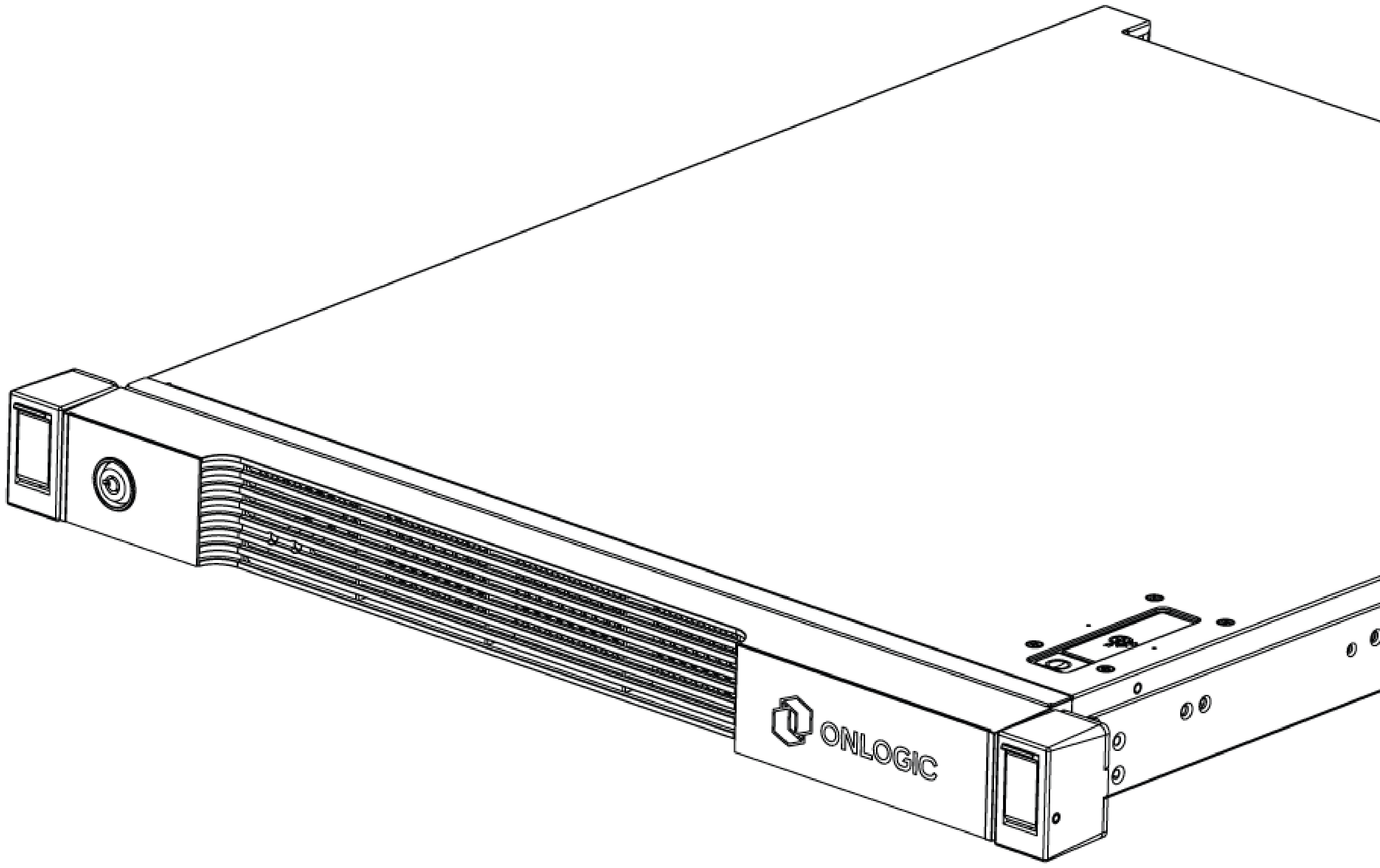
Axial Edge Server

Baseboard Management Controller (BMC) User Guide



Revision History

Date	Revision History
05/03/2023	First release of Axial Baseboard Management Controller (BMC) User Guide

Table of Contents

1.0 - Introduction

Welcome to the Axial Edge Server Baseboard Management Controller (BMC) User Guide.

The BMC is an important component of edge server systems that allows for remote management and monitoring of hardware, even when the system is powered off.

This user's guide provides essential information on how to configure and use the BMC to ensure efficient operation of your system. The intent of this guide is to help you understand the key features and functions of the BMC, including how to access and use the remote management interface capabilities, monitor system health, configure security settings, and more.

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

2.0 - What is a BMC?

A Baseboard Management Controller (BMC) is a dedicated microcontroller or processor that is integrated into a server's motherboard. The BMC provides out-of-band management capabilities for the server system, allowing administrators to monitor, manage, and control the server hardware even when the main operating system is not running or is unresponsive.

The BMC provides several valuable features for server systems, including:

- **Remote management:** The BMC provides remote management capabilities, allowing administrators to access and manage the server hardware remotely, even if the server is powered off or the main operating system is not running.
- **System health monitoring:** The BMC constantly monitors the health of the server system, including component temperatures, fan speeds, and power voltages. It can alert administrators to potential issues before they become critical and cause downtime.
- **Virtual media support:** The BMC supports virtual media, allowing administrators to remotely mount ISO images, disk images, and other media types to the server as if they were physically present.
- **Power management:** The BMC provides power management capabilities, allowing administrators to remotely power on, power off, or reboot the server.
- **Security:** The BMC provides a separate management interface that is isolated from the main operating system, which can enhance server security by limiting access to critical system management functions.

The BMC is an extremely valuable component of a server system, providing essential out-of-band management capabilities that can help administrators maintain the health and availability of their server infrastructure.

3.0 - Methods of Accessing to the BMC

Prior to discussing the specifics for accessing and configuring the BMC, it is important to review the supported methods of access.

Fundamentally, the BMC can be accessed by one of the two following methods:

- **Out-of-band (Network connected)**: This method leverages network connectivity to the BMC either through the Dedicated management port or via a network controller supporting NC-SI (Network Controller Sideband Interface).
- **In-band (From the local OS)**: This method utilizes the KCS (Keyboard Controller Style) interface to communicate with the BMC via IPMI.

Out-of-band management supports a wide variety of protocols and interfaces for communicating with the BMC, such as IPMI, RedFish, a Web Browser (HTTP/HTTPS), or SSH. Additionally, as Out-of-Band management is network connected, it's easy to monitor and configure multiple systems that share a common management network.

In-band management is limited to IPMI access and is subject to OS dependencies, tools, utilities, and/or drivers.

The primary intent of this document is to focus on the Out-of-Band (network connected) management configuration and capabilities that are enabled by OnLogic's Axial Edge Server BMCs.

4.0 - Supported Out-of-band Management Access Protocols

The following access protocols/methods are supported by Axial Edge Server BMCs:

- IPMI 2.0
- RedFish
- Web Browser (HTTP/HTTPS)
- SSH
- SNMP

5.0 - Network Configuration

The contents of this section will outline the ways in which the OnLogic Axial Edge Server BMC's network connectivity may be used and configured.

5.1 - What is a Dedicated Management Ethernet Interface?

The dedicated management Ethernet interface of a BMC is a separate network interface that only communicates and connects with the BMC. This network connection is isolated from the system's operating system and is typically connected to a dedicated management network.

Benefits:

- **Security:** As the dedicated management Ethernet interface of a BMC provides physical isolation from the server's network interfaces and the host OS, the dedicated management Ethernet interface is typically used when network separation and security is critical.
- **Network Congestion and Performance:** Since the dedicated management Ethernet interface does not share traffic with the host OS, there is no network throughput impact to the applications running in the host OS.

Drawbacks:

- **Networking Infrastructure:** A drawback of leveraging the dedicated management Ethernet interface for BMC is the increased need for cabling and network architecture to maintain a dedicated and independent management network.

5.2 - What is a Shared NIC (NC-SI) Management Ethernet Interface?

A Shared NIC (NC-SI) management Ethernet interface of a BMC is a type of network interface that allows the BMC to share one of the system's network interfaces for management traffic. This is accomplished using the NC-SI protocol, which is a low-level interface that allows the BMC to communicate with the system's network controller.

Benefits:

- **Network Infrastructure:** The need for a separate dedicated management network is eliminated, simplifying cabling and equipment requirements.
- **Flexibility:** As Shared NIC may be capable of being used with 1GbE, 10GbE, or other high speed network controllers, there is an inherent flexibility in terms of network connectivity options for accessing the BMC.

Drawbacks:

- **Network Congestion and Performance:** Sharing the server's network interface for management traffic can potentially lead to network congestion, which can affect the performance of both the management traffic and the server's data traffic.
- **Security:** By sharing the server's network interface for management traffic, the management traffic is not isolated from the server's data network, which can potentially increase the risk of security breaches if the appropriate network isolation measures are not considered.

5.3 - BMC Networking Defaults

As previously noted in the previous sections , the BMC can be accessible via a dedicated Ethernet management port, or through a shared network interface (NC-SI) with the host system.

Out of the box (system defaults), an OnLogic Axial Edge Server BMC is configured to operate using DHCP (Dynamic Host Configuration Protocol) in a Bonded mode, meaning that the BMC can lease an IP address and become accessible either via the 1GbE Dedicated management interface OR via a Shared NIC (NC-SI) capable port from the system's 1GbE network controller.

This configuration can be changed by accessing the UEFI System Setup / Server Mgmt configuration page during system boot, or via the web based user interface. Within these configuration pages, it is possible to configure static IP addresses, modify the bonding mode, disable NC-SI capable ports, or utilize different NC-SI capable ports (if available).

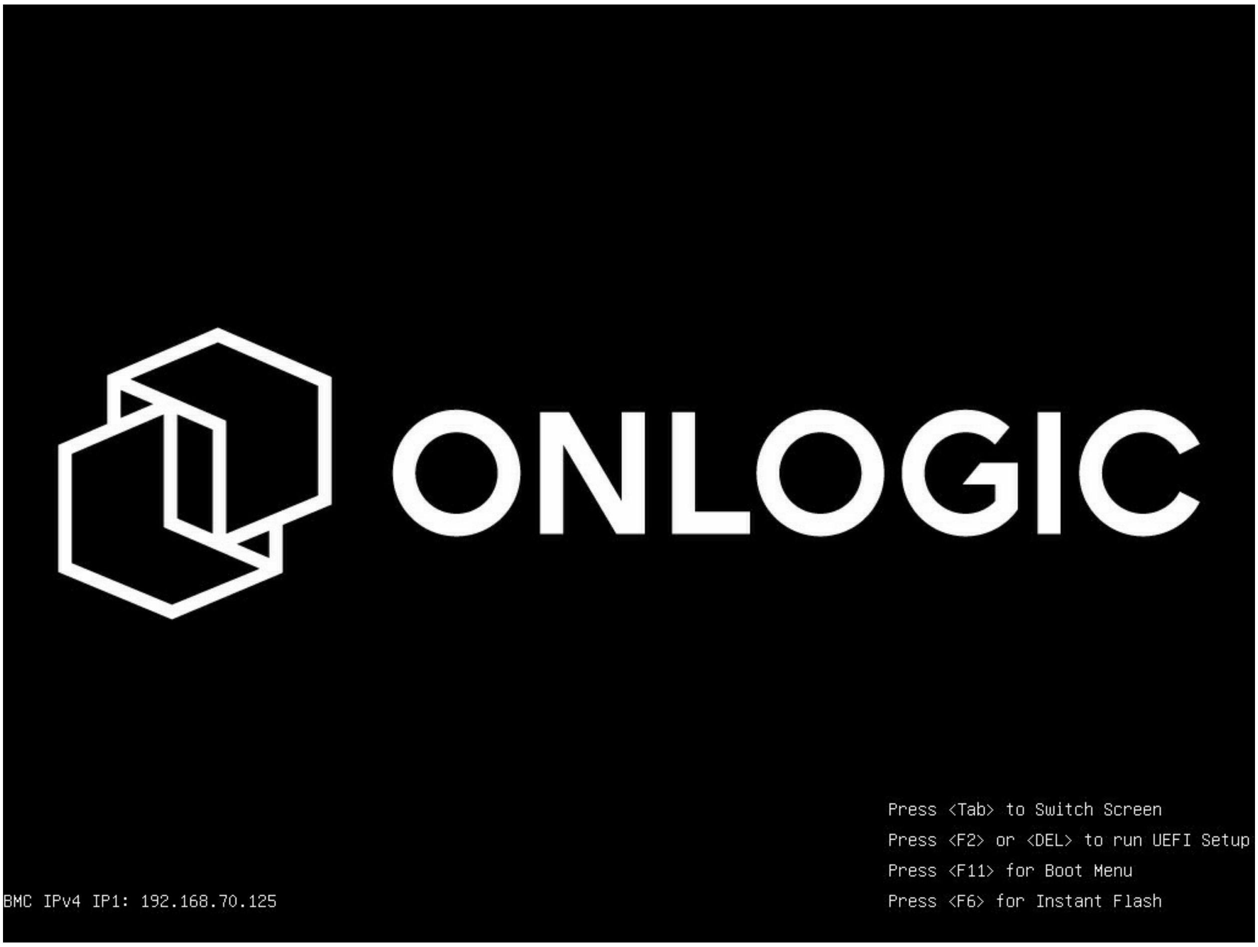
Note: Axial Edge Servers support both IPv4 and IPv6.

5.4 - Determining BMC IP Address with DHCP

When configuring the BMC IP address via DHCP, it is possible to determine the IP from various methods as outlined in this section.

5.4.1 - Boot Splash Screen

If and when it is possible to access the system's video output, the IP address(es) that the BMC has obtained via DHCP will be visually indicated on the boot splash screen in the lower left hand corner:

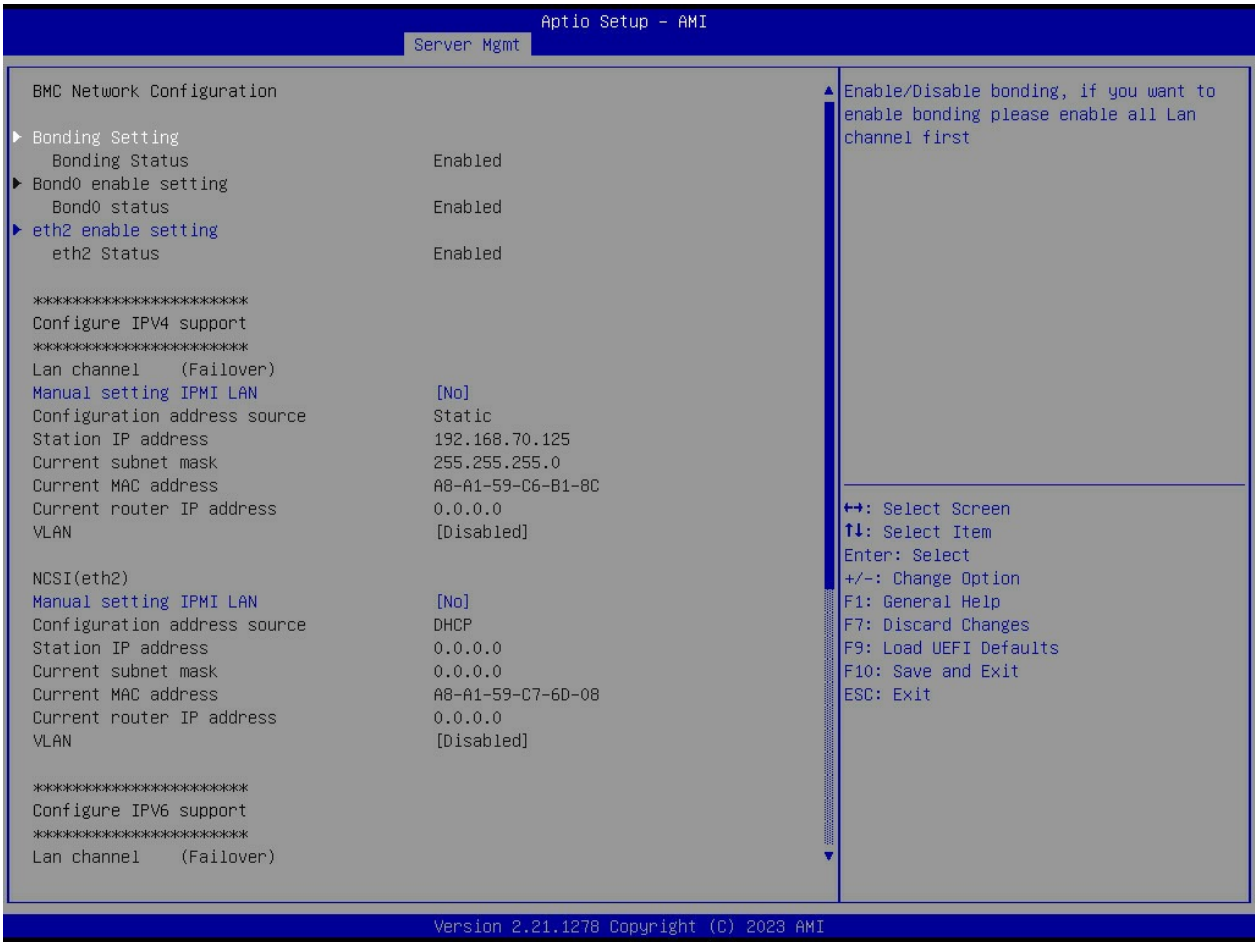


```
                                                 Press <Tab> to Switch Screen
                                                 Press <F2> or <DEL> to run UEFI Setup
                                                 Press <F11> for Boot Menu
BMC IPv4 IP1: 192.168.70.125                     Press <F6> for Instant Flash
```

5.4.2 - UEFI System Setup Menu

From the **UEFI System Setup / Server Mgmt** screen, the IP address(es) and network configuration information of the BMC will be shown.

E.g.



```
                              Aptio Setup - AMI
                       Server Mgmt

 BMC Network Configuration                          Enable/Disable bonding, if you want to
                                                    enable bonding please enable all Lan
▶ Bonding Setting                                   channel first
    Bonding Status                Enabled
▶ Bond0 enable setting
    Bond0 status                  Enabled
▶ eth2 enable setting
    eth2 Status                   Enabled

 **********************
 Configure IPV4 support
 **********************
 Lan channel    (Failover)
 Manual setting IPMI LAN          [No]
 Configuration address source     Static
 Station IP address               192.168.70.125
 Current subnet mask              255.255.255.0
 Current MAC address              A8-A1-59-C6-B1-8C
 Current router IP address        0.0.0.0           ↔: Select Screen
 VLAN                             [Disabled]        ↑↓: Select Item
                                                    Enter: Select
 NCSI(eth2)                                         +/-: Change Option
 Manual setting IPMI LAN          [No]              F1: General Help
 Configuration address source     DHCP              F7: Discard Changes
 Station IP address               0.0.0.0           F9: Load UEFI Defaults
 Current subnet mask              0.0.0.0           F10: Save and Exit
 Current MAC address              A8-A1-59-C7-6D-08 ESC: Exit
 Current router IP address        0.0.0.0
 VLAN                             [Disabled]

 **********************
 Configure IPV6 support
 **********************
 Lan channel    (Failover)

                  Version 2.21.1278 Copyright (C) 2023 AMI
```

5.4.3 - MAC Address via DHCP Server

Upon the IP address lease occurring from a DHCP server, the MAC address is typically logged along with the corresponding IP address, subnet mask, and lease duration.

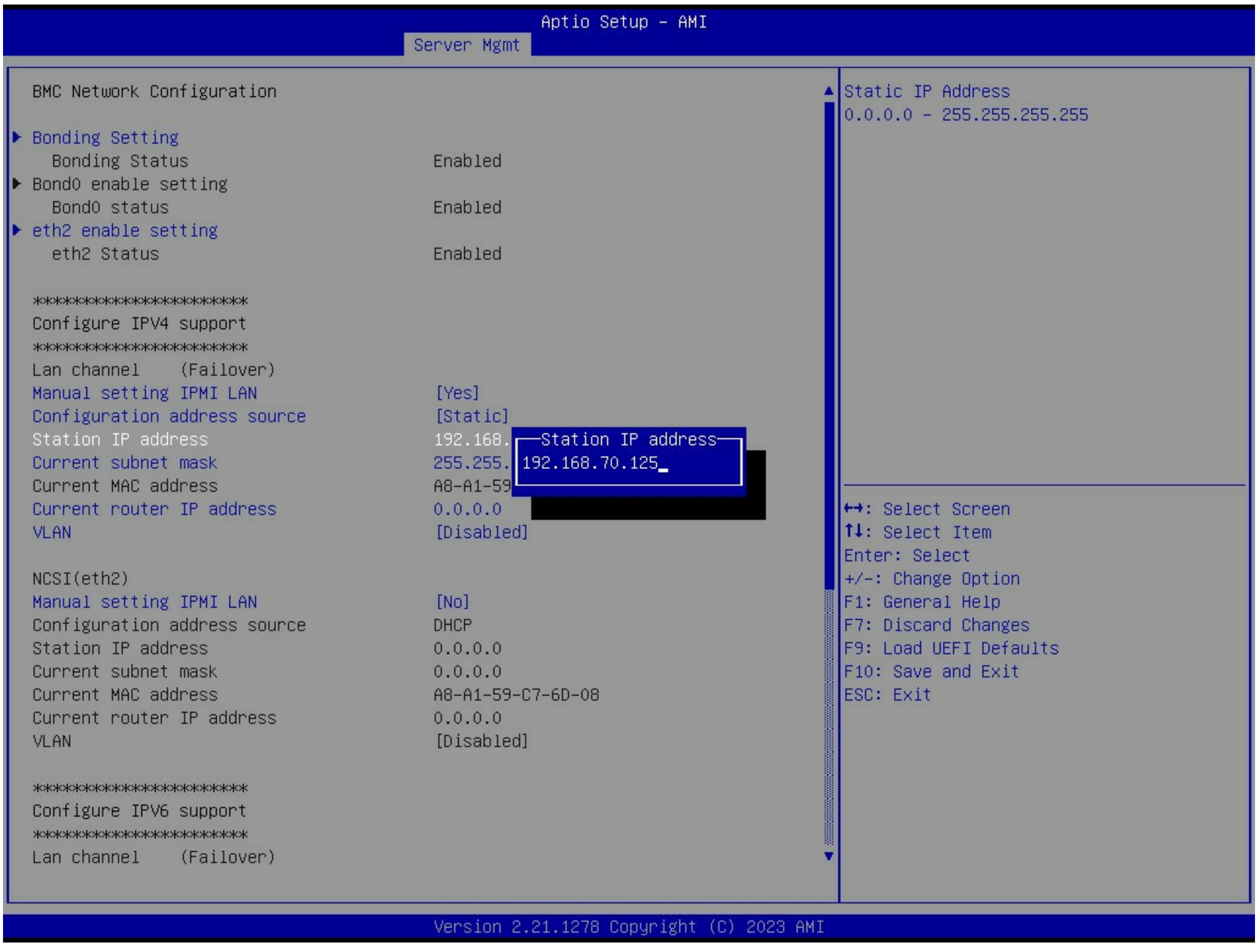
The MAC addresses of Axial Edge Server systems are accessible and barcode readable from the system's Service Label.

Note: Consult the system's product manual for the specific label location and BMC port information.

By correlating the MAC addresses from the Service Label of the Axial Edge server system to the MAC address information from a DHCP server, it is possible to determine the IP address of the Axial Edge Server BMC.

5.4.4 - Static IP Configuration

From the **UEFI System Setup / Server Mgmt** screen, the IP address(es) of the BMC can be manually set to a statically defined IP address. In this scenario, since the IP address is being statically set, it is known.



```
                                   Aptio Setup – AMI
                             Server Mgmt

 BMC Network Configuration                                   Static IP Address
                                                             0.0.0.0 – 255.255.255.255
▶ Bonding Setting
    Bonding Status                       Enabled
▶ Bond0 enable setting
    Bond0 status                         Enabled
▶ eth2 enable setting
    eth2 Status                          Enabled

  ************************
  Configure IPV4 support
  ************************
  Lan channel    (Failover)
  Manual setting IPMI LAN                [Yes]
  Configuration address source           [Static]
  Station IP address                     192.168.┌─Station IP address─┐
  Current subnet mask                    255.255.│192.168.70.125_     │
  Current MAC address                    A8-A1-59└────────────────────┘
  Current router IP address              0.0.0.0                       ↔: Select Screen
  VLAN                                   [Disabled]                    ↑↓: Select Item
                                                                       Enter: Select
  NCSI(eth2)                                                           +/-: Change Option
  Manual setting IPMI LAN                [No]                          F1: General Help
  Configuration address source           DHCP                          F7: Discard Changes
  Station IP address                     0.0.0.0                       F9: Load UEFI Defaults
  Current subnet mask                    0.0.0.0                       F10: Save and Exit
  Current MAC address                    A8-A1-59-C7-6D-08             ESC: Exit
  Current router IP address              0.0.0.0
  VLAN                                   [Disabled]

  ************************
  Configure IPV6 support
  ************************
  Lan channel    (Failover)

                       Version 2.21.1278 Copyright (C) 2023 AMI
```

6.0 - Web Interface

The BMC contains an embedded web server that allows users to configure the Axial Edge Server's BMC through a rich web browser based user interface (WebUI).

This interface provides a dashboard to display alerts or warnings for any issues that require attention.

Additionally, the interface provides access to an additional wide range of features and functions such as power management, system monitoring, firmware updates, system settings, and remote console access.

The remote console access feature allows users to connect to the system's console remotely, even if the operating system is not responding. This feature is particularly useful for troubleshooting and diagnosing system problems. Users can view the system's console output, enter commands, and interact with the system just as if they were physically present at the console.

6.1 - Supported Web Browsers

To access the WebUI, an HTML5 Browser is required. The table below outlines the minimum browser versions that are recommended for using the BMC WebUI.

Browser	Operating System	Minimum Recommended Version
Microsoft Edge (Chromium)	Windows	v109.0.1518.61
Google Chrome	Windows	v109.0.1518.61
	Linux	v107.0.5304.121
Mozilla Firefox	Windows	v107.0.1
	Linux	v107.0.1
Safari	MacOS	v16.0

Note: Microsoft Edge (Legacy) and Internet Explorer (all versions) are not supported, nor recommended.

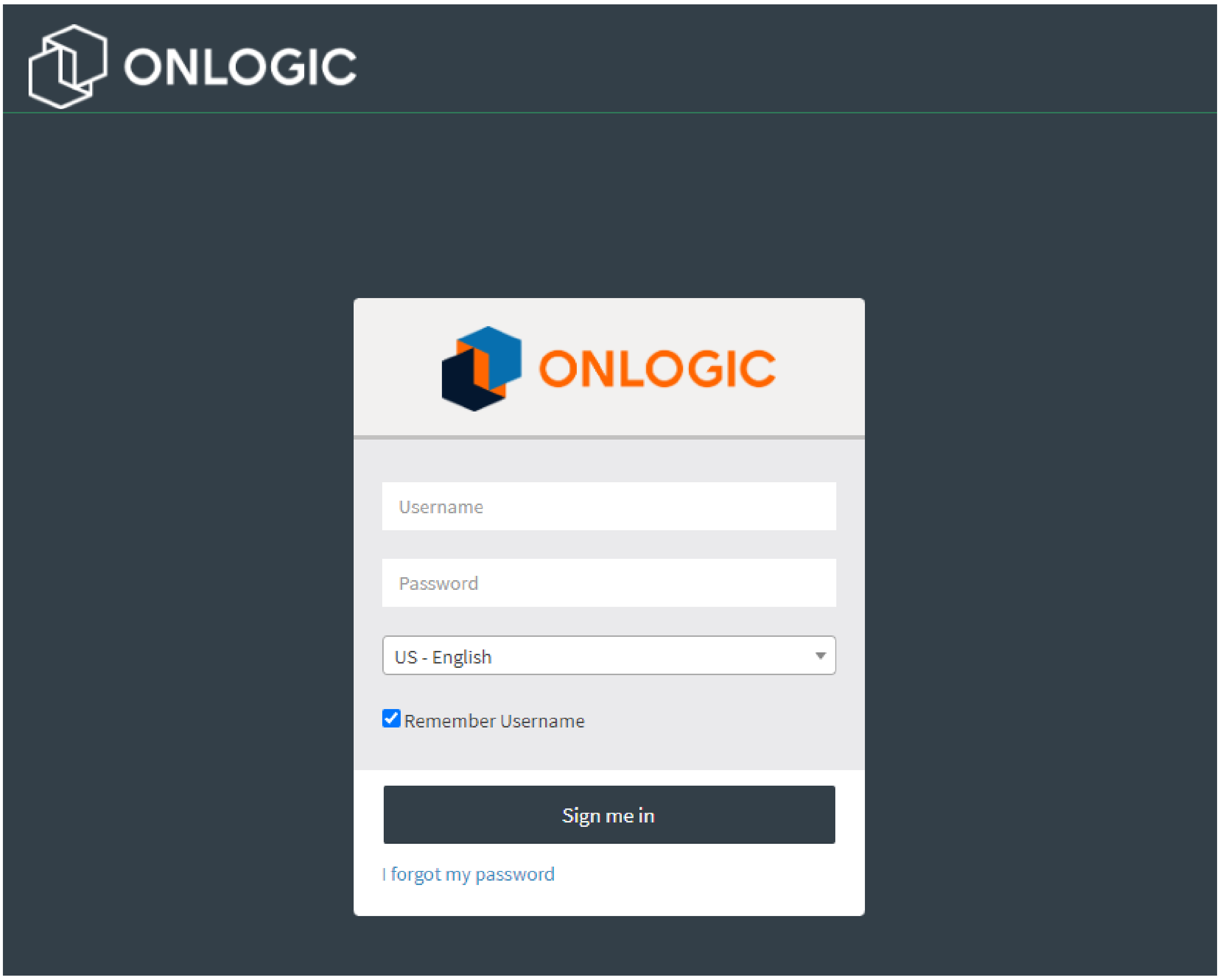
6.2 - First Login & Password Change

Upon first accessing the BMC WebUI service through a web browser, a login prompt requesting a username and a password will be presented.

Out of the box, all Axial Edge server systems will have a default Username and Password set as the following:

- **Username:** admin
- **Password:** admin

However, after the first initial login, user's will be immediately prompted to change the default password.



The login field descriptions are as follows:

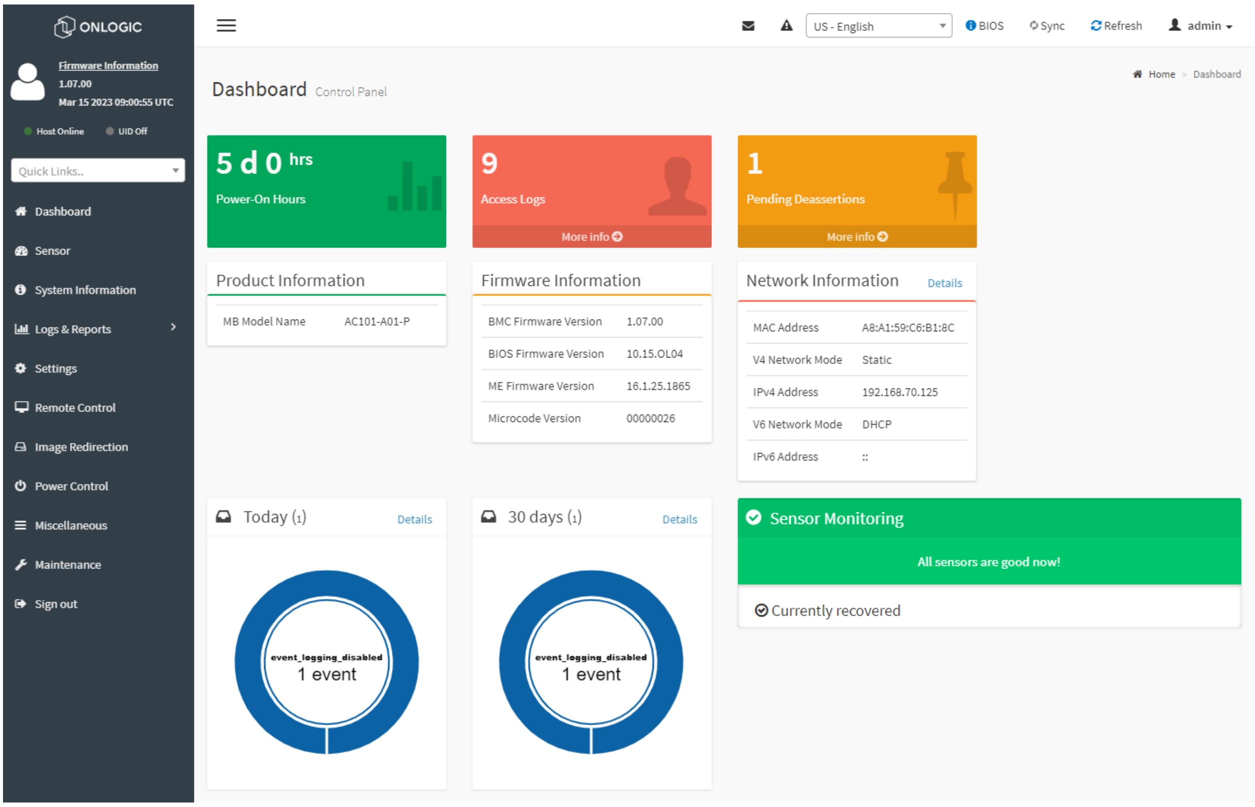
- **Username:** Enter the username of the desired login account
- **Password:** Enter the password of the desired login account
- **Language Menu:** Changes BMC WebUI supported language.
- **Remember Username:** Check this box to keep the username remembered in the browser settings.

- **Sign me in:** After entering the required credentials, click the **Sign me in** button to log in to the BMC WebUI.
- **I forgot my password:** The user can generate a new password using this link if the user forgot the password.

6.3 - Accessing BMC WebUI Service

After completing a successful login, the BMC WebUI will be displayed. The BMC WebUI has a navigation menu on the left hand side, quick links and user information along the top upper right hand corner, and the main page for viewing and displaying information relative to the selected links from the navigation menu.

Example:



Product Information

MB Model Name	AC101-A01-P

Firmware Information

BMC Firmware Version	1.07.00
BIOS Firmware Version	10.15.OL04
ME Firmware Version	16.1.25.1865
Microcode Version	00000026

Network Information Details

MAC Address	A8:A1:59:C6:B1:8C
V4 Network Mode	Static
IPv4 Address	192.168.70.125
V6 Network Mode	DHCP
IPv6 Address	::

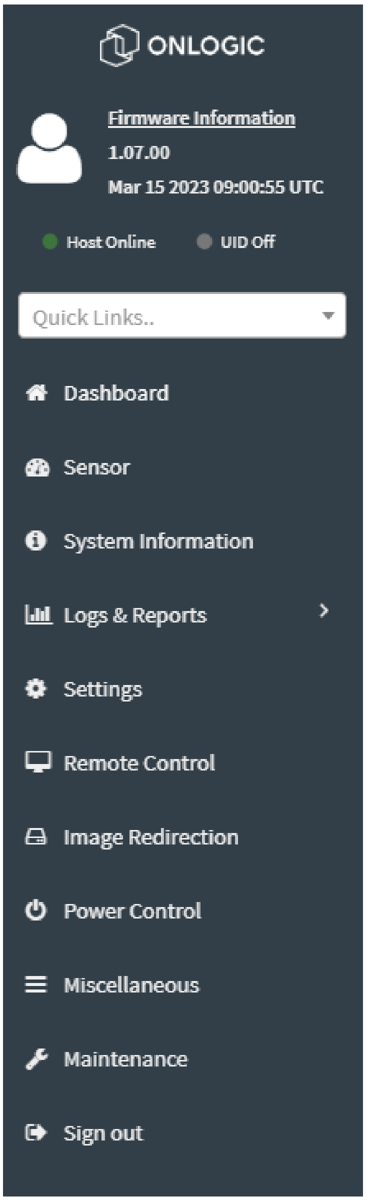
Sensor Monitoring

All sensors are good now!

Currently recovered

6.4 - Navigation Menu

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

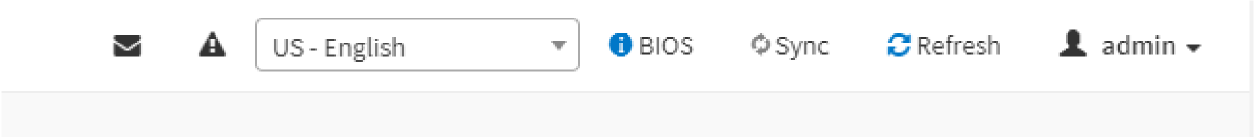


The Navigation Menu Displays and links to the following:

- BMC Firmware Information
- Date & Time
- Host Online Status (system power state)
- UID Status (system ID LED)
- Quick Links Search Bar
- Dashboard
- Sensor
- System Information
- Logs and Reports
  - IPMI Event Log
  - Audit Log
  - Post Code log
  - Debug Log
- Settings
- Remote Control
- Image Redirection
- Power Control
- Miscellaneous
- Maintenance
- Sign Out

6.5 - Quick Link and User Information

The Quick Link and User Information section is located in the upper right corner of BMC WebUI. It provides various links for users to view the information or modify the configuration.



6.5.1 - Quick Links

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

Icon	Quick Link Description
✉	**Message:** View the received event logs or alert messages in the popup window.
⚠	**Notification:** View the received notification in the popup window.
US - English ▾	**Language Menu:** Change the supported BMC WebUI language.
ℹ BIOS	**BIOS:** View / Change BIOS settings from the BMC UI.
●	**Switch:** Show or hide Dashboard Widgets.
⟳ Sync	**Sync:** Turn on/off the sync feature. Note: Enabling this feature will ensure that the latest Sensor and Events are updated dynamically when on these pages.
⟳ Refresh	**Refresh:** Reloads the current page.

6.5.2 - User Information

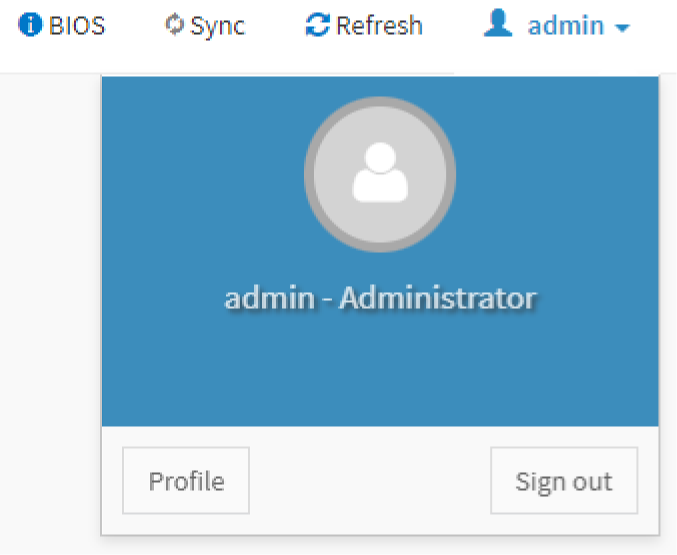
The User Information shows the logged-in user information.

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 to sign out of the current session.



6.5.3 - User Privilege

The BMC WebUI service provides five user privilege levels for the administrator to manage user account privileges. These privilege levels are as follows:

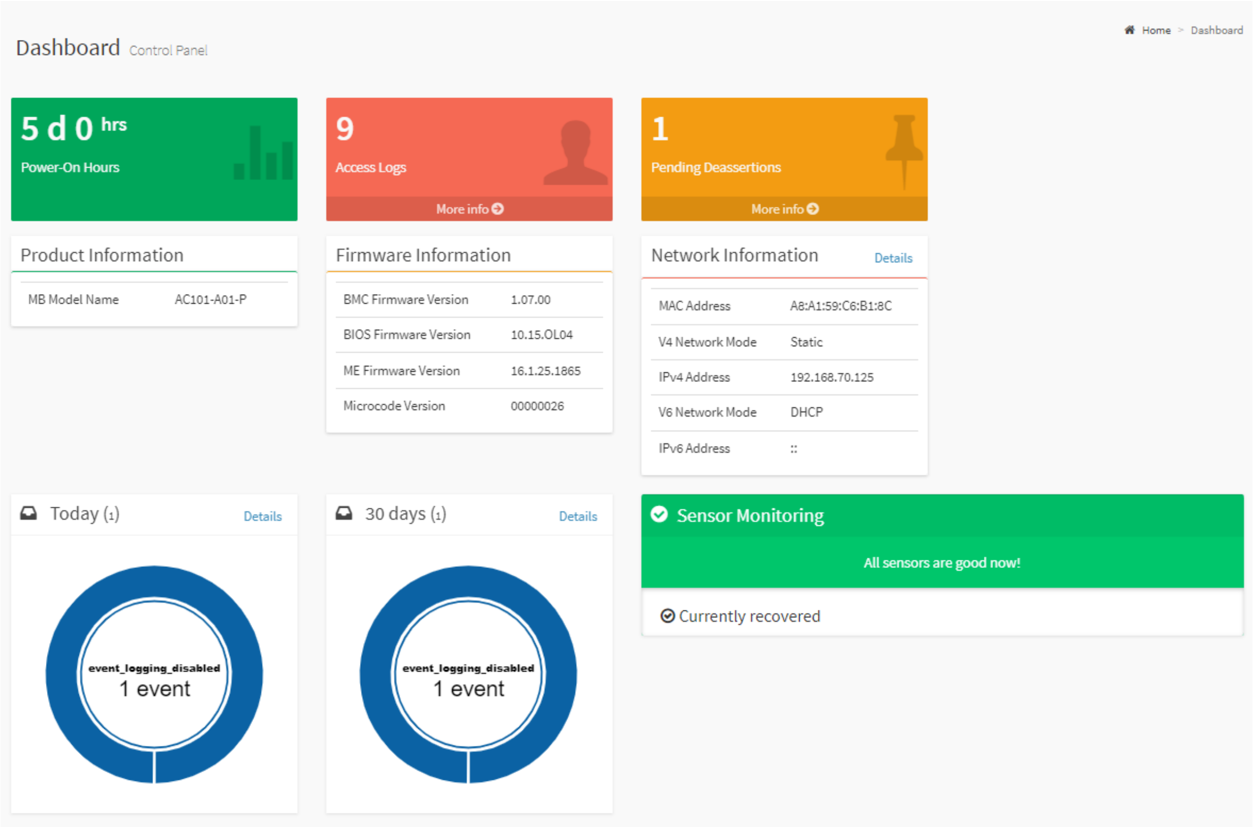
- **None:** Not allow login and access BMC WebUI Service.
- **User:** Only perform the allowed commands.
- **Operator:** All commands are allowed except configuration commands that can change the behavior of the out-of-band interfaces.
- **OEM:** All OEM commands are allowed.
- **Administrator:** All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

6.6 - Dashboard

The Dashboard provides the primary system information and a summary of the overall status. It is also the main status screen that is visible after logging into the BMC Web UI.

To navigate to the Dashboard page from any other page, click the Dashboard tab from the left Navigation Menu.

Below is an example image of the content displayed from the BMC WebUI's Dashboard:



Dashboard Control Panel

Home > Dashboard

5 d 0 hrs
Power-On Hours

9
Access Logs
More info

1
Pending Deassertions
More info

Product Information

MB Model Name	AC101-A01-P

Firmware Information

BMC Firmware Version	1.07.00
BIOS Firmware Version	10.15.OL04
ME Firmware Version	16.1.25.1865
Microcode Version	00000026

Network Information Details

MAC Address	A8:A1:59:C6:B1:8C
V4 Network Mode	Static
IPv4 Address	192.168.70.125
V6 Network Mode	DHCP
IPv6 Address	::

Today (1) Details

event_logging_disabled
1 event

30 days (1) Details

event_logging_disabled
1 event

Sensor Monitoring

All sensors are good now!

Currently recovered

The table below describes and outlines the various widgets that are displayed on the Axial Edge Server BMC:

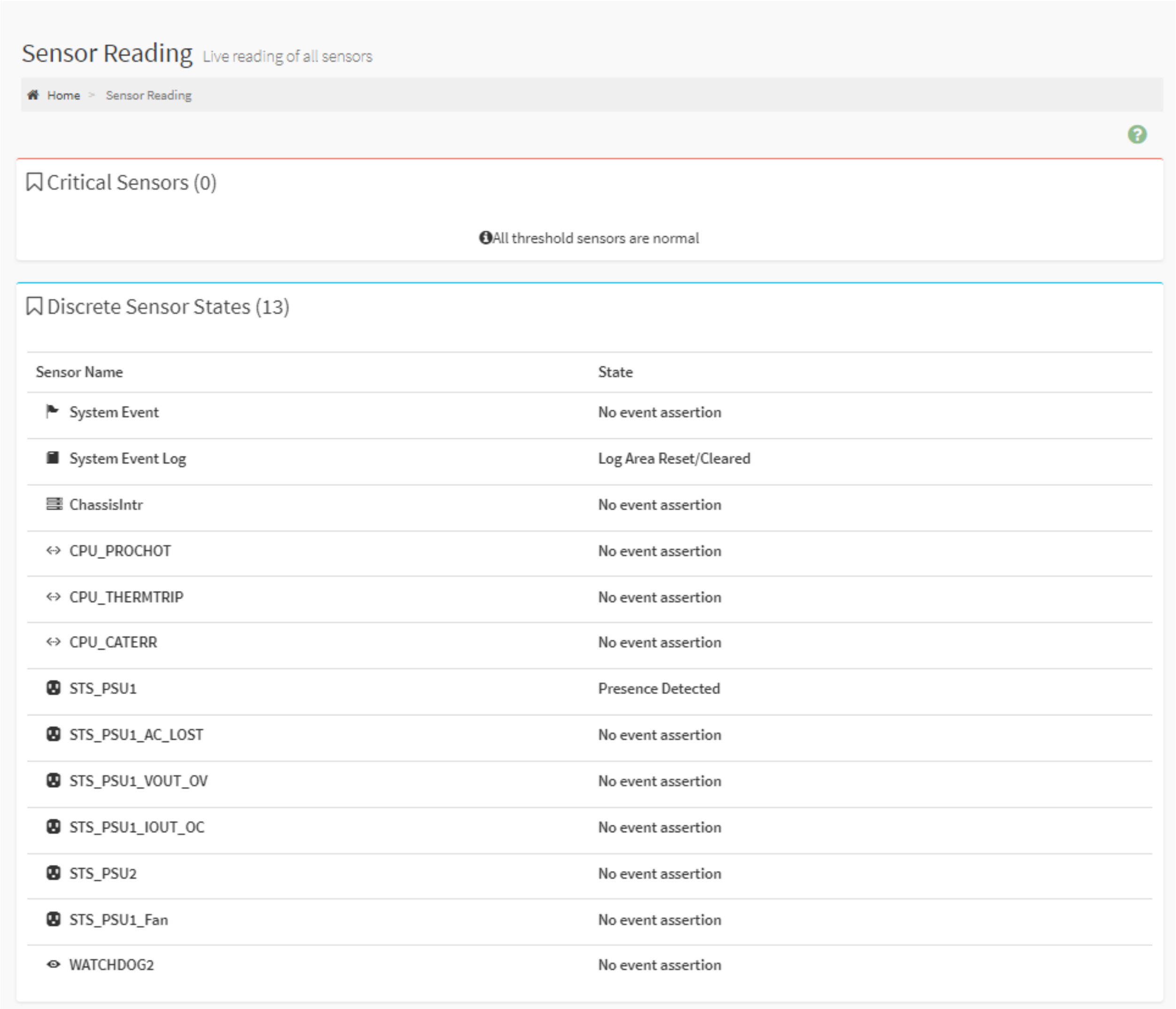
Dashboard Widget	Dashboard Widget Description
Power-On Duration	System power-on time. This duration will accumulate as long as the system is powered on. Note: Power-on time will be reset to zero if BMC firmware is flashed.
Pending Deassertions Summary	The number of all pending sensor events waiting for deassertion. Clicking **More Info** will go to the Event Log page.
Access Log Summary	The number of Access Logs which are generated via accessing the BMC WebUI. Clicking **More Info** will go to the Audit Log page.
Product Information	Lists related product information related fields such as motherboard name, system name, etc.
FIrmware Information	Lists BMC, UEFI (BIOS), ME (Management Engine), and Microcode firmware versions.
Network Information	It lists related network configuration information such as BMC 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.
Sensor Assertions	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.
Recent events	This item lists all the event logs which are generated by various sensors. Click the Details link on today and 30 days item then navigate to the Event Log page to view all event logs, which are filtered by today and 30 days respectively.

6.7 - Sensor Reading

The Sensor page provides all of the sensor related information for the system.

To view the Sensor Reading page, click the Sensor tab from the Navigation Menu.

Note: Turning on the Sync feature in the upper right hand corner of the WebUI will ensure that the latest Sensor information is updated dynamically while viewing the page. Additionally, sensor data will be graphed for the duration the page is being viewed.



Critical Sensors (0)

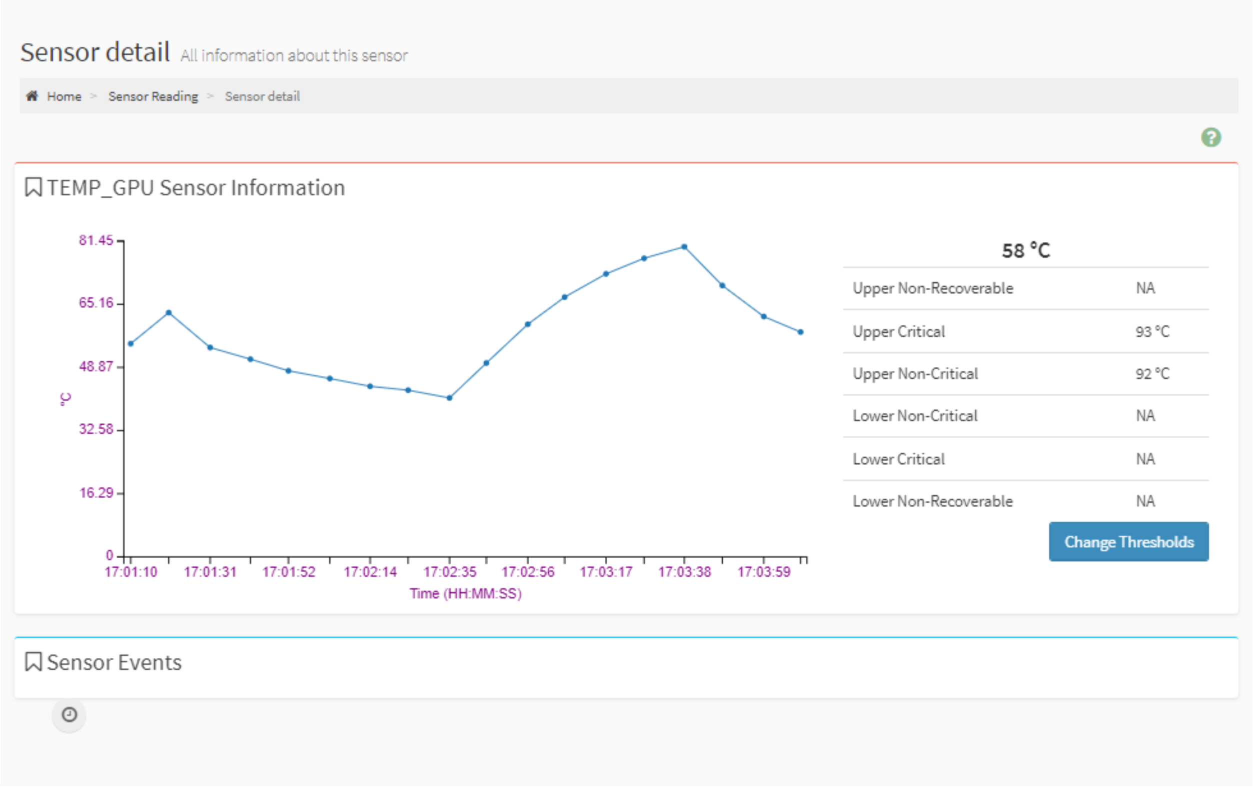
All threshold sensors are normal

Discrete Sensor States (13)

Sensor Name	State
System Event	No event assertion
System Event Log	Log Area Reset/Cleared
ChassisIntr	No event assertion
CPU_PROCHOT	No event assertion
CPU_THERMTRIP	No event assertion
CPU_CATERR	No event assertion
STS_PSU1	Presence Detected
STS_PSU1_AC_LOST	No event assertion
STS_PSU1_VOUT_OV	No event assertion
STS_PSU1_IOUT_OC	No event assertion
STS_PSU2	No event assertion
STS_PSU1_Fan	No event assertion
WATCHDOG2	No event assertion

6.7.1 - Sensor Detail

Clicking on a specific sensor from the Sensor Reading page will navigate to the Sensor detail for that selected sensor. The sensor Detail page will include information pertaining to the sensor threshold values, events, a graphical representation, and the ability to change the thresholds from the default values.



Sensor detail All information about this sensor

TEMP_GPU Sensor Information

58 °C	
Upper Non-Recoverable	NA
Upper Critical	93 °C
Upper Non-Critical	92 °C
Lower Non-Critical	NA
Lower Critical	NA
Lower Non-Recoverable	NA

Sensor Events

There are six types of sensor threshold values listed:

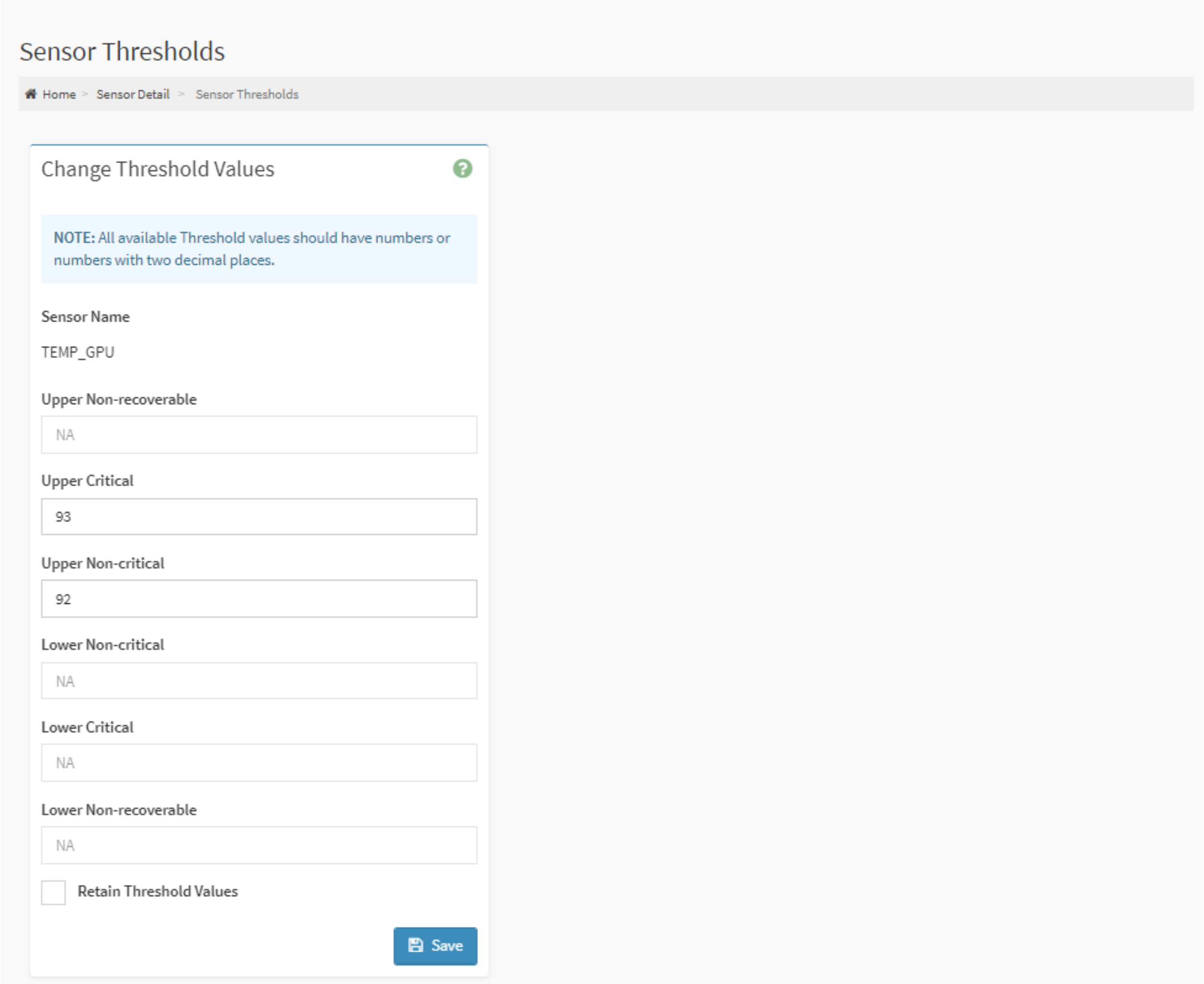
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)
- Lower Non-Critical (LNC)
- Lower Critical (LC)
- Lower Non-Recoverable (LNR)

When an event is triggered by the sensor, it will be listed in the Sensor Events group and noted in the IPMI Event log.

To a sensor’s threshold values, click the **Change Thresholds** button, which will navigate to the Sensor Thresholds page to modify the specific threshold values of the sensor.

6.7.1.1 - Change Thresholds

The Change Thresholds page allows users to modify the threshold values of selected sensor.



Sensor Thresholds

Change Threshold Values

NOTE: All available Threshold values should have numbers or numbers with two decimal places.

Sensor Name
TEMP_GPU

Upper Non-recoverable
NA

Upper Critical
93

Upper Non-critical
92

Lower Non-critical
NA

Lower Critical
NA

Lower Non-recoverable
NA

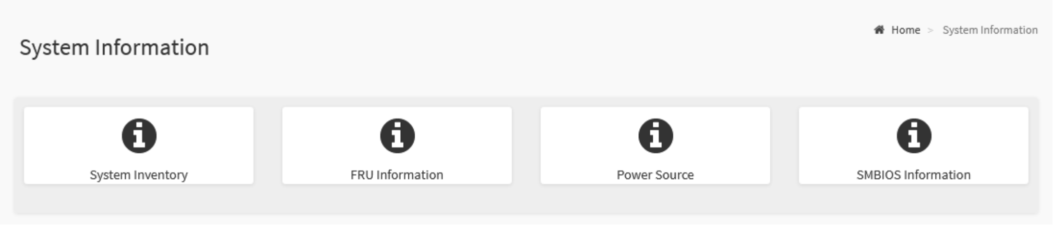
□ Retain Threshold Values

The adjustable fields on the Sensor Thresholds page include:

- **Sensor Name**: Indicates the device name of selected sensor.
- **Upper Non-Recoverable**: Specify the Upper Non-Recoverable (UNR) value for this sensor.
- **Upper Critical:** Specify the Upper Critical (UC) value for this sensor.
- **Upper Non-Critical**: Specify the Upper Non-Critical (UNC) value for this sensor.
- **Lower Non-Critical**: Specify the Lower Non-Critical (LNC) value for this sensor.
- **Lower Critical:** Specify the Lower Critical (LC) value for this sensor.
- **Lower Non-Recoverable:** Specify the Lower Non-Recoverable (LNC) value for this sensor.
- **Retain Threshold Values:** Set Retain Threshold Values.
- **Save:** Save the configured settings.

6.8 - System Information

The System Information page provides links to detailed information of the system, including System Inventory, FRU Information, Power, and SMBIOS information.



Each tab from the System Information page links to a specific page further outlining the detailed system information. These pages are discussed in the following sections.

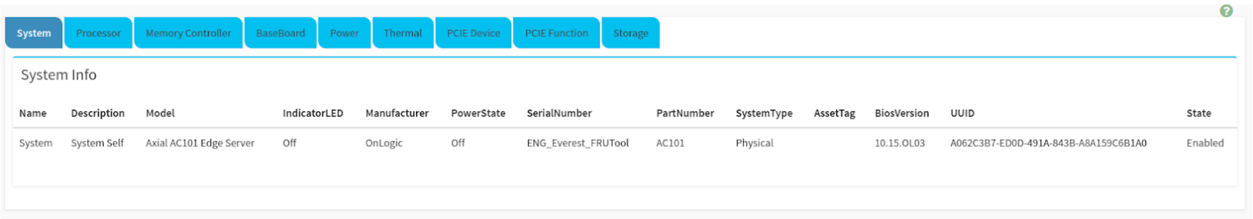
6.8.1 - System Inventory

The System Inventory page provides information on devices that are installed in the Axial Edge Server, including:

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

The details about each System Inventory tab are noted in the following sections.

6.8.1.1 - System



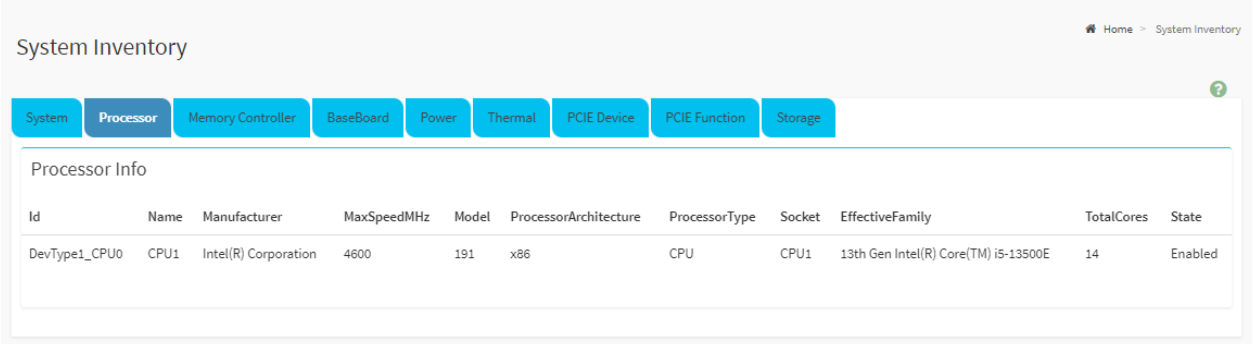
System Info

Name	Description	Model	IndicatorLED	Manufacturer	PowerState	SerialNumber	PartNumber	SystemType	AssetTag	BiosVersion	UUID	State
System	System Self	Axial AC101 Edge Server	Off	OnLogic	Off	ENG_Everest_FRUTool	AC101	Physical		10.15.OL03	A062C3B7-ED0D-491A-843B-A8A159C6B1A0	Enabled

Information Fields:

- Name
- Description
- Model
- Indicator LED
- Manufacturer
- Power State
- Serial Number
- Part Number
- System Type
- Asset Tag
- BIOS Version
- UUID
- State

6.8.1.2 - Processor



System Inventory

Processor Info

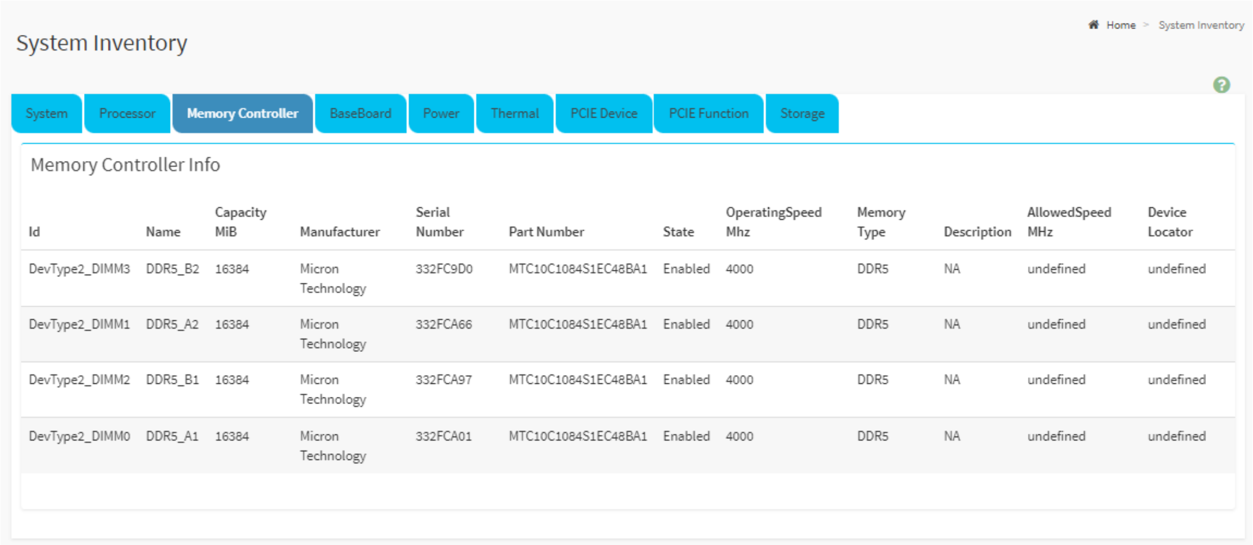
Id	Name	Manufacturer	MaxSpeedMHz	Model	ProcessorArchitecture	ProcessorType	Socket	EffectiveFamily	TotalCores	State
DevType1_CPU0	CPU1	Intel(R) Corporation	4600	191	x86	CPU	CPU1	13th Gen Intel(R) Core(TM) i5-13500E	14	Enabled

Information Fields:

- Id
- Name
- Manufacturer
- MaxSpeedMHz
- Model
- ProcessorArchitecture
- ProcessorType
- Socket

- EffectiveFamily
- TotalCores
- State

6.8.1.3 - Memory Controller



System Inventory

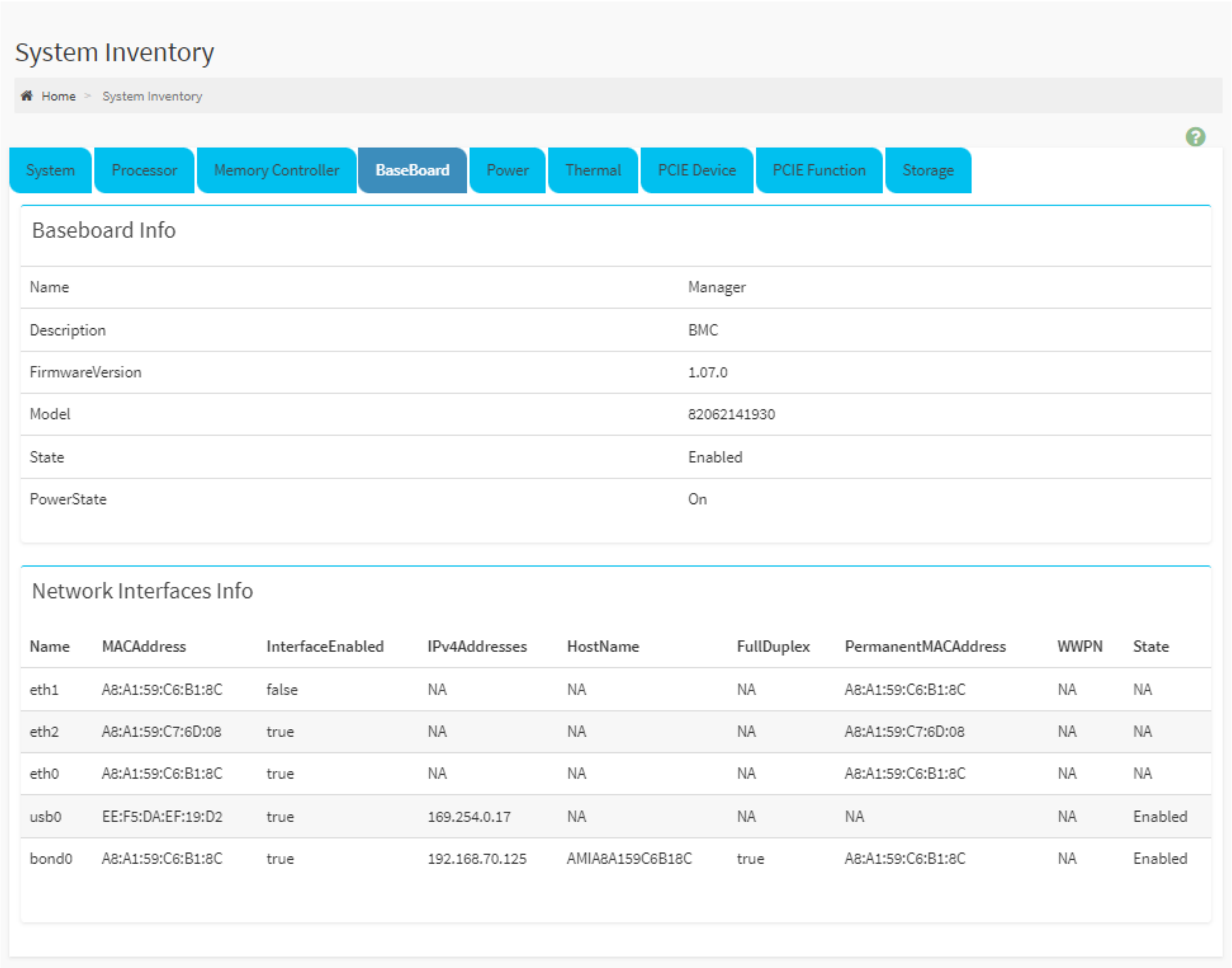
Memory Controller Info

Id	Name	Capacity MiB	Manufacturer	Serial Number	Part Number	State	OperatingSpeed Mhz	Memory Type	Description	AllowedSpeed MHz	Device Locator
DevType2_DIMM3	DDR5_B2	16384	Micron Technology	332FC9D0	MTC10C1084S1EC48BA1	Enabled	4000	DDR5	NA	undefined	undefined
DevType2_DIMM1	DDR5_A2	16384	Micron Technology	332FCA66	MTC10C1084S1EC48BA1	Enabled	4000	DDR5	NA	undefined	undefined
DevType2_DIMM2	DDR5_B1	16384	Micron Technology	332FCA97	MTC10C1084S1EC48BA1	Enabled	4000	DDR5	NA	undefined	undefined
DevType2_DIMM0	DDR5_A1	16384	Micron Technology	332FCA01	MTC10C1084S1EC48BA1	Enabled	4000	DDR5	NA	undefined	undefined

Information Fields:

- Ids
- Name
- Capacity Mib
- Manufacturer
- Serial Number
- Part Number
- State
- OperatingSpeed Mhz
- Memory Type
- Description
- AllowedSpeed Mhz
- Device Locator

6.8.1.4 - BaseBoard



System Inventory

Baseboard Info

Name	Manager
Description	BMC
FirmwareVersion	1.07.0
Model	82062141930
State	Enabled
PowerState	On

Network Interfaces Info

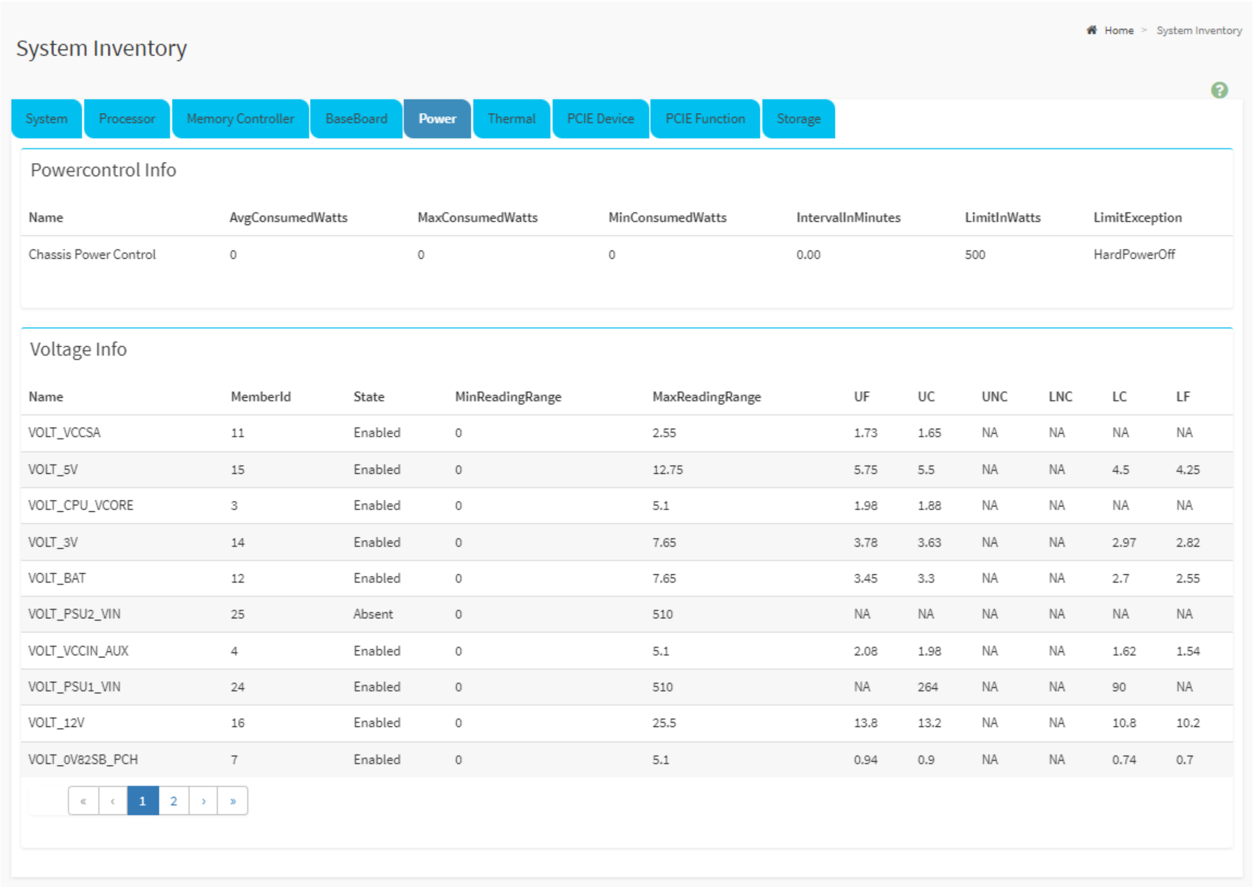
Name	MACAddress	InterfaceEnabled	IPv4Addresses	HostName	FullDuplex	PermanentMACAddress	WWPN	State
eth1	A8:A1:59:C6:B1:8C	false	NA	NA	NA	A8:A1:59:C6:B1:8C	NA	NA
eth2	A8:A1:59:C7:6D:08	true	NA	NA	NA	A8:A1:59:C7:6D:08	NA	NA
eth0	A8:A1:59:C6:B1:8C	true	NA	NA	NA	A8:A1:59:C6:B1:8C	NA	NA
usb0	EE:F5:DA:EF:19:D2	true	169.254.0.17	NA	NA	NA	NA	Enabled
bond0	A8:A1:59:C6:B1:8C	true	192.168.70.125	AMIA8A159C6B18C	true	A8:A1:59:C6:B1:8C	NA	Enabled

Information Fields:

- Baseboard Info
  - Name
  - Description
  - Firmware Version
  - Model
  - State
  - Power State

- Network Interfaces Info
  - Name
  - MAC Address
  - Interface Enabled
  - IPv4 Address
  - Host Name
  - Full Duplex
  - Permanent MAC Address
  - WWPN
  - State

6.8.1.5 - Power



Powercontrol Info

Name	AvgConsumedWatts	MaxConsumedWatts	MinConsumedWatts	IntervalInMinutes	LimitInWatts	LimitException
Chassis Power Control	0	0	0	0.00	500	HardPowerOff

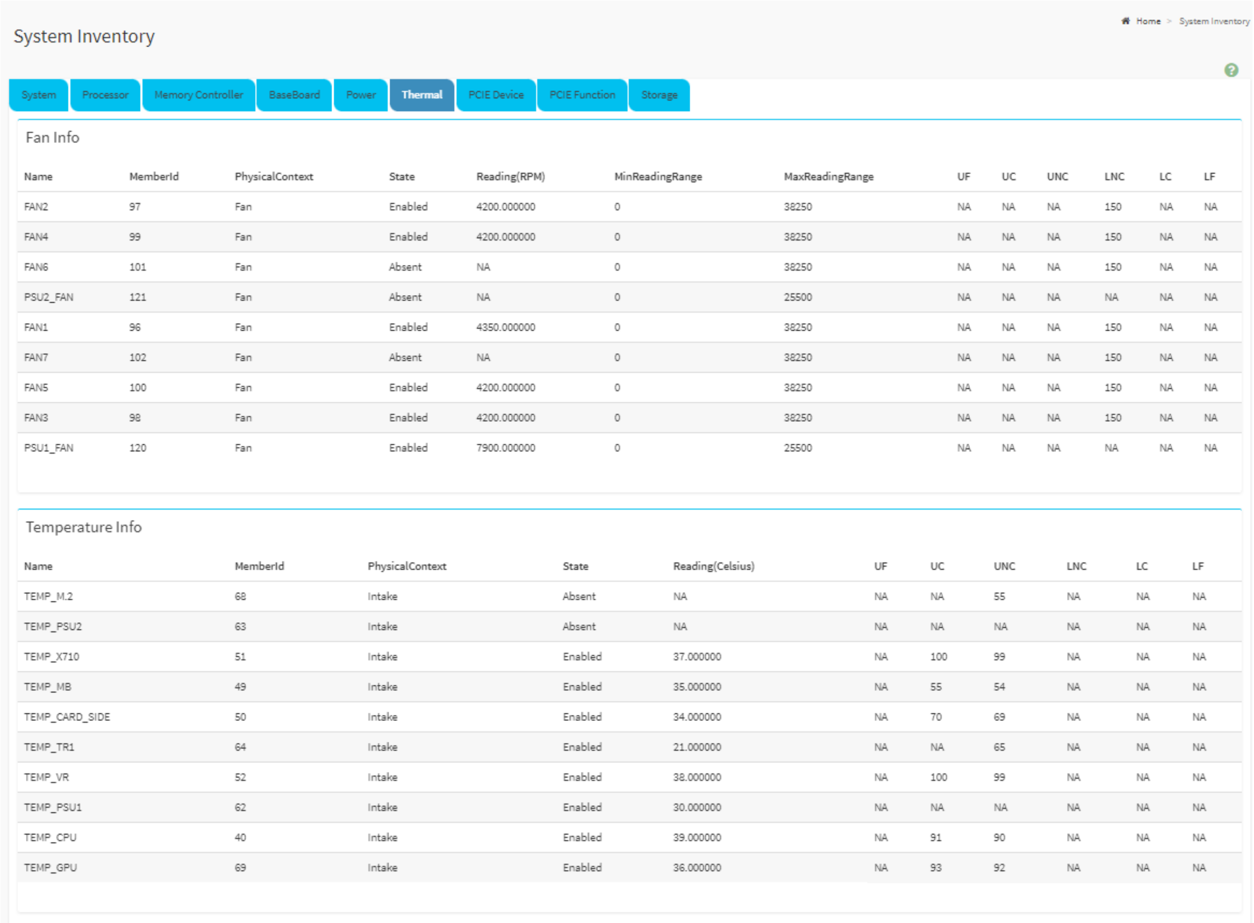
Voltage Info

Name	MemberId	State	MinReadingRange	MaxReadingRange	UF	UC	UNC	LNC	LC	LF
VOLT_VCCSA	11	Enabled	0	2.55	1.73	1.65	NA	NA	NA	NA
VOLT_5V	15	Enabled	0	12.75	5.75	5.5	NA	NA	4.5	4.25
VOLT_CPU_VCORE	3	Enabled	0	5.1	1.98	1.88	NA	NA	NA	NA
VOLT_3V	14	Enabled	0	7.65	3.78	3.63	NA	NA	2.97	2.82
VOLT_BAT	12	Enabled	0	7.65	3.45	3.3	NA	NA	2.7	2.55
VOLT_PSU2_VIN	25	Absent	0	510	NA	NA	NA	NA	NA	NA
VOLT_VCCIN_AUX	4	Enabled	0	5.1	2.08	1.98	NA	NA	1.62	1.54
VOLT_PSU1_VIN	24	Enabled	0	510	NA	264	NA	NA	90	NA
VOLT_12V	16	Enabled	0	25.5	13.8	13.2	NA	NA	10.8	10.2
VOLT_0V82SB_PCH	7	Enabled	0	5.1	0.94	0.9	NA	NA	0.74	0.7

Information Fields:

- Power Control Info
  - Name
  - Avg Consume Watts
  - Max Consume Watts
  - Min Consume Watts
  - Interval Minutes
  - Limit In Watts
  - Limit Exception
- Voltage Info
  - Name
  - Member Id
  - State
  - Min Reading Range
  - Max Reading Range
  - UF (Upper Failure)
  - UC (Upper Critical)
  - UNC (Upper Non-Critical)
  - LNC (Lower Non-Critical)
  - LC (Lower Critical)
  - LF (Lower Failure)

6.8.1.6 - Thermal



System Inventory

Fan Info

Name	MemberId	PhysicalContext	State	Reading(RPM)	MinReadingRange	MaxReadingRange	UF	UC	UNC	LNC	LC	LF
FAN2	97	Fan	Enabled	4200.000000	0	38250	NA	NA	NA	150	NA	NA
FAN4	99	Fan	Enabled	4200.000000	0	38250	NA	NA	NA	150	NA	NA
FAN6	101	Fan	Absent	NA	0	38250	NA	NA	NA	150	NA	NA
PSU2_FAN	121	Fan	Absent	NA	0	25500	NA	NA	NA	NA	NA	NA
FAN1	96	Fan	Enabled	4350.000000	0	38250	NA	NA	NA	150	NA	NA
FAN7	102	Fan	Absent	NA	0	38250	NA	NA	NA	150	NA	NA
FAN5	100	Fan	Enabled	4200.000000	0	38250	NA	NA	NA	150	NA	NA
FAN3	98	Fan	Enabled	4200.000000	0	38250	NA	NA	NA	150	NA	NA
PSU1_FAN	120	Fan	Enabled	7900.000000	0	25500	NA	NA	NA	NA	NA	NA

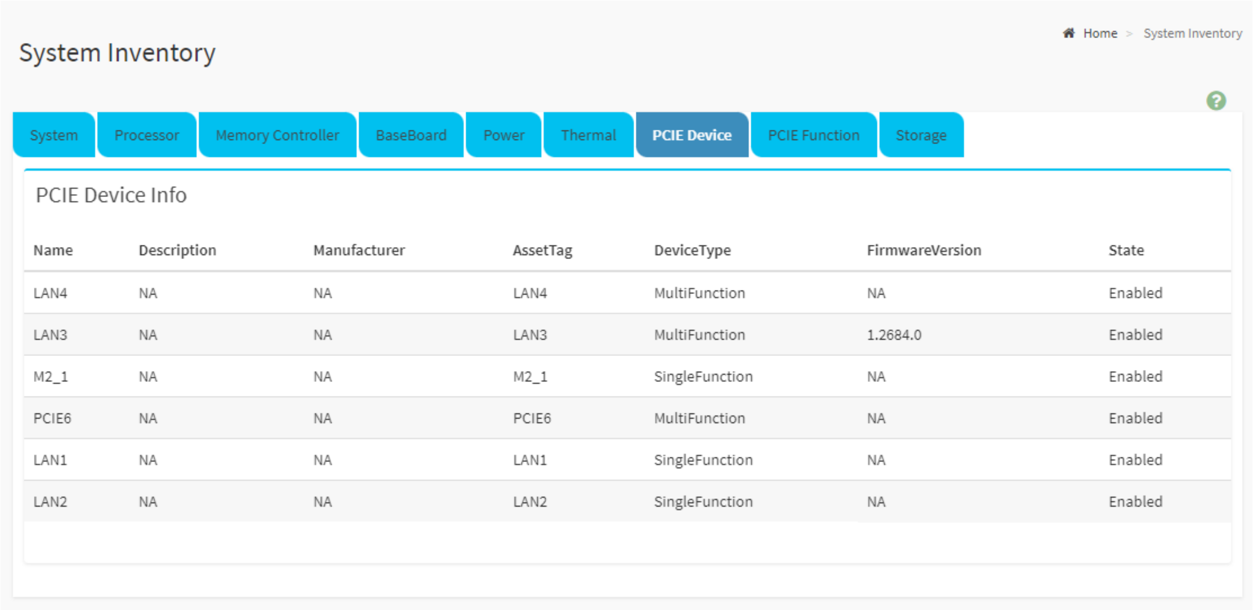
Temperature Info

Name	MemberId	PhysicalContext	State	Reading(Celsius)	UF	UC	UNC	LNC	LC	LF
TEMP_M.2	68	Intake	Absent	NA	NA	NA	55	NA	NA	NA
TEMP_PSU2	63	Intake	Absent	NA	NA	NA	NA	NA	NA	NA
TEMP_X710	51	Intake	Enabled	37.000000	NA	100	99	NA	NA	NA
TEMP_MB	49	Intake	Enabled	35.000000	NA	55	54	NA	NA	NA
TEMP_CARD_SIDE	50	Intake	Enabled	34.000000	NA	70	69	NA	NA	NA
TEMP_TR1	64	Intake	Enabled	21.000000	NA	NA	65	NA	NA	NA
TEMP_VR	52	Intake	Enabled	38.000000	NA	100	99	NA	NA	NA
TEMP_PSU1	62	Intake	Enabled	30.000000	NA	NA	NA	NA	NA	NA
TEMP_CPU	40	Intake	Enabled	39.000000	NA	91	90	NA	NA	NA
TEMP_GPU	69	Intake	Enabled	36.000000	NA	93	92	NA	NA	NA

Information Fields:

- Fan Info
  - Name
  - Member Id
  - Physical Context
  - State
  - Reading (PRM)
  - Min Reading Range
  - Max Reading Range
  - UF (Upper Failure)
  - UC (Upper Critical)
  - UNC (Upper Non-Critical)
  - LNC (Lower Non-Critical)
  - LC (Lower Critical)
  - LF (Lower Failure)
- Temperature Info
  - Name
  - Member Id
  - Physical Context
  - State
  - Reading (Celsius)
  - UF (Upper Failure)
  - UC (Upper Critical)
  - UNC (Upper Non-Critical)
  - LNC (Lower Non-Critical)
  - LC (Lower Critical)
  - LF (Lower Failure)

6.8.1.7 - PCIE Device



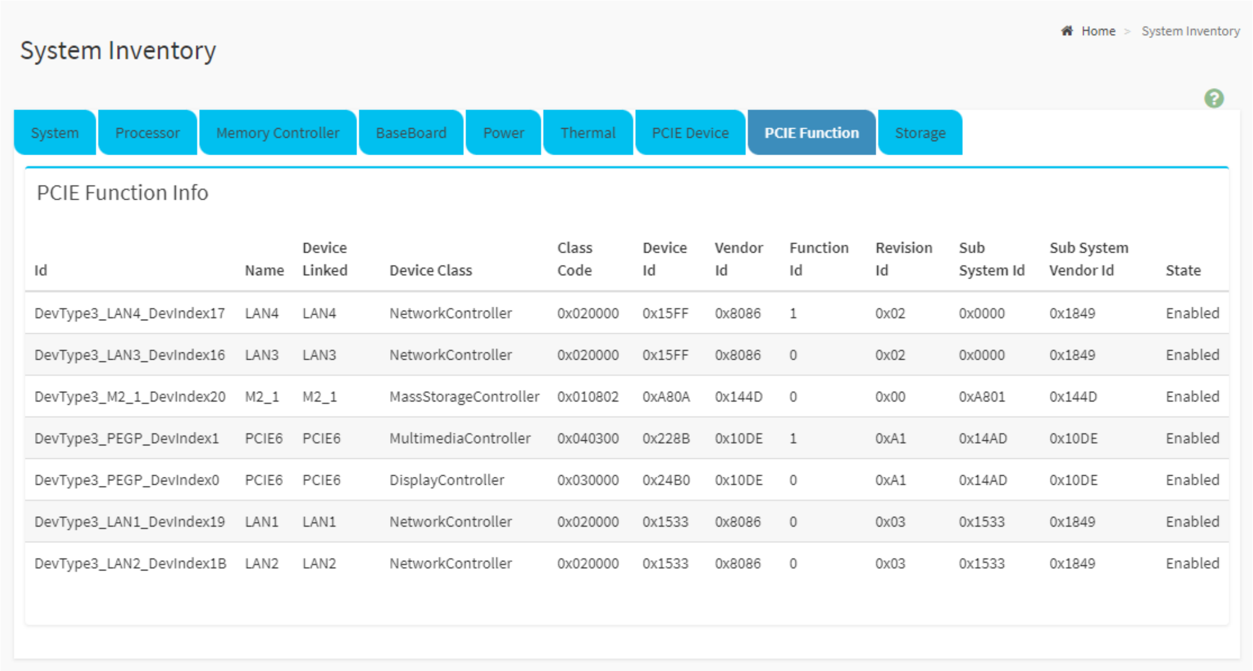
PCIE Device Info

Name	Description	Manufacturer	AssetTag	DeviceType	FirmwareVersion	State
LAN4	NA	NA	LAN4	MultiFunction	NA	Enabled
LAN3	NA	NA	LAN3	MultiFunction	1.2684.0	Enabled
M2_1	NA	NA	M2_1	SingleFunction	NA	Enabled
PCIE6	NA	NA	PCIE6	MultiFunction	NA	Enabled
LAN1	NA	NA	LAN1	SingleFunction	NA	Enabled
LAN2	NA	NA	LAN2	SingleFunction	NA	Enabled

Information Fields:

- Name
- Description
- Manufacturer
- Asset Tag
- Device Type
- Firmware Version
- State

6.8.1.8 - PCIE Function



System Inventory

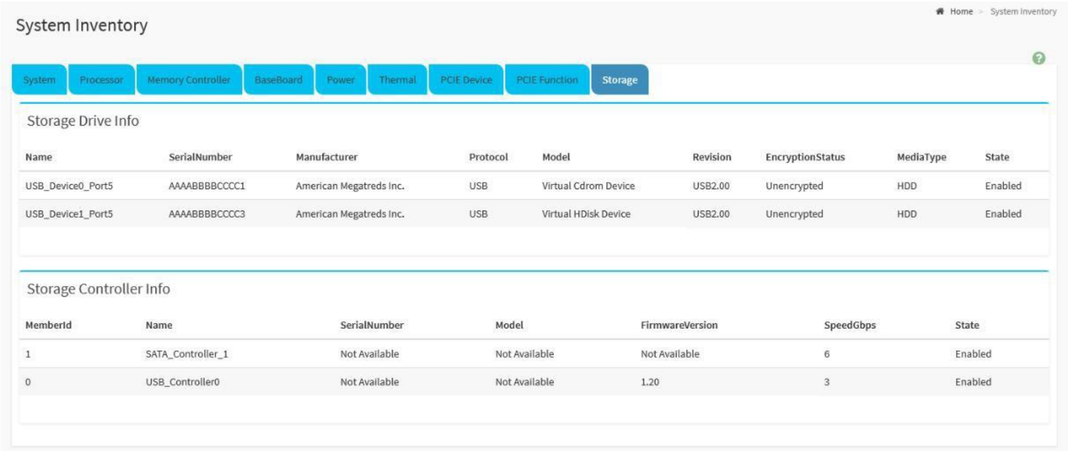
PCIE Function Info

Id	Name	Device Linked	Device Class	Class Code	Device Id	Vendor Id	Function Id	Revision Id	Sub System Id	Sub System Vendor Id	State
DevType3_LAN4_DevIndex17	LAN4	LAN4	NetworkController	0x020000	0x15FF	0x8086	1	0x02	0x0000	0x1849	Enabled
DevType3_LAN3_DevIndex16	LAN3	LAN3	NetworkController	0x020000	0x15FF	0x8086	0	0x02	0x0000	0x1849	Enabled
DevType3_M2_1_DevIndex20	M2_1	M2_1	MassStorageController	0x010802	0xA80A	0x144D	0	0x00	0xA801	0x144D	Enabled
DevType3_PEGP_DevIndex1	PCIE6	PCIE6	MultimediaController	0x040300	0x228B	0x10DE	1	0xA1	0x14AD	0x10DE	Enabled
DevType3_PEGP_DevIndex0	PCIE6	PCIE6	DisplayController	0x030000	0x24B0	0x10DE	0	0xA1	0x14AD	0x10DE	Enabled
DevType3_LAN1_DevIndex19	LAN1	LAN1	NetworkController	0x020000	0x1533	0x8086	0	0x03	0x1533	0x1849	Enabled
DevType3_LAN2_DevIndex1B	LAN2	LAN2	NetworkController	0x020000	0x1533	0x8086	0	0x03	0x1533	0x1849	Enabled

Information Fields:

- Id
- Name
- Device Linked
- Device Class
- Class Code
- Device Id
- Vendor Id
- Function Id
- Revision Id
- Sub System Id
- Sub System Vendor Id
- State

6.8.1.9 - Storage



System Inventory

Storage Drive Info

Name	SerialNumber	Manufacturer	Protocol	Model	Revision	EncryptionStatus	MediaType	State
USB_Device0_Port5	AAAABBBBCCCC1	American Megatreds Inc.	USB	Virtual Cdrom Device	USB2.00	Unencrypted	HDD	Enabled
USB_Device1_Port5	AAAABBBBCCCC3	American Megatreds Inc.	USB	Virtual HDisk Device	USB2.00	Unencrypted	HDD	Enabled

Storage Controller Info

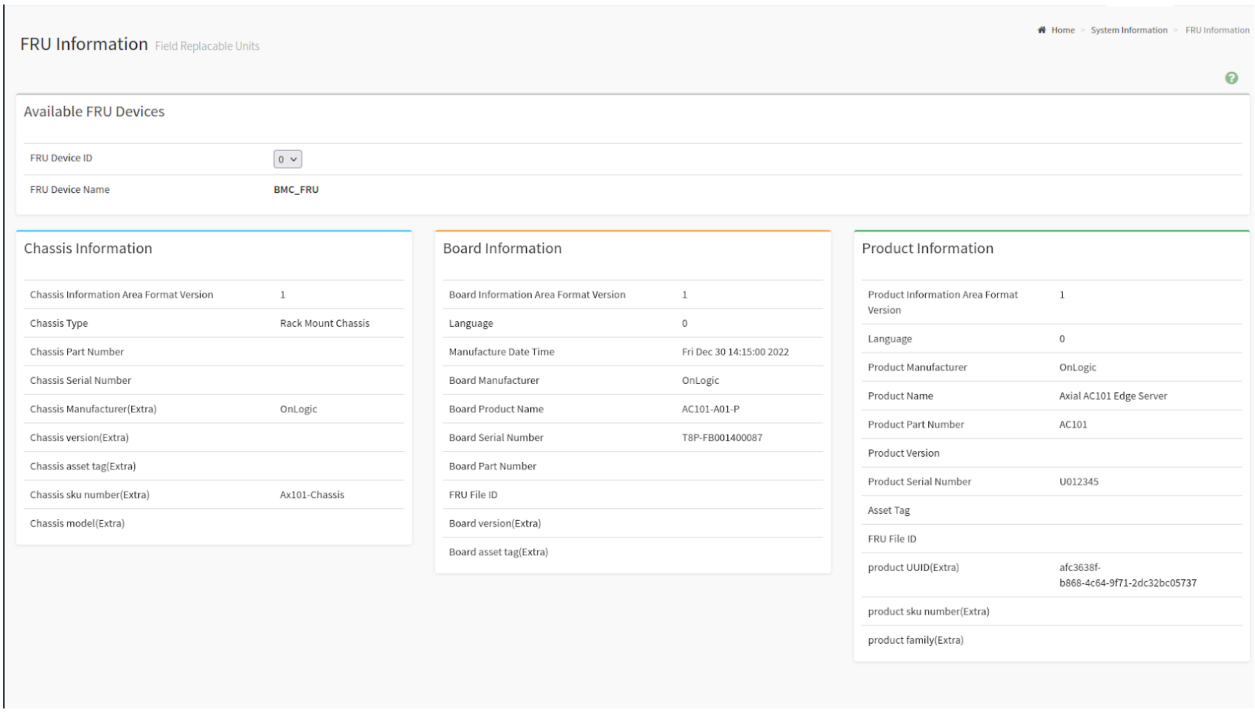
MemberId	Name	SerialNumber	Model	FirmwareVersion	SpeedGbps	State
1	SATA_Controller_1	Not Available	Not Available	Not Available	6	Enabled
0	USB_Controller0	Not Available	Not Available	1.20	3	Enabled

Information Fields:

- Storage Drive Info
  - Name
  - Serial Number
  - Manufacturer
  - Protocol
  - Model
  - Revision
  - Encryption Status
  - Media Type
  - State
- Storage Controller Info
  - Member Id
  - Name
  - Serial Number
  - Model
  - Firmware Version
  - Speed Gbps
  - State

6.8.2 - FRU Information

The FRU Information page provides product information relative to the Axial Edge Server devices.



FRU Information Field Replacable Units

Available FRU Devices

FRU Device ID	0
FRU Device Name	BMC_FRU

Chassis Information

Chassis Information Area Format Version	1
Chassis Type	Rack Mount Chassis
Chassis Part Number	
Chassis Serial Number	
Chassis Manufacturer(Extra)	OnLogic
Chassis version(Extra)	
Chassis asset tag(Extra)	
Chassis sku number(Extra)	Ax101-Chassis
Chassis model(Extra)	

Board Information

Board Information Area Format Version	1
Language	0
Manufacture Date Time	Fri Dec 30 14:15:00 2022
Board Manufacturer	OnLogic
Board Product Name	AC101-A01-P
Board Serial Number	T8P-FB001400087
Board Part Number	
FRU File ID	
Board version(Extra)	
Board asset tag(Extra)	

Product Information

Product Information Area Format Version	1
Language	0
Product Manufacturer	OnLogic
Product Name	Axial AC101 Edge Server
Product Part Number	AC101
Product Version	
Product Serial Number	U012345
Asset Tag	
FRU File ID	
product UUID(Extra)	afc3638f-b868-4c64-9f71-2dc32bc05737
product sku number(Extra)	
product family(Extra)	

The information listed on the page includes:

Available FRU Devices:

- FRU Device ID
- FRU Device Name

Chassis Information:

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Manufacturer (Extra)
- Chassis Version (Extra)
- Chassis Asset Tag (Extra)
- Chassis SKU Number (Extra)
- Chassis Model (Extra)

Board Information:

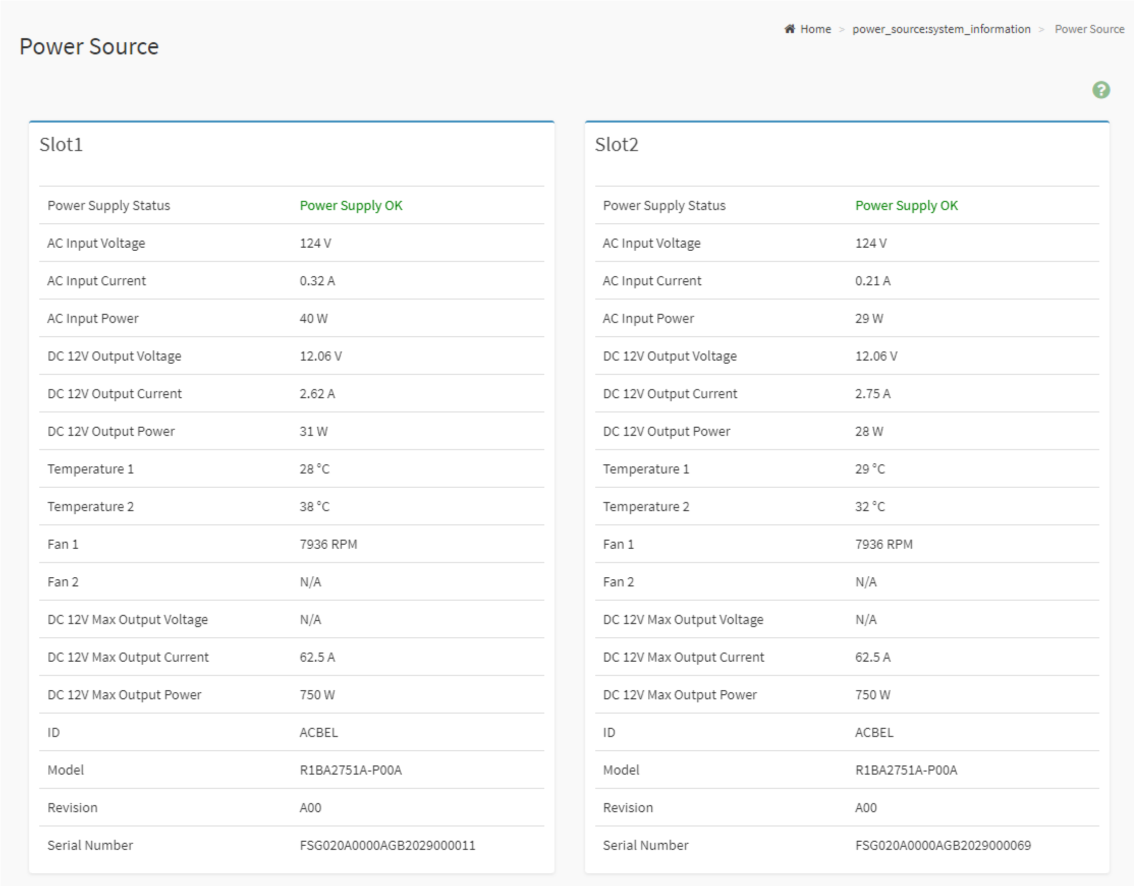
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Version (Extra)
- Board Asset Tag (Extra)

Product Information:

- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product UUID (Extra)
- Product SKU Number (Extra)
- Product Family (Extra)

6.8.3 - Power Source

The Power Source page provides information about each system power supply installed in the Axial Edge Server.



Slot1

Power Supply Status	Power Supply OK
AC Input Voltage	124 V
AC Input Current	0.32 A
AC Input Power	40 W
DC 12V Output Voltage	12.06 V
DC 12V Output Current	2.62 A
DC 12V Output Power	31 W
Temperature 1	28 °C
Temperature 2	38 °C
Fan 1	7936 RPM
Fan 2	N/A
DC 12V Max Output Voltage	N/A
DC 12V Max Output Current	62.5 A
DC 12V Max Output Power	750 W
ID	ACBEL
Model	R1BA2751A-P00A
Revision	A00
Serial Number	FSG020A0000AGB2029000011

Slot2

Power Supply Status	Power Supply OK
AC Input Voltage	124 V
AC Input Current	0.21 A
AC Input Power	29 W
DC 12V Output Voltage	12.06 V
DC 12V Output Current	2.75 A
DC 12V Output Power	28 W
Temperature 1	29 °C
Temperature 2	32 °C
Fan 1	7936 RPM
Fan 2	N/A
DC 12V Max Output Voltage	N/A
DC 12V Max Output Current	62.5 A
DC 12V Max Output Power	750 W
ID	ACBEL
Model	R1BA2751A-P00A
Revision	A00
Serial Number	FSG020A0000AGB2029000069

The information listed on the page includes the following for both PSU 1 and PSU 2:

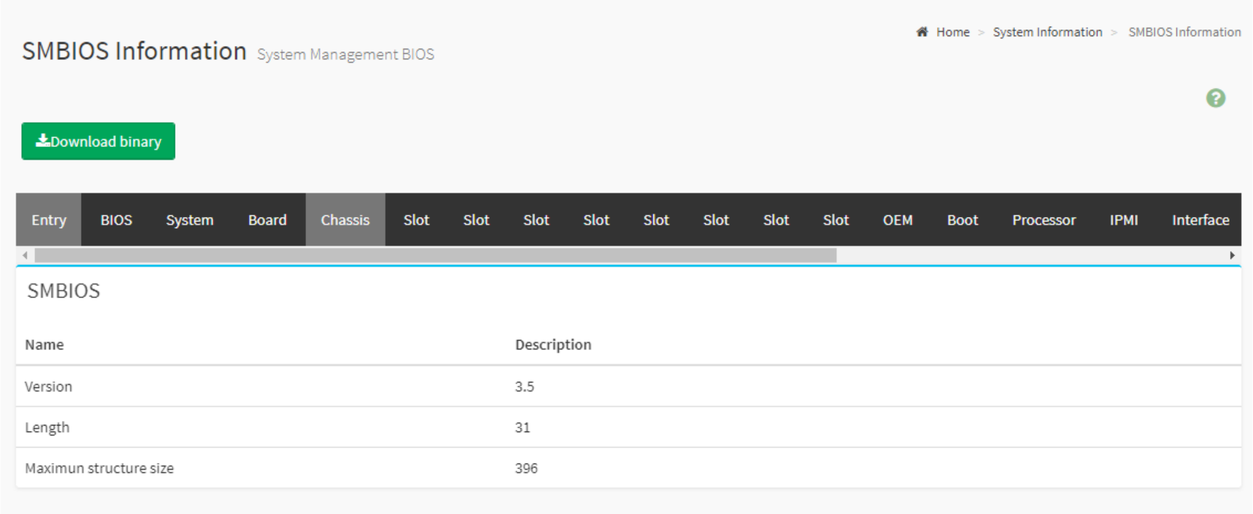
- Power Supply Status
- AC Input Voltage
- AC Input Current
- AC Input Power
- DC 12V Output Voltage
- DC 12V Output Current
- DC 12V Output Power
- Temperature 1
- Temperature 2
- Fan 1
- Fan 2
- DC 12V Max Output Voltage
- DC 12V Max Output Current
- DC 12V Max Output Power
- ID
- Model
- Revision
- Serial Number

Note: For specifics pertaining to the physical location of the PSUs within your system, please refer to the respective Axial Edge Server Product Manual.

6.8.4 - SMBIOS Information

The SMBIOS Information page provides information about SMBIOS.

For additional information pertaining to SMBIOS specifications and standards, please refer to https://www.dmtf.org/standards/smbios.



SMBIOS

Name	Description
Version	3.5
Length	31
Maximun structure size	396

To download the SMBIOS information in a raw data format, click the **Download binary** button to access the data.

Note: Hardware changes made to the system may not be reflected in the SMBIOS Information page until the system has successfully booted.

6.9 - Logs & Reports

The Axial Edge Server BMC provides logging and reporting capabilities for system events, errors, and informational messages. This logging is broken up into subsections relative to the categorization of the events.

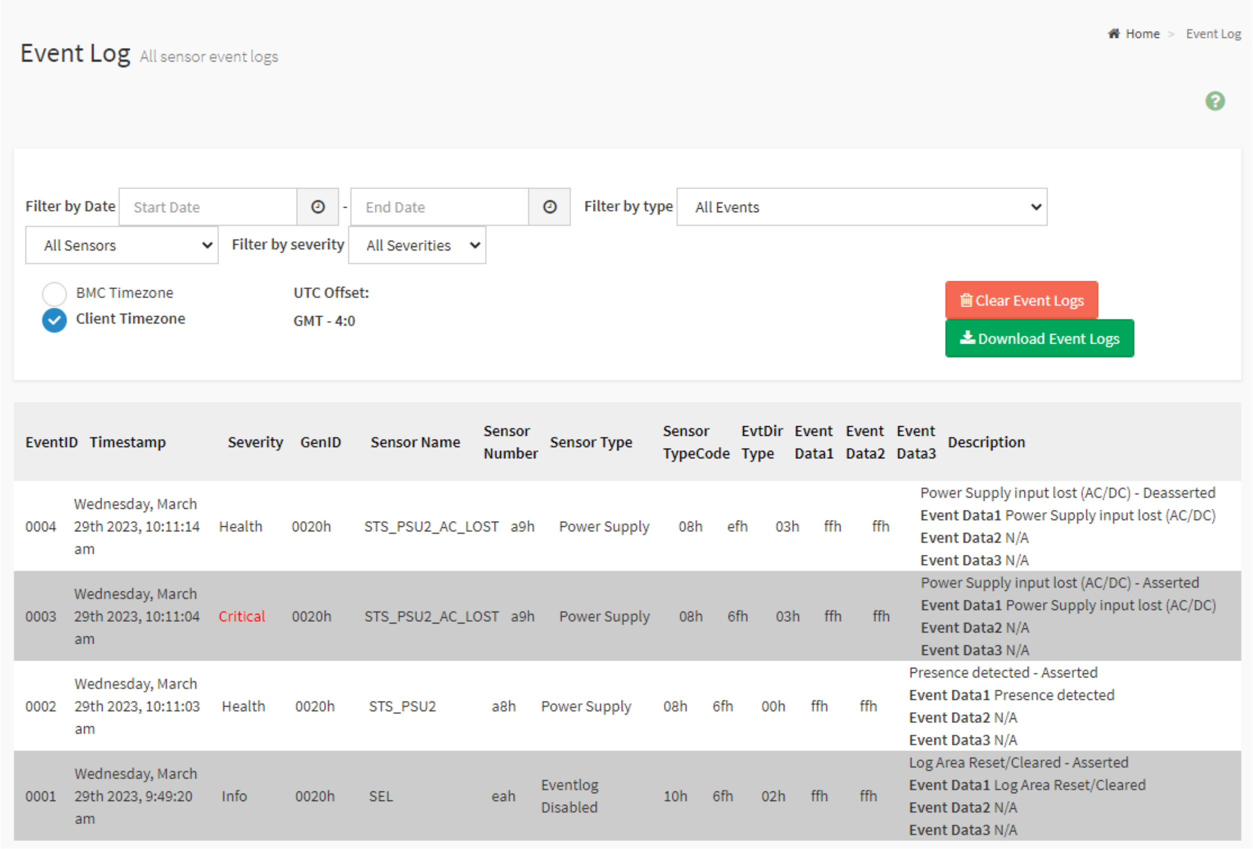
The logging subsections are as follows:

- IPMI Event Log
- System Log
- Audit Log
- Video Log
- Post Code Log
- Debug Log

From the Navigation Menu, these logging subsections can be directly accessed by expanding the sub-menu bar and clicking the respective subsection links.

6.9.1 - IPMI Event Log

The IPMI Event Log provides event log information which is generated by different sensors for users to monitor system status.



Filter by Date: Start Date - End Date
Filter by type: All Events
All Sensors
Filter by severity: All Severities

○ BMC Timezone
● Client Timezone

UTC Offset: GMT - 4:0

EventID	Timestamp	Severity	GenID	Sensor Name	Sensor Number	Sensor Type	Sensor TypeCode	EvtDir Type	Event Data1	Event Data2	Event Data3	Description
0004	Wednesday, March 29th 2023, 10:11:14 am	Health	0020h	STS_PSU2_AC_LOST	a9h	Power Supply	08h	efh	03h	ffh	ffh	Power Supply input lost (AC/DC) - Deasserted **Event Data1** Power Supply input lost (AC/DC) **Event Data2** N/A **Event Data3** N/A
0003	Wednesday, March 29th 2023, 10:11:04 am	Critical	0020h	STS_PSU2_AC_LOST	a9h	Power Supply	08h	6fh	03h	ffh	ffh	Power Supply input lost (AC/DC) - Asserted **Event Data1** Power Supply input lost (AC/DC) **Event Data2** N/A **Event Data3** N/A
0002	Wednesday, March 29th 2023, 10:11:03 am	Health	0020h	STS_PSU2	a8h	Power Supply	08h	6fh	00h	ffh	ffh	Presence detected - Asserted **Event Data1** Presence detected **Event Data2** N/A **Event Data3** N/A
0001	Wednesday, March 29th 2023, 9:49:20 am	Info	0020h	SEL	eah	Eventlog Disabled	10h	6fh	02h	ffh	ffh	Log Area Reset/Cleared - Asserted **Event Data1** Log Area Reset/Cleared **Event Data2** N/A **Event Data3** N/A

The IPMI Event Log can be filtered by adjusting the filter sections at the top of the page. The available filter fields are as follows:

- **Filter by Date:** The Start Date and End Date when the events occurred.
- **Filter by Type:** The Event Type and Sensor Type of the events.
- **Filter by Severity:** The Severity of the events

A user may also adjust the time zone reporting by toggling the **BMC Timezone** or **Client Timezone.** The timestamp value of events will be updated when the option has been changed.

Additionally, from the IPMI Event Log page, by clicking the respective buttons, it is also possible to:

- **Clear Event Logs:** Clicking the Clear Event Logs button will clear the records.
- **Download Event Logs:** Clicking the Download Event Logs button will download the event log in specific data format.

- **Download Event Logs Raw Data:** Clicking the Download Event Logs button will download the event log in raw format (typically reserved for unique support cases)

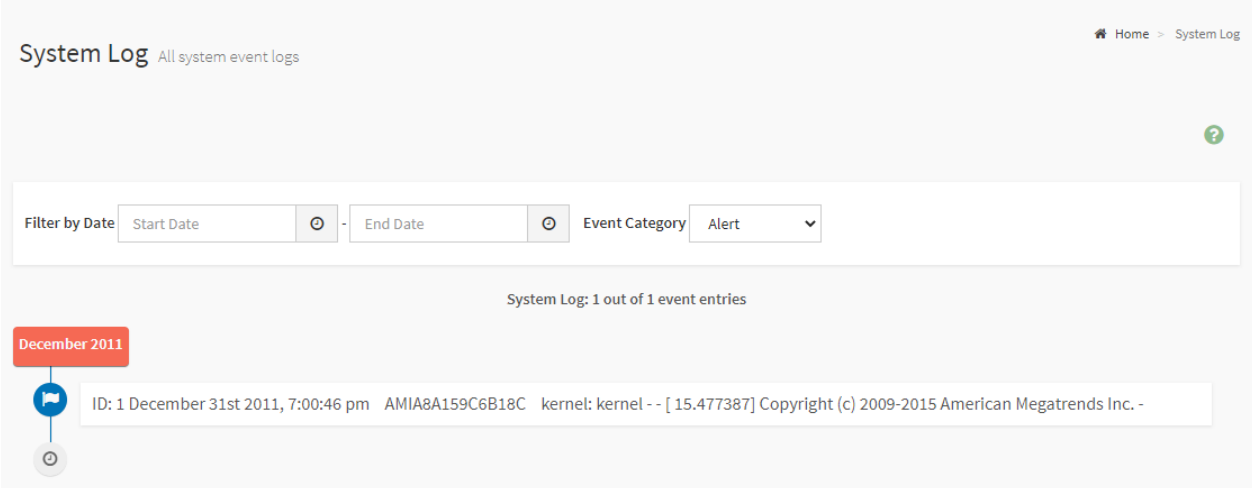
For each event record in the IPMI Event Log, the following fields will be populated:

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

6.9.2 - System Log

The System Log provides system events information that are uniquely generated by the BMC subsystem.

Note: To configure this feature, users may do so from the Advanced Log Settings page which is accessible from the **Navigation Menu** → **Settings** → **Log Settings** → **Advanced Log Settings tab**.



System Log: 1 out of 1 event entries

ID: 1 December 31st 2011, 7:00:46 pm AMIA8A159C6B18C kernel: kernel - - [15.477387] Copyright (c) 2009-2015 American Megatrends Inc. -

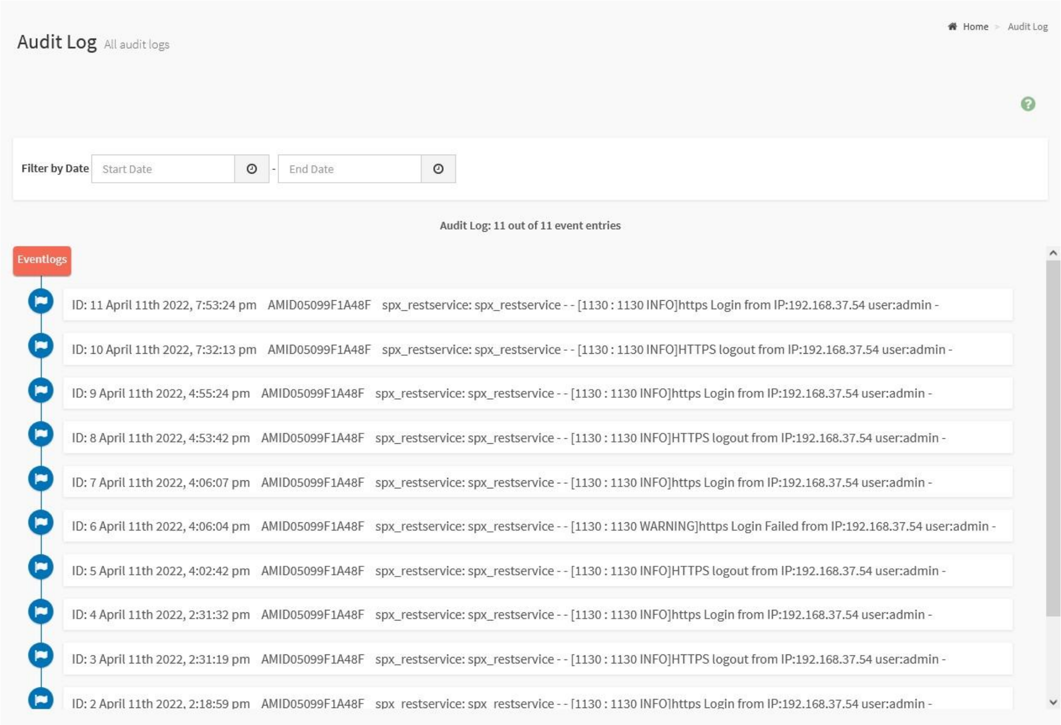
The System Log can be filtered by adjusting the filter sections at the top of the page. The available filter fields are as follows:

- **Filter by Date:** The Start Date and End Date when the events occurred.
- **Filter by Type:** The Event Type and Sensor Type of the events.
- **Filter by Event Category:** The Category of the events

6.9.3 - Audit Log

The Audit Log provides information pertaining to user logins to monitor access to the BMC.

Note: To configure this feature, users may do so from the Audit Log Settings page which is accessible from the **Navigation Menu** → **Settings** → **Log Settings** → **Advanced Log Settings tab**.



Audit Log: 11 out of 11 event entries

```
ID: 11 April 11th 2022, 7:53:24 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]https Login from IP:192.168.37.54 user:admin -
ID: 10 April 11th 2022, 7:32:13 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]HTTPS logout from IP:192.168.37.54 user:admin -
ID: 9 April 11th 2022, 4:55:24 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]https Login from IP:192.168.37.54 user:admin -
ID: 8 April 11th 2022, 4:53:42 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]HTTPS logout from IP:192.168.37.54 user:admin -
ID: 7 April 11th 2022, 4:06:07 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]https Login from IP:192.168.37.54 user:admin -
ID: 6 April 11th 2022, 4:06:04 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 WARNING]https Login Failed from IP:192.168.37.54 user:admin -
ID: 5 April 11th 2022, 4:02:42 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]HTTPS logout from IP:192.168.37.54 user:admin -
ID: 4 April 11th 2022, 2:31:32 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]https Login from IP:192.168.37.54 user:admin -
ID: 3 April 11th 2022, 2:31:19 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]HTTPS logout from IP:192.168.37.54 user:admin -
ID: 2 April 11th 2022, 2:18:59 pm   AMID05099F1A48F   spx_restservice: spx_restservice - - [1130 : 1130 INFO]https Login from IP:192.168.37.54 user:admin -
```

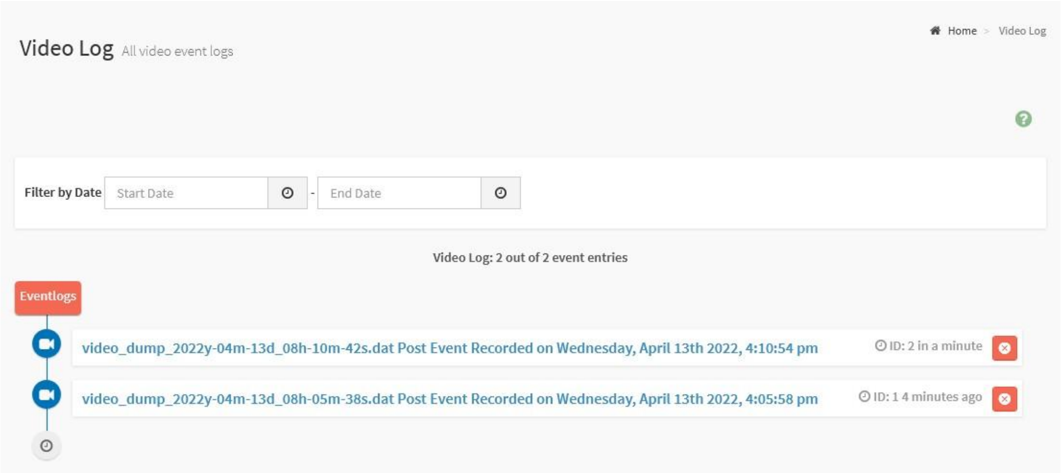
The Audit Log can be filtered by adjusting the filter sections at the top of the page. The available filter fields are as follows:

- **Filter by Date:** The Start Date and End Date when the events occurred.

6.9.4 - Video Log

The Video Log provides a log of the recorded video based on triggered events.

Note: To configure video recording triggers and the respective data store, users may navigate to the **Auto Video Settings** page which is accessible via the **Navigation Menu** → **Settings** → **Video Recording** → **Auto Video Settings**.



Video Log All video event logs

Home > Video Log

Filter by Date Start Date - End Date

Video Log: 2 out of 2 event entries

Eventlogs

video_dump_2022y-04m-13d_08h-10m-42s.dat Post Event Recorded on Wednesday, April 13th 2022, 4:10:54 pm ID: 2 in a minute

video_dump_2022y-04m-13d_08h-05m-38s.dat Post Event Recorded on Wednesday, April 13th 2022, 4:05:58 pm ID: 1 4 minutes ago

To view the recorded video, click the event record listed in the log.

Videos may be Downloaded directly to a local system.

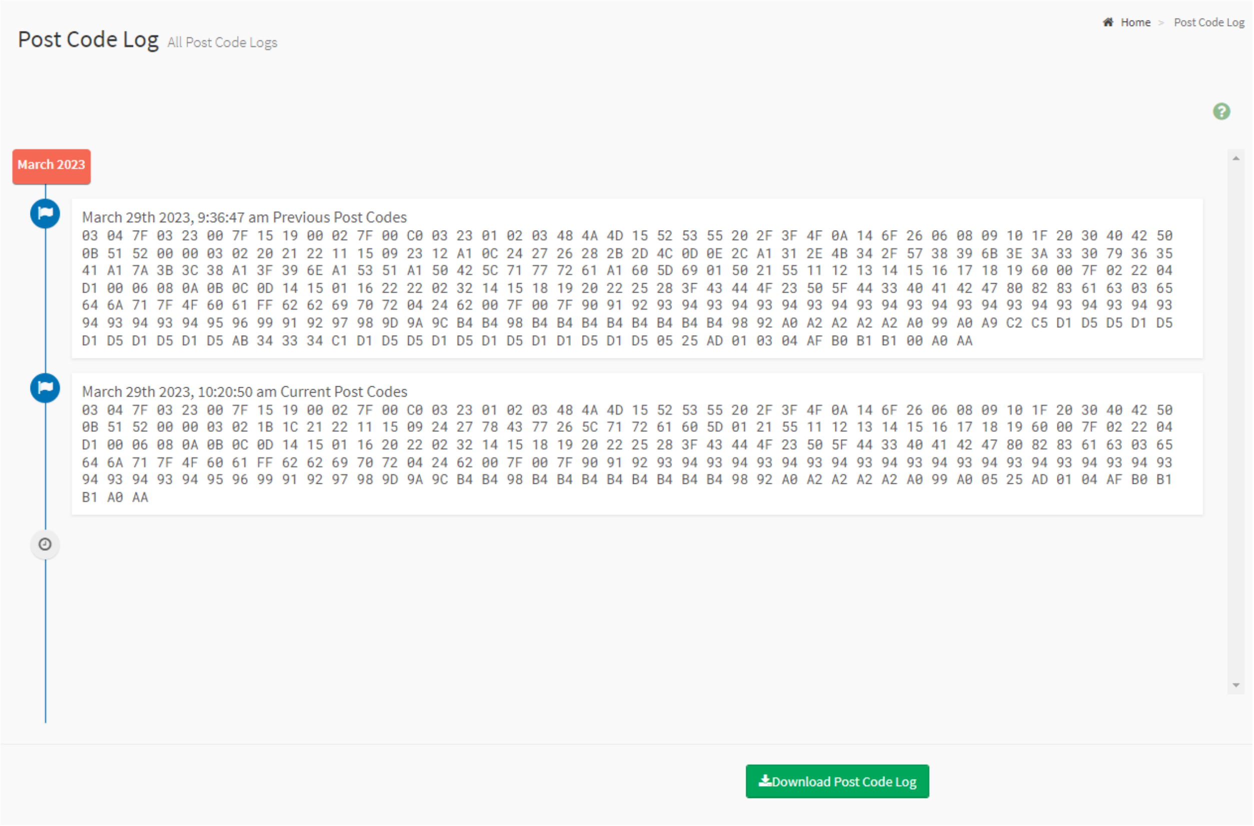
The Video Log can be filtered by adjusting the filter sections at the top of the page. The available filter fields are as follows:

- **Filter by Date:** The Start Date and End Date when the events occurred.

Clicking on the Delete Icon (⊗) will delete the video event record and its video.

6.9.5 - Post Code

The Post Code page provides the UEFI (BIOS) POST code information to monitor the BIOS POST process and system power-on status.



March 29th 2023, 9:36:47 am Previous Post Codes

```
03 04 7F 03 23 00 7F 15 19 00 02 7F 00 C0 03 23 01 02 03 48 4A 4D 15 52 53 55 20 2F 3F 4F 0A 14 6F 26 06 08 09 10 1F 20 30 40 42 50
0B 51 52 00 00 03 02 20 21 22 11 15 09 23 12 A1 0C 24 27 26 28 2B 2D 4C 0D 0E 2C A1 31 2E 4B 34 2F 57 38 39 6B 3E 3A 33 30 79 36 35
41 A1 7A 3B 3C 38 A1 3F 39 6E A1 53 51 A1 50 42 5C 71 77 72 61 A1 60 5D 69 01 50 21 55 11 12 13 14 15 16 17 18 19 60 00 7F 02 22 04
D1 00 06 08 0A 0B 0C 0D 14 15 01 16 22 22 02 32 14 15 18 19 20 22 25 28 3F 43 44 4F 23 50 5F 44 33 40 41 42 47 80 82 83 61 63 03 65
64 6A 71 7F 4F 60 61 FF 62 62 69 70 72 04 24 62 00 7F 00 7F 90 91 92 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93
94 93 94 93 94 95 96 99 91 92 97 98 9D 9A 9C B4 B4 98 B4 B4 B4 B4 B4 B4 B4 B4 98 92 A0 A2 A2 A2 A2 A0 99 A0 A9 C2 C5 D1 D5 D5 D1 D5
D1 D5 D1 D5 D1 D5 AB 34 33 34 C1 D1 D5 D5 D1 D5 D1 D5 D1 D1 D5 D1 D5 05 25 AD 01 03 04 AF B0 B1 B1 00 A0 AA
```

March 29th 2023, 10:20:50 am Current Post Codes

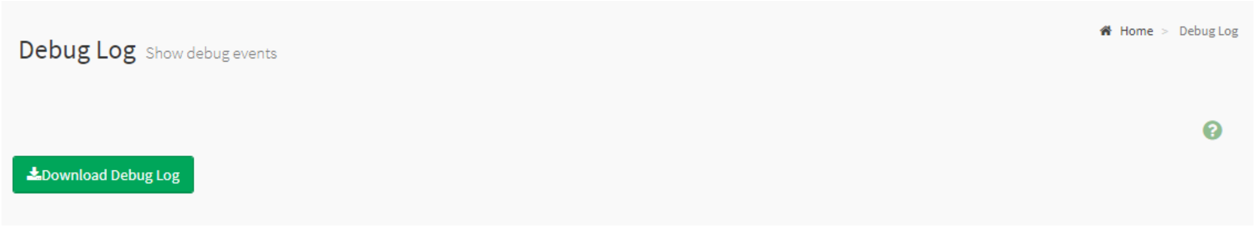
```
03 04 7F 03 23 00 7F 15 19 00 02 7F 00 C0 03 23 01 02 03 48 4A 4D 15 52 53 55 20 2F 3F 4F 0A 14 6F 26 06 08 09 10 1F 20 30 40 42 50
0B 51 52 00 00 03 02 1B 1C 21 22 11 15 09 24 27 78 43 77 26 5C 71 72 61 60 5D 01 21 55 11 12 13 14 15 16 17 18 19 60 00 7F 02 22 04
D1 00 06 08 0A 0B 0C 0D 14 15 01 16 20 22 02 32 14 15 18 19 20 22 25 28 3F 43 44 4F 23 50 5F 44 33 40 41 42 47 80 82 83 61 63 03 65
64 6A 71 7F 4F 60 61 FF 62 62 69 70 72 04 24 62 00 7F 00 7F 90 91 92 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93 94 93
94 93 94 93 94 95 96 99 91 92 97 98 9D 9A 9C B4 B4 98 B4 B4 B4 B4 B4 B4 B4 B4 98 92 A0 A2 A2 A2 A2 A0 99 A0 05 25 AD 01 04 AF B0 B1
B1 A0 AA
```

The Post Code Log may be downloaded and saved to a local system by clicking the **Download Post Code Log** button.

6.9.6 - Debug Log

The Debug Log page provides a mechanism to download all of the available logs and debug diagnostics stored in the BMC.

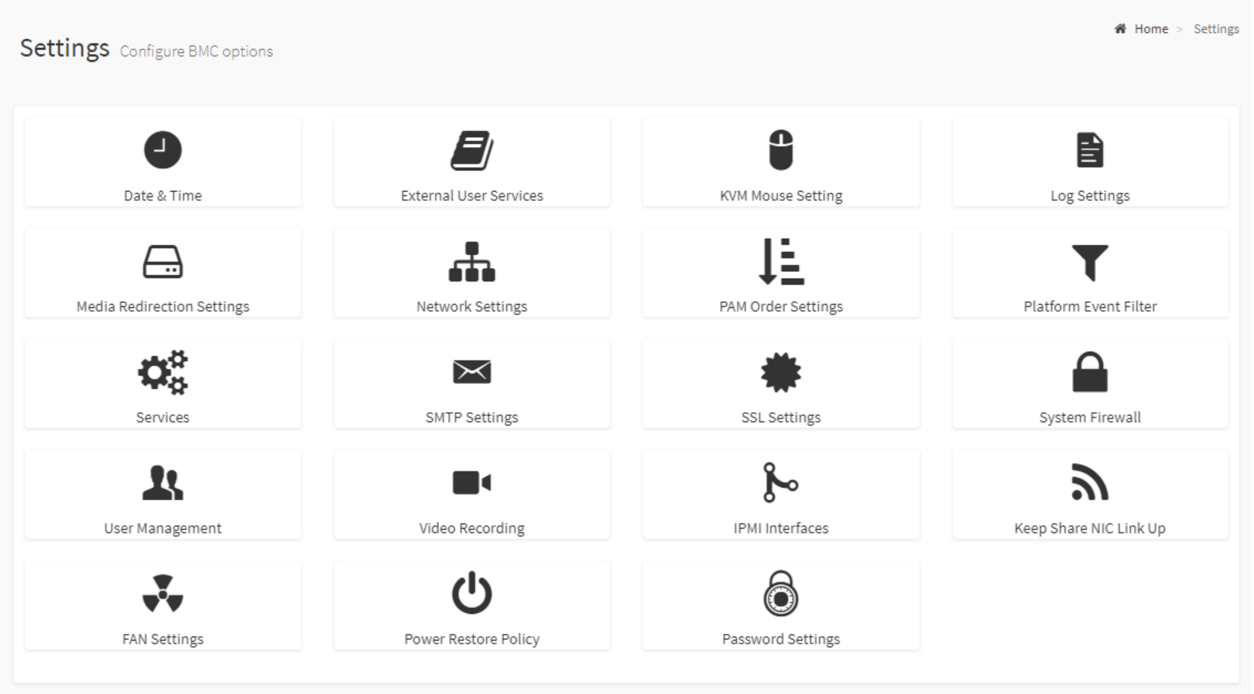
This feature is typically reserved to aid with customer support and problem determination.



The Debug Log may be downloaded and saved to a local system by clicking the **Download Debug Code Log** button.

6.10 - Settings

The Settings page provides access to the configurable parameters and services that are enabled by the BMC.



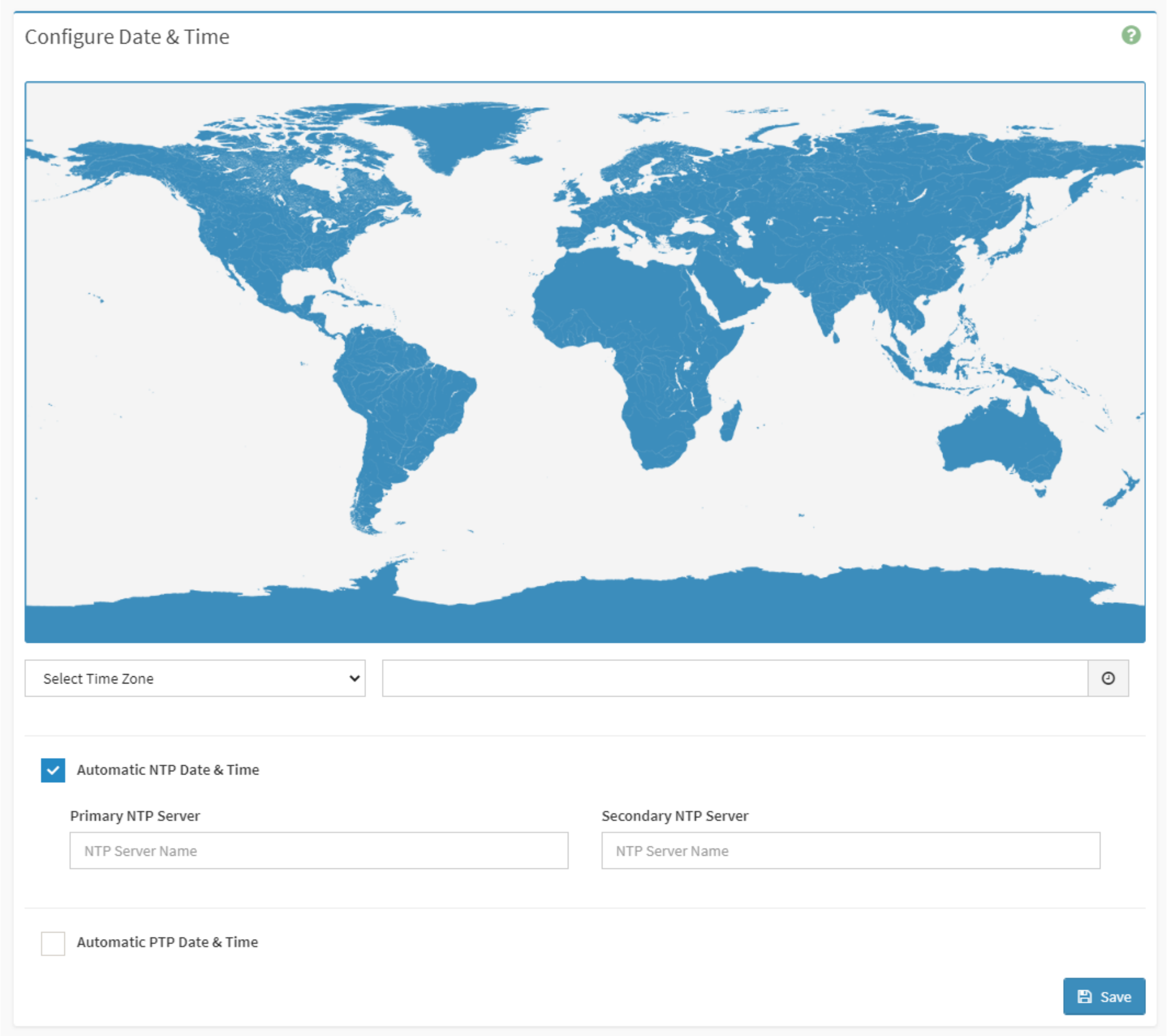
The configuration of these settings is broken down in the categories (pages) listed below:

- Date & Time
- External User Services
- KVM Mouse Setting
- Log Settings
- Media Redirection Settings
- Network Settings
- PAM Order Settings
- Platform Event Filter
- Services
- SMTP Settings
- SSL Settings
- System Firewall
- User Management
- Video Recording
- IPMI Interface
- Keep Share NIC Link Up
- FAN Settings
- Power Restore Policy
- Password Settings

The following subsections provide additional details and descriptions of the configurable settings.

6.10.1 - Date & Time

The Date & Time page provides the ability for users to configure the date and time of the BMC.



Configure Date & Time

☑ Automatic NTP Date & Time

Primary NTP Server: NTP Server Name

Secondary NTP Server: NTP Server Name

□ Automatic PTP Date & Time

Configurable Fields:

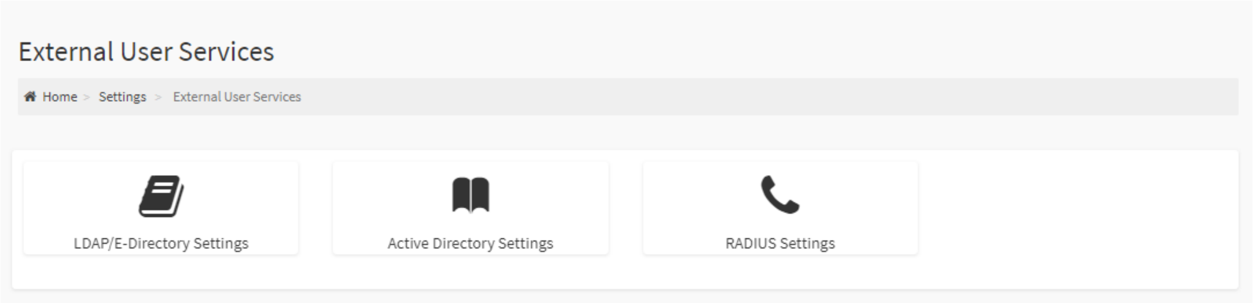
- **Configure Date & Time Map:** Visual display of time zone. Navigational line to select location.
- **Select Time Zone**: Used to set the date and time of the BMC.
- **Automatic Date & Time:** Check to enable Date and Time to synchronize with an NTP Server.
  - **Primary NTP Server:** The primary NTP server to use.
  - **Secondary NTP Server:** The secondary NTP server.
- **Clock Icon ⊙:** Manually modify the Date and Time.
- **Save:** Save the configured settings.

Note: Map selection is disabled if the time zone is set as Manual Offset.

Note: Time Zone settings will only be reflected only after saving the settings.

6.10.2 - External User Services

The External User Services page provides the ability to configure the BMC with external user services, such as LDAP/E-Directory, Active Directory, or RADIUS.



External User Services

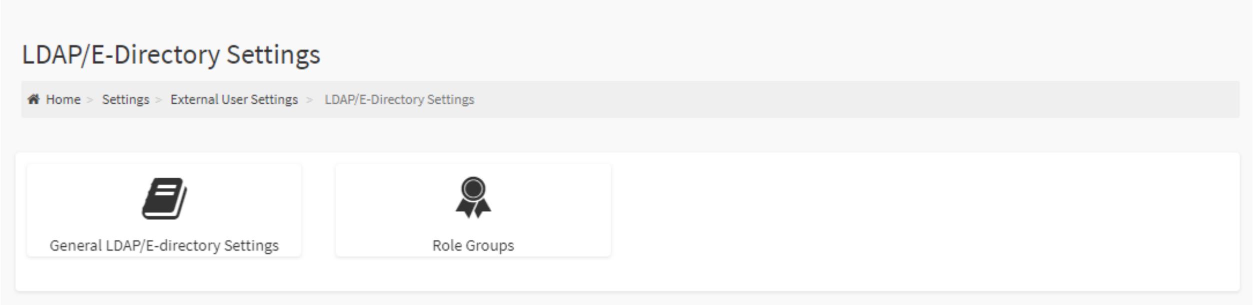
Home > Settings > External User Services

The enablement and configuration of these external user services are outlined in the following subsections.

6.10.2.1 - LDAP/E-Directory Settings

The LDAP/E-Directory Settings page provides two functional feature tabs for users to configure the LDAP settings. They are as follows:

- General LDAP/E-directory Settings
- Role Groups



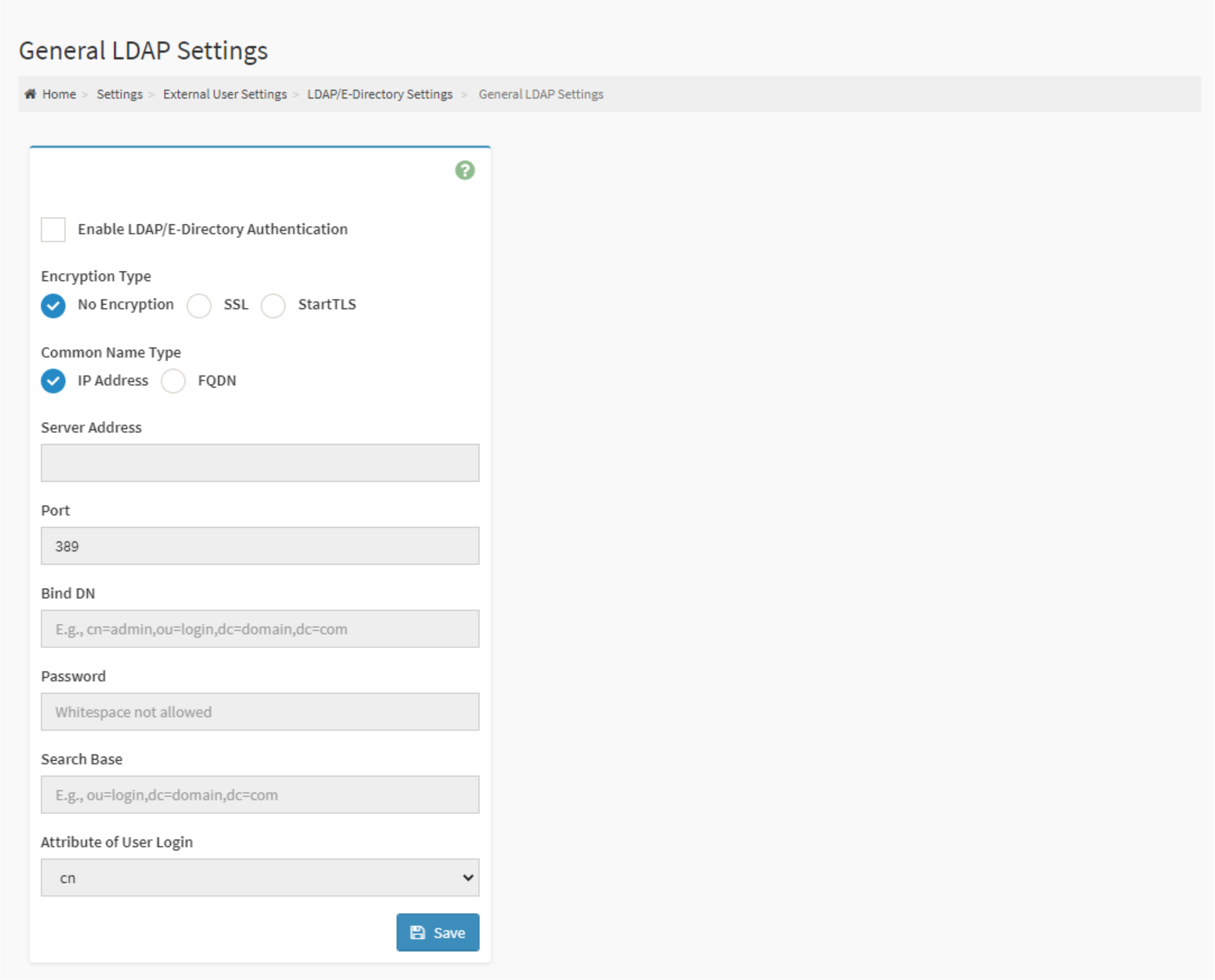
LDAP/E-Directory Settings

Home > Settings > External User Settings > LDAP/E-Directory Settings

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

6.10.2.1.1 - General LDAP/E-Directory Settings

The General LDAP Settings page provides the ability to configure the LDAP/E-Directory Settings.



General LDAP Settings

Home > Settings > External User Settings > LDAP/E-Directory Settings > General LDAP Settings

□ Enable LDAP/E-Directory Authentication

Encryption Type
● No Encryption ○ SSL ○ StartTLS

Common Name Type
● IP Address ○ FQDN

Server Address

Port
389

Bind DN
E.g., cn=admin,ou=login,dc=domain,dc=com

Password
Whitespace not allowed

Search Base
E.g., ou=login,dc=domain,dc=com

Attribute of User Login
cn

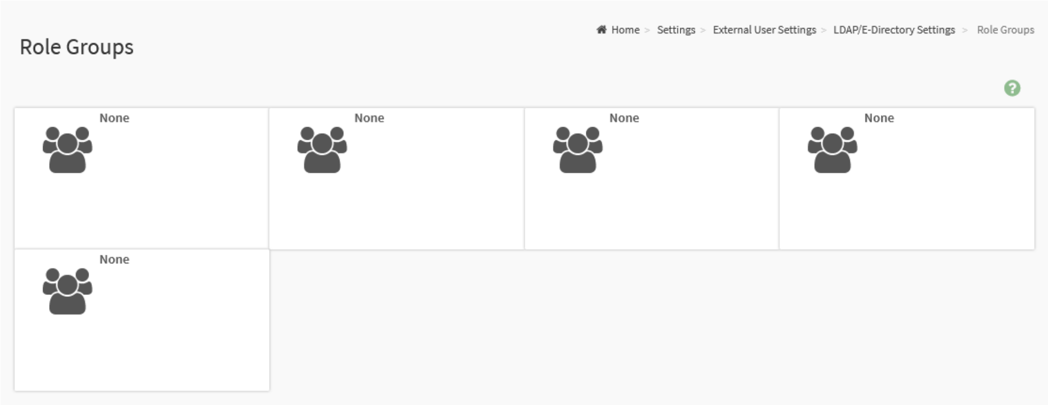
Configurable Fields:

- **Enable LDAP/E-Directory Authentication:** Click this option to enable LADP/E-Directory Settings.
- **Encryption Type:** Encryption type for LDAP/E-Directory (No Encryption, SSL, StartTLS). When using SSL or StartTLS, a CA certificate file, Certificate File and Private Key are required.
- **Common Name Type:** Select the Common Name Type (IP Address, FQDN)
- **Server Address:** Enter the LDAP/E-Directory server address. IPv4 and IPv6 address formats are supported. If using StartTLS with FQDN, ensure that an FQDN address is entered.
- **Port:** 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. Only cn or uid is supported.
- **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:** Save the configured settings.

6.10.2.1.2 Role Groups

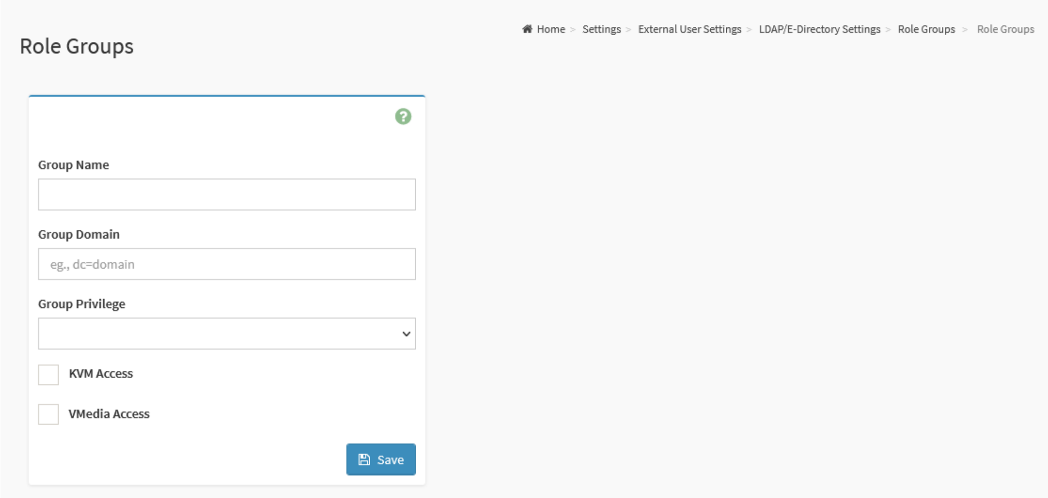
The LDAP Settings / Role Groups page provides the ability to add a new role group.



Role Groups

Home > Settings > External User Settings > LDAP/E-Directory Settings > Role Groups
None
None
None
None
None

To add a new role group, click on the Slot icon (👥) which will navigate to the Role Groups configuration page as follows:



Role Groups

Group Name

Group Domain: eg., dc=domain

Group Privilege

□ KVM Access

□ VMedia Access

Home > Settings > External User Settings > LDAP/E-Directory Settings > Role Groups > Role Groups
Save

Configurable Fields:

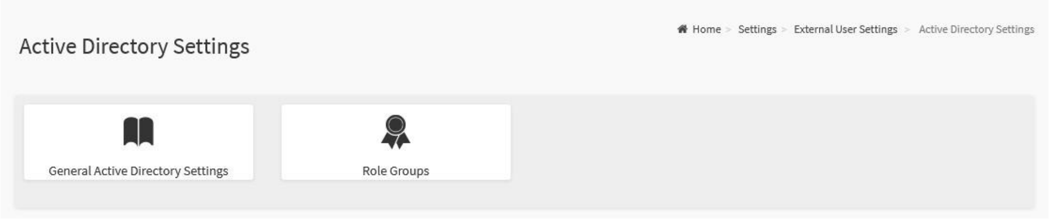
- **Group Name:** The Role Group Name that identifies the role group in LDAP/E-Directory.
- **Group Domain:** The Role Group Domain where the role group is located.
- **Group Privilege:** The Role Group level of privilege to be assigned for this role group

- **KVM Access:** Check to enable KVM privilege for the role group.
- **VMedia Access:** Check to enable VMedia privilege for the role group.
- **Save:** Save the configured settings.

6.10.2.2 - Active Directory Settings

The Active Directory Settings page provides two functional feature tabs for users to configure the Active Directory settings. They are as follows:

- General Active Directory Settings
- Role Groups



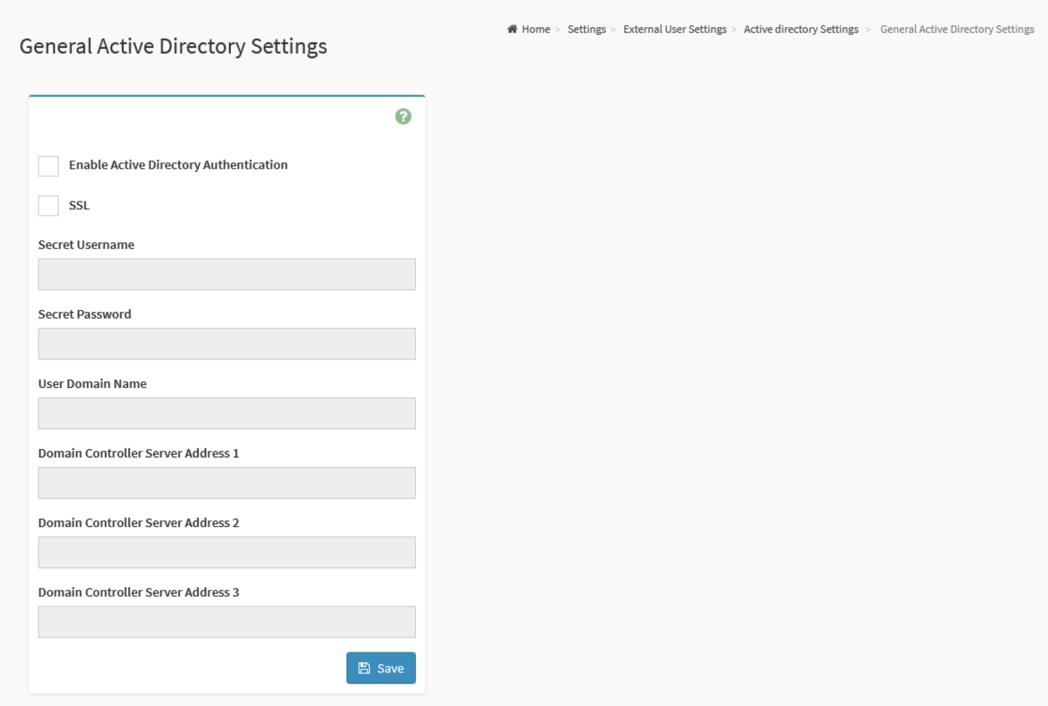
Active Directory Settings

Home > Settings > External User Settings > Active Directory Settings
General Active Directory Settings
Role Groups

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

6.10.2.2.1 General Active Directory Settings

The General Active Directory Settings page provides the ability for users to configure the Active Directory Settings.



General Active Directory Settings

Home > Settings > External User Settings > Active directory Settings > General Active Directory Settings

□ Enable Active Directory Authentication

□ SSL

Secret Username

Secret Password

User Domain Name

Domain Controller Server Address 1

Domain Controller Server Address 2

Domain Controller Server Address 3

Save

Configurable Fields:

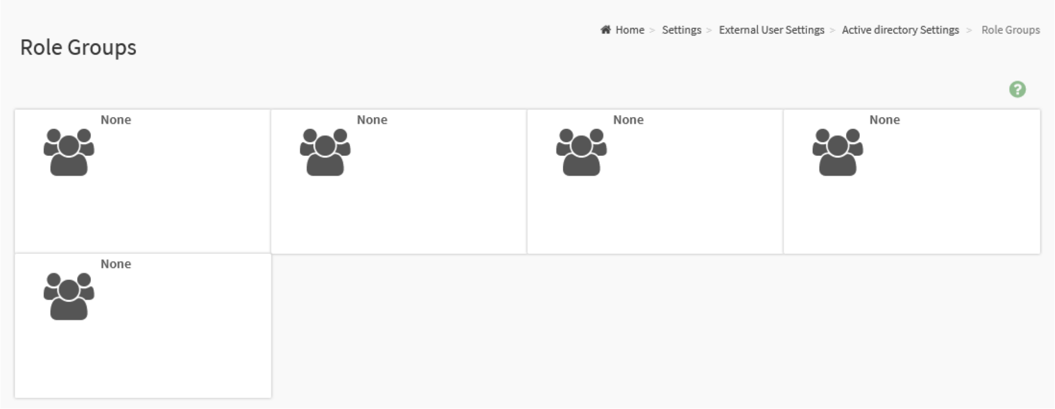
- **Enable Active Directory Authentication:** Check this option to enable Active Directory Settings.
- **SSL:** Check this option to enable SSL support.
- **Secret Username:** The Username of an administrator of the Active Directory Server.
- **Secret Password:** The Password of the administrator.
- **User Domain Name:** The Domain Name for the user e.g. MyDomain.com
- **Domain Controller Server Address 1:** The IP address of Active Directory server.
- **Domain Controller Server Address 2:** The IP address of Active Directory server.
- **Domain Controller Server Address 3:** The IP address of Active Directory server.

  Note: IPv4 and IPv6 address formats are supported for all Domain Controller Server Addresses.

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

6.10.2.2.2 Role Groups

The Active Directory Settings / Role Groups page provides the ability to add a new role group.



Role Groups

Home > Settings > External User Settings > Active directory Settings > Role Groups

None

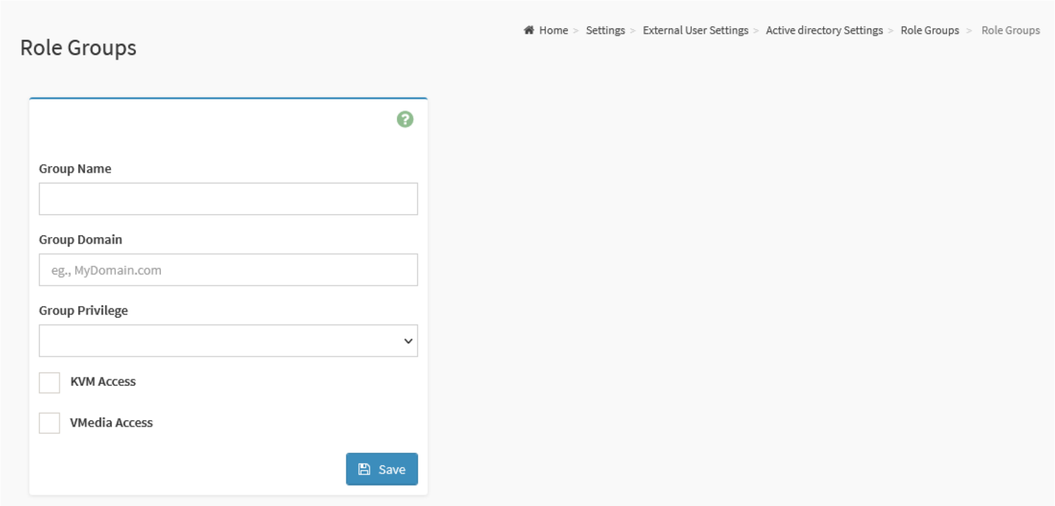
None

None

None

None

To add a new role group, click on the Slot icon (👥) which will navigate to the Role Groups configuration page as follows:



Role Groups

Home > Settings > External User Settings > Active directory Settings > Role Groups > Role Groups

Group Name

Group Domain

eg., MyDomain.com

Group Privilege

□ KVM Access

□ VMedia Access

Save

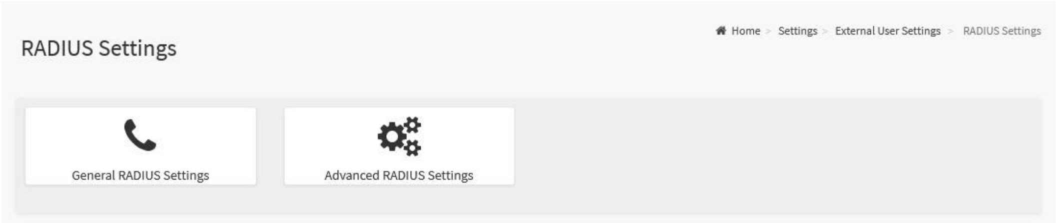
Configurable Fields:

- **Group Name:** The Role Group Name that identifies the role group in LDAP/E-Directory.
- **Group Domain:** The Role Group Domain where the role group is located.
- **Group Privilege:** The Role Group level of privilege to be assigned for this role group
- **KVM Access:** Check to enable KVM privilege for the role group.
- **VMedia Access:** Check to enable VMedia privilege for the role group.
- **Save:** Save the configured settings.

6.10.2.3 - RADIUS Settings

The RADIUS Settings page provides two functional feature tabs for users to configure the RADIUS settings. They are as follows:

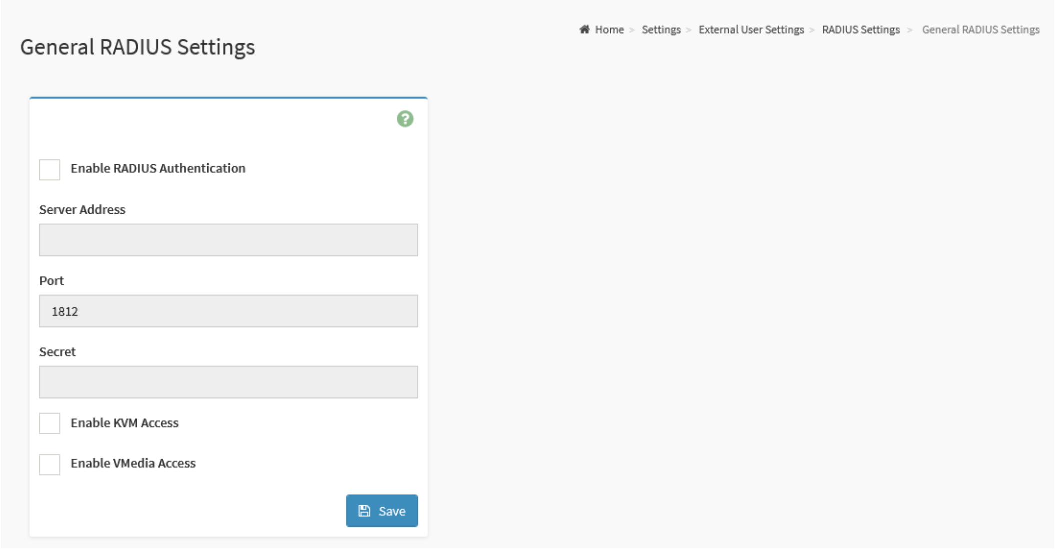
- General RADIUS Settings
- Advanced RADIUS Settings



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

6.10.2.3.1 General RADIUS Settings

The General RADIUS Settings page provides the ability for users to configure the RADIUS Settings.



General RADIUS Settings

Home > Settings > External User Settings > RADIUS Settings > General RADIUS Settings

□ Enable RADIUS Authentication

Server Address

Port

1812

Secret

□ Enable KVM Access

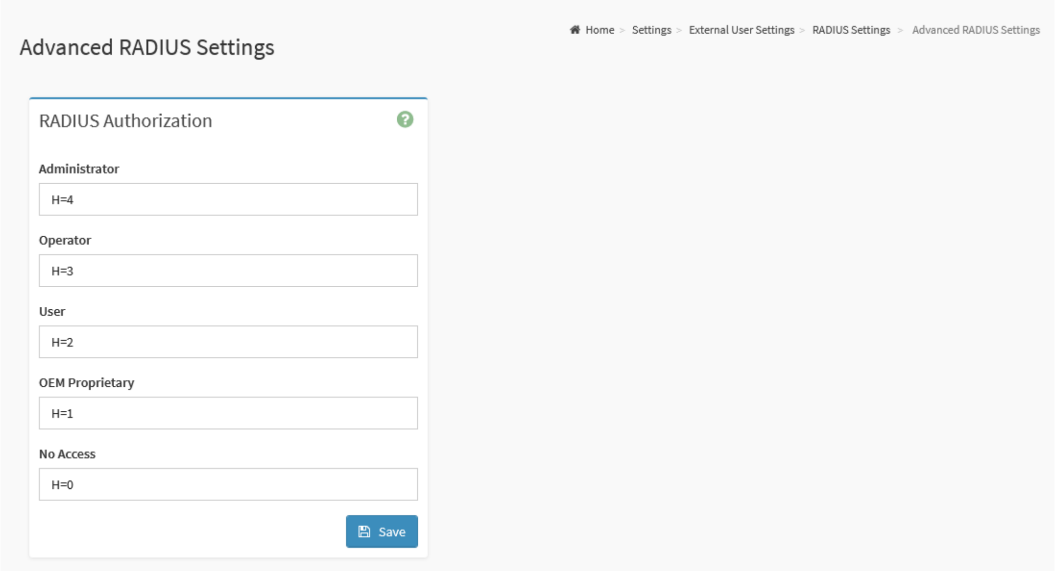
□ Enable VMedia Access

Configurable Fields:

- **Enable RADIUS Authentication:** Check to enable RADIUS Authentication.
- **Server Address:** The RADIUS Server Address.
- **Port:** The RADIUS Port number.
- **Secret:** Specify RADIUS Server Secret (Password).
- **KVM Access:** Check to enable KVM privilege for authenticated users.
- **VMedia Access:** Check to enable VMedia privilege for authenticated users.
- **Save:** Save the configured settings.

6.10.2.3.2 - Advanced RADIUS Settings

The Advanced RADIUS Settings page provides the ability for users to configure the RADIUS authorization.



Advanced RADIUS Settings

Home > Settings > External User Settings > RADIUS Settings > Advanced RADIUS Settings

RADIUS Authorization

Administrator: H=4

Operator: H=3

User: H=2

OEM Proprietary: H=1

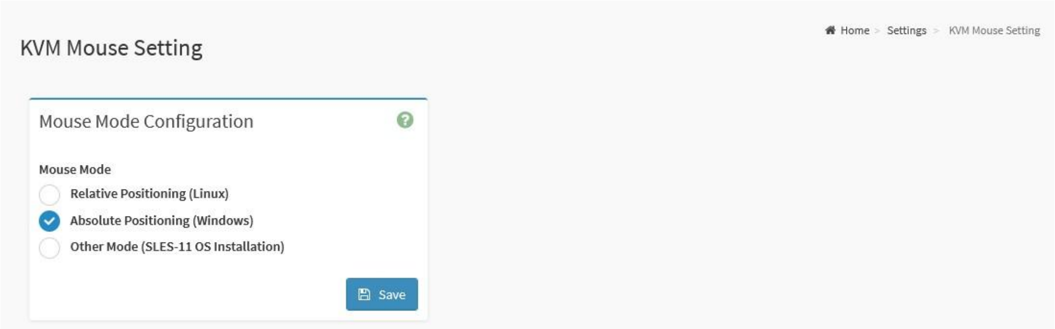
No Access: H=0

Configurable Fields:

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

6.10.3 - KVM Mouse Setting

In the BMC WebUI service, Redirection Console handles mouse emulation from local window to remote screen in either of three methods: Relative Mouse mode, Absolute Mouse mode, and Other Mouse mode.



KVM Mouse Setting

Home > Settings > KVM Mouse Setting

Mouse Mode Configuration

Mouse Mode

○ Relative Positioning (Linux)

● Absolute Positioning (Windows)

○ Other Mode (SLES-11 OS Installation)

Configurable Fields:

- **Relative Positioning (Linux):** The relative mode sends the calculated relative mouse position displacement to the system.
- **Absolute Positioning (Windows):** The absolute position of the local mouse is sent to the system.

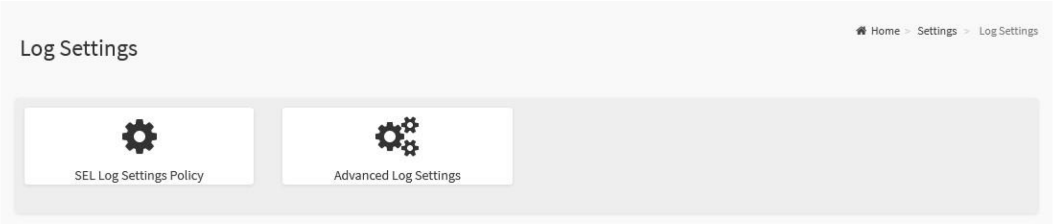
  Note: This setting is recommended for Windows and recent Linux releases (2021 and newer).

- **Other Mode (SLES-11 OS Installation):** This option sends the calculated displacement from the local mouse in the center position to the system.
- **Save:** Save the configured settings.

6.10.4 - Log Settings

Log Settings page provides the capability to configure the logging policies and settings. From the Log settings page, users will be able to configure the following:

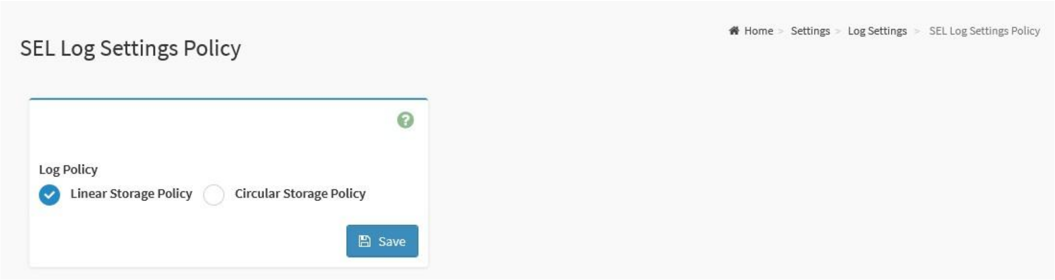
- SEL Log Settings Policy
- Advanced Log Settings



The details about each Log Settings page are listed in the following subsections.

6.10.4.1 - SEL Log Settings Policy

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



SEL Log Settings Policy

Home > Settings > Log Settings > SEL Log Settings Policy

Log Policy

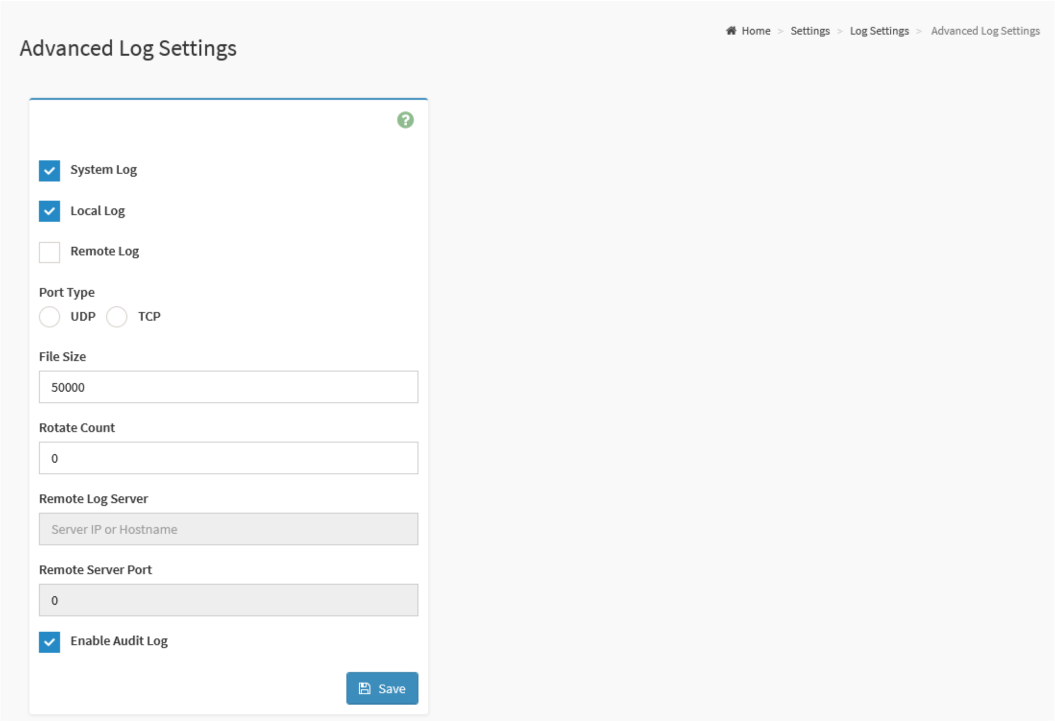
● Linear Storage Policy ○ Circular Storage Policy

Configurable Fields:

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

6.10.4.2 - Advanced Log Settings

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


Advanced Log Settings

Home > Settings > Log Settings > Advanced Log Settings

☑ System Log

☑ Local Log

□ Remote Log

Port Type

○ UDP ○ TCP

File Size: 50000

Rotate Count: 0

Remote Log Server: Server IP or Hostname

Remote Server Port: 0

☑ Enable Audit Log

Configurable Fields:

- **System Log:** Check to Enable System Log to view all system events for this device.
- **Local Log:** Check to save the log locally on the BMC.
- **Remote Log:** Check to save the logs on to a remote machine.
- **Port Type:** Port Type is supported with enable Remote Log, select either UDP or TCP
- **File Size:** Specify the size of the file in bytes if the selected log type is local.
- **Rotate Count:** 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 the rotate count is zero, then the old log information gets cleared permanently.

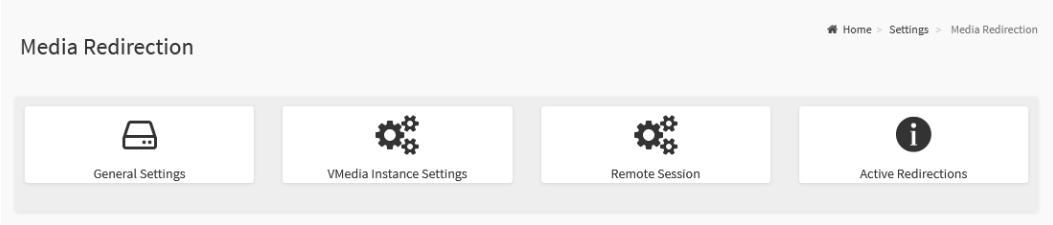
  Note: File Size and Rotate Count options are only available when Local Log is enabled.

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

6.10.5 - Media Redirection

Media Redirection page provides various functional feature tabs for users to configure the media into BMC for redirection, including

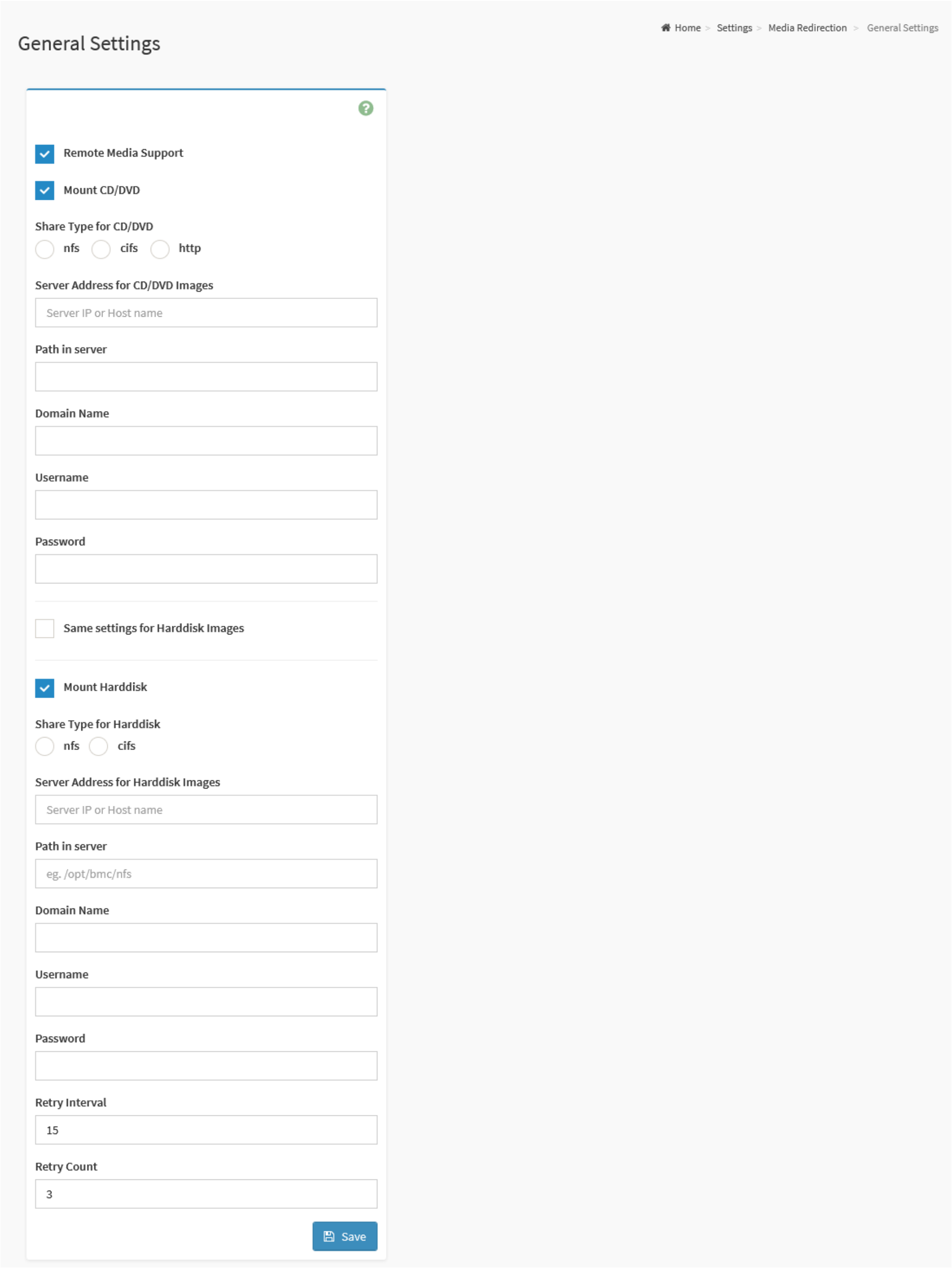
- General Settings
- VMedia Instance Settings
- Remote Session
- Active Redirections



The details of each Media Redirection page are listed in the following subsections.

6.10.5.1 - General Settings

This page provides the ability to configure the general Media Redirection settings.



General Settings

☑ Remote Media Support

☑ Mount CD/DVD

Share Type for CD/DVD

○ nfs ○ cifs ○ http

Server Address for CD/DVD Images: Server IP or Host name

Path in server:

Domain Name:

Username:

Password:

□ Same settings for Harddisk Images

☑ Mount Harddisk

Share Type for Harddisk

○ nfs ○ cifs

Server Address for Harddisk Images: Server IP or Host name

Path in server: eg. /opt/bmc/nfs

Domain Name:

Username:

Password:

Retry Interval: 15

Retry Count: 3

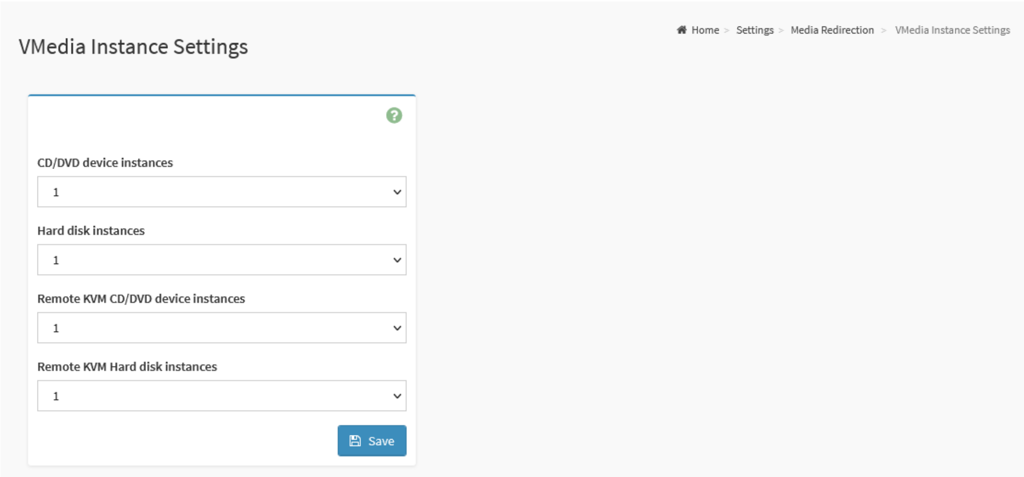
Configurable Fields:

- **Remote Media Support**: Click this option to enable Remote Media Support.
- **Mount CD/DVD:** Click this option to enable mount CD/DVD feature.
- **Mount Harddisk:** Click this option to enable the mount hard disk feature.
- **Share Type for CD/DVD:** Select Share Type for CD/DVD (**NFS**, **CIFS**, **HTTP**)
- **Share Type for Harddisk:** Select Share Type for Hard Disk (**NFS**, **CIFS**)
- **Server Address for CD/DVD Images:** Server address where remote media images are stored.
- **Server Address for Harddisk Images:** Server address where remote media images are stored.
- **Path in server:** Source path to the remote media images.
- **Domain Name:** The Domain Name if CIFS share type is selected.
- **Username:** The Username if CIFS share type is selected.
- **Password:** The Password if CIFS share type is selected.
- **Same settings for Harddisk Images:** Check this option to use the same server information entered for CD/DVD media type for the Hard disk remote media settings..
- **Retry Interval:** The retry interval to reconnect RMedia.
- **Retry Count:** The retry count to reconnect RMedia.
- **Save:** Save the configured settings.

.

6.10.5.2 - VMedia Instance Settings

This page provides the ability to configure the Virtual Media Instance settings.



VMedia Instance Settings

Home > Settings > Media Redirection > VMedia Instance Settings

CD/DVD device instances: 1

Hard disk instances: 1

Remote KVM CD/DVD device instances: 1

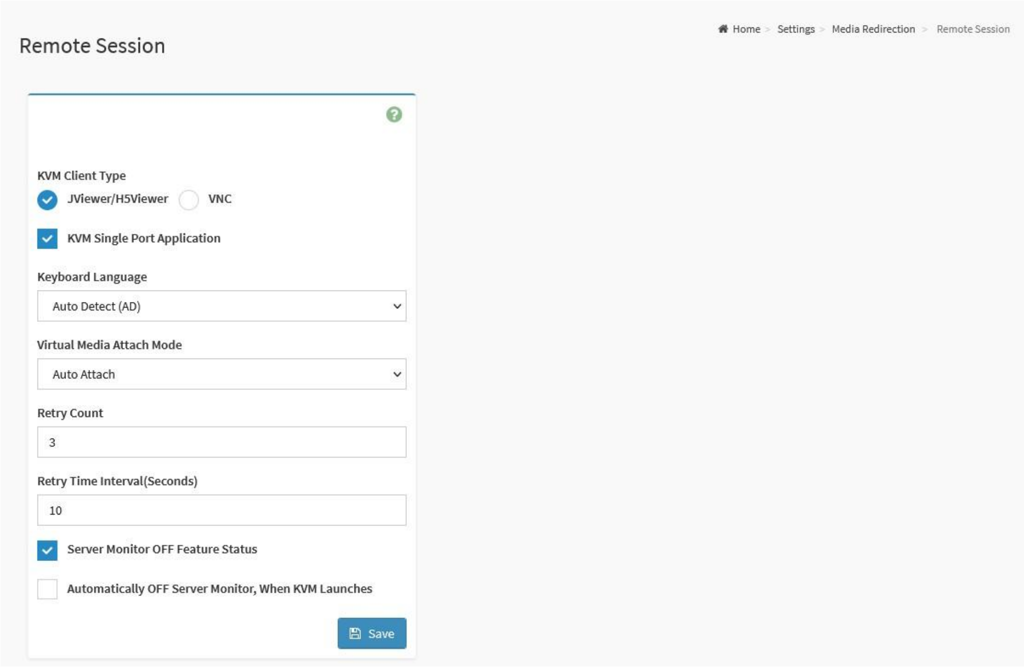
Remote KVM Hard disk instances: 1

Configurable Fields:

- **CD/DVD device instances:** The number of CD/DVD devices that are to be supported for Virtual Media redirection.
- **Hard disk instances:** The number of Hard disk devices to be supported for Virtual Media redirection.
- **Remote KVM CD/DVD device instances:** The number of Remote KVM CD/DVD devices that are to be supported for Virtual Media redirection
- **Remote KVM Hard disk instances:** The number of Remote KVM Hard disk devices to be supported for Virtual Media redirection.
- **Save:** Save the configured settings.

6.10.5.3 - Remote Session

This page provides the configuration settings for Remote Sessions.



Remote Session

Home > Settings > Media Redirection > Remote Session

KVM Client Type

● JViewer/H5Viewer ○ VNC

☑ KVM Single Port Application

Keyboard Language: Auto Detect (AD)

Virtual Media Attach Mode: Auto Attach

Retry Count: 3

Retry Time Interval(Seconds): 10

☑ Server Monitor OFF Feature Status

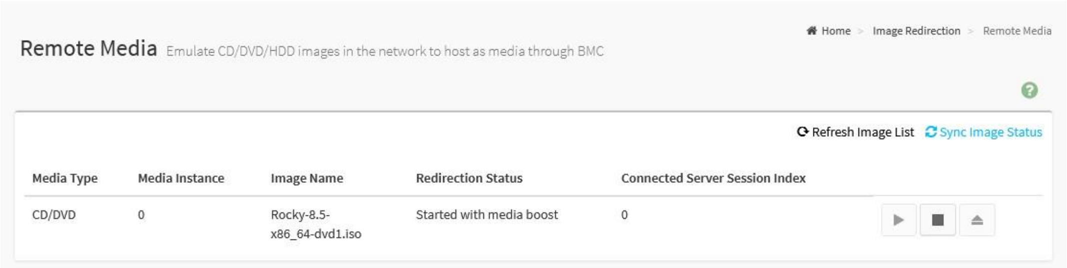
□ Automatically OFF Server Monitor, When KVM Launches

Configurable Fields:

- **KVM Client Type:** Select the KVM client type (JViewer/H5Viewer or VNC)
- **KVM Single Port Application:** Check this option to enable Single Port Application support
- **Keyboard Language:** The Keyboard Language.
- **Virtual Media Attach Mode:** The Virtual Media Attach Mode.
- **Retry Count :** Number of times to be retried when a KVM failure occurs. (Range: 1 to 20)
- **Retry Time Interval (Seconds):** Number of seconds to wait for subsequent retries. (Range 5 to 30)
- **Server Monitor OFF Feature Status:** Check this option to enable the Server Monitor OFF feature. Users can Lock or Unlock the local host monitor from the remote KVM window if this feature is enabled.
- **Automatically OFF Server Monitor, When KVM Launches:** Click this option to enable this feature.g
- **VNC Connection Types:** When VNC Connection is used, select **VNC over SSH** or **VNC on Stunnel**.
- **Save:** Save the configured settings.

6.10.5.4 - Active Redirections

This page provides settings for Remote Session configuration.



Remote Media Emulate CD/DVD/HDD images in the network to host as media through BMC

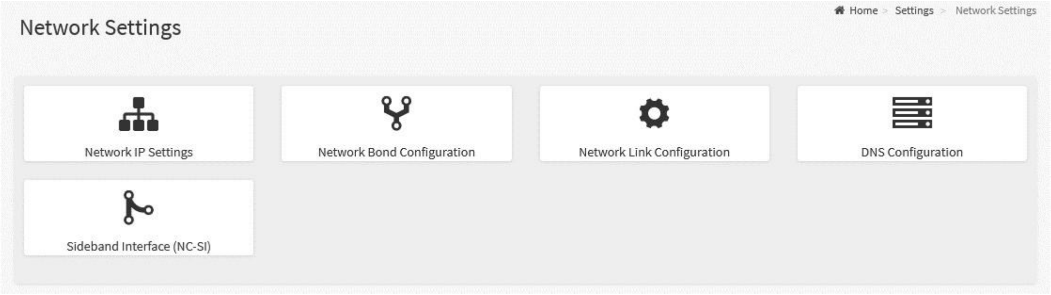
Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index	
CD/DVD	0	Rocky-8.5-x86_64-dvd1.iso	Started with media boost	0	▶ ■ ⏏

Configurable Fields:

- **Media Type:** The type Media devices supported for Active Redirections.
- **Media Instance:** The number of Media devices supported for Active Redirections.
- **Image Name:** The name of Media devices supported image for Active Redirections.
- **Redirection Status:** The Media redirections status.
- **Connected Server Session Index:** The number of connected server session index.
- **Play:** Click Play (▶) button to redirect the selected image.
- **Stop:** Click Stop (■) button to stop the remote image redirection.
- **Clear:** Click Clear (⏏) button to clear the selected image from the BMC.
- **Refresh Image List:** Click Refresh Image List (⟳) to get the latest list of Images from the Remote storage server.
- **Sync Image Status:** Click Sync Image Status (⟳) to Turn on/off the redirection status of Images from the BMC.

6.10.6 - Network Settings

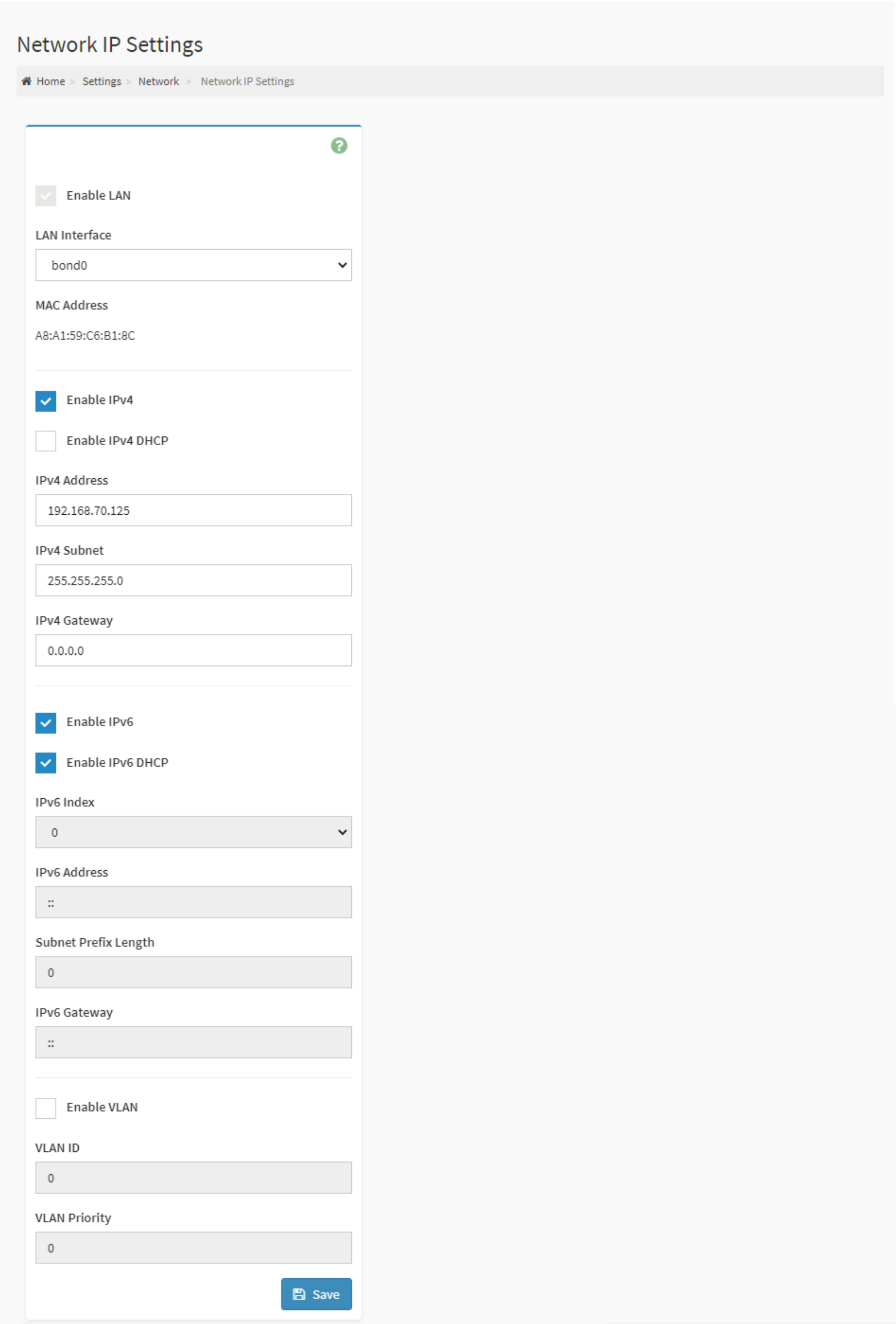
Network Settings page provides the ability to configure the network settings for the available BMC LAN channels (connections).


Network Settings
Home > Settings > Network Settings
Network IP Settings
Network Bond Configuration
Network Link Configuration
DNS Configuration
Sideband Interface (NC-SI)

The details of each Network Settings page are listed in the following subsections.

6.10.6.1 - Network IP Settings

This page provides the ability to configure the BCM’s Network IP Settings.



Network IP Settings

Home > Settings > Network > Network IP Settings

☑ Enable LAN

LAN Interface: bond0

MAC Address: A8:A1:59:C6:B1:8C

☑ Enable IPv4

□ Enable IPv4 DHCP

IPv4 Address: 192.168.70.125

IPv4 Subnet: 255.255.255.0

IPv4 Gateway: 0.0.0.0

☑ Enable IPv6

☑ Enable IPv6 DHCP

IPv6 Index: 0

IPv6 Address: ::

Subnet Prefix Length: 0

IPv6 Gateway: ::

□ Enable VLAN

VLAN ID: 0

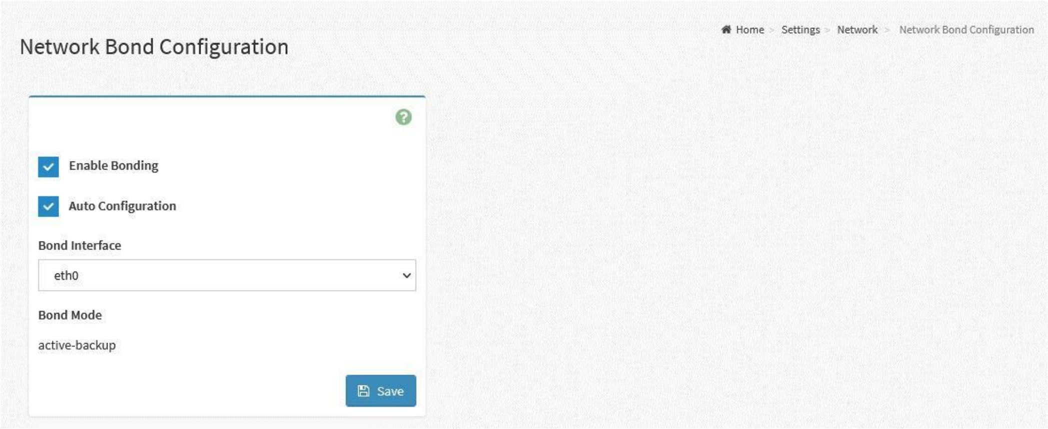
VLAN Priority: 0

Configurable Fields:

- **Enable LAN:** Click this option to 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:** Save the configured settings.

6.10.6.2 - Network Bond Configuration

This page provides the configurable settings for BMC Network Bonding.



Network Bond Configuration

Home > Settings > Network > Network Bond Configuration

☑ Enable Bonding

☑ Auto Configuration

Bond Interface: eth0

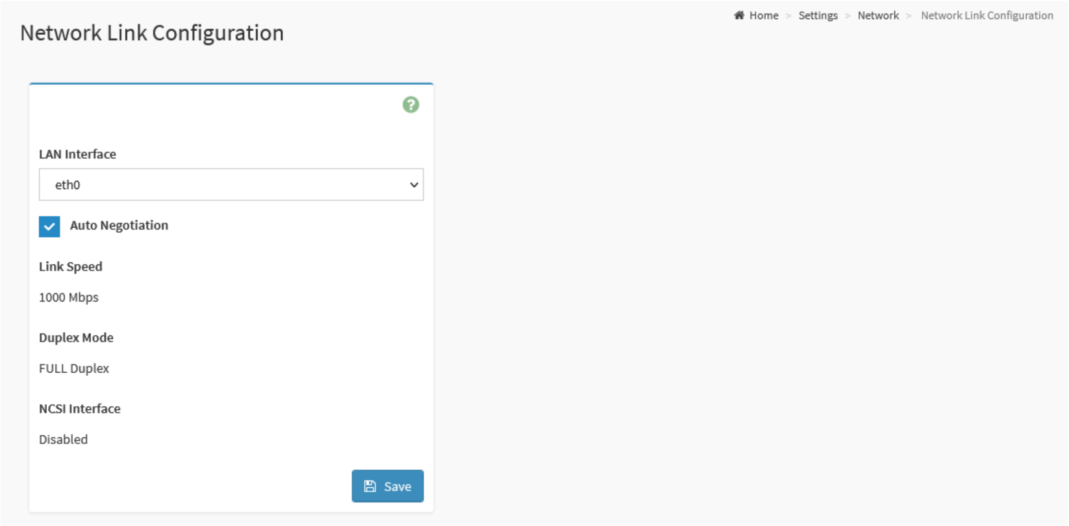
Bond Mode: active-backup

Configurable Fields:

- **Enable Bonding:** Check this option to enable bonding for the BMC network interfaces.
- **Auto Configuration:** Check this option to configure the interfaces automatically.
- **Bond Mode:** The current bonding BMC Network bonding mode in effect.
- **Save:** Save the configured settings.

6.10.6.3 Network Link Configuration

This page provides the ability to configure the BMC’s Network Link Configuration settings.



Network Link Configuration
Home > Settings > Network > Network Link Configuration
Save

LAN Interface
eth0

☑ Auto Negotiation

Link Speed
1000 Mbps

Duplex Mode
FULL Duplex

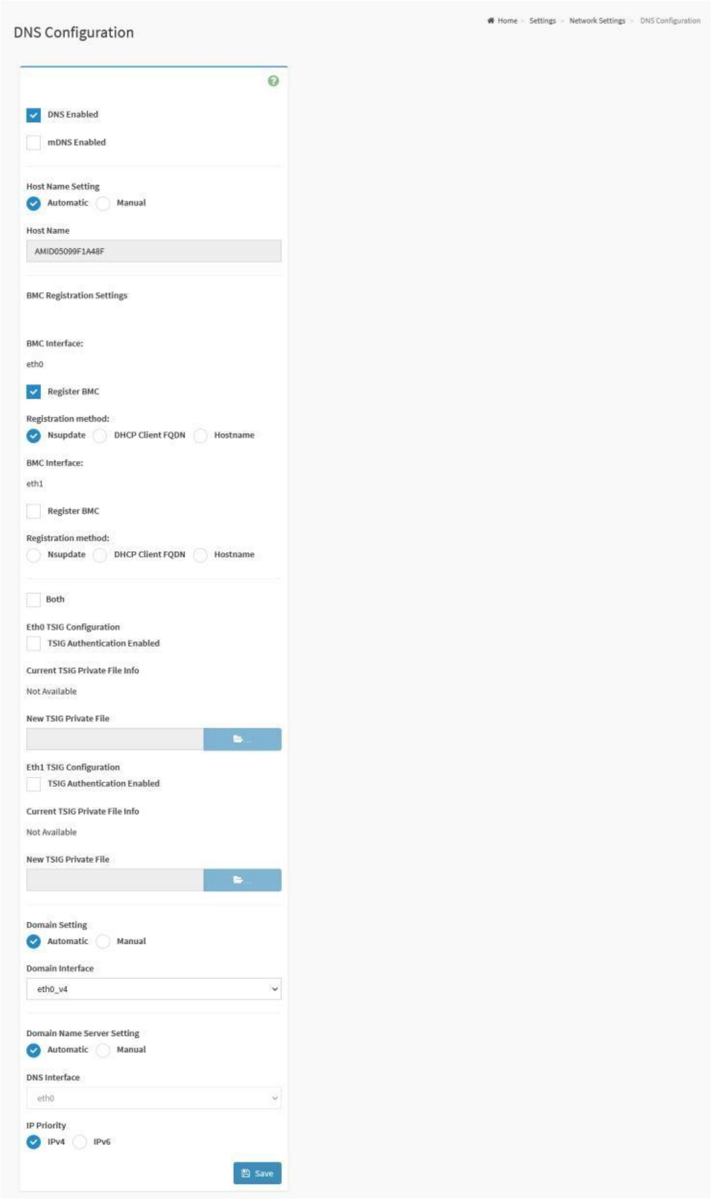
NCSI Interface
Disabled

Configurable Fields:

- **LAN Interface:** To select the network interface for which Link Speed and Duplex Mode are to be configured.
- **Auto Negotiation:** Click this option to enable the Auto Negotiation feature for the selected interface.
- **Link Speed:** Select the operated Link Speed from the drop menu.
- **Duplex Mode:** Select the operated Duplex Mode.
- **NCSI Interface**: Current NCSI interface status for the selected network interface.
- **Save:** Save the configured settings.

6.10.6.4 - DNS Configuration

This page provides the ability for users to configure the DNS Configuration settings should a Domain Name System (DNS) be used.



DNS Configuration

☑ DNS Enabled

□ mDNS Enabled

Host Name Setting

● Automatic ○ Manual

Host Name

AMID05099F1A48F

BMC Registration Settings

BMC Interface:

eth0

☑ Register BMC

Registration method:

● Nsupdate ○ DHCP Client FQDN ○ Hostname

BMC Interface:

eth1

□ Register BMC

Registration method:

○ Nsupdate ○ DHCP Client FQDN ○ Hostname

□ Both

Eth0 TSIG Configuration

□ TSIG Authentication Enabled

Current TSIG Private File Info

Not Available

New TSIG Private File

Eth1 TSIG Configuration

□ TSIG Authentication Enabled

Current TSIG Private File Info

Not Available

New TSIG Private File

Domain Setting

● Automatic ○ Manual

Domain Interface

eth0_v4

Domain Name Server Setting

● Automatic ○ Manual

DNS Interface

eth0

IP Priority

● IPv4 ○ IPv6

Configurable Fields:

- **DNS Enabled:** Check this option to enable all DNS services.
- **mDNS Enabled:** Check this option to enable Multicast DNS services.
- **Host Name Setting:**
    - Select either **Automatic** or **Manual** settings.
    - **Host Name:** If Host Name Settings is Manual, specify the host name.
- **BMC Registration Settings:**
    - **Register BMC:** Check the Interface (either bond0, eth0, eth1, or eth2) to Register
    - **Registration method:** For each interface, select the registration method
        - **Nsupdate:** Register with the DNS server using the nsupdate application.
        - **DHCP Client FQDN:** Register with the DNS server using DHCP option 81 (FQDN)
        - **Hostname:** Register with the DNS server using DHCP option 12 (Hostname)
- **TSIG Configuration:**
    - **TSIG Authentication Enabled:** Check this option to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
    - **Current TSIG Private File Info:** The information of Current TSIG private file along with its up-loaded date/time.
    - **New TSIG Private File:** Browse and navigate to the TSIG private file.
- **Domain Setting:** Select whether the domain interface is **Automatic** or is to be defined **Manually**. The configurable fields will adjust accordingly based on the selection.
    - When **Automatic** selected:
        - **Domain Interface:** Indicates the domain name of the device.
    - When **Manual** selected:
        - **Domain Name:** Input the domain name.
- **Domain Name Server Setting:** Select whether the domain interface is **Automatic** or is to be defined **Manually**. The configurable fields will adjust accordingly based on the selection.
    - When **Automatic** selected:
        - **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.
    - When **Manual** selected:
        - **DNS Server 1:** Specify the DNS Server 1 address to be configured for the BMC.
        - **DNS Server 2:** Specify the DNS Server 2 address to be configured for the BMC.
        - **DNS Server 3:** Specify the DNS Server 3 address to be configured for the BMC.

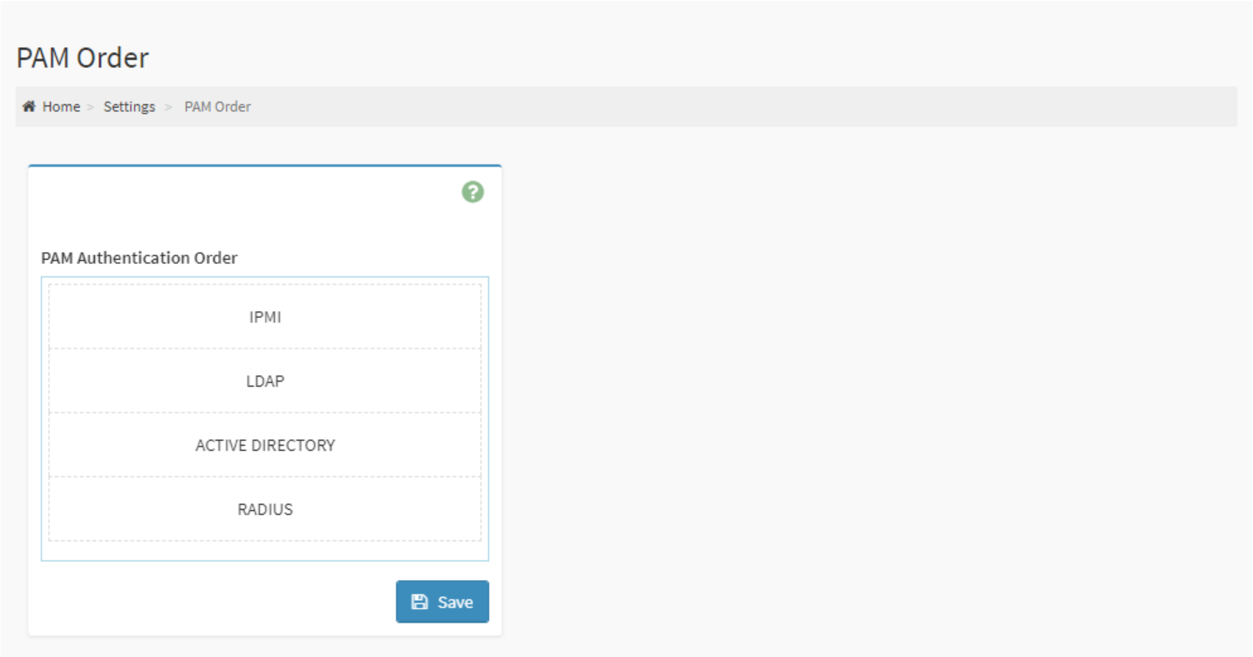
          Note: IPv4 and IPv6 address formats are supported.

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

6.10.7 - 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).

This page is used to configure the PAM order for user authentication into the BMC. It shows the list of PAM modules supported in the BMC. Drag and drop the PAM modules to change their position in the sequence.

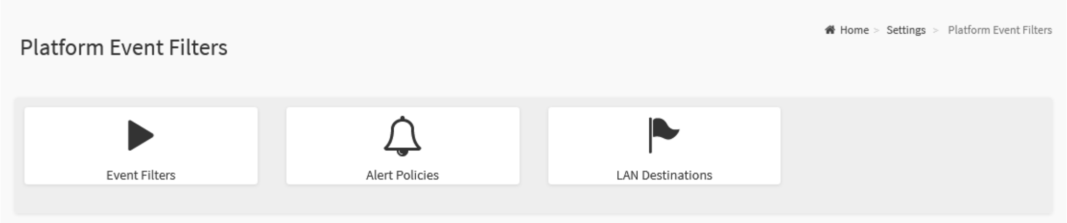


Configurable Fields:

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

6.10.8 - Platform Event Filters

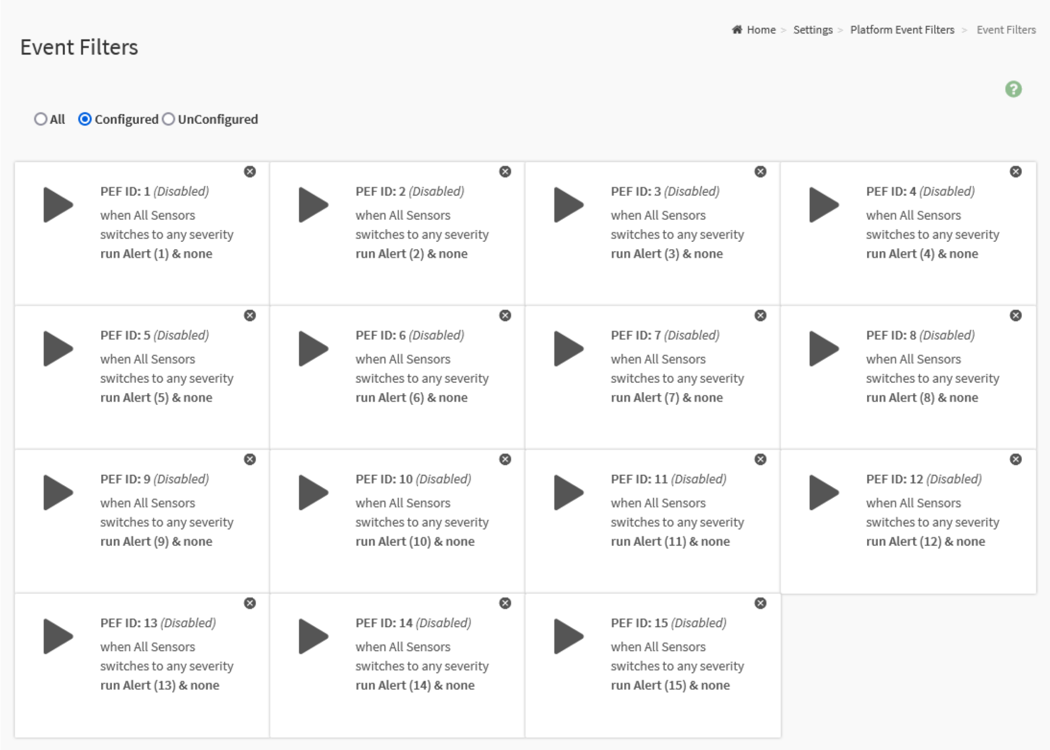
Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take an action based on an event it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.



The details of each Platform Event Filter page are listed in the following subsections.

6.10.8.1 - 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, or fan failure events.



Event Filters

Home > Settings > Platform Event Filters > Event Filters

○ All ● Configured ○ UnConfigured

PEF ID: 1 *(Disabled)* when All Sensors switches to any severity **run Alert (1) & none**

PEF ID: 2 *(Disabled)* when All Sensors switches to any severity **run Alert (2) & none**

PEF ID: 3 *(Disabled)* when All Sensors switches to any severity **run Alert (3) & none**

PEF ID: 4 *(Disabled)* when All Sensors switches to any severity **run Alert (4) & none**

PEF ID: 5 *(Disabled)* when All Sensors switches to any severity **run Alert (5) & none**

PEF ID: 6 *(Disabled)* when All Sensors switches to any severity **run Alert (6) & none**

PEF ID: 7 *(Disabled)* when All Sensors switches to any severity **run Alert (7) & none**

PEF ID: 8 *(Disabled)* when All Sensors switches to any severity **run Alert (8) & none**

PEF ID: 9 *(Disabled)* when All Sensors switches to any severity **run Alert (9) & none**

PEF ID: 10 *(Disabled)* when All Sensors switches to any severity **run Alert (10) & none**

PEF ID: 11 *(Disabled)* when All Sensors switches to any severity **run Alert (11) & none**

PEF ID: 12 *(Disabled)* when All Sensors switches to any severity **run Alert (12) & none**

PEF ID: 13 *(Disabled)* when All Sensors switches to any severity **run Alert (13) & none**

PEF ID: 14 *(Disabled)* when All Sensors switches to any severity **run Alert (14) & none**

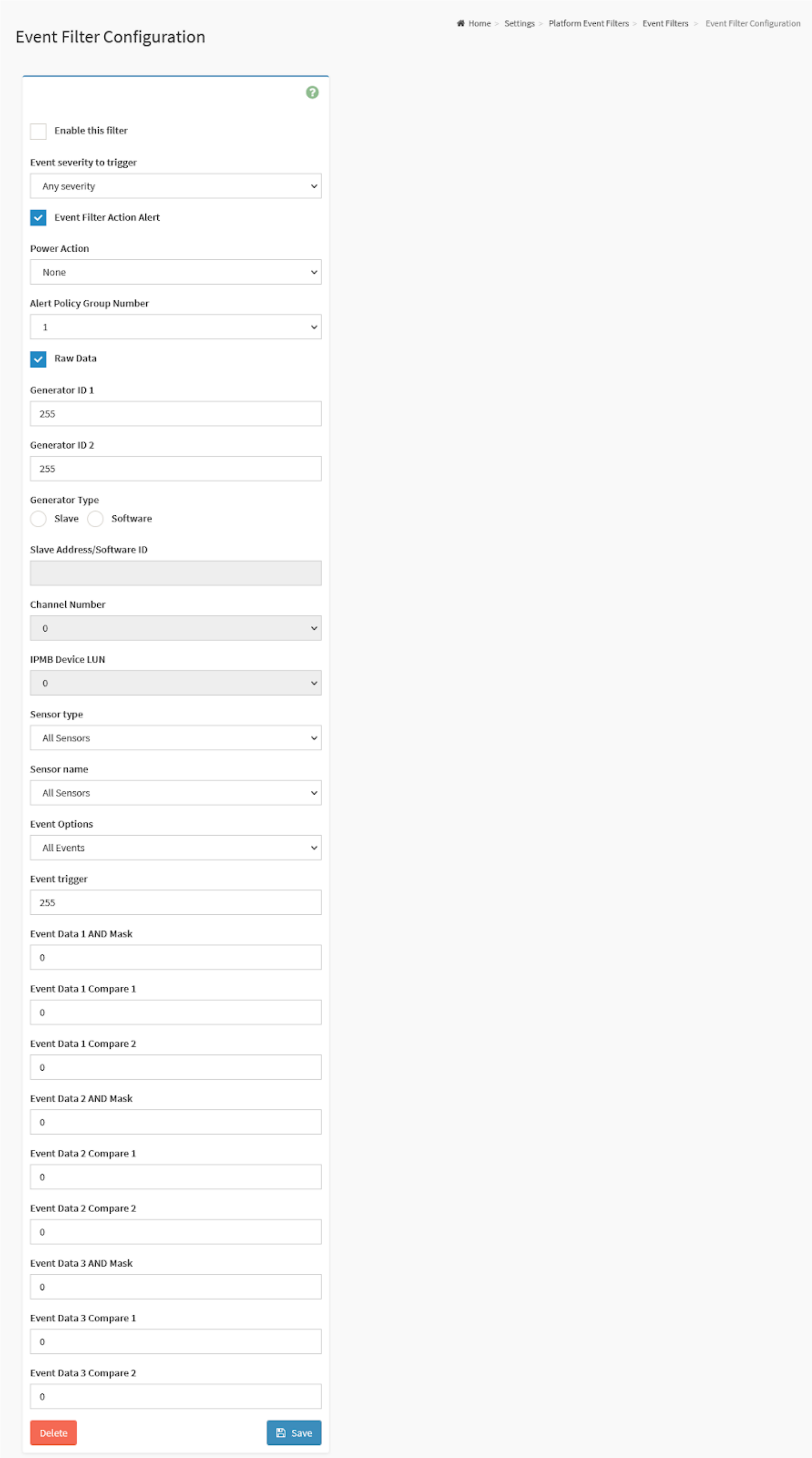
PEF ID: 15 *(Disabled)* when All Sensors switches to any severity **run Alert (15) & none**

The Platform Event Filters may be filtered using the following radio buttons:

- **All:** List all Platform Event Filters
- **Configured:** List only the Configured Platform Event Filters.
- **Unconfigured:** List only the Unconfigured Platform Event Filters.

To view the contents and parameters of a Platform Event Filter, select the icon (▶) to access the Event Filter Configuration page.

To Remove (unconfigure) the Platform Event Filter, select the Delete icon (⊗) on the top right corner of Platform Event Filter



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

Event Filter Configuration

□ Enable this filter

Event severity to trigger: Any severity

☑ Event Filter Action Alert

Power Action: None

Alert Policy Group Number: 1

☑ Raw Data

Generator ID 1: 255

Generator ID 2: 255

Generator Type: ○ Slave ○ Software

Slave Address/Software ID:

Channel Number: 0

IPMB Device LUN: 0

Sensor type: All Sensors

Sensor name: All Sensors

Event Options: All Events

Event trigger: 255

Event Data 1 AND Mask: 0

Event Data 1 Compare 1: 0

Event Data 1 Compare 2: 0

Event Data 2 AND Mask: 0

Event Data 2 Compare 1: 0

Event Data 2 Compare 2: 0

Event Data 3 AND Mask: 0

Event Data 3 Compare 1: 0

Event Data 3 Compare 2: 0

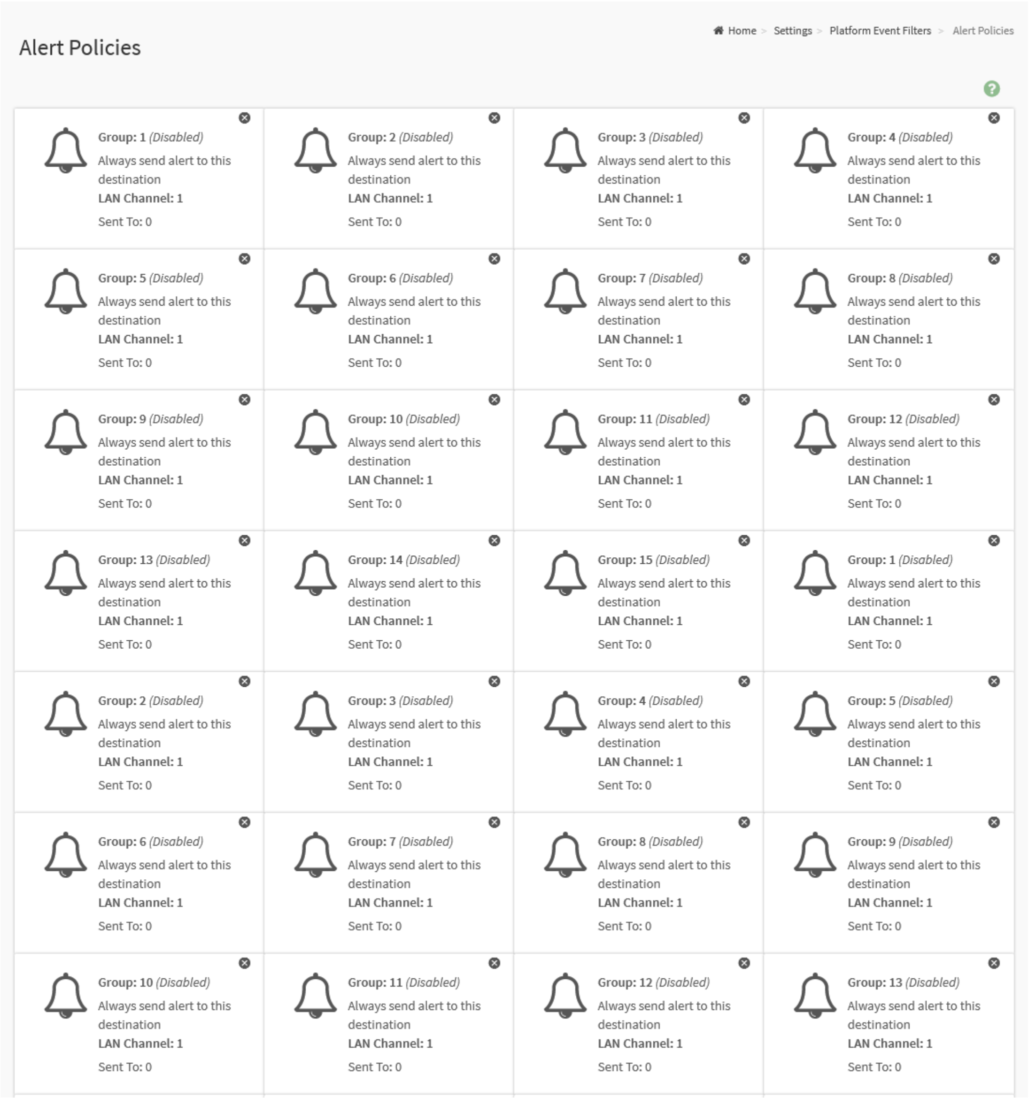
The configurable fields of each Platform Event Filter are listed below.

Configurable Fields (Platform Event Filter):

- **Enable this filter:** Check this option to enable the PEF settings.
- **Event severity to trigger:** Any one of the Event Severity from the drop-down list.
- **Event Filter Action Alert:** Check this option to enable PEF Alert action.
- **Power Action:** 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:** Check 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 the event was generated from IPMB.
    - **Software**: Select Software if the 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 BMC.
- **IPMB Device LUN:** Select the corresponding IPMB Device LUN if the event is generated by IPMB. (Not applicable for **Software** Generator type)
- **Sensor Type:** The type of sensor that will trigger the event filter action.
- **Sensor Name:** The particular sensor from the sensor list.
- **Event Options:** The 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:** Save the configured settings.

6.10.8.2 - Alert Policies

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



Alert Policies

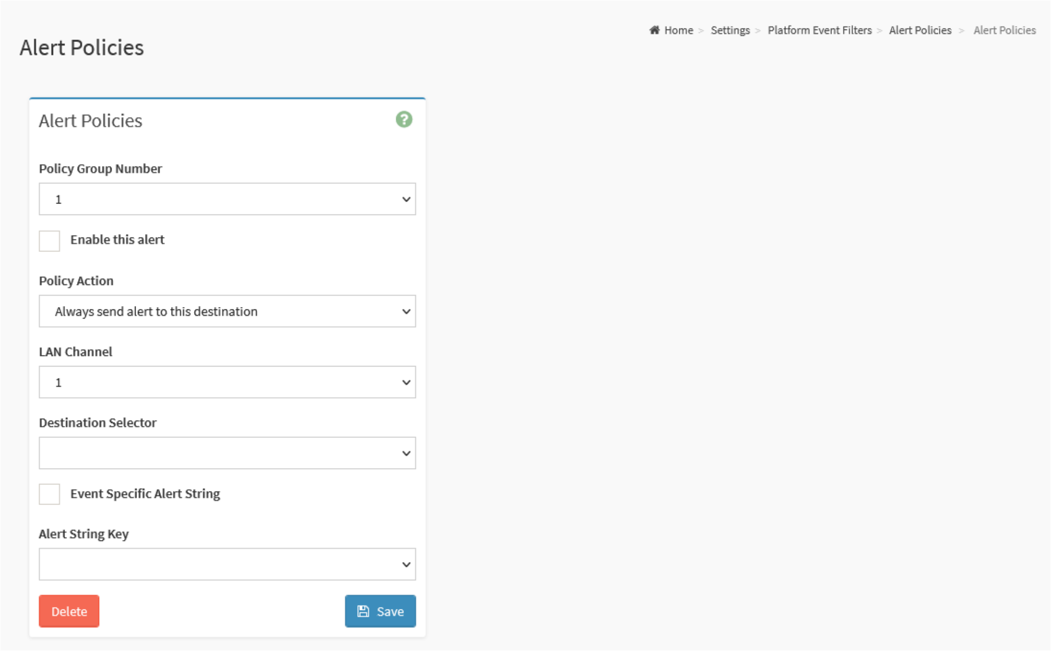
Home > Settings > Platform Event Filters > Alert Policies

Group: 1 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 2 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 3 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 4 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 5 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 6 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 7 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 8 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 9 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 10 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 11 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 12 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 13 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 14 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 15 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 1 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 2 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 3 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 4 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 5 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 6 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 7 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 8 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 9 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0
Group: 10 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 11 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 12 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0	**Group:** 13 *(Disabled)* Always send alert to this destination **LAN Channel: 1** Sent To: 0

To View/Edit the Alert Policy, click on the icon (🔔) to access the group's Alert Policy Configuration page.

Click on the Delete icon (⊗) on the top right corner of Alert Policy Slot to delete an Alert Policy from the list.

Editing an Alert Policy



Home > Settings > Platform Event Filters > Alert Policies > Alert Policies

Alert Policies

Alert Policies

Policy Group Number: 1

□ Enable this alert

Policy Action: Always send alert to this destination

LAN Channel: 1

Destination Selector:

□ Event Specific Alert String

Alert String Key:

Configurable Fields:

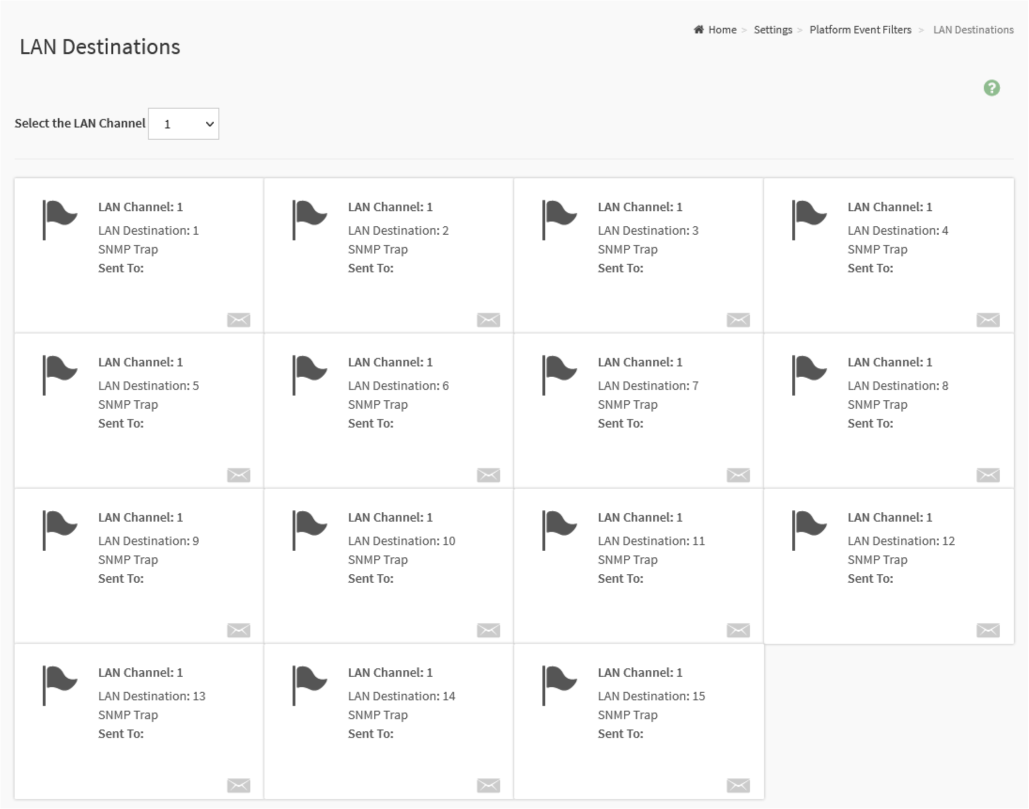
- **Policy Group Number:** Indicates the policy group number of the configuration.
- **Enable this alert:** Check this option to enable this alert policy.
- **Policy Action:** Select any one of the Policy Action sets from the list.
- **LAN Channel:** Select a particular channel from the available channel 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:** Delete the configured Alter Policy.
- **Save:** Save the configured settings.

6.10.8.3 - LAN Destinations

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



Home > Settings > Platform Event Filters > LAN Destinations

LAN Destinations

Select the LAN Channel 1

LAN Channel: 1
LAN Destination: 1
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 2
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 3
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 4
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 5
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 6
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 7
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 8
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 9
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 10
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 11
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 12
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 13
SNMP Trap
Sent To:

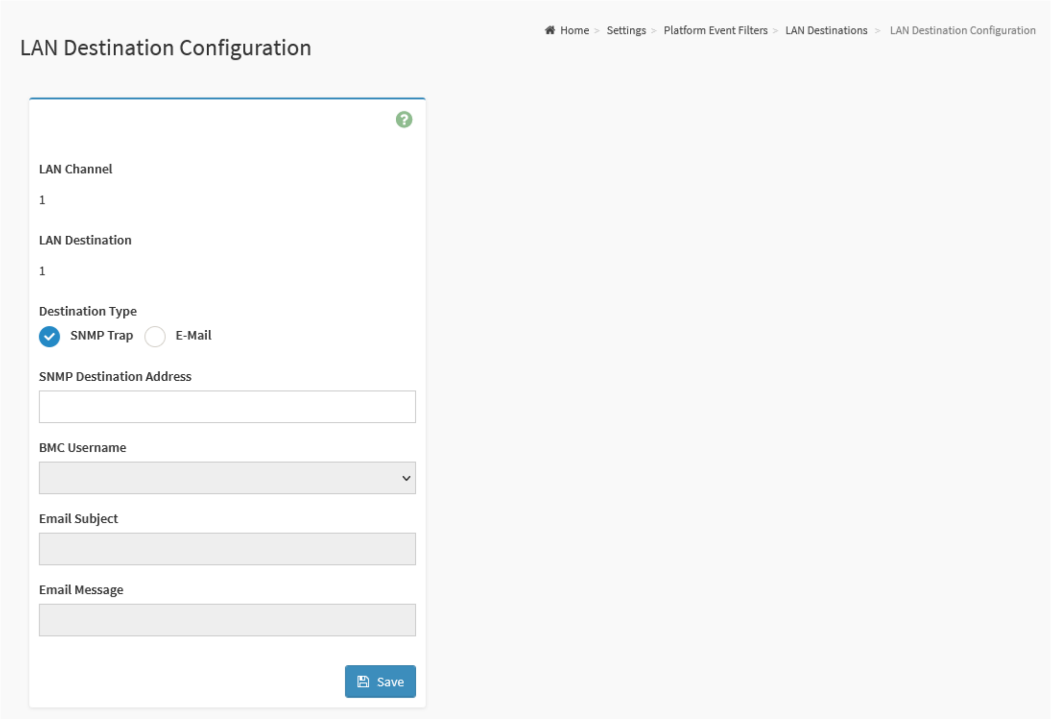
LAN Channel: 1
LAN Destination: 14
SNMP Trap
Sent To:

LAN Channel: 1
LAN Destination: 15
SNMP Trap
Sent To:

Configurable Fields:

- Select the LAN Channel: To select the LAN Channel number.
  - Select the LAN Destination Slot icon (⚑) then navigate to the LAN Destination Configuration page.
  - Select the Mail icon (✉) on the bottom right corner of LAN Destination Slot to send a test alert mail

LAN Destination Configuration Page



LAN Destination Configuration

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

LAN Channel

1

LAN Destination

1

Destination Type

● SNMP Trap ○ E-Mail

SNMP Destination Address

BMC Username

Email Subject

Email Message

Configurable Fields:

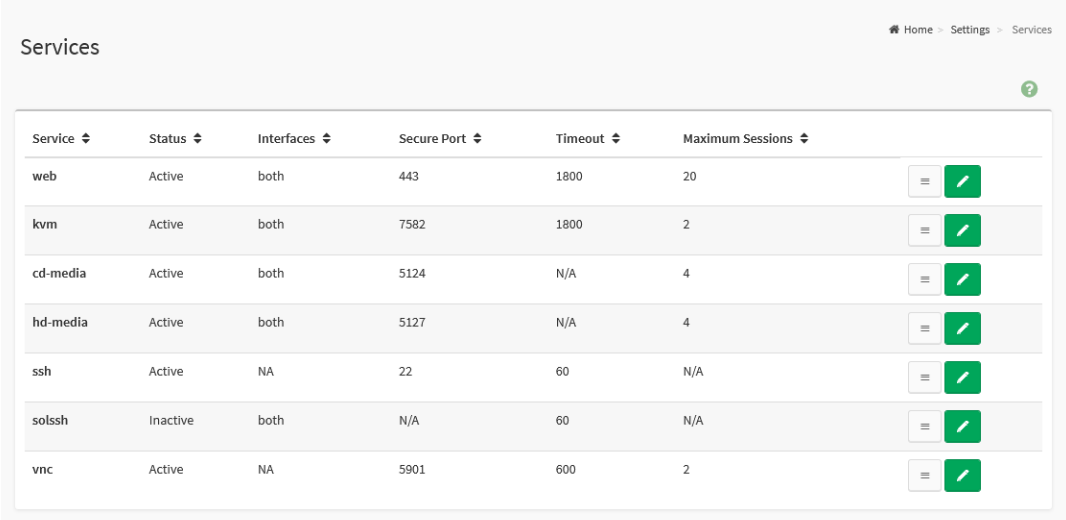
- **LAN Channel:** Indicates the LAN Channel Number of the selected slot
- **LAN Destination**: Indicates the Destination number of the selected slot
- **Destination Type:** Destination type can be either an SNMP Trap or an E- mail alert.
- **SNMP Trap:** If SNMP Trap is selected, then give the IP address 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 formats 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:** Save the configured settings.

6.10.9 - Services

This page provides the information about services running in the BMC. Only administrators can modify the service.



Services

Service	Status	Interfaces	Secure Port	Timeout	Maximum Sessions	
web	Active	both	443	1800	20	≡ ✎
kvm	Active	both	7582	1800	2	≡ ✎
cd-media	Active	both	5124	N/A	4	≡ ✎
hd-media	Active	both	5127	N/A	4	≡ ✎
ssh	Active	NA	22	60	N/A	≡ ✎
solssh	Inactive	both	N/A	60	N/A	≡ ✎
vnc	Active	NA	5901	600	2	≡ ✎

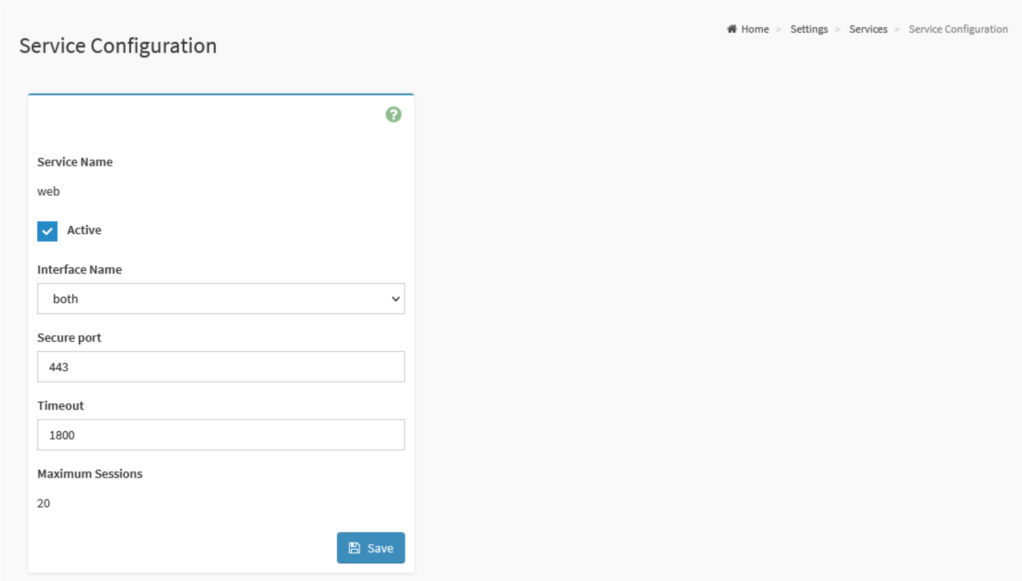
Configurable Fields:

- **Service:** Indicates the service name of the 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 the Service Configuration page to modify the services configuration.

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

Services Configuration Page



Service Configuration

Home > Settings > Services > Service Configuration

Service Name

web

☑ Active

Interface Name

both

Secure port

443

Timeout

1800

Maximum Sessions

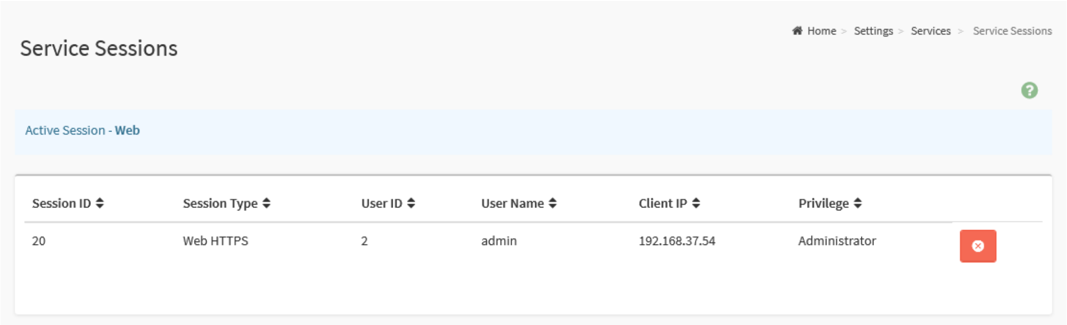
20

Save

Configurable Fields:

- **Service Name:** Indicates the name of the 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:** Save the configured settings

Services Sessions Page



Service Sessions

Home > Settings > Services > Service Sessions

Active Session - **Web**

Session ID	Session Type	User ID	User Name	Client IP	Privilege	
20	Web HTTPS	2	admin	192.168.37.54	Administrator	⊗

Configurable Fields:

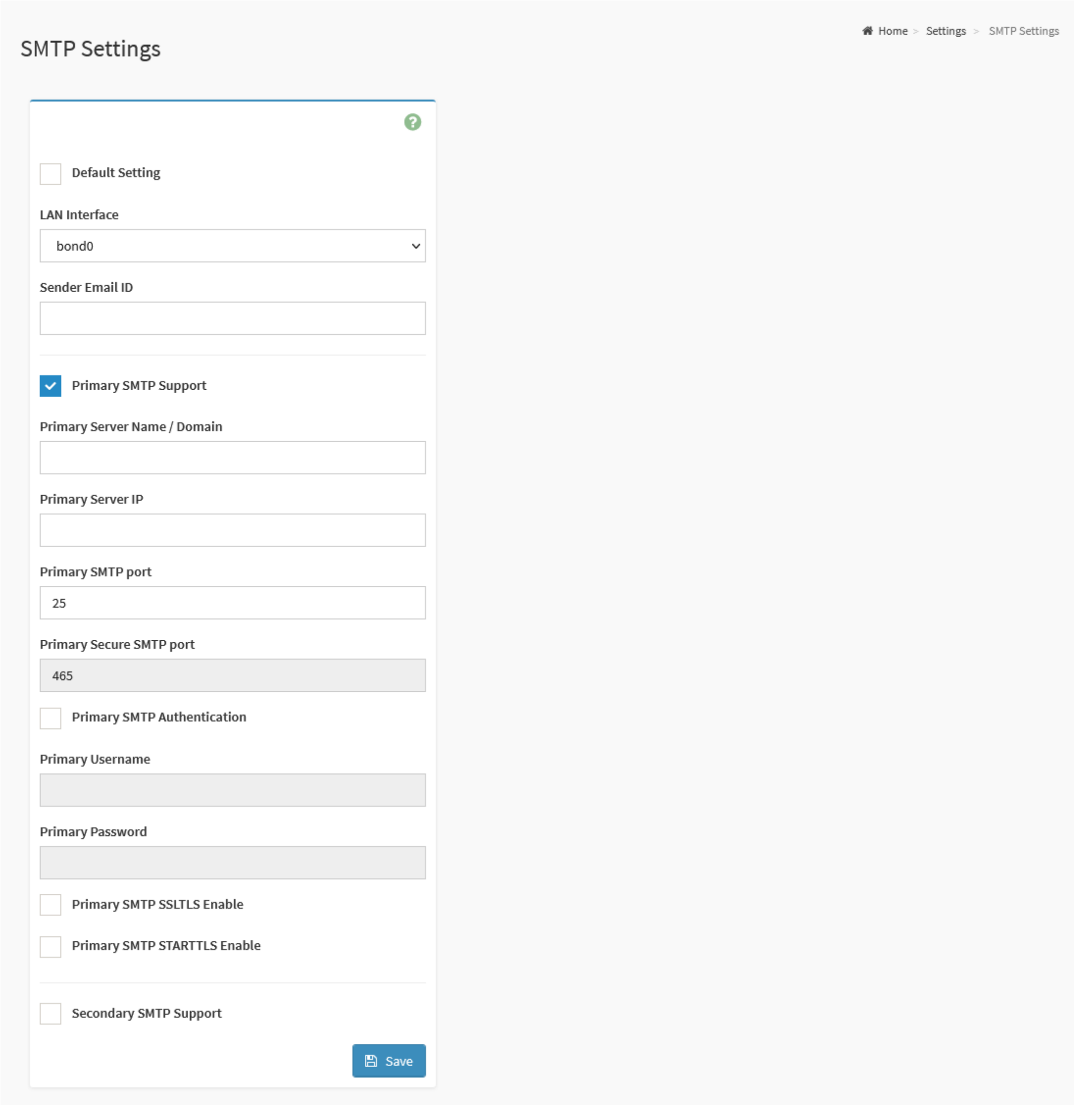
- **Session ID:** Indicates the ID number of this session.
- **Session Type:** Indicates the type of the active sessions.

- **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.

6.10.10 - SMTP Settings

Provides the ability for users to configure the SMTP settings of the device.



SMTP Settings

□ Default Setting

LAN Interface: bond0

Sender Email ID:

☑ Primary SMTP Support

Primary Server Name / Domain:

Primary Server IP:

Primary SMTP port: 25

Primary Secure SMTP port: 465

□ Primary SMTP Authentication

Primary Username:

Primary Password:

□ Primary SMTP SSLTLS Enable

□ Primary SMTP STARTTLS Enable

□ Secondary SMTP Support

Configurable Fields:

- **Default Setting:** Check this option to enable all parameters to 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.

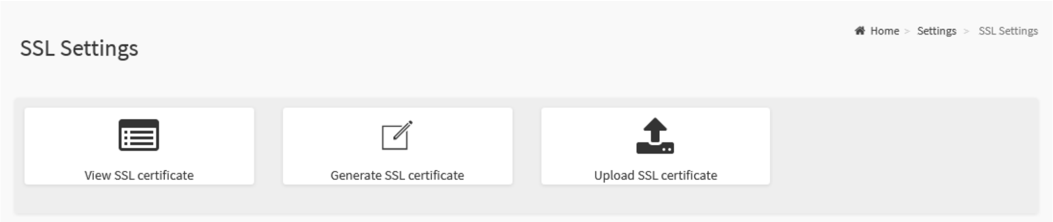
Primary and Secondary SMTP Support:

- **SMTP Support:** Check this option to enable SMTP support for the BMC.
- **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:** Check 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**: Check this option to enable the SMTP SSLTLS protocol.
- **SMTP STARTTLS Enable:** Check 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.

6.10.11 - SSL Settings

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

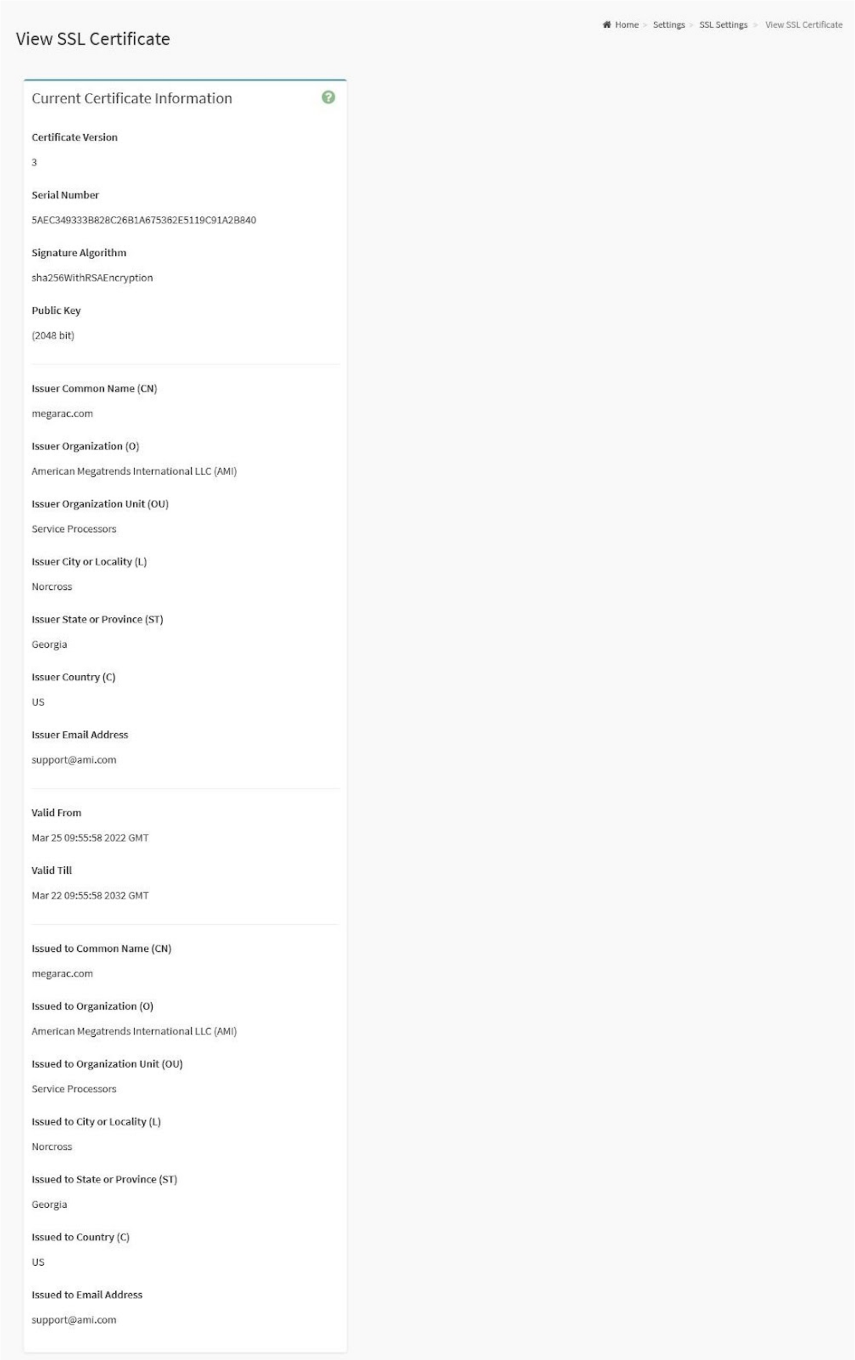
- View SSL Certificate
- Generate SSL Certificate
- Upload SSL Certificate



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

6.10.11.1 - View SSL Certificate

This page provides the information of current certificate information.



View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

5AEC349333B828C26B1A675362E5119C91A2B840

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

megarac.com

Issuer Organization (O)

American Megatrends International LLC (AMI)

Issuer Organization Unit (OU)

Service Processors

Issuer City or Locality (L)

Norcross

Issuer State or Province (ST)

Georgia

Issuer Country (C)

US

Issuer Email Address

support@ami.com

Valid From

Mar 25 09:55:58 2022 GMT

Valid Till

Mar 22 09:55:58 2032 GMT

Issued to Common Name (CN)

megarac.com

Issued to Organization (O)

American Megatrends International LLC (AMI)

Issued to Organization Unit (OU)

Service Processors

Issued to City or Locality (L)

Norcross

Issued to State or Province (ST)

Georgia

Issued to Country (C)

US

Issued to Email Address

support@ami.com

Informational Fields:

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:

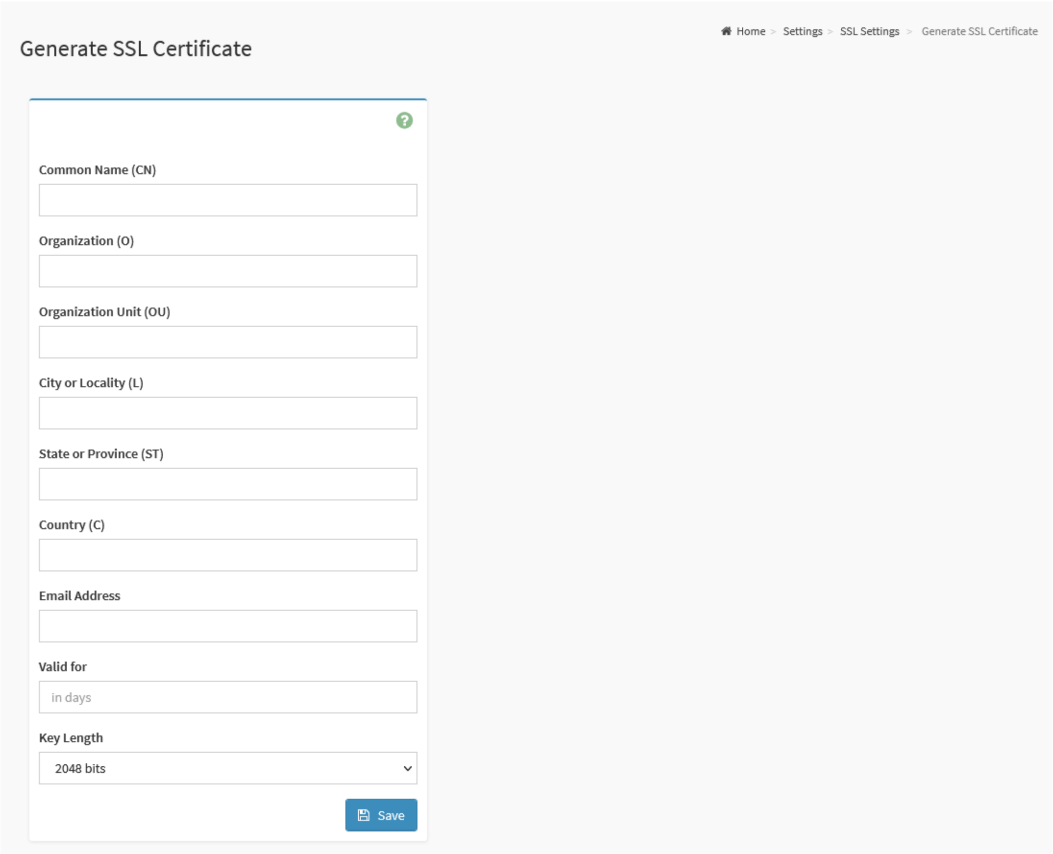
- Valid From
- Valid Till

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

6.10.11.2 - Generate SSL Certificate

This page provides the ability for users to generate SSL certificates through the BMC Web service.



Generate SSL Certificate

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for

in days

Key Length

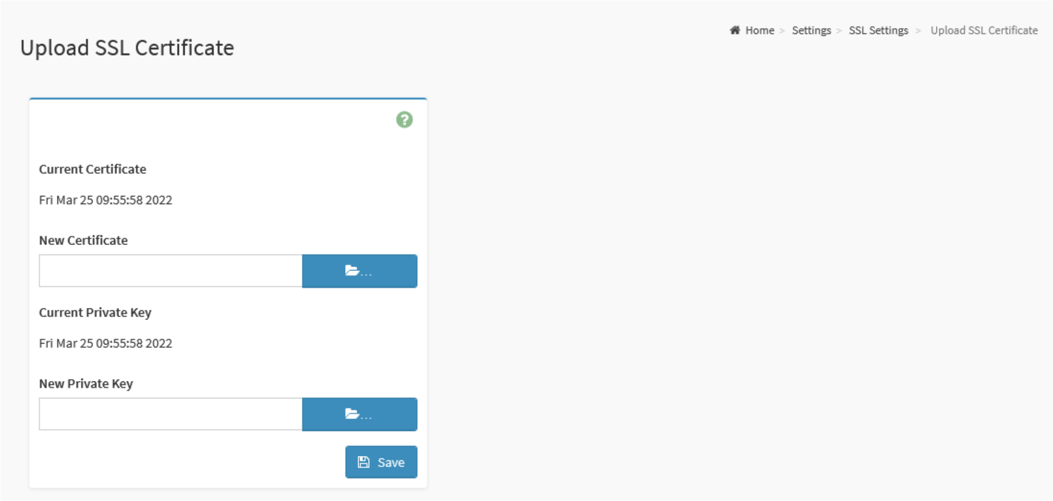
2048 bits

Configurable Fields:

- **Common Name (CN):** Specify the common name for which the certificate is to be generated.
- **Organization (O)**: Specify the name of the organization for which certificate is to be generated.
- **Organization Unit (OU):** Specify the Section or Unit of the organization for which certificate is to be generated.
- **City or Locality (L)**: Specify the City or Locality.
- **State or Province (ST):** Specify the State or Province.
- **Country (C):** Specify the Country code.
- **Email Address:** 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:** Save the configured settings.

6.10.11.3 - Upload SSL Certificate

This page provides the ability for users to upload the new SSL Certificate file into the BMC to replace the old one.



Upload SSL Certificate

Current Certificate

Fri Mar 25 09:55:58 2022

New Certificate

Current Private Key

Fri Mar 25 09:55:58 2022

New Private Key

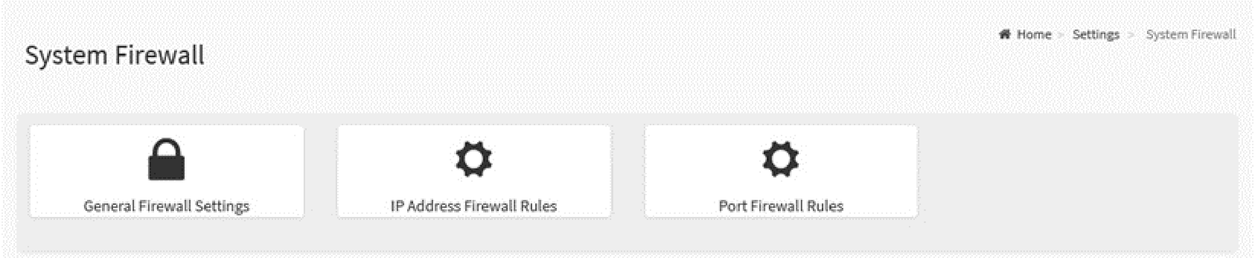
Configurable Fields:

- **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:** Save the configured settings.

6.10.12 - System Firewall

System Firewall page provides the feature tabs for users to configure the firewall settings:

- General Firewall Settings
- IP Firewall Rules
- Port Firewall Rules

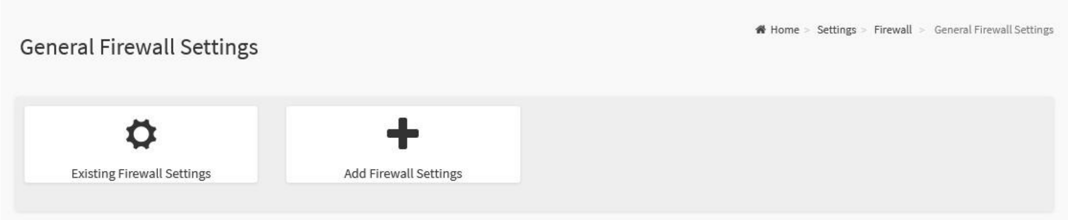

System Firewall
Home > Settings > System Firewall
General Firewall Settings
IP Address Firewall Rules
Port Firewall Rules

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

6.10.12.1 - General Firewall Settings

This page provides the following functional feature tabs for users to configure the General Firewall Settings and monitor the configured settings:

- Existing Firewall Settings
- Add Firewall Settings

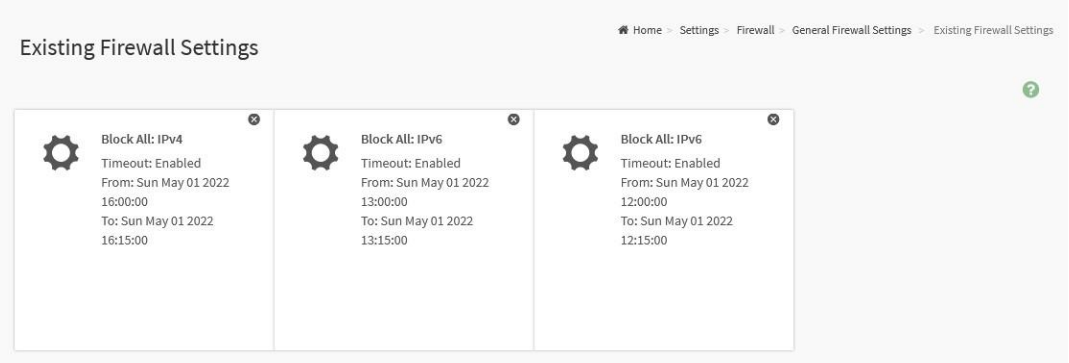

General Firewall Settings
Home > Settings > Firewall > General Firewall Settings
Existing Firewall Settings
Add Firewall Settings

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

6.10.12.1.1 - Existing Firewall Settings

This page lists all configured General Firewall Settings instances.

A blank page will be opened if users did not add any General Firewall Settings instance from **Add Firewall Settings** page



Existing Firewall Settings

Home > Settings > Firewall > General Firewall Settings > Existing Firewall Settings

Block All: IPv4
Timeout: Enabled
From: Sun May 01 2022 16:00:00
To: Sun May 01 2022 16:15:00

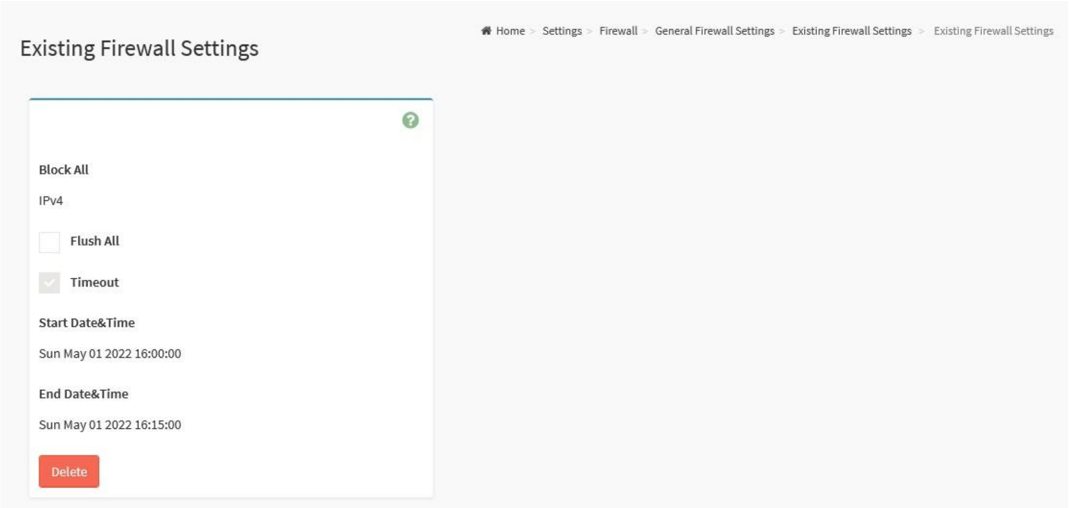
Block All: IPv6
Timeout: Enabled
From: Sun May 01 2022 13:00:00
To: Sun May 01 2022 13:15:00

Block All: IPv6
Timeout: Enabled
From: Sun May 01 2022 12:00:00
To: Sun May 01 2022 12:15:00

Click on the Slot icon (⚙) then navigate to the instance page.

Click on the Delete icon (⊗) then delete this firewall instance.

Instance Page:



Existing Firewall Settings

Home > Settings > Firewall > General Firewall Settings > Existing Firewall Settings > Existing Firewall Settings

Block All

IPv4

□ Flush All

☑ Timeout

Start Date&Time

Sun May 01 2022 16:00:00

End Date&Time

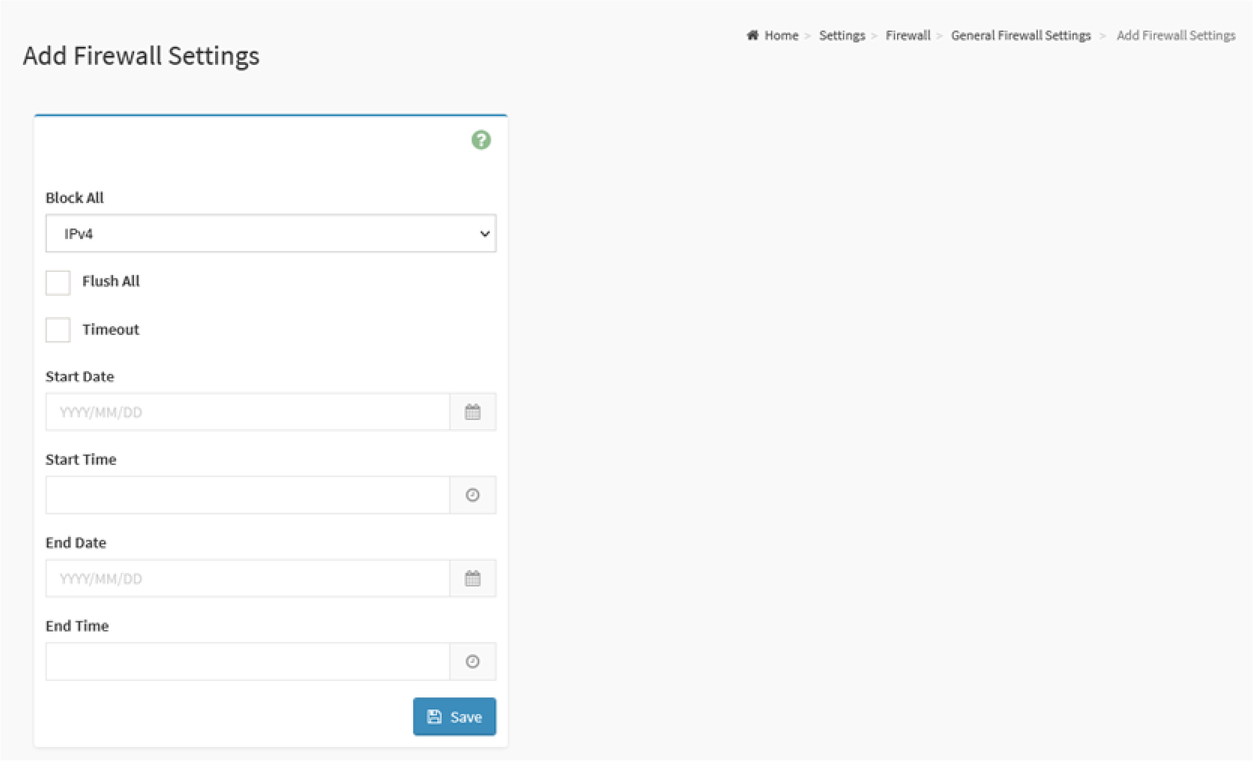
Sun May 01 2022 16:15:00

Configurable/Informational Fields:

- **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 a 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.

6.10.12.1.2 - Add Firewall Settings

This page provides the ability for users to add General Firewall Setting instances.



Add Firewall Settings

Home > Settings > Firewall > General Firewall Settings > Add Firewall Settings

Block All: IPv4

□ Flush All

□ Timeout

Start Date: YYYY/MM/DD

Start Time:

End Date: YYYY/MM/DD

End Time:

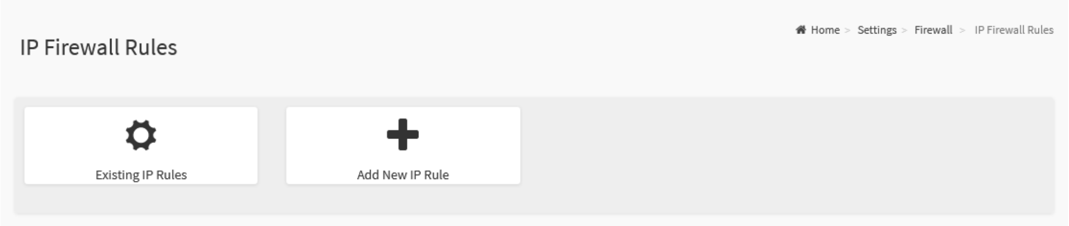
The fields on the Add Firmware Settings page include

- **Block All:** Select the protocol and block all the incoming IPs and Ports.
- **Flush All:** To flush all the system firewall settings.
- **Timeout:** Check this option to enable or disable firewall rules with timeout.
- **Start Date:** To specify a Start Date to start the respective firewall rule effect from the date.
- **Start Time:** To specify a Start Time to start the 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 an End Time to End respective firewall rule effect from the Time.
- **Save:** Save the configured settings.

6.10.12.2 - IP Firewall Rules

This page provides the ability for users to configure the IP Firewall Rules and monitor the configured settings for:

- Existing IP Rules
- Add New IP Rule

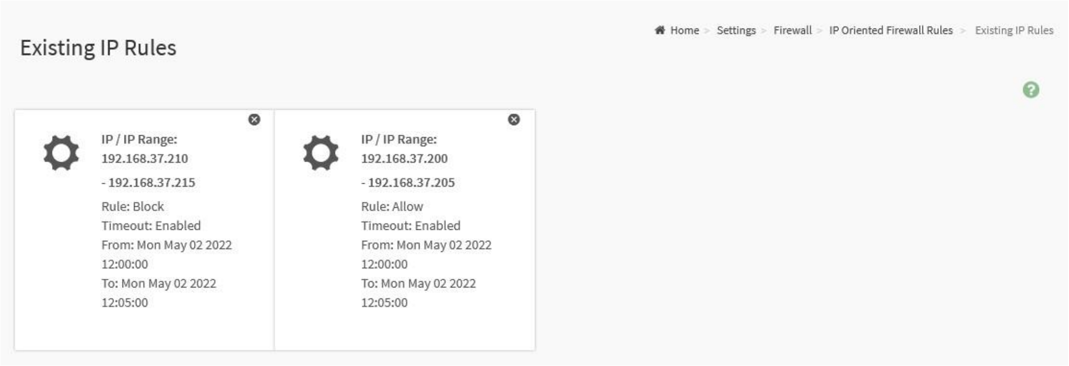


The details about each feature are listed in the following subsections.

6.10.12.2.1 - Existing IP Rules

This page lists all configured IP Firewall Rules instances.

A blank page will be opened if users did previously add any IP Firewall Rules instances from the Add New IP Rule page.

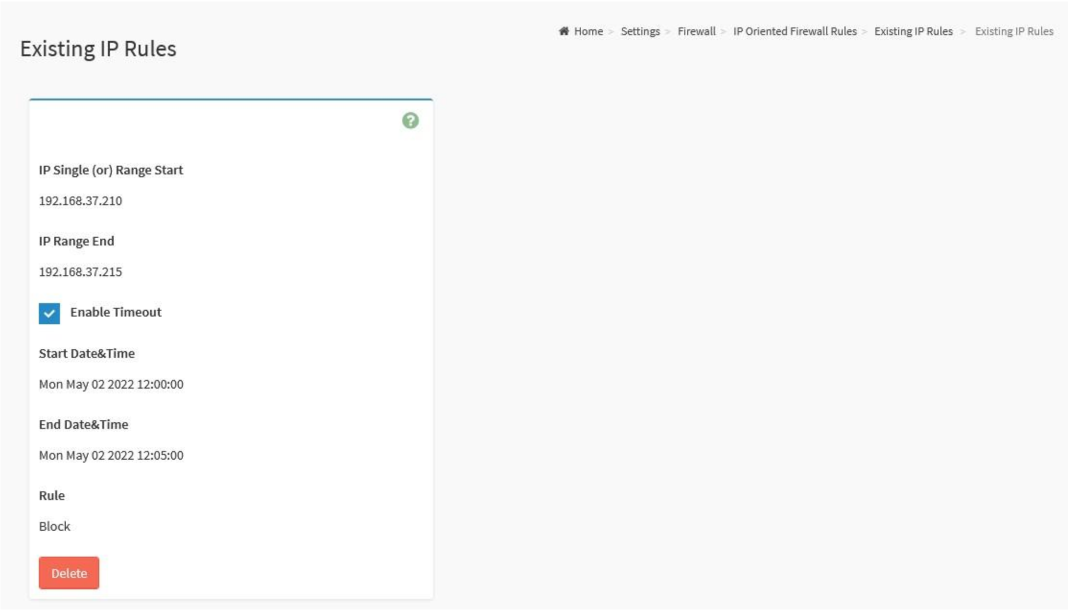

Existing IP Rules
Home > Settings > Firewall > IP Oriented Firewall Rules > Existing IP Rules

IP / IP Range:
192.168.37.210
- 192.168.37.215
Rule: Block
Timeout: Enabled
From: Mon May 02 2022
12:00:00
To: Mon May 02 2022
12:05:00

IP / IP Range:
192.168.37.200
- 192.168.37.205
Rule: Allow
Timeout: Enabled
From: Mon May 02 2022
12:00:00
To: Mon May 02 2022
12:05:00

Click on the Slot icon (⚙) then navigate to the instance page.

Click on the Delete icon (⊗) then delete the instance.


Home > Settings > Firewall > IP Oriented Firewall Rules > Existing IP Rules > Existing IP Rules

Existing IP Rules

IP Single (or) Range Start

192.168.37.210

IP Range End

192.168.37.215

☑ Enable Timeout

Start Date&Time

Mon May 02 2022 12:00:00

End Date&Time

Mon May 02 2022 12:05:00

Rule

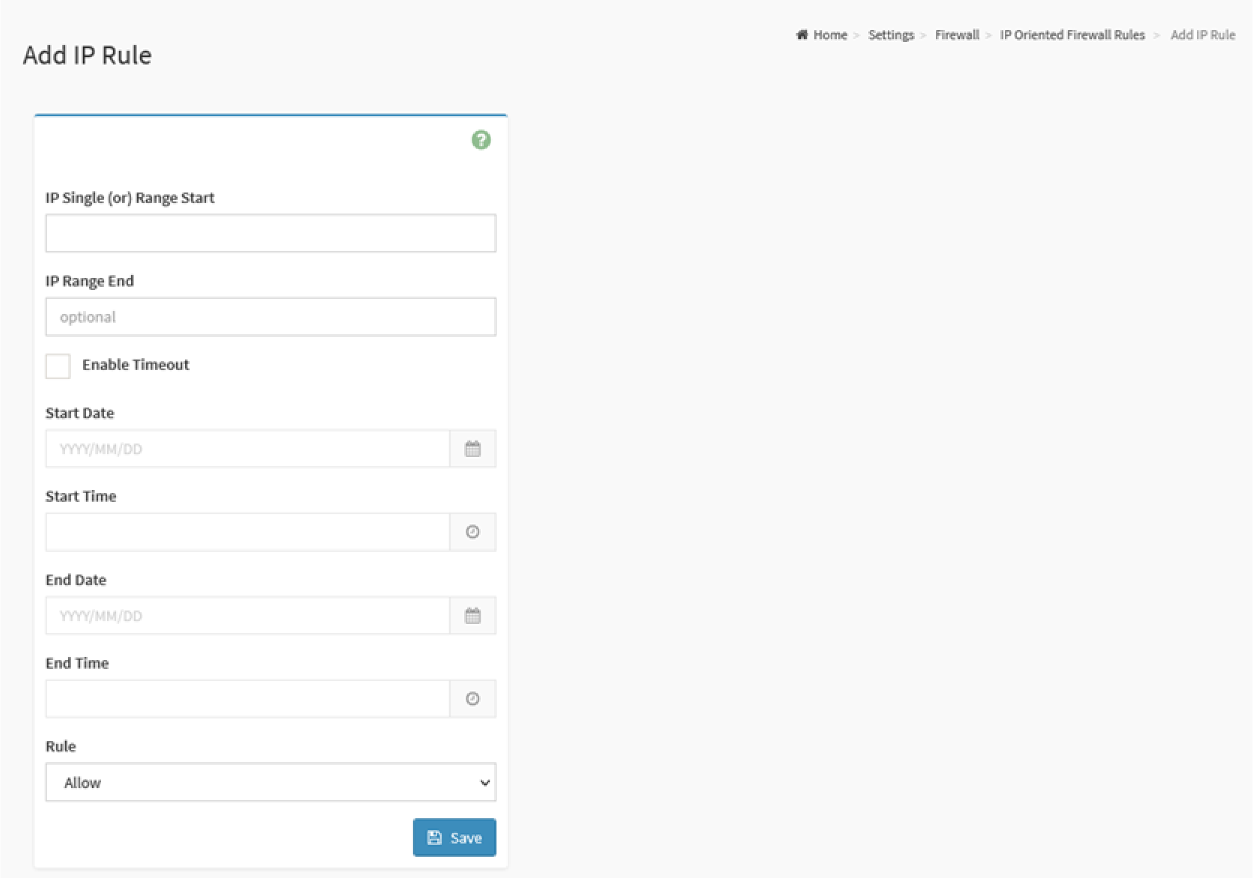
Block

Configurable/Information Fields:

- **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 with timeout feature enabled.
- **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.

6.10.12.2.2 - Add New IP Rule

This page provides the ability for users to add IP Firewall Rule instances.



Add IP Rule

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

IP Single (or) Range Start

IP Range End

optional

□ Enable Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

YYYY/MM/DD

End Time

Rule

Allow

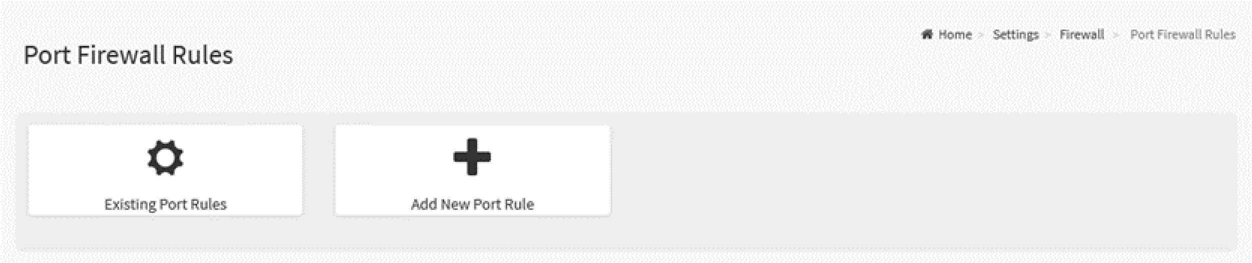
Configurable Fields:

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

6.10.12.3 - Port Firewall Rules

This page provides the ability for users to configure the Port Firewall Rules and monitor the configured settings such as:

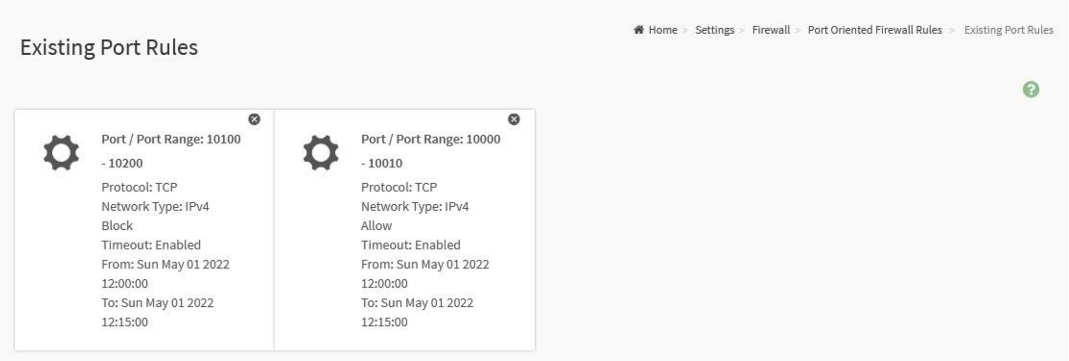
- Existing Port Rules
- Add New Port Rule



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

6.10.12.3.1 - Existing Port Rules

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

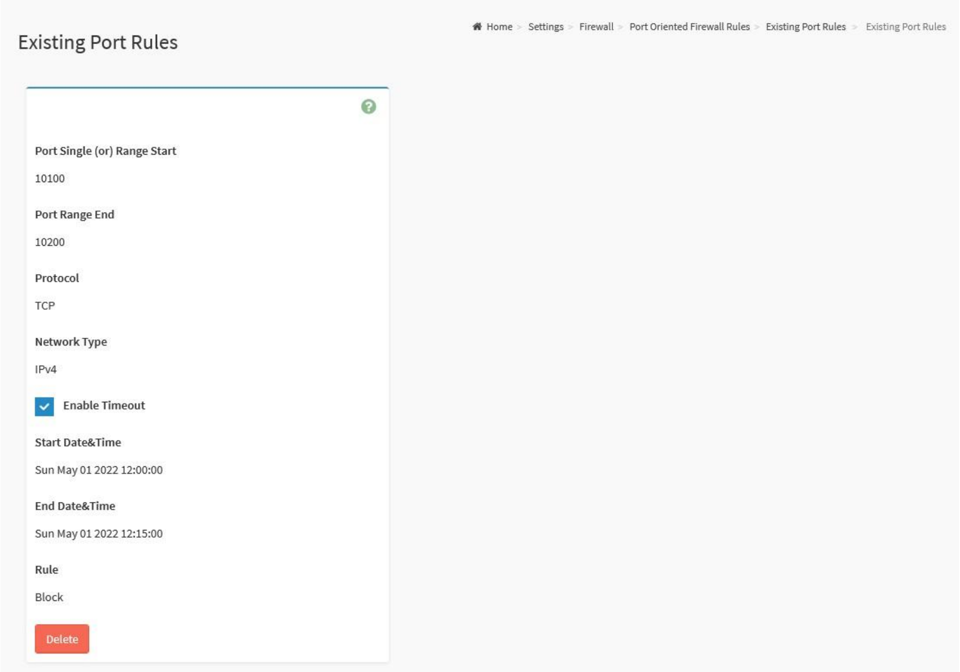

Existing Port Rules
Home > Settings > Firewall > Port Oriented Firewall Rules > Existing Port Rules

Port / Port Range: 10100 - 10200
Protocol: TCP
Network Type: IPv4
Block
Timeout: Enabled
From: Sun May 01 2022 12:00:00
To: Sun May 01 2022 12:15:00

Port / Port Range: 10000 - 10010
Protocol: TCP
Network Type: IPv4
Allow
Timeout: Enabled
From: Sun May 01 2022 12:00:00
To: Sun May 01 2022 12:15:00

Click on the Slot icon (⚙) then navigate to the instance page.

Click on the Delete icon (☒) to delete the instance.


Existing Port Rules
Home > Settings > Firewall > Port Oriented Firewall Rules > Existing Port Rules > Existing Port Rules

Port Single (or) Range Start
10100

Port Range End
10200

Protocol
TCP

Network Type
IPv4

☑ Enable Timeout

Start Date&Time
Sun May 01 2022 12:00:00

End Date&Time
Sun May 01 2022 12:15:00

Rule
Block

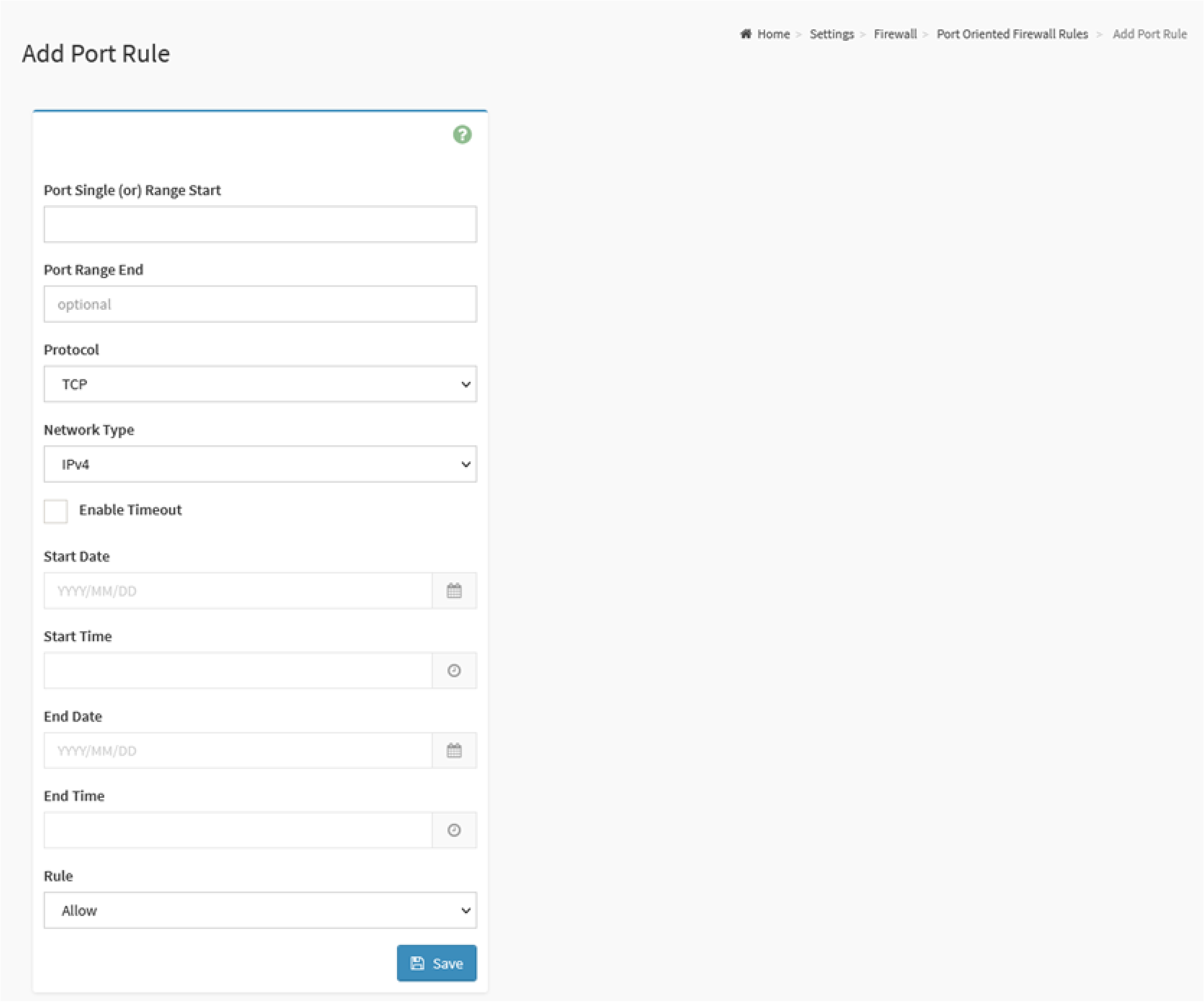
Informational Fields:

- **Port Single (or) Range Start:** This field indicates the port number or the start of range or port numbers.
- **Port Range End:** Indicates the end of range or port numbers.
- **Protocol:** Indicates the protocols for the configured port or range or ports.

- **Network Type:** 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:** Indicates Allow or Block status.
- **Delete:** Click this button to delete this instance.

6.10.12.3.2 - Add New Port Rule

This page provides the ability for users to add Port Firewall Rule instances.


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

Port Single (or) Range Start

Port Range End: optional

Protocol: TCP

Network Type: IPv4

□ Enable Timeout

Start Date: YYYY/MM/DD

Start Time

End Date: YYYY/MM/DD

End Time

Rule: Allow

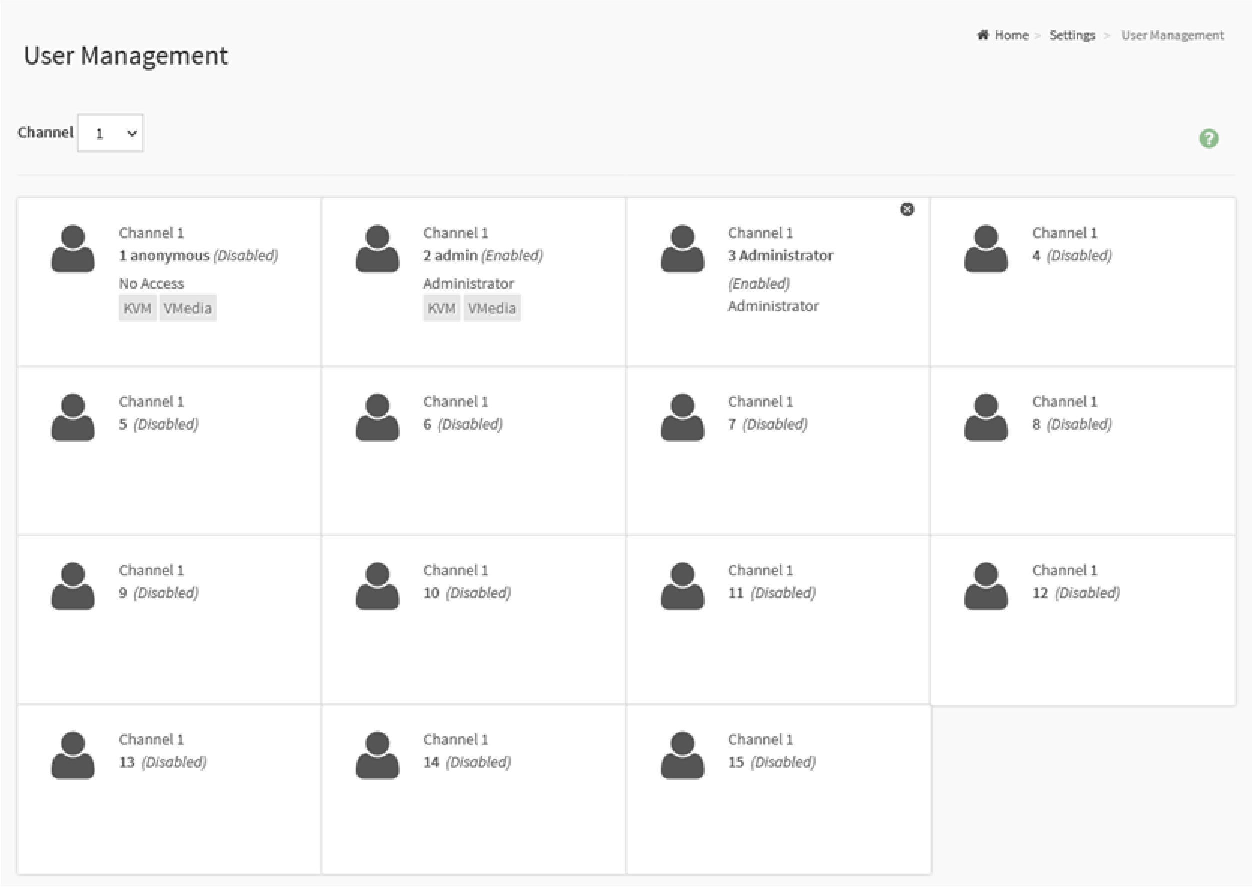
Configurable Fields:

- **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 enable 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:** Save the configured settings.

6.10.13 - User Management

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



User Management

Home > Settings > User Management

Channel 1

Channel 1 1 anonymous *(Disabled)* No Access KVM VMedia	Channel 1 2 admin *(Enabled)* Administrator KVM VMedia	Channel 1 3 Administrator *(Enabled)* Administrator	Channel 1 4 *(Disabled)*
Channel 1 5 *(Disabled)*	Channel 1 6 *(Disabled)*	Channel 1 7 *(Disabled)*	Channel 1 8 *(Disabled)*
Channel 1 9 *(Disabled)*	Channel 1 10 *(Disabled)*	Channel 1 11 *(Disabled)*	Channel 1 12 *(Disabled)*
Channel 1 13 *(Disabled)*	Channel 1 14 *(Disabled)*	Channel 1 15 *(Disabled)*	

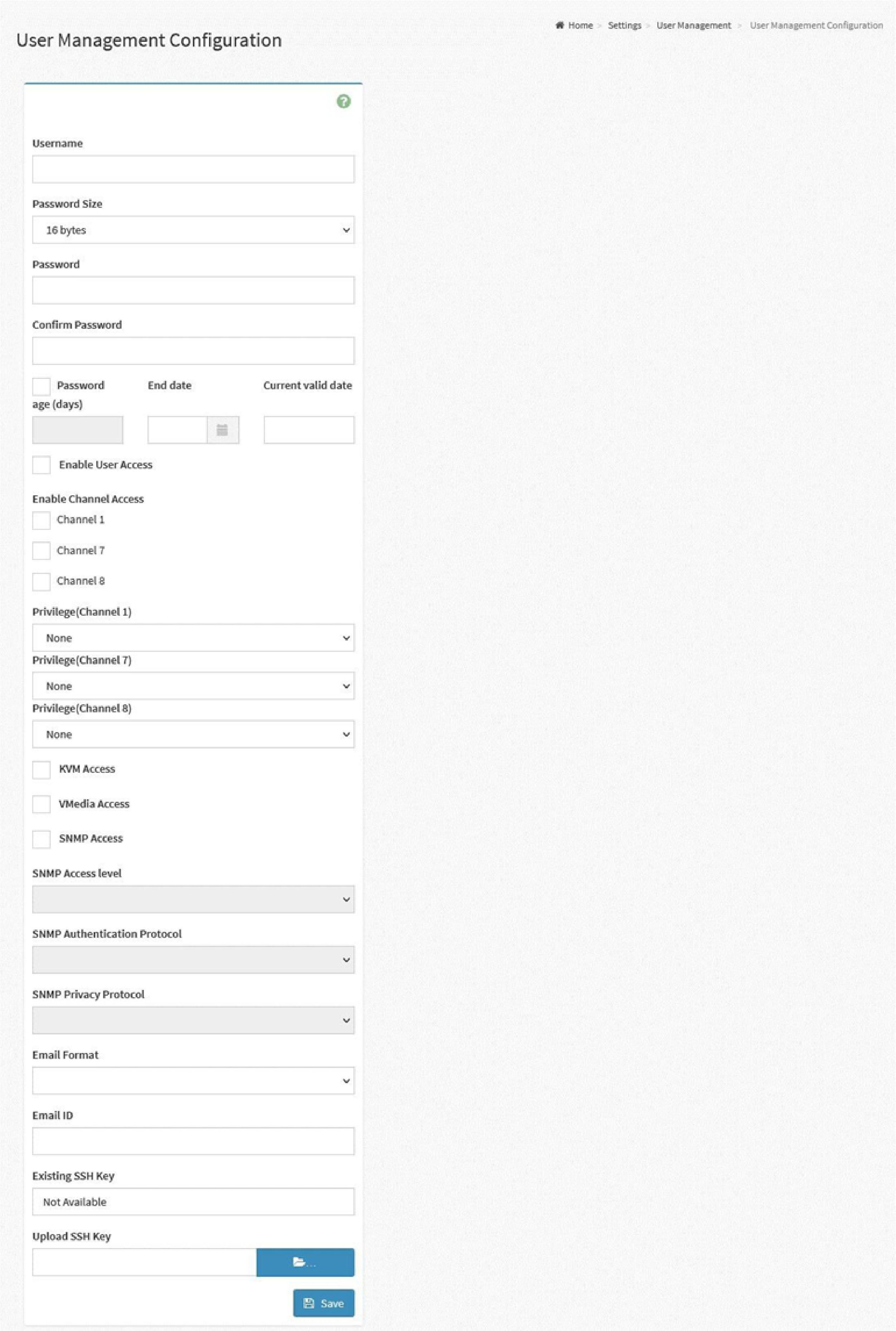
Channel 1 for users to connect to BMC through the dedicated BMC Management port.

Channel 7 or 8 for users connect to BMC through Shared NIC LAN port.

Note: Channel 7 is typically 1GbE Shared NIC, Channel 8 is typically 10GbE Shared NIC.

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

Click on the Delete icon (⊗) then delete this slot



Home > Settings > User Management > User Management Configuration

User Management Configuration

Username

Password Size

16 bytes

Password

Confirm Password

□ Password age (days) | End date | Current valid date

□ Enable User Access

Enable Channel Access

□ Channel 1

□ Channel 7

□ Channel 8

Privilege(Channel 1)

None

Privilege(Channel 7)

None

Privilege(Channel 8)

None

□ KVM Access

□ VMedia Access

□ SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format

Email ID

Existing SSH Key

Not Available

Upload SSH Key

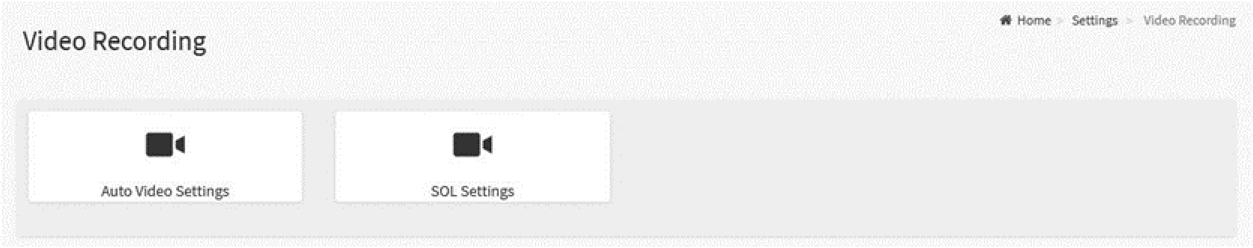
Configurable Fields:

- **Username:** Specify a name for the user.
- **Password Size:** 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 BMC service.
- **Enable Channel Access:** To select the channel/channels to enable the network access for the user.
- **Channel 1:** Allow user to access the BMC service through the dedicated BMC Management port.
- **Channel 7:** Allow user to access the BMC service through Share NIC LAN port. (Typically 1GbE Shared NIC interface)
- **Channel 8:** Allow user to access the BMC service through Share NIC LAN port. (Typically 10GbE Shared NIC interface)
- **Privilege (Channel 1), Privilege (Channel 7) and Privilege (Channel 8):** Select the privilege level for each channel to be assigned to this user for access to the BMC through the network interface. There are 5 levels of Network Privileges (Administrator, Operator, User, OEM and None).
- **KVM Access:** Check this option to assign the KVM privilege for the user.
- **VMedia Access:** Check this option to assign the VMedia privilege for the user.
- **SNMP Access:** Check this option to assign the SNMP privilege for the user.
- **SNMP Access level:** Select the SNMP access level for the user.
- **SNMP Authentication Protocol:** Select the Authentication Protocol for the user.
- **SNMP Privacy Protocol:** Select the Encryption algorithm to be used for the SNMP settings.
- **Email Format:** Specify the format for the email
- **Email ID:** Specify the email ID for the user.
- **Existing SSH Key:** If available, the uploaded SSH key information will be displayed.
- **Upload SSH Key:** Use the Browse button to navigate to the new public SSH key file.
- **Delete:** Click the Delete button to delete this user account.
- **Save:** Save the configured settings.

6.10.14 - Video Recording

Video Recording page provides the functional feature tab for users to configure the video recording settings, including

- Auto Video Settings
- SOL Settings

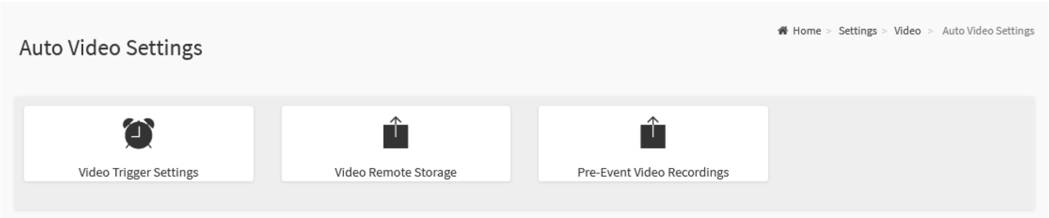


The details about each feature are listed in the following subsections.

6.10.14.1 - Auto Video Settings

This page provides the ability for users to configure the following events that will trigger auto video recording function of the KVM server:

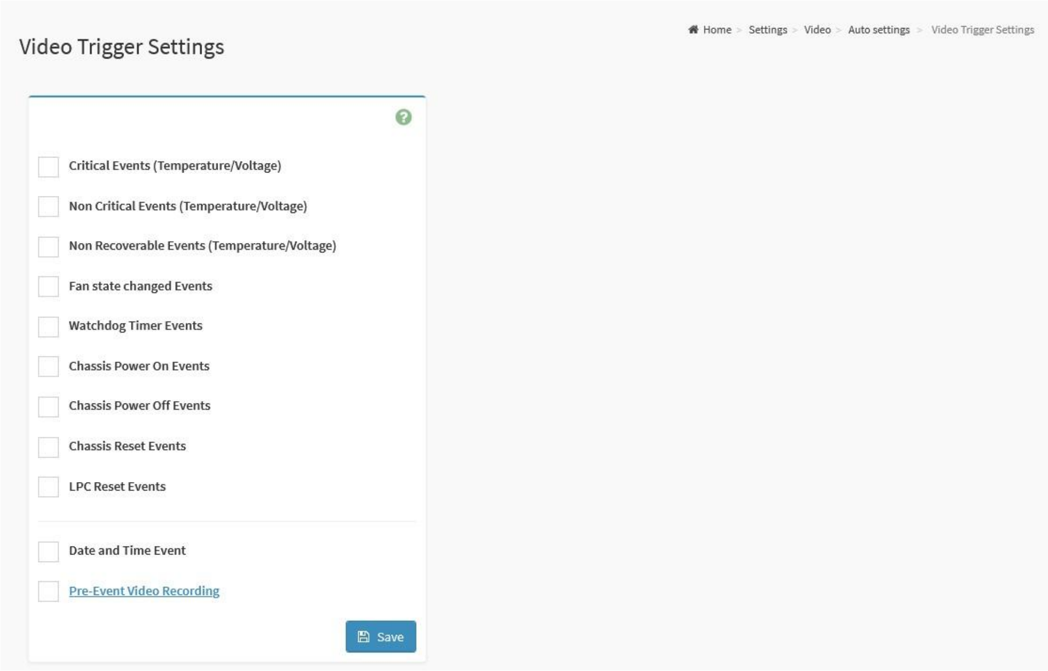
- Video Trigger Settings
- Video Remote Storage
- Pre-Event Video Recordings


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

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

6.10.14.1.1 - Video Trigger Settings

This page provides the ability for users to configure the video trigger settings.



Video Trigger Settings

Home > Settings > Video > Auto settings > Video Trigger Settings

□ Critical Events (Temperature/Voltage)

□ Non Critical Events (Temperature/Voltage)

□ Non Recoverable Events (Temperature/Voltage)

□ Fan state changed Events

□ Watchdog Timer Events

□ Chassis Power On Events

□ Chassis Power Off Events

□ Chassis Reset Events

□ LPC Reset Events

□ Date and Time Event

□ Pre-Event Video Recording

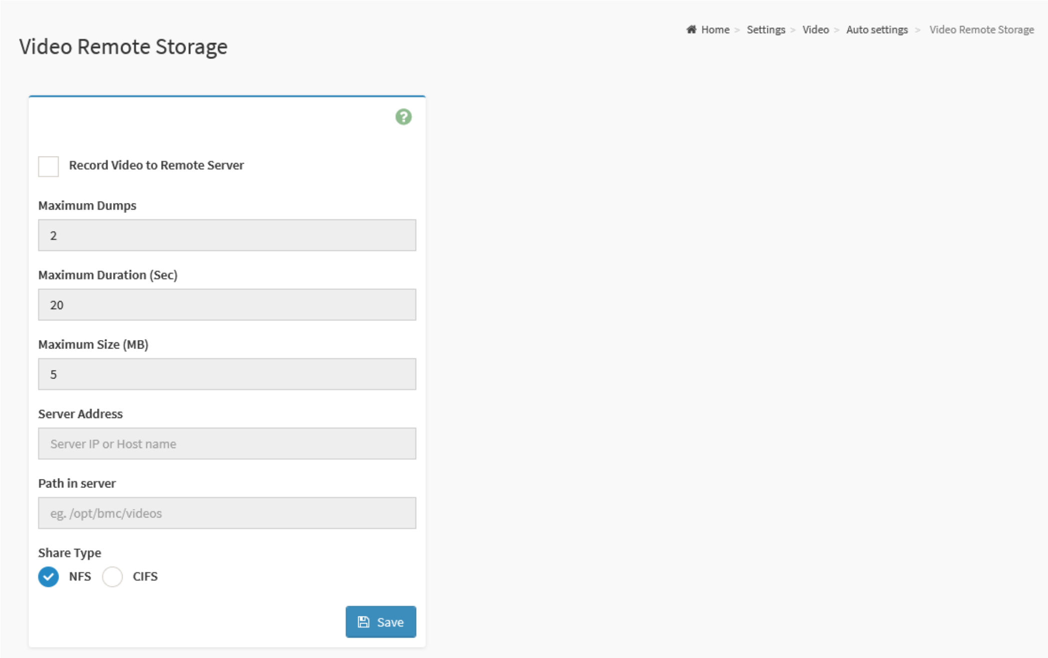
Configurable Fields:

- **Critical Events (Temperature/Voltage):** Check to trigger on critical sensor events.
- **Non-Critical Events (Temperature/Voltage):** Check to trigger on non-critical sensor events.
- **Non-Recoverable Events (Temperature/Voltage):** Check to trigger on non-recoverable sensor events.
- **Fan state changed Events:** Check to trigger on fan state changes.
- **Watchdog Timer Events:** Check to trigger on watchdog timer events.
- **Chassis Power-On Events:** Check to trigger on chassis power-on events.
- **Chassis Power-Off Events:** Check to trigger on chassis power-off events.
- **Chassis Reset Events:** Check to trigger on chassis reset events.
- **LPC Reset Events:** Check to configure on LPC reset events.
- **Date and Time Event:** Check to trigger at a date and time event.
- **Pre-Event Video Recording:** Check to configure the pre-event video recording parameters.
  - **Crash Reset:** Check to configure crash reset
    - **Pre-crash**
    - **Pre-reset**
- **Save:** Save the configured settings.

6.10.14.1.2 - Video Remote Storage

This page provides the ability for users to configure where videos may be recorded on a remote server.

Note: Due to storage limitations of the BMC, all videos recorded must be stored on a remote server, not within the BMC's local storage.



Home > Settings > Video > Auto settings > Video Remote Storage

Video Remote Storage

□ Record Video to Remote Server

Maximum Dumps: 2

Maximum Duration (Sec): 20

Maximum Size (MB): 5

Server Address: Server IP or Host name

Path in server: eg. /opt/bmc/videos

Share Type: ● NFS ○ CIFS

Configurable Fields:

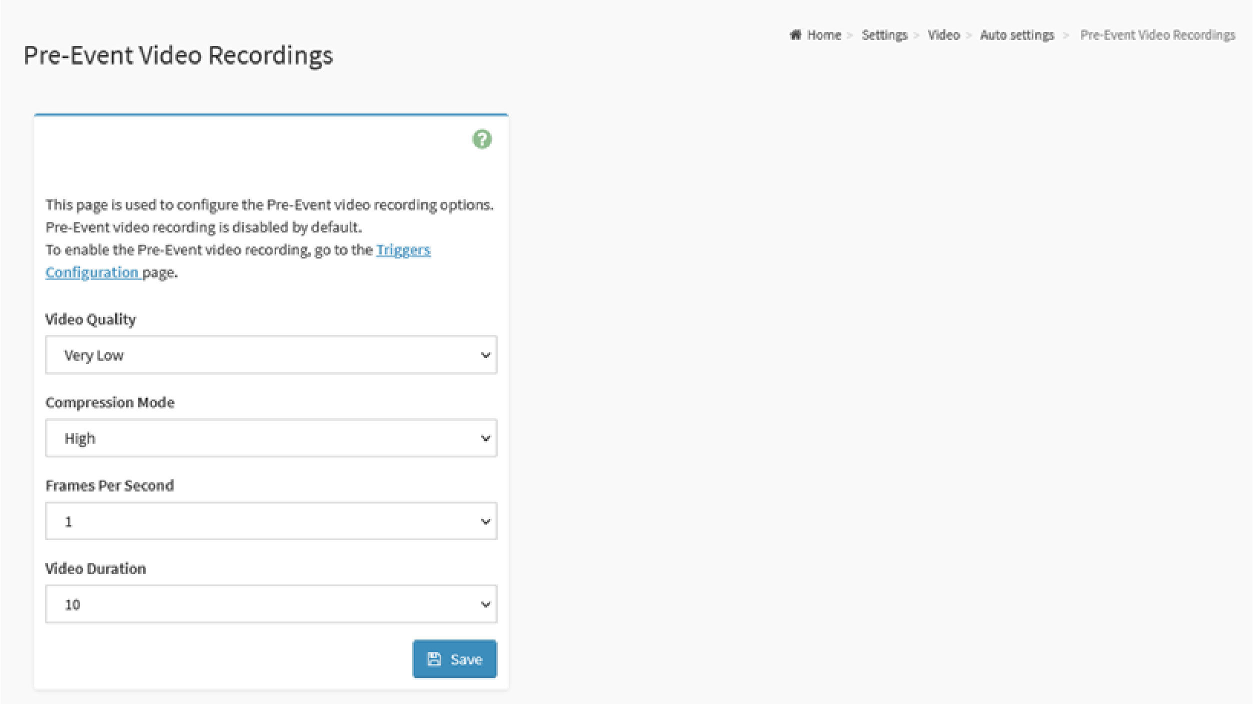
- **Record Video to Remote Server:** Check this option to enable Remote Video support.
- **Maximum Dumps:** Specify the number of Maximum Dumps, range from 1 to 100.
- **Maximum Duration (Sec):** Specify the number of Maximum Duration, range from 1 to 3600 seconds.
- **Maximum Size (MB):** Specify the number of Maximum size, range from 1 to 500 MB.
- **Server Address:** Address of the server where remote videos are to be stored.

  Note: IP Address and FQDN format are supported.

- **Path in server:** Specify the path in the remote server.
- **Share Type:** Select Share Type of the remote video server
  - NFS
  - CIFS
- **Save:** Save the configured settings.

6.10.14.1.3 - Pre-Event Video Recordings

This page provides the ability for users to configure the Pre-Event video recordings settings.



Home > Settings > Video > Auto settings > Pre-Event Video Recordings

Pre-Event Video Recordings

This page is used to configure the Pre-Event video recording options.
Pre-Event video recording is disabled by default.
To enable the Pre-Event video recording, go to the Triggers Configuration page.

Video Quality: Very Low

Compression Mode: High

Frames Per Second: 1

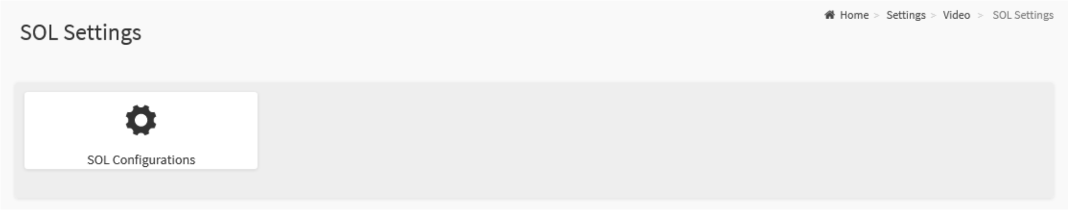
Video Duration: 10

Configurable Fields:

- **Video Quality:** Select the desired video quality from the options in the drop-down list.
- **Compression Mode:** Select the Compression Mode from the options listed in the drop-down list.
- **Frames Per Second:** Select the FPS to specify the desired number of frames per second.
- **Video Duration:** Select the desired video duration in seconds.
- **Save:** Save the configured settings.

6.10.14.2 - SOL Settings

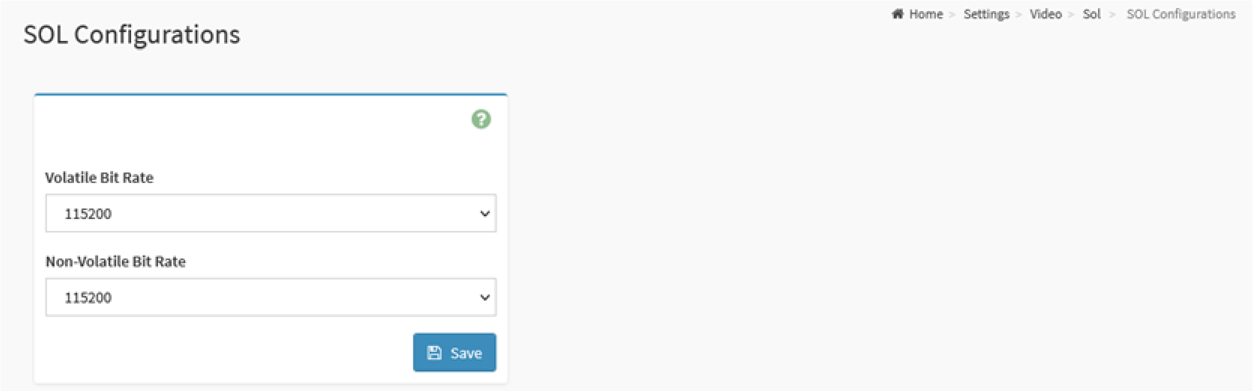
This page provides the tab for users to configure the SOL Settings of video recording.



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

6.10.14.2.1 - SOL Configurations

This page provides the ability for users to configure the Serial over Lan (SOL) configuration settings.



Volatile Bit Rate: 115200

Non-Volatile Bit Rate: 115200

Configurable Fields:

- **Volatile Bit Rate:** Select the Volatile Bit rate to determine which baud rate will be used for both IPMI and HTML based SOL.

  Note: After reboot, this field value will also overwrite the Non-Volatile Bit rate.

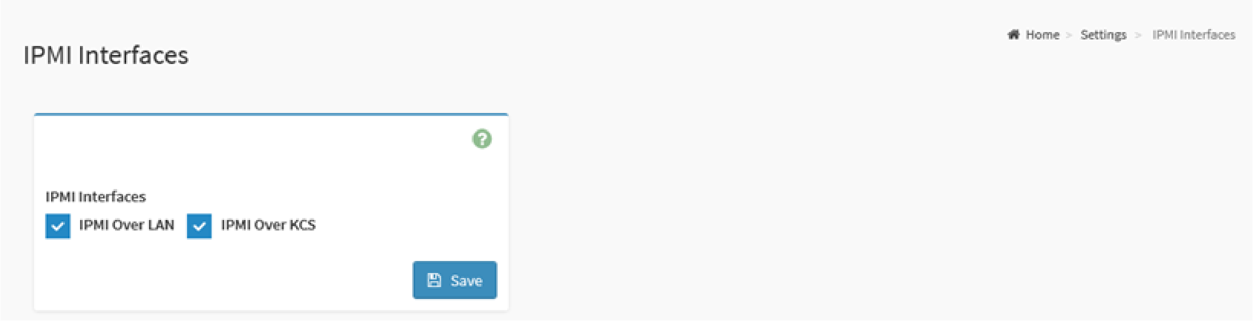
- **Non-Volatile Bit Rate:** To select the Non-Volatile Bit rate to determine which baud rate will be saved.

  Note: After reboot, this field value will also overwrite the Volatile Bit rate.

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

6.10.15 - IPMI Interfaces

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



IPMI Interfaces

IPMI Interfaces

☑ IPMI Over LAN ☑ IPMI Over KCS

Configurable Fields:

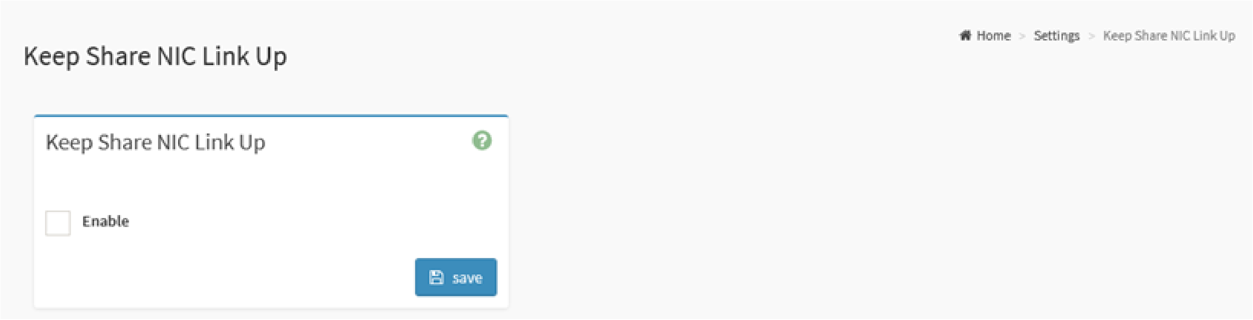
- **IPMI Interfaces:** Select the enabled interfaces for users to perform the IPMI communication.
  - **IPMI Over LAN:** Check this option to allow IPMI communication over LAN.
  - **IPMI Over KCS:** Check this option to allow IPMI communication over KCS.

    Note: KCS (Keyboard Control Style) interface is used as the default interface for IPMI communication within the system's local operating system. If IPMI commands (such as using ipmitool) are knowingly used by an application from the system's local OS, disabling this interface may impact functionality.

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

6.10.16 - Keep Share NIC Link Up

This page provides the option for users to configure the shared NIC PHY link up settings.



Keep Share NIC Link Up

Home > Settings > Keep Share NIC Link Up

Keep Share NIC Link Up

□ Enable

Configurable Fields:

- **Enabled:** Check this option to enable Keep Share NIC Link Up supported.

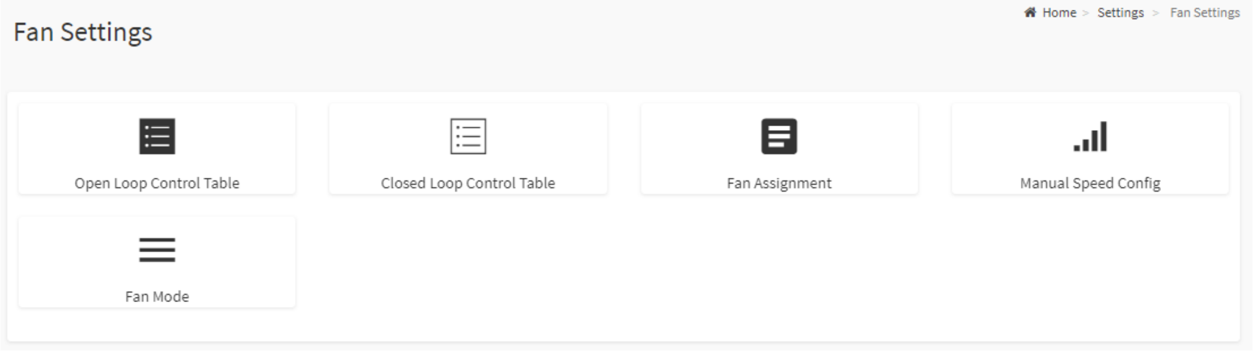
  Note: If enabled, the Share NIC PHY will keep the link up, avoiding shared NIC (NC-SI) link disconnects during system resets

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

6.10.17 - FAN Settings

FAN Settings page provides the ability for users to configure the system FAN settings which are controlled by the BMC. This includes:

- Open Loop Control Table
- Close Loop Control Table
- Fan Assignment
- Manual Speed Config
- Fan Mode



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

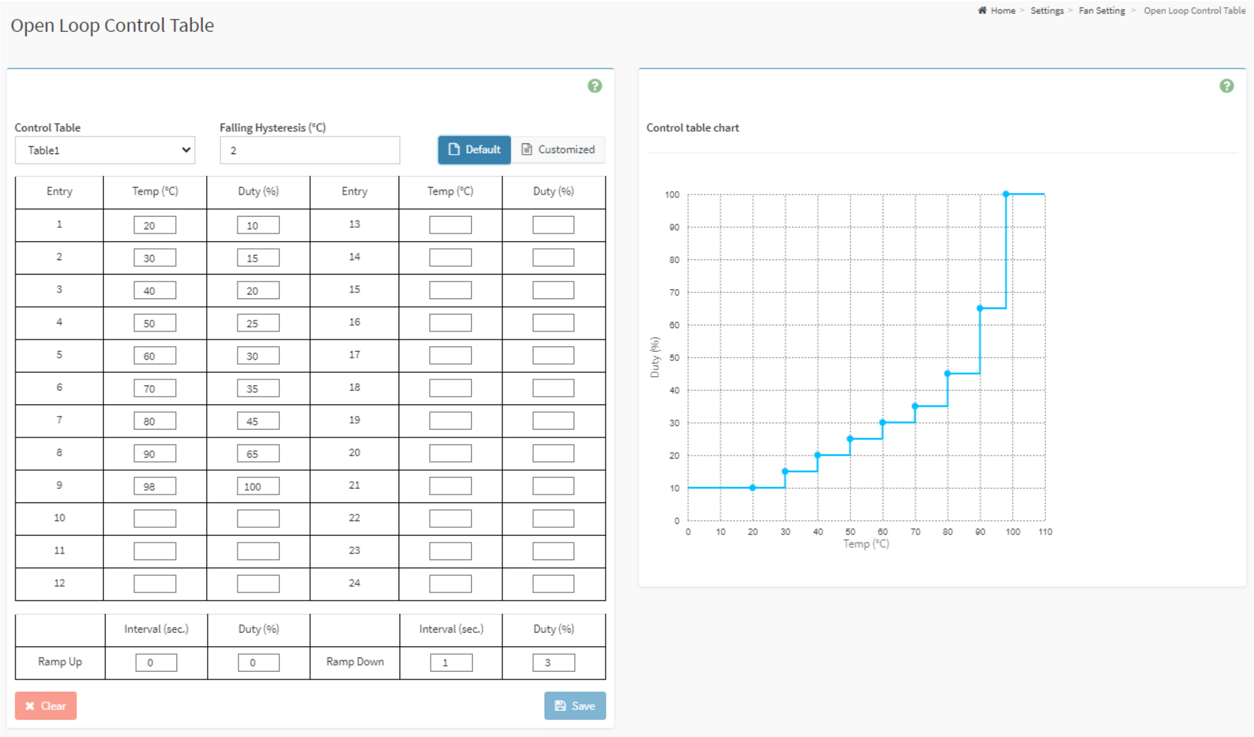
Note: The default Fan Settings may vary from among Axial Edge Server systems, but are set to ensure adequate cooling, acoustics, and power consumption relative to the standard supported configurations. Modification to the Fan Settings should only be performed by an experienced professional as changes may impact the performance or stability of the system.

Please consult system product manuals for additional default fan configuration details..

6.10.17.1 - Open Loop Control Table

This page provides the ability for users to configure the Open Loop Control Table settings.

After a table is created, Users can add the new FAN table from the Temperature Sensor and Corresponding Fan Table page.



Control Table: Table1

Falling Hysteresis (°C): 2

Entry	Temp (°C)	Duty (%)	Entry	Temp (°C)	Duty (%)
1	20	10	13		
2	30	15	14		
3	40	20	15		
4	50	25	16		
5	60	30	17		
6	70	35	18		
7	80	45	19		
8	90	65	20		
9	98	100	21		
10			22		
11			23		
12			24		

	Interval (sec.)	Duty (%)		Interval (sec.)	Duty (%)
Ramp Up	0	0	Ramp Down	1	3

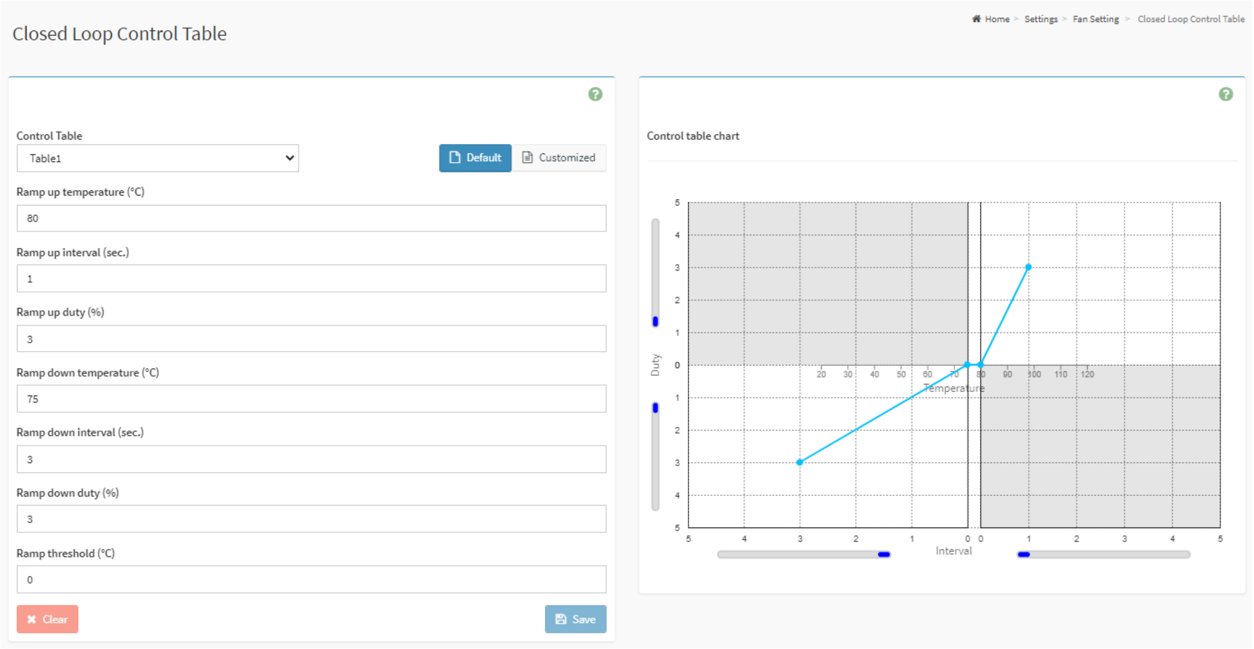
Configurable Fields:

- **Control Table:** Select the table which to be defined.
- **Falling Hysteresis (°C):** Temperature tolerance to prevent fan speed switching too fast.
- **Entry:** Indicates the condition number.
- **Temp (°C):** Specify the temperature for this entry.
- **Duty (%):** Specify the FAN duty for this entry.
- **Default:** Click the Default button will load the default setting values of the selected table.
- **Customized:** Click the Customized button to configure your own settings values for the selected table.
- **Ramp Up / Ramp Down:** Increasing or decreasing fan speed by a ramp rate to minimize perceived noise, set both interval and duty to zero to disable it. Fan speed will be adjusted to the next step immediately according to the table if disabled.
- **Clear:** To clear current settings value on the web.
- **Save:** Save the configured settings.

6.10.17.2 - Close Loop Control Table

This page provides the ability for users to configure Close Loop Control Table settings.

After a table is created, Users can add the new FAN table from the Temperature Sensor and Corresponding Fan Table page.



Closed Loop Control Table

Control Table: Table1

Ramp up temperature (°C): 80

Ramp up interval (sec.): 1

Ramp up duty (%): 3

Ramp down temperature (°C): 75

Ramp down interval (sec.): 3

Ramp down duty (%): 3

Ramp threshold (°C): 0

Configurable Fields:

- **Table:** Select the table which to be used.
- **Ramp up temperature (°C):** Temperature upper bound setting, fan speed will start to increase when the temperature gets above this setting.
- **Ramp up interval (sec.):** Steps up the fan speed at this time interval setting.
- **Ramp up duty (%):** Fan speed will increase by this duty setting when temperature hits the ramp up temperature setting.
- **Ramp down temperature (°C):** Temperature lower bound setting, fan speed will start to decrease when the temperature gets below this setting.
- **Ramp down interval (sec.):** Steps down the fan speed at this time interval setting.
- **Ramp down duty (%):** Fan speed will decrease by this duty setting when temperature hits the ramp down temperature setting.
- **Ramp threshold (°C):** Minimum temperature for this closed loop table to take effect.
- **Default:** Click the Default button will load the default setting values of the selected table.
- **Customized:** Click the Customized button to configure your own settings values for the selected table.
- **Clear:** Clear current settings value on the web.
- **Save:** Save the configured settings.

6.10.17.3 - Fan Assignment

This page provides the ability for users to assign a Fan Table (Open Loop or Closed Loop) to the temperature sensors in the system.

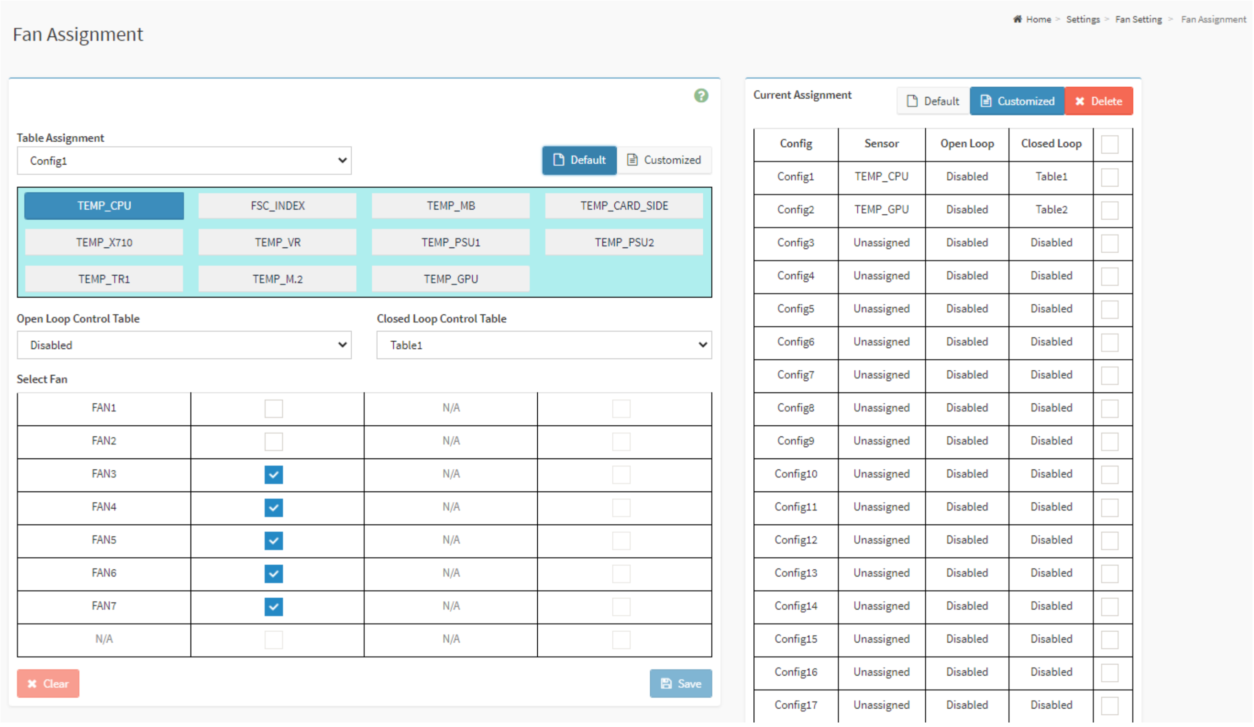


Table Assignment: Config1

Open Loop Control Table: Disabled

Closed Loop Control Table: Table1

Select Fan

FAN1	☐	N/A	☐
FAN2	☐	N/A	☐
FAN3	☑	N/A	☐
FAN4	☑	N/A	☐
FAN5	☑	N/A	☐
FAN6	☑	N/A	☐
FAN7	☑	N/A	☐
N/A	☐	N/A	☐

Config	Sensor	Open Loop	Closed Loop	☐
Config1	TEMP_CPU	Disabled	Table1	☐
Config2	TEMP_GPU	Disabled	Table2	☐
Config3	Unassigned	Disabled	Disabled	☐
Config4	Unassigned	Disabled	Disabled	☐
Config5	Unassigned	Disabled	Disabled	☐
Config6	Unassigned	Disabled	Disabled	☐
Config7	Unassigned	Disabled	Disabled	☐
Config8	Unassigned	Disabled	Disabled	☐
Config9	Unassigned	Disabled	Disabled	☐
Config10	Unassigned	Disabled	Disabled	☐
Config11	Unassigned	Disabled	Disabled	☐
Config12	Unassigned	Disabled	Disabled	☐
Config13	Unassigned	Disabled	Disabled	☐
Config14	Unassigned	Disabled	Disabled	☐
Config15	Unassigned	Disabled	Disabled	☐
Config16	Unassigned	Disabled	Disabled	☐
Config17	Unassigned	Disabled	Disabled	☐

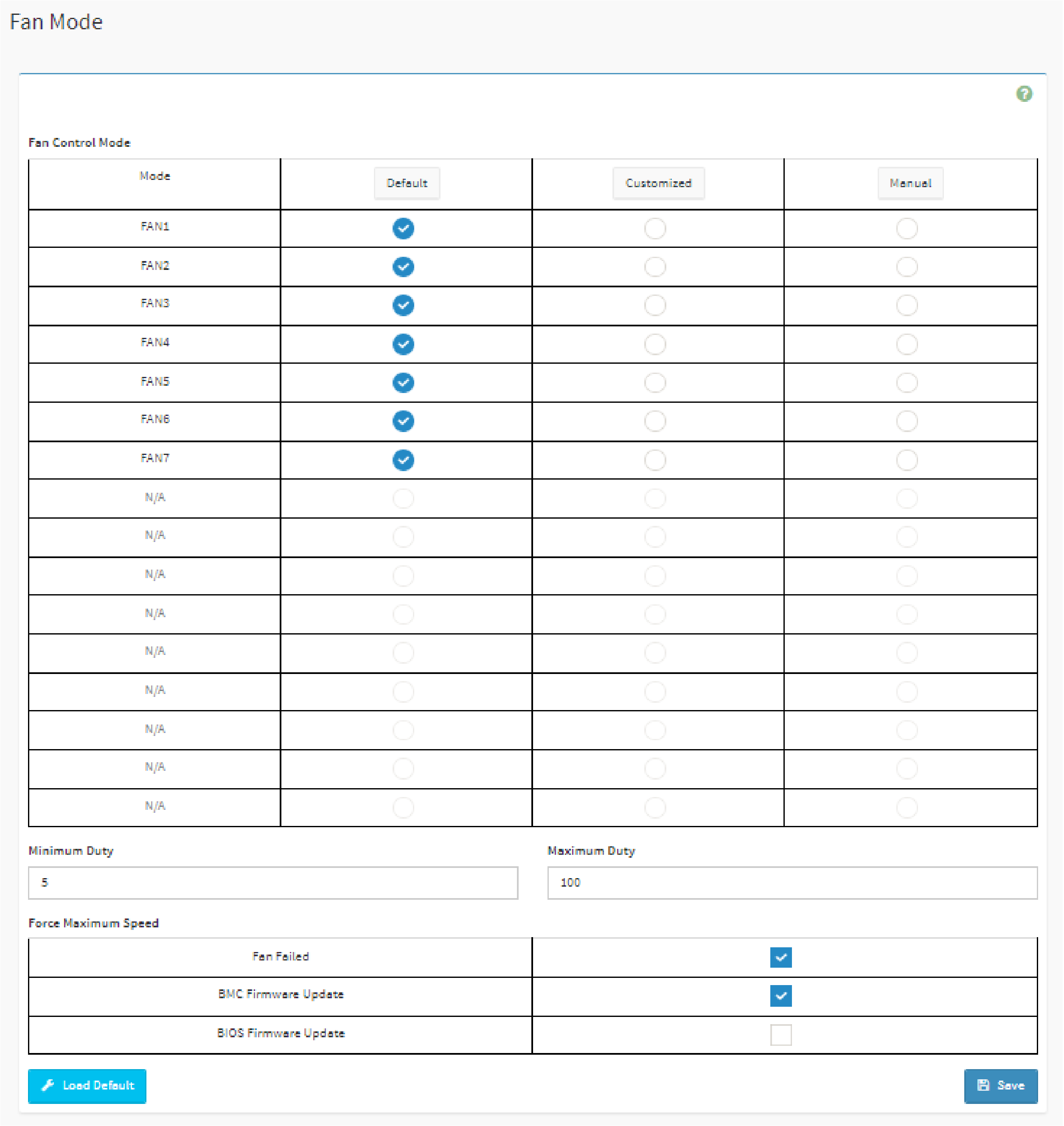
<u>Configurable Fields:</u>

- **Table Assignment:** Select the Configuration to modify. Config assignments are listed in the left table. The table assignment (config) is relative to the selected (dark blue) temperature sensor(s).
    - **Default:** Click Default button to load the default setting value (the default selected FAN) of the selected temperature sensor.
    - **Customized:** Click the Customized button to modify the settings value for the selected FAN.
    - **Open Loop Control Table:** Select the Open Loop Control Table which to be used. If no table assignment applies, set to Disabled.
    - **Close Loop Control Table:** Select the Close Loop Control Table which to be used. If no table assignment applies, set to Disabled.
    - **Select Fan:** Check the fans which are affected by the selected table and sensor combination.
    - **Clear:** Removes sensor and table assignment of the configuration
    - **Save:** Save the configured settings.
- **Current Assignment:** Lists the current sensor & table configuration assignments as they are saved from the Table Assignments section.
    - **Default:** Show the default configuration settings.

- **Customized:** Show the customized sensor & table configuration settings.
- **Delete:** Clears the selected (checked) sensor & table configuration.

6.10.17.4 - Fan Mode

This page provides the ability for users to configure the Fan Control Mode settings.



Fan Mode

Fan Control Mode

Mode	Default	Customized	Manual
FAN1	●	○	○
FAN2	●	○	○
FAN3	●	○	○
FAN4	●	○	○
FAN5	●	○	○
FAN6	●	○	○
FAN7	●	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○
N/A	○	○	○

Minimum Duty: 5

Maximum Duty: 100

Force Maximum Speed

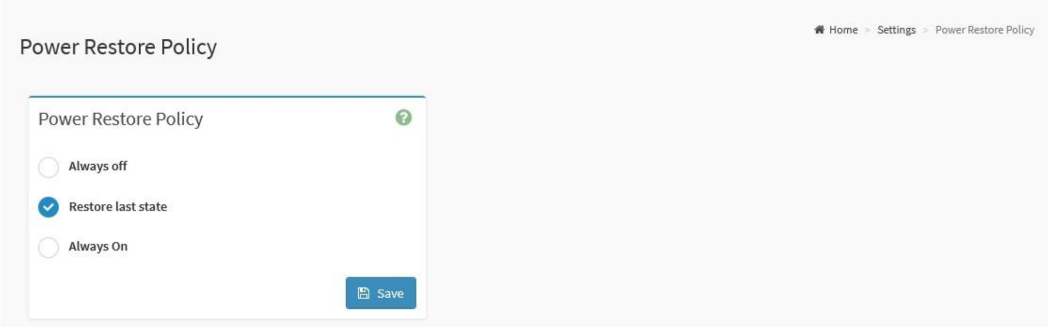
Fan Failed	☑
BMC Firmware Update	☑
BIOS Firmware Update	□

Configurable Fields:

- **Fan Control Mode:** Select the control mode for each Fan listed in the table.
  - Default will operate according to pre-programmed firmware values.
  - Customized will operate in accordance with the customized fan assignment settings (from Fan Assignment page).
  - Manual will operate in accordance with the statically defined manual fan values (from Manual Speed Config page).
- **Minimum Duty (%):** The minimum duty cycle of the fans.
- **Maximum Duty (%):** The maximum duty cycle of the fans.
- **Force Maximum Speed:** Additional parameters which may cause the system fans to ramp to the maximum speed.
- **Load Defaults:** Load the pre-programmed default values of the form.
- **Save:** Save the configured settings.

6.10.18 - Power Restore Policy

Power Restore Policy page provides the ability for users to configure the power restore policy settings.



○ Always off
● Restore last state
○ Always On

Configurable Fields:

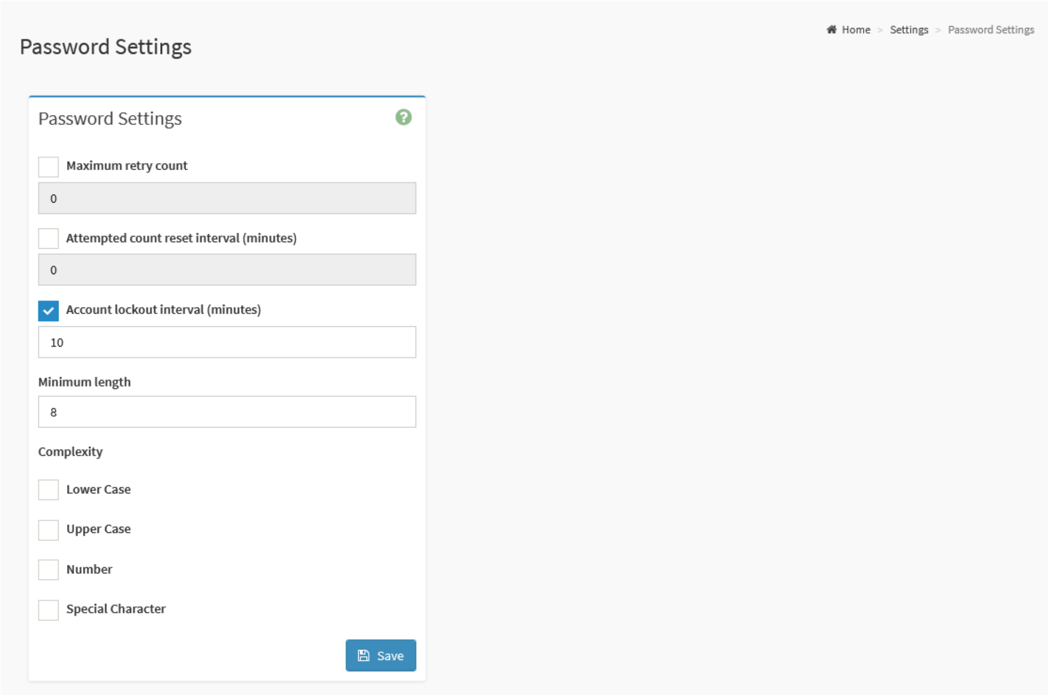
- **Always off:** After the power is restored, the system will remain off.
- **Restore last state:** Restore the system to the same state as before the power failure

  Note: Restore last state is the system default.

- **Always On:** After the power is restored, the system will automatically power-on.
- **Save:** Save the configured settings.

6.10.19 - Password Settings

Password Settings page allows users to configure the password policy.



Password Settings

Home > Settings > Password Settings

Password Settings

□ Maximum retry count

0

□ Attempted count reset interval (minutes)

0

☑ Account lockout interval (minutes)

10

Minimum length

8

Complexity

□ Lower Case

□ Upper Case

□ Number

□ Special Character

Configurable Fields:

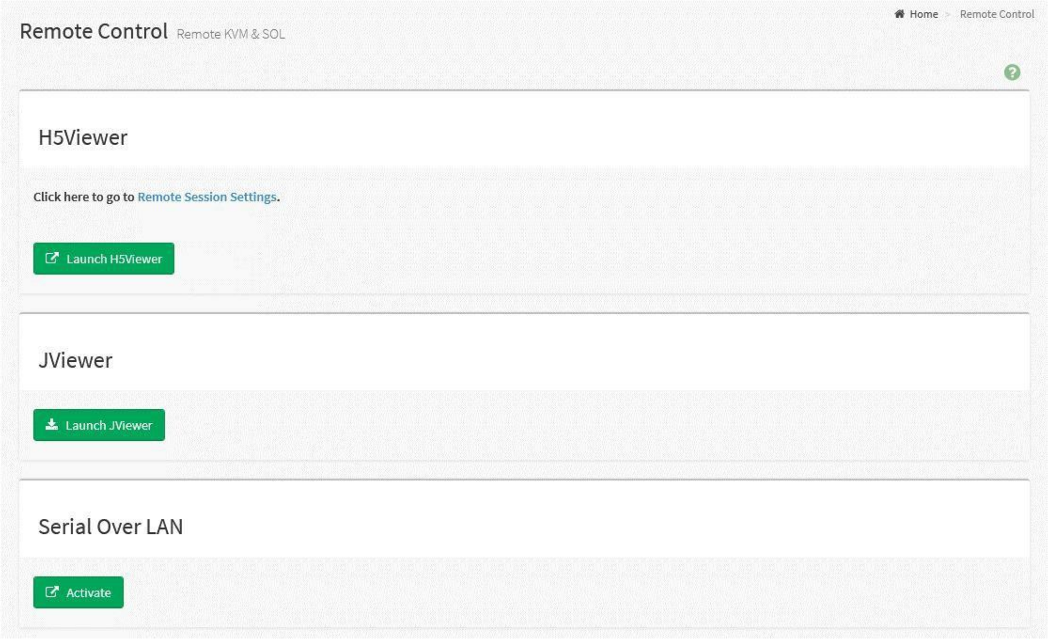
- **Maximum retry count:** Check this option to enable this feature. When set, this value specifies the Maximum Retry Count. Users will be locked out if the number of failed login attempts reach this setting.
- **Attempted count reset interval (minutes):** Check this option to enable this feature. When set, this value specifies the attempted count reset interval.
- **Account lockout interval (minutes):** Check this option to enable this feature. When set, this value indicates the lockout interval.
- **Minimum length:** Set the minimum password length.
- **Complexity:** Check the desired password enforcement rules to increase password complexity.
  - **Lower Case:** Password must have lower case character.
  - **Upper Case**: Password must have upper case character.
  - **Number:** Password must have number.
  - **Special Character:** Password must have a special character.
- **Save:** Save the configured settings.

6.11 - Remote Control

The BMC WebUI provides useful remote control services as follows:

- H5Viewer: Remote control KVM via HTML5 web interface
- JViewer: Remote control KVM via Java Runtime Environment (JRE) interface
- Serial Over LAN: Remote control via Serial Over LAN.

The Remote Control page provides links for users to launch the desired remote KVM or SOL service.



Remote Control Remote KVM & SOL

H5Viewer

Click here to go to Remote Session Settings.

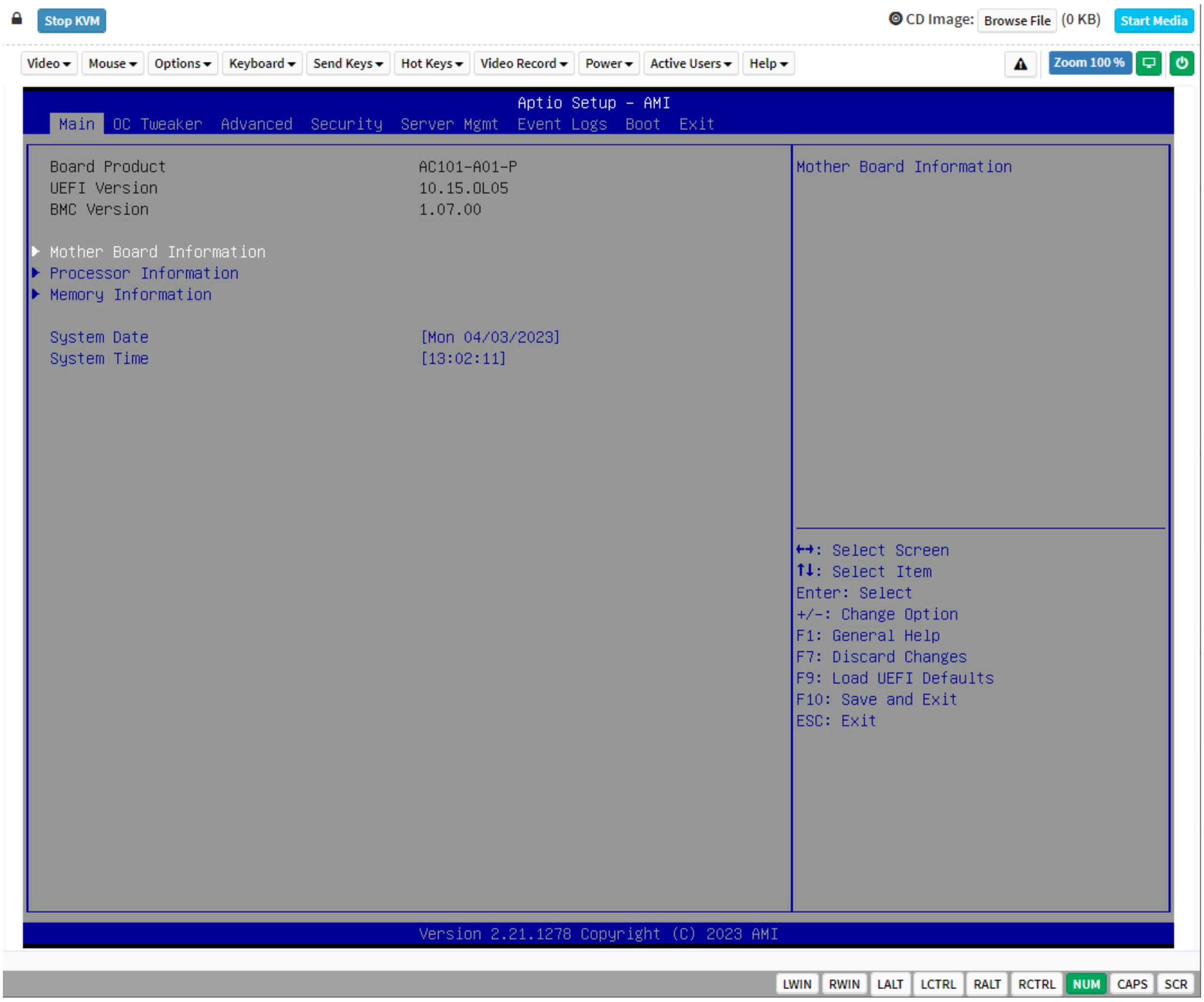
JViewer

Serial Over LAN

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

6.11.1 - H5Viewer

H5Viewer provides a remote KVM service for users to remote control the host through the HTML5 environment.



```
                                Aptio Setup - AMI
   Main  OC Tweaker  Advanced  Security  Server Mgmt  Event Logs  Boot  Exit

  Board Product                       AC101-A01-P           Mother Board Information
  UEFI Version                        10.15.0L05
  BMC Version                         1.07.00

▶ Mother Board Information
▶ Processor Information
▶ Memory Information

  System Date                         [Mon 04/03/2023]
  System Time                         [13:02:11]
                                                            ↔: Select Screen
                                                            ↑↓: Select Item
                                                            Enter: Select
                                                            +/-: Change Option
                                                            F1: General Help
                                                            F7: Discard Changes
                                                            F9: Load UEFI Defaults
                                                            F10: Save and Exit
                                                            ESC: Exit

                    Version 2.21.1278 Copyright (C) 2023 AMI
```

Video Menu:

- **Pause Video:** Click this button to pause the Console Redirection.
- **Resume Video**: Click this button to resume the Console Redirection when the session is paused.
- **Refresh Video:** Click this button to update the display shown in the Console Redirection window.
- **Host Display**
  - **Display On:** Click this button to enable this feature. The host display will be turned on if this feature is enabled.
  - **Display Off:** Click this button to enable this feature. The host display will be blank if this feature is enabled, but users can view the host screen in the Console Redirection window.
- **Capture Screen:** Click this button to take a screenshot of the host screen and save it in the client system.

Mouse Menu:

- **Show Client Cursor:** Click this button to show or hide the local mouse cursor on the remote client system.
- **Mouse Mode:** This option handles mouse emulation from local window to remote screen using below methods. Only Administrators have the privilege to configure this option.
    - **Absolute Mouse Mode:** The absolute position of the local mouse is sent to the server if this option is selected.
    - **Relative Mouse Mode:** The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
    - **Other Mouse Mode:** This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

Option Menu:

- **Zone**
    - **Normal:** Click this button to set the screen size to default size.
    - **Zoom In:** Click this button to increase the screen size. This zoom varies from 100% to 150% with an interval of 10%.
    - **Zoom Out:** Click this button to decrease the screen size. This zoom varies from 100% to 50% with an interval of 10%.
- **Block Privilege Request:** Enable or disable the access privilege for the user.
    - Partial Permission
    - No Permission
- **Band Width:** Select the band width for the Console Redirection window
    - Auto Detect
    - 256Kbps
    - 512Kbps
    - 1Mbps
    - 10Mbps
    - 100Mbps
- **Compression Mode:** This option helps to compress the video data transfer to the specific mode.
    - YUV 420
    - YUV 444
    - YUV 444 + 2 color VQ
    - YUV 444 + 4 color VQ
- **DTC Quantization Table:** This option helps to select the video quality.
    - 0 Best Quality
    - 1
    - 2
    - 3
    - 4
    - 5

    - 6

Keyboard Menu:

- **Keyboard Layout:** This feature is fully compatible when host and client have the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.
    - **English U.S**
    - **German**
    - **Japanese**
- **Virtual Keyboard:** Click this button to open a virtual keyboard on the Console Redirection window.

Send Keys Menu:

- **Hold Down**
    - **Right Ctrl Key:** Click this button to act as hold down the right-side <CTRL> key when in Console Redirection.
    - **Right Alt Key:** Click this button to act as hold down the right-side <ALT> key when in Console Redirection.
    - **Right Windows Key:** Click this button to act as hold down the right-side <WIN> key when in Console Redirection.
    - **Left Ctrl Key:** Click this button to act as hold down the left-side <CTRL> key when in Console Redirection.
    - **Left Alt Key:** Click this button to act as hold down the left-side <ALT> key when in Console Redirection.
    - **Left Windows Key:** Click this button to act as hold down the left- side <WIN> key when in Console Redirection.
- **Press and Release**
    - **Ctrl+Alt+Del:** Click this button to act as a single hit the <CTRL>, <ALT> and <DEL> keys down simultaneously on the host that the user is redirecting.
    - **Left Windows Key:** Click this button to act as a single hit the left- side <WIN> key when in Console Redirection.
    - **Right Windows Key:** Click this button to act as a single hit the right- side <WIN> key when in Console Redirection.
    - **Context Menu Key:** Click this button to act as a single hit the context menu key when in Console Redirection.
    - **Print Screen Key:** Click this button to act as a single hit the print screen key when in Console Redirection.

Hot Keys Menu:

- **Add Hot Keys:** Click this button to open the User Define Macros window to add a hot key macro. The configured key events are saved in the BMC.

Video Record Menu:

- **Record Video:** Click this button to start recording the screen.
- **Stop Recording:** Click this button to stop the recording.

- **Record Settings:** Click this button to open the Record Settings window to configure the settings.
  - **Video Length:** To specify the value for video length, range of 1 to 1800 seconds.
  - **Video Compression:** To specify the value for video compression, range of 0.1 (low image quality) to 0.9 (high image quality).
  - **Normalized video resolution to 1024 X 768:** Enable this feature that host video will be scaled to 1024 x 768 in the recorded video file.
  - **OK:** Click this button to save the configured settings.
  - **Cancel:** Click this button to leave this window without saving the settings.

Power Menu:

- **Reset Server:** To reboot the system without powering off (warm boot).
- **Immediate Shutdown:** To perform Power OFF Immediately.
- **Orderly Shutdown:** To Power OFF the server in proper order.
- **Power On Server:** To Power ON the server.
- **Power Cycle Server:** To first power off, and then reboot the system (cold boot).

Active Users Menu:

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

Help Menu:

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

Quick Buttons:

- ⚠: This quick button will show/hide notifications dropdown menu, which will contain the list of notifications displayed by H5Viewer.
- Zoom 100 %: This quick button indicates the current zoom value in percentage.
- 🟩🟥: This quick button indicates the current host monitor status. If the icon is in green color then the host monitor is unlocked. If the icon is in red color then the host monitor is locked. Clicking the button to change the monitor status.
- ⏻⏻: This quick button indicates the current server power status. If the icon is in green color, the server power status is powered on. If the icon is in red color, the server power status is powered off. Click this button to toggle immediate power off/power on the host.
- Stop KVM: Click this button to close the current KVM session and Console Redirection window.
- ❓CD Image: Browse File (0 KB): Click the Browse File button to select the image file to remote mount the image file to the host.
- ☐ Media Boost: Click the Media Boost button to boost up the image mount process.
- Start Media: Click the Start Media button to start the remote mount of the selected image file.

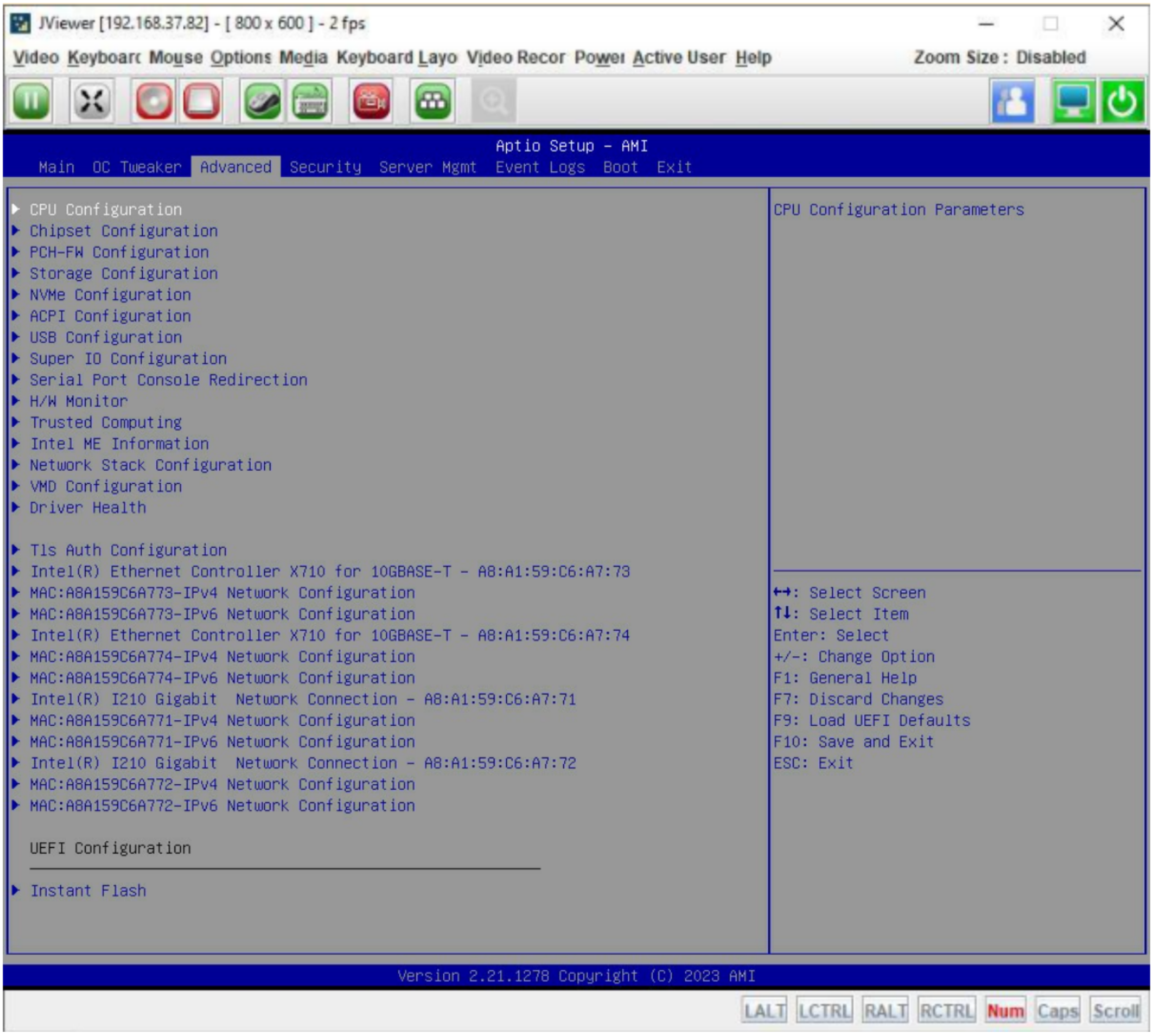
- Stop Media : Click the Stop Media button to stop the remote mount of the image file.

Status Bar Buttons:

- LWIN RWIN LALT LCTRL RALT RCTRL NUM CAPS SCR : Num/Caps/Scroll lock buttons are LED status buttons that denote the current status of Num/Caps/Scroll lock in the host.

6.11.2 - JViewer

JViewer is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE must be installed in the client's system to use the JViewer.


JViewer [192.168.37.82] - [800 x 600] - 2 fps
Video Keyboar Mouse Options Media Keyboard Layo Video Recor Powe Active User Help
Zoom Size : Disabled
LALT LCTRL RALT RCTRL Num Caps Scroll

```
                          Aptio Setup - AMI
  Main  OC Tweaker  Advanced  Security  Server Mgmt  Event Logs  Boot  Exit

▶ CPU Configuration                                          CPU Configuration Parameters
▶ Chipset Configuration
▶ PCH-FW Configuration
▶ Storage Configuration
▶ NVMe Configuration
▶ ACPI Configuration
▶ USB Configuration
▶ Super IO Configuration
▶ Serial Port Console Redirection
▶ H/W Monitor
▶ Trusted Computing
▶ Intel ME Information
▶ Network Stack Configuration
▶ VMD Configuration
▶ Driver Health

▶ Tls Auth Configuration
▶ Intel(R) Ethernet Controller X710 for 10GBASE-T - A8:A1:59:C6:A7:73
▶ MAC:A8A159C6A773-IPv4 Network Configuration                 ↔: Select Screen
▶ MAC:A8A159C6A773-IPv6 Network Configuration                 ↑↓: Select Item
▶ Intel(R) Ethernet Controller X710 for 10GBASE-T - A8:A1:59:C6:A7:74  Enter: Select
▶ MAC:A8A159C6A774-IPv4 Network Configuration                 +/-: Change Option
▶ MAC:A8A159C6A774-IPv6 Network Configuration                 F1: General Help
▶ Intel(R) I210 Gigabit  Network Connection - A8:A1:59:C6:A7:71  F7: Discard Changes
▶ MAC:A8A159C6A771-IPv4 Network Configuration                 F9: Load UEFI Defaults
▶ MAC:A8A159C6A771-IPv6 Network Configuration                 F10: Save and Exit
▶ Intel(R) I210 Gigabit  Network Connection - A8:A1:59:C6:A7:72  ESC: Exit
▶ MAC:A8A159C6A772-IPv4 Network Configuration
▶ MAC:A8A159C6A772-IPv6 Network Configuration

  UEFI Configuration
  ──────────────────────────────────────────
▶ Instant Flash

              Version 2.21.1278 Copyright (C) 2023 AMI
```

Video Menu:

- **Pause Redirection:** Click this button to pause the Console Redirection.
- **Resume Redirection:** Click this button to resume the Console Redirection when the session is paused.
- **Refresh Video:** Click this button to update the display shown in the Console Redirection window.
- **Turn ON Host Display:** Click this button to enable this feature. The host display will be turn on if this feature is enabled.
- **Turn OFF Host Display:** Click this button to enable this feature. The host display will be blank if this feature is enabled, but users can view the host screen in the Console Redirection window.

- **Capture Screen:** Click this button to take a screenshot of the host screen and save it in the client system.
- **Full Screen:** Click this button to view the Console Redirection in full screen mode (Maximize).
- **Compression Mode:** This option helps to compress the video data transfer to the specific mode.
    - YUV 420
    - YUV 444
    - YUV 444 + 2 color VQ
    - YUV 444 + 4 color VQ
- **DTC Quantization Table:** This option helps to select the video quality.
    - 0 Best Quality
    - 1
    - 2
    - 3
    - 4
    - 5
    - 6
    - 7 Worst Quality
- **Exit:** Click this button to exit the Console Redirection screen.

Keyboard Menu:

- **Hold Right Ctrl Key:** Click this button to act as hold down the right-side <CTRL> key when in Console Redirection.
- **Hold Right Alt Key:** Click this button to act as hold down the right-side <ALT> key when in Console Redirection.
- **Hold Left Ctrl Key:** Click this button to act as hold down the left-side <CTRL> key when in Console Redirection.
- **Hold Left Alt Key:** Click this button to act as hold down the left-side <ALT> key when in Console Redirection.
- **Left Windows Key:** Click this button to act as the left-side <WIN> key when in Console Redirection. Users can also decide how the key should be pressed: Hold Down or Press and Release.
    - Hold Down
    - Press and Release
- **Right Windows Key:** Click this button to act as the right-side <WIN> key when in Console Redirection. Users can also decide how the key should be pressed: Hold Down or Press and Release.
    - Hold Down
    - Press and Release
- **Ctrl+Alt+Del:** Click this button to act as a single hit the <CTRL>, <ALT> and <DEL> keys down simultaneously on the host that the user is redirecting.
- **Context Menu Key:** Click this button to act as a single hit the context menu key when in Console Redirection.
- **Hot Key**

    - **Add Hot Keys:** Click this button to open the User Define Macros window and add a hot key macro. The configured key events are saved in the BMC.
- **Full Keyboard Support:** Enable this option to provide full keyboard support. This option is used to trigger the Ctrl and Alt key directly to host from the physical keyboard.

Mouse Menu:

- **Show Cursor:** Click this button to show or hide the local mouse cursor on the remote client system.
- **Mouse Calibration:** This option can be used only if the mouse mode is relative.
- **Mouse Mode:** This option handles mouse emulation from local window to remote screen using below methods. Only the Administrator has the privilege to configure this option.
    - **Absolute Mouse Mode:** The absolute position of the local mouse is sent to the server if this option is selected.
    - **Relative Mouse Mode:** The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
    - **Other Mouse Mode:** This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

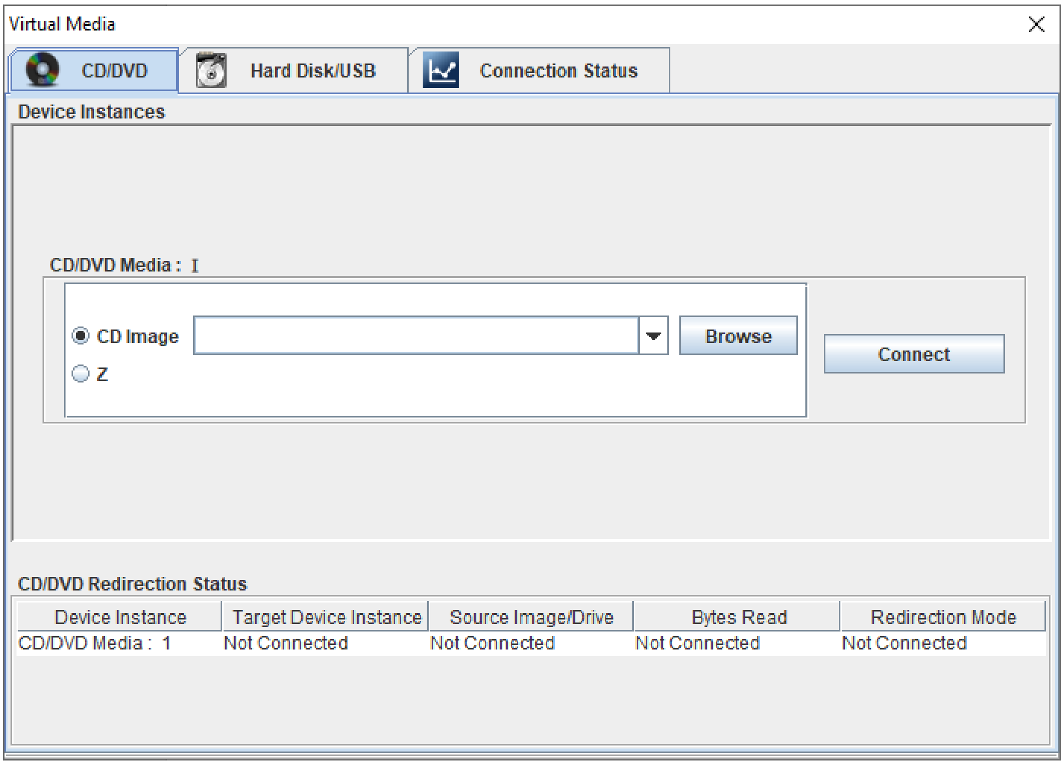
Option Menu:

- **Band Width:** Select the bandwidth for the Console Redirection window
    - Auto Detect
    - 256Kbps
    - 512Kbps
    - 1Mbps
    - 10Mbps
    - 100Mbps
- **Zone:**
    - Zoom In: Click this button to increase the screen size. This zoom varies from 100% to 150% with an interval of 10%.
    - Zoom Out: Click this button to decrease the screen size. This zoom varies from 100% to 50% with an interval of 10%.
    - Actual Size: Click this button to set the screen size to default size.
    - Fit to Client Resolution: If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen.
    - Fit to Host Resolution: If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.
- **Send IPMI Command:** Click this button to open the IPMI Command Dialog window, users can enter the raw IPMI command in the Hexadecimal field as hexadecimal value and click Send. The response will be displayed on the IPMI Command Dialog window.
- **GUI Language:** Select the desired GUI language.
    - Chinese - [CN]
    - English – [EN]

    - French – [FR]
- **Block Privilege Request:** Enable or disable the access privilege for the user.
    - Allow Only Video
    - Deny Access

Media Menu:

- **Virtual Media Wizard...:** Click this button to open the Virtual Media window.



Device Instance	Target Device Instance	Source Image/Drive	Bytes Read	Redirection Mode
CD/DVD Media : 1	Not Connected	Not Connected	Not Connected	Not Connected

The virtual media application will allow users to redirect different media to the host system. The application supports CD/DVD, Hard Disk/USB devices as well as image files.

Keyboard Layout Menu:

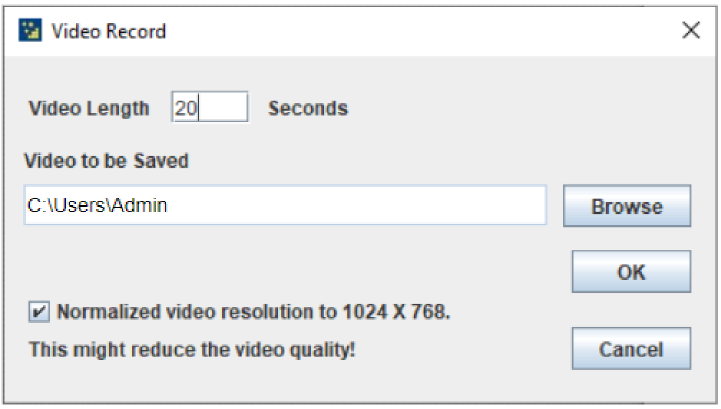
- **Auto Detect:** This option is used to detect keyboard layout automatically.
- **Physical Keyboard:**
    - **Host Platform:** This feature contains two options Windows and Linux.
    - **List of Host Physical Keyboard languages supported:**
        - English –US
        - English – UK
        - French
        - French (Belgium)
        - German (Germany)
        - German (Switzerland)
        - Japanese
        - Spanish
        - Italian
        - Danish
        - Finnish
        - Norwegian (Norway)
        - Portuguese (Portugal)
        - Swedish
        - Dutch (Netherland)
        - Dutch (Belgium)
        - Turkish – F
        - Turkish – Q
- **SoftKeyboard:** This option allows the user to select the keyboard layout. It will show the dialog

similar to Windows On-screen keyboard. If the client and host languages are different, the user can select the soft keyboard that corresponds to the host keyboard layout from the list shown in JViewer, and use it to avoid typo errors.

- **List of Soft Physical Keyboard languages supported:**
  - English –US
  - English – UK
  - Spanish
  - French
  - German (Germany)
  - Italian
  - Danish
  - Finnish
  - German (Switzerland)
  - Norwegian (Norway)
  - Portuguese (Portugal)
  - Swedish
  - Hebrew
  - French (Belgium)
  - Dutch (Netherland)
  - Dutch (Belgium)
  - Russian (Russia)
  - Japanese (QWERTY)
  - Japanese (Hiragana)
  - Japanese (Katakana)
  - Turkish – F
  - Turkish – Q

Video Record Menu:

- **Start Record:** Click this button to start recording the screen.
- **Stop Record:** Click this button to stop the recording.
- **Record Settings:** Click this button to open the Record Settings window to configure the settings.


Video Record

Video Length 20 Seconds

Video to be Saved

C:\Users\Admin

☑ Normalized video resolution to 1024 X 768.

This might reduce the video quality!

- **Video Length:** To specify the value for video length.
- **Video to be Saved:** To specify the location where to save the video file.
- **Normalized video resolution to 1024 X 768:** Enable this feature that host video will be scaled to 1024 x 768 in the recorded video file.
- **OK:** Click this button to save the configured settings.
- **Cancel:** Click this button to leave this window without saving the settings.

Power Menu:

- **Reset Server:** Reboot the system without powering off (warm boot).
- **Immediate Shutdown:** To perform Power OFF Immediately.
- **Orderly Shutdown:** To Power OFF the server in proper order.
- **Power On Server:** To Power ON the server.
- **Power Cycle Server:** To first power off, and then reboot the system (cold boot).

Active Users Menu:

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

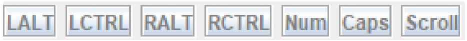
Help Menu:

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

Quick Buttons:

- ▶: This quick button is used to play the Console Redirection after being paused.
- ⏸: This quick button is used to pause the Console Redirection.
- ⛶: This quick button is used to view the Console Redirection in full screen mode.
- 💿: This quick button is used to open the CD/DVD window of the Virtual Media application.
- 🖴: This quick button is used to open the Hard Disk/USB window of the Virtual Media application.
- 🖱: This quick button is used to show or hide the mouse cursor on the remote client system.
- ⌨: This quick button is used to open a soft keyboard on the Console Redirection window.
- 🎥: This quick button is used to start video recording.
- ⌨: This quick button is used to display the available hotkeys.
- 👤: This quick button indicates the active users.
- 🖥 🖥 : This quick button indicates the current host monitor status. If the icon is in green color then the host monitor is unlocked. If the icon is in red color then the host monitor is locked. Clicking the button to change the monitor status.
- ⏻ ⏻: This quick button indicates the current server power status. If the icon is in green color, the server power status is powered on. If the icon is in red color, the server power status is powered off. Click this button to toggle immediate power off/power on the host.

Status Bar Buttons:

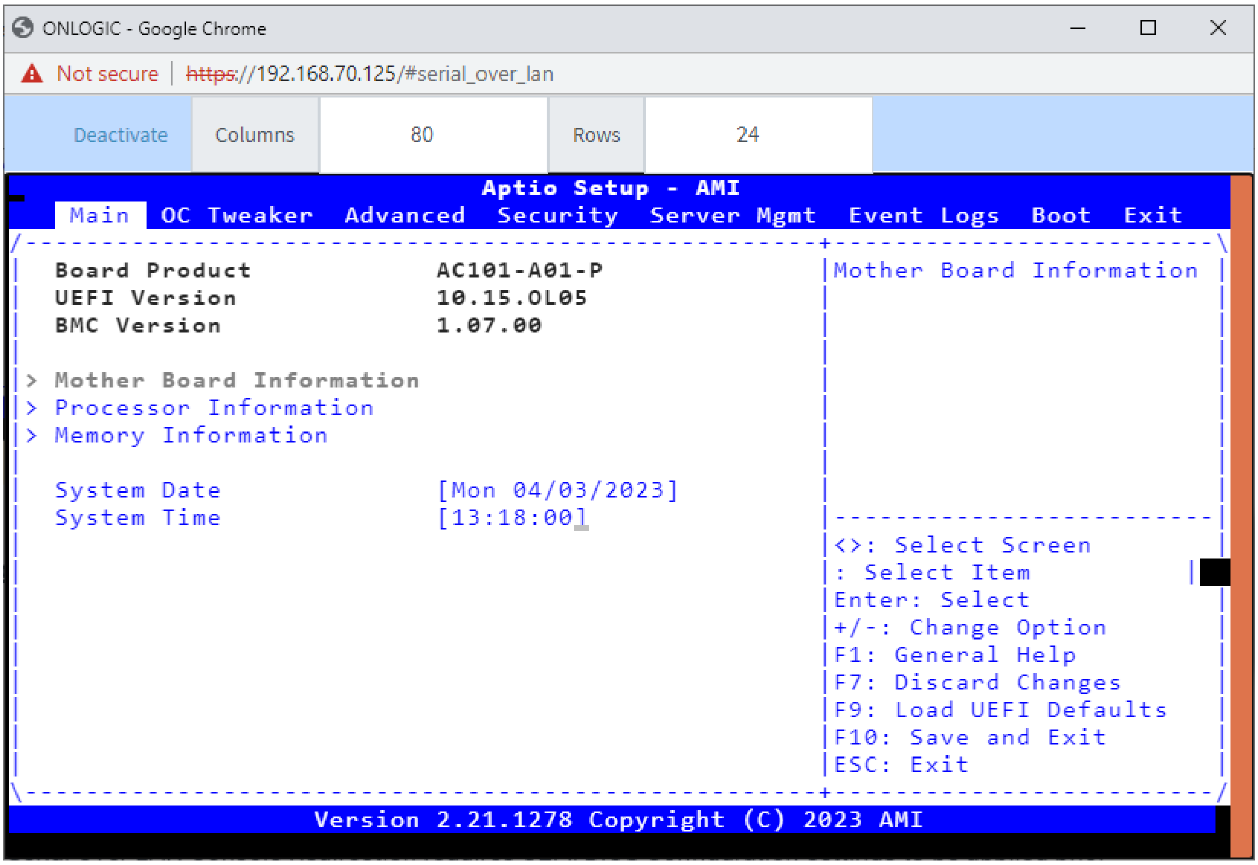
- 

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

6.11.3 - Serial Over LAN

Serial Over LAN (SOL) is a mechanism that enables the input and output of the serial port for a managed system to be redirected over IP.

In this feature, Serial data is transmitted to HTML5 Web UI through websocket.



```
                        Aptio Setup - AMI
  Main  OC Tweaker  Advanced  Security  Server Mgmt  Event Logs  Boot  Exit
/-----------------------------------------------------+--------------------------\
|  Board Product              AC101-A01-P              |Mother Board Information |
|  UEFI Version               10.15.OL05               |                         |
|  BMC Version                1.07.00                  |                         |
|                                                      |                         |
|> Mother Board Information                            |                         |
|> Processor Information                               |                         |
|> Memory Information                                  |                         |
|                                                      |                         |
|  System Date                [Mon 04/03/2023]         |                         |
|  System Time                [13:18:00]               |-------------------------|
|                                                      |<>: Select Screen        |
|                                                      |: Select Item            |
|                                                      |Enter: Select            |
|                                                      |+/-: Change Option       |
|                                                      |F1: General Help         |
|                                                      |F7: Discard Changes      |
|                                                      |F9: Load UEFI Defaults   |
|                                                      |F10: Save and Exit       |
|                                                      |ESC: Exit                |
\-----------------------------------------------------+--------------------------/
                Version 2.21.1278 Copyright (C) 2023 AMI
```

Configuration Menu:

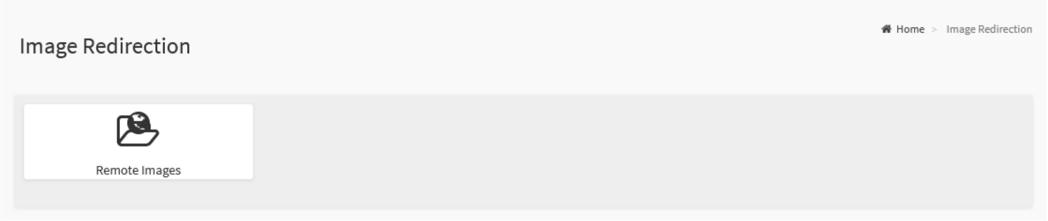
- **Deactivate:** Click Deactivate button to stop the SOL session.
- **Columns:** Adjust the Column size.
- **Rows:** Adjust the Row size.

Note: Serial Over LAN Console Redirection requires UEFI/BIOS Configuration settings to be applied prior to use. Ensure that SOL Console Redirection is Enabled in BIOS settings before activating the Serial Over LAN feature.

To enable SOL Console Redirection from UEFI System Setup, enter System Setup using the <F2> or <Del> keys on boot, then go to Advanced → Serial Port Console Redirection → SOL → Console Redirection and set to Enabled.

6.12- Image Redirection

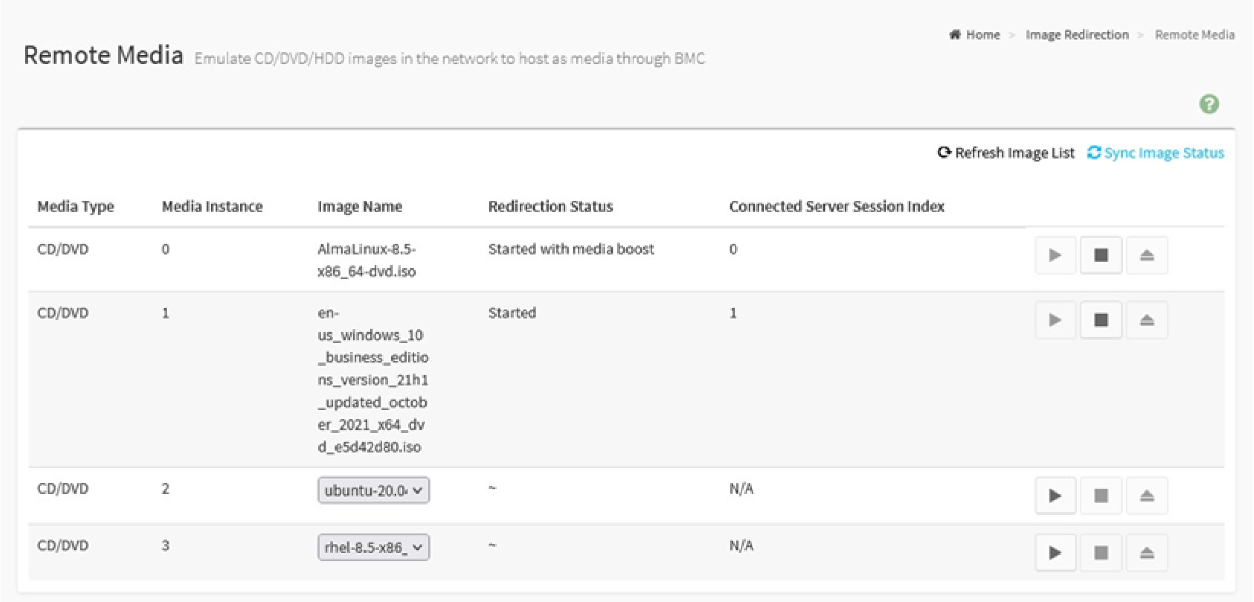
The Image Redirection page provides the feature tab for users to access and modify the state of remote image redirection.



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

6.12.1 - Remote Images

The Remote Images page provides the ability for users to view the configured images on BMC and modify the state.



Remote Media Emulate CD/DVD/HDD images in the network to host as media through BMC

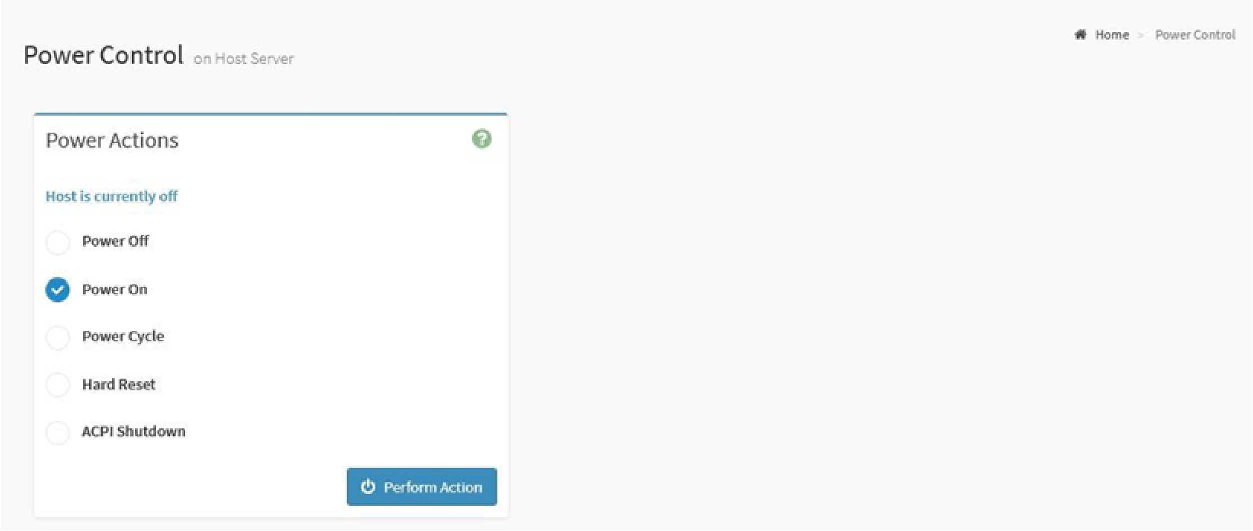
Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index	
CD/DVD	0	AlmaLinux-8.5-x86_64-dvd.iso	Started with media boost	0	▶ ■ ⏏
CD/DVD	1	en-us_windows_10_business_editions_version_21h1_updated_october_2021_x64_dvd_e5d42d80.iso	Started	1	▶ ■ ⏏
CD/DVD	2	ubuntu-20.0	~	N/A	▶ ■ ⏏
CD/DVD	3	rhel-8.5-x86_	~	N/A	▶ ■ ⏏

Configurable/Informational Fields:

- **Media Type:** The type Media devices supported for Active Redirections.
- **Media Instance**: The number of Media devices supported for Active Redirections.
- **Image Name:** The name of Media devices supported image for Active Redirections.
- **Redirection Status:** The status of the image redirection for Active Redirections.
- **Connected Server Session Index:** Indicates the number of connected server session index.
- **Play:** Click Play (▶) button to redirect the selected image.
- **Stop:** Click Stop (■) button to stop the remote image redirection.
- **Clear:** Click Clear (⏏) button to clear the selected image from the BMC.
- **Refresh Image List:** Click Refresh Image List (⟳) to get the latest list of Images from the Remote storage server.
- **Sync Image Status:** Click Sync Image Status (⟳) to Turn on/off the redirection status of Images from the BMC.

6.13 - Power Control

The Power Control page provides the ability for users to view and configure the power state of the host.



Power Control on Host Server

Home > Power Control

Power Actions

Host is currently off

○ Power Off

● Power On

○ Power Cycle

○ Hard Reset

○ ACPI Shutdown

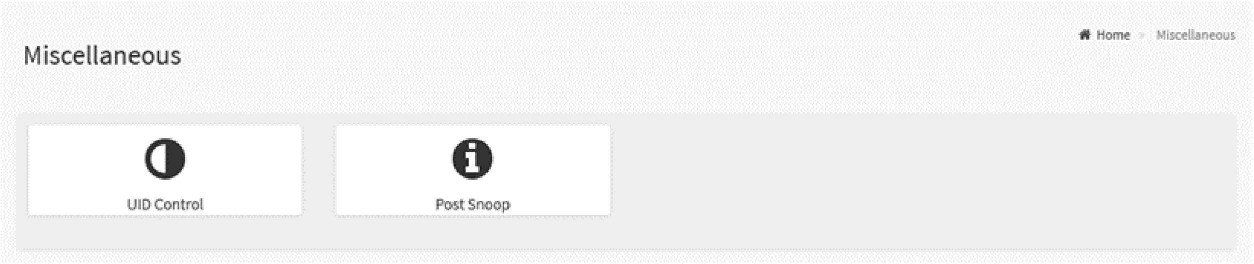
Configurable Fields:

- **Power Off:** Select to immediately power off the host.
- **Power On:** Select to power on the host.
- **Power Cycle:** Select to select this option, the host will first power off, and then reboot the host (cold boot).
- **Hard Reset:** Select to reboot the host without powering off (warm boot).
- **ACPI Shutdown:** Select to initiate operating system shutdown prior to the shutdown.
- **Perform Action:** Execute the selected power action.

6.14 - Miscellaneous

The Miscellaneous page provides links to pages where users can configure and monitor the following:

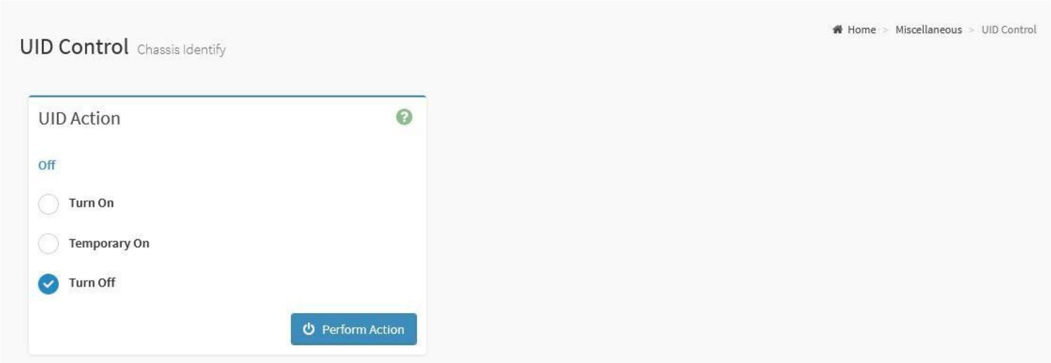
- UID Control
- Post Snoop



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

6.14.1 - UID Control

UID Control page provides the ability for users to configure Unit ID LED, which is used to assist with physical identification of the server system’s location.



UID Control Chassis Identify

UID Action

Off

○ Turn On

○ Temporary On

● Turn Off

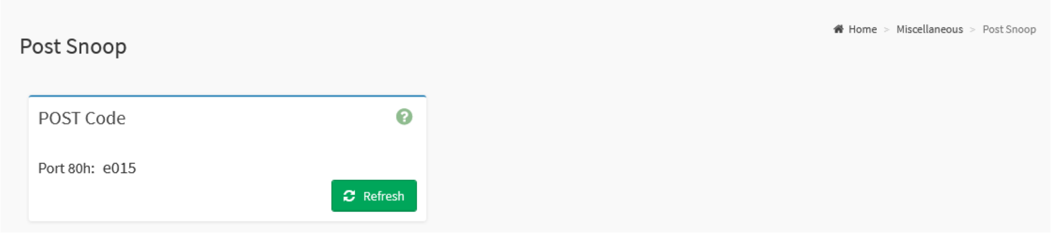
<u>Configurable Fields:</u>

- **UID Action**
    - **Status**: Indicates current UID status.
- **Turn On:** To turn on UID LED.
- **Temporary On:** To temporary turn on UID LED (15 sec blink).
- **Turn Off:** To turn off the UID LED.
- **Perform Action:** Click Perform Action button to executing selected UID action

.

6.14.2 - Post Snoop

The Post Snoop page provides users the ability to view the latest BIOS POST code which was snooped by BMC.



Port 80h: e015

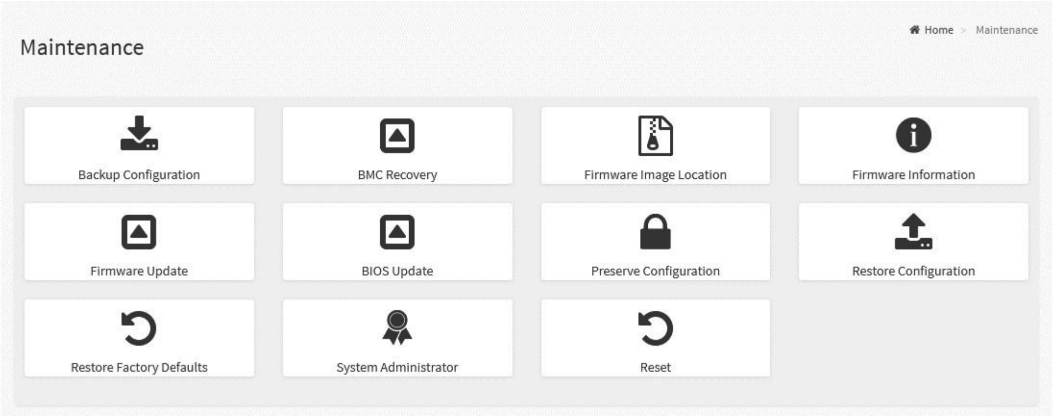
Informational Fields:

- **Port 80h:** Indicates the latest BIOS POST code.
- **Refresh:** Click the Refresh button to update the latest BIOS POST code.

6.15 - Maintenance

The Maintenance page provides the ability for users to perform the following maintenance tasks:

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

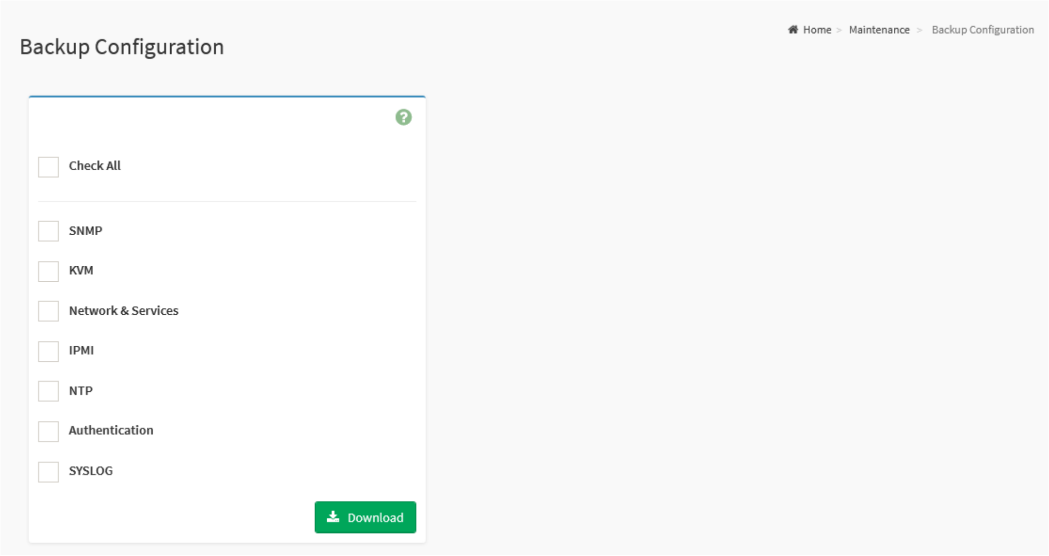


The details about each feature are listed in the following subsections.

6.15.1 - Backup Configuration

Backup Configuration page provides the ability for users to select the specific configuration items to be backed up and downloaded to a local client.

Note: Backup Configurations may only be restored to systems from which they were originally taken. Backup Configurations are not intended to be applied to different systems, even of the same type and configuration.



Backup Configuration

Home > Maintenance > Backup Configuration

□ Check All

□ SNMP

□ KVM

□ Network & Services

□ IPMI

□ NTP

□ Authentication

□ SYSLOG

Download

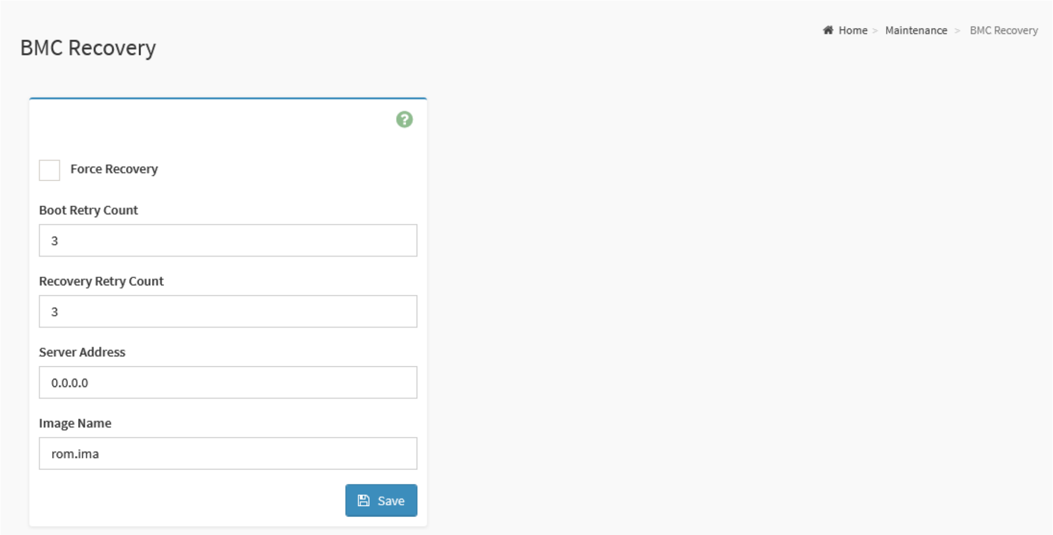
Configurable Fields:

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

6.15.2 - BMC Recovery

The BMC Recovery page provides the ability for users to configure the BMC Recovery settings.

The BMC Auto-Recovery is a mechanism to flash and boot the recovery image when the primary image in the SPI-ROM is corrupted or fails to boot. It provides an additional failover mechanism for BMC firmware.



BMC Recovery

□ Force Recovery

Boot Retry Count: 3

Recovery Retry Count: 3

Server Address: 0.0.0.0

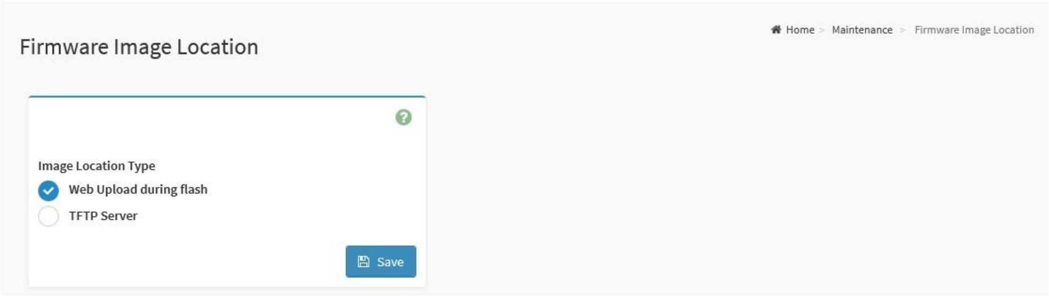
Image Name: rom.ima

Configurable Fields:

- **Force Recovery:** Check this option to start auto-recovery immediately at the next reboot.
- **Boot Retry Count:** Specific the number of retries to reset the BMC and this count ranges from 1 to 5.
- **Recovery Retry Count:** Specific the number of retries to recover firmware image during the recovery process and This count ranges from 1 to 5.
- **Server Address:** Address of the server where the firmware image is stored.
- **Image Name:** To edit the default recovery image name on TFTP server.
- **Save:** Save the configured settings

6.15.3 - Firmware Image Location

The Firmware Image Location page provides the ability for users to configure the image transfer protocol for transferring the firmware image onto BMC.



Firmware Image Location

Image Location Type

● Web Upload during flash

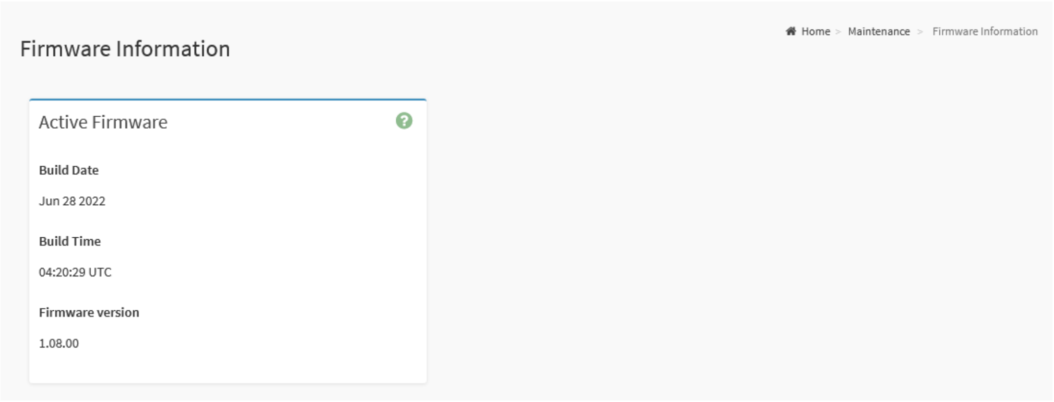
○ TFTP Server

Configurable Fields:

- **Image Location Type:** Select the type of transfer the firmware image into the BMC 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:** Specify the address of the TFTP server where the firmware image is 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:** Save the configured settings.

6.15.4 - Firmware Information

The Firmware Information page provides the current BMC firmware information.



Firmware Information

Active Firmware

Build Date

Jun 28 2022

Build Time

04:20:29 UTC

Firmware version

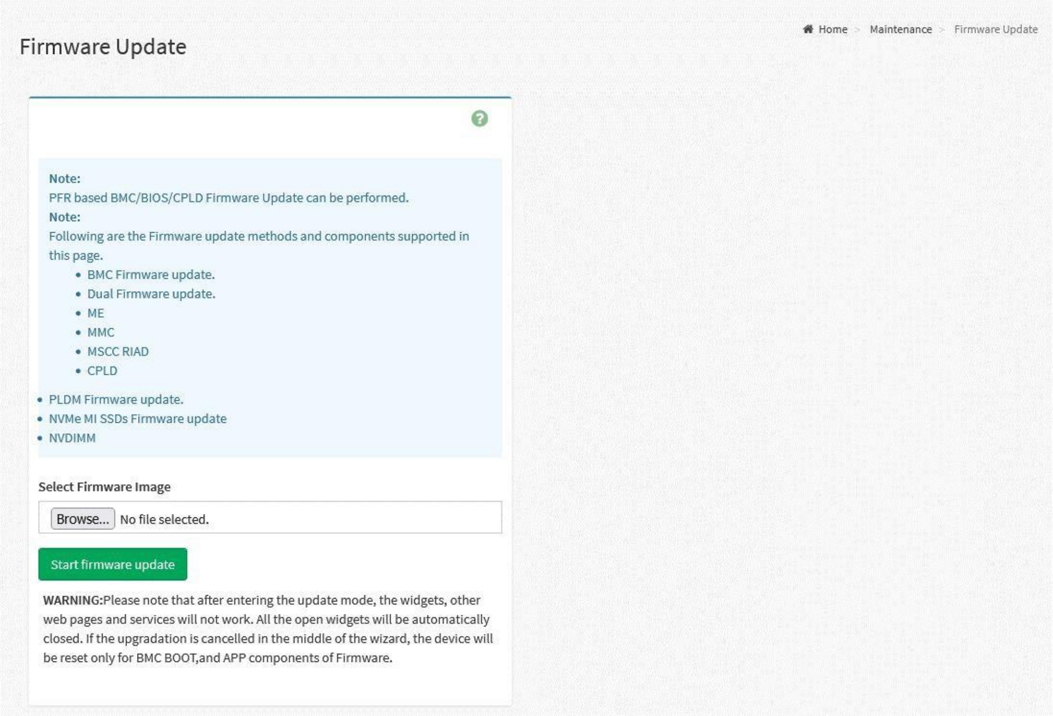
1.08.00

Informational Fields:

- **Build Date:** Indicate the build date of the active BMC image.
- **Build Time:** Indicate the build time of the active BMC image.
- **Firmware Version:** Indicate the firmware version of the active BMC image.

6.15.5 - Firmware Update

The Firmware Update page provides the option for users to update firmware through BMC web service. This is the location where BMC firmware updates are to be applied.



Firmware Update

Note:
PFR based BMC/BIOS/CPLD Firmware Update can be performed.
Note:
Following are the Firmware update methods and components supported in this page.

- BMC Firmware update.
- Dual Firmware update.
- ME
- MMC
- MSCC RIAD
- CPLD
- PLDM Firmware update.
- NVMe MI SSDs Firmware update
- NVDIMM

Select Firmware Image

Browse... No file selected.

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

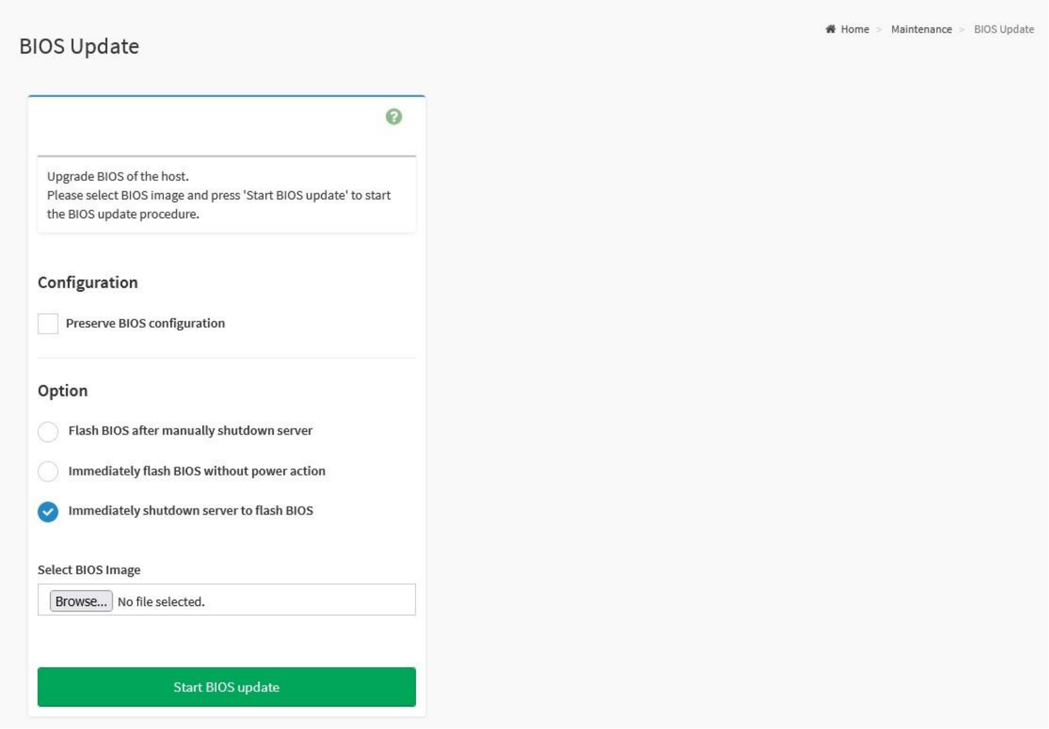
Configurable Fields:

- **Select Firmware Image:** 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 start the firmware update process.

Note: To update firmware, follow the prompts on the page. Firmware images will first be uploaded to the BMC and user's will be prompted prior to initiating the firmware flashing procedure.

6.15.6 - BIOS Update

The BIOS Update page provides the option for users to update host BIOS through BMC web service.



BIOS Update

Upgrade BIOS of the host.
Please select BIOS image and press 'Start BIOS update' to start the BIOS update procedure.

Configuration

□ Preserve BIOS configuration

Option

○ Flash BIOS after manually shutdown server

○ Immediately flash BIOS without power action

● Immediately shutdown server to flash BIOS

Select BIOS Image

Browse... No file selected.

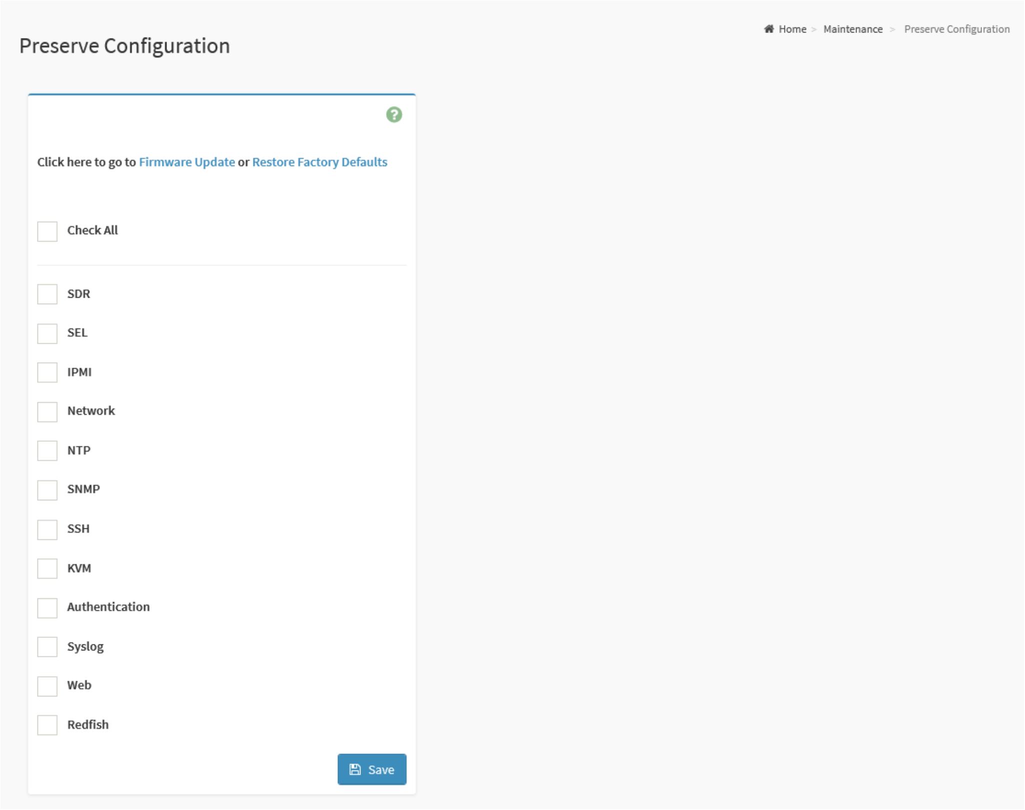
Configurable Fields:

- **Configuration**
    - **Preserve BIOS configuration:** Click this option to preserve current BIOS configuration settings.
- **Option**
    - **Flash BIOS after manually shutdown server:** Select this option to wait for manually shutdown server to flash BIOS firmware image.
    - **Immediately flash BIOS without power action:** Select this option to flash BIOS firmware image immediately.
    - **Immediately shutdown server to flash BIOS:** Select this option to shutdown server immediately to flash BIOS firmware image.
- **Select BIOS Image:** Click the Browse button to open file upload window, then select the updated BIOS firmware image file.
- **Start BIOS Update:** Click Start BIOS Update button to start the BIOS update process.

Note: To update firmware, follow the prompts on the page. Firmware images will first be uploaded to the BMC and user's will be prompted prior to initiating the firmware flashing procedure.

6.15.7 - Preserve Configuration

The Preserve Configuration page provides the ability for users to configure the settings to be preserved when flashing BMC firmware images.

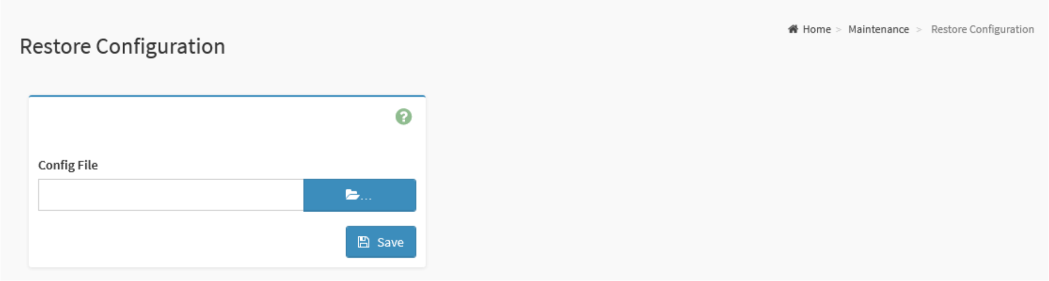


Configurable Fields:

- **Check All:** Check this option to select all configuration items listed on the page.
- **SDR:** Check this option to preserve the SDR settings.
- **SEL:** Check this option to preserve the SEL settings.
- **IPMI:** Check this option to preserve the IPMI settings.
- **Network:** Check this option to preserve the Network settings.
- **NTP:** Check this option to preserve the NTP settings.
- **SNMP:** Check this option to preserve the SNMP settings.
- **SSH:** Check this option to preserve the SSH settings.
- **KVM:** Check this option to preserve the KVM settings.
- **Authentication:** Check this option to e preserve the Authentication settings.
- **Syslog:** Check this option to preserve the Syslog settings.
- **Web:** Check this option to preserve the Web settings.
- **Redfish:** Check this option to preserve the Redfish settings.
- **Save:** Save the configured settings.

6.15.8 - Restore Configuration

The Restore Configuration page provides the option for users to restore configuration settings through BMC web service with the backup file created from the Backup Configuration page.

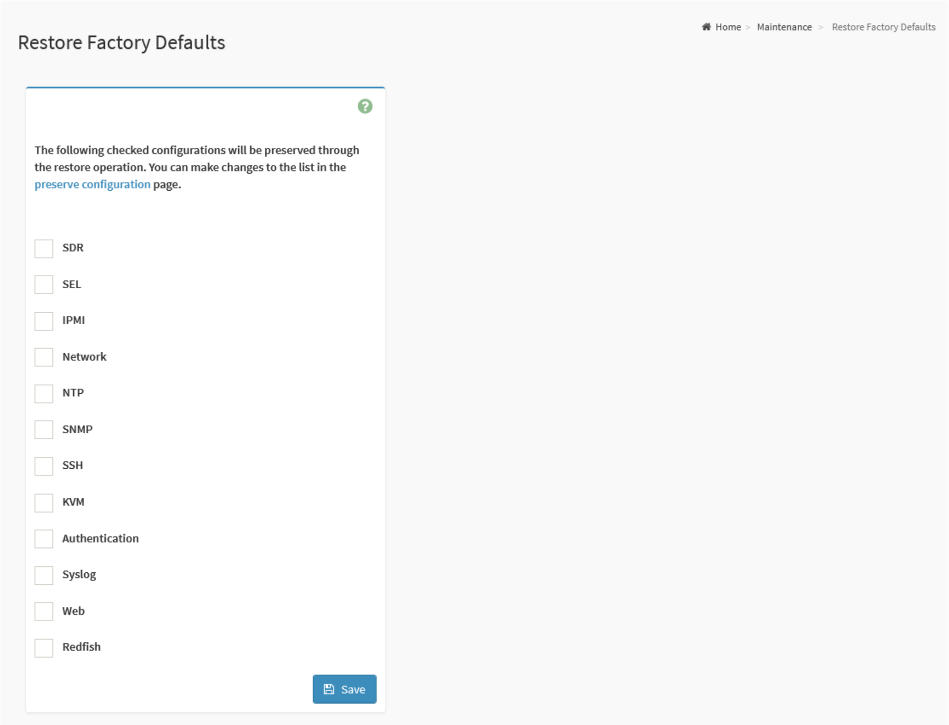


Configurable Fields:

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

6.15.9 - Restore Factory Defaults

The Restore Factory Defaults page provides the ability for users to modify the configuration settings that are preserved during a restoration of factory defaults.



Restore Factory Defaults

The following checked configurations will be preserved through the restore operation. You can make changes to the list in the preserve configuration page.

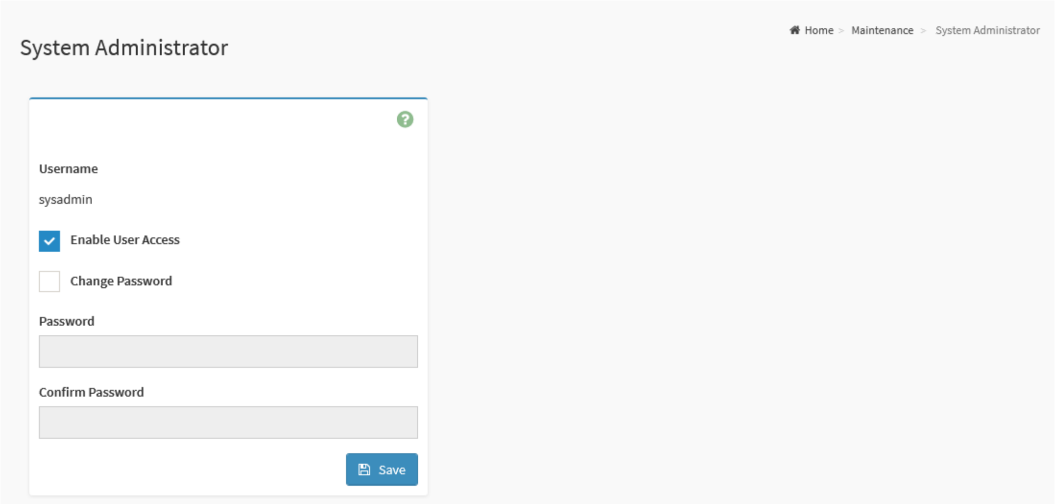
□ SDR
□ SEL
□ IPMI
□ Network
□ NTP
□ SNMP
□ SSH
□ KVM
□ Authentication
□ Syslog
□ Web
□ Redfish

Configurable Fields:

- **SDR:** Check this option to preserve the SDR settings during the restore factory defaults process.
- **SEL:** Check this option to preserve the SEL settings during the restore factory defaults process.
- **IPMI:** Check this option to preserve the IPMI settings during the restore factory defaults process.
- **Network:** Check this option to preserve the Network settings during the restore factory defaults process.
- **NTP:** Check this option to preserve the NTP settings during the restore factory defaults process.
- **SNMP:** Check this option to preserve the SNMP settings during the restore factory defaults process.
- SSH: Check this option to preserve the SSH settings during the restore factory defaults process.
- **KVM**: Check this option to preserve the KVM settings during the restore factory defaults process.
- **Authentication:** Check this option to preserve the Authentication settings during the restore factory defaults process.
- **Syslog:** Check this option to preserve the Syslog settings during the restore factory defaults process.
- **Web:** Check this option to preserve the Web settings during the restore factory defaults process.
- **Redfish:** Check this option to preserve the Redfish settings during the restore factory defaults process.
- **Save:** To perform the restore factory defaults process with configured settings.

6.15.10 - System Administrator

The System Administrator page provides the ability for users to configure the System Administrator settings.



System Administrator

Username
sysadmin

☑ Enable User Access

□ Change Password

Password

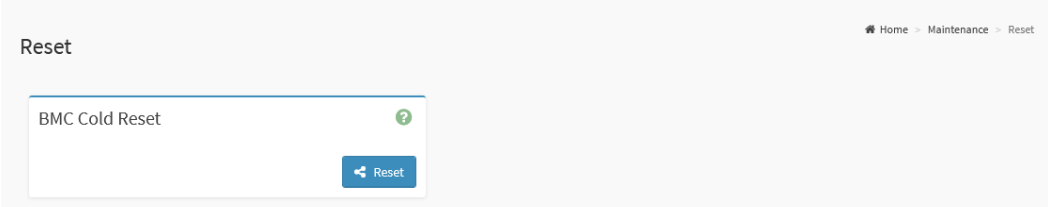
Confirm Password

Configurable Fields:

- **Username:** Indicates the username of System Administrator.
- **Enable User Access:** Click this option to enable user access for the system administrator.
- **Change Password:** Click this option to enable change password.
- **Password:** The new password for the system administrator account.
- **Confirm Password:** The same new password for the system administrator account to confirm.
- **Save**: Save the configured settings.

6.15.11 - Reset

The Reset page provides the option for users to perform a cold reset of the Baseboard Management Controller.



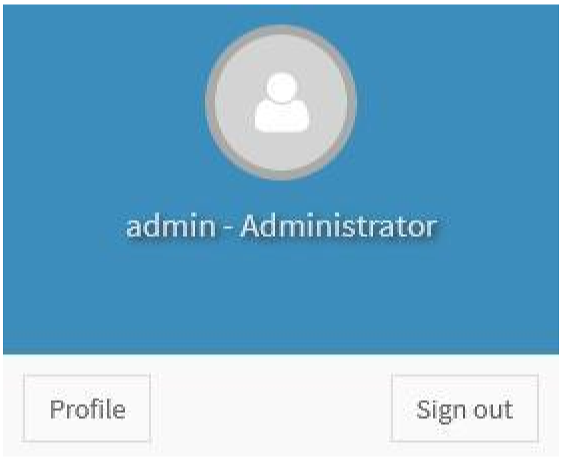
Configurable Fields:

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

6.16 - Sign Out

It is always recommended to ensure that inactive users Sign Out of the BMC WebUI.

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



7.0 - Intelligent Platform Management Interface (IPMI)

This section provides an overview of the IPMI commands that are supported by the Axial Edge Server BMC, along with their descriptions and usage instructions.

7.1 - IPMI Version

The Axial Edge Server BMC is compatible with the IPMI 2.0 specification.

For additional IPMI 2.0 specification details, please refer to the following:
https://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ipmi-second-gen-interface-spec-v2-rev1-1.pdf

7.2 - Using IPMItool

IPMItool is a command-line interface tool that allows system administrators to manage and monitor servers remotely (via network connectivity to the BMC) or locally (via KCS interface).

For additional public information pertaining to IPMItool, please refer to the following:
https://github.com/ipmitool/ipmitool

7.2.1 - Using IPMItool locally (KCS Interface)

This section will briefly outline how to use IPMItool from an OS that is running on an Axial Edge Server. It should be noted that IPMItool can be compiled to run on Windows, the ability to support local ipmitool command execution via the KCS interface may not operate properly.

1. Ensure that the ipmitool utility is installed by running the following command:

   ```
   >ipmitool -V
   ipmitool version 1.8.19
   ```

   Note: If not installed, make sure to install it using the appropriate procedure for the OS.

2. Ensure that the KCS interface is enabled within your UEFI System Setup menu.

   Note: The KCS interface is typically enabled by default.

3. Execute an example ipmitool command locally against the BMC.

   ```
   > ipmitool power status

   Chassis Power is on
   ```

7.2.2 - Using IPMItool remotely (Network Interface)

This section will briefly outline how to use IPMItool to query a network connected Axial Edge Server BMC from a remote client.

To execute IPMI commands against the BMC of a server remotely:

1. Ensure that your remote client has network connectivity to the BMC.
2. A **<BMC Host IP Address>** must be specified
3. A **<Username>** must be specified
4. A **<Password>** must be specified
5. The Username/Password must have appropriate credentials to perform IPMI commands.

Using the same example command (mc info) as above, but running the command from a remote client, the command would be as follows:

ipmitool -I lanplus -H **<BMC Host IP Address>** -U **<Username>** -P **<Password>** power status

```
e.g.
> ipmitool -I lanplus -H 192.168.70.125 -U admin -P mypassword power status

Chassis Power is on
```

7.3 - Common IPMItool Commands

Listed in the table below are some common IPMItool commands.

For the latest official IPMItool manpage, please refer to the following:

https://github.com/ipmitool/ipmitool/blob/master/doc/ipmitool.1.in

Command	**Description**
ipmitool lan print	Displays the current LAN configuration of the BMC (Baseboard Management Controller)
ipmitool power status	Displays the power status of the host system
ipmitool power on	Powers on the host system
ipmitool power off	Powers off the host system
ipmitool power reset	Performs a hard reset of the host system
ipmitool chassis status	Displays the current status of the chassis, including power, fans, and temperature sensors
ipmitool chassis power status	Displays the power status of the chassis
ipmitool chassis power on	Powers on the chassis

ipmitool chassis power off	Powers off the chassis
ipmitool chassis power reset	Performs a hard reset of the chassis
ipmitool sensor list	Displays a list of available sensors on the BMC
ipmitool sensor get	Displays the current reading of a specific sensor
ipmitool sel list	Displays the System Event Log (SEL)
ipmitool sel clear	Clears the System Event Log (SEL)

7.4 - Supported OEM IPMI Commands

This section provides the information of the OEM IPMI commands supported on BMC AST2600 controller of OnLogic mainboards.

The Network Function (NetFN) of OnLogic OEM IPMI Commands is shown in the following:

- NetFn: 0x3A

The supported OEM IPMI Commands are listed in the following:

- 0x52 – Master Write Read
- 0x67 – Get Boot Complete
- 0x82 – Set Sensor Monitor
- 0x83 – Get Sensor Monitor

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

7.4.1 - Master Write Read (0x67)

	Byte	Data Field
Request Data	1	I2C Bus
	2	Slave Address
	3	Read Count
	4:N	Data Write (Up to 50 Bytes)
Response Data	1	Completion Code
	2:N	Data Read

7.4.2 - Get Boot Complete (0x67)

	Byte	Data Field
Request Data	-	-
Response Data	1	Completion Code
	2	BMC Boot State 00h = BMC is booting 01h = BMC boot completed

7.4.3 - Set Sensor Monitor (0x82)

	Byte	Data Field
Request Data	1	Sensor Monitor Config 00h = Disable 01h = Enable
Response Data	1	Completion Code

7.4.4 - Get Sensor Monitor (0x83)

	Byte	Data Field
Request Data	-	-
Response Data	1	Completion Code
	2	Sensor Monitor Config 00h = BMC is booting 01h = BMC boot completed

End of Document