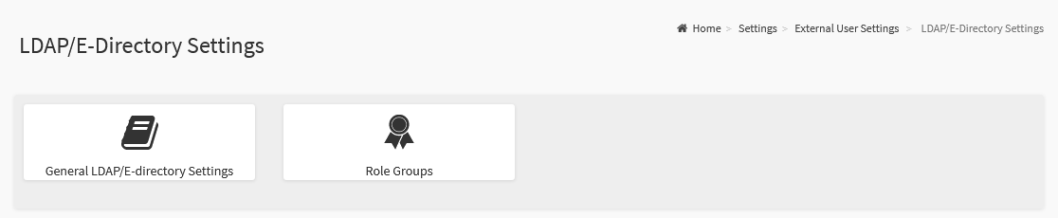
The Lightweight Directory Access Protocol (LDAP)/E-Directory is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

LDAP/E-Directory Settings page provides two functional feature tabs for users to configure the LDAP settings, including

- **General LDAP/E-directory Settings**
- **Role Groups**

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

Figure 21. Snapshot of LDAP/E-Directory Settings Page



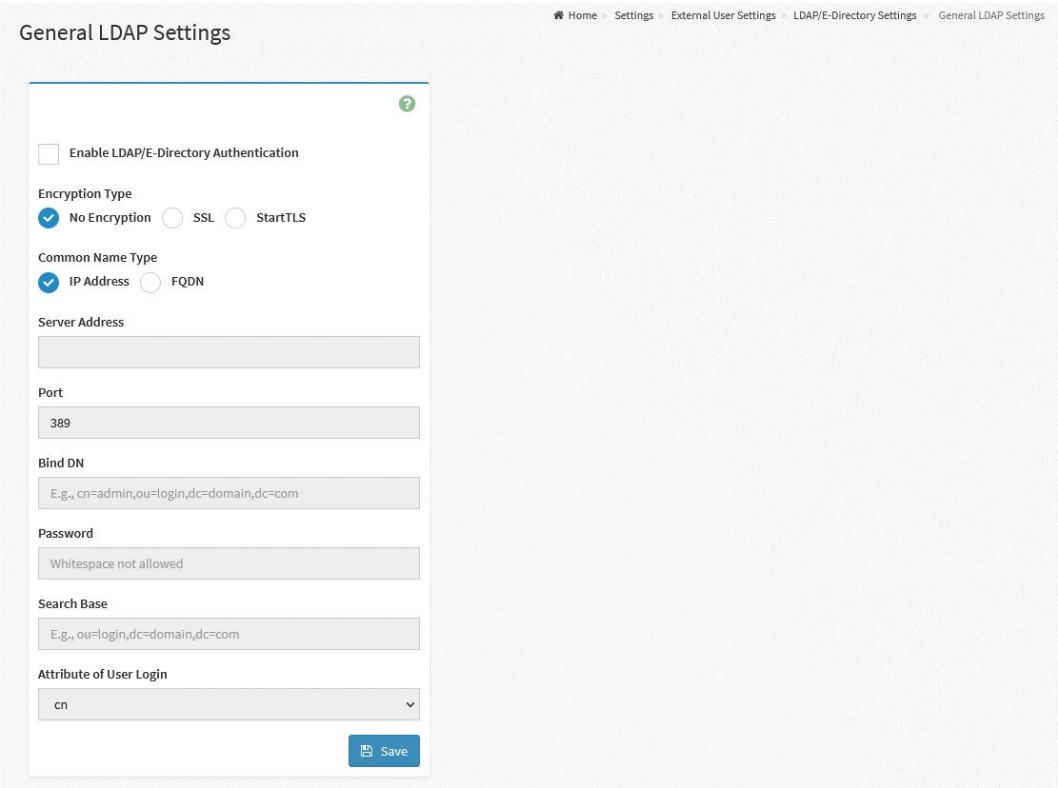
The details about each feature are listed in the following.

2.10.2.1.1 General LDAP/E-Directory Settings

This page provides various options for users to configure the LDAP/E-Directory Settings.

To view the General LDAP/E-Directory Settings page, click the **Settings** -> **External User Services** -> **LDAP/E-Directory Settings** -> **General LDAP/E-Directory Settings** tab from the menu bar.

Figure 22. Snapshot of General LDAP/E-Directory Settings Page



The fields on the General LDAP/E-Directory Settings page include

- **Enable LDAP/E-Directory Authentication:** Click this option to enable LADP/E-Directory Settings.
- **Encryption Type:** Select the encryption type for LDAP/E-Directory.
  - **No Encryption**
  - **SSL**
  - **StartTLS**
- **Common Name Type:** Select the Common Name Type.
  - **IP Address**

- **FQDN**

- **Server Address:** Enter the LDAP/E-Directory server address, IPv4 and IPv6 address format are supported.

  Note: Enter a FQDN address if using StartTLS with FQDN.
- **Port:** Specify the LDAP/E-Directory Port.
- **Bind DN:** The Bind DN is used in bind operations, which authenticates the client to the server.
- **Password:** The Bind password is also used in the bind authentication operations between client and server.
- **Search Base:** The Search Base allows the LDAP/E-Directory server to find which part of the external directory tree is to be searched
- **Attribute of User Login:** The Attribute of User Login field indicates to the LDAP/E-Directory server which attribute should be used to identify the user.

  Note: It only supports cn or uid.
- **CA certificate file:** Select CA Certificate File from the Browse field to identify the certificate of the trusted CA certs.
- **Certificate File:** Select the Certificate File to find the client certificate filename.
- **Private Key:** Select Private Key to find the client private key filename.
- **Save:** To save the configured settings.

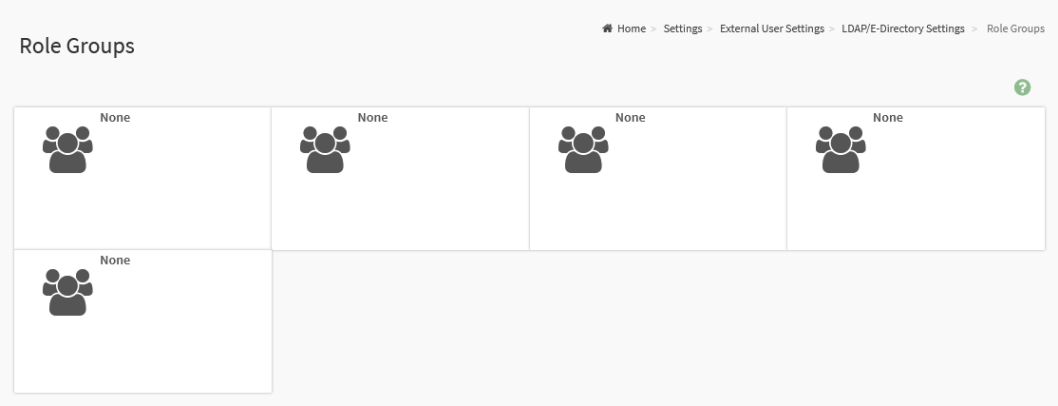
Note: **CA certificate file**, **Certificate File** and **Private Key** are required, when SSL or StartTLS is enabled.

2.10.2.1.2 Role Groups

This page provides the feature for users to add a new group to the device.

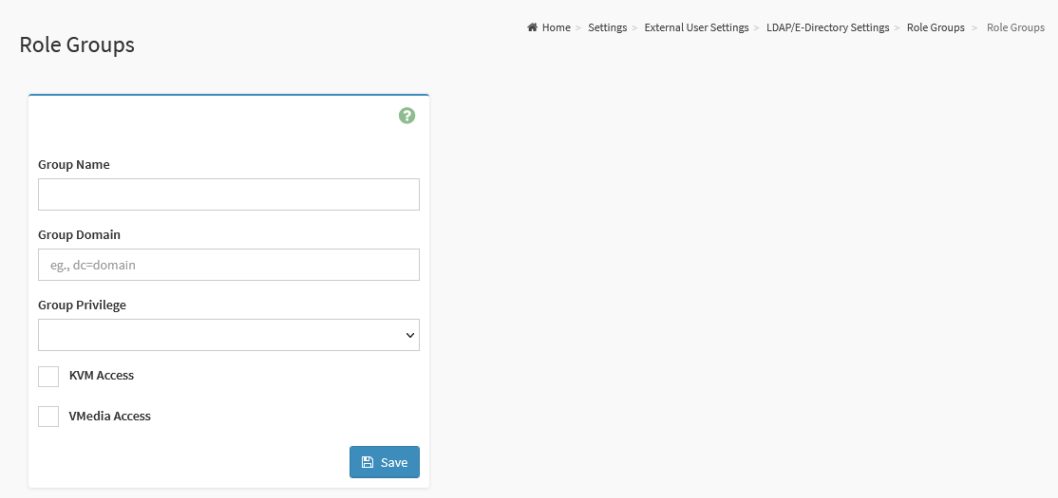
To view the Role Groups page, click the **Settings** -> **External User Services** -> **LDAP/E-Directory Settings** -> **Role Groups** tab from the menu bar.

Figure 23. Snapshot of Role Groups Slots



Click on the **Slot** icon ( ) then navigate to the Add Role Groups page.

Figure 24. Snapshot of Add Role Groups Page



The fields on the Add Role Groups page include

- **Group Name:** Enter the Role Group Name. This name identifies the role group in LDAP/E-Directory.
- **Group Domain:** Enter the Role Group Domain. This is the domain where the role group is located.

- **Group Privilege:** Enter the Role Group Privilege. This is the level of privilege to be assigned for this role group
- **KVM Access:** This field used to assign the KVM privilege for this role group.
- **VMedia Access:** This field used to assign the VMedia privilege for this role group.
- **Save:** To save the configured settings.

2.10.2.2 Active Directory Settings

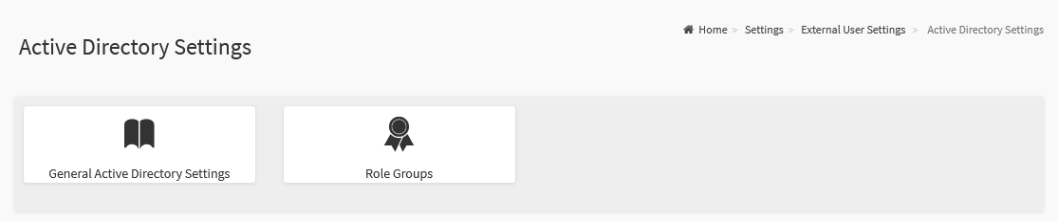
Active Directory (AD) is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains.

Active Directory Settings page provides two functional feature tabs for users to configure the Active Directory settings, including

- **General Active Directory Settings**
- **Role Groups**

To view the Active Directory Settings page, click the **Settings** -> **External User Services** -> **Active Directory Settings** tab from the menu bar.

Figure 25. Snapshot of Active Directory Settings Page



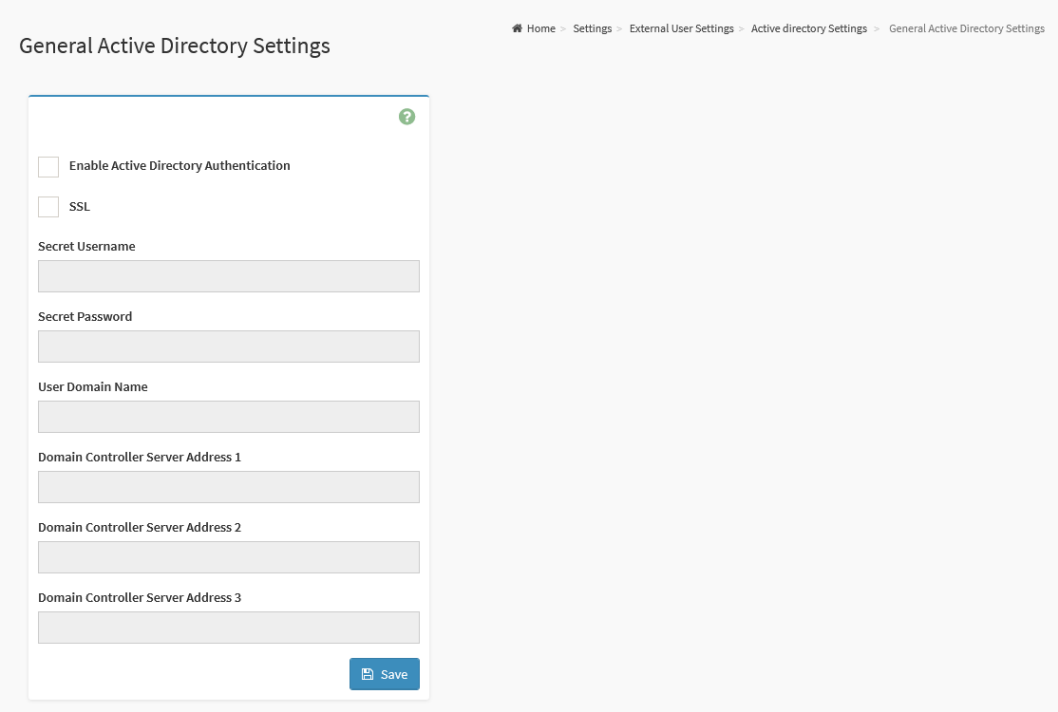
The details about each feature are listed in the following.

2.10.2.2.1 General Active Directory Settings

This page provides various options for users to configure the Active Directory Settings.

To view the Active Directory Settings page, click the **Settings** -> **External User Services** -> **Active Directory Settings** -> **General Active Directory Settings** tab from the menu bar.

Figure 26. Snapshot of General Active Directory Settings Page



The fields on the General Active Directory Settings page include

- **Enable Active Directory Authentication:** Click this option to enable Active Directory Settings.
- **SSL:** Click this option to enable SSL support.
- **Secret Username:** Specify the Username of an administrator of the Active Directory Server.
- **Secret Password:** Specify the Password of the administrator.
- **User Domain Name:** Specify the Domain Name for the user e.g. MyDomain.com
- **Domain Controller Server Address 1:** Enter the IP address of Active Directory server. IPv4 and IPv6 address format are supported.

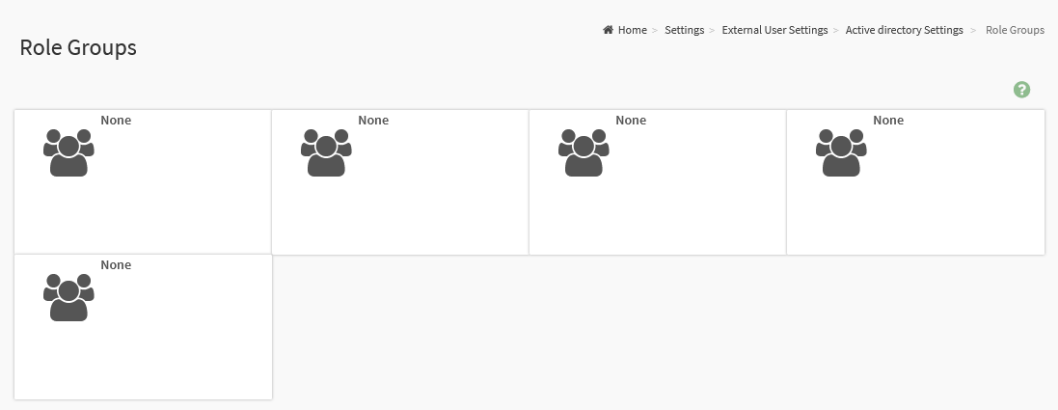
- **Domain Controller Server Address 2:** Enter the IP address of Active Directory server. IPv4 and IPv6 address format are supported.
- **Domain Controller Server Address 3:** Enter the IP address of Active Directory server. IPv4 and IPv6 address format are supported.
- **Save:** To save the configured settings.

2.10.2.2.2 Role Groups

This page provides the feature for users to add a new group to the device.

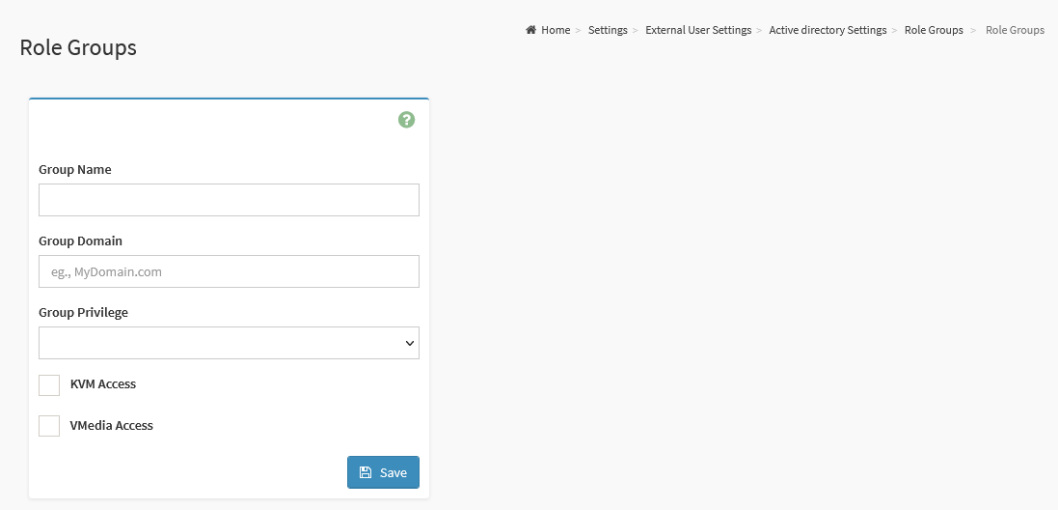
To view the Role Groups page, click the **Settings** -> **External User Services** -> **Active Directory Settings** -> **Role Groups** tab from the menu bar.

Figure 27. Snapshot of Role Groups Slots



Click on the **Slot** icon ( ) then navigate to the Add Role Groups page.

Figure 28. Snapshot of Add Role Groups Page



The fields on the Add Role Groups page include

- **Group Name:** Enter the Role Group Name. This name identifies the role group in Active Directory.
- **Group Domain:** Enter the Role Group Domain. This is the domain where the role group is located.

- **Group Privilege:** Enter the Role Group Privilege. This is the level of privilege to be assigned for this role group
- **KVM Access:** This field used to assign the KVM privilege for this role group.
- **VMedia Access:** This field used to assign the VMedia privilege for this role group.
- **Save:** To save the configured settings.

2.10.2.3 RADIUS Settings

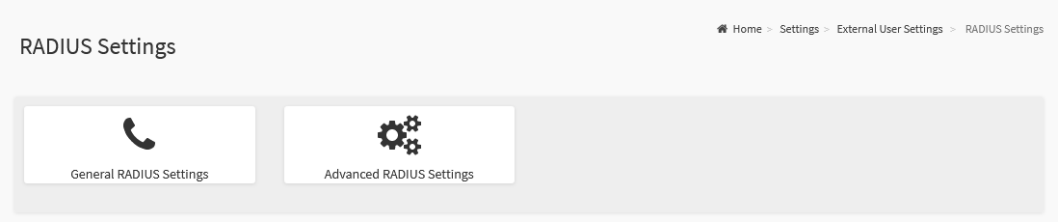
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

RADIUS Settings page provides two functional feature tabs for users to configure the RADIUS settings, including

- **General RADIUS Settings**
- **Advanced RADIUS Settings**

To view the RADIUS Settings page, click the **Settings** -> **External User Services** -> **RADIUS Settings** tab from the menu bar.

Figure 29. Snapshot of RADIUS Settings Page



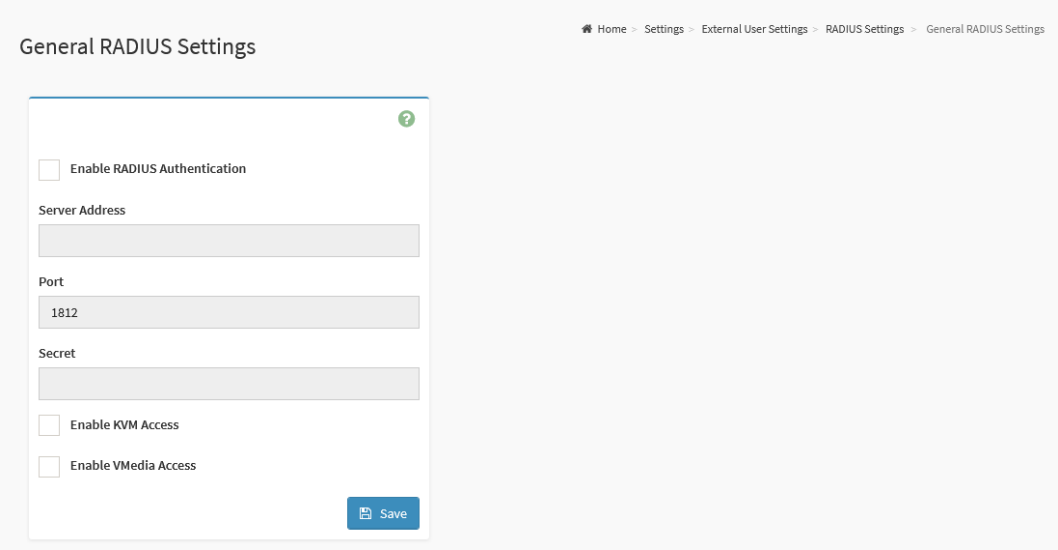
The details about each feature are listed in the following.

2.10.2.3.1 General RADIUS Settings

This page provides various options for users to configure the RADIUS Settings.

To view the General RADIUS Settings page, click the **Settings** -> **External User Services** -> **RADIUS Settings** -> **General RADIUS Settings** tab from the menu bar.

Figure 30. Snapshot of General RADIUS Settings Page



The fields on the General RADIUS Settings page include

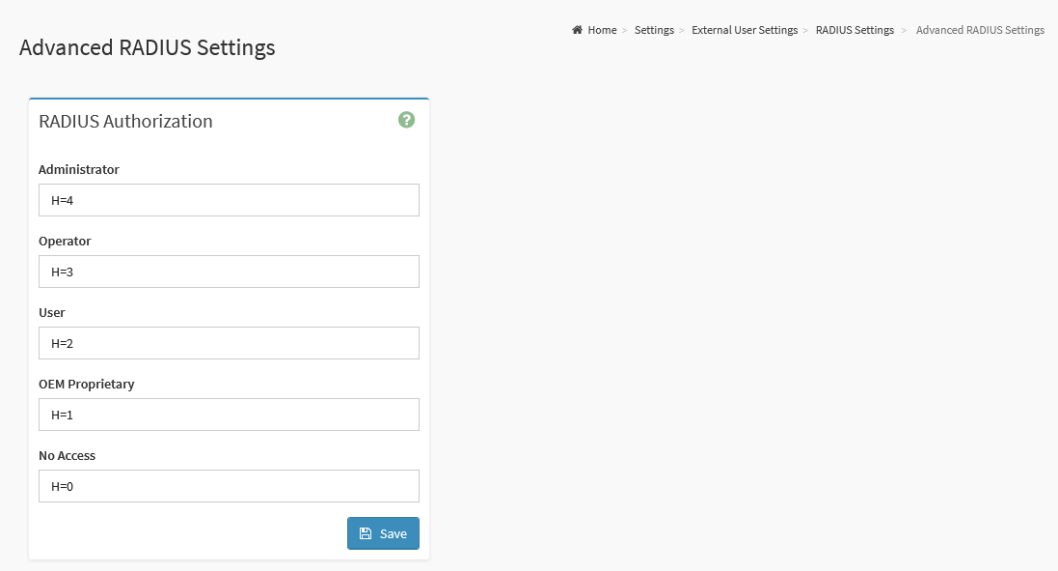
- **Enable RADIUS Authentication:** Check this option to enable RADIUS Authentication.
- **Server Address:** Specify RADIUS Server Address.
- **Port:** Specify the RADIUS Port number.
- **Secret:** Specify RADIUS Server Secret (Password).
- **Enable KVM Access:** This field used to assign the KVM privilege for authenticated users.
- **Enable VMedia Access:** This field used to assign the VMedia privilege for authenticated users.
- **Save:** To save the configured settings.

2.10.2.3.2 Advanced RADIUS Settings

This page provides various options for users to configure the RADIUS authorization.

To view the Advanced RADIUS Settings page, click the **Settings** -> **External User Services** -> **RADIUS Settings** -> **Advanced RADIUS Settings** tab from the menu bar.

Figure 31. Snapshot of Advanced RADIUS Settings Page



The fields on the Advanced RADIUS Settings page include

- **Administrator:** Enter the Vendor-Specific value for Administrator.
- **Operator:** Enter the Vendor-Specific value for Operator.
- **User:** Enter the Vendor-Specific value for User.
- **OEM Proprietary:** Enter the Vendor-Specific value for OEM Proprietary.
- **No Access:** Enter the Vendor-Specific value for No Access.
- **Save:** To save the configured settings.

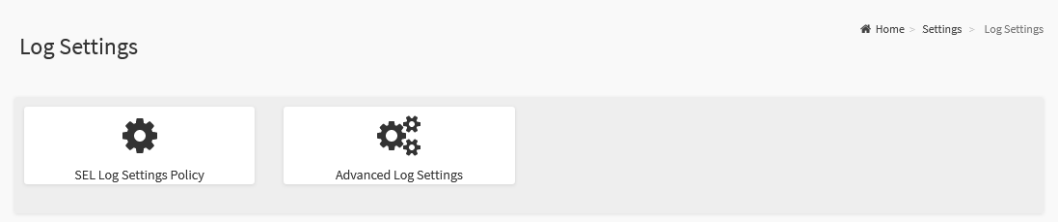
2.10.3 Log Settings

Log Settings page provides two functional feature tabs for users to configure the log policy and advance settings, including

- **SEL Log Settings Policy**
- **Advanced Log Settings**

To view the Log Settings page, click the **Settings** -> **Log Settings** tab from the menu bar.

Figure 32. Snapshot of Log Settings Page



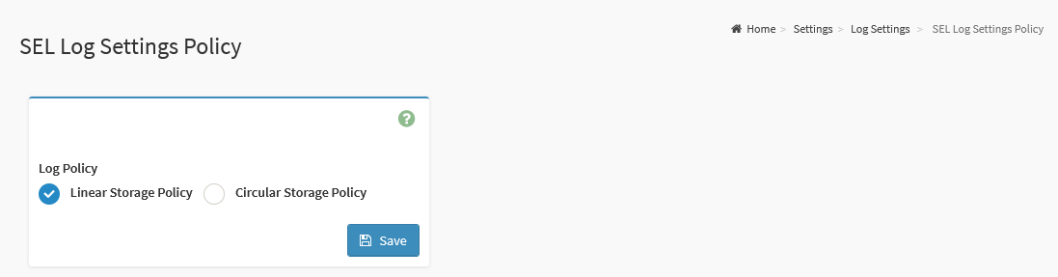
The details about each feature are listed in the following.

2.10.3.1 SEL Log Settings Policy

This page provides various options for users to configure the log policy for the event log.

To view the SEL Log Settings Policy page, click the **Settings** -> **Log Settings** -> **SEL Log Settings Policy** tab from the menu bar.

Figure 33. Snapshot of SEL Log Settings Policy Page



The fields on the SEL Log Settings Policy page include

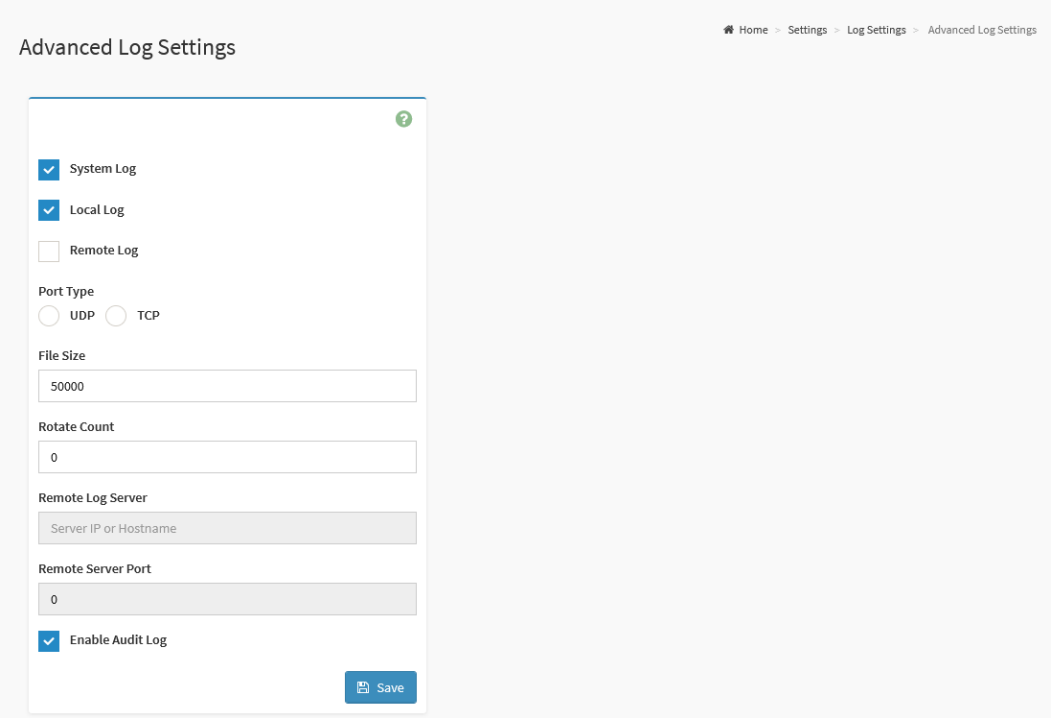
- **Log Policy**
  - **Linear Storage Policy:** Click this option to enable Linear Storage Policy.
  - **Circular Storage Policy:** Click this option to enable Circular Storage Policy.
- **Save:** To save the configured settings.

2.10.3.2 Advanced Log Settings

This page provides various options for users to configure the advanced log settings for the event log.

To view the Advanced Log Settings Policy page, click the **Settings** -> **Log Settings** -> **Advanced Log Settings** tab from the menu bar.

Figure 34. Snapshot of Advanced Log Settings Page



The fields on the Advanced Log Settings page include

- **System Log:** Click this option to enable System Log to view all system events for this device.
- **Local Log:** Click this option to save the log locally (CMM).
- **Remote Log:** Click this option to save the logs in a remote machine.
- **Port Type:** Port Type is supported with enable Remote Log, select either **UDP** or **TCP** for Remote Log feature used.
  - **UDP**
  - **TCP**
- **File Size:** Specify the size of the file in bytes if the selected log type is local.
- **Rotate Count:** To back up the log information in back up files. 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.

Note: **File Size** and **Rotate Count** options will be available only when Local Log is enabled.

- **Remote Log Server:** Specify the Remote server address to log the system events.
- **Remote Server Port:** Specify the Remote server port address to log the system events.
- **Enable Audit Log:** Click this option to enable Audit Log to view all audit events for this device.
- **Save:** To save the configured settings.

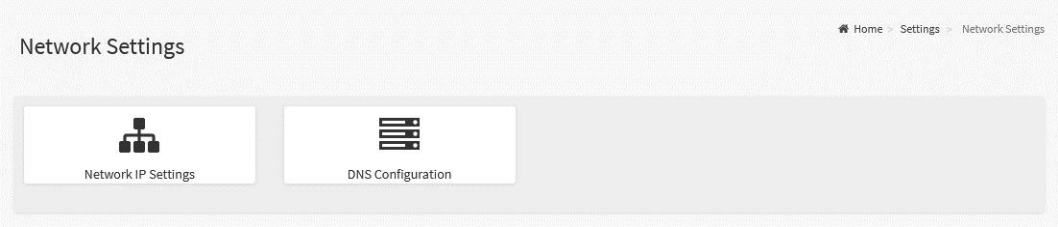
2.10.4 Network Settings

Network Settings page provides various options for users to configure the network settings for the available LAN channels, including

- **Network IP Settings**
- **DNS Configuration**

To view the Network Settings page, click the **Settings** -> **Network Settings** tab from the menu bar.

Figure 35. Snapshot of Network Settings Page



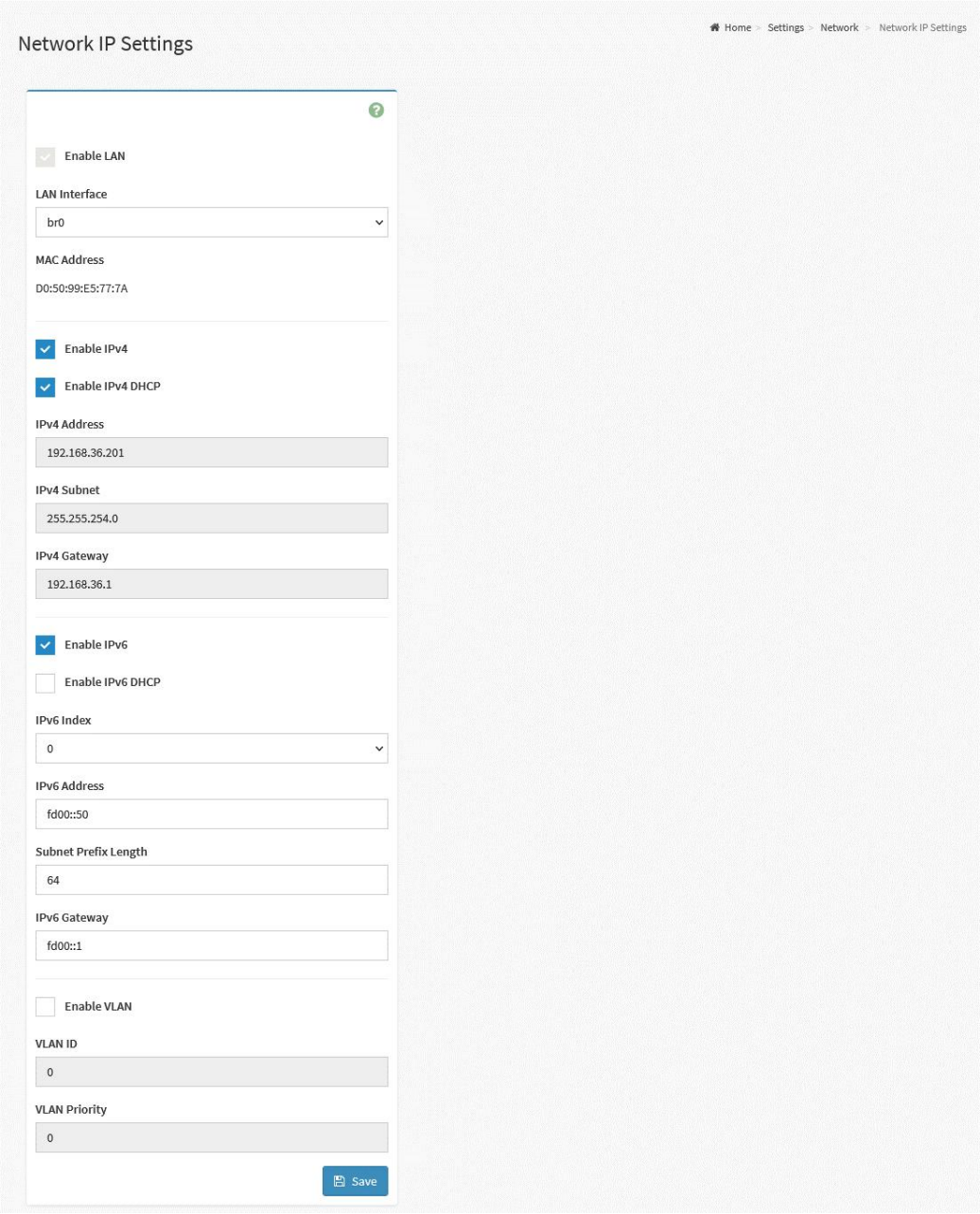
The details about each feature are listed in the following.

2.10.4.1 Network IP Settings

This page provides various options for users to configure the Network IP Settings.

To view the Network IP Settings page, click the **Settings** -> **Network Settings** -> **Network IP Settings** tab from the menu bar.

Figure 36. Snapshot of Network IP Settings Page



The fields on the Network IP Settings page include

- **Enable LAN:** Click this option the enable LAN support for the interface.
- **LAN Interface:** Lists the supported LAN interface, select the LAN interface to be configured.
- **MAC Address:** Indicates the selected LAN interface MAC address.
- **Enable IPv4:** Click this option to enable IPv4 support for the selected interface.
- **Enable IPv4 DHCP:** Click this option to dynamically configure IPv4 address using Dynamic Host Configuration Protocol (DHCP).
- **IPv4 Address:** If DHCP is disabled, specify a static IPv4 for the interface.
- **IPv4 Subnet:** If DHCP is disabled, specify a static Subnet Mask.
- **IPv4 Gateway:** If DHCP is disabled, specify a static Default Gateway.
- **Enable IPv6:** Click this option to enable IPv6 support for the selected interface.
- **Enable IPv6 DHCP:** Click this option to dynamically configure an IPv6 address using Dynamic Host Configuration v6 Protocol (DHCPv6).
- **IPv6 Index:** Select the IPv6 Index.
- **IPv6 Address:** Specify a static IPv6 address for the selected interface.
- **Subnet Prefix Length:** Specify the subnet prefix length for the IPv6 settings.
- **IPv6 Gateway:** Specify an IPv6 gateway for the selected interface.
- **Enable VLAN:** Click this option to enable VLAN support for the selected interface.
- **VLAN ID:** Specify an ID for this VLAN configuration.
- **VLAN Priority:** Specify the priority for VLAN configuration.
- **Save:** To save the configured settings.

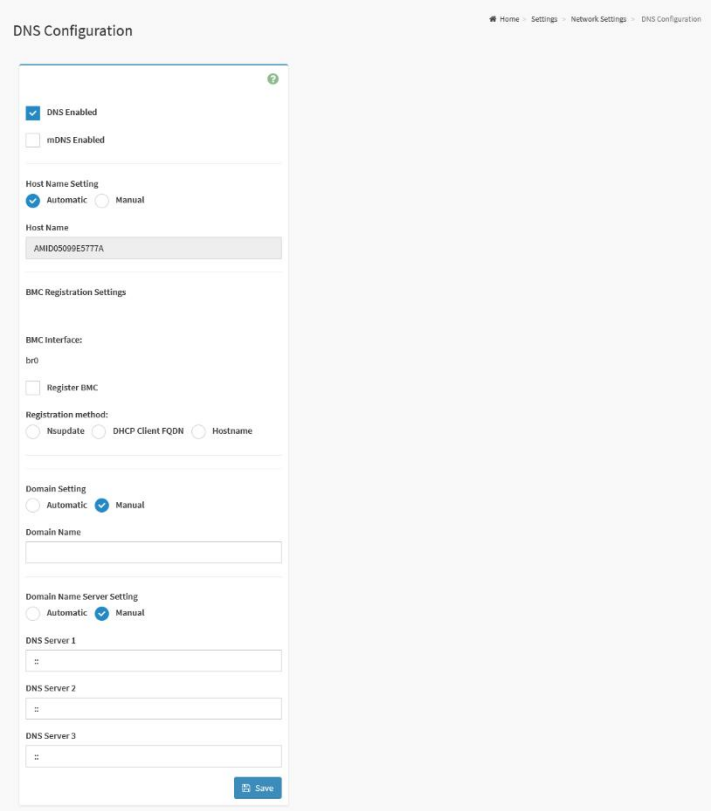
2.10.4.2 DNS Configuration

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.

This page provides various options for users to configure the DNS Configuration settings.

To view the Network IP Settings page, click the **Settings** -> **Network Settings -**> **DNS Configuration** tab from the menu bar.

Figure 37. Snapshot of DNS Configuration Page



The fields on the DNS Configuration page include

- **DNS Enabled:** Click this option to enable all DNS services.
- **mDNS Enabled:** Click this option to enable Multicast DNS services.
- **Host Name Setting:** Select either Automatic or Manual settings.
  - **Automatic**
  - **Manual**
- **Host Name:** Indicates Host Name of device. If Host Name Settings is

Manual, specify the host name of device.

BMC Registration Settings:

- **BMC Interface:** Options to register the BMC through the Interface.

Eth0 and Eth1:

- **Register BMC:** To register BMC through registration method.
- **Registration method:** Options to register the BMC through the below registration methods.
  - **Nsupdate:** Register with the DNS server using the nsupdate application.
  - **DHCP Client FQDN:** Register with the DNS server using DHCP option 81.
  - **Hostname:** Register with the DNS server using DHCP option 12.
- **Domain Setting:** Select whether the domain interface will be configured manually or automatically.
  - **Automatic:** If **Automatic** is selected, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
  - **Manual:** If **Manual** is selected, specify the domain name of the device.
- **Domain Interface:** Indicates the domain name of the device.
- **Domain Name:** Specify the domain name of the device.
- **DNS Interface:** Specify the interface to be used.
- **IP Priority:**
  - **IPv4:** If IPv4 is selected, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
  - **IPv6:** If IPv6 is selected, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.
- **DNS Server 1, 2, and 3:** Specify the DNS server address to be configured for the CMM.
  Note: IPv4 and IPv6 address format are supported.
- **Save:** To save the configured settings.

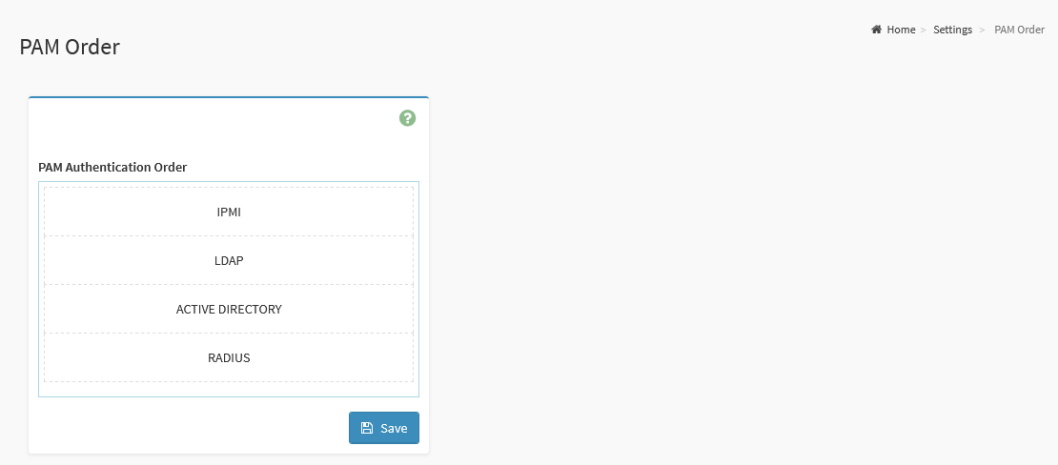
2.10.5 PAM Order Settings

Pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API).

PAM Order Settings page provides the options for users to configure the PAM ordering for user authentication in to the CMM.

To view the PAM Order Settings page, click the **Settings** -> **PAM Order Settings** tab from the menu bar.

Figure 38. Snapshot of PAM Order Settings Page



The fields on the PAM Order Settings page include

- **PAM Module:** lists the available PAM modules supported in the CMM. Select the required PAM module and click and drag the required PAM module. It can be moved UP or DOWN to change its arrangement order.
- **Save:** To save the configured settings.

2.10.6 Platform Event Filters

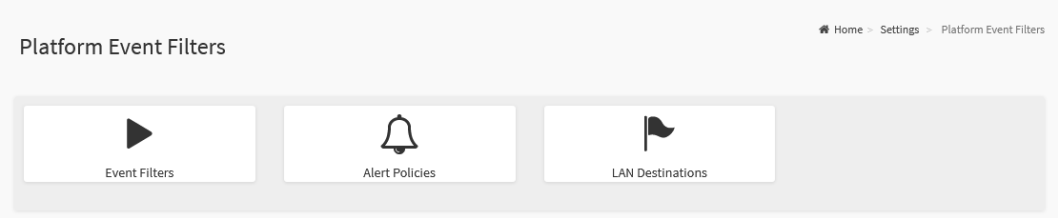
Platform Event Filter (PEF) provides a mechanism for configuring the CMM to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

Platform Event Filters page provides various functional feature tabs for users to configure the PEF feature, including

- **Event Filters**
- **Alert Policies**
- **LAN Destinations**

To view the Platform Event Filters page, click the **Settings** -> **Platform Event Filters** tab from the menu bar.

Figure 39. Snapshot of Platform Event Filters Page



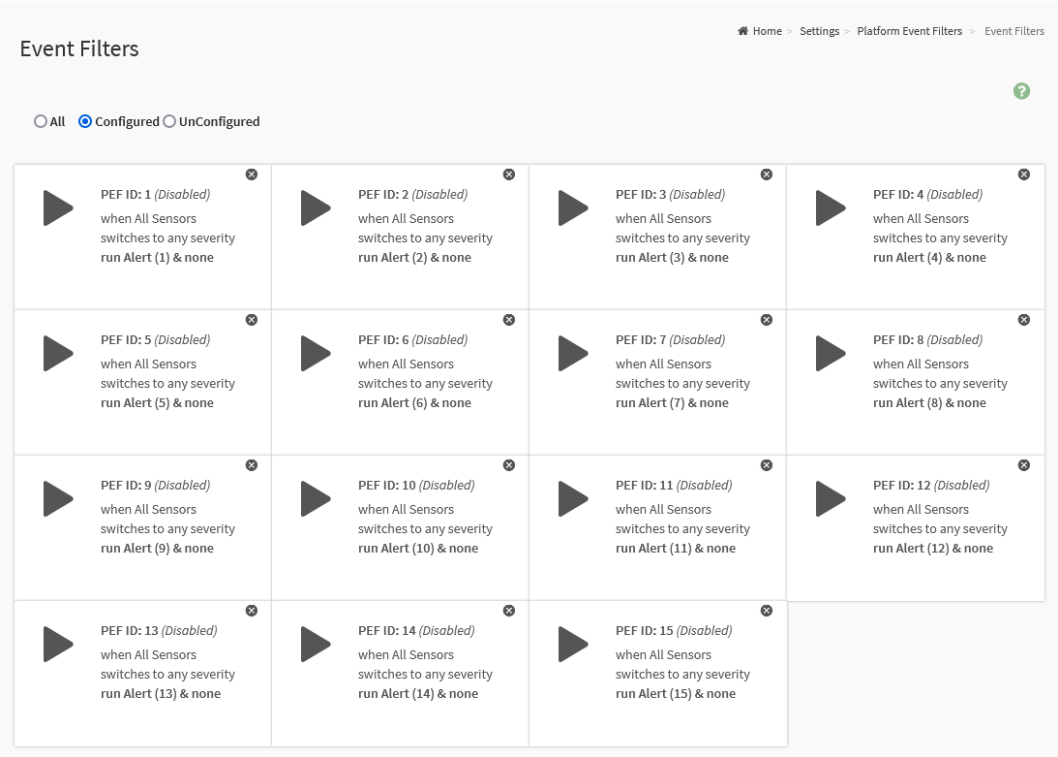
The details about each feature are listed in the following.

2.10.6.1 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,

To view the Event Filters page, click the **Settings** -> **Platform Event Filters** -> **Event Filters** tab from the menu bar.

Figure 40. Snapshot of Platform Event Filters Slot List Page



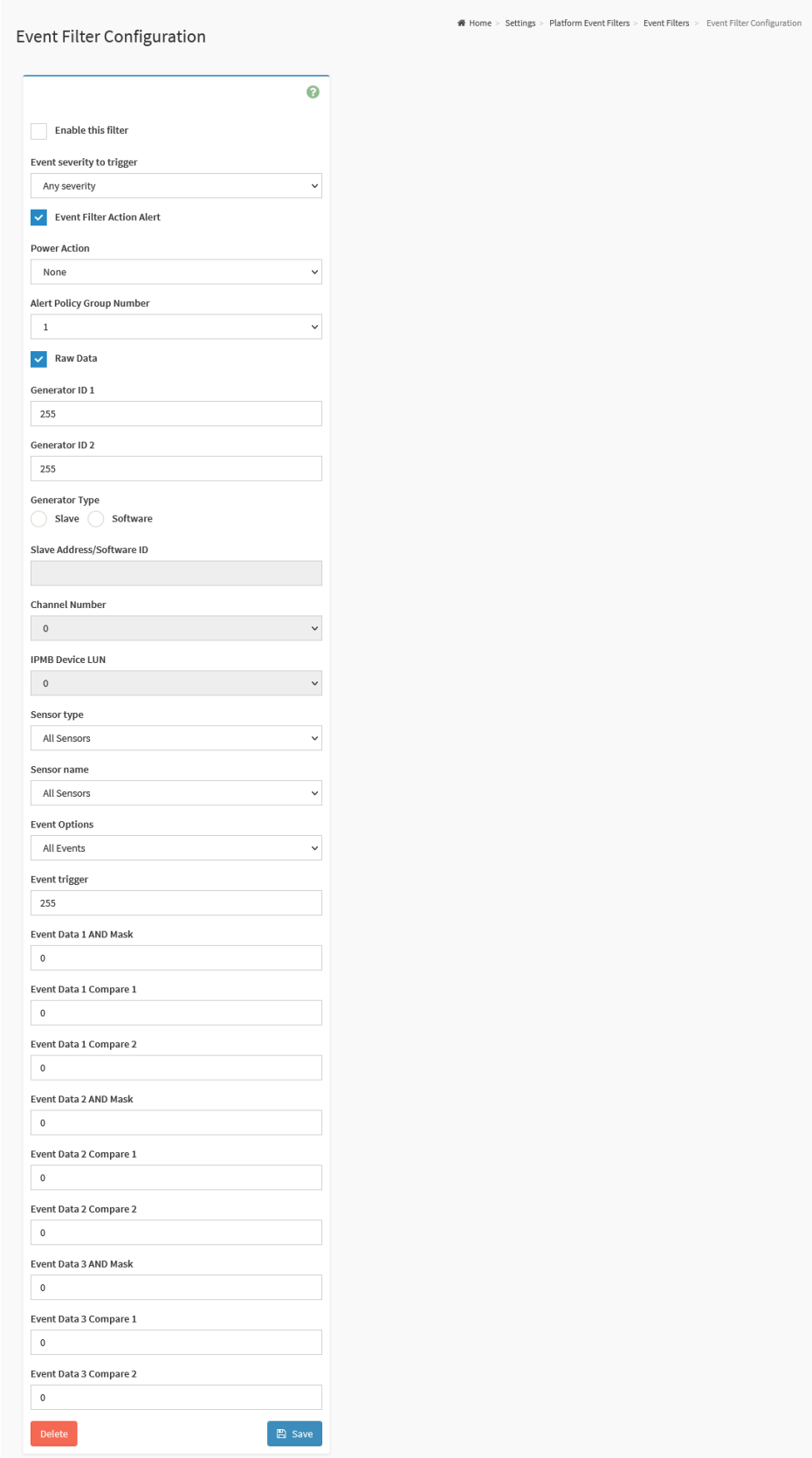
The fields on the Event Filters page include

- **All:** Click this option to lists all slots.
- **Configured:** Click this option to lists all configured slots.
- **Unconfigured:** Click this option to lists all unconfigured slots.

Click on the **Event Filters Slot** icon (▶) then navigate to the Event Filter Configuration page.

Click on the **Delete** icon (⊗) on the top right corner of Event Filters Slot to directly to delete a slot from the list.

Figure 41. Snapshot of Event Filters Configuration Page



The fields on the Event Filters Configuration page include

- **Enable this filter:** Click this option to enable the PEF settings.
- **Event severity to trigger:** Select any one of the Event Severity from the drop-down list.
- **Event Filter Action Alert:** Click this option to enable PEF Alert action.
- **Power Action:** Select any one of the **Power Action** either Power down, Power reset or Power cycle from the drop-down list.
- **Alert Policy Group Number:** Select any one of the configured Alert Policy Group Number from the drop-down list.
  Note: Alert Policy has to be configured under **Settings** -> **Platform Event Filters** -> **Alert Policies**.
- **Raw Data:** Click this option to enter the Generator ID with raw data.
- **Generator ID 1:** Specify the raw generator ID1 data value.
- **Generator ID 2:** Specify the raw generator ID2 data value.
- **Generator Type:**
  - **Slave:** Select **Slave** if event was generated from IPMB.
  - **Software:** Select **Software** if event was generated from system software.
- **Slave Address/Software ID:** Specify corresponding I2C Slave Address or System Software ID.
- **Channel Number:** Select the particular channel number through which the event message is received over. Choose '0' if the event message is received via the system interface, primary IPMB, or internally generated by the CMM.
- **IPMB Device LUN:** Select the corresponding IPMB Device LUN if event is generated by IPMB.
- **Sensor Type:** Select the type of sensor that will trigger the event filter action.
- **Sensor Name:** Select the particular sensor from the sensor list.
- **Event Options:** Select event option to be either All events or Sensor specific events.
- **Event Trigger:** This field is used to give Event/Reading type value. Value ranges from 0 to 255.
- **Event Data 1 AND Mask:** This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255.

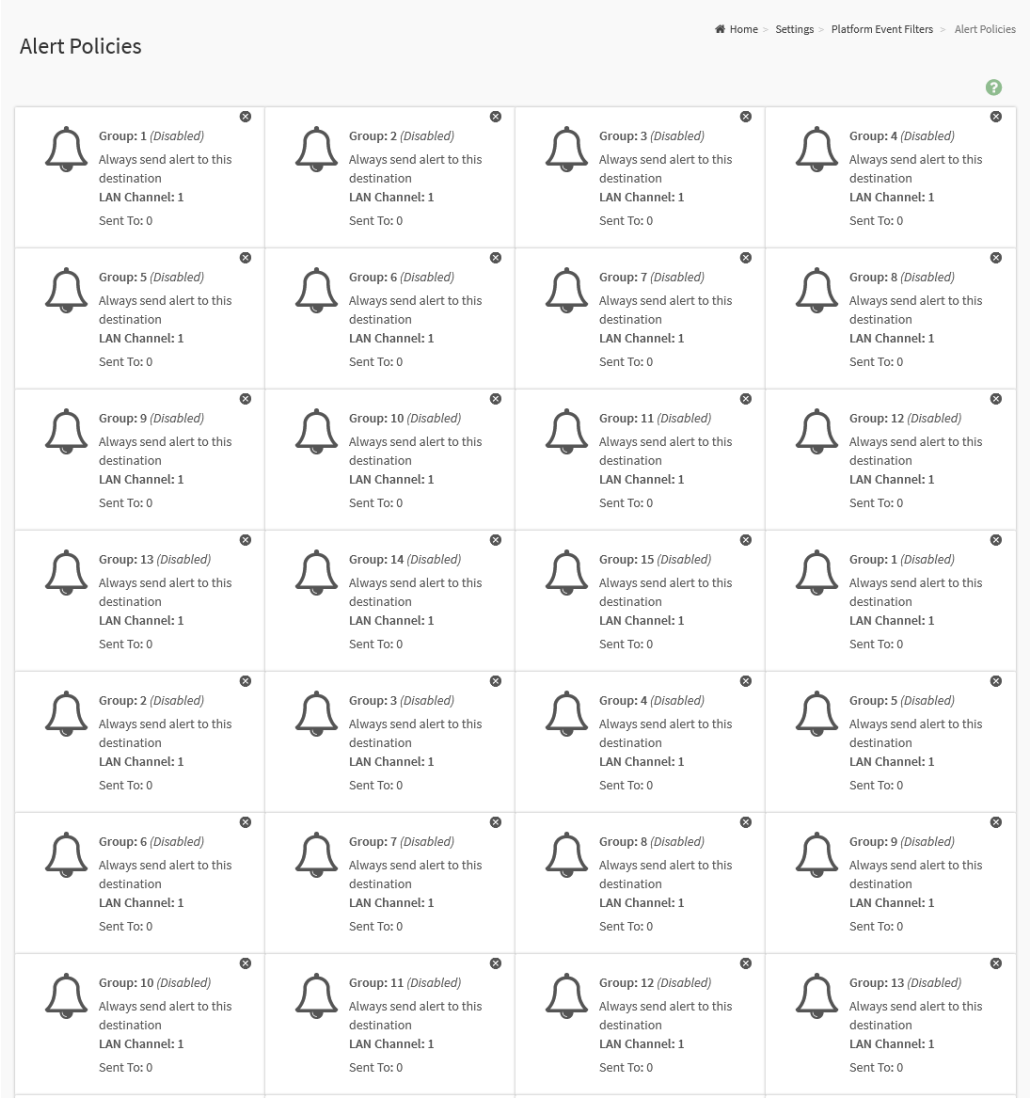
- **Event Data 1 Compare 1:** This field is used to indicate whether each bit position's comparison is an exact comparison or not.
- **Event Data 1 Compare 2:** This field is used to indicate whether each bit position's comparison is an exact comparison or not. Value ranges from 0 to 255.
- **Event Data 2 AND Mask** and **Event Data 3 AND Mask:** These fields are similar to Event Data 1 AND Mask.
- **Event Data 2 Compare 1** and **Event Data 3 Compare 1:** These fields are similar to Event Data 1 Compare 1.
- **Event Data 2 Compare 2** and **Event Data 3 Compare 2:** These fields are similar to Event Data 1 Compare 2.
- **Delete:** To delete the existing filter.
- **Save:** To save the configured settings.

2.10.6.2 Alert Policies

This page provides the feature for users to configure the Alert Policy for PEF configuration.

To view the Alter Policies page, click the **Settings** -> **Platform Event Filters** -> **Alter Policies** tab from the menu bar.

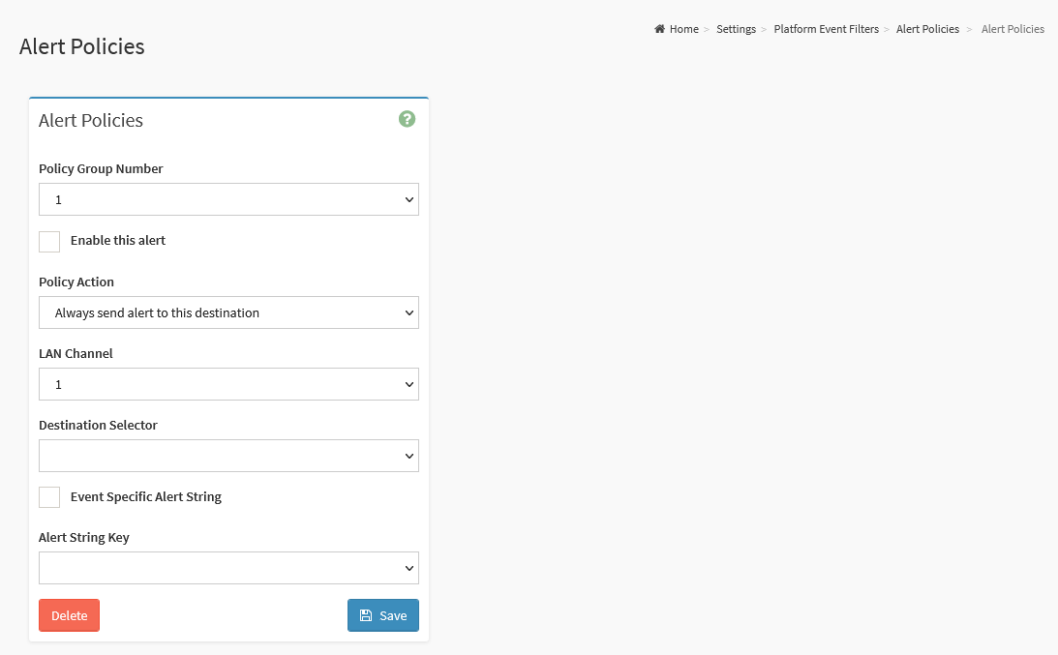
Figure 42. Snapshot of Alert Policies Page



Click on the **Alert Policy Slot** icon ( ) then navigate to the Alert Policies Configuration page.

Click on the **Delete** icon ( ) on the top right corner of Alert Policy Slot to directly to delete a slot from the list.

Figure 43. Snapshot of Alert Policies Configuration Page



The fields on the Alert Policies Configuration page include

- **Policy Group Number:** Indicates the policy group number of the configuration.
- **Enable this alert:** Click this option to enable this alert policy.
- **Policy Action:** Select any one of the Policy Action set from the list.
- **LAN Channel:** Select a particular channel from the available channel list.
- **Destination Selector:** Select a particular destination from the configured destination list.

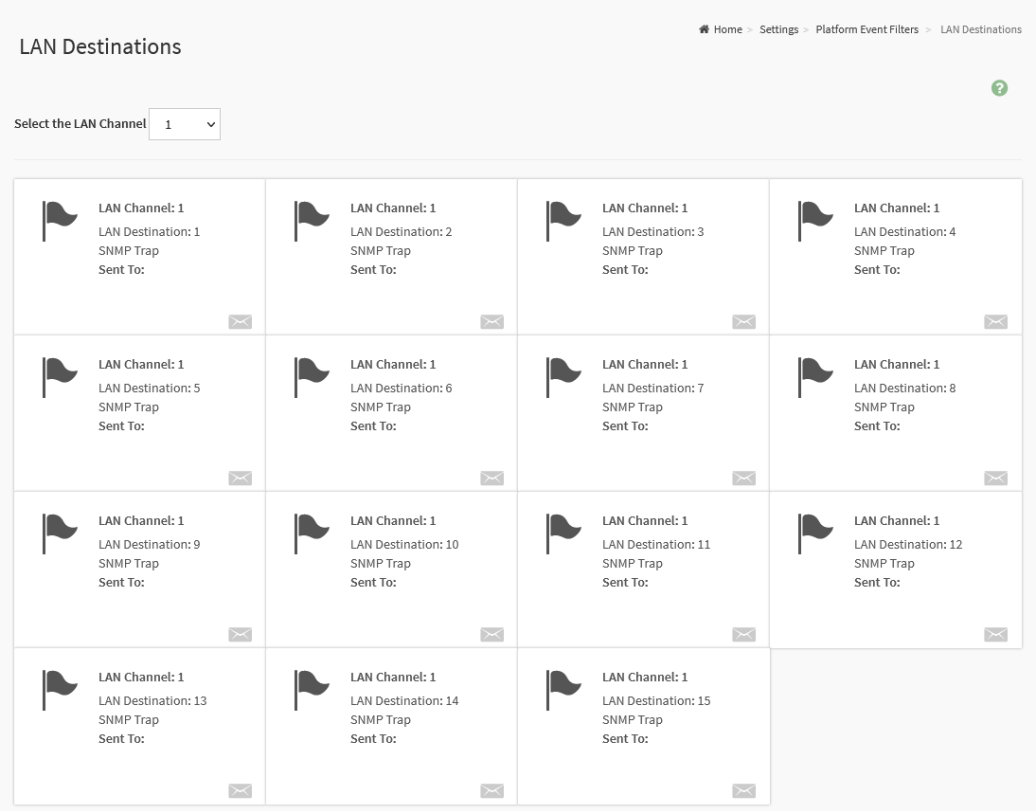
  Note: LAN Destination has to be configured under **Settings** ->**Platform Event Filters** -> **LAN Destinations**.
- **Event Specific Alert String:** Specify an event-specific Alert String.
- **Alert String Key:** Specify which string is to be sent for this Alert Policy entry.
- **Delete:** To delete the configured Alter Policy.
- **Save:** To save the configured settings.

2.10.6.3 LAN Destinations

This page provides the feature for users to configure the LAN Destinations for PEF configuration.

To view the LAN Destinations page, click the **Settings** -> **Platform Event Filters** -> **LAN Destinations** tab from the menu bar.

Figure 44. Snapshot of LAN Destinations Page



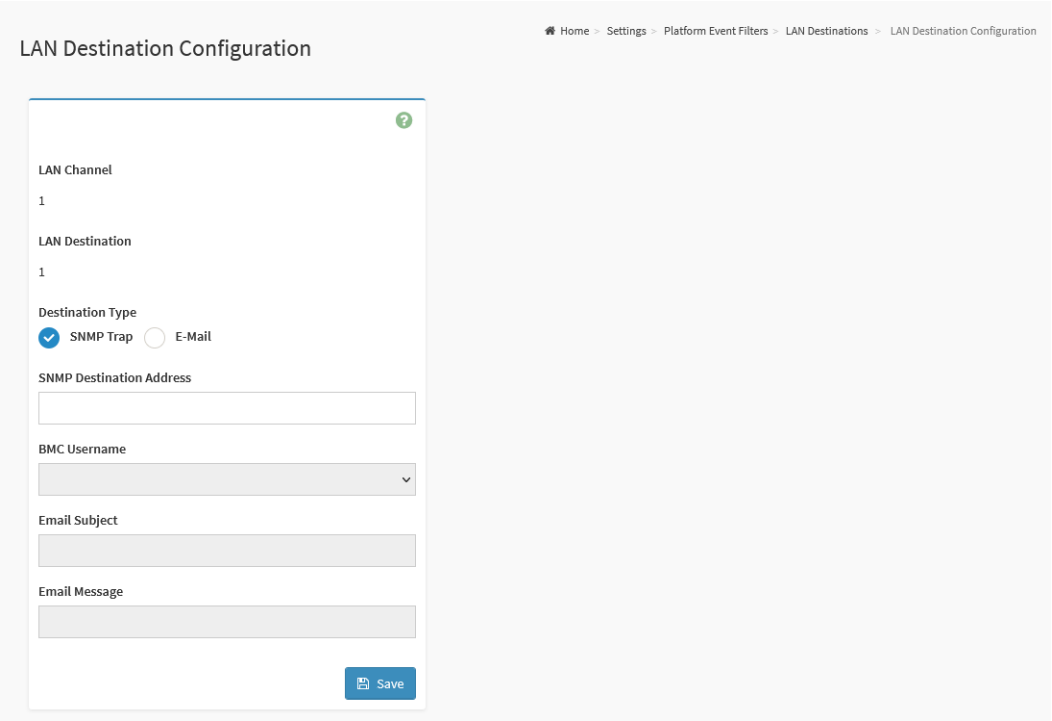
The fields on the LAN Destinations page include

- **Select the LAN Channel:** To select the LAN Channel number.

Click on the **LAN Destination Slot** icon ( ) then navigate to the LAN Destination Configuration page.

Click on the **Mail** icon ( ) on the bottom right corner of LAN Destination Slot to send a test alert mail.

Figure 45. Snapshot of LAN Destinations Configuration Page



The fields on the LAN Destinations Configuration page include

- **LAN Channel:** Indicates the LAN Channel Number of the selected slot
- **LAN Destination:** Indicates the Destination number of the selected slot
- **Destination Type:** Destination type can be either an SNMP Trap or an E-mail alert.
  - **SNMP Trap:** If **SNMP Trap** is selected, then give the IP address of the system that will receive the alert.
  - **E-Mail:** If **E-Mail** is selected, then choose the user to whom the email alert has to be sent.
- **SNMP Destination Address:** Specify the IP address of the system that will receive the alert. IPv4 and IPv6 IP address format are supported.
- **BMC Username:** Select the user to whom the email alert has to be sent.
- **Email Subject** and **Email Message:** 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.

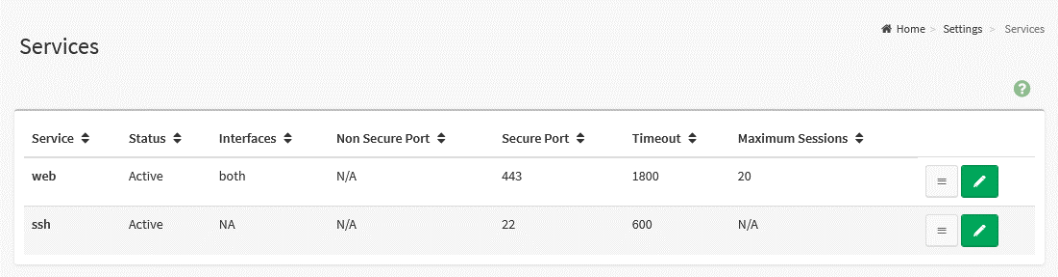
  NOTE: These fields are not applicable for 'AMI-Format' email users.
- **Save:** To save the configured settings.

2.10.7 Services

This page provides the information about services running in the CMM. Only administrator can modify the service.

To view the Services page, click the **Settings** -> **Services** tab from the menu bar.

Figure 46. Snapshot of Services Page



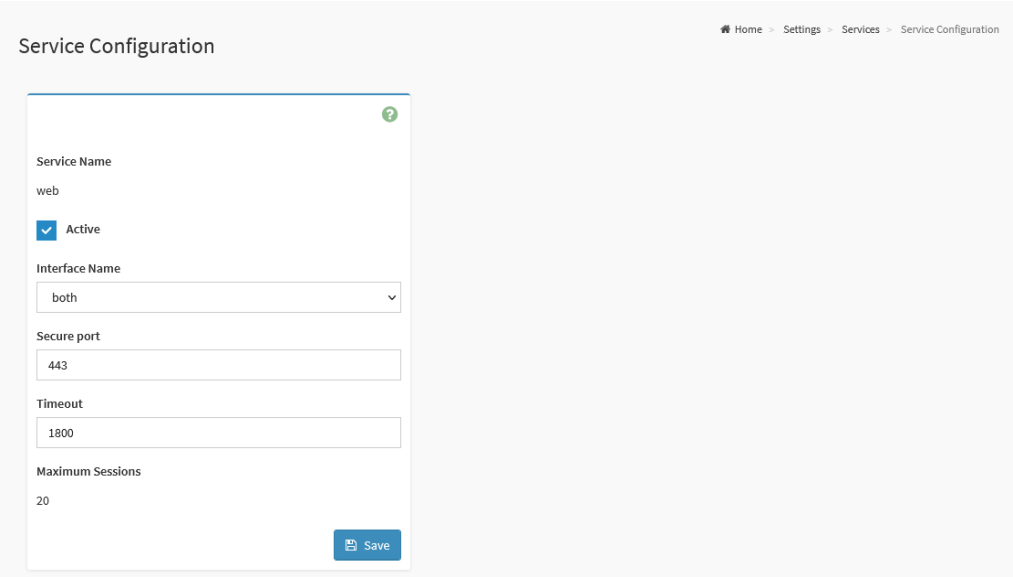
The fields on the Services page include

- **Service:** Indicates the service name of selected slot.
- **Status:** Indicates the current status of the service, either active or inactive state.
- **Interfaces:** Indicates the interface in which service is running.
- **Secure Port:** Indicates the secure port number for the service.
- **Timeout:** Indicates the session timeout value of the service.
- **Maximum Session:** Indicates the maximum number of allowed sessions for the service.

Click on the **Edit** icon ( ) then navigate to Service Configuration page to modify the services configuration.

Click on the **View** icon ( ) then navigate to Service Sessions page to view or terminate the connected session for this service.

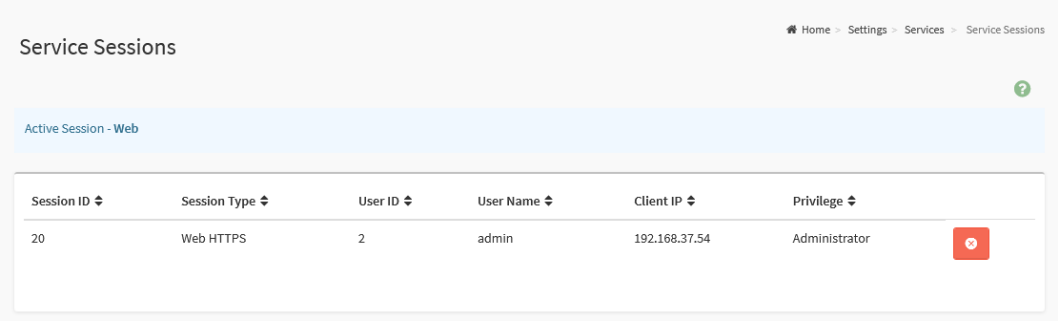
Figure 47. Snapshot of Services Configuration Page



The fields on the Services Configuration page include

- **Service Name:** Indicates the name of selected service.
- **Active:** Indicates the current status of the service, either active or inactive. Click this option to activate the service.
- **Interface Name:** Indicates the interface on which the service is running
- **Secure port:** Used to configure secure port numbers for the services.
- **Timeout:** Specify the timeout value.
- **Maximum Sessions:** Indicates the maximum number of allowed sessions for the service.
- **Save:** To save the configured settings.

Figure 48. Snapshot of Services Sessions Page



The fields on the Services Sessions page include

- **Session ID:** Indicates the ID number of this session.
- **Session Type:** Indicates the type of the active sessions.
- **User ID:** Indicates the ID number of the user.
- **User Name:** Indicates the name of the user.
- **Client IP:** Indicates the IP addresses that are already configured for the active sessions.
- **Privilege:** Indicates the access privilege of the user.

Click on the **Terminate** icon ( ) to terminate the particular session of the service.

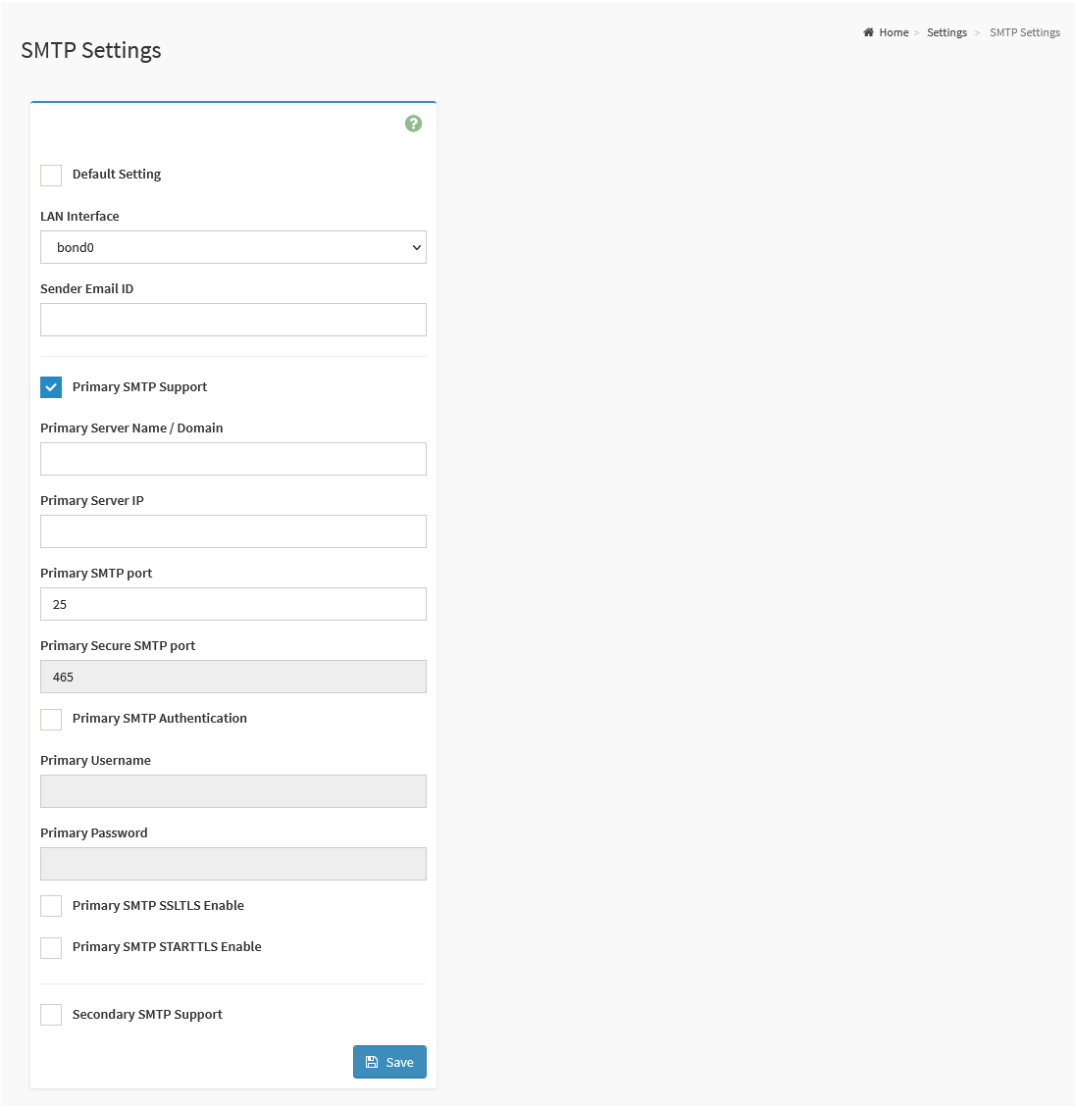
2.10.8 SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an internet standard communication protocol for electronic mail transmission.

This page provides various options for users to configure the SMTP settings of the device.

To view the SMTP Settings page, click the **Settings** -> **SMTP Settings** tab from the menu bar.

Figure 49. Snapshot of SMTP Settings Page



The fields on the SMTP Settings page include

- **Default Setting:** Click this option to enable all parameters use default values.
- **LAN Interface:** Indicates the list of LAN channels available.
- **Sender Email ID:** To specify a valid 'Sender Email ID' on the SMTP Server.

Primary and Secondary SMTP Support:

- **SMTP Support:** Click this option to enable SMTP support for the CMM.
- **Server Name / Domain:** To specify the 'Machine Name' of the SMTP Server.
- **Server IP:** To specify the 'IP address' of the SMTP Server.
- **SMTP port:** To specify the SMTP Port.
- **Secure SMTP port:** To specify the SMTP Secure Port.
- **SMTP Authentication:** Click this option 'Enable' to enable SMTP Authentication.
- **Username:** To specify the username required to access SMTP Accounts.
- **Password:** To specify the password for the SMTP User Account.
- **SMTP SSLTLS Enable:** Click this option t enable the SMTP SSLTLS protocol.
- **SMTP STARTTLS Enable:** Click this option to enable the SMTP STARTTLS protocol.
    - **Upload SMTP CA Certificate File:** Use Browse button to navigate to upload CACERT. CACERT key file should be of pem type.
    - **Upload SMTP Certificate File:** Use Browse button to navigate to upload CERT. CERT key file should be of pem type.
    - **Upload SMTP Private Key:** Use Browse button to navigate to upload SMTP KEY. SMTP key file should be of pem type.

2.10.9 SSL Settings

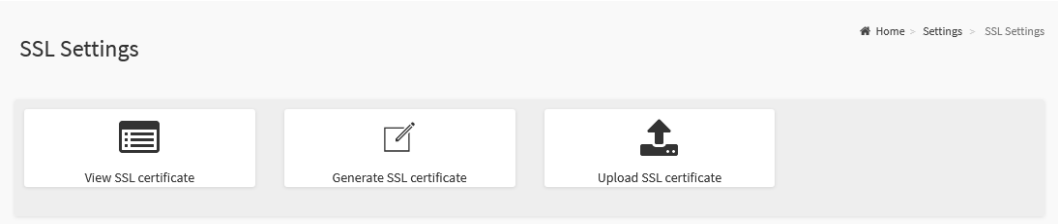
The Secure Socket Layer (SSL) protocol is a networking protocol designed for securing connections between web clients and web servers over an insecure network. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions.

SSL Settings page provides various functional feature tabs for users to monitor or configure the SSL settings value, including

- **View SSL Certificate**
- **Generate SSL Certificate**
- **Upload SSL Certificate**

To view the SSL Settings page, click the **Settings** -> **SSL Settings** tab from the menu bar.

Figure 50. Snapshot of SSL Settings Page



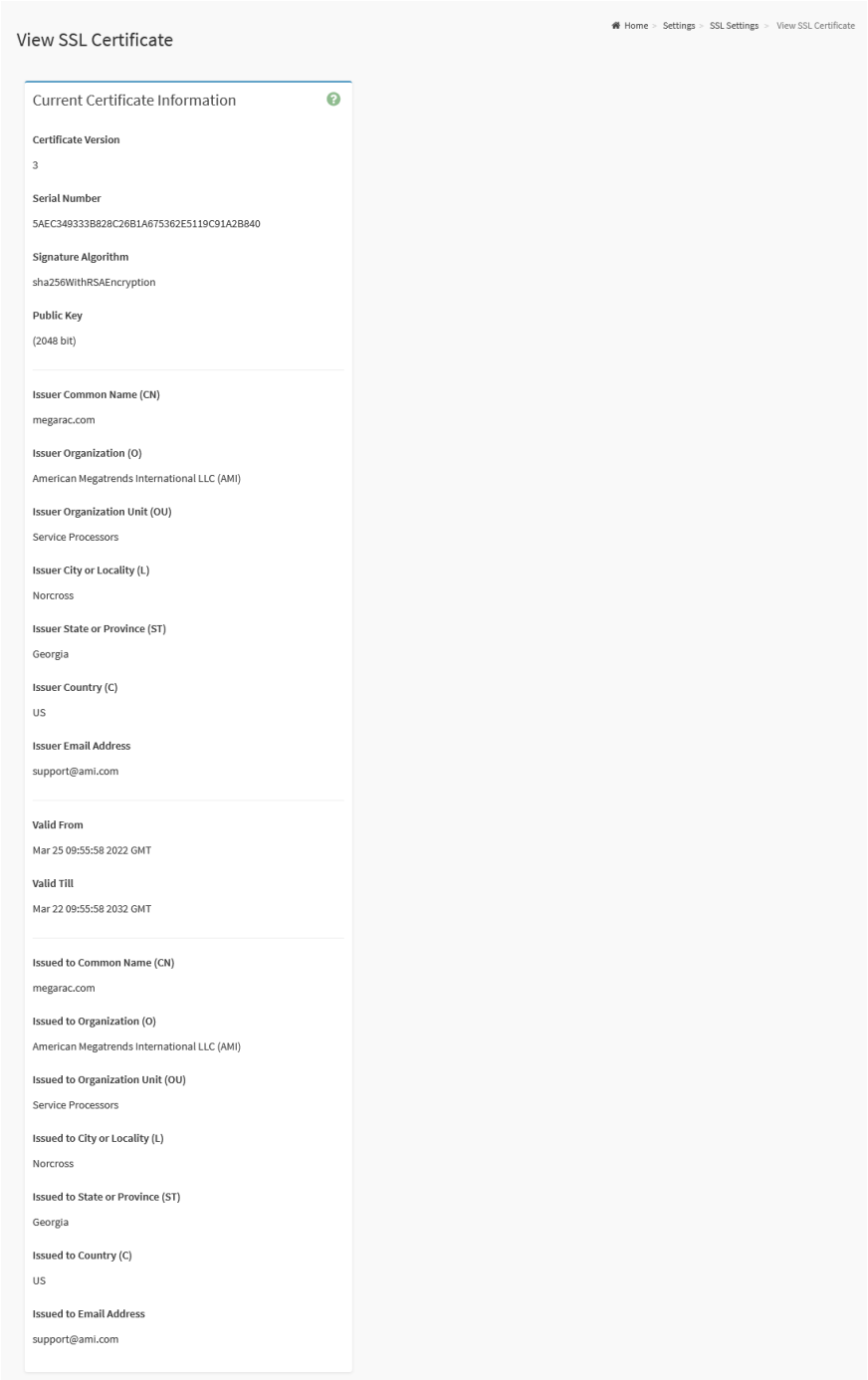
The details about each feature are listed in the following.

2.10.9.1 View SSL Certificate

This page provides the information of current certificate information.

To view the View SSL Certificate page, click the **Settings** -> **SSL Settings** -> **View SSL Certificate** tab from the menu bar.

Figure 51. Snapshot of View SSL Certificate Page



The fields on the View SSL Certificate page include

Basic Information:

- **Certificate Version**
- **Serial Number**
- **Signature Algorithm**
- **Public Key**

Issued From:

- **Issuer Common Name (CN)**
- **Issuer Organization (O)**
- **Issuer Organization Unit (OU)**
- **Issuer City or Locality (L)**
- **Issuer State or Province (ST)**
- **Issuer Country (C)**
- **Issuer Email Address**

Validity Information:

- **Valid From**
- **Valid Till**

Issued To:

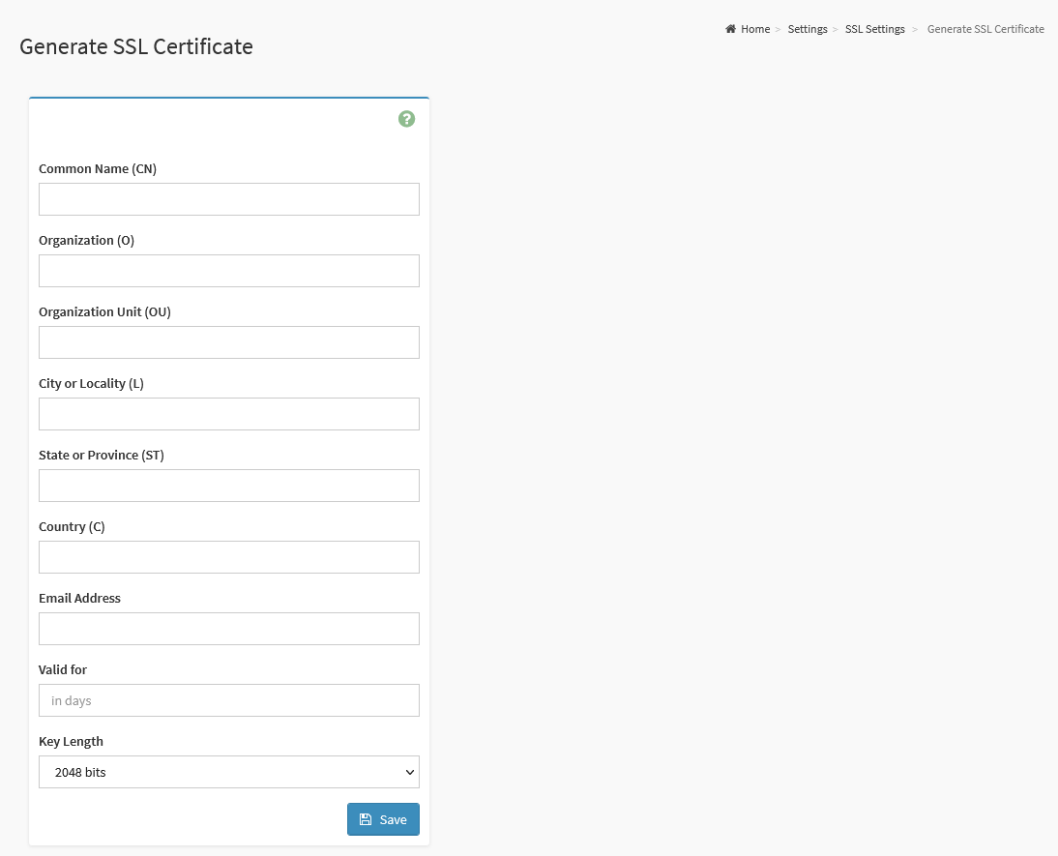
- **Issued to Common Name (CN)**
- **Issued to Organization (O)**
- **Issued to Organization Unit (OU)**
- **Issued to City or Locality (L)**
- **Issued to State or Province (ST)**
- **Issued to Country (C)**
- **Issued to Email Address**

2.10.9.2 Generate SSL Certificate

This page provides the various options for users to generate SSL certificate through the CMM Web service.

To view the Generate SSL Certificate page, click the **Settings** -> **SSL Settings** -> **Generate SSL Certificate** tab from the menu bar.

Figure 52. Snapshot of Generate SSL Certificate Page



The fields on the Generate SSL Certificate page include

- **Common Name (CN):** To specify the common name for which the certificate is to be generated.
- **Organization (O):** To specify the name of the organization for which certificate is to be generated.
- **Organization Unit (OU):** To specify the Section or Unit of the organization for which certificate is to be generated.
- **City or Locality (L):** To specify the City or Locality.
- **State or Province (ST):** To specify the State or Province.

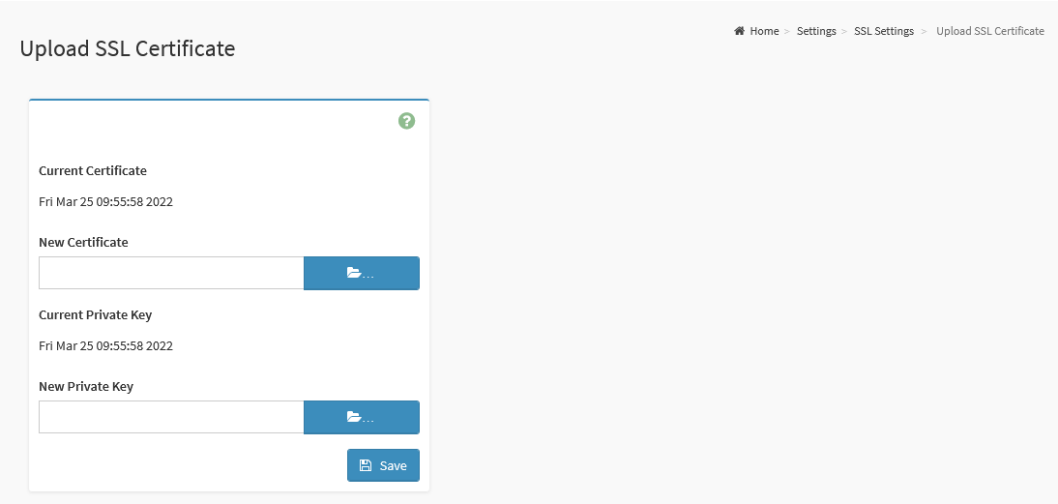
- **Country (C):** To specify the Country code.
- **Email Address:** To specify the Email Address of the organization.
- **Valid for:** Requested validity days for the certificate.
- **Key Length:** Select the key length bit value of the certificate.
- **Save:** To save the configured settings.

2.10.9.3 Upload SSL Certificate

This page provides the various options for users to upload the new SSL Certificate file into the CMM to replace the old one.

To view the Upload SSL Certificate page, click the **Settings** -> **SSL Settings** -> **Upload SSL Certificate** tab from the menu bar.

Figure 53. Snapshot of Upload SSL Certificate Page



The fields on the Upload SSL Certificate page include

- **Current Certificate:** The information of the Current Certificate and date/time of its upload will be displayed (read-only).
- **New Certificate:** Browse and navigate to the new certificate file. Certificate file should be of pem type.
- **Current Private Key:** Information for the current private key and date/time when it was uploaded will be displayed (read-only).
- **New Private Key:** Browse and navigate to the private key file. Private Key file should be of pem type.
- **Save:** To save the configured settings.

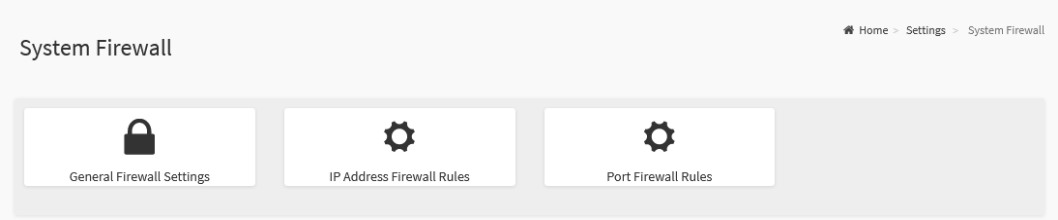
2.10.10 System Firewall

System Firewall page provides various functional feature tabs for users to configure the firewall settings, including

- **General Firewall Settings**
- **IP Address Firewall Rules**
- **Port Firewall Rules**

To view the System Firewall page, click the **Settings** -> **System Firewall** tab from the menu bar.

Figure 54. Snapshot of System Firewall Page



The details about each feature are listed in the following.

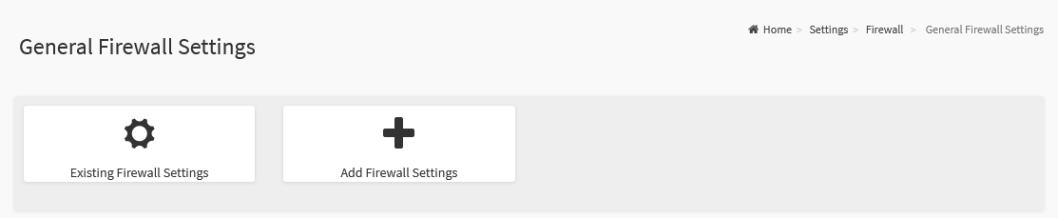
2.10.10.1 General Firewall Settings

This page provides various functional feature tabs for users to configure the General Firewall Settings and monitor the configured settings, including

- **Existing Firewall Settings**
- **Add Firewall Settings**

To view the General Firewall Settings page, click the **Settings** -> **System Firewall** -> **General Firewall Settings** tab from the menu bar.

Figure 55. Snapshot of General Firewall Settings Page



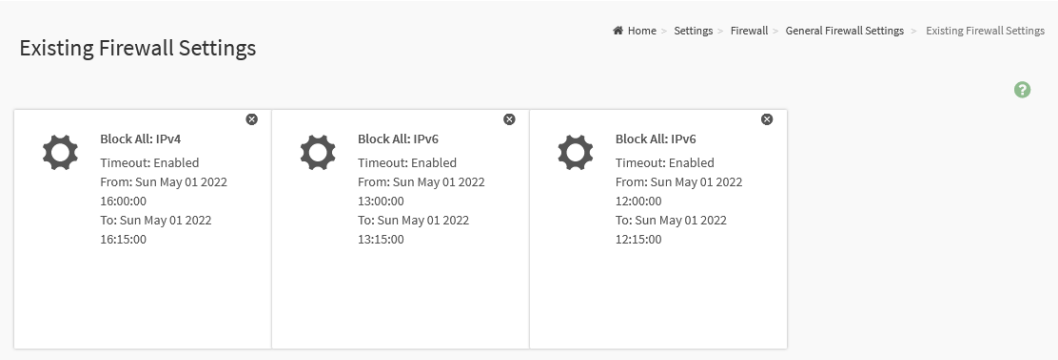
The details about each feature are listed in the following.

2.10.10.1.1 Existing Firewall Settings

This page lists all configured General Firewall Settings instance. A blank page will be opened if users did not add any General Firewall Settings instance from **Add Firewall Settings**.

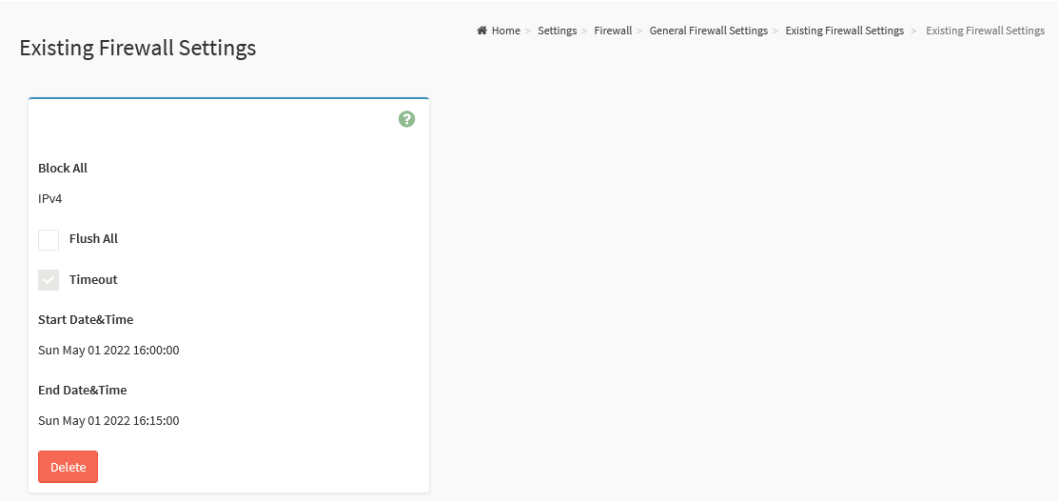
To view the Existing Firewall Settings page, click the **Settings** -> **System Firewall** -> **General Firewall Settings -> Existing Firewall Settings** tab from the menu bar.

Figure 56. Snapshot of Existing Firewall Settings Page of General Firewall Settings



Click on the **Slot** icon ( ) then navigate to instance page.
Click on the **Delete** icon ( ) then delete this slot.

Figure 57. Snapshot of Existing Firewall Settings Instance Page of General Firewall Settings



The fields on the Existing Firmware Settings instance page include

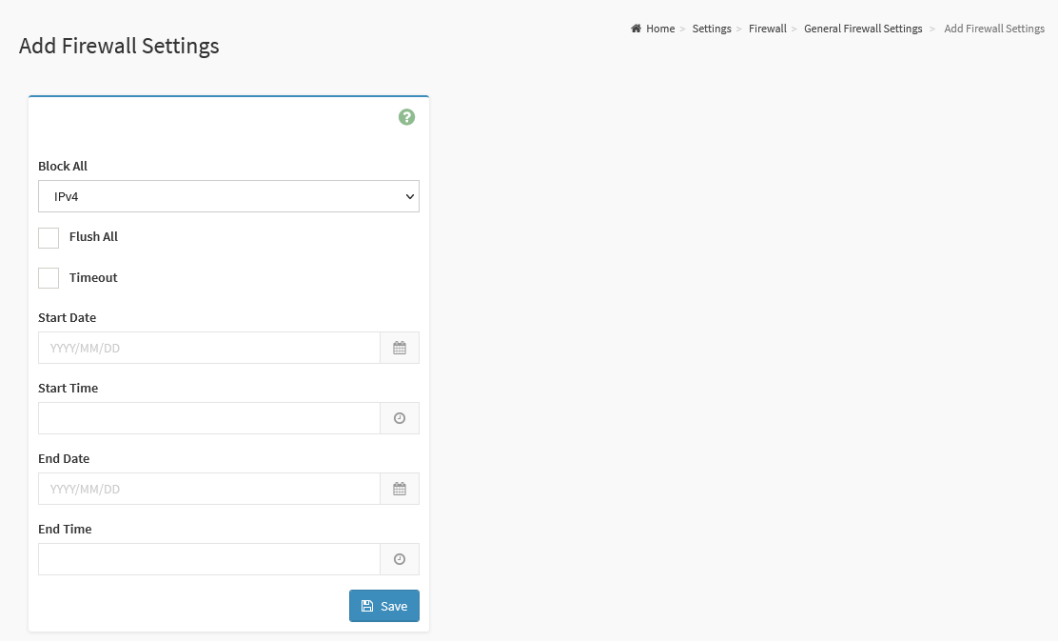
- **Block All:** This option will block all incoming IPs and Ports.
- **Flush All:** This option is used to flush all existing system firewall rules.
- **Timeout:** This field indicates the firewall rules whether with timeout feature.
- **Start Date&Time:** The firewall rule will become effective from this date.
- **End Date&Time:** The firewall rule will expire on this date.
- **Delete:** Click this button to delete this instance.

2.10.10.1.2 Add Firewall Settings

This page provides various options for users to add General Firewall Settings instance.

To view the Add Firewall Settings page, click the **Settings** -> **System Firewall** -> **General Firewall Settings -> Add Firewall Settings** tab from the menu bar.

Figure 58. Snapshot of Add Firewall Settings page of General Firewall Settings



The fields on the Add Firmware Settings page include

- **Block All:** Select the protocol and block all the incoming IP's and Port's.
- **Flush All:** To flush all the system firewall settings.
- **Timeout:** Click this option to enable or disable firewall rules with timeout.
- **Start Date:** To specify a **Start Date** to start respective firewall rule effect from the date.
- **Start Time:** To specify a **Start Time** to start respective firewall rule effect from the Time.
- **End Date:** To specify an **End Date** to end respective firewall rule effect from the date.
- **End Time:** To specify a End Time to End respective firewall rule effect

from the Time.

- **Save:** To save the configured settings.

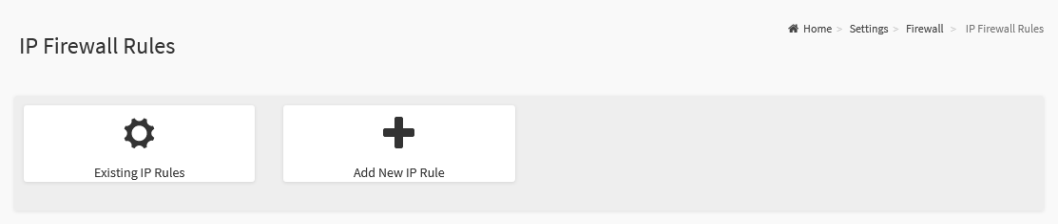
2.10.10.2 IP Address Firewall Rules

This page provides various functional feature tabs for users to configure the IP Firewall Rules and monitor the configured settings, including

- **Existing IP Rules**
- **Add New IP Rule**

To view the IP Firewall Rules page, click the **Settings** -> **System Firewall** -> **IP Address Firewall Rules** tab from the menu bar.

Figure 59. Snapshot of IP Firewall Rules Page



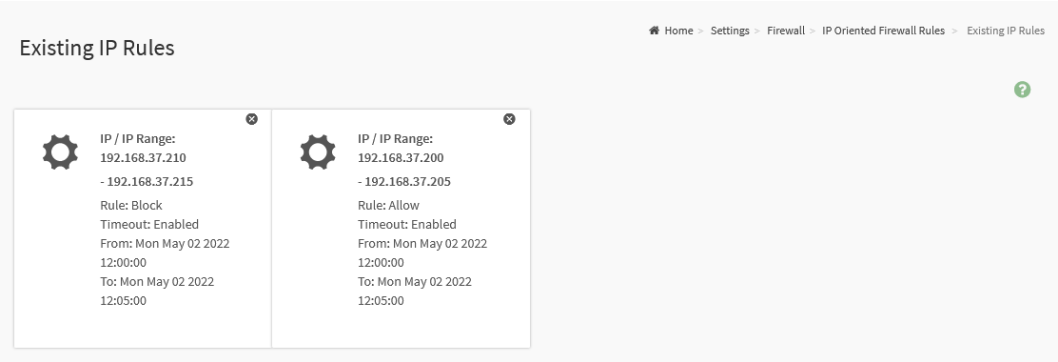
The details about each feature are listed in the following.

2.10.10.2.1 Existing IP Rules

This page lists all configured IP Firewall Rules instances. A blank page will be opened if users did not add any IP Firewall Rules instance from **Add New IP Rule**.

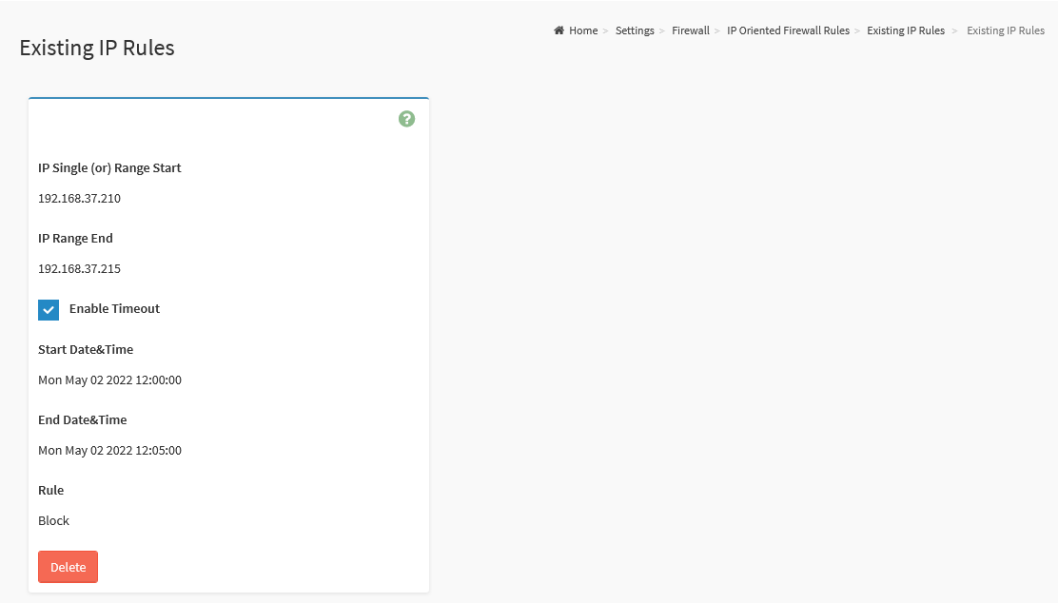
To view the Existing IP Rules page, click the **Settings** -> **System Firewall** -> **IP Address Firewall Rules -> Existing IP Rules** tab from the menu bar.

Figure 60. Snapshot of Existing IP Rules Page



Click on the **Slot** icon ( ) then navigate to instance page.
Click on the **Delete** icon ( ) then delete this slot.

Figure 61. Snapshot of Existing IP Rules Instance Page of IP Firewall Rules



The fields on the Existing IP Rules instance page include

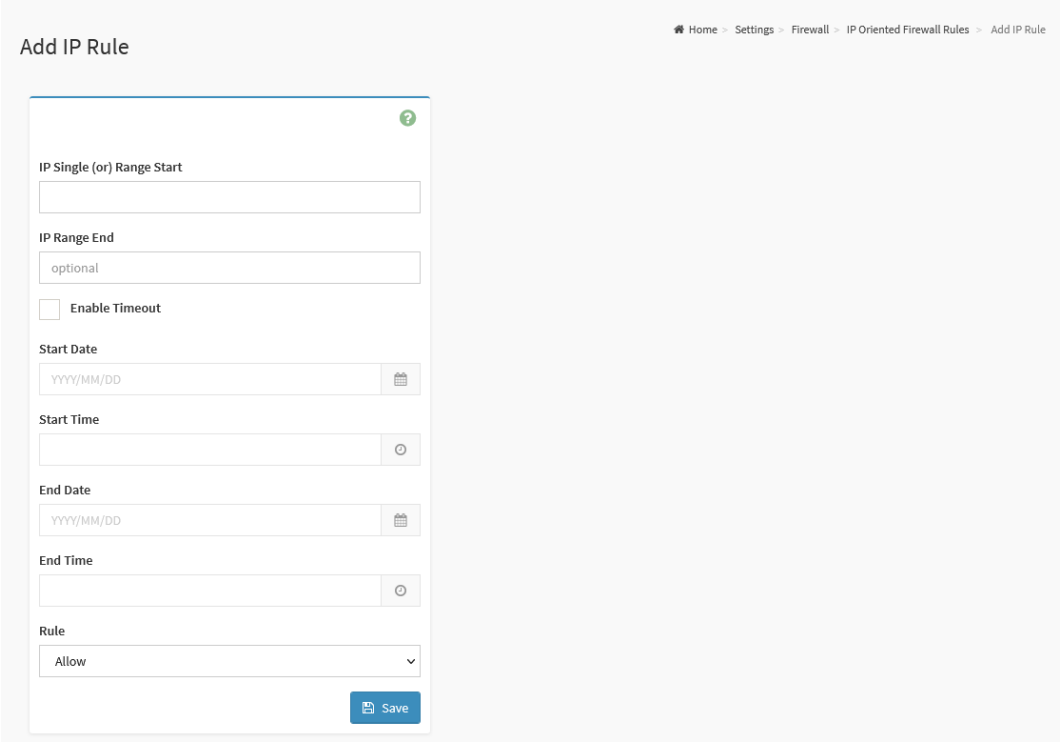
- **IP Single (or) Range Start:** This field indicates IP Address or the start of a Range of IP Addresses
- **IP Range End:** This field indicates the end of a Range of IP Addresses
- **Enable Timeout:** This field indicates the firewall rules whether with timeout feature.
- **Start Date&Time:** The respective firewall rule effect will start from this date and time.
- **End Date&Time:** The respective firewall rule effect will end from this date and time.
- **Rule:** This field indicates the current setting of the listed IP or Range of IP rules (Allow or Block).
- **Delete:** Click this button to delete this instance.

2.10.10.2.2 Add New IP Rule

This page provides various options for users to add IP Firewall Rule instance.

To view the Add New IP Rule page, click the **Settings** -> **System Firewall** -> **IP Address Firewall Rules -> Add New IP Rule** tab from the menu bar.

Figure 62. Snapshot of Add IP Rules Instance Page of IP Firewall Rules



The fields on the Add IP Rule instance page include

- **IP Single (or) Range Start:** To specify an IP Address or the start of a Range of IP Addresses. IP Address must follow the IPv4 Address format:
- **IP Range End:** To specify an end of an IP address range.
- **Enable Timeout:** To enabled or 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 IP Address or Range of IP Addressed rules (Allow or Block) status.
- **Save:** To save the configured settings.

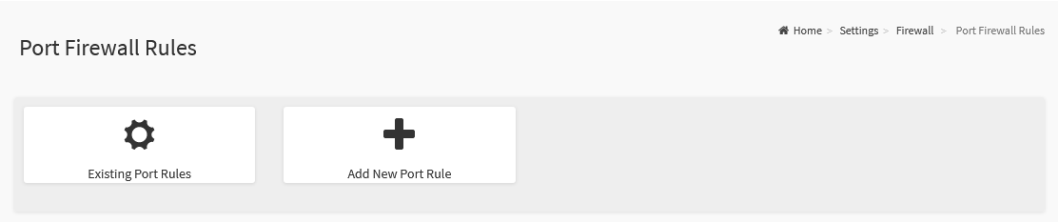
2.10.10.3 Port Firewall Rules

This page provides various functional feature tabs for users to configure the Port Firewall Rules and monitor the configured settings, including

- **Existing Port Rules**
- **Add New Port Rule**

To view the IP Firewall Rules page, click the **Settings** -> **System Firewall** -> **Port Firewall Rules** tab from the menu bar.

Figure 63. Snapshot of Port Firewall Rules Page



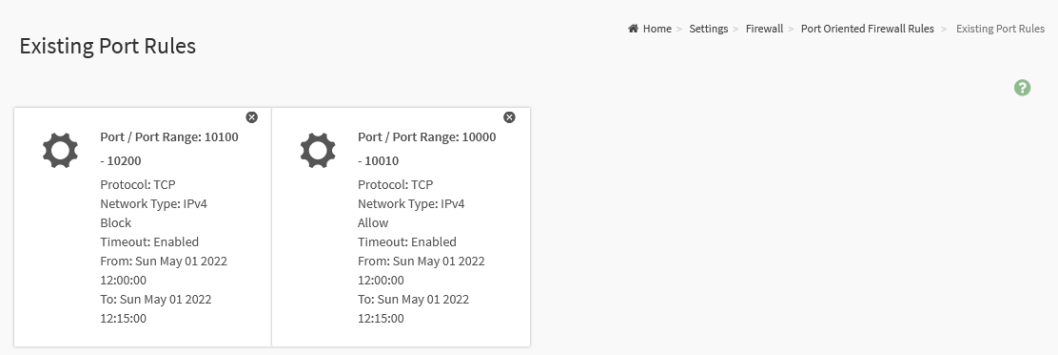
The details about each feature are listed in the following.

2.10.10.3.1 Existing Port Rules

This page lists all configured Port Firewall Rules instances. A blank page will be opened if users did not add any Port Firewall Rules instance from **Add New Port Rule**.

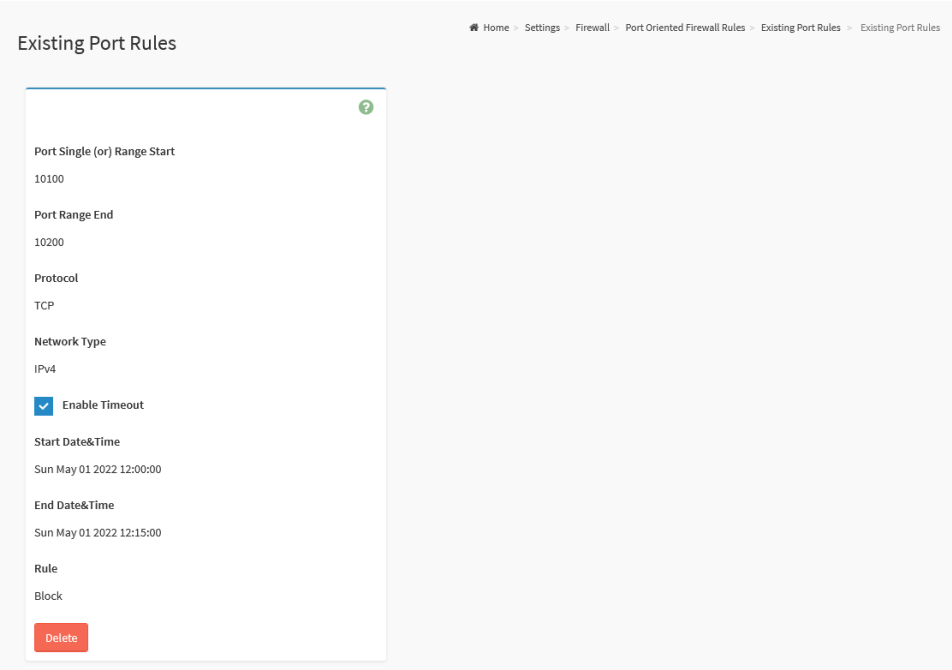
To view the Existing Port Rules page, click the **Settings** -> **System Firewall** -> **Port Firewall Rules -> Existing Port Rules** tab from the menu bar.

Figure 64. Snapshot of Existing Port Rules Page



Click on the **Slot** icon ( ) then navigate to instance page.
Click on the **Delete** icon ( ) then delete this slot.

Figure 65. Snapshot of Existing Port Rules Instance Page of Port Firewall Rules



The fields on the Existing Port Rules instance page include

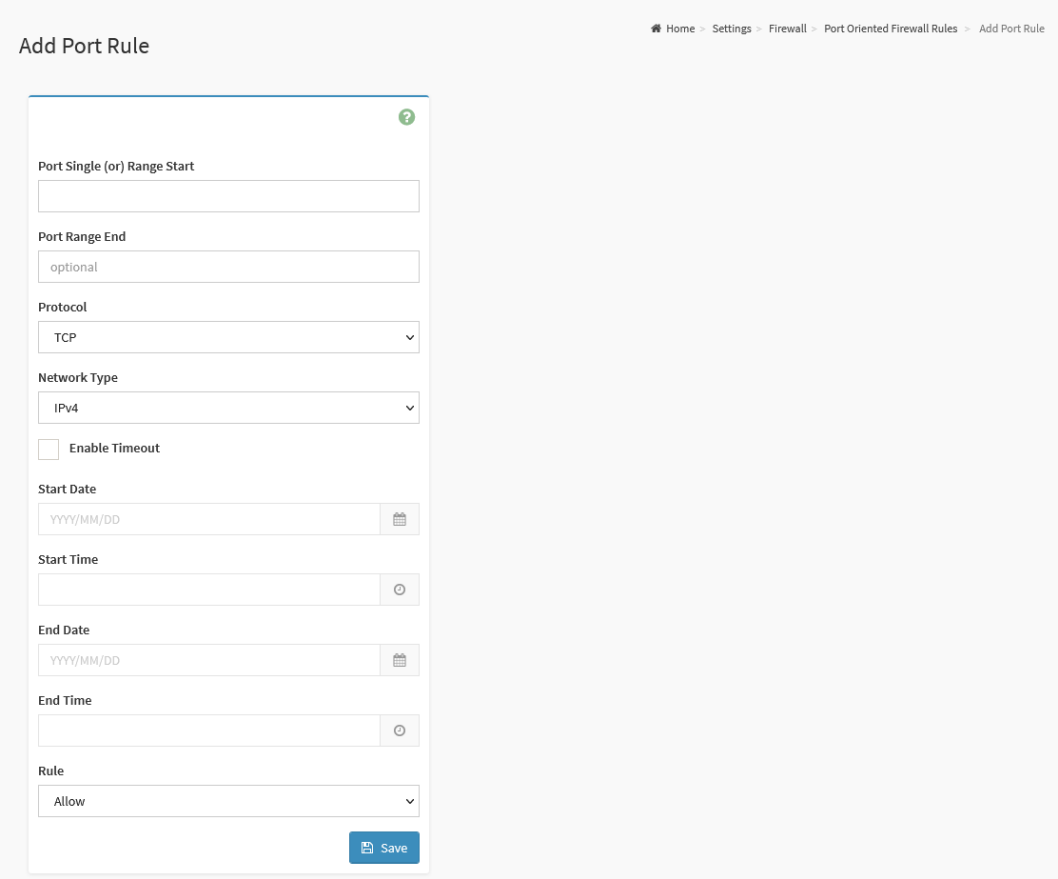
- **Port Single (or) Range Start:** This field indicates the port number or the start of range or port numbers.
- **Port Range End:** This field indicates the end of range or port numbers.
- **Protocol:** This field indicates the protocols for the configured port or range or ports.
- **Network Type:** this field indicates the affected network type for the configured port or range of port numbers.
- **Enable Timeout:** This field indicates the firewall rules whether with timeout feature.
- **Start Date&Time:** The respective firewall rule effect will start from this date and time.
- **End Date&Time:** The respective firewall rule effect will end from this date and time.
- **Rule:** To indicates **Allow** or **Block** status.
- **Delete:** Click this button to delete this instance.

2.10.10.3.2 Add New Port Rule

This page provides various options for users to add Port Firewall Rule instance.

To view the Add New Port Rule page, click the **Settings** -> **System Firewall** -> **Port Firewall Rules -> Add New Port Rule** tab from the menu bar.

Figure 66. Snapshot of Add Port Rules Instance Page of Port Firewall Rules



The fields on the Add Port Rule instance page include

- **Port Single (or) Range Start:** To specify the port number or start of a range of port numbers.
- **Port Range End:** To specify the end of a range of port numbers.
- **Protocol:** To select the protocol for the configured port or port ranges.
- **Network Type:** To select the affected network type for the configured port or port ranges.
- **Enable Timeout:** Click this option to enabled or disabled timeout.

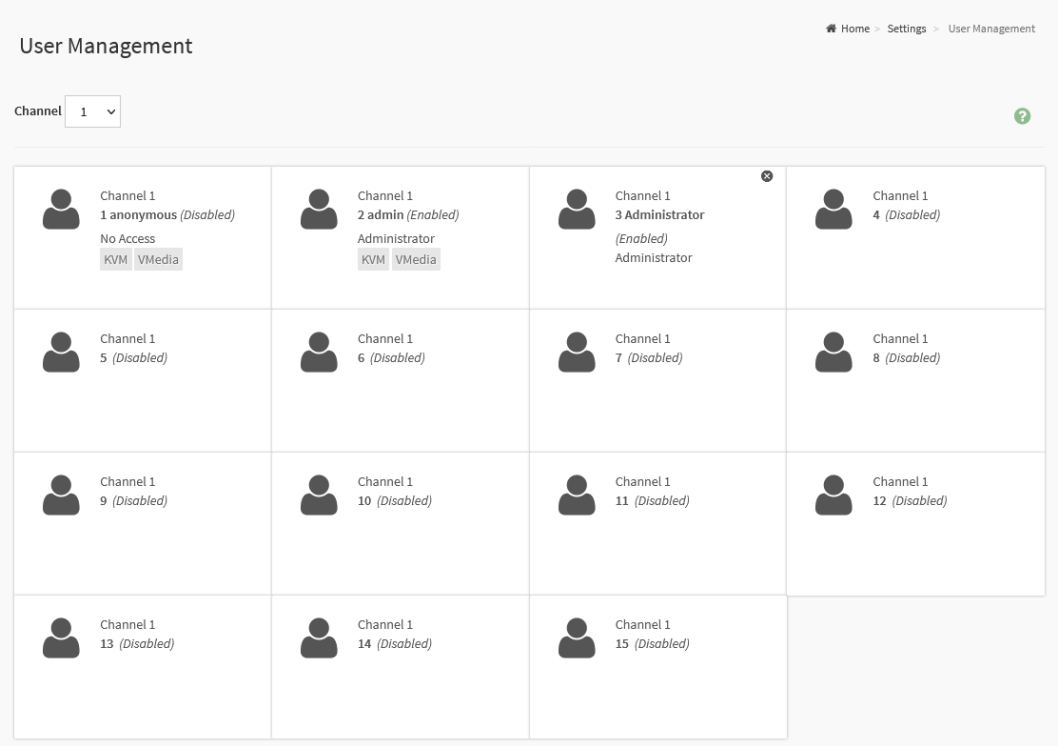
- **Start Date:** The respective firewall rule effect will start from this date.
- **Start Time:** The respective firewall rule effect will start from this time.
- **End Date:** The respective firewall rule effect will end from this date.
- **End Time:** The respective firewall rule effect will end from this time.
- **Rule:** To indicate **Allow** or **Block** status.
- **Save:** To save the configured settings.

2.10.11 User Management

User Management page provides various options for users to view the current list of user slots for the CMM, and allow users to add a new user and modify or delete existing user.

To view the User Management page, click the **Settings** -> **User Management** tab from the menu bar.

Figure 67. Snapshot of User Management Page



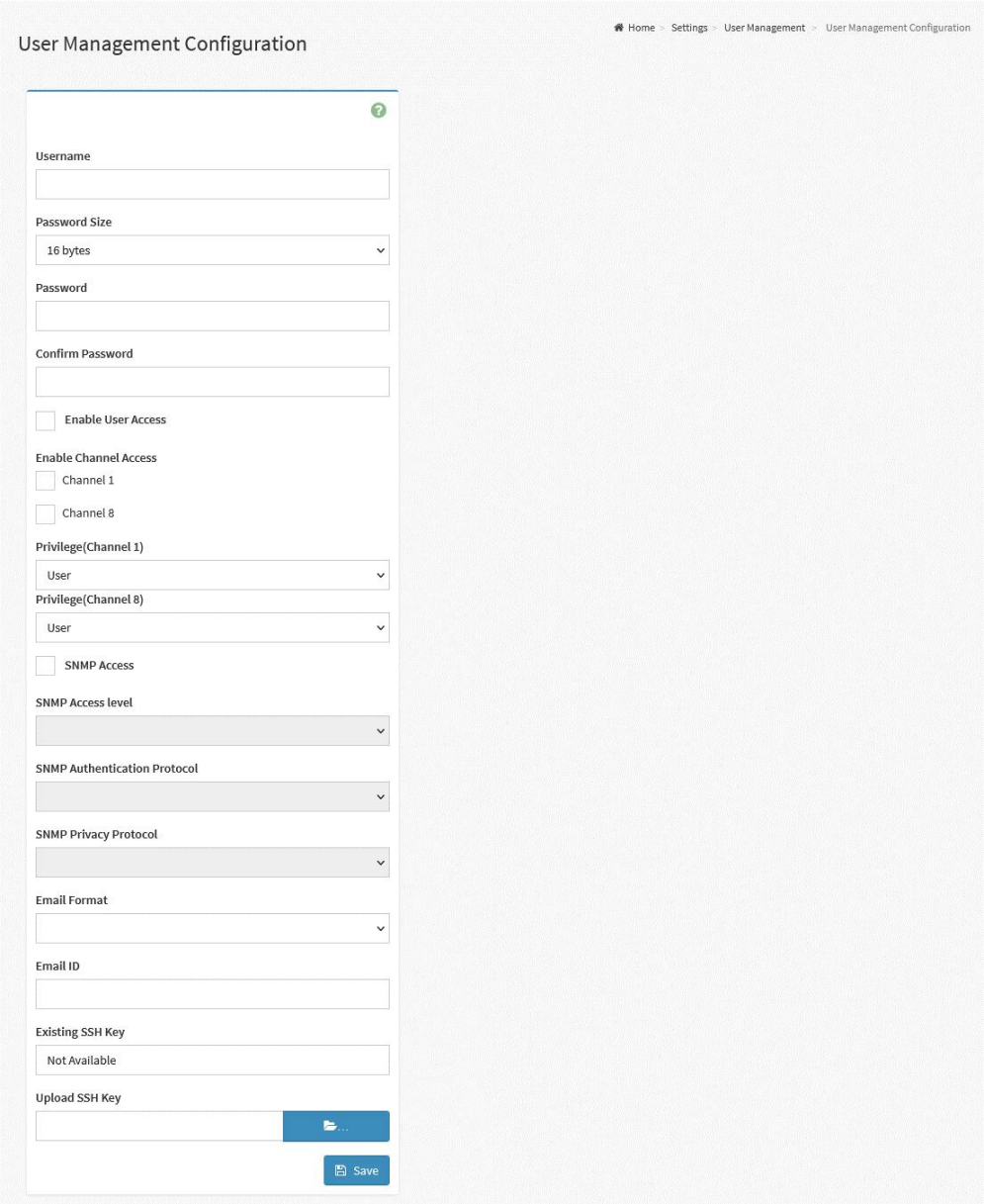
Channel 1 for users connect to CMM through dedicated IPMI LAN port.

Channel 8 for users connect to CMM through Share NIC LAN port.

Click on the **User** icon ( ) then navigate to User Management Configuration page.

Click on the **Delete** icon ( ) then delete this slot.

Figure 68. Snapshot of User Management Configuration Page



The fields on the User Management Configuration page include

- **Username:** To specify a name for the user.
- **Password Size:** To select the preferred size for the password.
- **Password:** Password field is mandatory and should meet the password policy requirements.
- **Confirm Password:** Entering the password again to confirm the password.

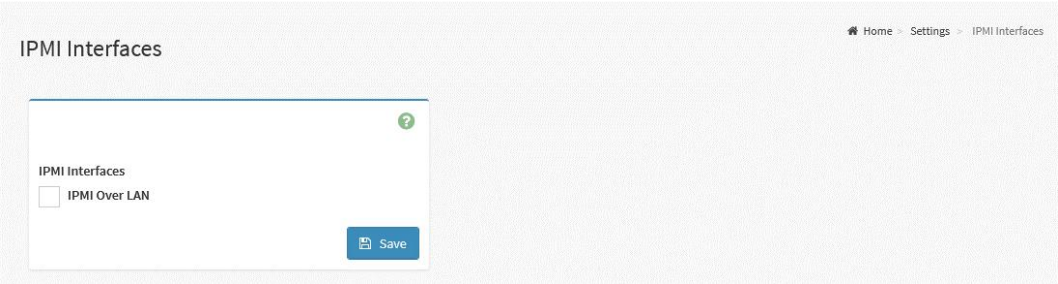
- **Password age (days):** Enable and set the maximum password age.
- **End date:** To select the date for the expired date of password age.
- **Current valid date:** To indicate valid date of current.
- **Enable User Access:** Click this option to enable this user account to access the CMM service.
- **Enable Channel Access:** To select the channel/channels to enable the network access for the user.
  - **Channel 1:** Allow user to access the CMM service through dedicated IPMI LAN port.
  - **Channel 8:** Allow user to access the CMM service through Share NIC LAN port.
- **Privilege (Channel 1)** and **Privilege (Channel 8):** Select the privilege level for each channel to be assigned to this user for access to the CMM through the network interface. There are 5 levels of Network Privileges (Administrator, Operator, User, OEM and None).
- **KVM Access:** Click this option to assign the KVM privilege for the user.
- **VMedia Access:** Click this option to assign the VMedia privilege for the user.
- **SNMP Access:** Click this option to assign the SNMP privilege for the user.
- **SNMP Access level:** To select the SNMP access level for the user.
- **SNMP Authentication Protocol:** To select the Authentication Protocol for the user.
- **SNMP Privacy Protocol:** To select the Encryption algorithm to be used for the SNMP settings.
- **Email Format:** To specify the format for the email
- **Email ID:** To specify the email ID for the user.
- **Existing SSH Key:** If available, the uploaded SSH key information will be displayed.
- **Upload SSH Key:** Use Browse button to navigate to the new public SSH key file.
- **Delete:** Click Delete button to delete this user account.
- **Save:** To save the configured settings.

2.10.12 IPMI Interfaces

IPMI Interfaces page provides various options for users to configure the IPMI communication interface settings.

To view the IPMI Interfaces page, click the **Settings** -> **IPMI Interfaces** tab from the menu bar.

Figure 69. Snapshot of IPMI Interfaces Page



The fields on the IPMI Interfaces page include

- **IPMI Interfaces:** To select the interface which allow users to perform the IPMI communication.
  - **IPMI Over LAN:** Click this option to allows the IPMI communication over LAN.
- **Save:** To save the configured settings.

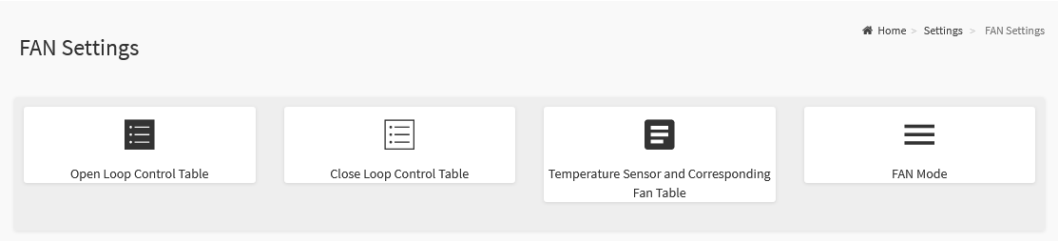
2.10.13 FAN Settings

FAN Settings page provides various functional feature tabs for users to configure the system FAN settings which control by the CMM, including

- **Open Loop Control Table**
- **Close Loop Control Table**
- **Temperature Sensor and Corresponding Fan Table**
- **FAN Mode**

To view the FAN Settings page, click the **Settings** -> **FAN Settings** tab from the menu bar.

Figure 70. Snapshot of FAN Settings Page



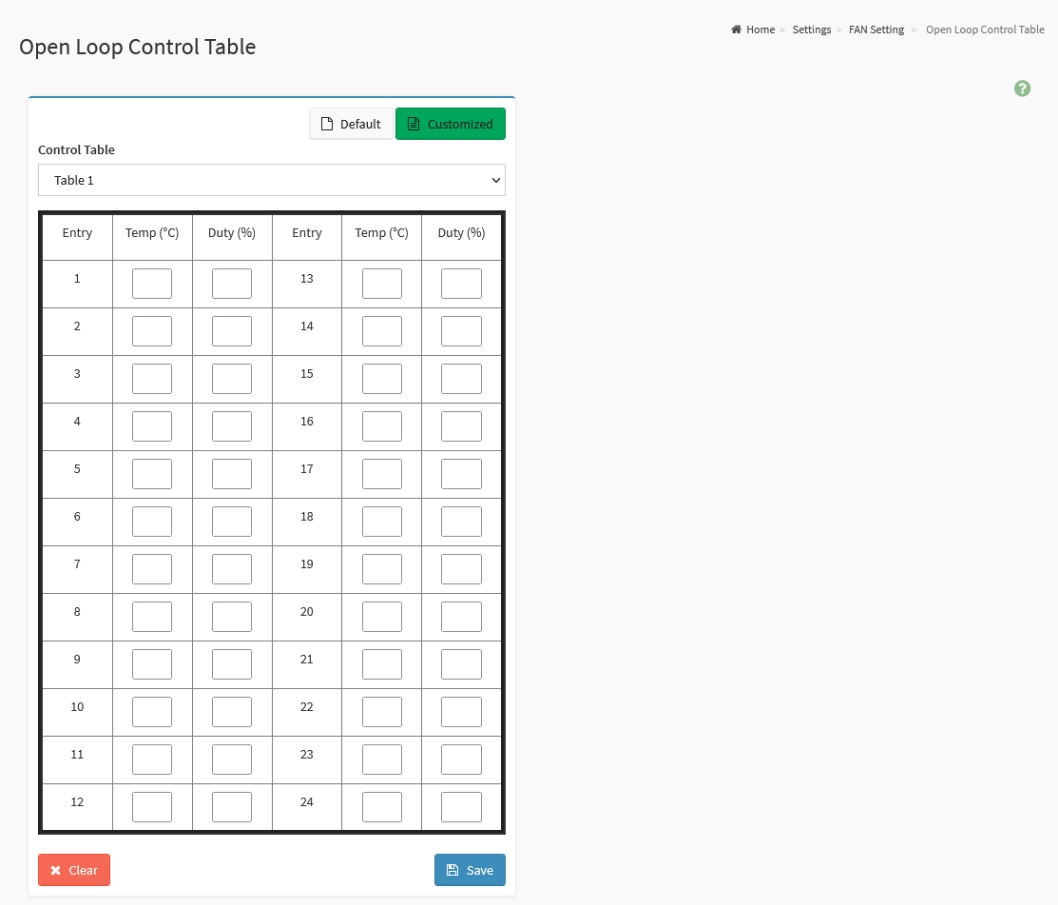
The details about each feature are listed in the following.

2.10.13.1 Open Loop Control Table

This page provides various options for users to configure the Open Loop Control Table settings, users can add the new FAN table from **Temperature Sensor and Corresponding Fan Table**

To view the Open Loop Control Table FAN page, click the **Settings** -> **FAN Settings** -> **Open Loop Control Table FAN** tab from the menu bar.

Figure 71. Snapshot of Open Loop Control Table Page



The fields on the Open Loop Control Table page include

- **Control Table:** To select the table which to be used.
- **Entry:** Indicates the condition number.
- **Temp (°C):** To specify the temperature for this entry.
- **Duty (%):** To specify the FAN duty for this entry.
- **Default:** Click **Default** button to loading the default setting value of selected table.

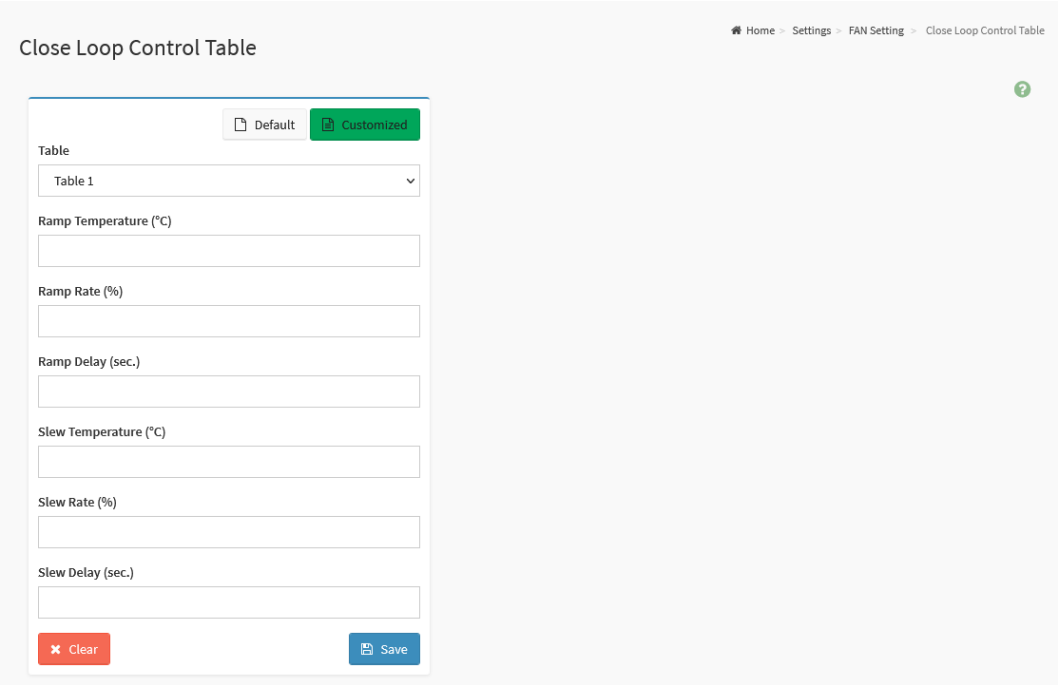
- **Customized:** Click the **Customized** button to modify the settings value for selected table.
- **Clear:** To clear current settings value on the web.
- **Save:** To save the configured settings.

2.10.13.2 Close Loop Control Table

This page provides various options for users to configure the Close Loop Control Table settings, users can add the new FAN table from **Temperature Sensor and Corresponding Fan Table**

To view the Open Loop Control Table FAN page, click the **Settings** -> **FAN Settings** -> **Close Loop Control Table FAN** tab from the menu bar.

Figure 72. Snapshot of Close Loop Control Table Page



The fields on the Close Loop Control Table page include

- **Table:** To select the table which to be used.
- **Ramp Temperature (°C):** To specify the value for Ramp Temperature.
- **Ramp Rate (%):** To specify the value for Ramp Rate.
- **Ramp Delay (sec.):** To specify the value for Ramp Delay.
- **Slew Temperature (°C):** To specify the value for Slew Temperature.
- **Slew Rate (%):** To specify the value for Slew Rate.
- **Slew Delay (sec.):** To specify the value for Slew Delay.
- **Default:** Click **Default** button to loading the default setting value of selected table.
- **Customized:** Click the **Customized** button to modify the settings value

for selected table.

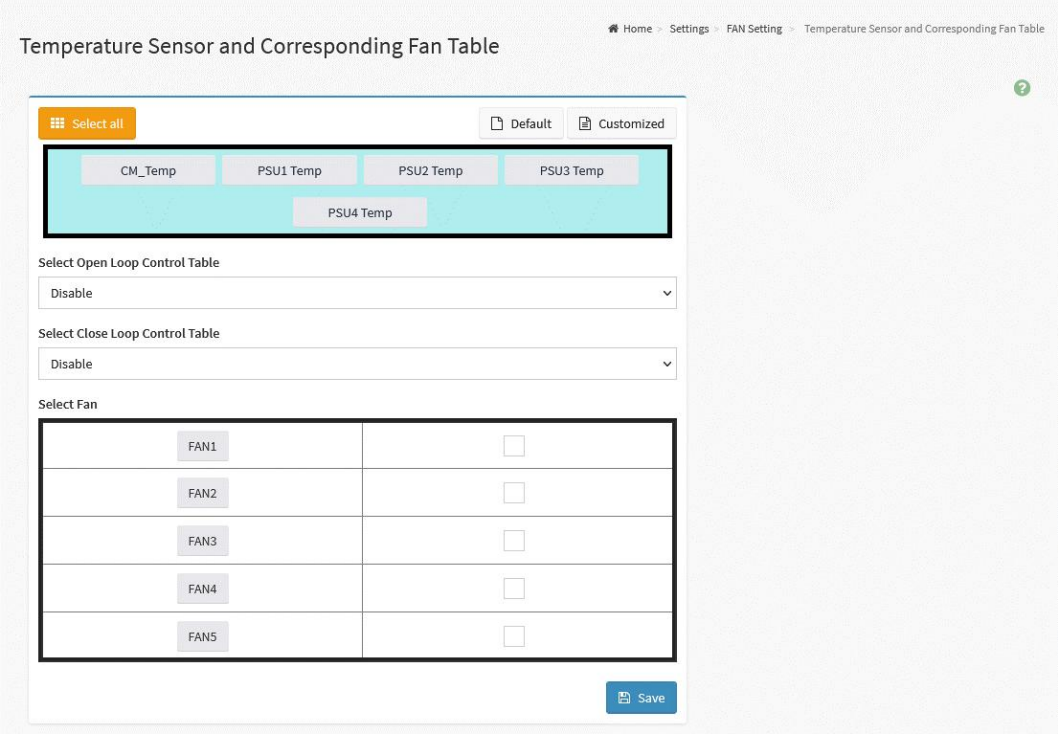
- **Clear:** To clear current settings value on the web.
- **Save:** To save the configured settings.

2.10.13.3 Temperature Sensor and Corresponding Fan Table

This page provides various options for users to configure the temperature sensor and FAN table settings for **Open Loop Control Table** and **Close Loop Control Table** use.

To view the Temperature Sensor and Corresponding Fan Table page, click the **Settings** -> **FAN Settings** -> **Temperature Sensor and Corresponding Fan Table** tab from the menu bar.

Figure 73. Snapshot of Temperature Sensor and Corresponding Fan Table Page



The fields on the Temperature Sensor and Corresponding Fan Table page include

- **Select Open Loop Control Table:** To select the Open Loop Control Table which to be used.
- **Select Close Loop Control Table:** To select the Close Loop Control Table which to be used.
- **Select Fan:** To select the FAN which affect in the selected table.
- **Select All:** Click this button to select all sensors in the sensor list.

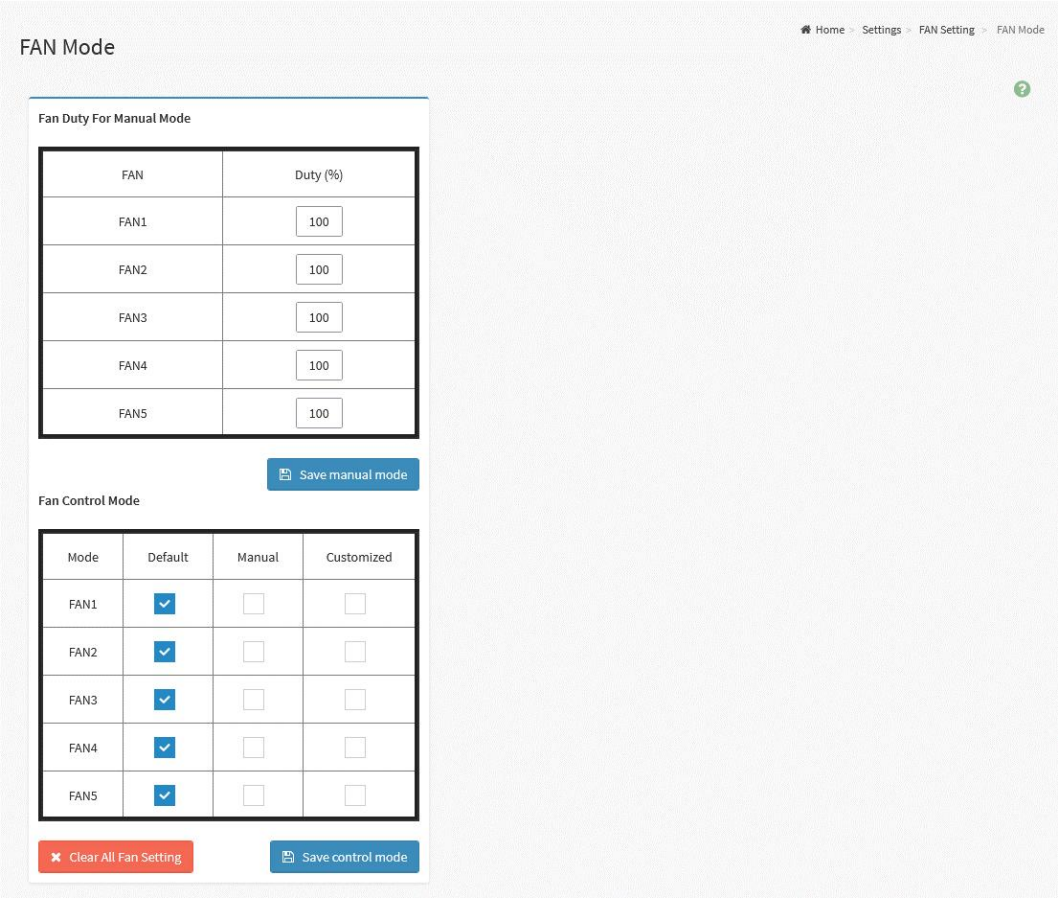
- **Default:** Click **Default** button to loading the default setting value (the default selected FAN) of selected temperature sensor.
- **Customized:** Click the **Customized** button to modify the settings value for the selected FAN.
- **Save:** To save the configured settings.

2.10.13.4 FAN Mode

This page provides various options for users to configure the fan control mode settings, including control mode and fan duty for manual mode.

To view the FAN Mode page, click the **Settings** -> **FAN Settings** -> **FAN Mode** tab from the menu bar.

Figure 74. Snapshot of FAN Mode Page



The fields on the FAN Mode page include

- **Fan Duty For Manual Mode:** To specify the fan duty value for the specific FAN while runs in manual mode.
- **Save manual mode:** To save the configured settings of Manual Mode.
- **Fan Control Mode:** To select the fan control mode.
- **Clear All Fan Setting:** Click **Clear All Fan Setting** button to clear current setting value.
- **Save Control Mode:** Click **Save Control Mode** button to save the configured settings.

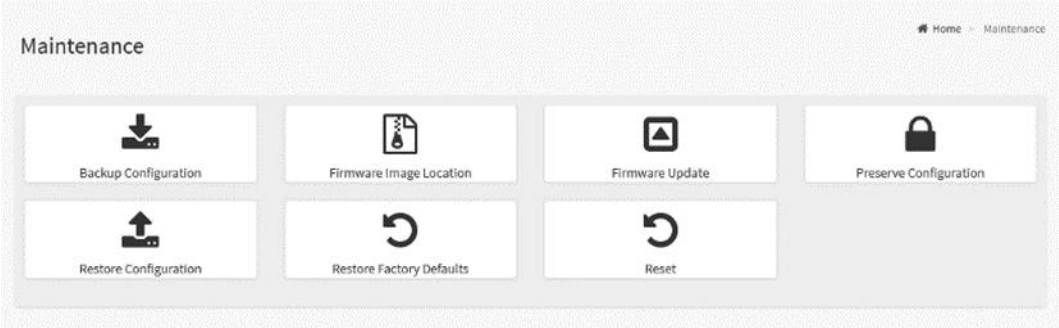
2.11 Maintenance

Maintenance page provides various functional feature for users to do maintenance task on the device, including

- **Backup Configuration**
- **Firmware Image Location**
- **Firmware Update**
- **Preserve Configuration**
- **Restore Configuration**
- **Restore Factory Defaults**
- **Reset**

To view the Maintenance page, click the **Maintenance** tab from the menu bar.

Figure 75. Snapshot of Maintenance Page



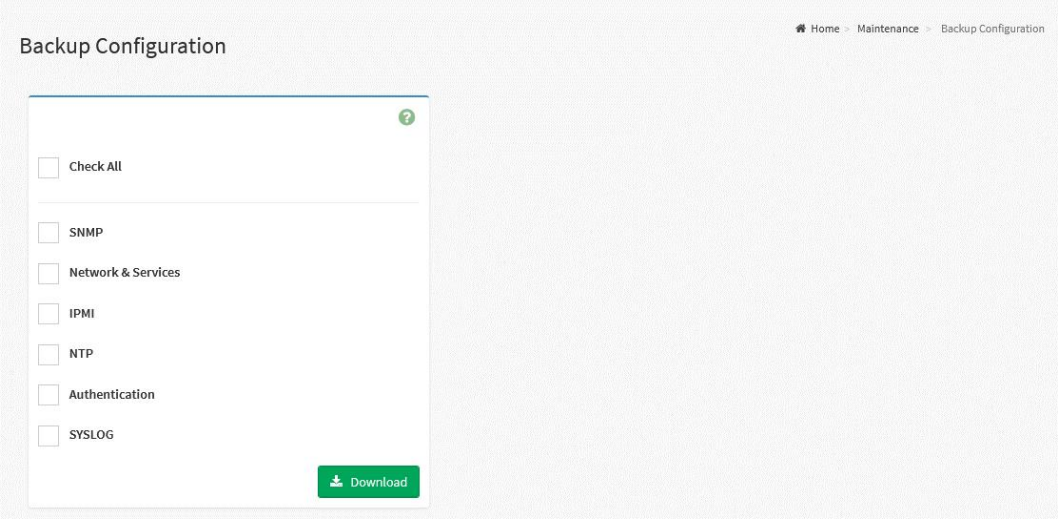
The details about each feature are listed in the following.

2.11.1 Backup Configuration

Backup Configuration page provides various options for users to select the specific configuration items to be backup in case of **Backup Configuration**.

To view the Backup Configuration page, click the **Maintenance** -> **Backup Configuration** tab from the menu bar.

Figure 76. Snapshot of Backup Configuration Page



The fields on the Backup Configuration page include

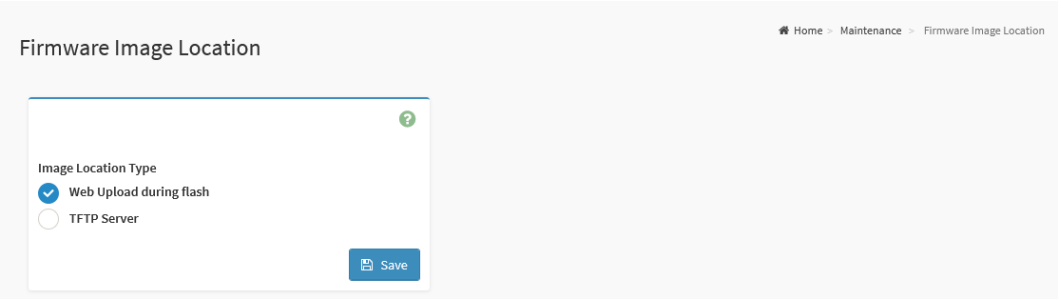
- **Check All:** Click this option to select all configuration items listed on the page.
- **SNMP:** Click this option to be backup SNMP settings.
- **Network & Services:** Click this option to be backup Network & Services settings.
- **IPMI:** Click this option to be backup IPMI settings.
- **NTP:** Click this option to be backup NTP settings.
- **Authentication:** Click this option to be backup Authentication settings.
- **SYSLOG:** Click this option to be backup SYSLOG file.
- **Download:** Click **Download** button to download the selected item backup file.

2.11.2 Firmware Image Location

Firmware Image Location page provides various options for users to configure the image transfer protocol for transfer the firmware image onto CMM.

To view the Firmware Image Location page, click the **Maintenance** -> **Firmware Image Location** tab from the menu bar.

Figure 77. Snapshot of Firmware Image Location Page



The fields on the Firmware Image Location page include

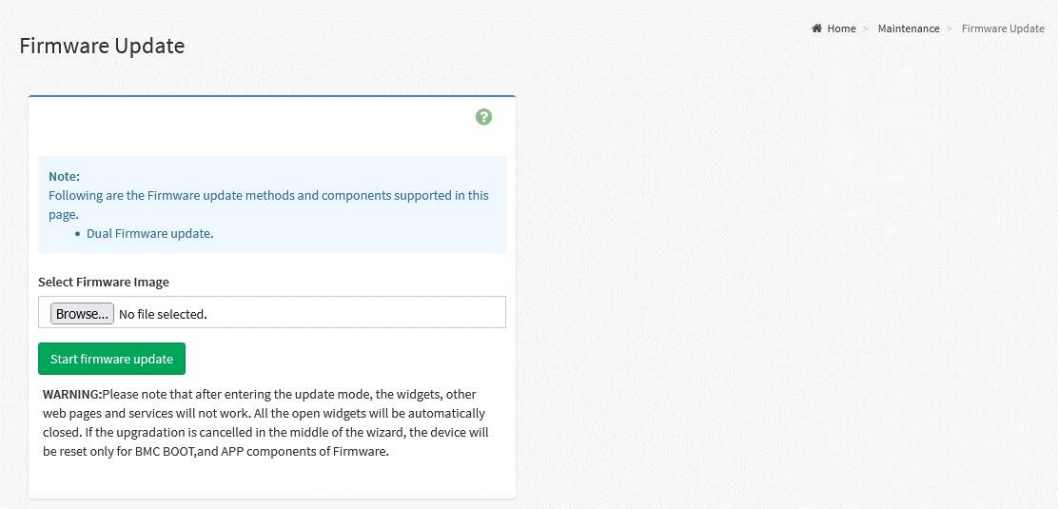
- **Image Location Type:** To select the type of transfer the firmware image into the CMM either **Web Upload during flash** or **TFTP Server**.
  - **Web Upload during flash:** Transfer firmware image through web service.
  - **TFTP Server:** Transfer firmware image through TFTP protocol.
    - **TFTP Server Address:** To specify the address of TFTP server where the firmware image stored.
    - **TFTP Image Name:** To specify the firmware image file name.
    - **TFTP Retry Count:** To specify the number of times to be retried in case a transfer failure occurs.
- **Save:** To save the configured settings.

2.11.3 Firmware Update

Firmware Update page provides the option for users to update the CMM firmware through CMM web service.

To view the Firmware Update page, click the **Maintenance** -> **Firmware Update** tab from the menu bar.

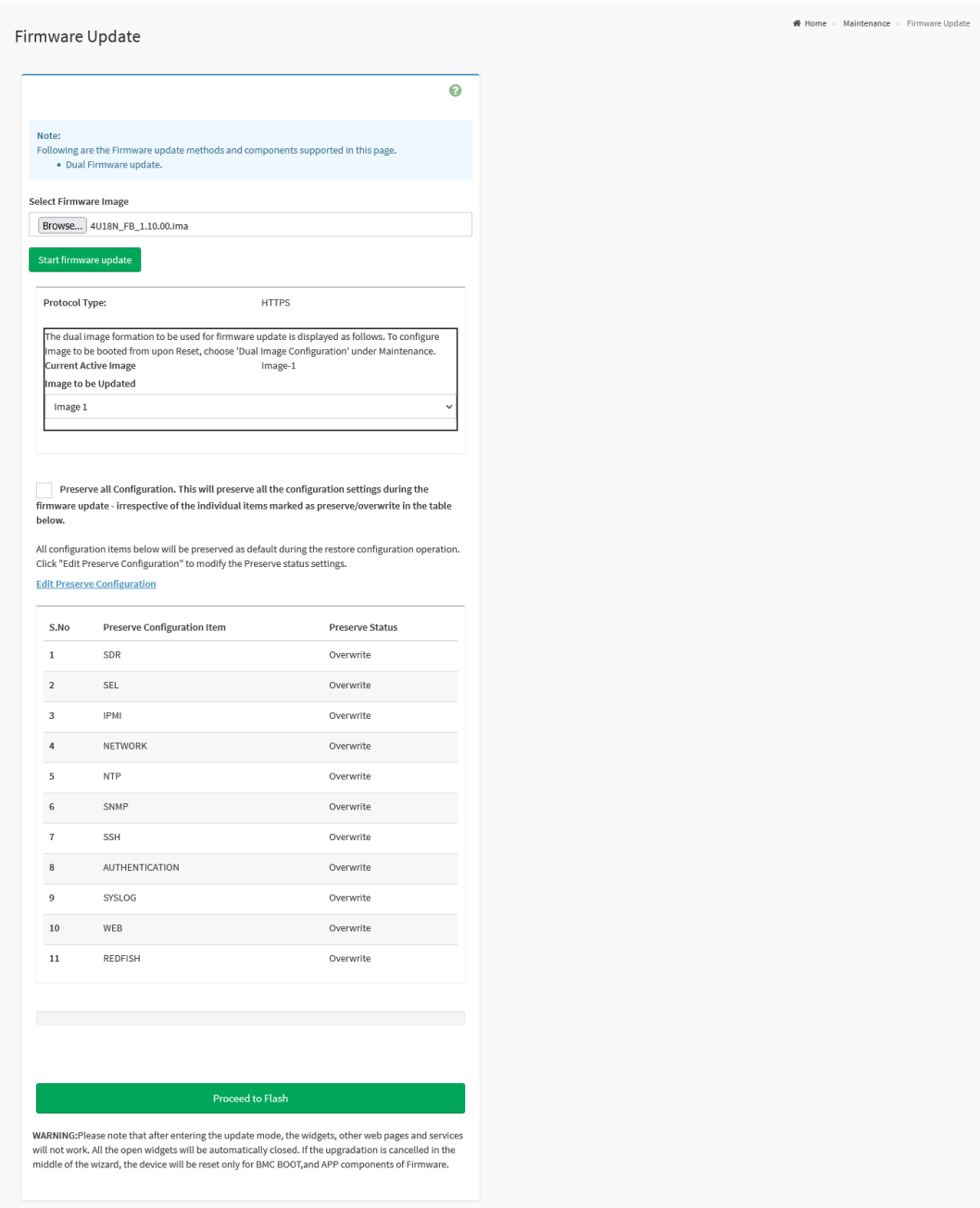
Figure 78. Snapshot of Firmware Update Page



The fields on the Firmware Update page include

- **Browse:** Click the Browse button to open file upload window, then select the to be updated firmware image file.
- **Start Firmware Update:** Click the Start Firmware Update button to navigate to the Firmware Update Configuration page.

Figure 79. Snapshot of Firmware Update Configuration Page

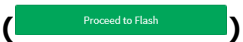


The fields on the Firmware Update Configuration page include

- **Start Firmware Update (** Start firmware update **)**
- **Protocol Type:** Indicates the protocol type of firmware update process used.
- **Current Active Image:** Indicates the current used image on the CMM.
- **Image to be Updated:** Select the target to be updated the CMM

firmware. Supported targets are listed below:

- **Inactive Image:** Select this target that will updating the Inactive Image firmware content.
- **Image 1:** Select this target that will updating the Image 1 firmware content.
- **Image 2:** Select this target that will updating the Image 2 firmware content.
- **Both Images:** Select this target that will updating the both Image 1 and Image 2 firmware content.

- **Preserve all Configuration:** Click this option to preserve all supported configuration settings that listed on the page.
- **Edit Preserve Configuration:** Click this link and navigate to the Preserve Configuration page to edit the preserve configuration settings.
- **Proceed to Flash (

):** Click this button to start firmware update process with users' configuration settings.

2.11.3.1 Updating CMM Firmware

Users can update the CMM firmware using the CMM WebUI service.

The firmware update will clean all current settings on the CMM firmware by default, users can edit the preserve configuration settings to preserve the specify item settings, or click preserve all configuration option the preserve all current settings on the firmware update configuration page.

During the CMM firmware update process, it is normal that some or all fan of the fan devices in the system to run at 100% speed.

2.11.3.1.1 Updating CMM Firmware Using WebUI Service.

To update the CMM firmware using the CMM WebUI service:

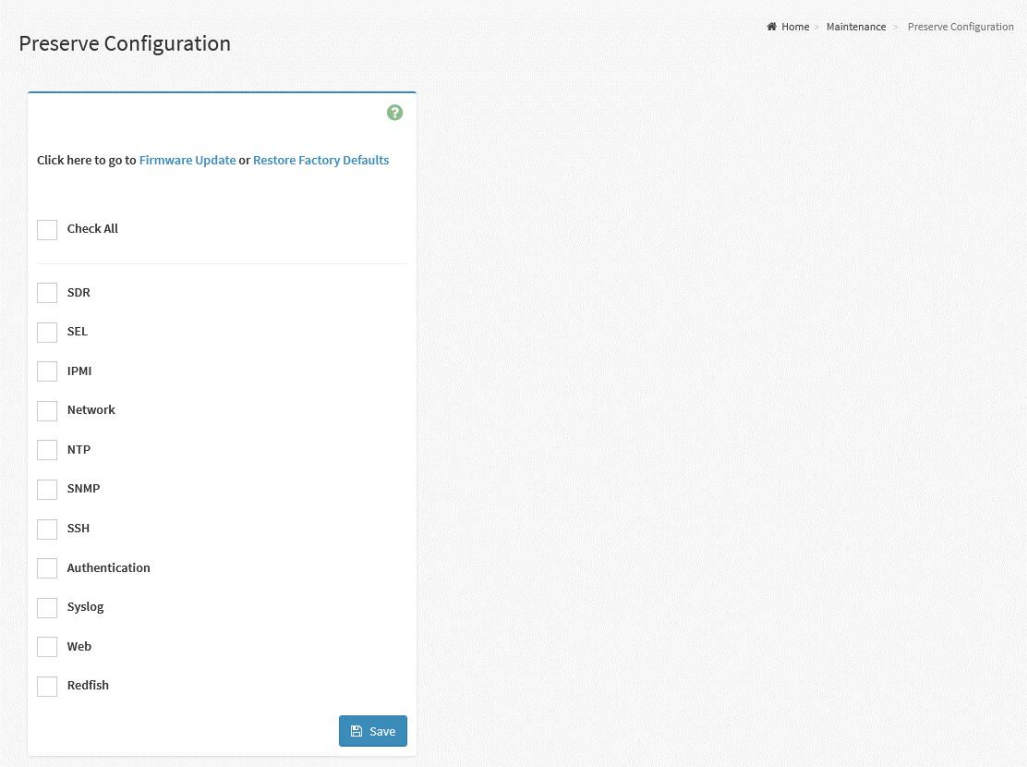
1. Go to the following page:
   Maintenance -> **Firmware Update**
   The Firmware Update page is displayed.
2. In the Firmware Update page, click the **Browser** button to open file upload window and select the to be updated firmware file, then click the **Start Firmware Update** button to navigate to Firmware Update Configuration page.
3. In the Firmware Update Configuration page, edit the options of preserve configuration settings for firmware update process.
4. Click the **Proceed to Flash** button to start the CMM firmware update process, and then click the **OK** button in the popup window to continue.

2.11.4 Preserve Configuration

Preserve Configuration page provides various options for users to configure the to be preserved configuration settings while flashing CMM firmware image.

To view the Preserve Configuration page, click the **Maintenance** -> **Preserve Configuration** tab from the menu bar.

Figure 80. Snapshot of Preserve Configuration Page



The fields on the Preserve Configuration page include

- **Check All:** Click this option to select all configuration items listed on the page.
- **SDR:** Click this option to be preserve the SDR settings.
- **SEL:** Click this option to be preserve the SEL settings.
- **IPMI:** Click this option to be preserve the IPMI settings.
- **Network:** Click this option to be preserve the Network settings.
- **NTP:** Click this option to be preserve the NTP settings.
- **SNMP:** Click this option to be preserve the SNMP settings.

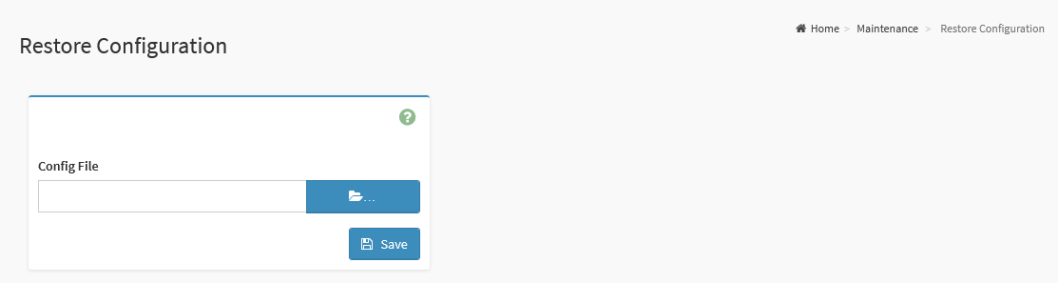
- **SSH:** Click this option to be preserve the SSH settings.
- **Authentication:** Click this option to be preserve the Authentication settings.
- **Syslog:** Click this option to be preserve the Syslog settings.
- **Web:** Click this option to be preserve the Web settings.
- **Redfish:** Click this option to be preserve the Redfish settings.
- **Save:** To save the configured settings.

2.11.5 Restore Configuration

Restore Configuration page provides the option for users to restoring configuration settings through CMM web service with the backup file. Users can generate the configuration backup file from the **Backup Configuration** page.

To view the Restore Configuration page, click the **Maintenance** -> **Restore Configuration** tab from the menu bar.

Figure 81. Snapshot of Restore Configuration Page



The fields on the Restore Configuration page include

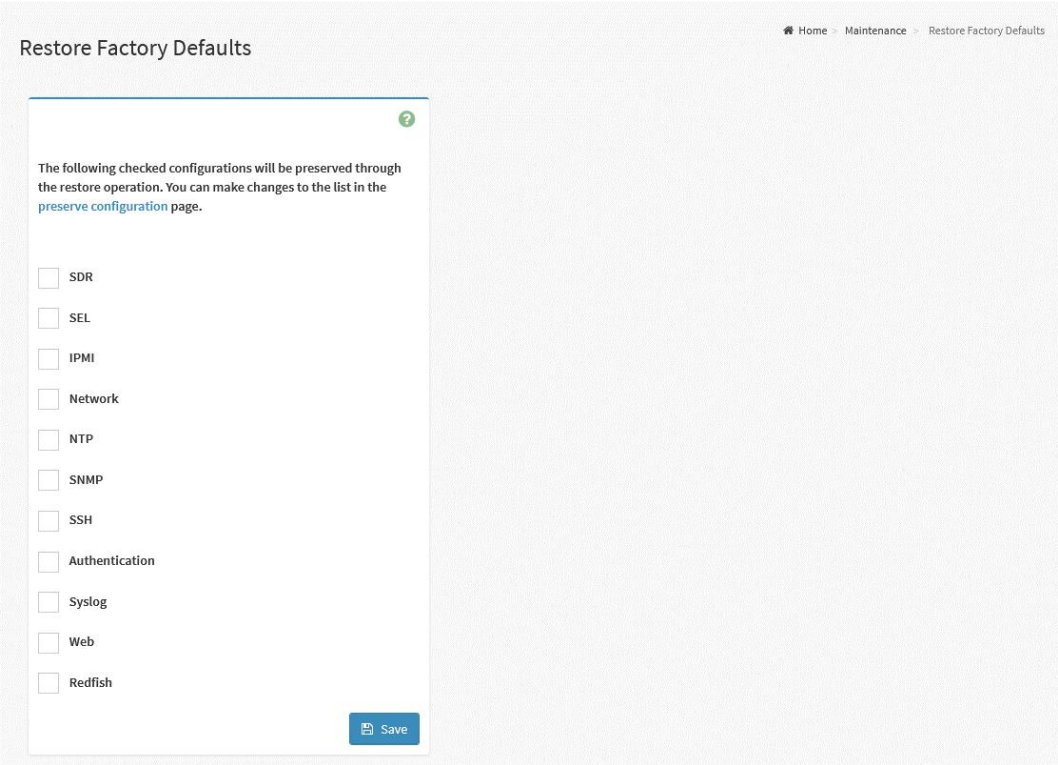
- **Config File:** Click the **Browse** icon ( ) to open file upload window, then select the to be updated backup config file.
- **Save:** Click the **Save** button to start the restore configuration process.

2.11.6 Restore Factory Defaults

Restore Factory Defaults page provides various options for users to configure the preserve configurations, which will be preserved during the process of restore CMM firmware settings to the factory defaults.

To view the Restore Factory Defaults page, click the **Maintenance** -> **Restore Factory Defaults** tab from the menu bar.

Figure 82. Snapshot of Restore Factory Defaults Page



The fields on the Restore Factory Defaults page include

- **SDR:** Click this option to preserve the SDR settings during restore factory defaults process.
- **SEL:** Click this option to preserve the SEL settings during restore factory defaults process.
- **IPMI:** Click this option to preserve the IPMI settings during restore factory defaults process.
- **Network:** Click this option to preserve the Network settings during restore factory defaults process.

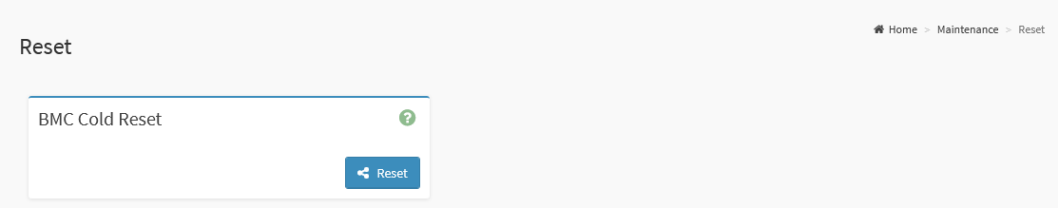
- **NTP:** Click this option to preserve the NTP settings during restore factory defaults process.
- **SNMP:** Click this option to preserve the SNMP settings during restore factory defaults process.
- **SSH:** Click this option to preserve the SSH settings during restore factory defaults process.
- **Authentication:** Click this option to preserve the Authentication settings during restore factory defaults process.
- **Syslog:** Click this option to preserve the Syslog settings during restore factory defaults process.
- **Web:** Click this option to preserve the Web settings during restore factory defaults process.
- **Redfish:** Click this option to preserve the Redfish settings during restore factory defaults process.
- **Save:** To perform the restore factory defaults process with configured settings.

2.11.7 Reset

Reset page provide the option for users to perform a BMC cold reset to reset the device.

To view the Reset page, click the **Maintenance** -> **Reset** tab from the menu bar.

Figure 83. Snapshot of Reset Page



The fields on the Reset page include

- **Reset:** Click the **Reset** button to perform a BMC cold reset to reset the device.

2.12 Sign Out

To log out the CMM web service properly, click the **Sign out** button or tab is recommended.

To perform a sing out, click the **Sign out** tab from the menu bar or click the **Sign out** button from the current user window on the top right corner of the CMM WebUI screen.

Figure 84. Snapshot of Sign Out Button on the Current User Window