HPM-GNRDE

IPMI Setup User's Manual

1st Ed –18 April 2025

FCC Statement



THIS DEVICE COMPLIES WITH PART 15 FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE.

(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS "A" DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES.

THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS.

OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

Notice

This guide is designed for experienced users to setup the system within the shortest time. For detailed information, please always refer to the electronic user's manual.

Copyright Notice

Copyright © 2025 Avalue Technology Inc., ALL RIGHTS RESERVED.

No part of this document may be reproduced, copied, translated, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior written permission of the original manufacturer.

Trademark Acknowledgement

Brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Avalue Technology Inc. reserves the right to make changes, without notice, to any product, including circuits and/or software described or contained in this manual in order to improve design and/or performance. Avalue Technology assumes no responsibility or liability for the

use of the described product(s), conveys no license or title under any patent, copyright, or masks work rights to these products, and makes no representations or warranties that these products are free from patent, copyright, or mask work right infringement, unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Avalue Technology Inc. makes no representation or warranty that such application will be suitable for the specified use without further testing or modification.

Life Support Policy

Avalue Technology's PRODUCTS ARE NOT FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE PRIOR WRITTEN APPROVAL OF Avalue Technology Inc.

As used herein:

1. Life support devices or systems are devices or systems which, (a) are intended for surgical implant into body, or (b) support or sustain life and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in significant injury to the user.
2. A critical component is any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

A Message to the Customer

Avalue Customer Services

Each and every Avalue's product is built to the most exacting specifications to ensure reliable performance in the harsh and demanding conditions typical of industrial environments. Whether your new Avalue device is destined for the laboratory or the factory floor, you can be assured that your product will provide the reliability and ease of operation for which the name Avalue has come to be known.

Your satisfaction is our primary concern. Here is a guide to Avalue's customer services. To ensure you get the full benefit of our services, please follow the instructions below carefully.

Technical Support

We want you to get the maximum performance from your products. So if you run into technical difficulties, we are here to help. For the most frequently asked questions, you can easily find answers in your product documentation. These answers are normally a lot more detailed than the ones we can give over the phone. So please consult the user's manual

first.

To receive the latest version of the user's manual; please visit our Web site at:
www.avalue.com

Product Warranty

Avalue warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Avalue, or which have been subject to misuse, abuse, accident or improper installation. Avalue assumes no liability under the terms of this warranty as a consequence of such events. Because of Avalue's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If any of Avalue's products is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time, and freight. Please consult your dealer for more details. If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU type and speed, Avalue's products model name, hardware & BIOS revision number, other hardware and software used, etc.) Note anything abnormal and list any on-screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information available.
3. If your product is diagnosed as defective, obtain an RMA (return material authorization) number from your dealer. This allows us to process your good return more quickly.
4. Carefully pack the defective product, a complete Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Content

1. HARDWARE 7
1.1 SYSTEM SPEC 8
1.2 PLATFORM AND BMC COMPONENTS 9
1.3 I2C BLOCK DIAGRAM 10
1.4 I2CBUS ACCESS 11
2. WEB UI 13
2.1 Log in 14
2.2 HOME>DASH BOARD 16
2.3 HOME>SENSOR 17
2.4 HOME> FRU INFORMATION 19
2.5 HOME> LOGS & REPORTS 19
2.6 HOME> SETTINGS 22
2.7 HOME> REMOTE CONTROL 79
2.8 HOME>IMAGE REDIRECTION 81
2.9 HOME> POWER CONTROL 81
2.10 HOME> MAINTENANCE 84
2.11 HOME> SIGN OUT 93
APPENDIX-A BMC HARDWRE: AST2600 94
APPENDIX-B IPMI COMMANDS SUPPORT TABLE 97
APPENDIX-C IPMI OEM COMMANDS LIST 102
APPENDIX-D SENSOR TABLE 103
APPENDIX-E DEFAULT CONFIGURATION 108
APPENDIX-F FIRMWARE UPDATE 109
APPENDIX-G SMART FAN CONFIGURATION 126
APPENDIX-H SYSTEM EVENT LOG(SEL) 128
APPENDIX-I IPMI TO GET BIOS POST CODE 133
APPENDIX-J REMOTE CONTROL-Serial Over LAN 135
APPENDIX-K Dedicated vs Shared IPMI port 136

Glossary & Abbreviation

Glossary & Abbreviation	Explanation
BMC	Baseboard Management Controller, this is the common abbreviation for an IPMI Baseboard Management Controller
BMC	Integrated Baseboard Management Controller, this is the name for the 2nd generation of BMC hardware, we use AST2600 on Platform
IMM	Integrated Management Module, this means the same as BMC
IPMI	Intelligent Platform Management Interface, a standardized system management interface
IPMB	Intelligent Platform Management Bus, I2C based bus
SOL	Serial Over LAN, Host serial port traffic redirected over a LAN connection for remote control and management
SDR	Sensor Data Record, A data record that provides platform management sensor type, locations, event generation, and access information
Serial Port Sharing	Ability to share a serial connector between the BMC's serial controller and a system serial controller by using circuitry to allow it to be switched between the two
POST	Power On Self Test
OEM	Original Equipment Manufacturer
FRU	Field Replaceable Unit
VPD	Vital Product Data, this is the term given to system component manufacturing information such as, but not limited to, serial number and FRU part number
SEL	System Event Log
SMS	System Management Software
SMM	System Management Mode
NMI	Non Maskable Interrupt
SMI	System Management Interrupt
IERR	Internal Error. A signal from the Intel Architecture processors indicating an internal error condition
PERR	Parity Error. A signal on the PCI bus that indicates a parity error on the bus
SERR	System Error. A signal on the PCI bus that indicates a 'fatal' error on the bus
PECI	Platform Environment Control Interface
FRB	Fault Resilient Booting

1. HARDWARE

1.1 SYSTEM SPEC

Refer to Figure 1-1. System Block Diagram.

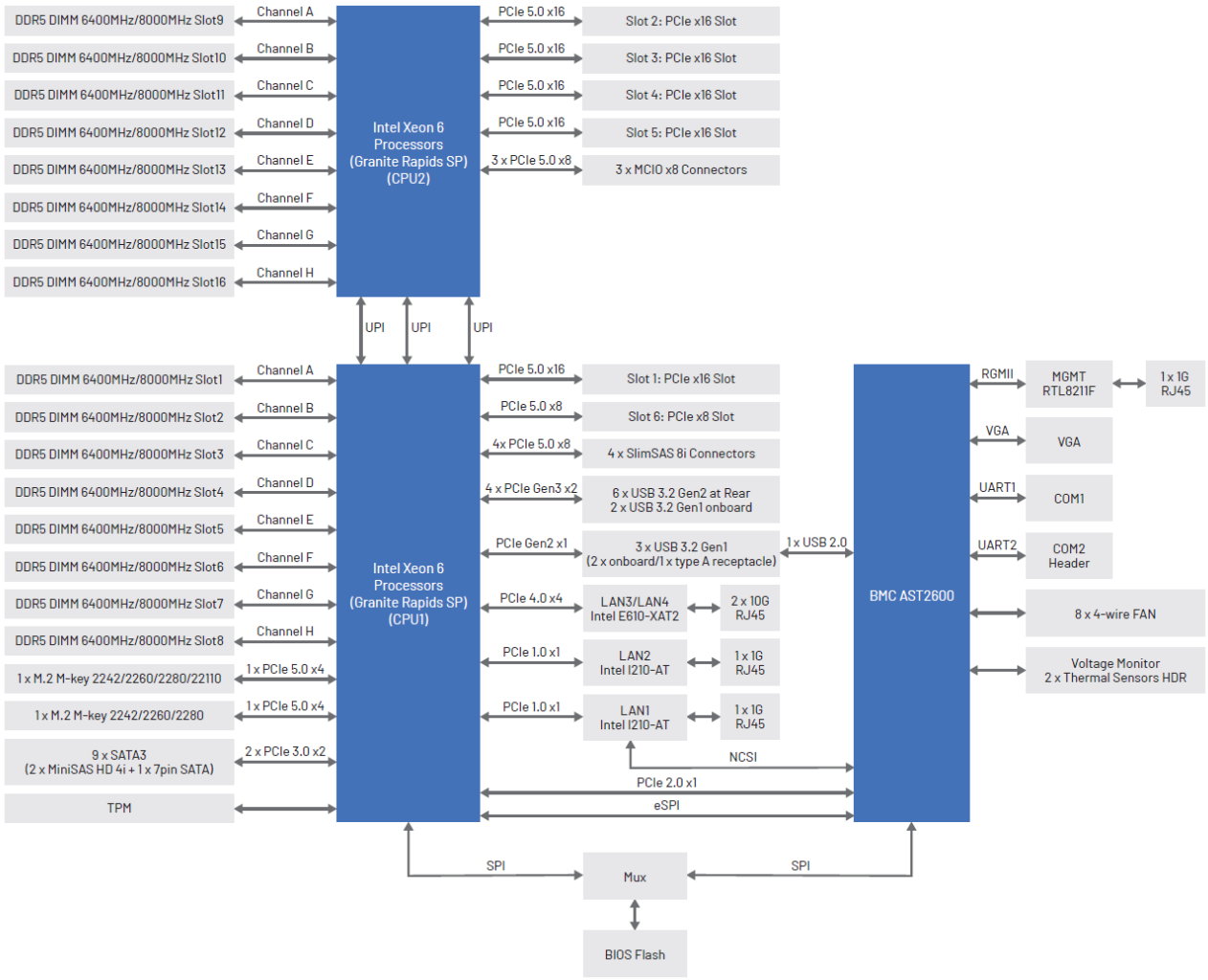


Figure 1-1 System block diagram

1.2 PLATFORM AND BMC COMPONENTS

Table 1-1 Main component related to BMC

Intel platform	CPU(Granite Rapids SP)
BMC	AST2600
Flash ROM	BIOS: 64MB BMC: 64MB
BMC Memory	512MB
BMC LAN	RGMII1: Dedicated PHY RTL8211F RMII3: Shared NIC I210AT
FRU device	CAT24C512
UART	UART1: System UART UART5: BMC console
LED	BMC Heartbeat LED On: The power is connected LED Blinks: BMC firmware is ready
Button	Power button System Reset button
CPLD	Intel 10M25DAF484C8G
Firmware Vendor of Code Base	AMI MegaRAC v13.8

1.3 I2C BLOCK DIAGRAM

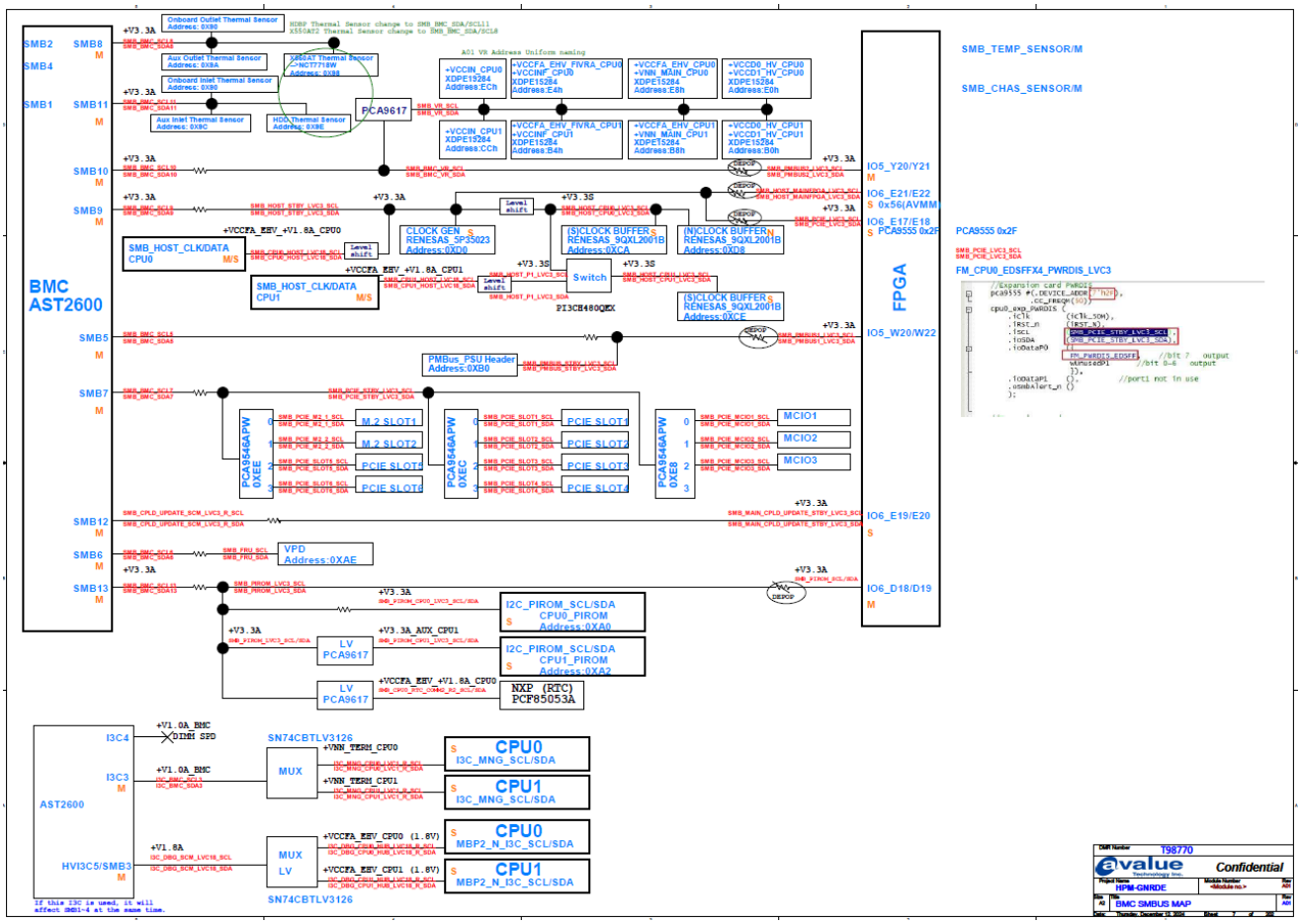


Figure 1-2 I2c block diagram

1.4 I2CBUS ACCESS

The BMC provides the Master Write-Read command via its interface with system software. The Master Write-Read command provides low-level access to non-intelligent devices on the IPMB, such as FRU SEEPROMs. The Master Write-Read command provides a subset of the possible I2C and SMBus operations that covers most I2C/SMBus-compatible devices. In addition to supporting non-intelligent devices on the IPMB, the Master Write-Read command also provides access to non-intelligent devices on Private Busses behind management controllers. The main purpose of this is to support FRU SEEPROMs on Private Busses.

Table 1-2 Master Write-Read Bus IDs

Physical Bus Number	Slave address	Remark	
5	0xB0	PMBus PSU Header	
6	0xAE	VPD	
7	0xEE	PCA9546APW Channel 0	M.2 SLOT 1
		PCA9546APW Channel 1	M.2 SLOT 2
		PCA9546APW Channel 2	PCIE SLOT 5
		PCA9546APW Channel 3	PCIE SLOT 6
	0xEC	PCA9546APW Channel 0	PCIE SLOT 1
		PCA9546APW Channel 1	PCIE SLOT 2
		PCA9546APW Channel 2	PCIE SLOT 3
		PCA9546APW Channel 3	PCIE SLOT 4
	0xE8	PCA9546APW Channel 0	MCIO 1
		PCA9546APW Channel 1	MCIO 2
		PCA9546APW Channel 2	MCIO 3
8	0x9A	AUX Outlet Thermal Sensor	
	0x98	X550AT Thermal Sensor	
9	0xD0	CLOCK GEN RENESAS 5P35023	
	0xD8	(N)CLOCK BUFFER RENESAS 9QXL2001B	
	0xCA	(S)CLOCK BUFFER RENESAS 9QXL2001B	
	0xCE	(S)CLOCK BUFFER RENESAS 9QXL2001B	
10	0xEC	VCCIN CPU0 XDPE 19284	
	0xE4	VCCFA EHV FIVRA CPU0 VCCINF CPU0 XDPE 15284	
	0xE8	VCCFA EHV CPU0	

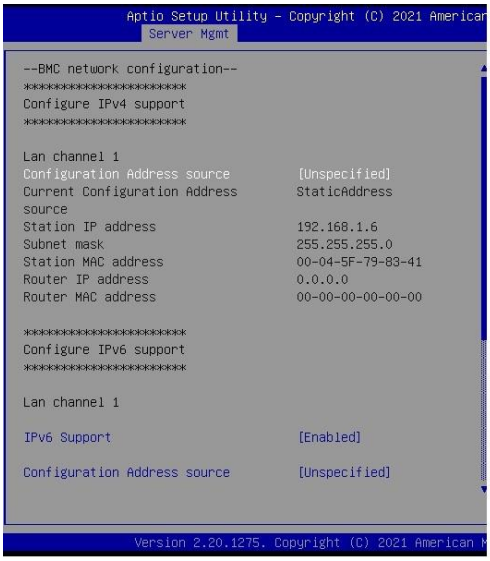
		VNN MAIN CPU0 XDPE 15284
	0xE0	VCCD0 HV CPU0 VCCD1 HV CPU0 XDPE 15284
	0xCC	VCCIN CPU1 XDPE 19284
	0xB4	VCCFA EHV FIVRA CPU1 VCCINF CPU1 XDPE 15284
	0xB8	VCCFA EHV CPU1 VNN MAIN CPU1 XDPE 15284
	0xB0	VCCD0 HV CPU1 VCCD1 HV CPU1 XDPE 15284
11	0x9C	Aux Inlet Thermal Sensor
	0x9E	HDD Thermal Sensor
13	0xA0	CPU0 PIROM
	0xA2	CPU1 PIROM

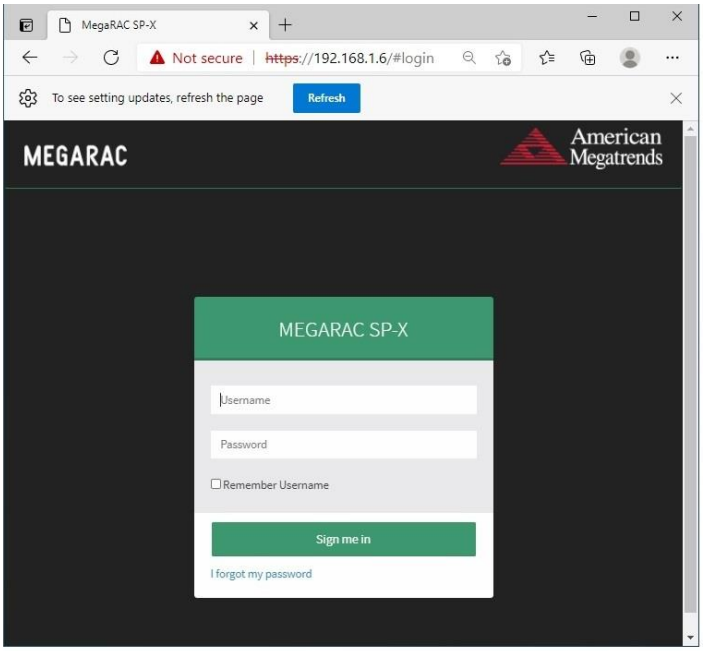
2. WEB UI

2.1 Log in

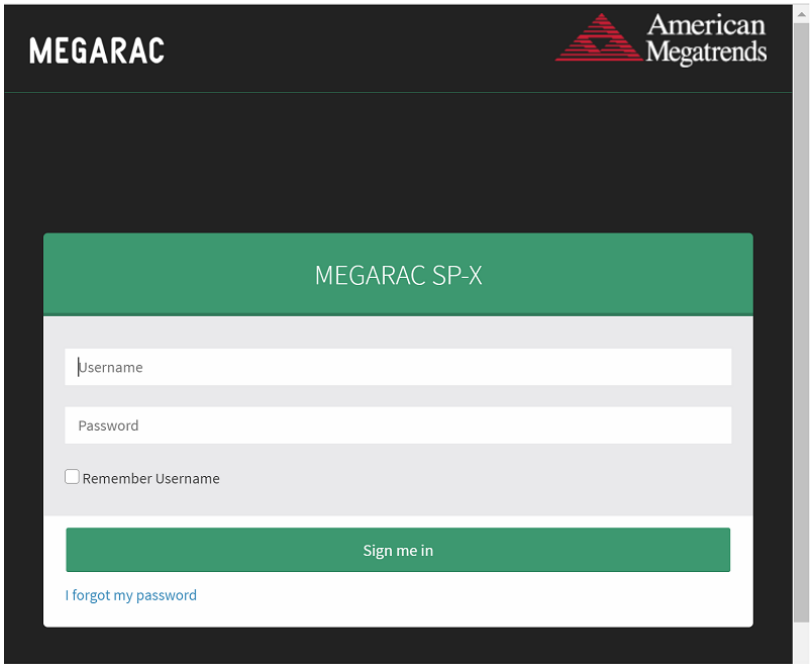
Power on your server and enter BIOS to configure BMC IP.

Prepare another client PC and open web browser to type: https://<BMC IP> then you will see the login page of BMC web UI.

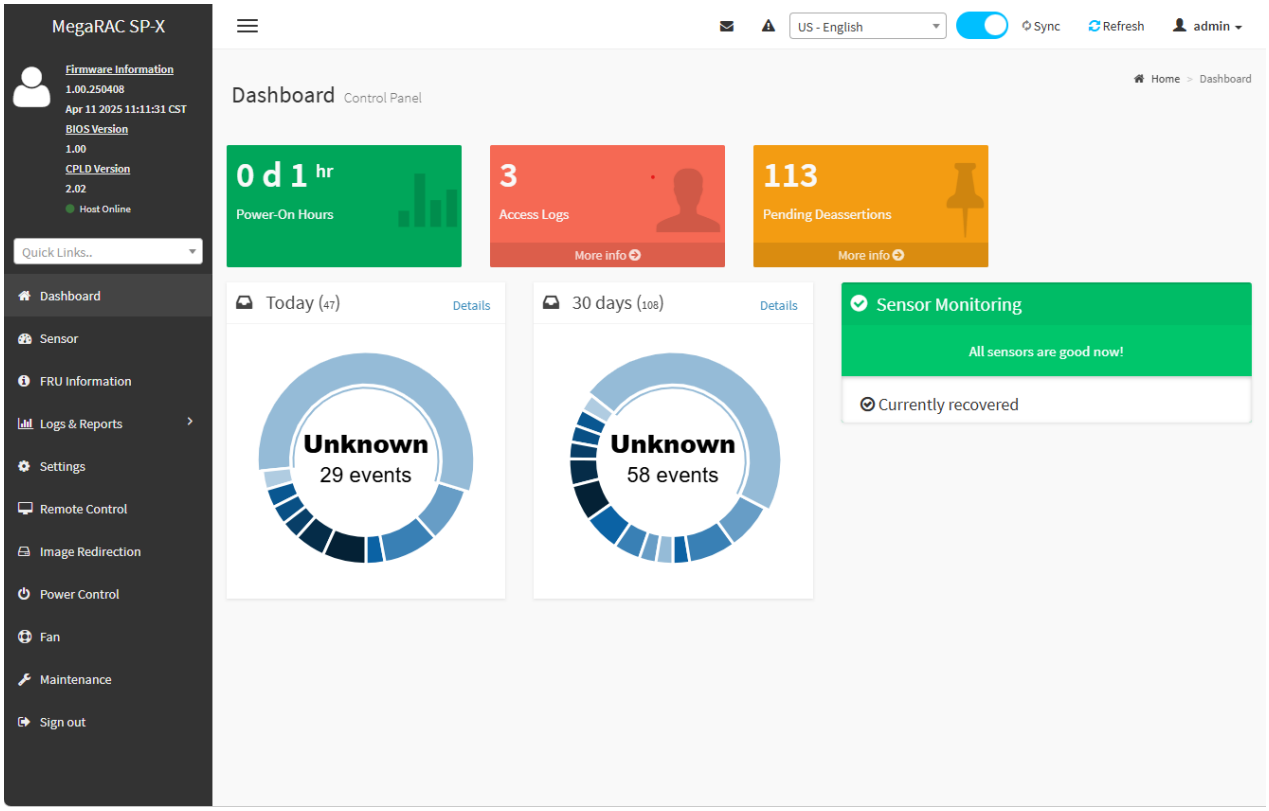








Login(default):admin ,password(default):admin



① Firmware Information : contains BMC/BIOS/CPLD firmware version

② Quick search bar : short-cut for the available menu and sub-menu pages

③ Menu Bar :

Menu Bar	Function
Dashboard	The Overall status of the system
Sensor	Realtime onboard sensor status.
FRU information	System information store in FRU
Logs & Reports	IPMI event log/system event log/audit log/video log
Settings	various settings related BMC
Remote control	Remote control through H5view or Jview
Image Redirection	Configure the images into BMC for redirection
Power Control	Power on/reset/shutdown system
Fan Control	Provide several method to control fan
Maintenance	Firmware image maintenance and factory default settings
Sign out	To log out from the Web UI

④ 

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

⚠	Click the icon to view the notification received
Sync	Click the icon to synchronize with Latest Sensor and Event Log updates.
Refresh	Click the icon or pressing key F5 to reload the current page.
admin	This option shows the logged-in user name and privilege. There are five kinds of privileges. User: Only valid commands are allowed. Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces. Administrator: All BMC commands are allowed. No Access: Login access denied. OEM: All OEM commands are allowed

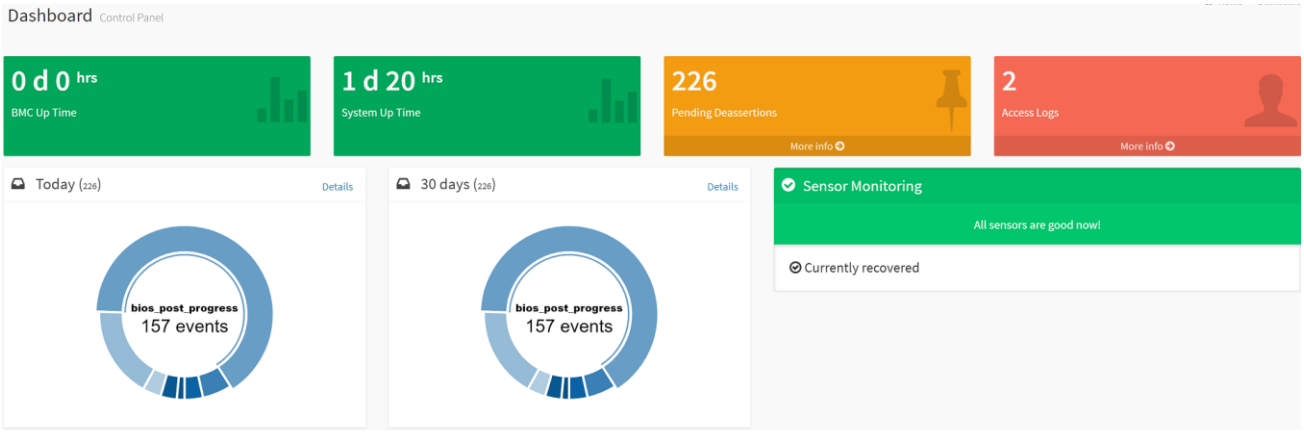
⑤ The location of the main page

⑥ Main page that show content and configuration options

Click this icon on some main page will show more detail explanation.

2.2 HOME>DASH BOARD

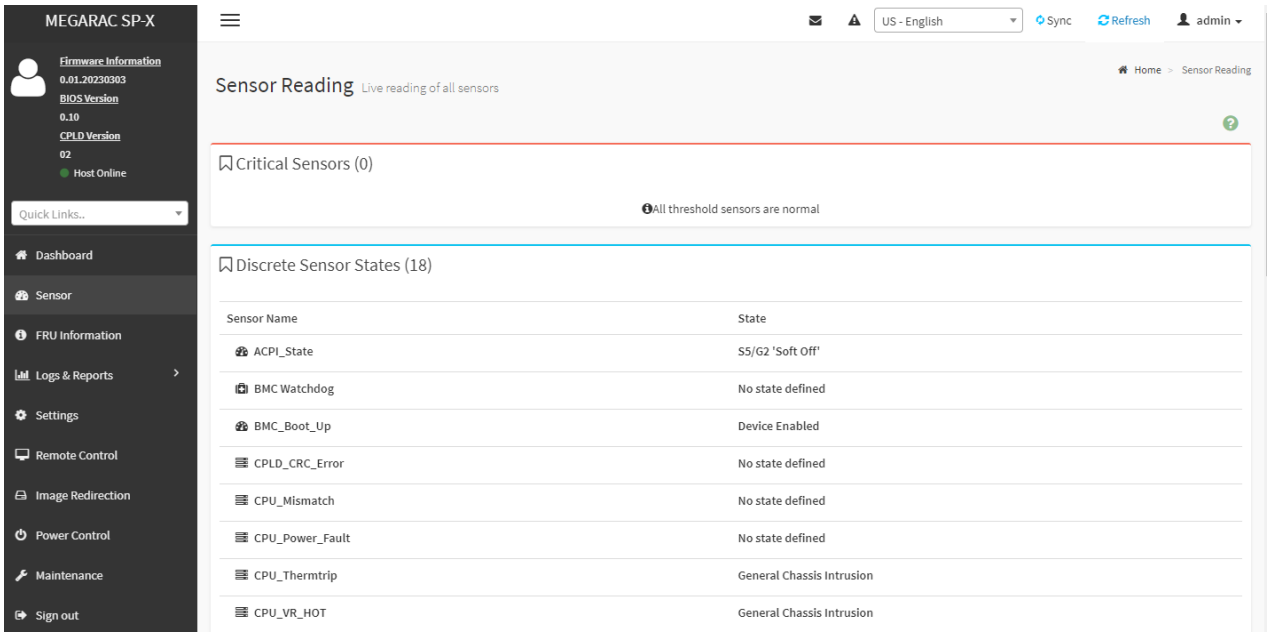
This page show overall information related BMC and status of device behind BMC



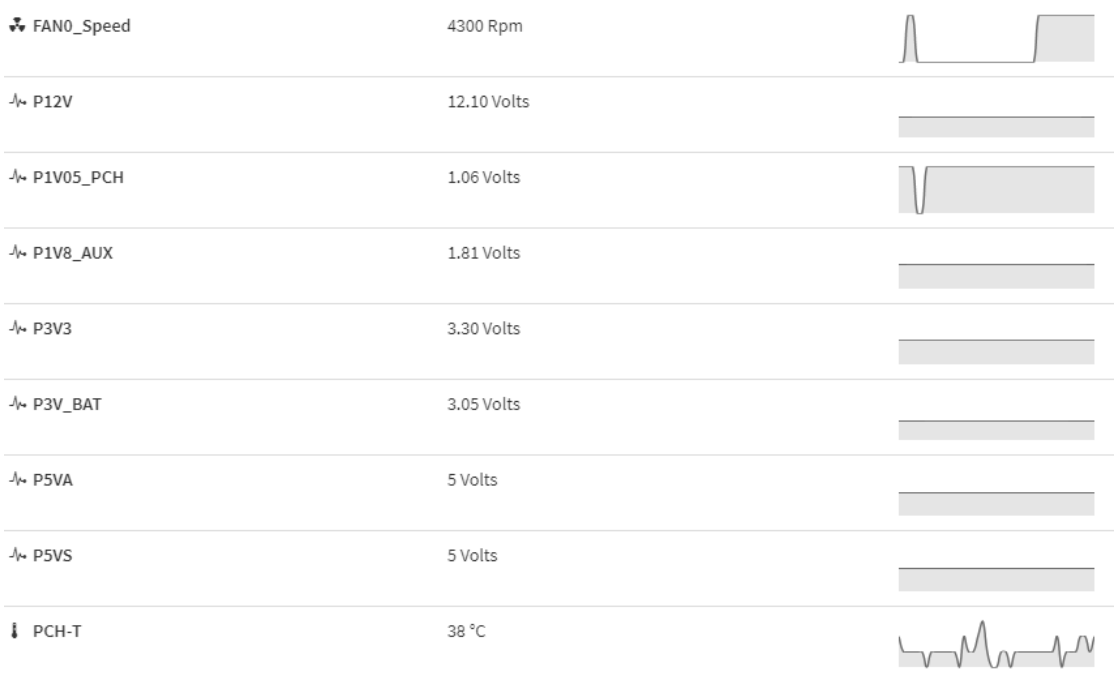
Item	Description
System Up Time	Timer that keep on accumulated while System on. Flash BMC f/w will reset this to zero.
Power-On Hours	Power-On Hours will keep on accumulated and will be reset to zero when you flash a new image.
Access Logs	Click more info to view the Audit Log page
Today	This list event logs occurred by the different sensors today, click details link to view the event logs
30 Days	This list event logs occurred by the different sensors within 30 days, click details link to view the event logs
Sensor Monitoring	Report the status of critical sensors.

2.3 HOME>SENSOR

This page show all of the sensors reading data in real-time , click on one of them to enter detail sensor page respectively.



Sensor Name	Reading	Behavior
CPU1-T	35 °C	
DIMM1-T	0 °C	
DIMM2-T	0 °C	
DIMM3-T	0 °C	
DIMM4-T	35 °C	
DIMM5-T	0 °C	
DIMM6-T	0 °C	
FAN0_Speed	4200 Rpm	
P12V	12.10 Volts	
P1V05_PCH	1.05 Volts	
P1V8_AUX	1.81 Volts	
P3V3	3.30 Volts	

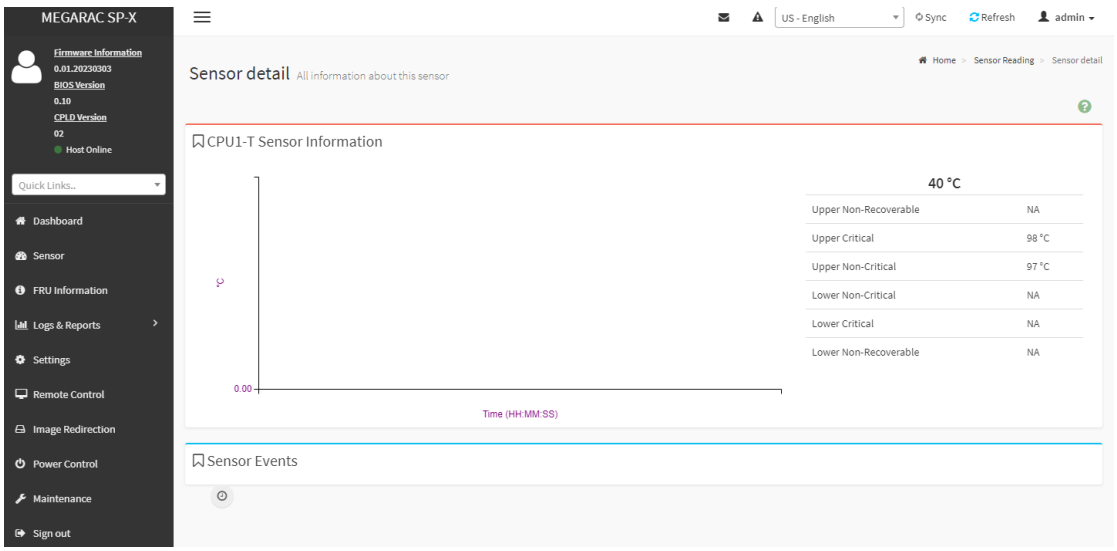


2.3.1 Home> Sensor Reading>Sensor detail

This page show the particular sensor thresholds contains

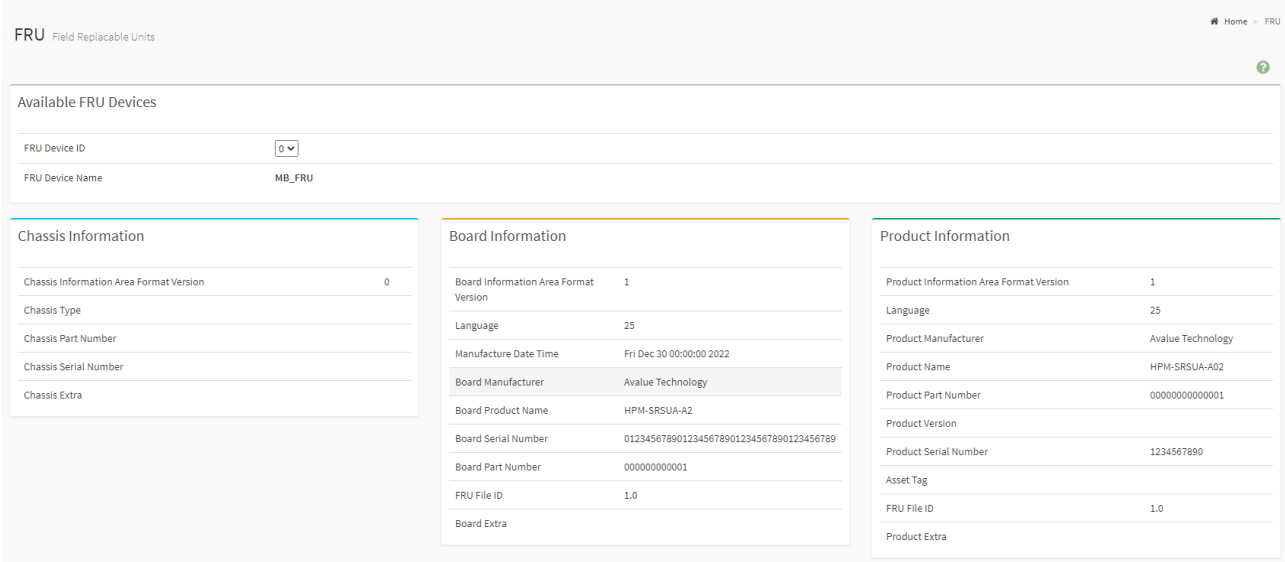
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)
- Lower Non-Critical (LNC)
- Lower Critical (LC)
- Lower Non-Recoverable (LNR)

Click "Change Thresholds" button to enter sensor threshold page.



2.4 HOME> FRU INFORMATION

This page display FRU information that be stored in eeprom

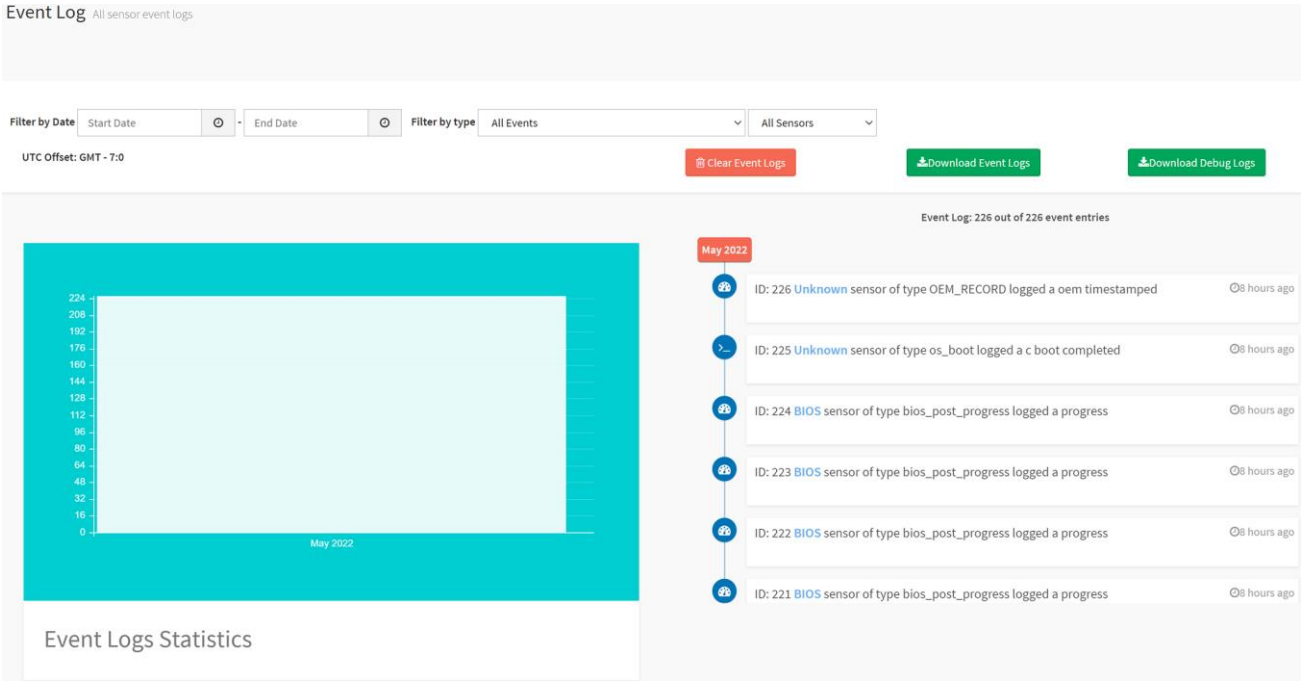


FRU device ID	**Select the device ID from the drop down list**
FRU Device Name	The name of eeprom that store FRU information

2.5 HOME> LOGS & REPORTS

2.5.1 Home> Logs & Reports >IPMI Event Log

This page displays the ipmi event logs and user can filter event logs by date/type/sensor

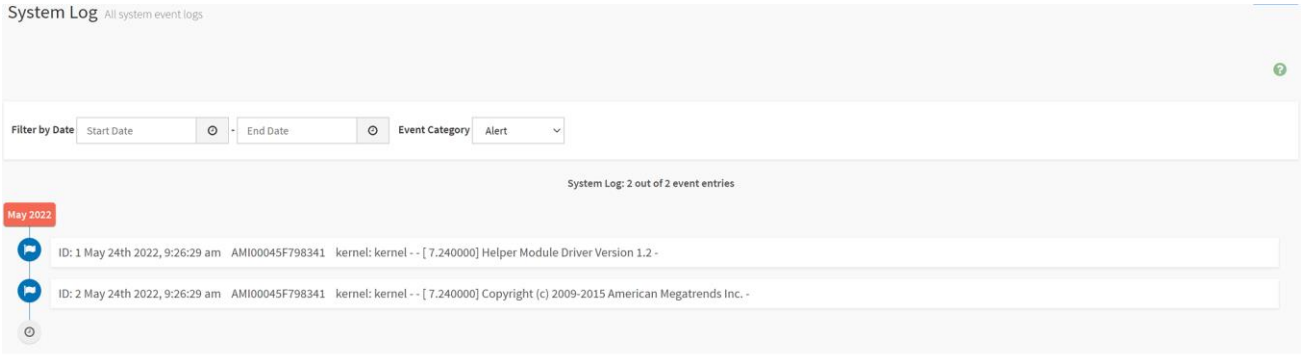


Item	Option	Description
Filter by Date	● Start Date ● End Date	Click field of "Start Date" or "End Date" to select the

		duration of filter
Filter by type	● All Events ● System Event Records ● OEM Event Record ● BIOS Generated Events ● SMI Handler Events ● System Management Software Events ● System Software – OEM Events ● Remote Console Software Events ● Terminal Mode Remote Console software Events	IPMI event logs can be filtered by this selected event type.
Filter by sensor	● All Sensors ● +V12S_CPU1 ● ….	IPMI event logs can be filtered by this selected sensor.

2.5.2 Home> Logs & Reports >System Event Log

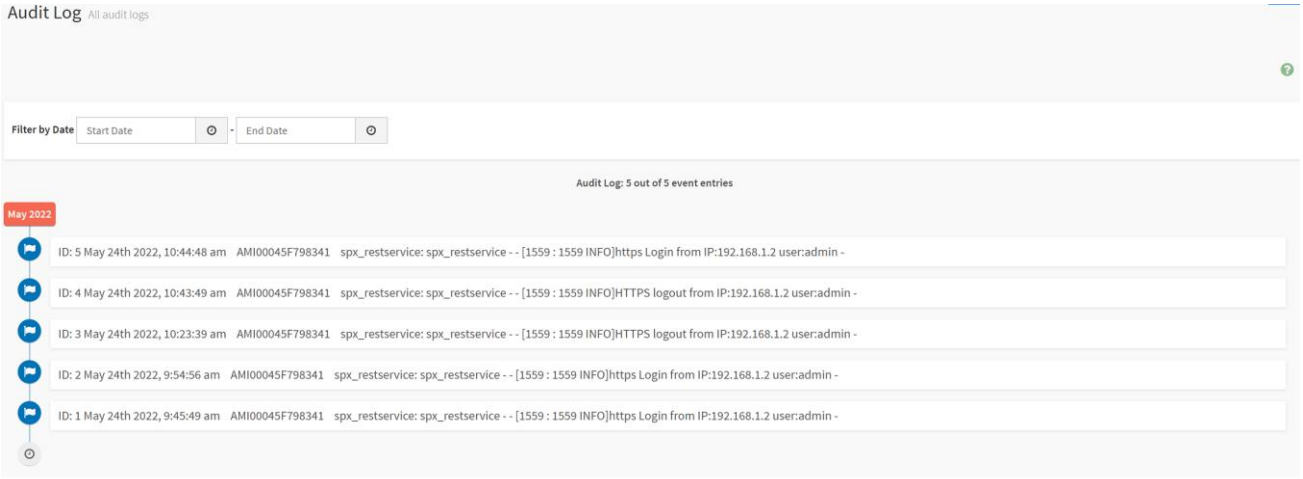
This page displays the system event logs and user can filter event logs by date/category



Item	Option	Description
Filter by Date	● Start Date ● End Date	Click field of "Start Date" or "End Date" to select the duration of filter
Event Category	● Alert ● Critical ● Error ● Notification ● Warning ● Debug ● Emergency ● Information	System event logs can be filtered by this selected event category.

2.5.3 Home> Logs & Reports >Audit Log

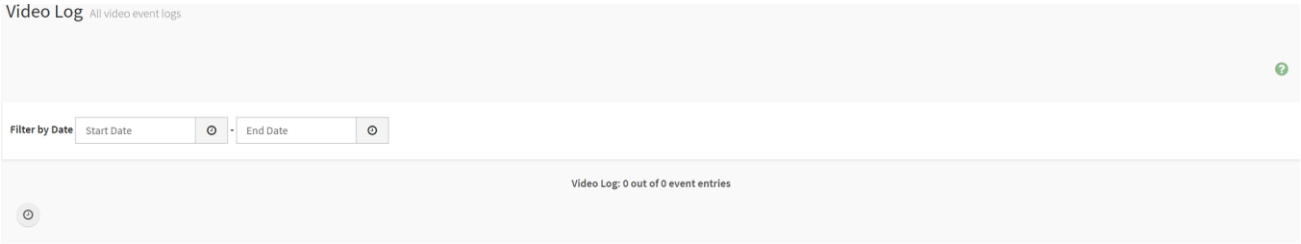
This page displays the audit logs and user can filter audit logs by date



Item	Option	Description
Filter by Date	● Start Date ● End Date	Click field of "Start Date" or "End Date" to select the duration of filter

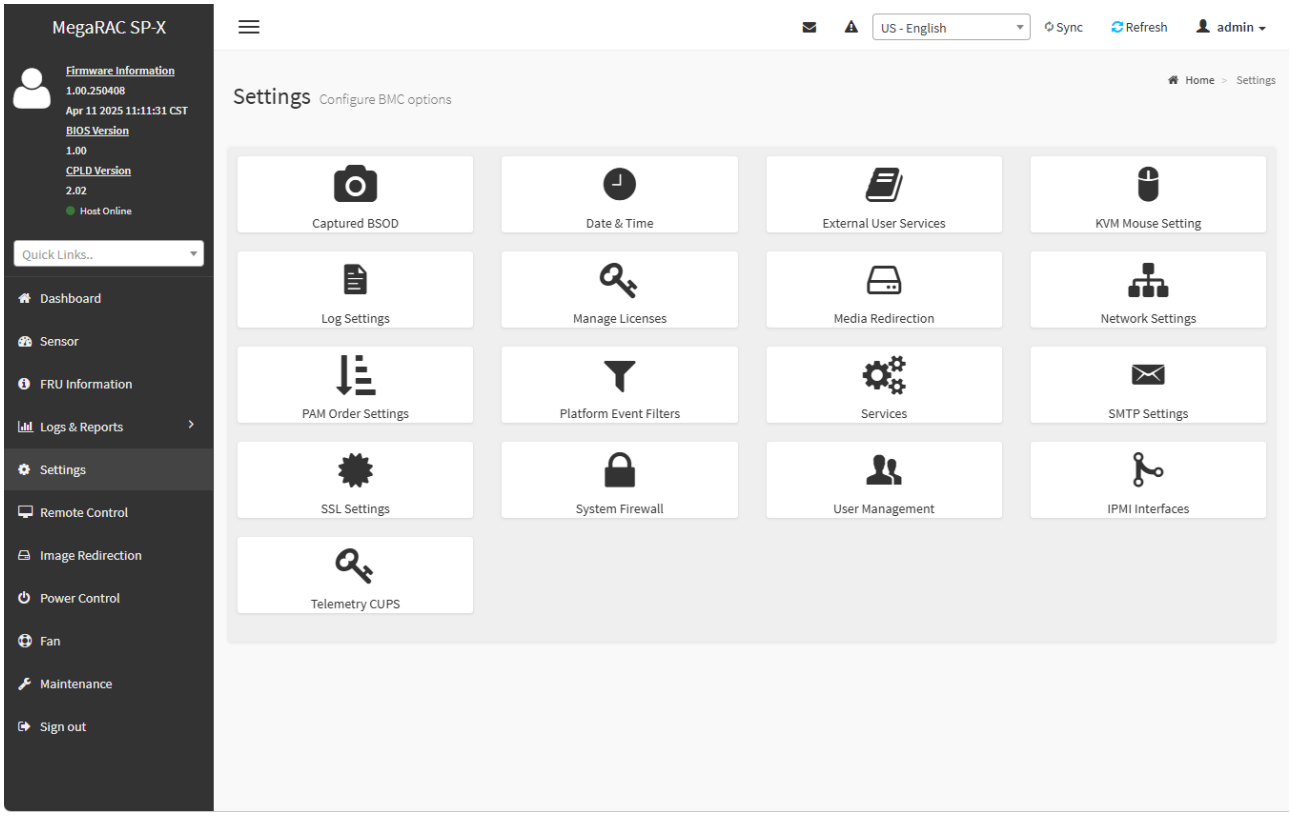
2.5.4 Home> Logs & Reports >Video Log

This page displays the audit logs and user can filter video logs by date



Item	Option	Description
Filter by Date	● Start Date ● End Date	Click field of "Start Date" or "End Date" to select the duration of filter

2.6 HOME> SETTINGS

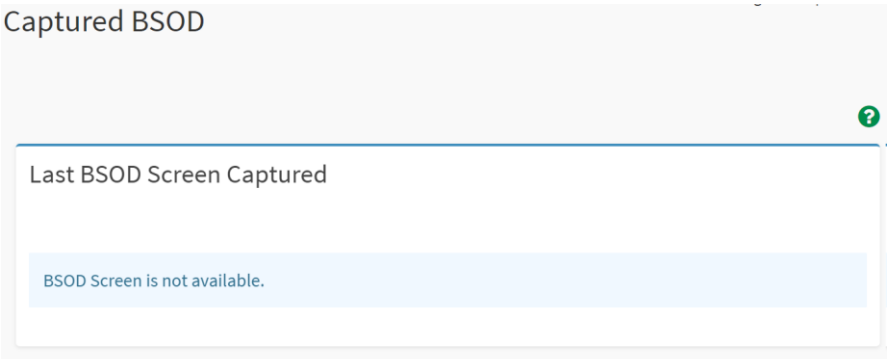


Item	Description
Captured BSOD	Captured snapshot of BSOD if the host system crashed
Date & Time	Set the date and time on the BMC
External User Services	Configure server settings to authenticate users
KVM Mouse Setting	Some settings of mouse emulation for KVM
Log Settings	Log settings for SEL log and Audit log
Manage Licenses	This page displays available licenses for this system, and the validity period for each.
Media Redirection	Configure the media into BMC for redirection
Network Settings	Configure the network settings for the available LAN channels
PAM Order Settings	Configure the PAM ordering for user authentication in to the BMC
Platform Event Filter	Configure Event Severity to trigger alert or power action
Services	Allow Administrator to modify services contain web/kvm/media/ssh.
SMTP Settings	E-mail message is one of alert and set SMTP for e-mail transmission across IP networks.
SSL Settings	SSL Certificate for secure transactions between webserver and browsers
System Firewall	Configure the firewall settings
User Management	Add a new user and modify or delete the existing users
IPMI Interfaces	Configure the IPMI Interfaces, IPMI Communication will not be performed over

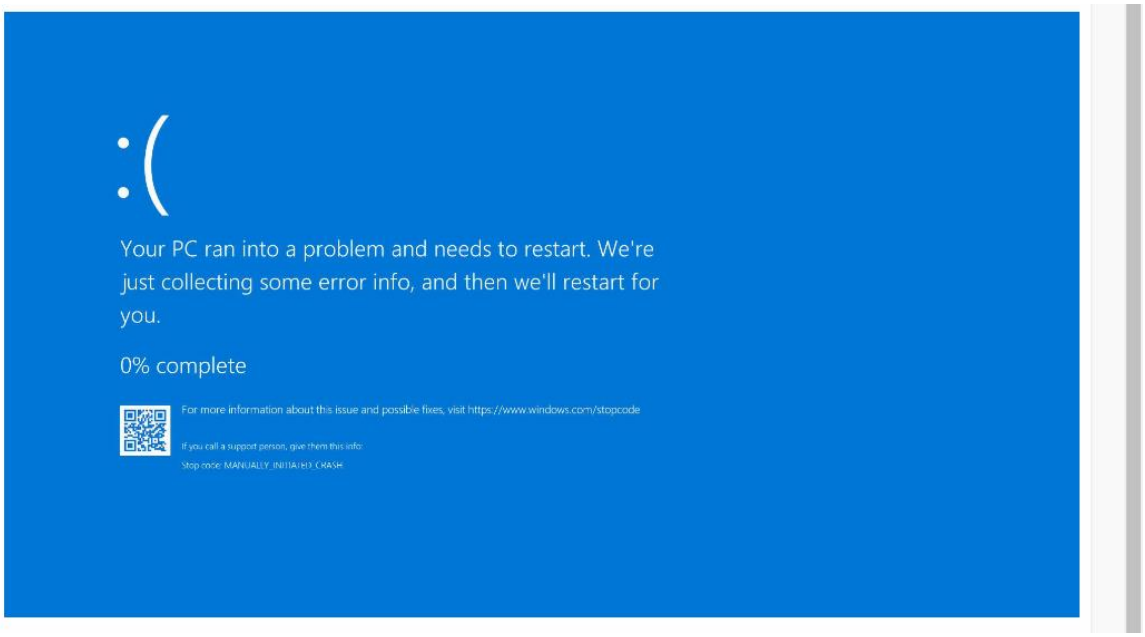
	LAN/KCS interface if it is disabled.
Telemetry CUPS	CUPs provides a mechanism to Compute Usage per second for CPU, Memory and ADD in cards. Also describe how much CPU/Memory and IIO current and average usage per second.

2.6.1 Home> Settings >Capture BSOD

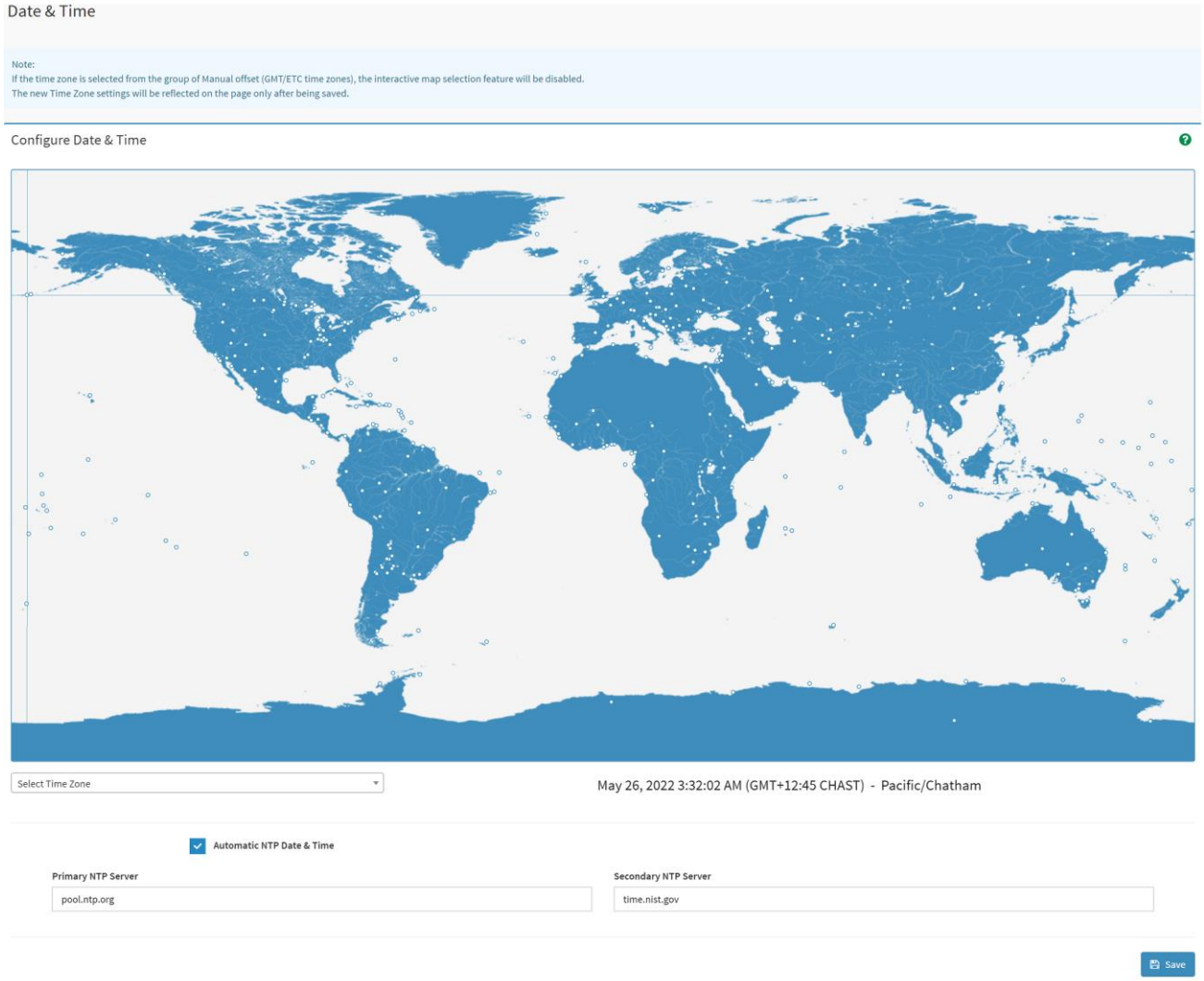
This page displays a snapshot of the blue screen captured at the time when/if the host system crashed since the last reboot.
Note: KVM service should be-enabled to display the BSOD. This can be configured under 'Settings ->Services->KVM'.



BMC captured last BSOD screen if system occurred BSOD.

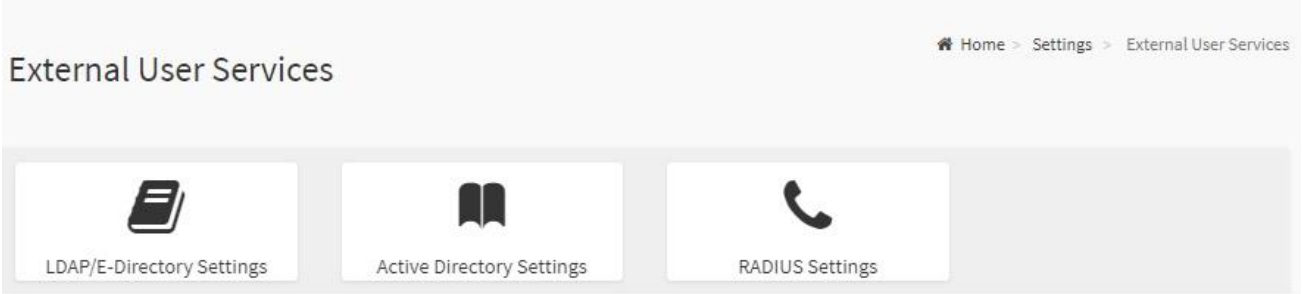


2.6.2 Home> Setting >Date & Time

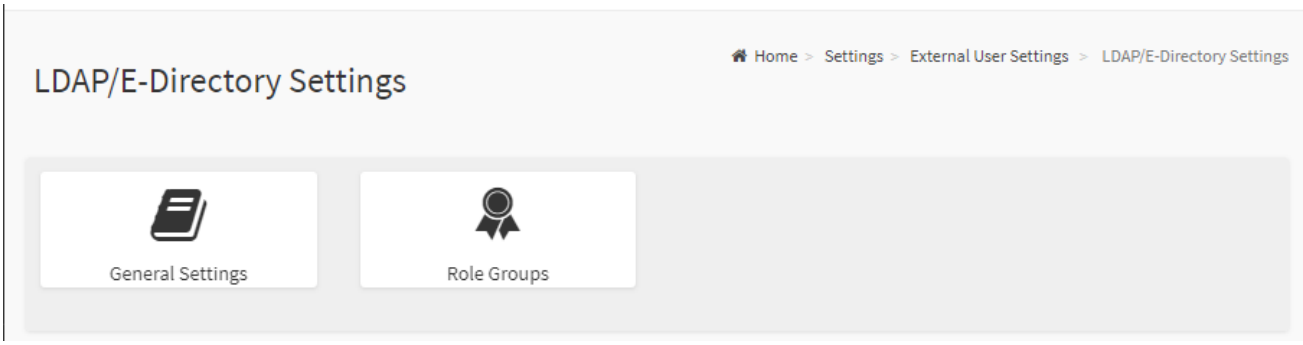


Item	Description
Select Time Zone	Choose the Time Zone either by using the drop-down option or by hovering over the map and double-clicking on a location name.
Automatic NTP Date & Time	You can select to have the time automatically synchronized to a NTP server (or two) ,which you can configure below.
Primary NTP Server	This field is used to configure a primary NTP server to use when automatically setting the date and time
Secondary NTP Server	This field is used to configure a secondary NTP server to use when automatically setting the date and time

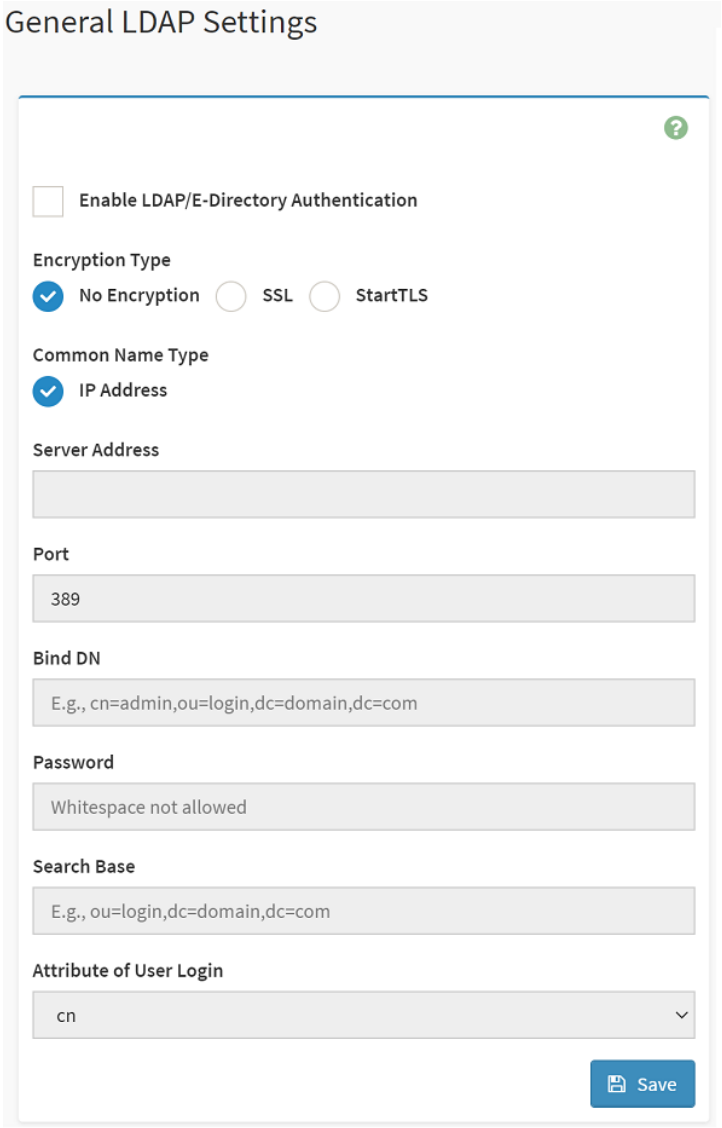
2.6.3 Home> Setting >External User Services



2.6.3.1 Home> Settings >LDAP/E-Directory Settings



2.6.3.1.1 Home> Settings >LDAP/E-Directory Settings >General LDAP Settings

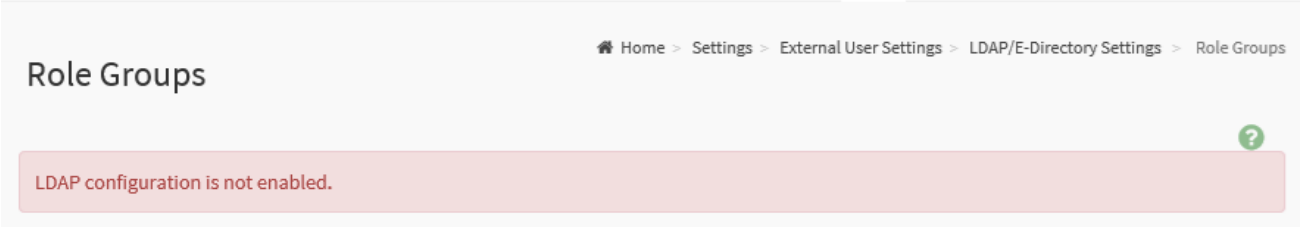


Item	Option	Description
Enabled LDAP/E-Directory Authentication	☑ ☐	Checked to enable LDAP/E-Directory settings. Note: During login prompt,use username to login as an LDAP Group member.
Encryption Type	● No Encryption ● SSL ● StartTLS	Encryption type for LDAP/E-Directory Note:Configure proper port number when SSL is enabled
Common Name Type	● IP Address	Select the Common Name Type as IP Address
Server Address		Enter the IP address of LDAP server in the field
Port		Specify the LDAP Port in the field and range from 1

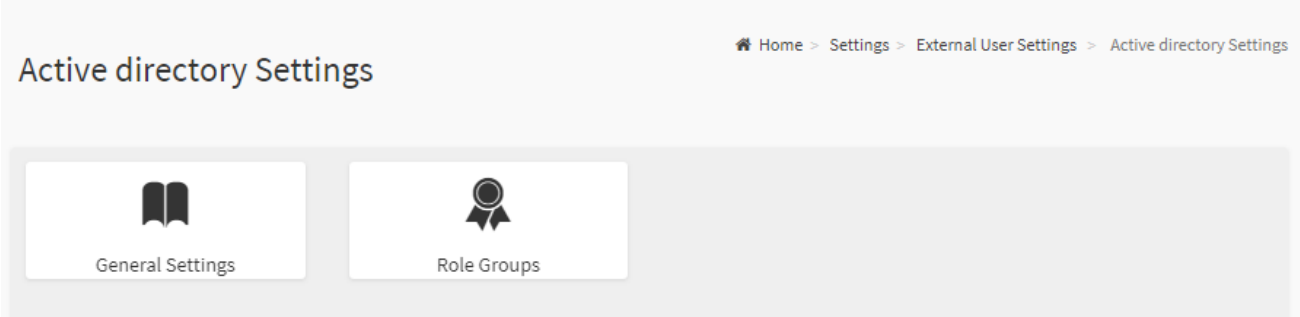
		to 65535. Default port is 389 For SSL connections,default port is 636
Bind DN	Example: cn=manager,ou=login, dc=domain,dc=com	Specify the Bind DN that is used during bind operation, which authenticates the client to the server. Note:Bind DN is a string of 4 to 253 alpha-numeric characters. It must start with an alphabetical character. Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
Password		Enter the password in the Password field Note: ♦ at least 1 character long ♦ not allow more than 48 characters ♦ white space is not allowed.
Search Base	Example: ou=login, dc=domain,dc=com	Enter the Search Base. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory Note: Search base is a string of 4 to 253 alpha-numeric characters. It must start with an alphabetical character Special Symbols like dot(.),comma(,),hyphen(-), underscore(_), equal-to(=) are allowed.
Attribute of User Login	● cn ● uid	Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.
Save	Save	Click button to save the changes made

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

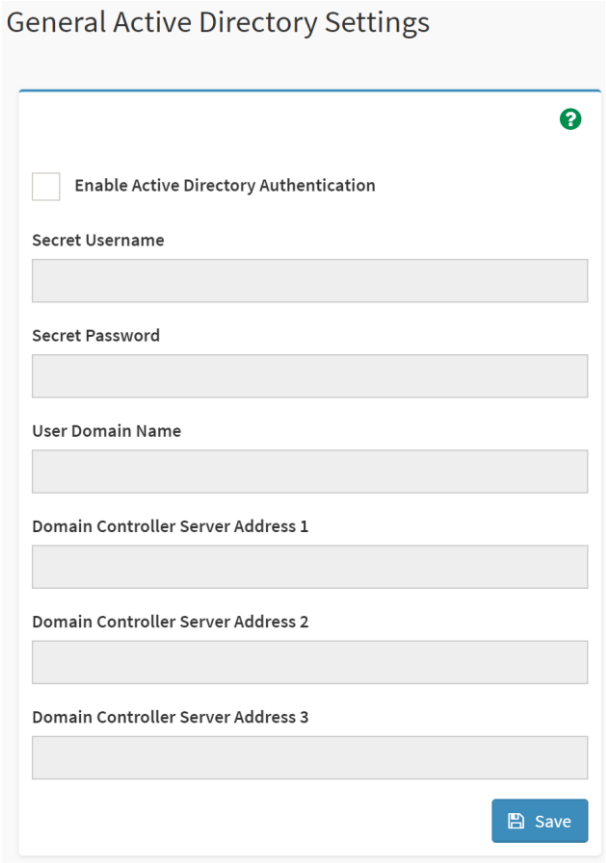
Note: Free/Uncofigured slots are denoted by the word 'None'
To add a Role Group, select a free box and click on it
To modify a Role Group, click on its name.
To delete a Role Group, click on the X icon present at the right top corner for that box.



2.6.3.2.1 Home> Settings > External User Services >Active directory Settings



2.6.3.2.2 Home> Setting > External User Services >Active directory Settings> General Active Directory Settings



Item	Option	Description
Enable Active Directory Authentication	☑ ☐	Enable/Disable Active Directory Authentication
Secret Username		Specify the Username of an administrator of the Active Directory Server. • A string of 1 to 64 alpha-numeric characters • Start with an alphabetical character • Case-sensitve • Specail characters and spaces are not allowed Note: If Secret Username and Password are not needed, both fields can remain blank.(However,this will affect the ability to reorder the PAM sequence)
Secret Password		Specify the Password of the administrator. • At least 6 characters long • White space is not allowed

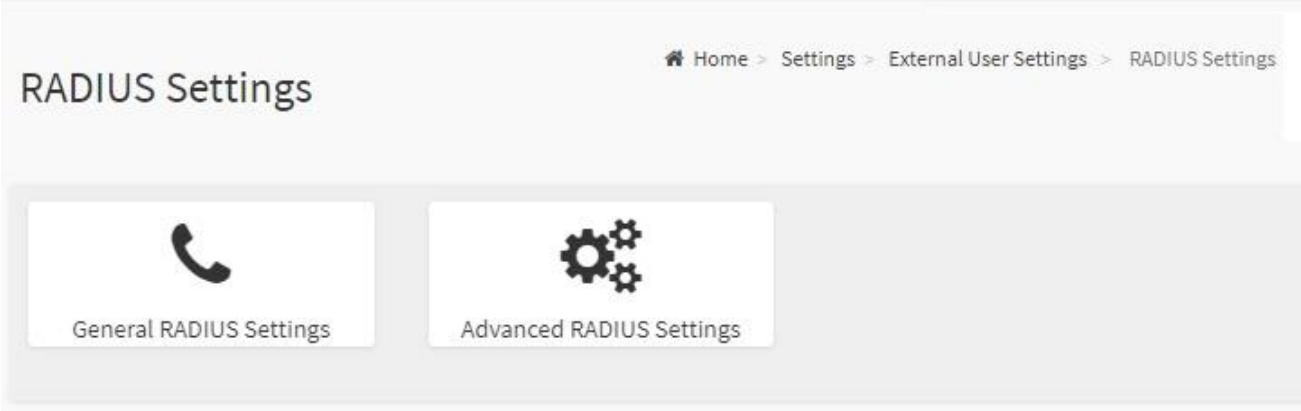
		Note: This field will not allow more than 127 characters.
User Domain Name		Specify the Domain Nmae for the user e.g. MyDomain.com
Domain Controller Server Address 1		Enter the IP address of Active Directory server. At least one Domain Controller Server Address must be configured. IPv4/IPv6 formats are supported
Domain Controller Server Address 2		
Domain Controller Server Address 3		
Save	Save	Click button to save the changes made

2.6.3.2.3Home> Settings > External User Services >Active directory Settings>Role Groups

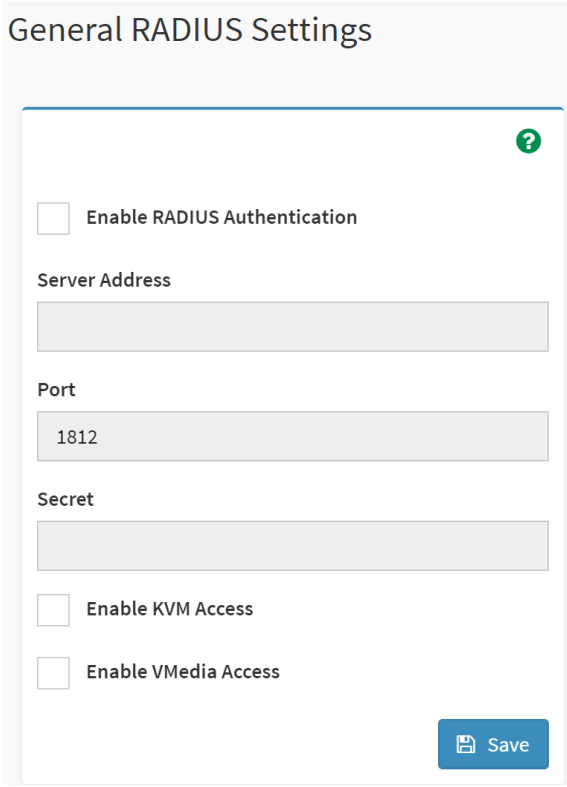
Note: Free/Uncofigured slots are denoted by the word 'None'
To add a Role Group ,click on a free box and configure its privilege and access.
To modify a Role Group ,click on it
To delete a Role Group, click on the X present at the right top cornet of its box.



2.6.3.3.1 Home> Settings>External User Services>RADIUS Settings

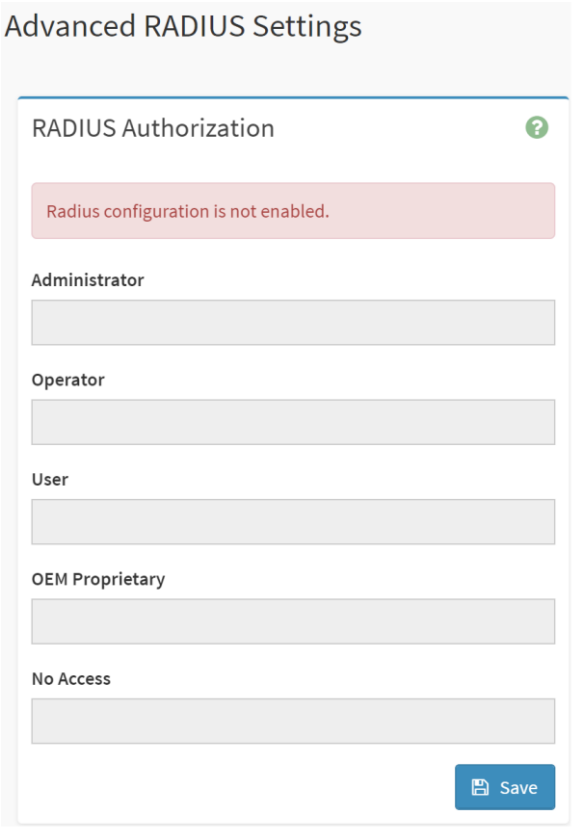


2.6.3.3.2 Home> Settings>External User Services>RADIUS Settings >General RADIUS Settings



Item	Option	Description
Enable RADIUS Authentication	☑ ☐	Enable/Disable RADIUS Authentication
Server Address		The ip address of RADIUS server Note: IP Address (both IPv4 and IPv6 format) FQDN (Fully Qualified Domain Name) format
Port		The RADIUS Port number.(from 1 to 65535) Default Port is 1812
Secret		The Authentication Secret for RADIUS server ♦ not allow more than 31 characters. ♦ must be at least 4 characters long. ♦ white space is not allowed.
Enable KVM Access	☑ ☐	Enable/Disable access to KVM for RADIUS authenticated users
Enable VMedia Access	☑ ☐	Enable/Disable access to VMedia for RADIUS authenticated users
Save	Save	Click button to save the changes made

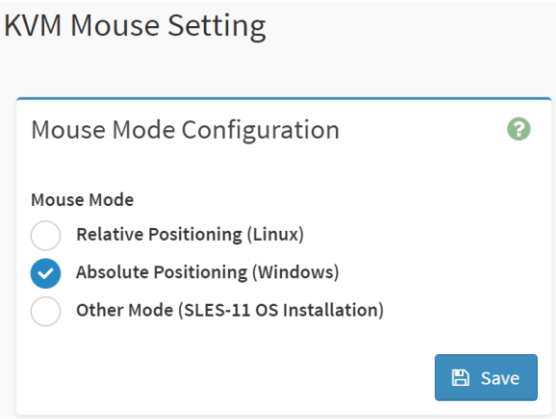
2.6.3.3.3 Home>Settings>External User Services>RADIUS Settings >Advanced RADIUS Settings



Item	Option	Description
Administrator		Radius User Authorization For authorization purposes, you should configure Vendor Specific Attributes for the radius users on the server. Example: Add Vendor-Specific attribute cd /usr/share/freeradius vim dictionary.adtest (Add content below) # dictionary.adtest VENDOR ADTest 58 # Standard attribute BEGIN-VENDOR ADTest ATTRIBUTE ADTest-group 1 string END-VENDOR ADTest vim dictionary (Add this line)
Operator		
User		
OEM Proprietary		
No Access		

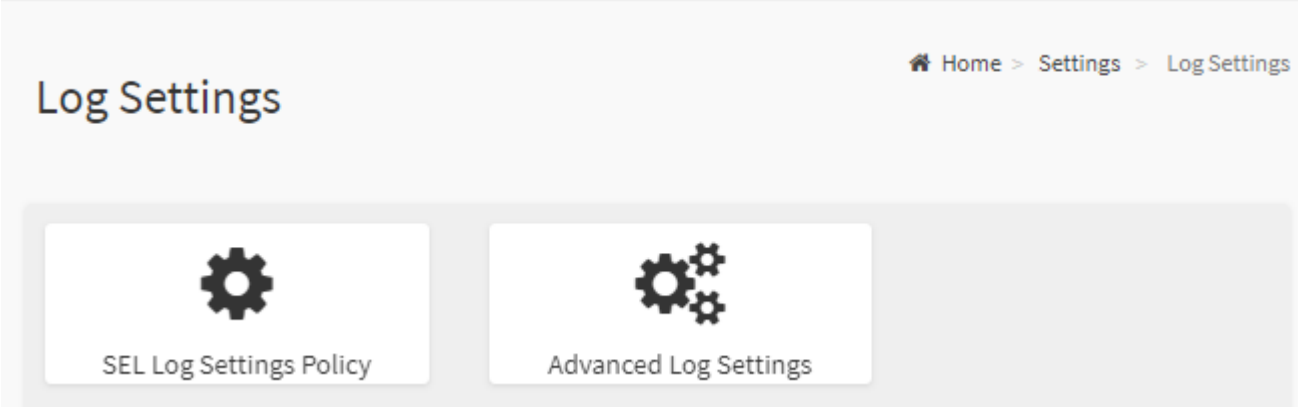
		$INCLUDE dictionary.adtest Add users: vim users (Add below content) "RadiusTest1" Cleartext-Password := "000000" Service-Type = Administrative-User, Auth-Type := System, ADTest-group := "H=4" NOTES: These fields will not allow more than 127 characters. '#' is not allowed.
Save	Save	Click button to save the changes made

2.6.4 Home>Settings>KVM Mouse Setting

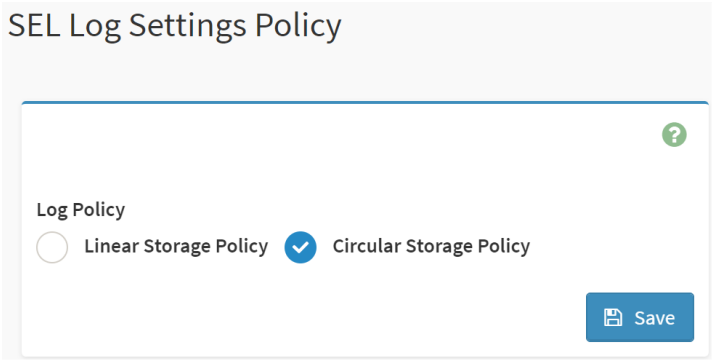


Item	Option	Description
Mouse Mode	● Relative Positioning(Linux) ● Absolute Positioning(Windows) ● Other Mode (SLES-11 OS Installation)	Select in either of three methods to calculate mouse position.
Save	Save	Click button to save the changes made

2.6.5 Home>Settings>Log Settings

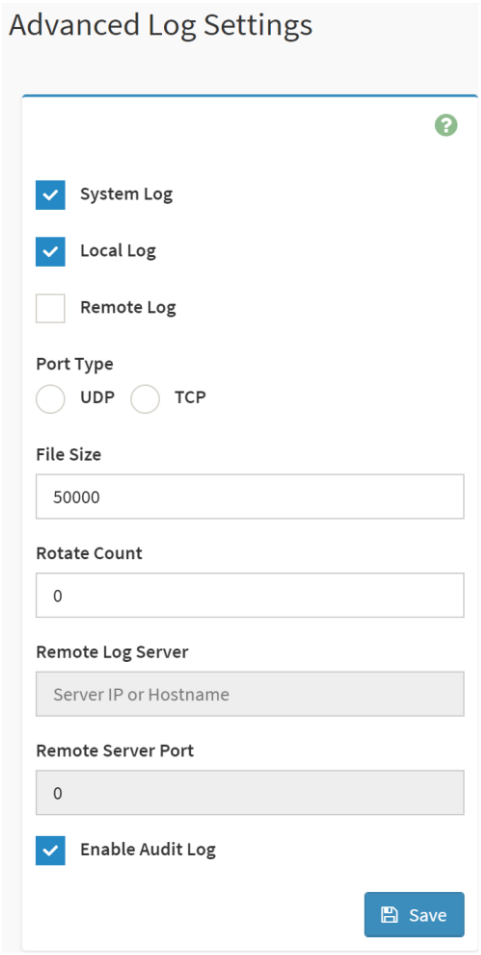


2.6.5.1 Home> Settings>Log Settings>SEL Log Settings Policy



Item	Option	Description
Log Policy	● Linear Storage Policy ● Circular Storage Policy	This field is used to configure the log policy for the event log.
Save	Save	Click button to save the changes made

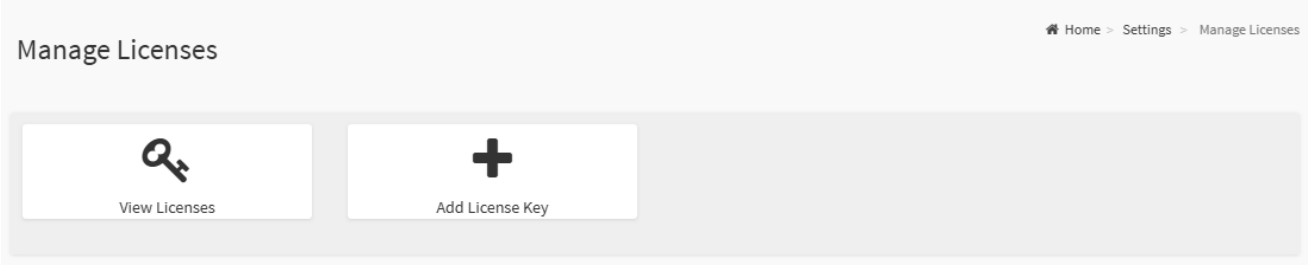
2.6.5.2 Home> Settings>Log Settings>Advanced Log Settings



Item	Option	Description
System Log	☑ ☐	Select Enable System Log to view all system events. Entries can be filtered base on their classification levels
Local Log	☑ ☐	Select local log to save the logs locally (BMC)
Remote Log	☑ ☐	Select remote log to save the logs in a remote machine.
Port Type	● UDP ● TCP	Port type is supported with the enable of Remote Log. User can select either UDP/TCP as per the requirement.
File Size		If Local log is selected ,specify the size of the file in bytes. ♦ Size ranges from 3 to 65535 ♦ Log files are rotated when the size is larger than the mentioned bytes , with regards for the last rotation time interval(1 minute).
Rotate Count		When logged information exceeds the specified file size, the old log information automatically gets moved to back up files based on the rotate count value. If the rotate count is zero , the old log information

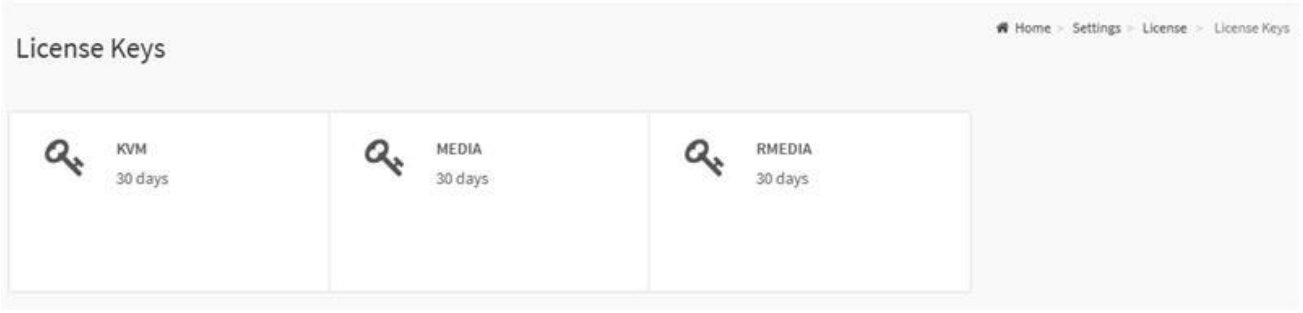
		gets cleared permanently each time.
Remote Log Server		Specify the remote server address to log system events. Server address support the following: ♦ IP Address (Both IPv4 and IPv6 format). ♦ FQDN (Fully qualified domain name) format
Remote Server Port		Specify the port number to log system events Note: If entering port number 0 , it will set port number as default. The default port number is 514
Enable Audit Log		Select Enable Audit Log to view all audit events for this device.
Save	Save	Click button to save the changes made

2.6.6 Home > Settings > Manage Licenses



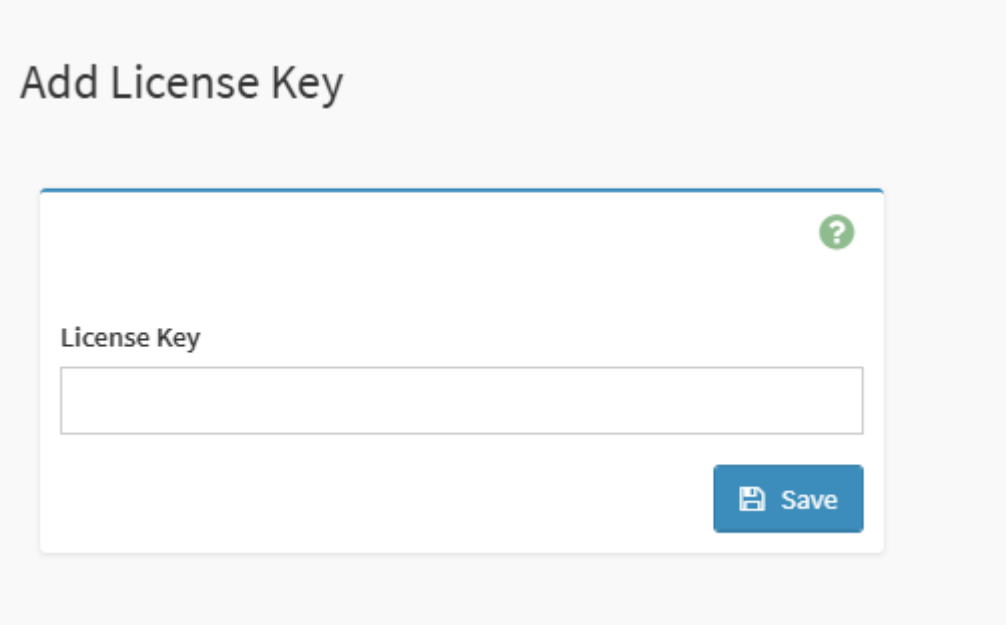
2.6.6.1 Home > Settings > Manage Licenses > View Licenses

This page could view all available licenses for this system, and the validity period for each.

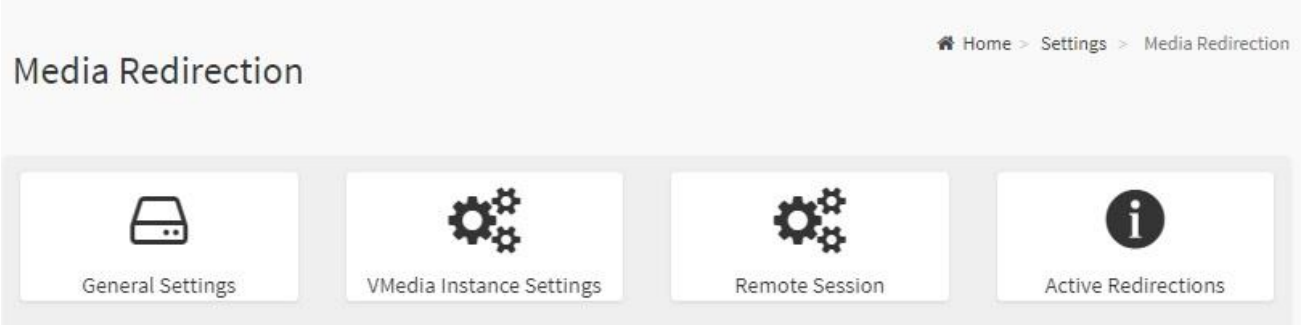


2.6.6.2 Home > Settings > Manage Licenses > Add License Key

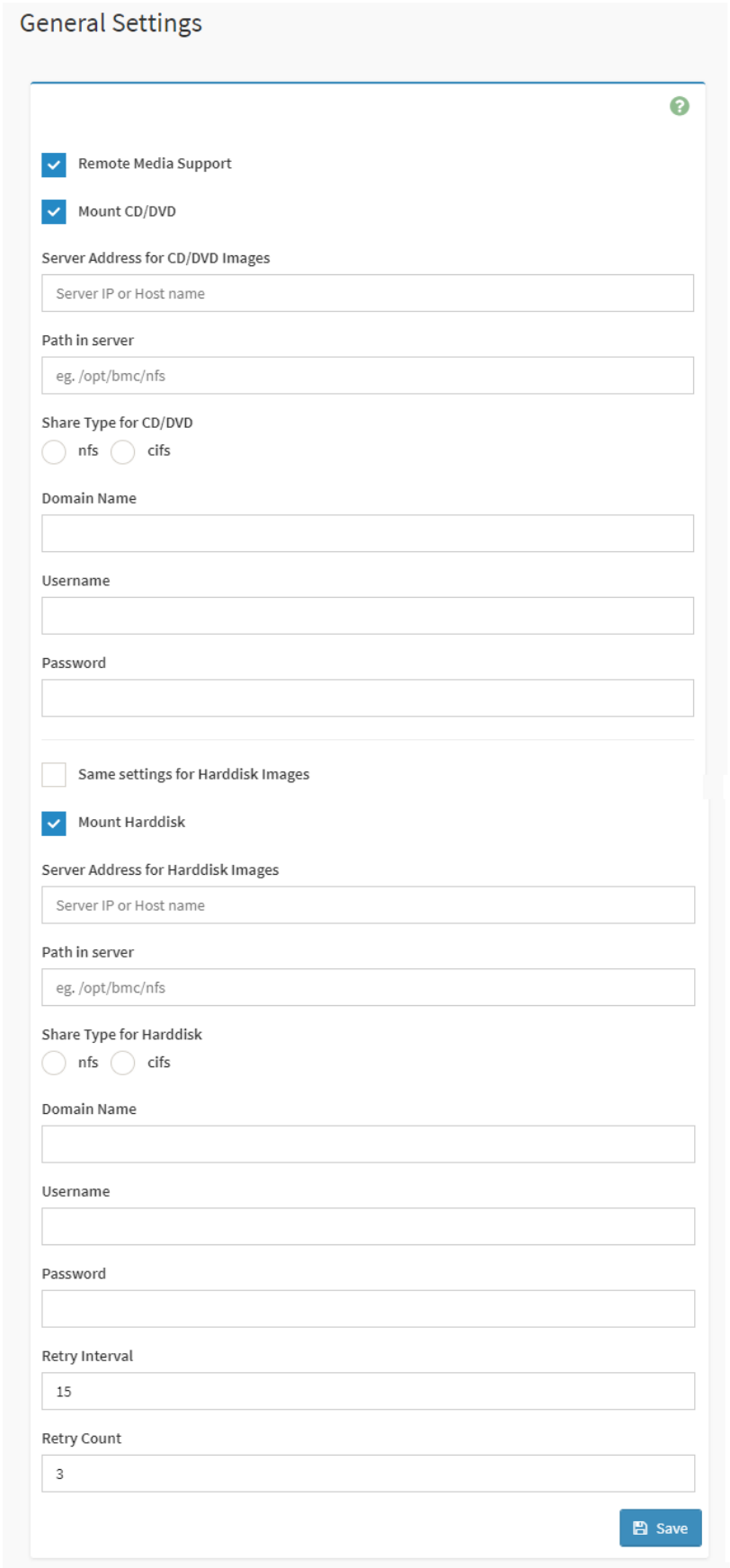
Upload license key on this page.



2.6.7 Home>Settings>Media Redirection



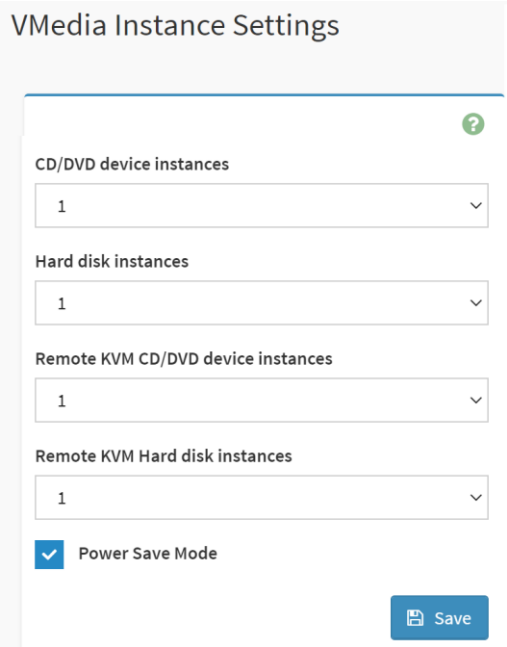
2.6.7.1 Home>Settings>Media Redirection>General Settings



Item	Option	Description
Remote Media Support	☑ ☐	To enable or disable Remote Media support ,check or uncheck this box. If it is selected ,then the following remote media types will be displayed ♦ CD/DVD ♦ Hard disk User can configure different settings for the different remote media types. Configuration options will be displayed for each media type, or the same options can be applied to both.
Mount CD/DVD	☑ ☐	To enable or disable Mount CD/DVD support ,check or uncheck this box.
Server Address for CD/DVD image		Address of the server where remote videos are to be stored. We support the following: ♦ IPv4/IPv6 format. ♦ FQDN(Fully qualified domain name) format
Path in server		Path must be alpha-numeric and the following special characters are only allowed: '/' , '\' , '-' , '_' , '.' , ':'
Share Type for CD/DVD	● nfs ● cifs	Share Type of the remote media server : either NFS or Samba(CIFS).
Domain Name		If Share Type is Samba(CIFS) , then enter user credentials to authenticate the server. Note: Domain Name field is optional.
Username		
Password		
Same settings for Harddisk images	☑ ☐	If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type as well.
Mount Harddisk	☑ ☐	To enable or disable Mount Harddisk support ,check or uncheck this box.
Server Address for Harddisk images		Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format
Path in server		Path must be alpha-numeric and the following special characters are only allowed: '/' , '\' , '-', '_' , '.' , ':'
Share Type for Harddisk	● nfs ● cifs	Share Type of the remote media server : either NFS or Samba(CIFS).

Domain Name		If Share Type is Samba(CIFS), then enter user credentials to authenticate the server. Note : Domain Name field is optional.
Username		
Password		
Retry Interval		Specify the Retry Interval and range should be from 15 to 30.Default value will be 15
Retry Count		Specify the Retry Count and range should be from 3 to 6. Default value will be 3
System Log		Select Enable System Log to view all system events. Entries can be filtered base on their classification levels
Save	Save	Click button to save the changes made

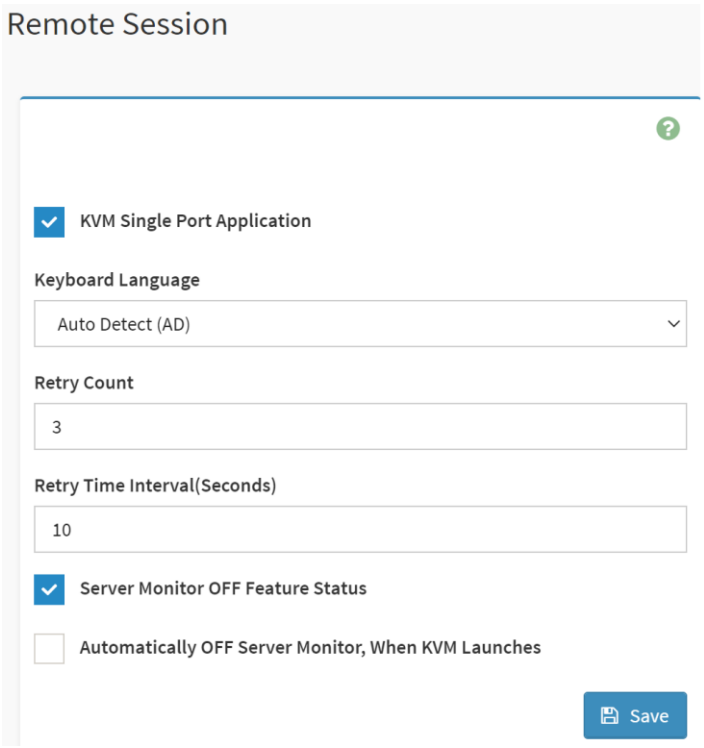
2.6.7.2 Home>Settings>Media Redirection>VMedia Instance Settings



Item	Option	Description
CD/DVD device instances	0-4	Select the number of CD/DVD devices that are to be supported for Virtual Media redirection
Hard disk instances	0-4	Select the number of Hard disk devices to be supported for Virtual Media redirection
Remote KVM CD/DVD device instances	0-4	Select the number of Remote KVM CD/DVD devices that are to be supported for Virtual Media redirection
Remote KVM Hard disk	0-4	Select the number of Remote KVM Hard disk devices that

instances		are to be supported for Virtual Media redirection
Power Save Mode	☑ ☐	Check this option to enable Power Save Mode in BMC
Save	Save	Click button to save the changes made

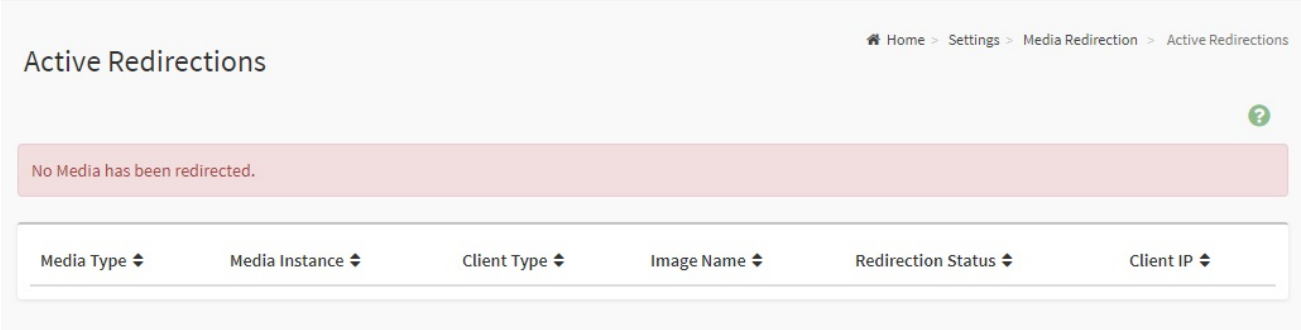
2.6.7.3 Home>Settings>Media Redirection>Remote Session



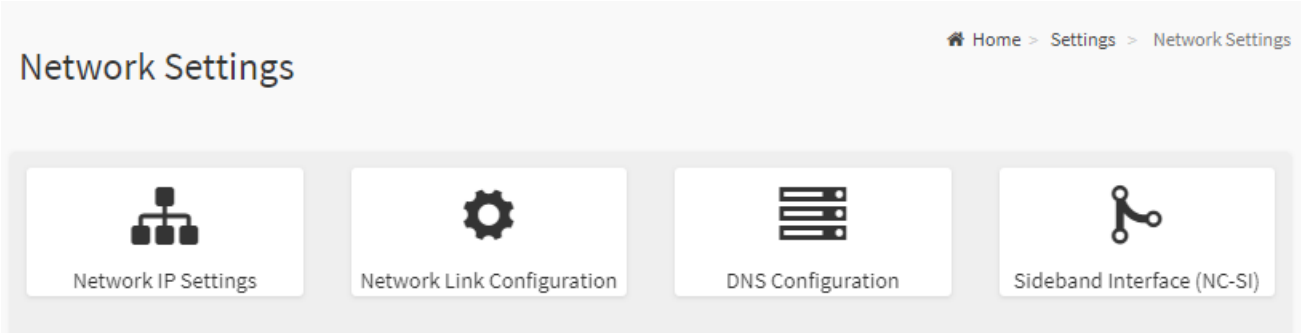
Item	Option	Description
KVM Single Port Application	☑ ☐	Check this option to enable Single Port Application support in BMC
Keyboard Language		Select the Keyboard Language
Retry Count	1 to 20	Number of times to be retried when a KVM failure occurs. Retry count ranges from 1 to 20
Retry Time Interval(Seconds)	5 to 30	Number of seconds to wait for subsequent retries. Time interval ranges from 5 to 30 seconds
Server Monitor OFF Feature Status	☑ ☐	Check this option to enable the Server Monitor OFF feature
Automatically OFF Server Monitor, When KVM Launches	☑ ☐	Check this option to enable Automatically OFF Server Monitor when KVM is launched
Save	Save	Click button to save the changes made

2.6.7.4 Home>Settings>Media Redirection>Active Redirections

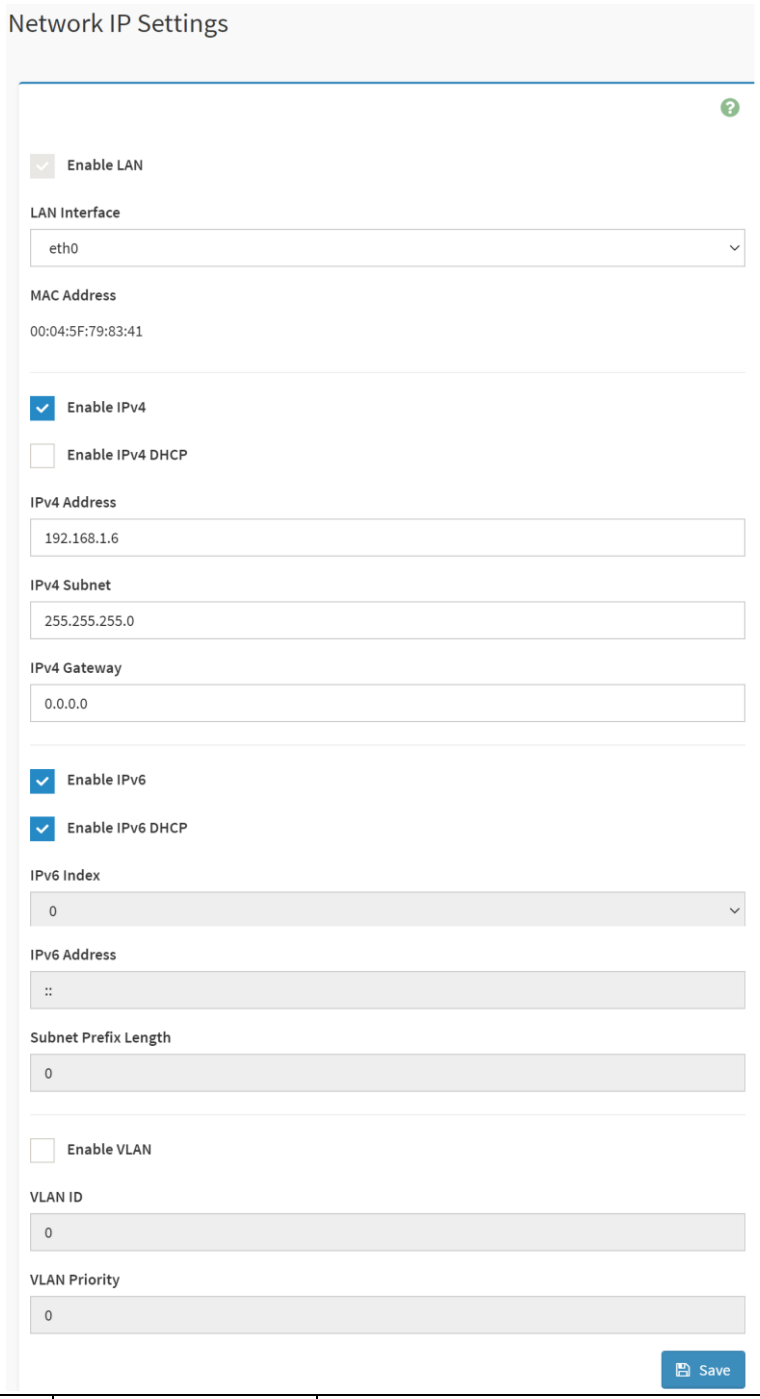
Below is a list of Media which are being redirected currently . Shown for each is the status and other basic information.



2.6.8 Home>Settings>Network Settings



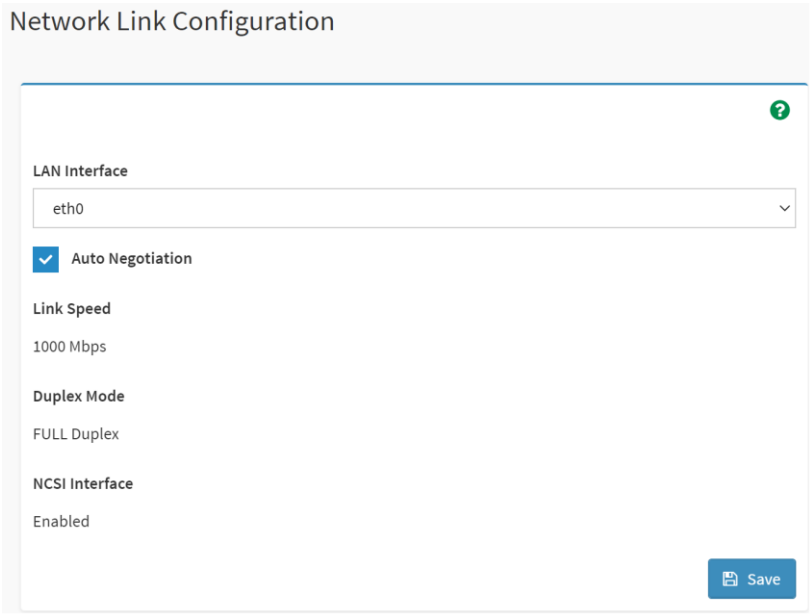
2.6.8.1 Home>Settings>Network Settings>Network IP Settings



Item	Option	Description
Enabled IPv4	☑ ☐	Enable/Disabled IP of BMC lan is ipv4 address format
Enabled IPv4 DHCP	☑ ☐	IPv4 is assigned by DHCP server or manual settings
IPv4 Address		Fill out specific the static IPv4 address for lan of BMC

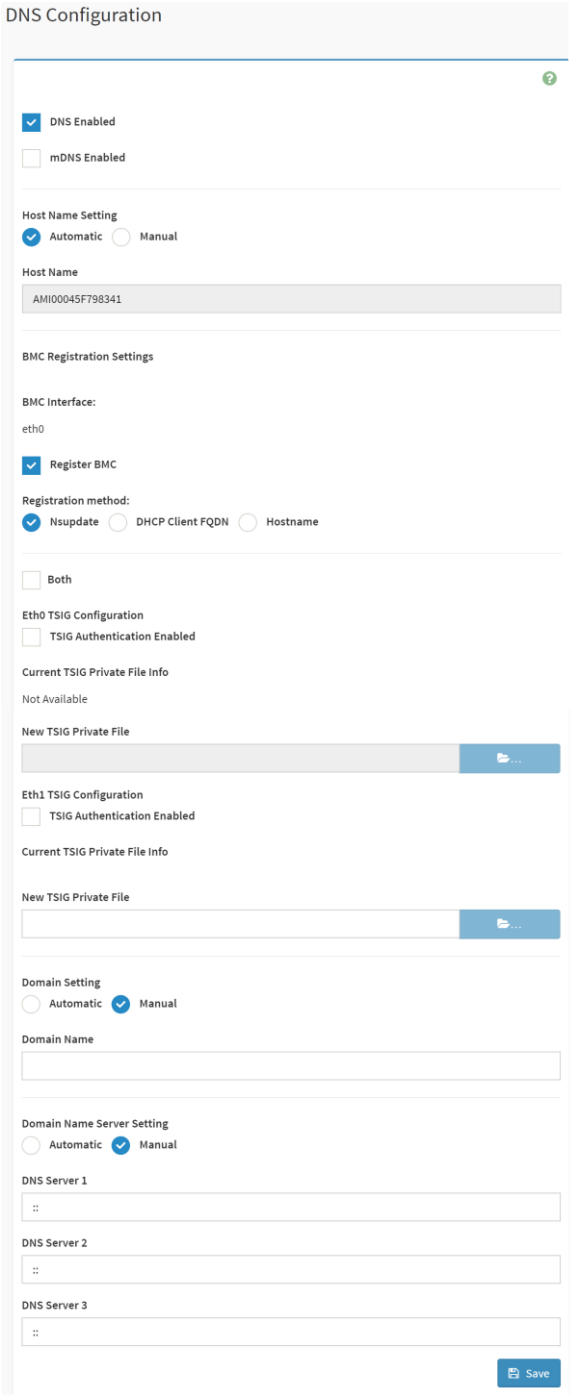
IPv4 Subnet Mask		Fill out specific the static IPv4 Subnet Mask for lan of BMC
IPv4 Default Gateway		Fill out specific the static IPv4 Default Gateway for lan of BMC
Enabled IPv6	☑ ☐	IP of BMC lan is ipv6 address format
Enabled IPV6 DHCP	☑ ☐	IPv6 is assigned by DHCP server or manual settings
IPv6 Index		To specify a static IPv6 Index to be configured to the device
IPv6 Address		To specify a static IPv6 address to be configured to the device
Subnet Prefix length	from 0 to 128	To specify the subnet prefix length for the IPv6 settings.
Enabled VLAN	☑ ☐	To enable/disable VLAN support
VLAN ID	From 2 to 4094	Specify an ID for this VLAN configuration
VLAN Priority	From 0 to 7	The priority for VLAN configuration. 7 is the highest priority.
Save	Save	Click button to save the changes made

2.6.8.2 Home>Settings>Network Settings>Network Link Configuration



Item	Option	Description
LAN Interface	eth0	Select the network interface for which the Link speed and duplex made are to be configured.
Auto Negotiation		This option is enabled to allow the device to perform automatic configuration, allowing it to achieve the best possible mode of operation (speed and duplex)over a link.
Link Speed	● 10 ● 100 ● 1000 ● (Auto Negotiation)	Link speed options are dependent on the capabilities of the network interface. Speed can be 10/100/1000 Mbps. Note:Link speed of 1000Mbps is not applicable when Auto Negotiation is set to OFF
Duplex Mode	● Full duplex ● Halt duplex	Select any one of the following duplex modes. Halt duplex Full duplex
NCSI Interface		NCSI interface Enable/Disable
Save		Click button to save the changes made

2.6.8.3 Home>Settings>Network Settings>DNS Configuration

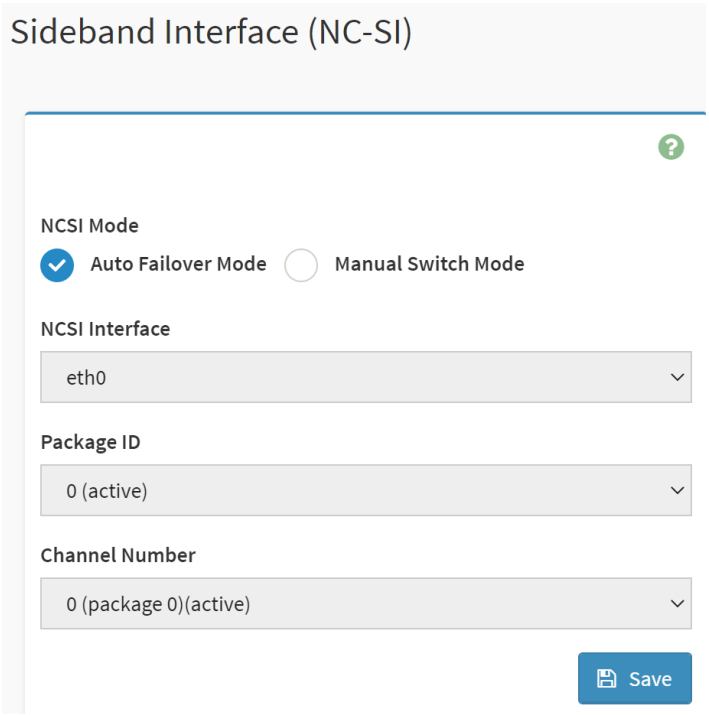


Item	Option	Description
DNS Enabled	☑ ☐	Check this box to enable all DNS services
mDNS Enabled	☑ ☐	Check this box to enable Multicast DNS
Host Name	● Automatic	Select whether the host name will be configured manually or

Setting	● Manual	automatically.
Host Name		If Automatic is selected ,the this field automatically display the hostname. Otherwise,please enter the desired hostname for the device.
Register BMC	☑	Check this box to enable Register BMC
Registration method	● Nsupdate ● DHCP client FQDN ● Hostname	Nsupdate-Register with the DNS server using the nsupdate application DHCP client FQDN-Register with the DNS server using DHCP option 81 Hostname-Register with the DNS server using DHCP option 12 Note: Hostname option should be selected if the DHCP server does not support option 81 and Hostname method registration does not support IPv6 Domain interface.
Both	☑	Check this box to modify TSIG authentication for both interfaces.
TSIG Authentication Enabled(Eth0)	☑	Check this box to enable TSIG Authentication – if registering DNS via nsupdate only.
New TSIG Private File(Eth0)		Browse for a new TSIG private file to be uploaded to the BMC
TSIG Authentication Enabled(Eth1)	☑	Check this box to enable TSIG authentication – if registering DNS via nsupdate only
New TSIG Private File(Eth1)		Browse for a new TSIG private file to be uploaded to the BMC.
Domain Setting	● Automatic ● Manual	Select whether the domain interface will be configured manually or automatically.
Domain Name		Displays the domain name of the device, or ,if 'Manual' was selected, specify the domain name of the device.
Domain Name Sever Setting	● Automatic ● Manual	Select whether the DNS interface will be configured manually or automatically.
DNS Server 1		Specify the DNS(Domain Name System) server address to be configured for the BMC. IPv4 addresss should be given in dotted decimal representation.
DNS Server 2		

DNS Server 3		IPv6 address are supported and must be global unicast addresses.
Save	Save	Click button to save the changes made

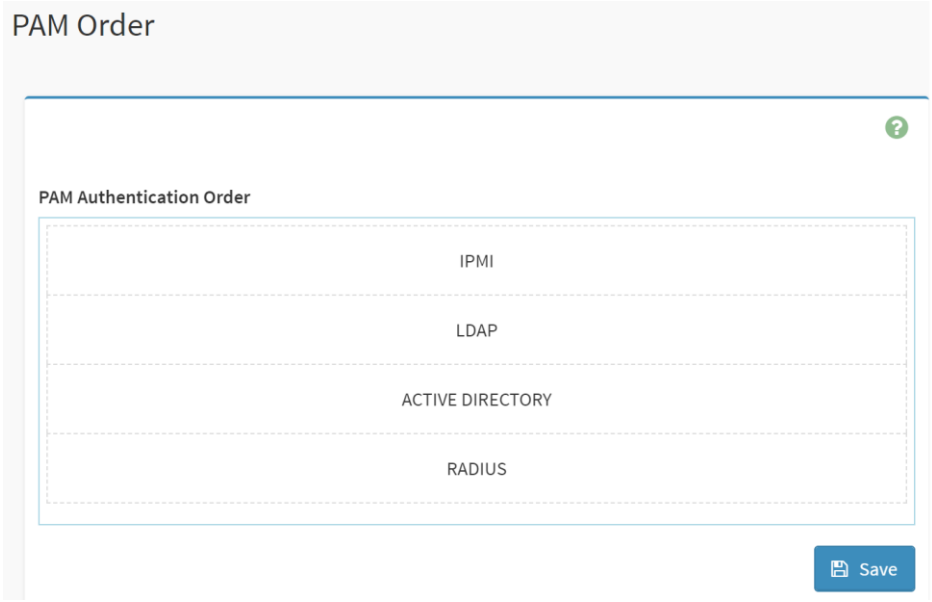
2.6.8.4 Home>Settings>Network Settings>Sideband Interface



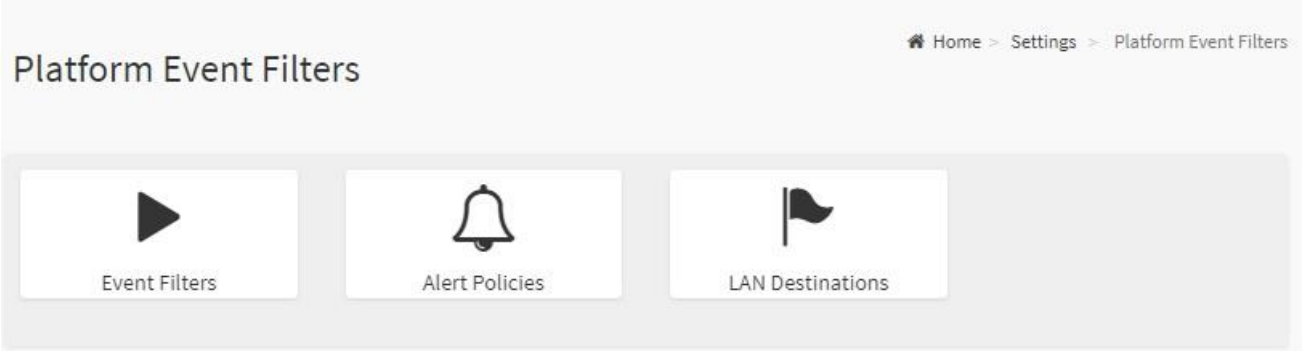
Item	Option	Description
NCSI Mode	● Auto Failover Mode ● Manual Switch Mode	Select the NCSI mode
NCSI Interface	eth0	Choose the interface name for which to configure NCSI settings
Package ID		Choose the package ID to be configured for the selected interface.
Channel Number		Choose the channel number to be configured for the selected interface.
Save	Save	Click button to save the changes made

2.6.9 Home>Settings>PAM Order

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.

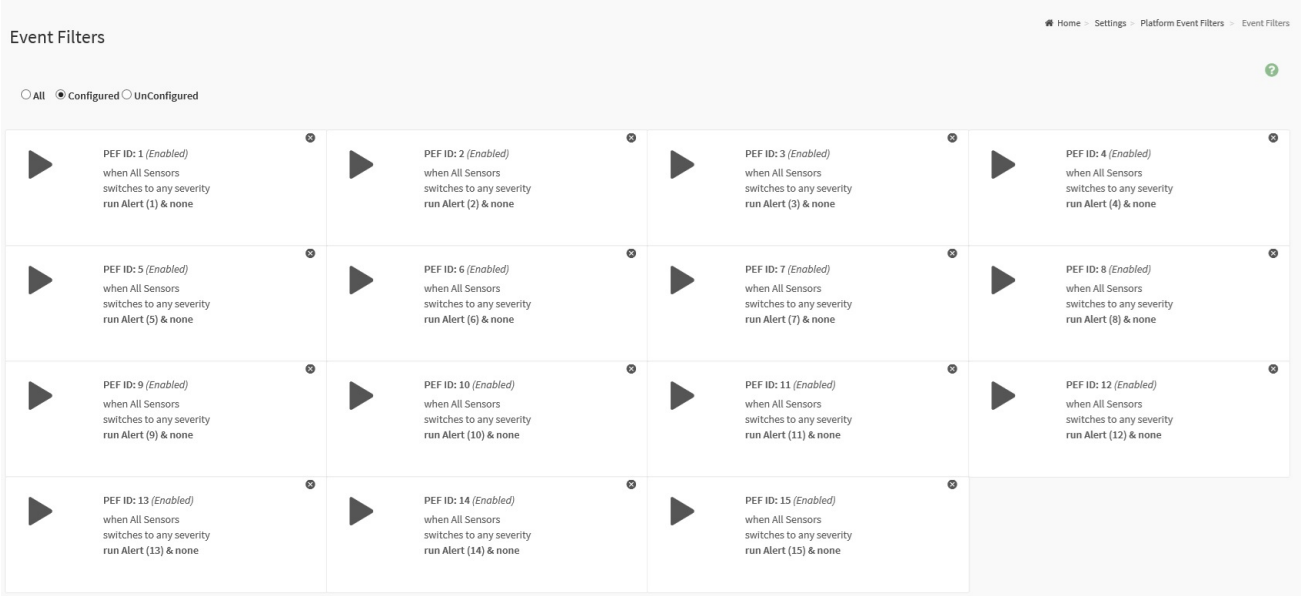


2.6.10 Home>Settings>Platform Event Filter

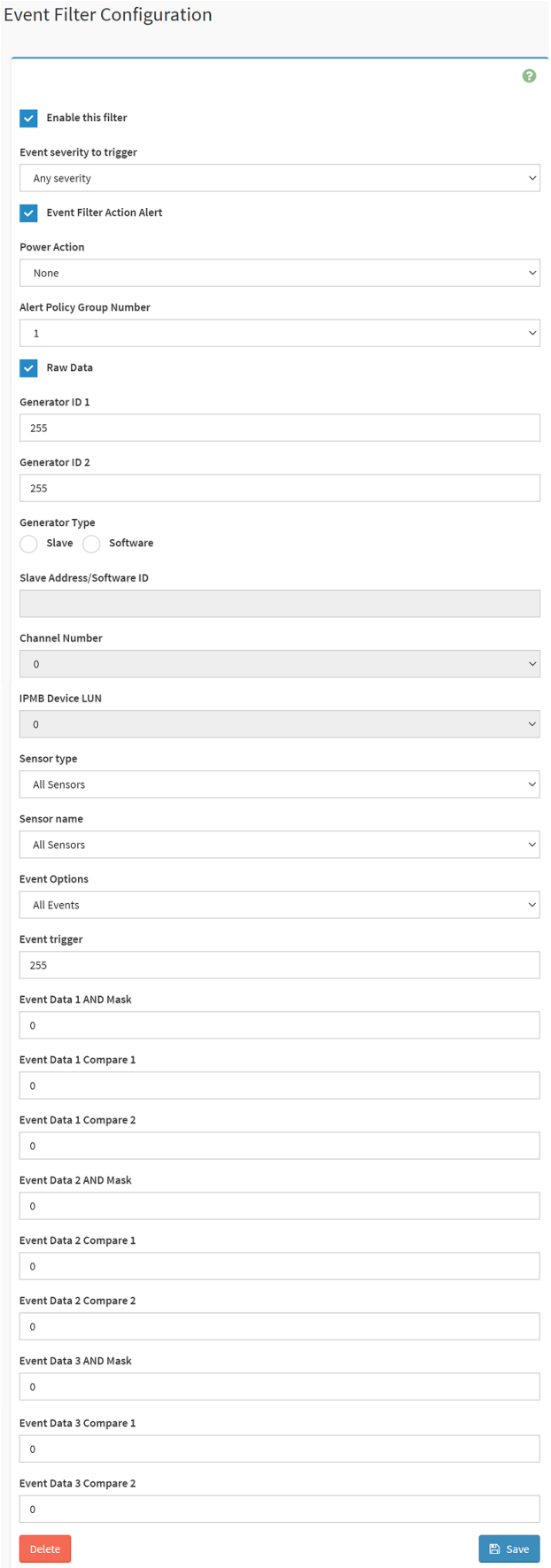


2.6.10.1 Home>Settings>Platform Event Filter >Event Filters

You can modify or add new event filters from here. By default, 15 event filter entries are configured among the 40 available slots. Choose All option to view available Configured and Unconfigured slots.
Choose Configured/Unconfigured option to view available Configured/Unconfigured slots.
Choose x icon to delete an event filter slot from the list



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

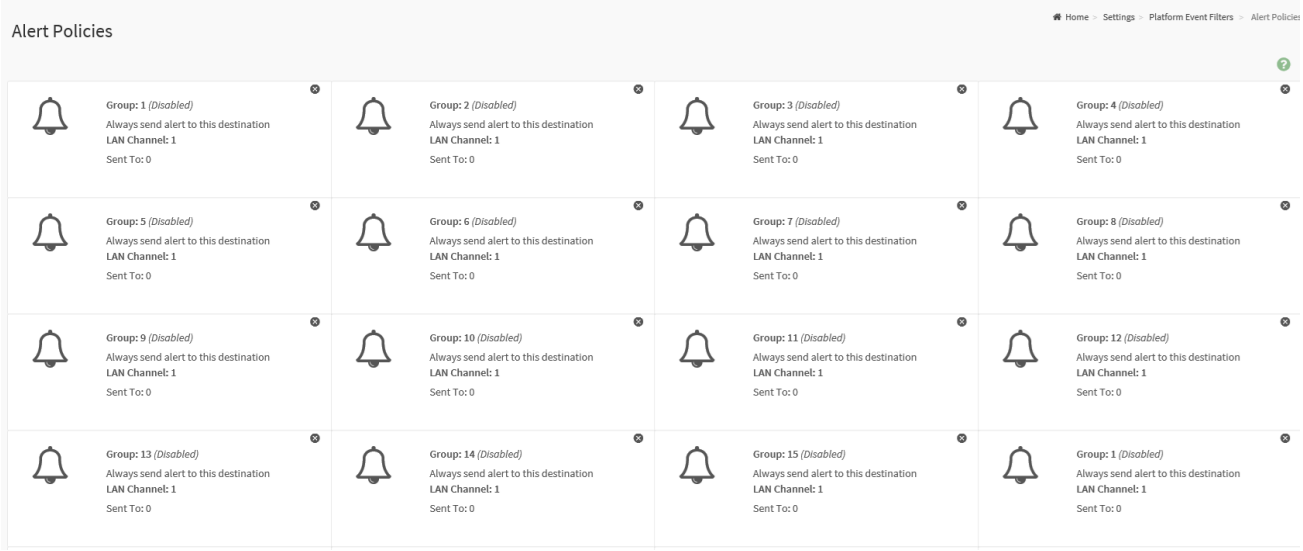


Item	Option	Description
Enable this filter	☑ ☐	Check the option 'Enable' to enable the PEF settings
Event severity to trigger	● Any severity ● New monitor state ● New information ● Normal state ● Non-Critical stage ● Critical state ● Non-Recoverable state	Choose any one of the Event Severity from the dropdown lists.
Event Filter Action Alert	☑ ☐	Check this option to enable PEF Alert action.
Power Action	● None ● Power Down ● Power Cycle ● Reset	Choose Power action to be either Power down, Reset or Power cycle from the dropdown list.
Alert Policy Group Number	1-15	Choose configured alert policy number from the dropdown list. Note: Alert Policy can be configured under Configuration->PEF->Alert Policy.
Raw Data	☑ ☐	Enable this option to enter the Generator ID with raw data.
Generator ID 1		Enter the raw generator ID1 data value.
Generator ID 2		Enter the raw generator ID2 data value. Note: In the RAW data field, prefix the value with '0x' to specify hexadecimal value.
Generator Type	● Slave ● Software	Choose the event generator as Slave Address – if event is generated from IPMB
Slave Address /Software ID		Choose System Software ID – if event is generated from system software
Channel Number		Choose 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		Choose the corresponding IPMB Device LUN if event is generated by IPMB

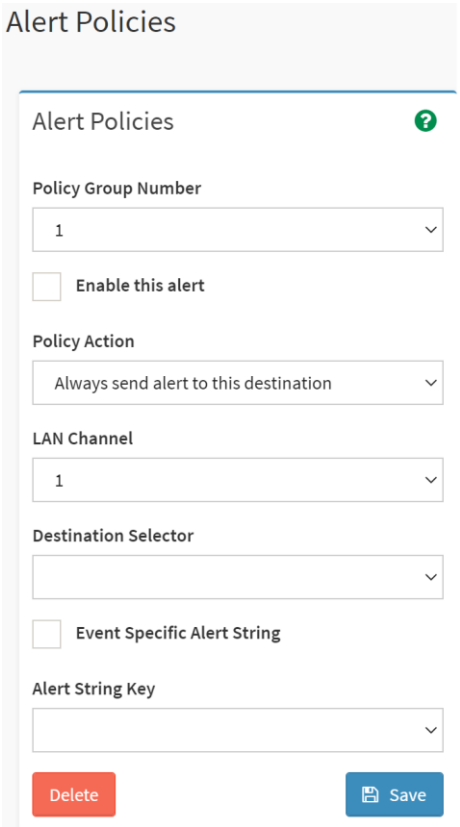
Sensor type	• All Sensors • Voltage • Temperature • Fan • Processor	Select the type of sensor that will trigger the event filter action.
Sensor Name	• All Sensors • +V12S_CPU1 • +V5A • …….	Choose the particular sensor from the sensor list.
Event Options	• All Events • Sensor Events	Choose event option to be either All events or Sensor specific events
Event trigger	0-255	This field is used to give Event/Reading type vale. Value ranges from 0 to 255
Event Data 1 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
Event Data 1 Compare1	0-255	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 1 Compare2	0-255	
Event Data 2 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
Event Data 2 Compare1	0-255	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 Compare2	0-255	
Event Data 3 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
Event Data 3 Compare1	0-255	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 3 Compare2	0-255	
Save	Save	Click button to save the changes made

2.6.10.2 Home>Settings>Platform Event Filters>Alert Policies

It shows all configured Alert policies and available slots.
You can modify or add new alert policy entry from here
Click x icon to delete an alert policy from the list
A maximum of 60 slots are available.



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

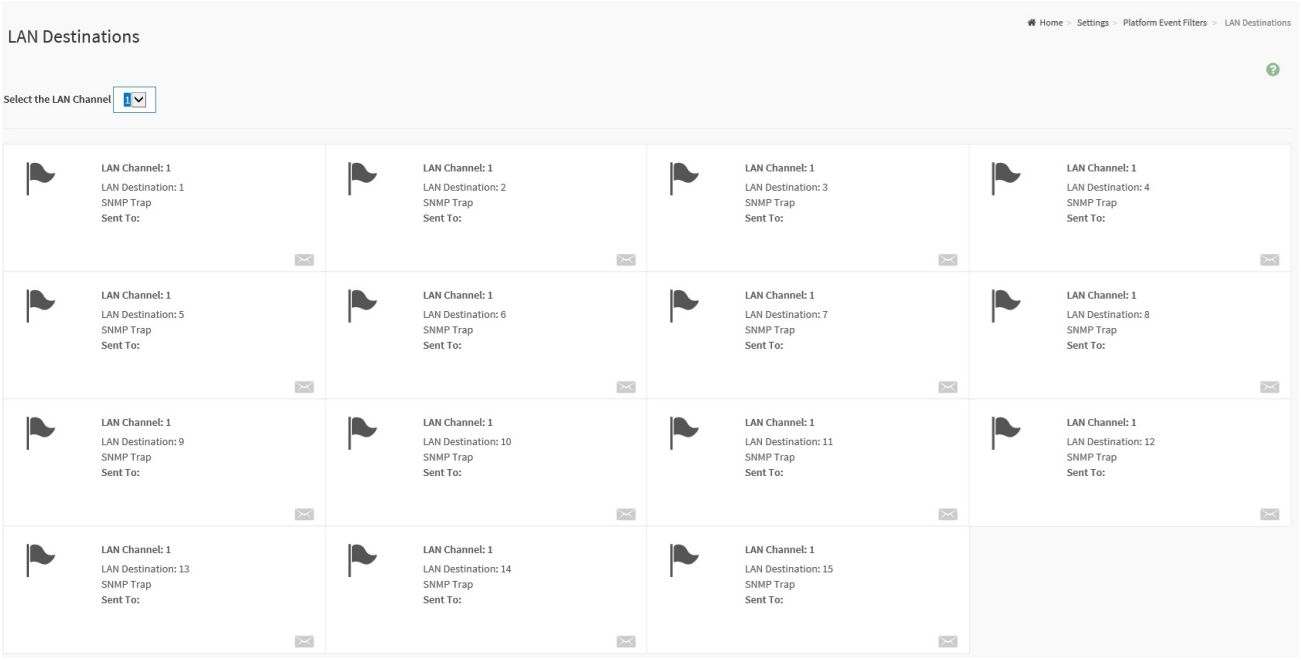


Item	Option	Description
Policy Group Number	1-15	Choose a policy number that was configured in the Event filter table
Enable this alert	☑ ☐	Check the option 'Enable' to enable the policy settings.
Policy Action	● Always send alert to this destination ● If previous successful ,skip this and comtinue(if configured) ● If previous successful ,switch to another channel (if configured) ● If previous successful ,switch to methods(if configured)	Choose any one of the Policy set values from the list. 0- Always send alert to this destination 1- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set. 2- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel. 3- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel. 4- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
LAN Channel	1	Choose a LAN channel for the policy
Destination Selector	1-15	Choose a destination from the configured destination list. Note: LAN Destinations have to be configured – under Configuration->PEF->LAN Destination
Event Specific Alert String	☑ ☐	Choose the box to specify an event specific Alert String
Alert String Key	1-40	Choose from a set of values (all linked to strings that are kept in the PEF configuration parameters), to specify which is to be sent for this Alert Policy entry.

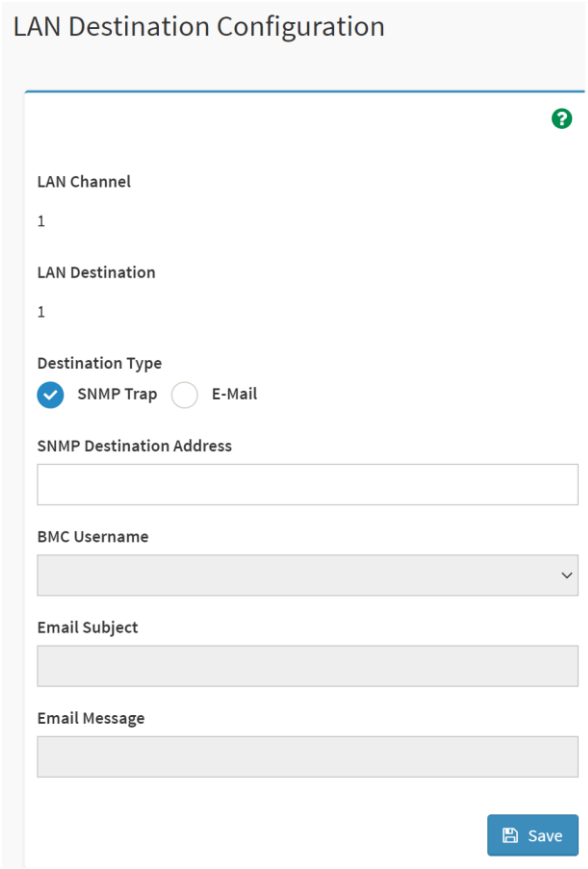
Delete	Delete	Click button to delete the changes
Save	Save	Click button to save the changes made

2.6.10.3 Home>Settings>Platform Event Filters>LAN Destinations

This shows all LAN destination slots. You can modify or add a new LAN destination entry from here.
Click x icon to delete an entry from the list.
A maximum of 15 slots are available.
Select an applicable LAN Channel from the list
Send Test Alert: Select a configured slot and click 'Send Test Alert' to generate a sample alert message to the configured destination.
Note: Test alert for emails can be sent only when SMTP configuration is enabled. This can be done under 'Settings->SMTP'. Make suer that SMTP server address and port numbers are configured properly.



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



Item	Option	Description
LAN Channel	1	Displays LAN Channel Number of the selected slot(read only)
LAN Destination	1	Displays Destination number of the selected slot(read only)
Destination Type	● SNMP Trap ● E-Mail	Select destination type.
SNMP Destination Address		If Destination type is SNMP Trap, then give the IP address of the system that will receive the alert. Destination address will support IPv4/IPv6 format
BMC Username		If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. Note: Email address for the user has to be configured under Settings->Users Management.
Email Subject		These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email

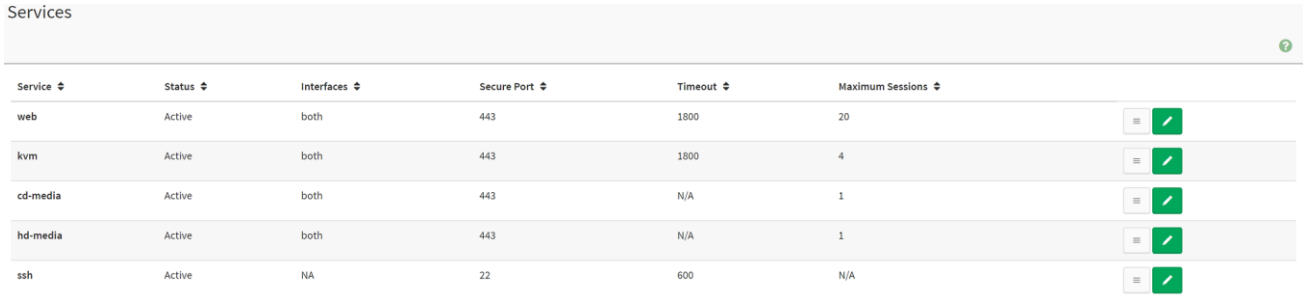
		address of the user in case of any severity events with a subject specified in subject field and will contain the messsage field's content as the email body. Note: These fields are not applicable for 'AMI-Format' email users.
Email Message		This fields must be configured if email alert is chosen as destination type. An email will be sent to the configurated 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	Click button to save the changes made

2.6.11 Home>Settings>Services

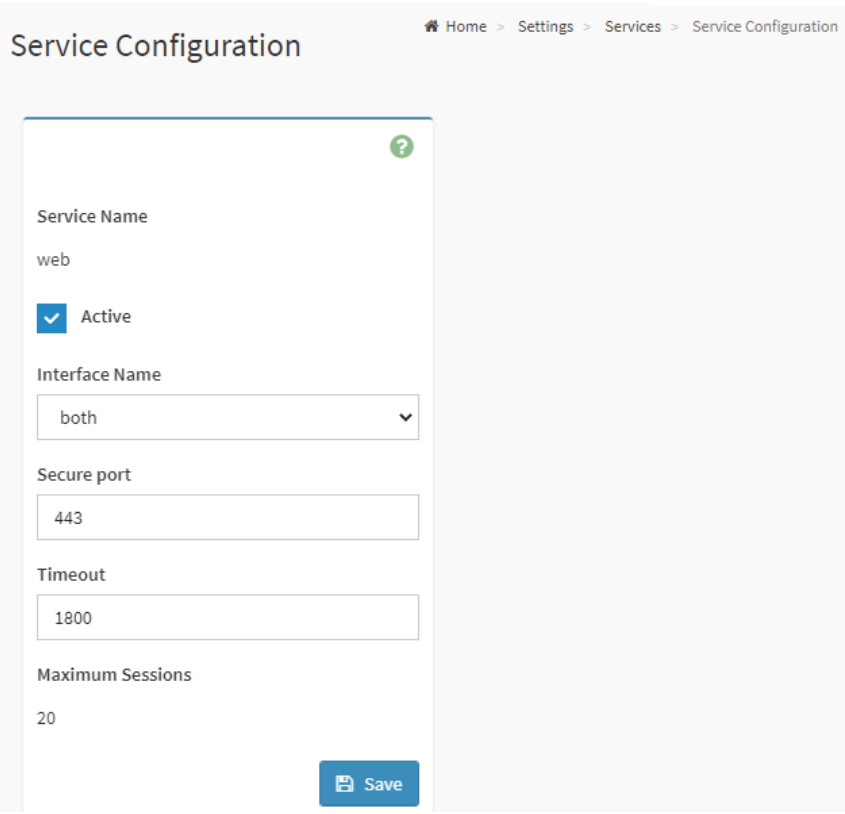
Below is a list of services running on this BMC. Also provided are the current status and other basic information about each.
Note: To modify a service, user must be an Administrator.

Click on  icon to modify the services configuration.

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



Home>Settings>Services> Service Configuration



Item	Option	Description
Service Name		Displays service name of the selected slot (read only)
Active	☑ ☐	Current State Displays the current status of the service, either active or inactive. Check this box to activate the service.
Interface Name	● eth0 ● both	This indicate the interface on which the service is running. The user can choose any one of the available interfaces. Note: Service mapping to disabled interfaces will not work. ♦ Status of interface can be checked/enabled,under Configuation->Network->LAN Settings. ♦ Media and KVM interfaces are readonly when single port is enabled
Secure port		Used to configure secure port numbers for the services. ♦ Web default port is 443 ♦ KVM default port is 7582 ♦ CD Media default port is 5124 ♦ HD Media default port is 5127 ♦ SSH default port is 22

		• Port value ranges form 1 to 65535 Note : Port 80 is blocked for TCP/UDP protocols
Timeout		Where supported , user can configure the session timeout value. • Web and KVM timeout value ranges from 300 to 1800 seconds. • Web timeout will be ignored if there is any ongoing KVM session • SSH timeout value ranges from 60 to 1800 seconds • Timeout value should be in multiples of 60 seconds.
Maximum Sessions		Displays the maximum number of allowed sessions for the service.
Save	Save	Click button to save the changes made

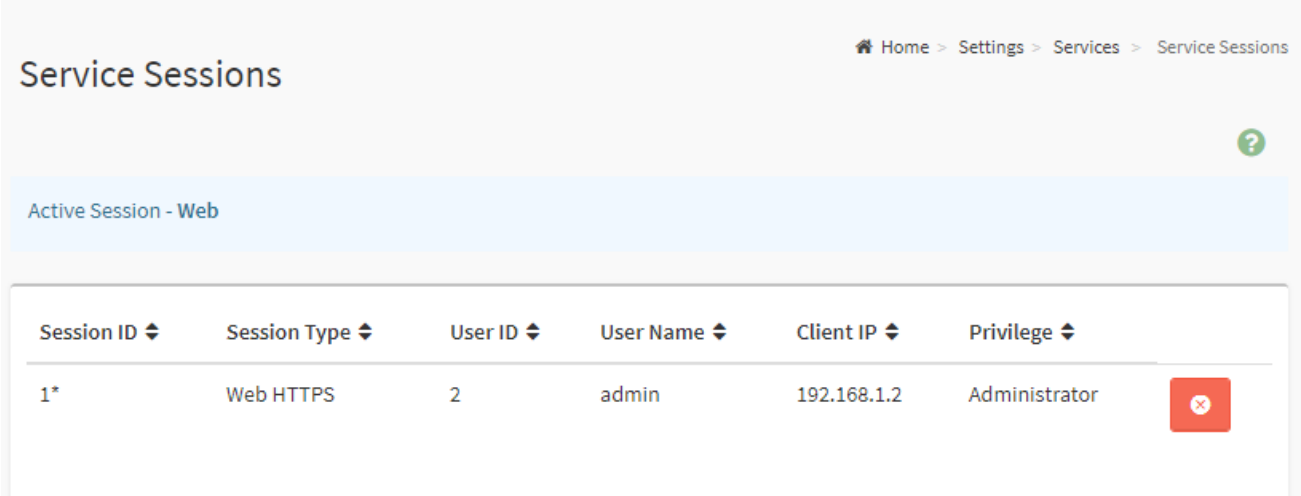
Home>Settings>Services> Service Sessions

This page displays basic information about the Active sessions on this BMC. To terminate the session , user must be an Administrator.

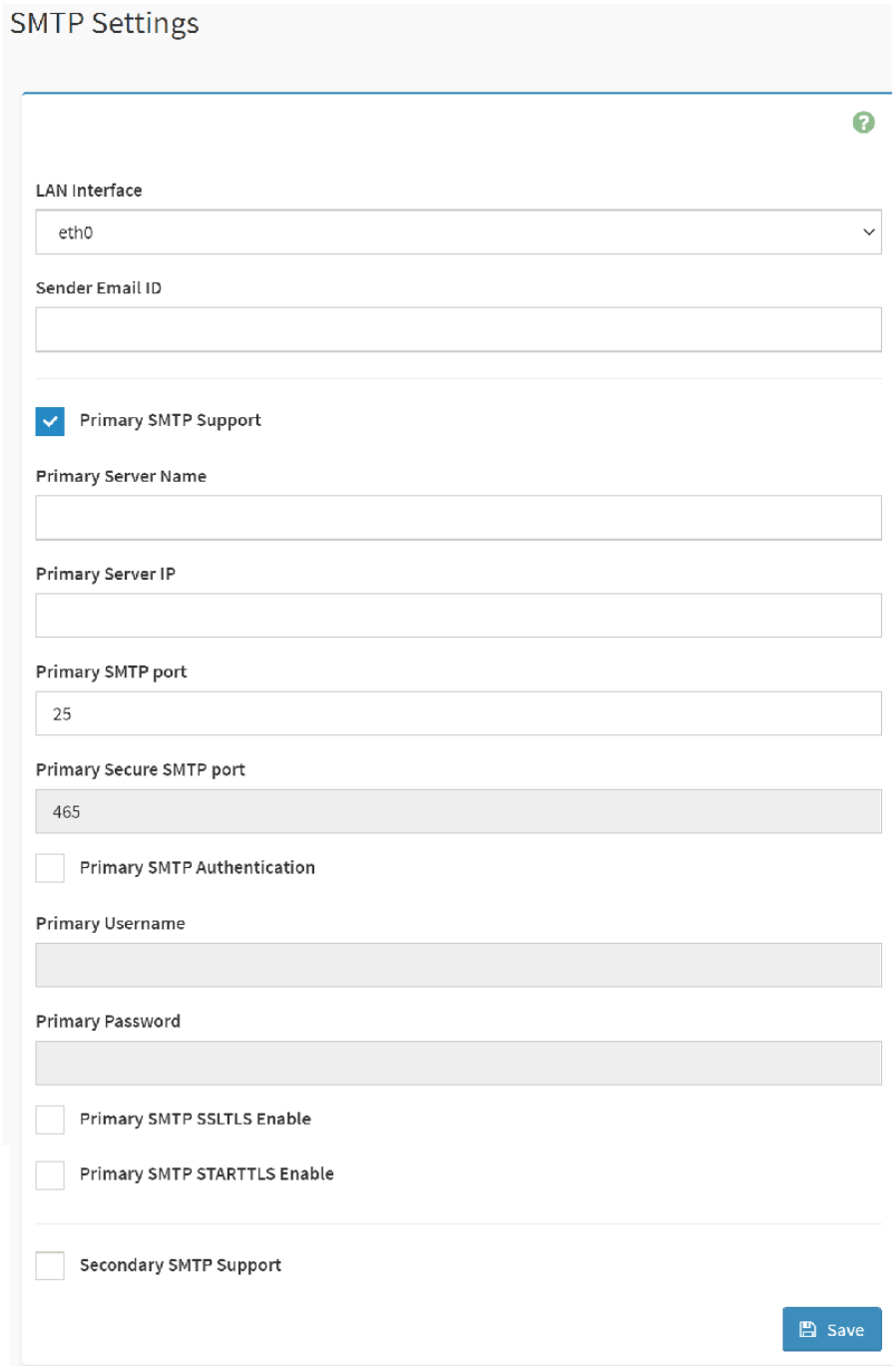
Click on  to terminate the particular session of the service

Note : The default user ID ranges for the supported PAM Modules are:

- Active Directory User : from 3000 – 3999
- LDAP/E-Directory User : from 2000 – 2999
- RADIUS User : from 4000 - 4999



2.6.12 Home>Settings> SMTP Settings

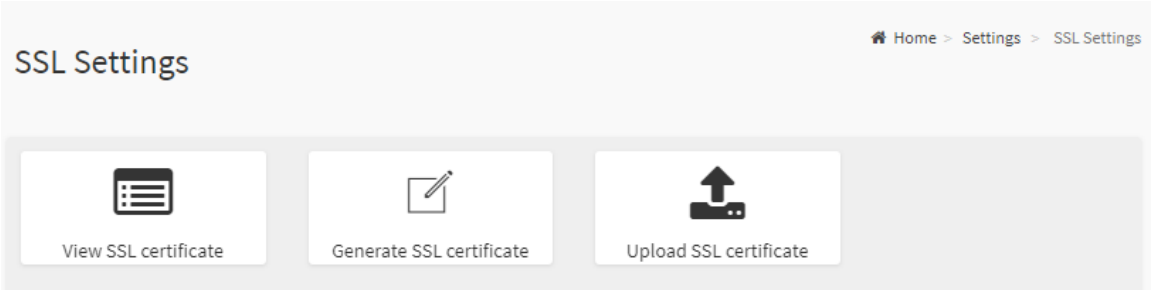


Item	Option	Description
Lan interface	eth0	Select the Lan interface to be configured
Sender Email ID		Enter a valid 'Sender Email ID' on the SMTP Server. Maximum allowed size for Email ID is 64 bytes,which includes username and domain name.
Primary SMTP	☑	Check this option to enable SMTP support for the BMC

Support	☐	
Primary Server Name		Enter the 'Machine Name' of the SMTP Server. This field is for information Purpose Only. Machine Name is a string of 25 alpha-numeric characters maximu. Spaces and special characters are not allowed
Primary Server IP		Enter the Server Address for the SMTP server Server address will support the following ♦ IPv4/IPv6 address format ♦ Host name format
Primary SMTP port		Specify the SMTP port Default port is 25 Port value ranges from 1 to 65535
Primary Secure SMTP port		Specify the SMTP secure port Default port is 465 Port value ranges from 1 to 65535
Primary SMTP Authentication	☑ ☐	Check the option 'Enable' to enable SMTP Authentication. Note: Support SMTP Server Authentication Types are: CRAM-MD5. LOGIN PLAIN If the SMTP server does not support any of the above authentication types, the user will get an error message starting, 'Authentication type is not supported by SMTP Server'
Primary Username		Enter user name required to access SMTP Accounts. User Name can be of length 4 to 64 alpha-numeric characters, '.' , '@' , '-' ,'_' It must start win an alphabetical character Other special characters are not allowed
Primary Password		Enter the password for the SMTP User Account. Password must be at least 4 characters long. White space is not allowed Note:This field will not allow more than 64 characters.
Primary SMTP SSLTLS Enable	☑ ☐	Check the option to enable the SMTP SSLTLS protocol
Primary SMTP STARTTLS Enable	☑ ☐	Check the option to enable the SMTP STARTTLS protocol

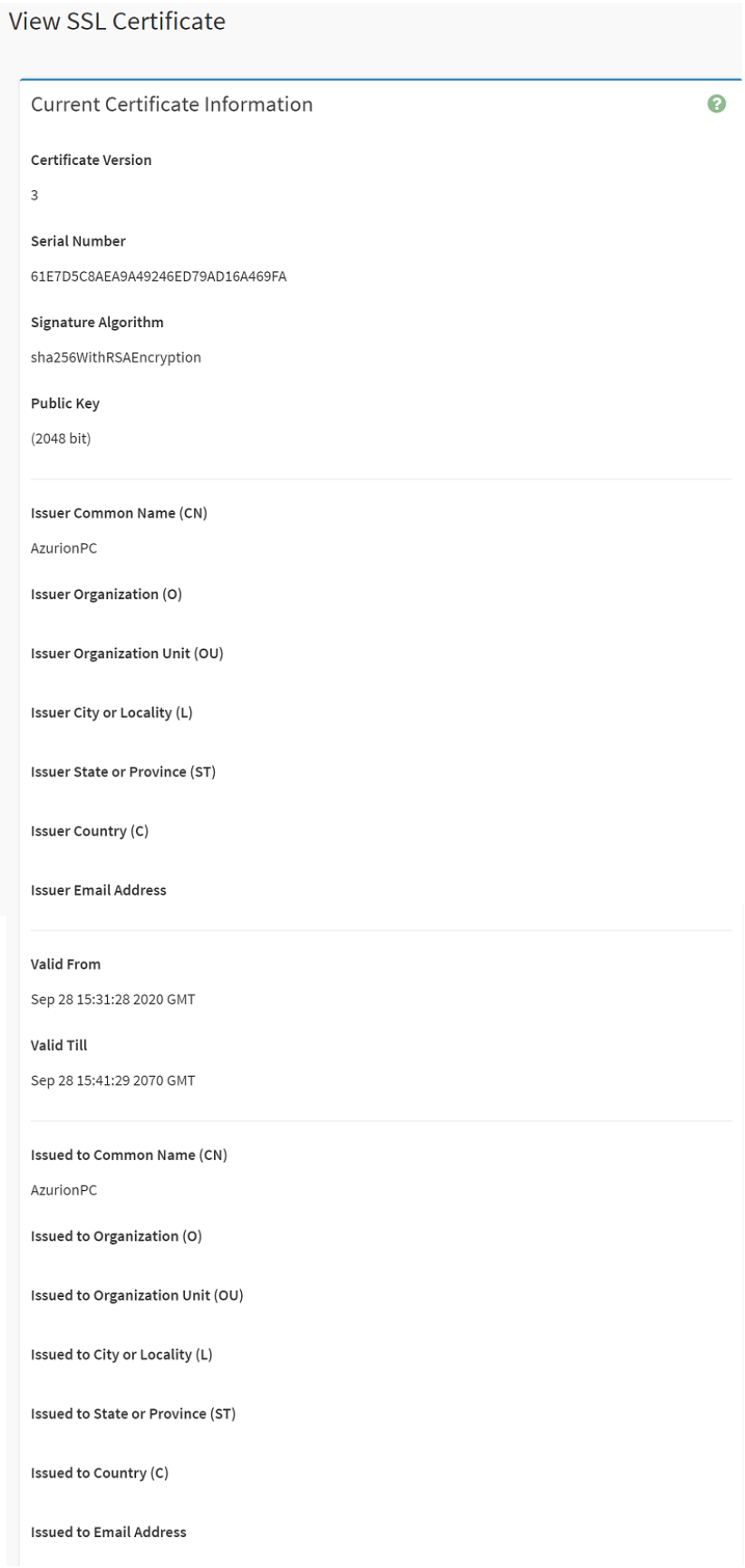
Secondry SMTP Support	☑ ☐	Check this option to enable Secondary SMTP support for the BMC.
Save	Save	Click button to save the changes made

2.6.13 Home>Settings>SSL Settings

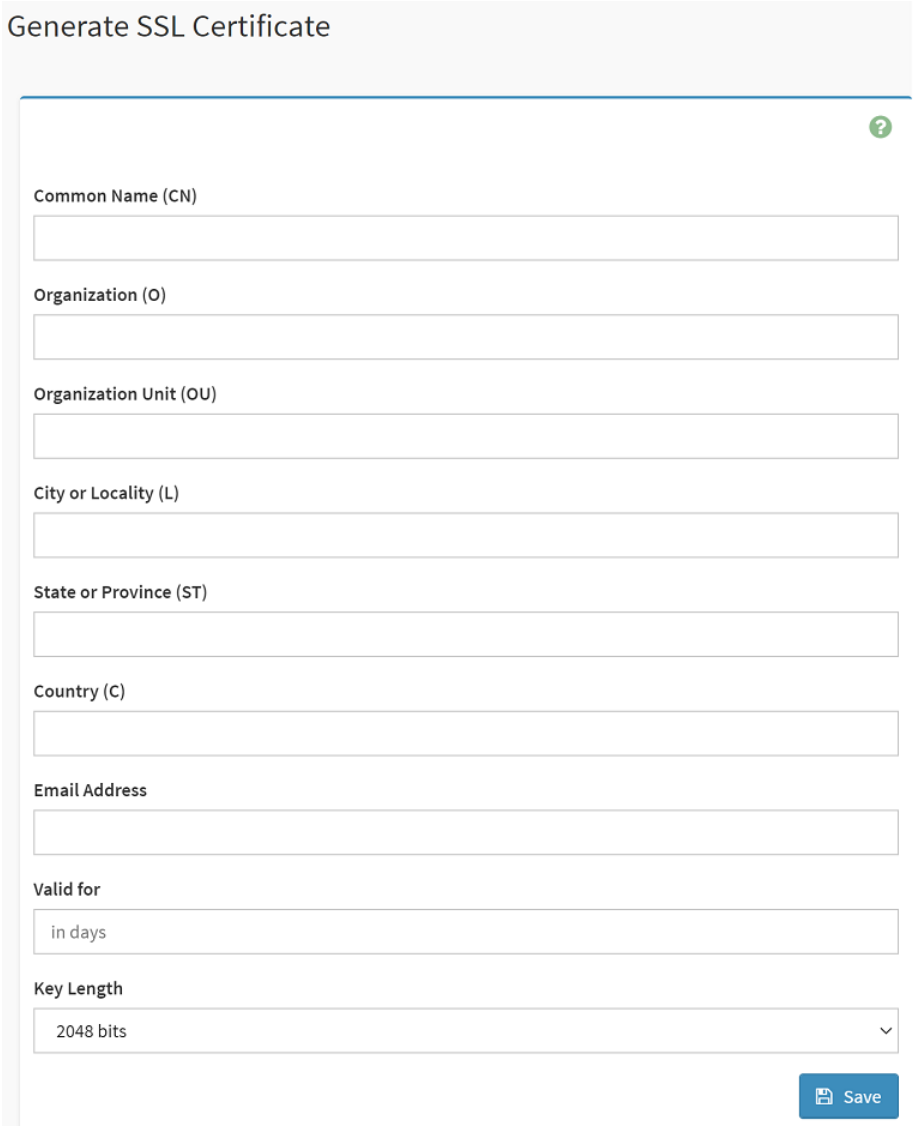


2.6.13.1 Home>Settings>SSL Settings> View SSL Certificate

This page displays the Current Certificate Information.



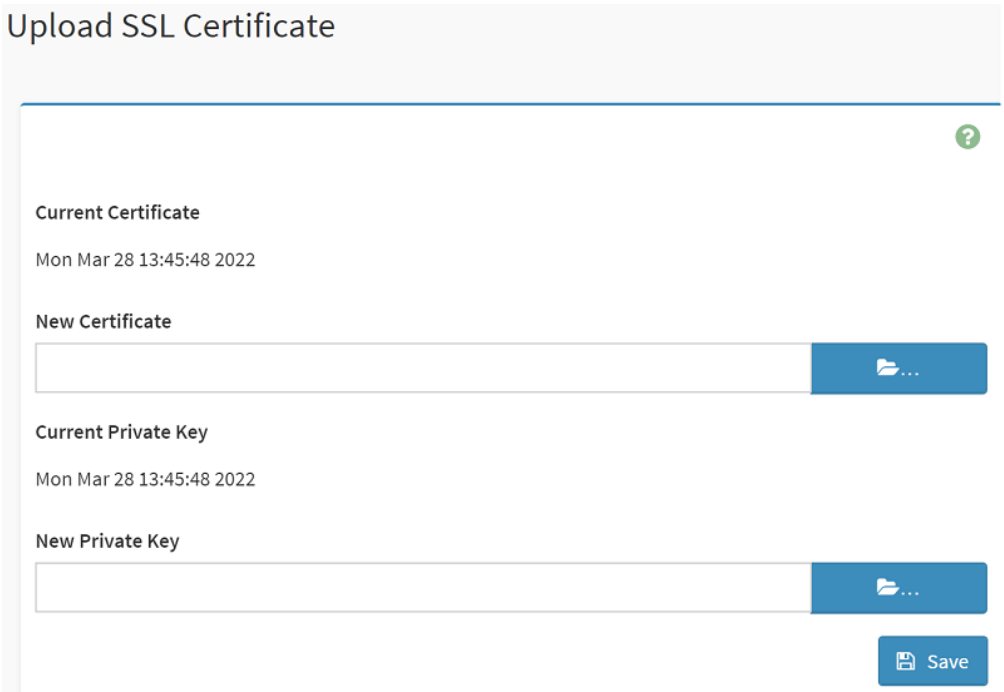
2.6.13.2 Home>Settings>SSL Settings>Generate SSL Certificate



Item	Option	Description
Common Name(CN)		Common name for which the certificate is to be generated. ♦ Maximum of 64 alpha-numeric characters ♦ Character '#' and '$' are not allowed.
Organizaion(O)		Name of the organization for which certificate is to be generated. ♦ Maximum of 64 alpha-numeric characters ♦ Character '#' and '$' are not allowed.
Organizaion Unit(OU)		Section or Unit of the organization for which certificate is to be generated ♦ Maximum of 64 alpha-numeric characters ♦ Character '#' and '$' are not allowed.
City or Locality(L)		City or Locality. ♦ Maximum of 64 alpha-numeric characters

		• Character '#' and '$' are not allowed.
State or Province(ST)		State or Province. • Maximum of 64 alpha-numeric characters • Character '#' and '$' are not allowed.
Country(C)		Country code. • Only two characters are allowed • Special characters are not allowed
Email Address		Email addresss of organization
Valid for		Requested validity days for the certificate Value ranges form 1 to 3650 days
Key Length	2048 bits	Choose the key length bit value of the certificare.
Save	Save	Click button to save the changes made

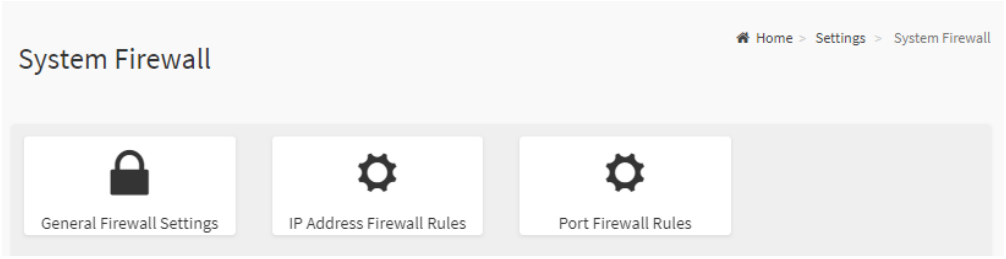
2.6.13.3 Home>Settings>SSL Settings>Upload SSL Certificate



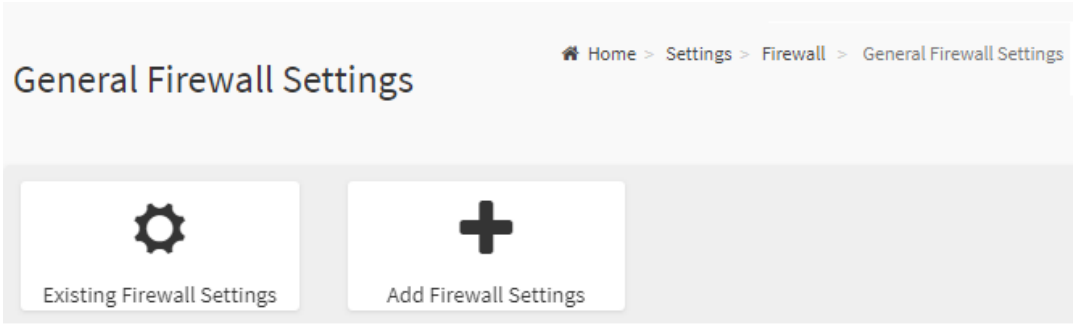
Item	Option	Description
Current Certificate		The information of the Current Certificate and date/time of its upload will be displayed(read-only)
New Certificate		Browse and navigate to the new certificate file. Certificate file should be of pem type.
Current Private Key		Information for the current private 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		Click button to save the changes made

2.6.14 Home>Settings>System firewall

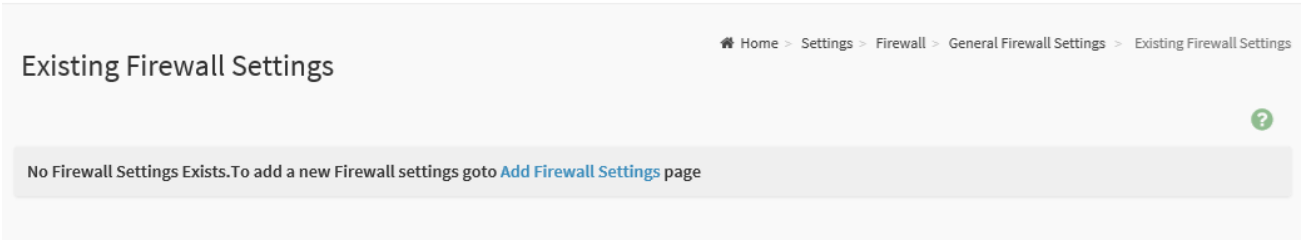


2.6.14.1 Home>Settings> Firewall >General Firewall Settings

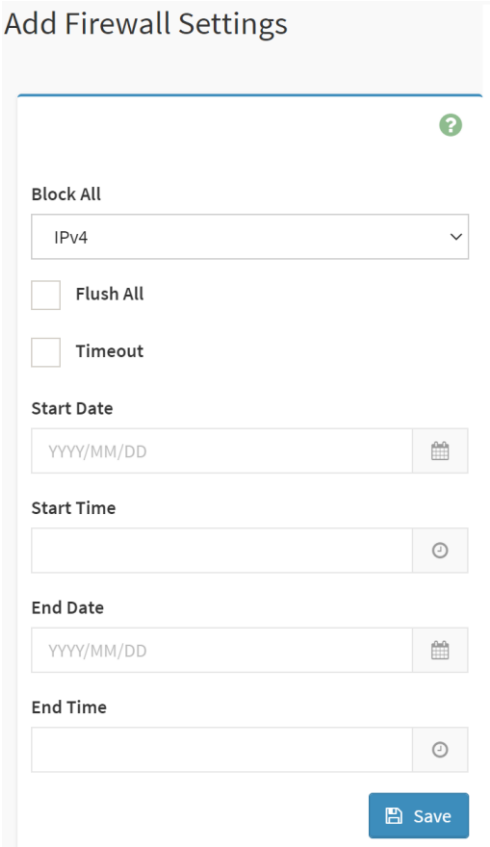


2.6.14.2 Home>Settings>System firewall >General Firewall Setting >Existing Firewall Settings

This page displays the list of general firewall rules on this BMC

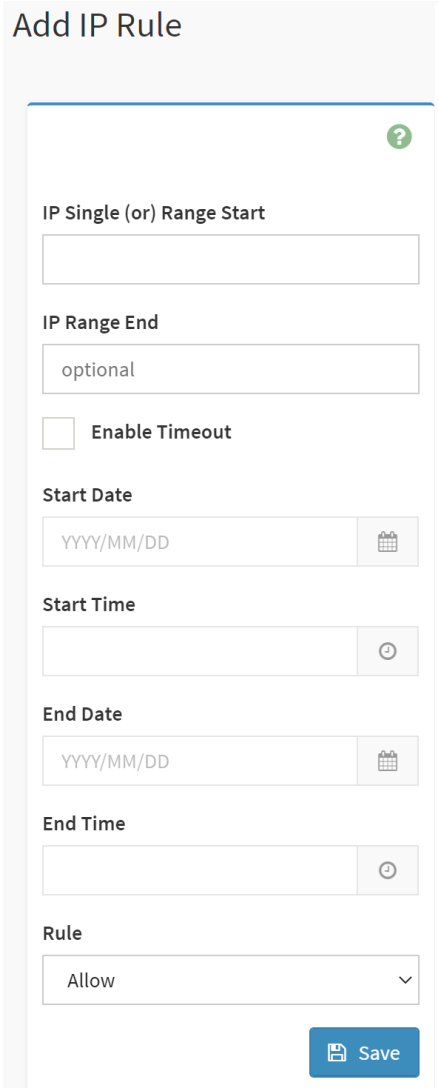


2.6.14.3 Home>Settings> Firewall >General Firewall Setting >Add Firewall Settings



Item	Option	Description
Block All	● IPv4 ● IPv6 ● Both	This option will block all incoming IPs and Ports
Flush All	☑ ☐	This option is used to flush all existing system firewall rules
Timeout	☑ ☐	This option is used to enable or disable firewall rules with timeout.
Start Date		The firewall rule will become effective from this date
Start Time		The firewall rule will become effective from this time
End Date		The firewall rule will expire on this date
End Time		The firewall rule will expire at this time
Save	Save	Click button to save the changes made

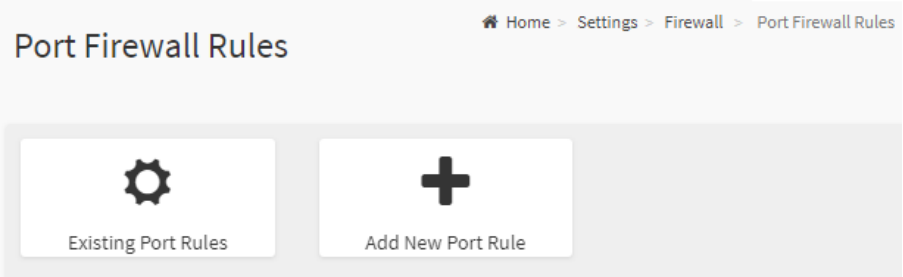
2.6.14.4 Home>Settings>Firewall >General Firewall Setting >IP Firewall Rules >Add IP Rule



Item	Option	Description
IP Single (or) Range Start		This field is used for entering an IP address or the start of a range of IP addresses. IP address must follow the IPv4 format.
IP Range End		This field is used to indicate the IP address or end of an IP address range
Enable Timeout		This option is used to enable or disable timeout
Start Date		The firewall rule will become effective from this date
Start Time		The firewall rule will become effective from this time

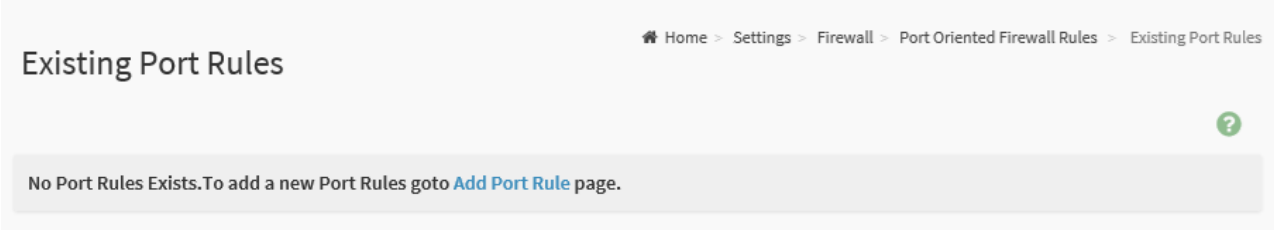
End Date		The firewall rule will expire on this date
End Time		The firewall rule will expire at this time
Rule	● Allow ● Block	This field is used for allow or block this rule.
Save	Save	Click button to save the changes made

2.6.14.5 Home>Settings>System Firewall >Port Firewall Rules

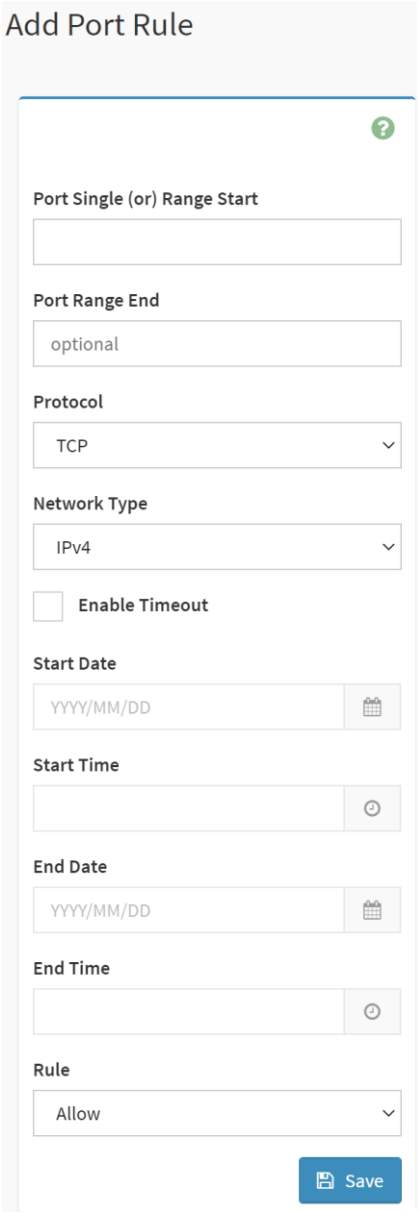


2.6.14.6 Home>Settings>System Firewall >Port Firewall Rules >Existing Port Rules

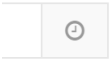
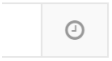
This page display the list of existing IP firewall rules



2.6.14.7 Home>Settings>System Firewall >Port Firewall Rules >Add Port Rule

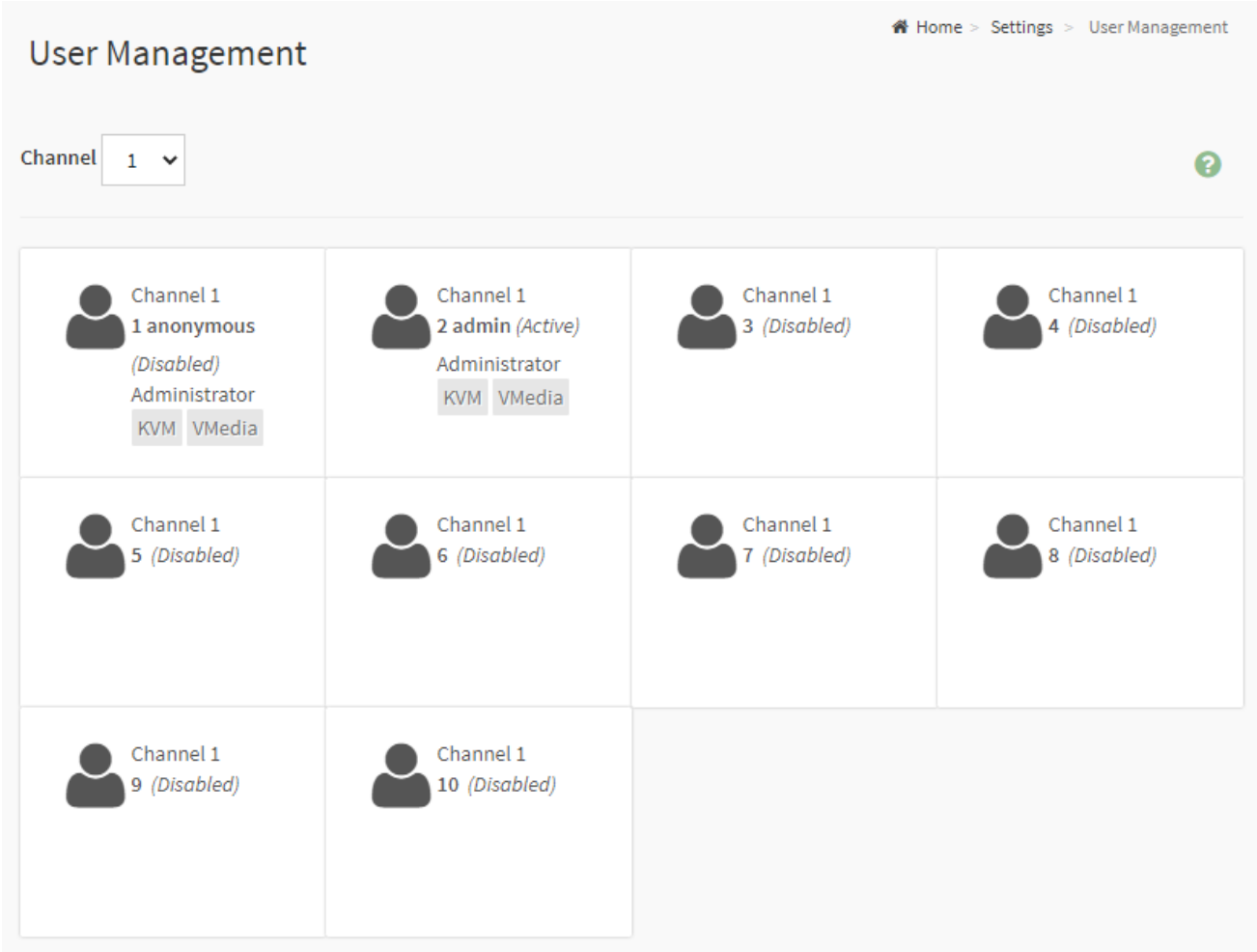


Item	Option	Description
IP Single (or) Range Start		This field is used to specify the Port or start of a range of Port Addresses. Port value ranges from 1 to 65535. Note: Port 80 is blocked for TCP/UDP protocols
IP Range End		This field is used to configure the Port or end of a range of Port Addresses
Protocol	● TCP ● UDP ● Both	Select which protocol to support.
Network Type	● IPv4	Select which network type to support.

	● IPv6 ● Both	
Enable Timeout		This option is used to configure timeout support for the new rule.
Start Date		Click field to select the duration of filter
Start Time		Click field to select the duration of filter
End Date		Click field to select the duration of filter
End Time		Click field to select the duration of filter
Rule	● Allow ● Block	This field is used for allow or block this rule.
Save		Click button to save the changes made

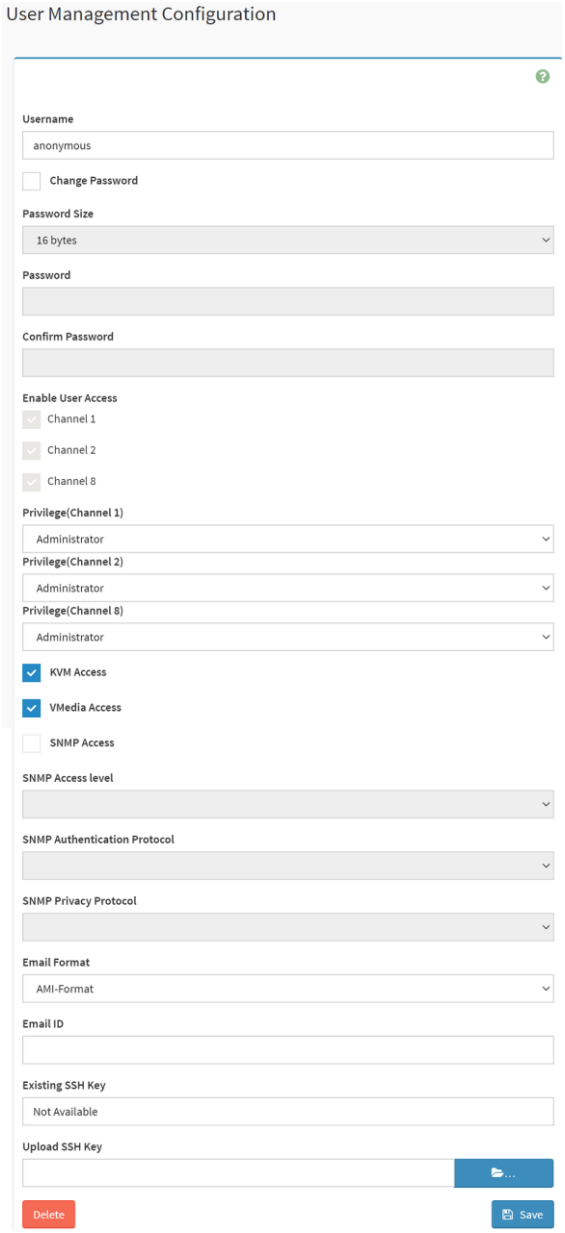
2.6.15 Home>Settings>User management

The list below shows the currently configured user for each LAN channel. To Add or Edit a user, click on any available slot. To Delete a user from the list, click its x icon.



Item	Option	Description
Channel	● 1 ● 2 ● 8	

2.6.15.1 Home>Settings>User management> User Management Configuration

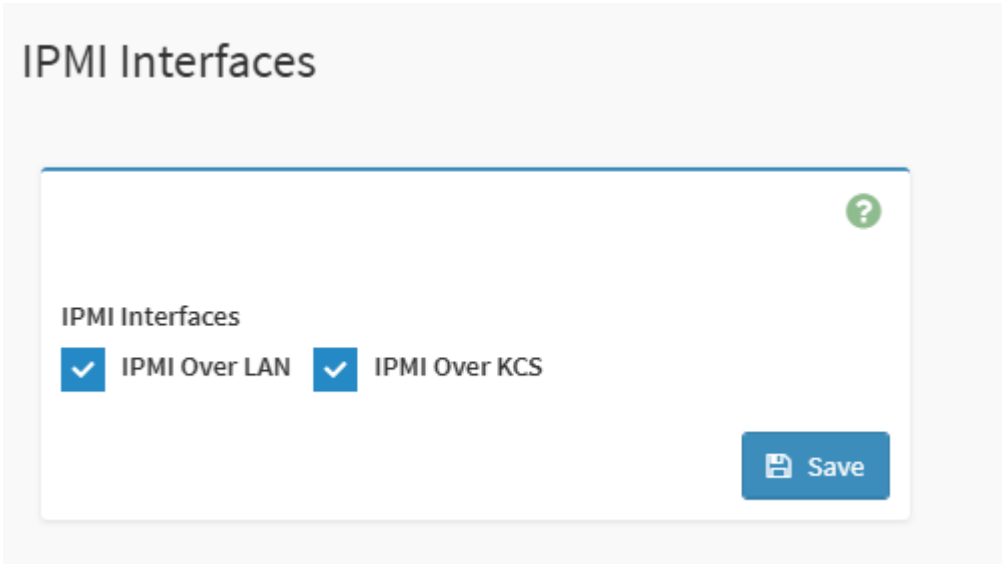


Item	Option	Description
Username		Enter the name of the new user. ♦ String of 1 to 16 alpha-numeric characters. ♦ Start with an alphabetical character. ♦ Case-sensitive ♦ '-' , '_' , '@' are allowed.
Change Password	☑ ☐	Select this option to change the password.
Password Size	● 16 bytes	Select the preferred size for the password.

	• 20 bytes	
Password		Enter a strong password consisting of at least one upper case letter,alpha-numeric characters,and special characters Note: Password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.
Confirm Password	☑ ☐	Confirm the password
Channel 1	☑ ☐	Check the boxed to enabled network access for the user. Upon enabling, the corresponding IPMI messaging privilege will be assigned to the user. Note: It is recommended that the IPMI messaging option should be enabled as well if user is created through IPMI
Channel 2	☑ ☐	
Channel 8	☑ ☐	
Privilege(Channel 1)	• User • Administrator • Operator • None • OEM	Select the privilege level for each channel to be assigned to this user for access to the BMC through the netowrk interface. There are 5 levels of Network Privileges ♦ User ♦ Administrator ♦ Operator ♦ None ♦ OEM
Privilege(Channel 2)	• User • Administrator • Operator • None • OEM	
Privilege(Channel 8)	• User • Administrator • Operator • None • OEM	
KVM Access	☑ ☐	This checkbox is used to assign the KVM privilege for the user
VMedia Access	☑ ☐	This checkbox is used to assign the VMedia privilege for the user
SNMP Access	☑ ☐	Check the box to enable SNMP access for the user.
SNMP Access level		Choose the SNMP Access level option for user from the SNMP Access level (SHA or MD5) drop-down list. Either it can be Read Only or Read Write.
SNMP		Choose an SNMP Authentication Protocol for this user.

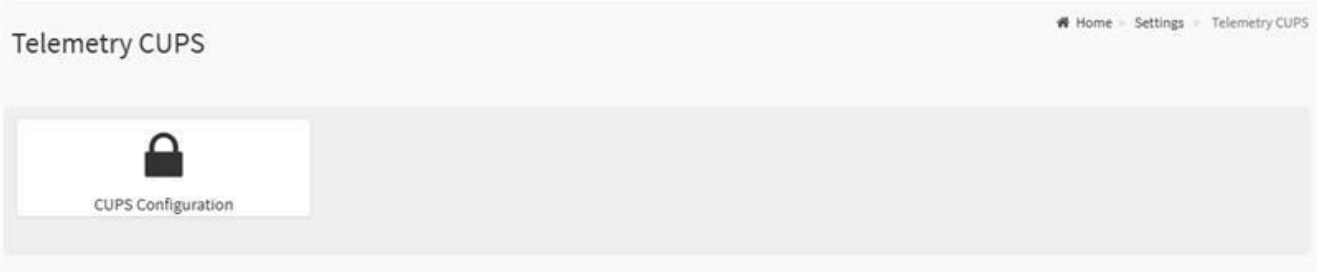
Authentication Protocol		Note: Password field becomes mandatory whenever the authentication protocol is changed.
SNMP Privacy Protocol		Choose the Encryption algorithm to be used for the SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.
Email Format	• AMI-Format • Fixed Subject-Format	AMI-Format: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description. Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.
Email ID		enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address. Maximum allowed size for Email ID is 64bytes (including username and domain name.)
Existing SSH Key		If available, the uploaded SSH key information will be displayed(read-only)
Upload SSH Key	...	Use Browse button to navigate to the new public SSH key file. SSH key file should be of pub type.
Save	Save	Click button to save the changes made

2.6.16 Home > Settings > IPMI Interfaces



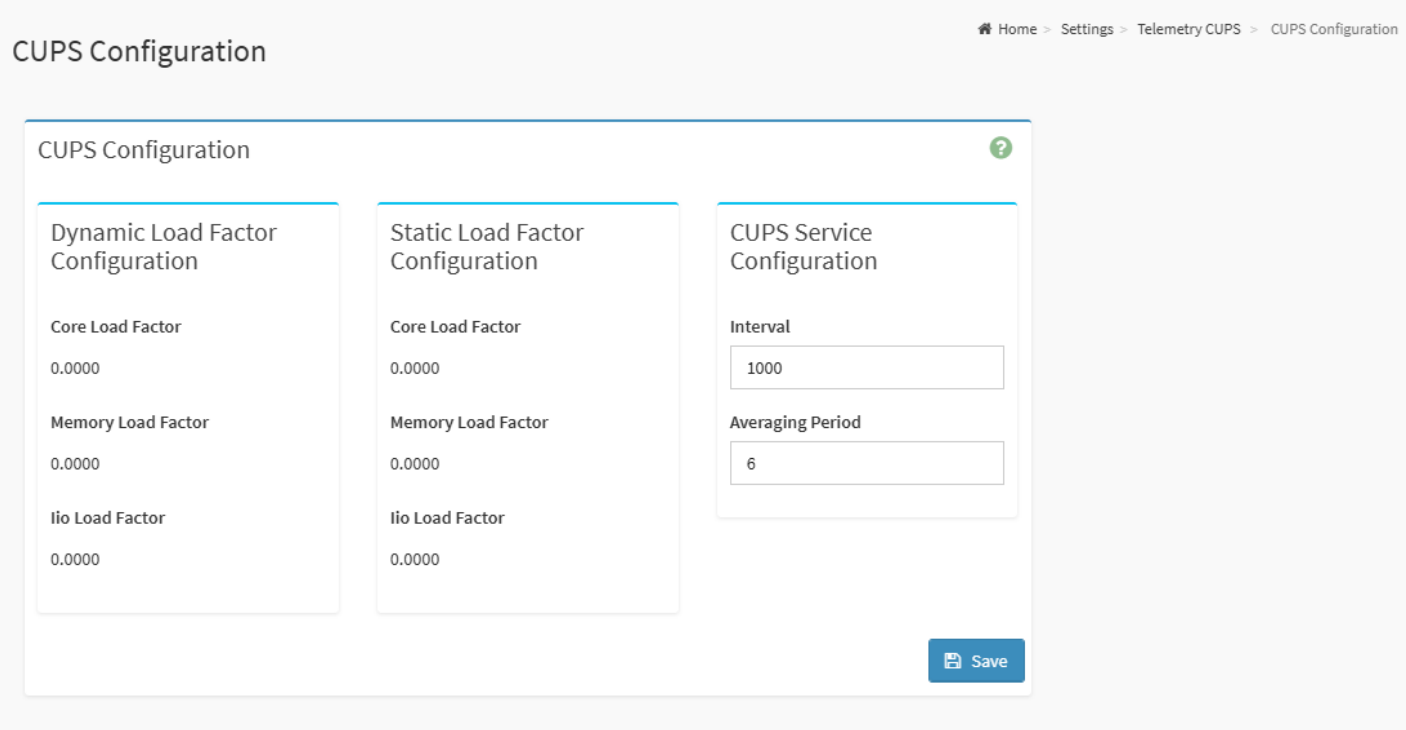
2.6.17 Home > Settings > Telemetry CUPS

CUPs provides a mechanism to Compute Usage per second for CPU, Memory and ADD in cards. Also describe how much CPU/Memory and IIO current and average usage per second.



2.6.17.1 Home > Settings > Telemetry CUPS > CUPS Configuration

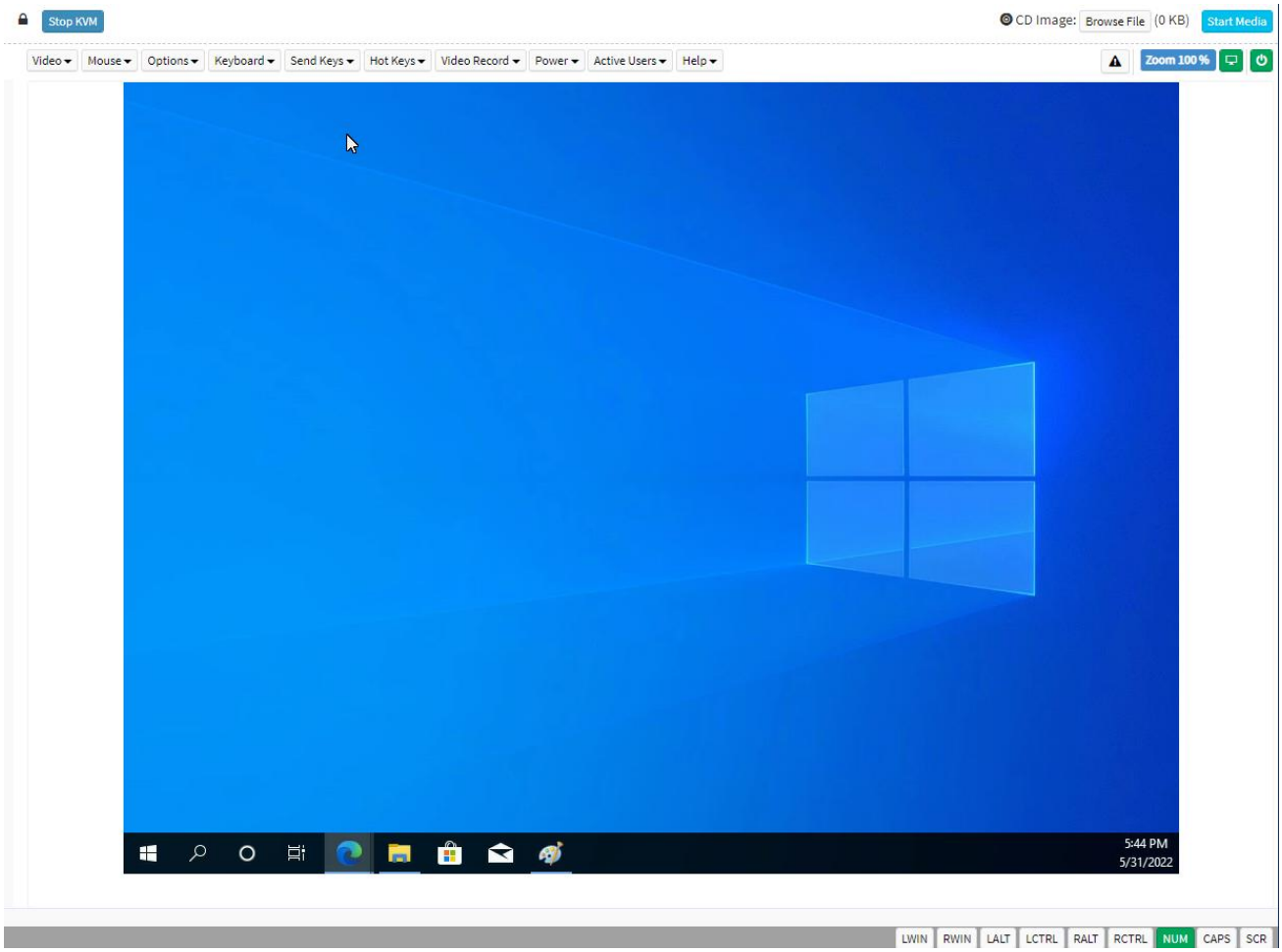
This page could config setting of interval and averaging period.



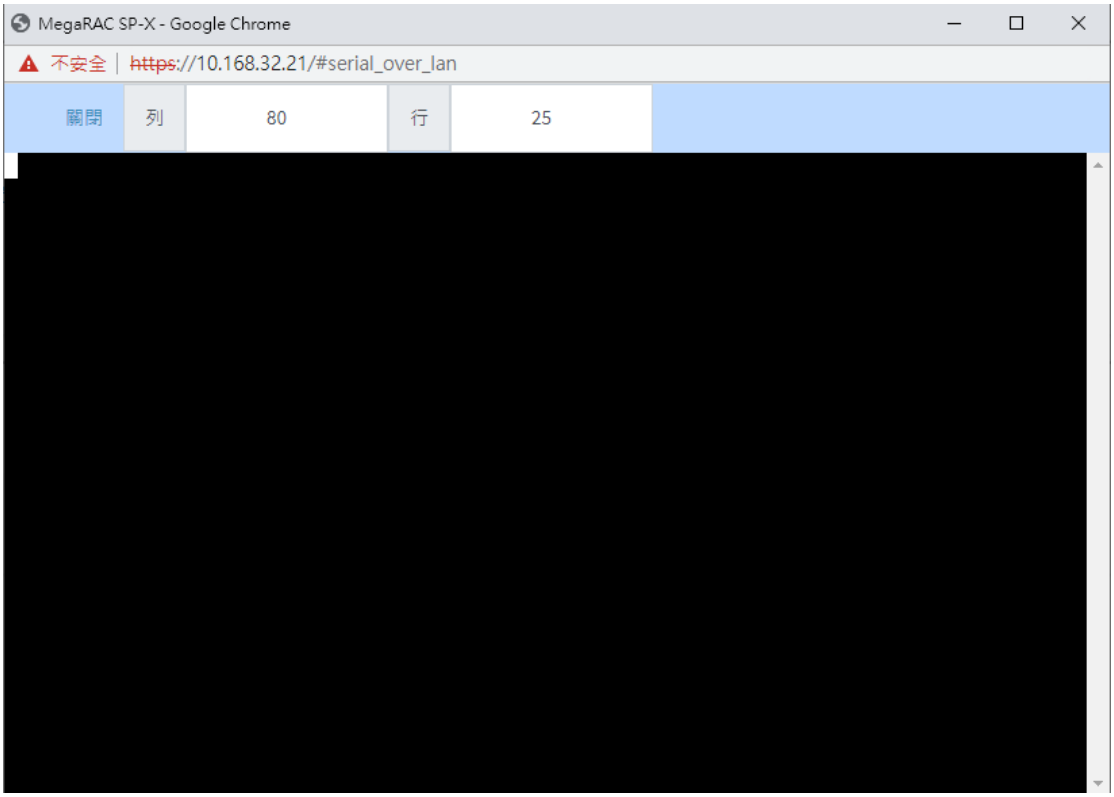
2.7 HOME> REMOTE CONTROL



2.7.1 Home>Remote Control >H5Viewer



2.7.2 Home>Remote Control >Serial Over LAN

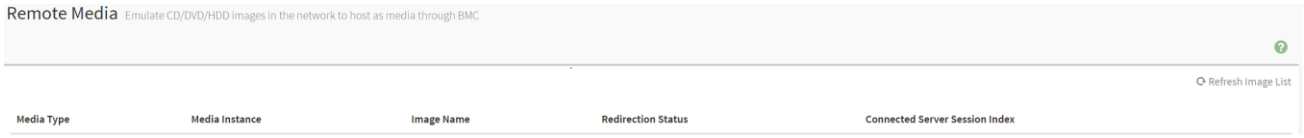


2.8 HOME>IMAGE REDIRECTION



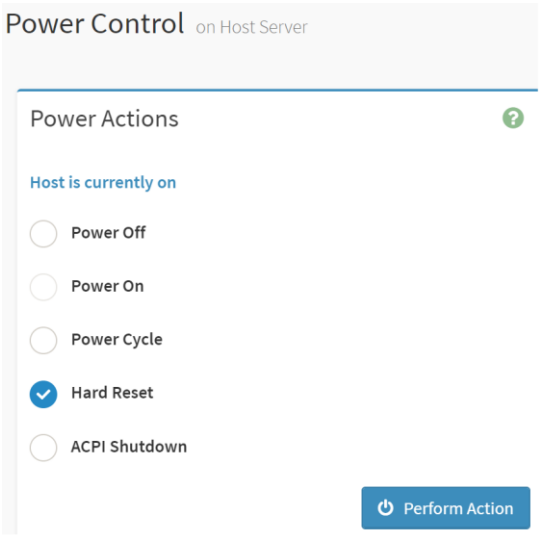
2.8.1 Home >Image Redirection>Remote Media

The displayed table shows remote images available to the BMC. You can start redirection or clear the image from here. Up to 4 images can be added for each image type, depending on your configuration.



2.9 HOME> POWER CONTROL

If user first open Power Control page ,this icon means host is currently on this power stage.

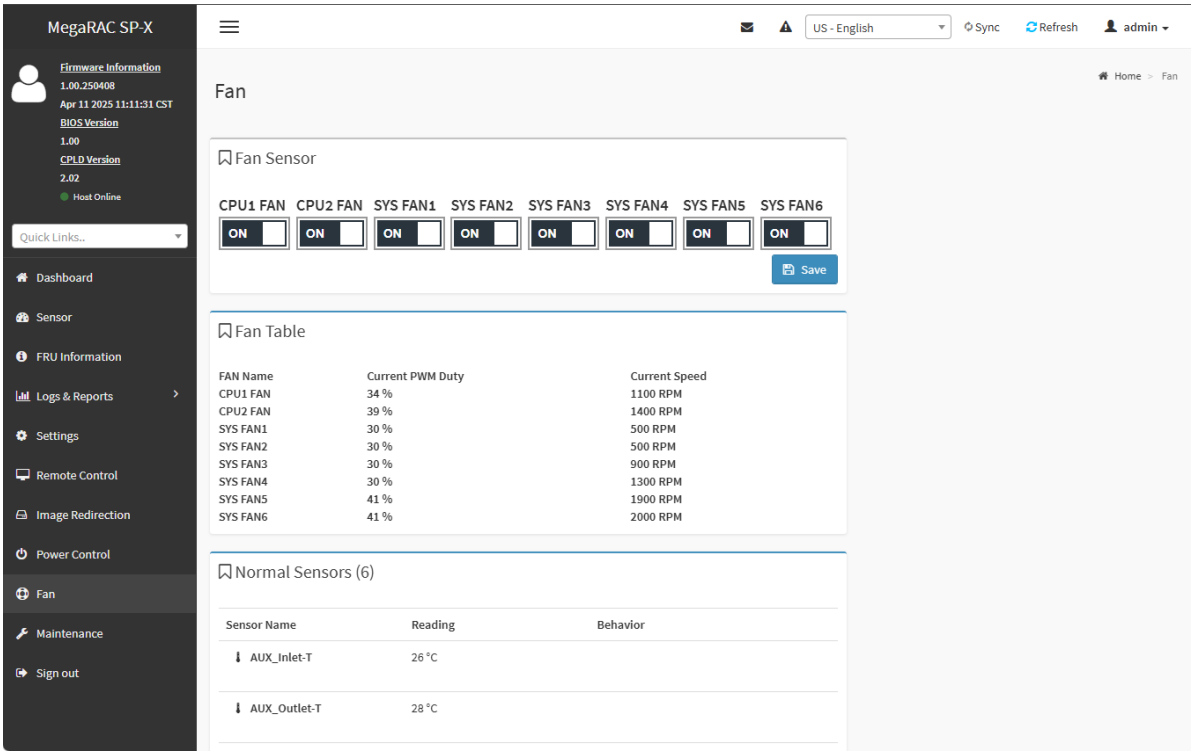


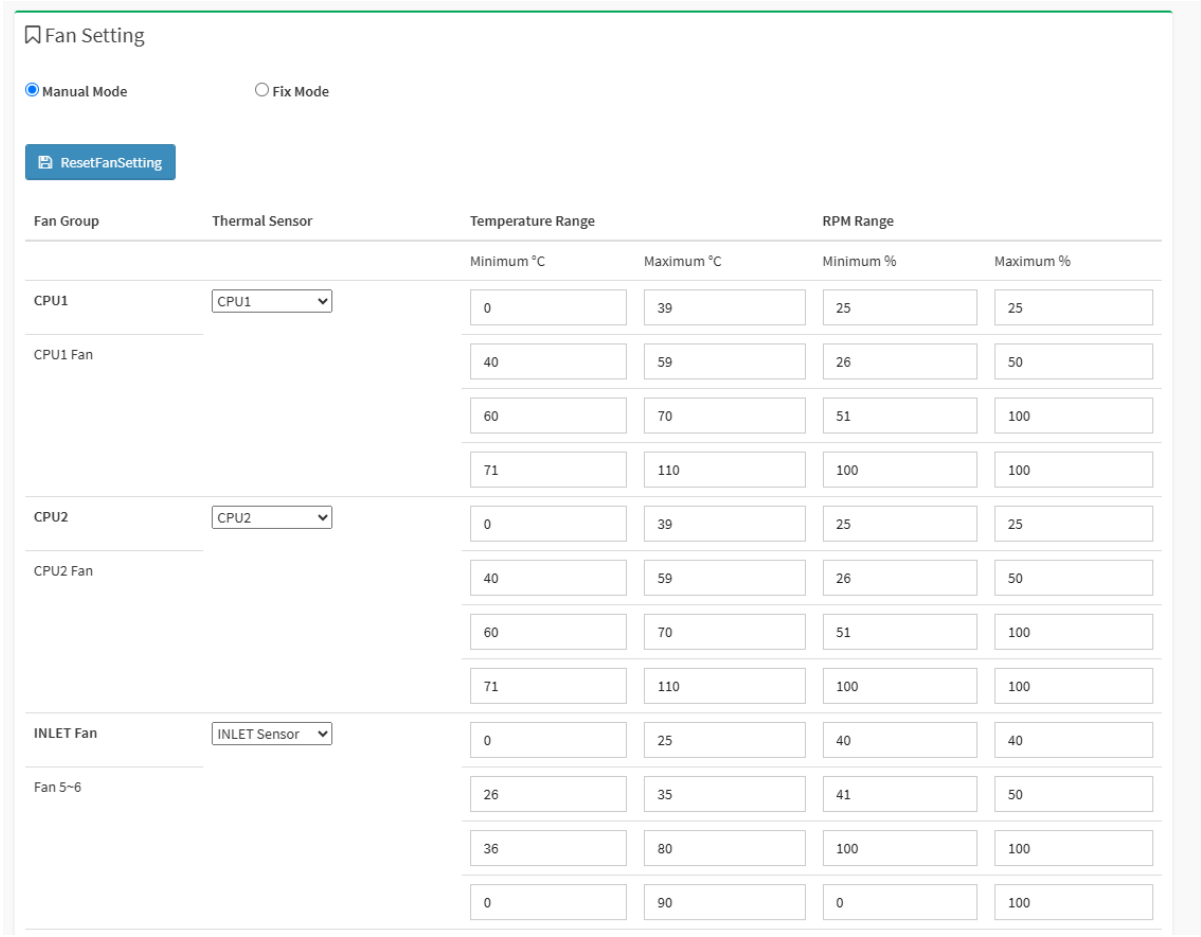
Item	Option	Description

Power Control	Power Off	Select this option to power off the server
	Power On	Select this option to power on the server
	Power Cycle	Select this option to first power off, and then reboot the system (cold boot)
	Hard Reset	Select this option to reboot the system without powering off (warm boot)
	ACPI Shutdown	Select this option to initiate operating system shutdown prior to the shutdown
Perform Action		Click button to perform the selected power action above immediately

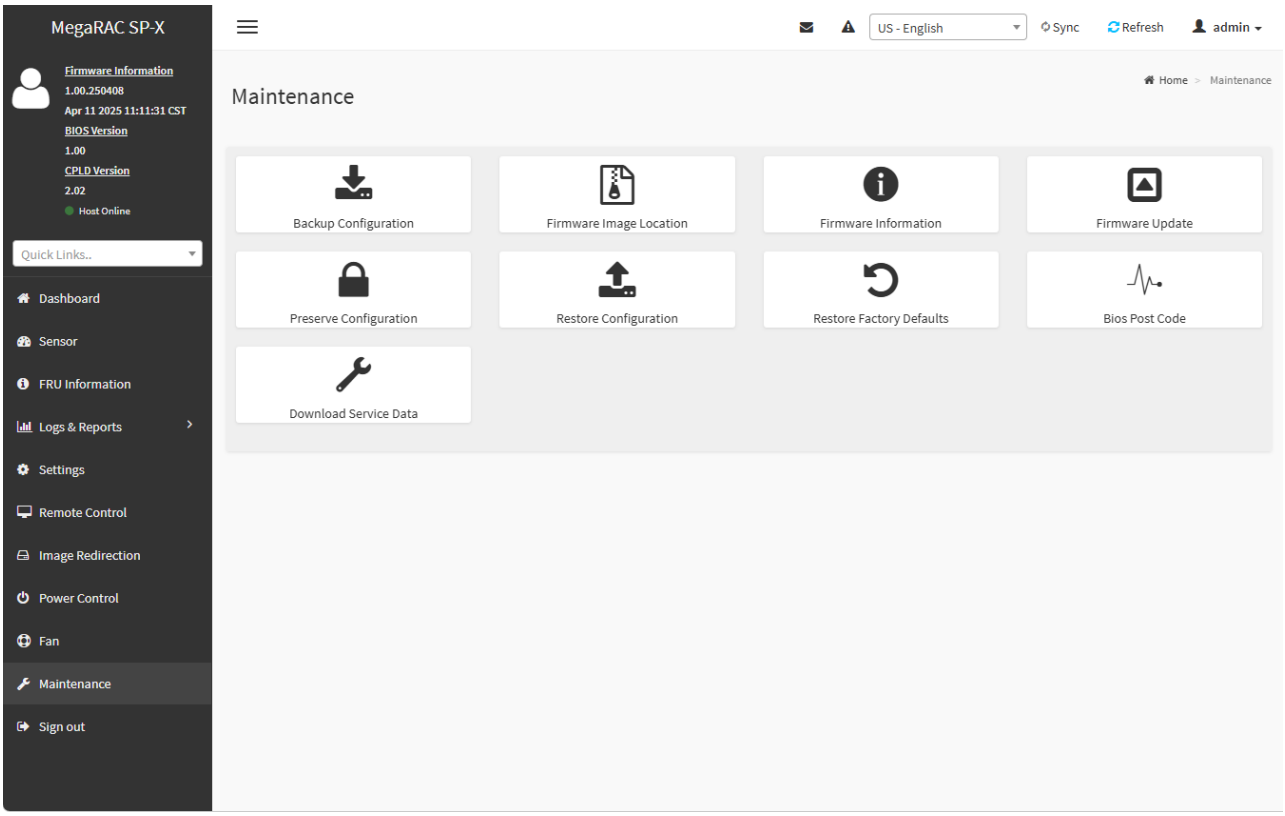
2.10 HOME> FAN

This page can perform FAN Sensor and FAN Mode control.



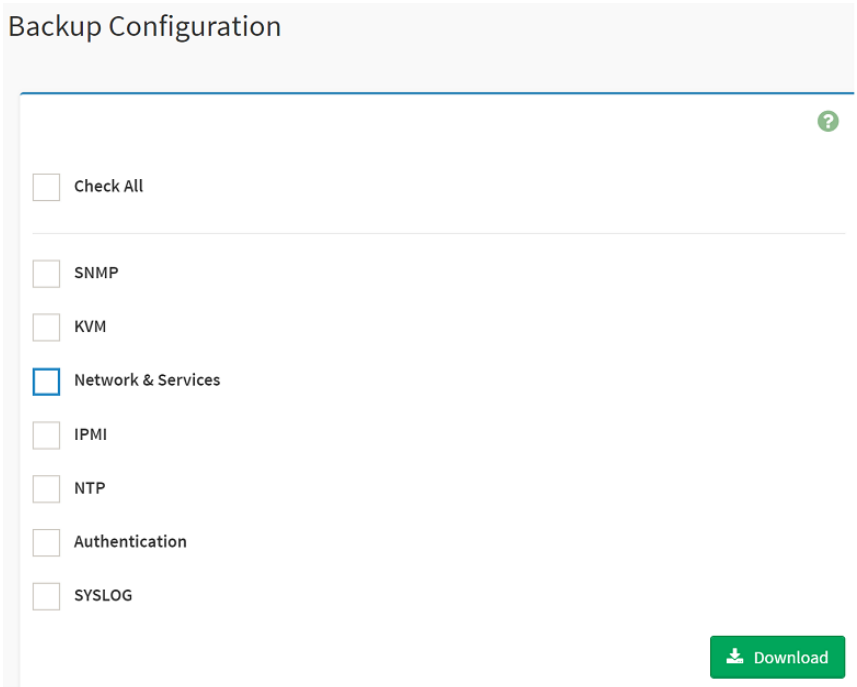


2.11 HOME> MAINTENANCE



2.11.1 Home>Maintenance >Backup Configuration

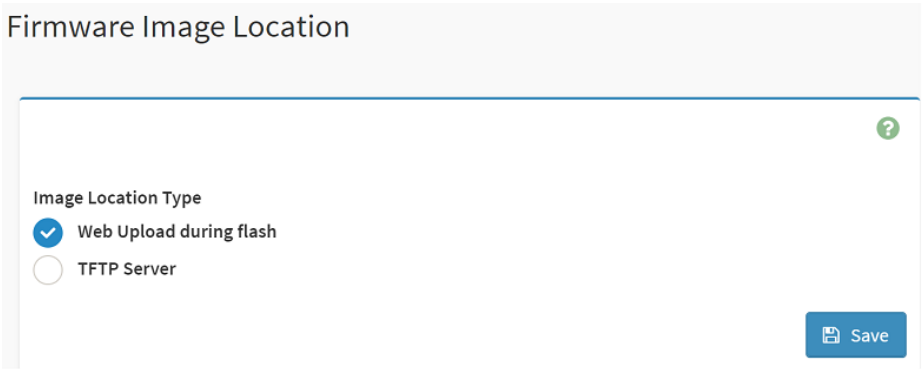
Check the component that needs to be backed up. You will be able to save the backup config file to a location of your choice. That saved file can be used to restore the configuration when needed.



Item	Option	Description
Check All	☑ ☐	Set all following check box as checked
SNMP	☑ ☐	Select this option to backup SNMP configuration
KVM	☑ ☐	Select this option to backup KVM configuration
Network & Services	☑ ☐	Select this option to backup Network & Services configuration
IPMI	☑ ☐	Select this option to backup IPMI configuration
NTP	☑ ☐	Select this option to backup NTP configuration
Authentication	☑ ☐	Select this option to backup Authentication configuration
SYSLOG	☑ ☐	Select this option to backup SYSLOG configuration
Download	Download	Click this button to backup selected config above as a file.

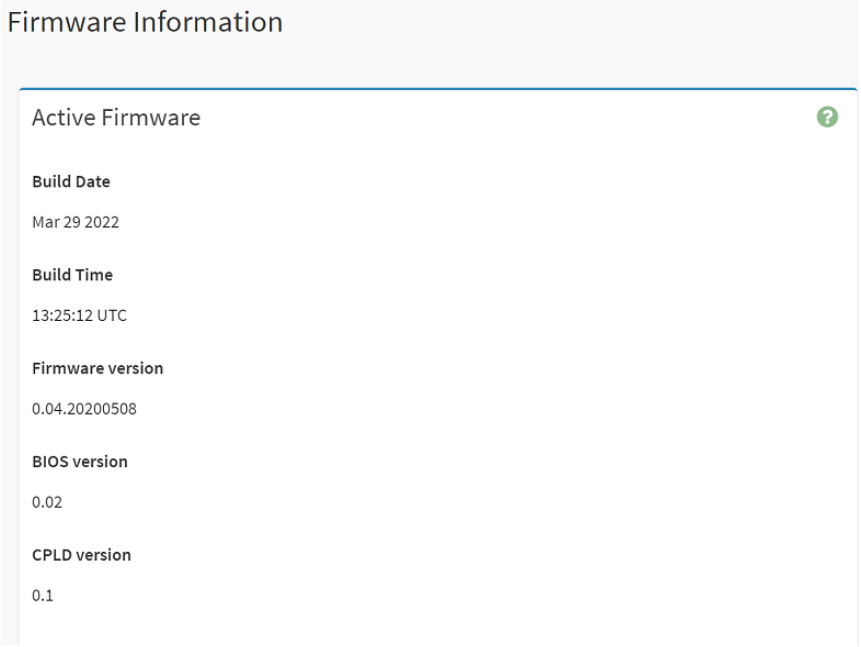
2.11.2 Home>Maintenance >Firmware Image Location

Protocol to be used to transfer the firmware image onto the BMC



Item	Option	Description
Image Location Type	● Web Upload during flash ● TFTP Server	Type of location to transfer the fw image into the BMC either Web Update during flash or TFTP Server
Save	Save	Click button to save the changes made

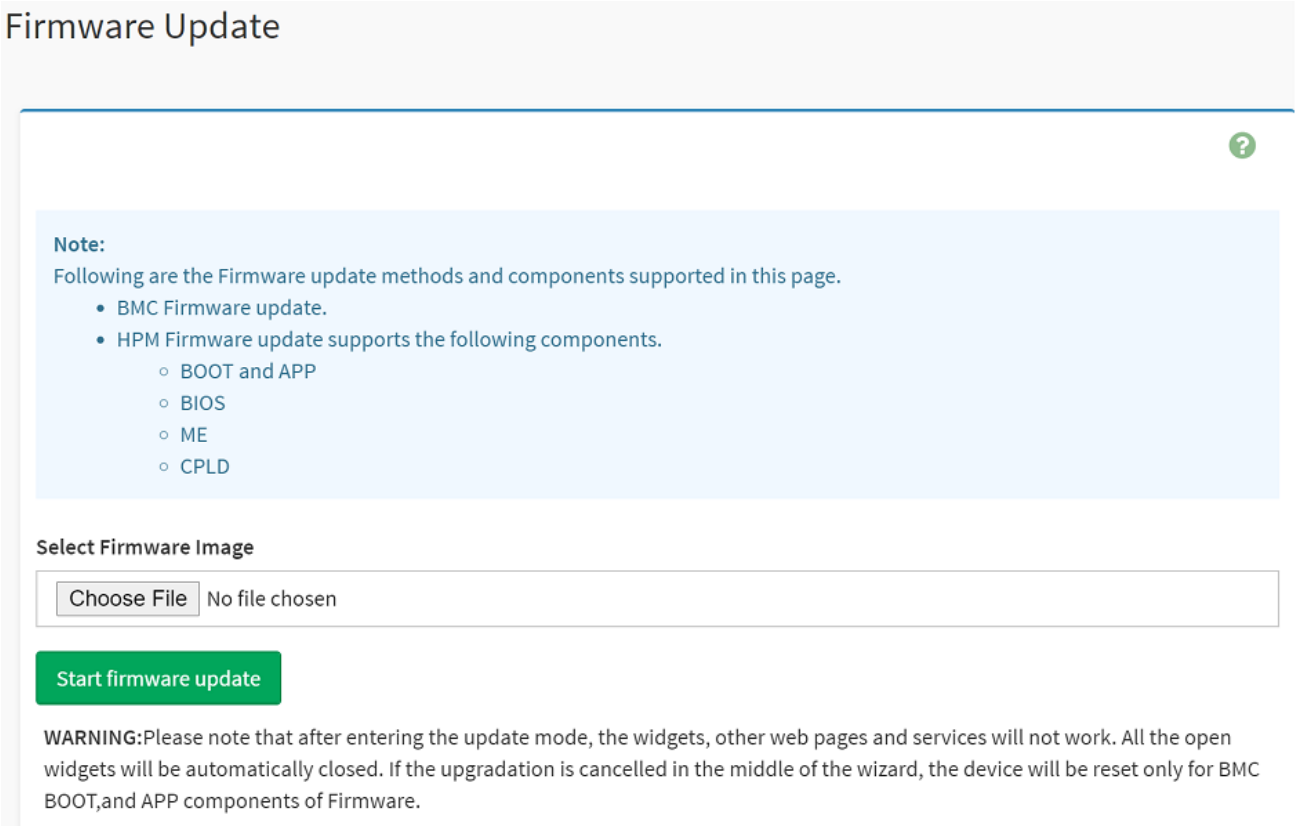
2.11.3 Home>Maintenance >Firmware Information



Item	Description
Build Date	Give the build date of the active BMC image
Build Time	Give the build time of the active BMC image
Firmware version	Displays the firmware version of the active BMC image
BIOS version	Displays the firmware version of the active BIOS image
CPLD version	Displays the firmware version of the active CPLD image

2.11.4 Home>Maintenance >Firmware Update

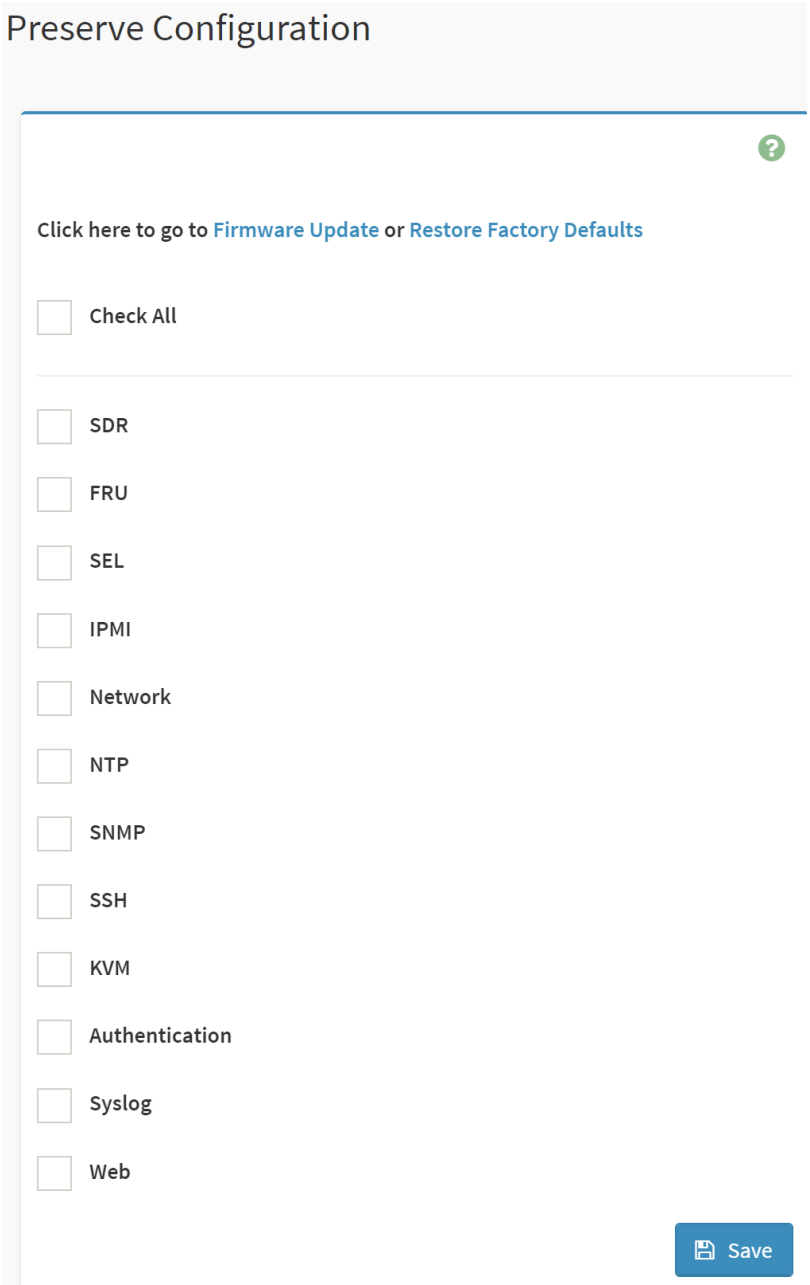
Choose the firmware image to be updated



Item	Option	Description
Choose File	Choose File	Click the button to choose firmware file for update
Start firmware update	Start firmware update	After choose firmware file,click the button to start firmware update.

2.11.5 Home>Maintenance >Preserve Configuration

Check the configuration that needs to be preserved when a Restore Configuration operation is performed

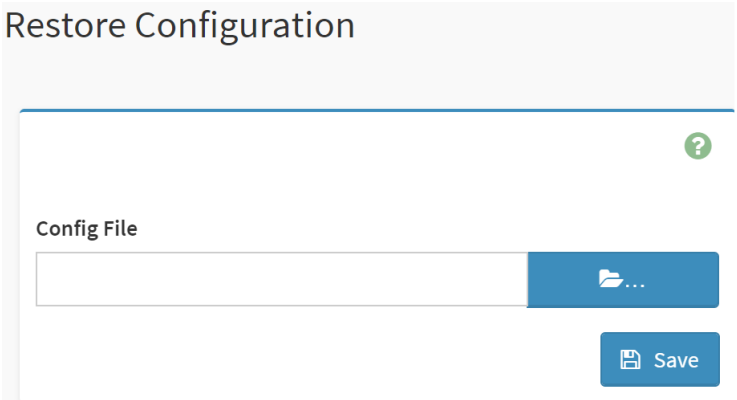


Item	Option	Description
Check All	☑ ☐	Checked this option to set all following check box as checked
SDR	☑ ☐	Checked this option to preserve SDR configuration
FRU	☑ ☐	Checked this option to preserve FRU configuration
SEL	☑	Checked this option to preserve SEL configuration

	☐	
IPMI	☑	Checked this option to preserve IPMI configuration
Network	☑	Checked this option to preserve Network configuration
NTP	☑	Checked this option to preserve NTP configuration
SNMP	☑	Checked this option to preserve SNMP configuration
SSH	☑	Checked this option to preserve SSH configuration
KVM	☑	Checked this option to preserve KVM configuration
Authentication	☑	Checked this option to preserve Authentication configuration
Syslog	☑	Checked this option to preserve Syslog configuration
Web	☑	Checked this option to preserve Web configuration
Save	Save	Click the button to save the changes made

2.11.6 Home>Maintenance >Restore Configuration

Use Browse button to navigate to a previously-saved configuration file then click save button to perform restore configuration

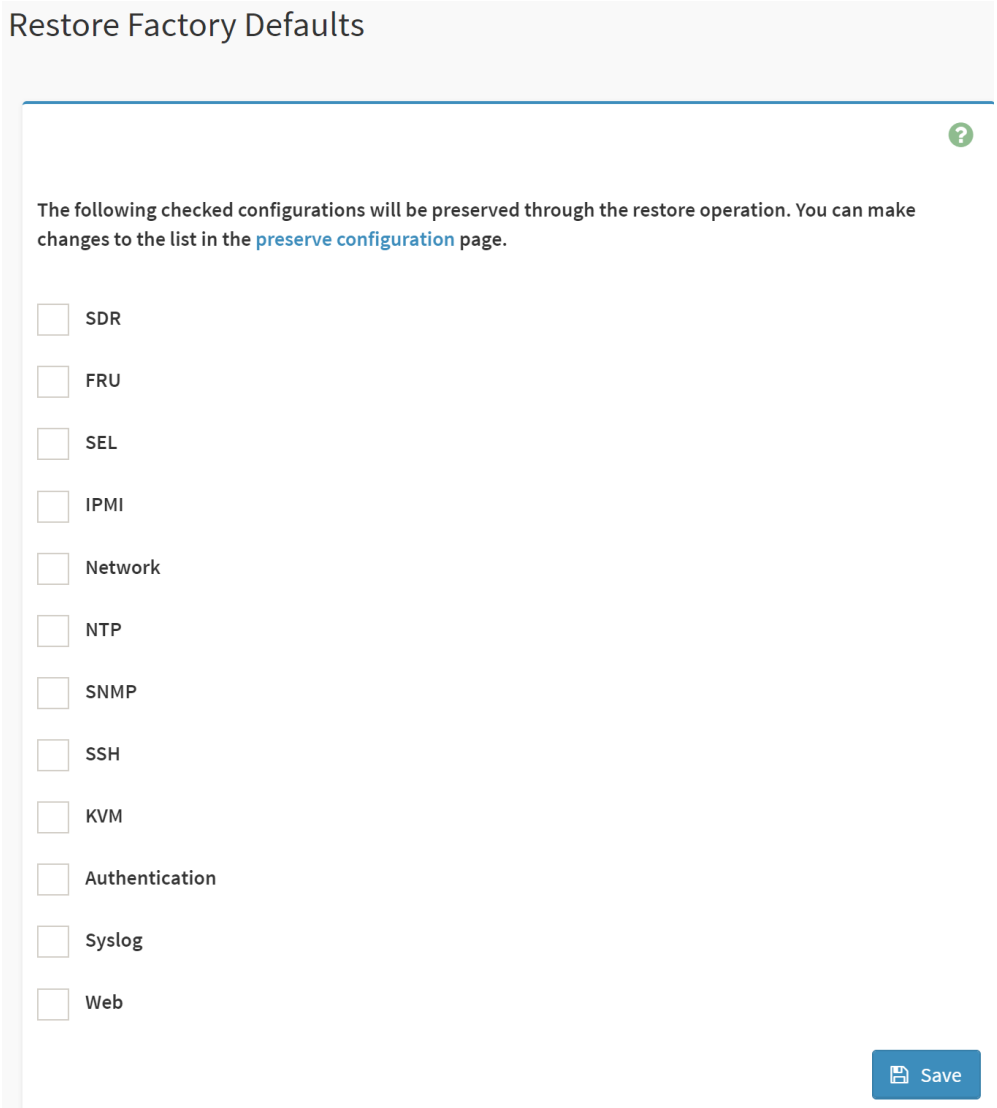


Item	Option	Description
Config File	...	Click the button to select a previously-saved configuration file

Save	Save	After select config file ,click the button to perform restore configuration

2.11.7 Home>Maintenance >Restore Factory Defaults

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

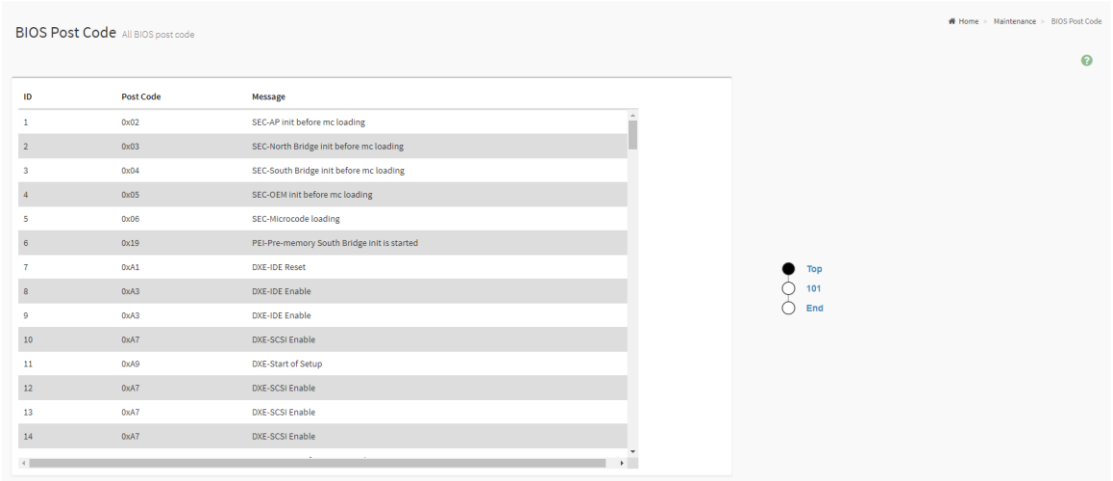


Item	Option	Description
SDR	☑ ☐	Checked this option to preserve SDR configuration while Restore Factory Defaults
FRU	☑ ☐	Checked this option to preserve FRU configuration while Restore Factory Defaults
SEL	☑ ☐	Checked this option to preserve SEL configuration while Restore Factory Defaults

IPMI	☑ ☐	Checked this option to preserve IPMI configuration while Restore Factory Defaults
Network	☑ ☐	Checked this option to preserve Network configuration while Restore Factory Defaults
NTP	☑ ☐	Checked this option to preserve NTP configuration while Restore Factory Defaults
SNMP	☑ ☐	Checked this option to preserve SNMP configuration while Restore Factory Defaults
SSH	☑ ☐	Checked this option to preserve SSH configuration while Restore Factory Defaults
KVM	☑ ☐	Checked this option to preserve KVM configuration while Restore Factory Defaults
Authentication	☑ ☐	Checked this option to preserve Authentication configuration while Restore Factory Defaults
Syslog	☑ ☐	Checked this option to preserve Syslog configuration while Restore Factory Defaults
Web	☑ ☐	Checked this option to preserve Web configuration while Restore Factory Defaults
Save	Save	Click the button to perform Restore Factory Defaults

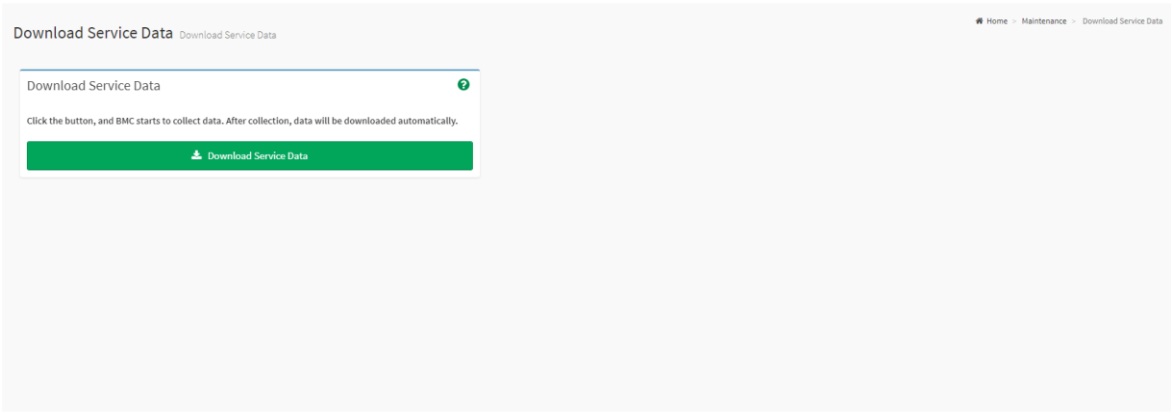
2.11.8 Home>Maintenance > Bios Post code

Collect all post from Bios.

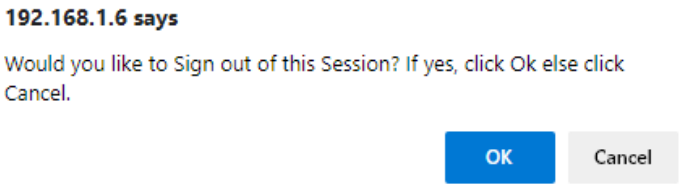


2.11.9 Home>Maintenance > Download Service Data

Clicking the button allows you to obtain the service data for your system. Normally you would only do this at the request of support personnel.



2.12 HOME> SIGN OUT



APPENDIX-A BMC HARDWRE: AST2600

AST2600 is the 7th generation of Integrated Remote Management Processor introduced by ASPEED Tech- nology Inc. Its a vastly integrated SOC device playing as a service processor to support various functions required for highly manageable server platforms. In this generation, the CPU performance is improved signifi- cantly by integrating 1.2GHz dual-core ARM Cortex A7 (r0p5) 32-bit CPU with FPU. Debug access is through ARM CoreSight SOC-400 into CPU. Additionally, most of the controllers are improved with more features or performance. AST2600 also supports more interfaces including PCIe Gen2 1x bus interface and root com- plex which can make BMC to have expended control capacity. New adopted DisplayPort 1.1a also fits next generation display interface. Finally real secure boot function with secure OTP memory can improve the BMC security. Figure-1 clearly illustrates the chip architecture of the BMC. The detailed features of the individual internal blocks will be descried in the following chapters.

The chip architecture is showed below:

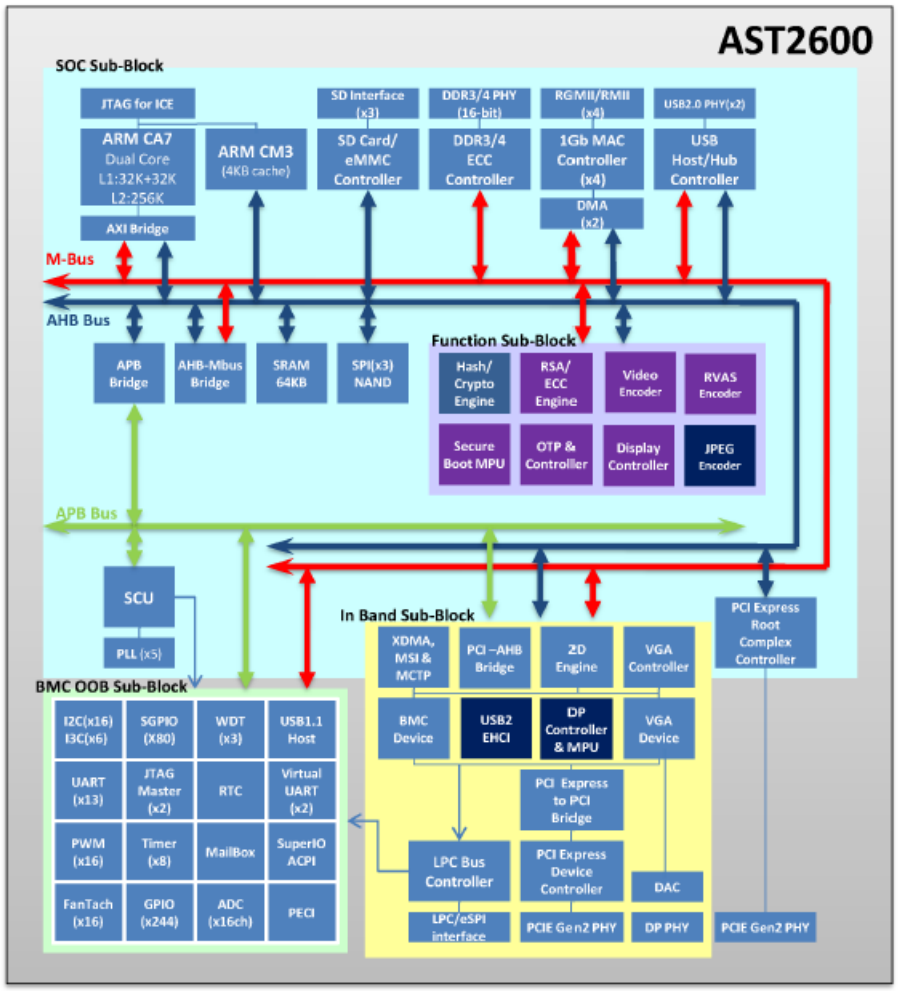


Figure A-1 AST2600 Chip Architecture

The following list is a summary of the BMC management hardware features utilized by the BMC:

- Embedded dual-core ARM Cortex A7 32-bit RISC CPU (r0p5). Max. 1.2GHz
- Embedded one more 32-bit ARM Cortex M3 CPU (r2p1). Max. 200MHz.
- Built-in PCI Express 2.0 Bridge Controller & PCI Express Gen 2 PHY
- Built-in PCI Express 2.0 Root Complex Controller & PCI Express Gen 2 PHY
- VGA Display Controller
- Video Compression Engine
- Four 10/100/1000 Mbps Fast Ethernet MAC
- DDR4 SDRAM Controller. Max. 800MHz
- Support 3 portion of internal SRAM buffer: 64KB or 24KB or 1KB
- System Control Unit
- AHB Controller
- Firmware SPI Memory Controller
- SPI Master Controller
- SD/SDIO/eMMC Host Controller
- USB2.0 Virtual Hub Controller
- USB2.0\1.1 Device Controller & USB2.0\1.1 Host Controller
- 64-bit 2D Graphics Accelerator
- 16 sets of multi-function I2C/SMBus Serial Interface Controller
- 6 sets MIPI I3C Serial Interface Controller
- GPIO Controller. Support up to 244 GPIO pins, which are 31 sets
- Master Serial GPIO Controller. Support 2 maters: 1st 128 In/Out; 2nd 80 In/Out
- Slave serial GPIO monitor. Support 2 sets: max 32 drives for each channel
- Fan Tachometer Controller. Up to 16 tachometer inputs
- PWM Controller. Up to 16 PWM outputs
- Hardware Secure Boot
- UART (16550) Controllers. Up to 3686.4K baud-rate except UART5 921.6K baud-rate
- Built-in 8 sets of 32-bit Timer modules
- Built-in 8 sets of 32-bit Watchdog Timer modules
- 64 bytes Battery Backed SRAM
- LPC Bus Interfaces
- eSPI interface
- System SPI Flash Controller
- Super I/O controller
- Hash & Crypto Engine
- RTC Time Clock

ADC Controller. 16 sets of 10 bits analog-to-digital converter
Intel PECI 4.1 Compliant
JTAG Master Controller
MCTP Controller
MSI Controller
X-DMA Controller

The more information can refer to the Datasheet of AST2600.

APPENDIX-B IPMI COMMANDS SUPPORT TABLE

All option commands and all option parameters of mandatory commands in the command list below are not insured for supporting. Some mandatory commands may be not supported according to FW PRD.

Command	NetFn	CMD	M/O	Supported	Comments
IPMI Device "Global" Commands					
Get Device ID	App	01h	M	V	
Broadcast 'Get Device ID'[1]	App	01h	M		
Cold Reset	App	02h	O	V	
Warm Reset	App	03h	O	V	
Get Self Test Results	App	04h	M	V	
Manufacturing Test On	App	05h	O	V	need password
Set ACPI Power State	App	06h	O	V	
Get ACPI Power State	App	07h	O	V	
Get Device GUID	App	08h	O	V	
Get NetFn Support	App	09h	O	V	
Get Command Support	App	0Ah	O	V	
Get Command Sub-function Support	App	0Bh	O	V	
Get Configurable Commands	App	0Ch	O	V	
Get Configurable Command Sub-functions	App	0Dh	O	V	
Set Command Enables	App	60h	O		
Get Command Enables	App	61h	O	V	
Set Command Sub-function Enables	App	62h	O		
Get Command Sub-function Enables	App	63h	O		
Get OEM NetFn IANA Support	App	64h	O	V	
BMC Watchdog Timer Commands					
Reset Watchdog Timer	App	22h	M	V	
Set Watchdog Timer	App	24h	M	V	
Get Watchdog Timer	App	25h	M	V	
BMC Device and Messaging Commands					
Set BMC Global Enables	App	2Eh	M	V	"Only Supported: SEL Logging Enable / Disable, Event message buffer Enable/disable"
Get BMC Global Enables	App	2Fh	M	V	
Clear Message Flags	App	30h	M	V	
Get Message Flags	App	31h	M	V	
Enable Message Channel Receive	App	32h	O	V	
Get Message	App	33h	M	V	
Send Message	App	34h	M	V	not support Send Raw
Read Event Message Buffer	App	35h	O	V	
Get BT Interface Capabilities	App	36h	O	V	
Get System GUID	App	37h	O	V	

Get Channel Authentication Capabilities	App	38h	O	V	
Get Session Challenge	App	39h	O	V	
Activate Session	App	3Ah	O	V	
Set Session Privilege Level	App	3Bh	O	V	
Close Session	App	3Ch	O	V	
Get Session Info	App	3Dh	O	V	
Get AuthCode	App	3Fh	O	V	
Set Channel Access	App	40h	M	V	"Only support: disabled, always availible, shared mode"
Get Channel Access	App	41h	M	V	
Get Channel Info Command	App	42h	O	V	
Set User Access Command	App	43h	O	V	Not support user session limit
Get User Access Command	App	44h	O	V	
Set User Name	App	45h	O	V	
Get User Name Command	App	46h	O	V	
Set User Password Command	App	47h	O	V	
Activate Payload	App	48h	O	V	
Deactivate Payload	App	49h	O	V	
Get Payload Activation Status	App	4Ah	O	V	
Get Payload Instance Info	App	4Bh	O	V	
Set User Payload Access	App	4Ch	O	V	
Get User Payload Access	App	4Dh	O	V	
Get Channel Payload Support	App	4Eh	O	V	
Get Channel Payload Version	App	4Fh	O	V	
Get Channel OEM Payload Info	App	50h	O	V	
Master Write-Read	App	52h	M	V	
Get Channel Cipher Suites	App	54h	O	V	
Suspend/Resume Payload Encryption	App	55h	O	V	
Set Channel Security Keys	App	56h	O	V	
Get System Interface Capabilities	App	57h	O	V	Only 01h(KCS) is supported
Set System Info Parameters	App	58h	O	V	
Get System Info Parameters	App	59h	O	V	
Chassis Device Commands					
Get Chassis Capabilities	Chassis	00h	M	V	
Get Chassis Status	Chassis	01h	M	V	
ChassisControl	Chassis	02h	M	V	
Chassis Reset	Chassis	03h	O		This command is combined to Chassis Control command in IPMI v1.5
Chassis Identify	Chassis	04h	O	V	
Set Chassis Capabilities	Chassis	05h	O	V	
Set Power Restore Policy	Chassis	06h	O		
Get System Restart Cause	Chassis	07h	O	V	Only 01h (cycle,hardware reset), 04h,8h,9h supported
Set System Boot Options	Chassis	08h	O	V	
Get System Boot Options	Chassis	09h	O	V	
Set Front Panel Button Enables	Chassis	0Ah	O		
Set Power Cycle Interval	Chassis	0Bh	O	V	
Get POH Counter	Chassis	0Fh	O	V	
Event Commands					
Set Event Receiver	S/E	00h	M	V	
Get Event Receiver	S/E	01h	M	V	
Platform Event (a.k.a. "Event Message")	S/E	02h	M	V	
PEF and Alerting Commands					
Get PEF Capabilities	S/E	10h	M	V	

Arm PEF Postpone Timer	S/E	11h	M	V	
Set PEF Configuration Parameters	S/E	12h	M	V	Does not support parameter 15.
Get PEF Configuration Parameters	S/E	13h	M	V	Does not support parameter 15.
Set Last Processed Event ID	S/E	14h	M	V	
Get Last Processed Event ID	S/E	15h	M	V	
Alert Immediate	S/E	16h	O	V	
PET Acknowledge	S/E	17h	O	V	
Sensor Device Commands					
Get Device SDR Info	S/E	20h	O	V	
Get Device SDR	S/E	21h	O	V	
Reserve Device SDR Repository	S/E	22h	O	V	
Get Sensor Reading Factors	S/E	23h	O	V	Support linear sensors only.
Set Sensor Hysteresis	S/E	24h	O	V	
Get Sensor Hysteresis	S/E	25h	O	V	
Set Sensor Threshold	S/E	26h	O	V	
Get Sensor Threshold	S/E	27h	O	V	
Set Sensor Event Enable	S/E	28h	O	V	
Get Sensor Event Enable	S/E	29h	O	V	
Re-arm Sensor Events	S/E	2Ah	O	V	
Get Sensor Event Status	S/E	2Bh	O	V	
Get Sensor Reading	S/E	2Dh	M	V	
Set Sensor Type	S/E	2Eh	O	V	
Get Sensor Type	S/E	2Fh	O	V	
Set Sensor Reading and Event Status	S/E	30h	O	V	Sensor should be settable (just for FW engineer debug purpose internally)
FRU Device Commands					
Get FRU Inventory Area Info	Storage	10h	M	V	
Read FRU Data	Storage	11h	M	V	
Write FRU Data	Storage	12h	M	V	
SDR Device Commands					
Get SDR Repository Info	Storage	20h	M	V	
Get SDR Repository Allocation	Storage	21h	O	V	
Reserve SDR Repository	Storage	22h	M	V	
Get SDR	Storage	23h	M	V	
Add SDR	Storage	24h	O	V	
Partial Add SDR	Storage	25h	M	V	
Delete SDR	Storage	26h	O		
Clear SDR Repository	Storage	27h	M	V	
Get SDR Repository Time	Storage	28h	O	V	
Set SDR Repository Time	Storage	29h	O		
Enter SDR Repository Update	Storage	2Ah	O		
Exit SDR Repository Update	Storage	2Bh	O		
Run Initialization Agent	Storage	2Ch	O	V	
SEL Device Commands					
Get SEL Info	Storage	40h	M	V	
Get SEL Allocation Info	Storage	41h	O	V	
Reserve SEL	Storage	42h	O	V	
Get SEL Entry	Storage	43h	M	V	
Add SEL Entry	Storage	44h	M	V	
Partial Add SEL Entry	Storage	45h	O	V	
Delete SEL Entry	Storage	46h	O	V	
Clear SEL	Storage	47h	M	V	
Get SEL Time	Storage	48h	M	V	
Set SEL Time	Storage	49h	M	V	
Get Auxiliary Log Status	Storage	5Ah	O		
Set Auxiliary Log Status	Storage	5Bh	O		

Get SEL Time UTC Offset	Storage	5Ch	O	V	
Set SEL Time UTC Offset	Storage	5Dh	O	V	
LAN Device Commands					
Set LAN Configuration Parameter	Transport	01h	M	V	param #9, 25 are not support
Get LAN Configuration Parameters	Transport	02h	M	V	param #9, 25 are not support
Suspend BMC ARPs	Transport	03h	O	V	
Get IP/UDP/RMCP Statistics	Transport	04h	O		
Serial/Modem Device Commands					
Set Serial/Modem Configuration	Transport	10h	M	V	
Get Serial/Modem Configuration	Transport	11h	M	V	
Set Serial/Modem Mux	Transport	12h	O	V	
Get TAP Response Codes	Transport	13h	O		
Set PPP UDP Proxy Transmit	Transport	14h	O		
Get PPP UDP Proxy Transmit	Transport	15h	O		
Send PPP UDP Proxy Packet	Transport	16h	O		
Get PPP UDP Proxy Receive	Transport	17h	O		
Callback	Transport	19h	O		
Set User Callback Options	Transport	1Ah	O		
Get User Callback Options	Transport	1Bh	O		
Set Serial Routing Mux Command	Transport	1Ch	O		
SOL Activating	Transport	20h	O		
Set SOL Configuration Parameters	Transport	21h	O	V	param #7 is not support
Get SOL Configuration Parameters	Transport	22h	O	V	param #7 is not support
Command Forwarding Commands					
Forwarded Command	Transport	30h	O		
Set Forwarded Commands	Transport	31h	O		
Get Forwarded Commands	Transport	32h	O		
Enable Forwarded Commands	Transport	33h	O		
Bridge Management Commands					
Get Bridge State	Bridge	00h	O		
Set Bridge State	Bridge	01h	O		
Get ICMB Address	Bridge	02h	O		
Set ICMB Address	Bridge	03h	O		
Set Bridge ProxyAddress	Bridge	04h	O		
Get Bridge Statistics	Bridge	05h	O		

Get ICMB Capabilities	Bridge	06h	O		
Clear Bridge Statistics	Bridge	08h	O		
Get Bridge Proxy Address	Bridge	09h	O		
Get ICMB Connector Info	Bridge	0Ah	O		
Get ICMB Connection ID	Bridge	0Bh	O		
Send ICMB Connection ID	Bridge	0Ch	O		
Discovery Commands (ICMB)					
PrepareForDiscovery	Bridge	10h	O		
GetAddresses	Bridge	11h	O		
SetDiscovered	Bridge	12h	O		
GetChassisDeviceId	Bridge	13h	O		
SetChassisDeviceId	Bridge	14h	O		
Bridging Commands (ICMB)					
BridgeRequest	Bridge	20h	O		
BridgeMessage	Bridge	21h	O		
Event Commands (ICMB)					
GetEventCount	Bridge	30h	O		
SetEventDestination	Bridge	31h	O		
SetEventReceptionState	Bridge	32h	O		
SendICMBEventMessage	Bridge	33h	O		
GetEventDestination (optional)	Bridge	34h	O		
GetEventReceptionState (optional)	Bridge	35h	O		
Other Bridge Commands					
Error Report (optional)	Bridge	FFh	O		
OEM Commands for Bridge NetFn					
OEM Commands	Bridge	C0h -FE h	O		

APPENDIX-C IPMI OEM COMMANDS LIST

Command	NetFn	CMD	DATA Length	DATA Value	Comments
Set Fan Mode	0x30	01h	1	0~1	**Input data:** 0=standard speed , 1=manual speed
Get Fan Mode	0x30	30h	0		**Response data:** 0=standard speed , 1=manual speed
Set FRU Lock	0x30	31h	1	0~1	**Input data:** 0=disable FRU eeprom write protect 1=enable FRU eeprom write protect
Set Fan Speed	0x30	35h	2	Byte1 : 0~06h Byte2 : 0~64h	**Input data:** Byte 1 = fan number Byte2 = PWM duty cycle
Get Fan Speed	0x30	36h	0		**Response data:** Byte1 = CPU1_FAN pwm duty cycle Byte2 = SYS_FAN1pwm duty cycle Byte3 = SYS_FAN2 pwm duty cycle Byte4 = SYS_FAN3 pwm duty cycle Byte5 = SYS_FAN4 pwm duty cycle Byte6 = SYS_FAN5 pwm duty cycle Byte7 = SYS_FAN6 pwm duty cycle Byte8 = CPU2_FAN pwm duty cycle
Get BIOS Version	0x30	38h	0		**Response data** Byte1 = Low version Byte2 = High version
Get CPLD Version	0x30	39h	0		**Response data** Byte1 = Low version Byte2 = High version

APPENDIX-D SENSOR TABLE

IPMI provides a sixteen byte string identifier (Sensor ID) in each SDR. This ASCII based string will need to be interpreted by system management software (SMS) for display and alerting purposes. Sensors provided by BMC are listed in the following Table E-1:

AUX_Inlet-T	27 degrees C	ok
AUX_Outlet-T	28 degrees C	ok
Board_Inlet-T	40 degrees C	ok
Board_Outlet-T	47 degrees C	ok
HDD_AREA-T	26 degrees C	ok
CPU1-T	48 degrees C	ok
CPU2-T	52 degrees C	ok
DIMM1-T	42 degrees C	ok
DIMM2-T	44 degrees C	ok
DIMM3-T	43 degrees C	ok
DIMM4-T	41 degrees C	ok
DIMM5-T	47 degrees C	ok
DIMM6-T	48 degrees C	ok
DIMM7-T	49 degrees C	ok
DIMM8-T	47 degrees C	ok
DIMM9-T	51 degrees C	ok
DIMM10-T	52 degrees C	ok
DIMM11-T	52 degrees C	ok

DIMM12-T	49 degrees C	ok
DIMM13-T	47 degrees C	ok
DIMM14-T	49 degrees C	ok
DIMM15-T	48 degrees C	ok
DIMM16-T	44 degrees C	ok
PCIe1_GPU-T	0 degrees C	ok
PCIe2_GPU-T	0 degrees C	ok
PCIe3_GPU-T	0 degrees C	ok
PCIe4_GPU-T	0 degrees C	ok
PCIe5_GPU-T	0 degrees C	ok
PCIe6_GPU-T	0 degrees C	ok
VIN_CPU1-T	56 degrees C	ok
VFA_FIVRA_CPU1-T	50 degrees C	ok
VINF_CPU1-T	51 degrees C	ok
VFA_EHV_CPU1-T	50 degrees C	ok
VNN_MAIN_CPU1-T	44 degrees C	ok
VD0_HV_CPU1-T	53 degrees C	ok
VD1_HV_CPU1-T	54 degrees C	ok
VIN_CPU2-T	61 degrees C	ok
VFA_FIVRA_CPU2-T	56 degrees C	ok
VINF_CPU2-T	55 degrees C	ok
VFA_EHV_CPU2-T	52 degrees C	ok
VNN_MAIN_CPU2-T	51 degrees C	ok
VD0_HV_CPU2-T	55 degrees C	ok

VD1_HV_CPU2-	55 degrees C	ok
P12V	5 Volts	ok
P5V_AUX	5 Volts	ok
P3V3	3.30 Volts	ok
P5V	5 Volts	ok
P3V_AUX	3.25 Volts	ok
P2V5_AUX	2.50 Volts	ok
P1V8_AUX	1.79 Volts	ok
P3V_BAT	3.20 Volts	ok
P1V2_AUX	1.19 Volts	ok
P1V_AUX	1 Volts	ok
P1V25	1.25 Volts	ok
VIN_CPU1	1.82 Volts	ok
VFA_FIVRA_CPU1	1.80 Volts	ok
VINF_CPU1	0.71 Volts	ok
VFA_EHV_CPU1	1.79 Volts	ok
VNN_MAIN_CPU1	0.99 Volts	ok
VD0_HV_CPU1	1.11 Volts	ok
VD1_HV_CPU1	1.11 Volts	ok
VIN_CPU2	1.81 Volts	ok
VFA_FIVRA_CPU2	1.80 Volts	ok
VINF_CPU2	0.71 Volts	ok
VFA_EHV_CPU2	1.80 Volts	ok
VNN_MAIN_CPU2	0.99 Volts	ok

VD0_HV_CPU2	1.11 Volts	ok
VD1_HV_CPU2	1.11 Volts	ok
CPU1_FAN_Speed	1100 RPM	ok
CPU2_FAN_Speed	1600 RPM	ok
SYS_FAN1_Speed	500 RPM	ok
SYS_FAN2_Speed	500 RPM	ok
SYS_FAN3_Speed	900 RPM	ok
SYS_FAN4_Speed	1300 RPM	ok
SYS_FAN5_Speed	2000 RPM	ok
SYS_FAN6_Speed	2100 RPM	ok
PSU_AC_PIN	no reading	ns
PSU_AC_VIN	no reading	ns
PSU_AC_CIN	no reading	ns
PSU_DC_POUT	no reading	ns
PSU_DC_VOUT	no reading	ns
PSU_DC_COUT	no reading	ns
PSU-T1	no reading	ns
PSU-T2	no reading	ns
PUS_FAN1	no reading	ns
VR Watchdog	0x00	ok
IPMI Watchdog	0x00	ok
ChassisIntrusion	0x00	ok
Reset_Button	0x00	ok
Power_Button	0x00	ok

System Event Log	0x00	ok
BMC Watchdog	0x00	ok
ACPI_State	0x00	ok
System Event	0x00	ok
BMC_Boot_Up	0x00	ok
HstCpuUTZ	no reading	ns
HstMBwUTZ	no reading	ns
HstPCIBwUTZ	no reading	ns
CupsIndex	no reading	ns
AvgHstCpuUTZ	no reading	ns
AvgHstMBwUTZ	no reading	ns
AvgHstPciBwUTZ	no reading	ns
AverageCupsIndex	no reading	ns

APPENDIX-E DEFAULT CONFIGURATION

A host based utility will be available to configure the BMC. This utility can be used to set parameters such as IP address and other LAN parameters, and/or SEL and SDR time. The utilities include BIOS and IPMI utility. The host based utility has high priority to send command to BMC.

Table F-1 Default Configuration

Parameter Name	Default Value
User IDs	**(User/Password/Privilege/Channels)**
USER ID 1:	NULL/NULL/User/LAN
USER ID 2:	root/root/Administrator/LAN
LAN Channel	
IP Address Source	DHCP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
PEF Alerting	Disable
Per-message Authentication	Disable
User Level Authentication	Disable
Access Mode	Always Available
Privilege Level Limit	Administrator
SOL	
SOL Enable	Enable SOL payload
Payload Authentication/Authentication	Force encryption/ Authentication controlled by remote software
SOL Privilege Level Limit	Administrator
SOL non-volatile bit rate	115200 bps
SOL volatile bit rate	115200 bps
Power Restore Policy	chassis always powers up after AC on

APPENDIX-F FIRMWARE UPDATE

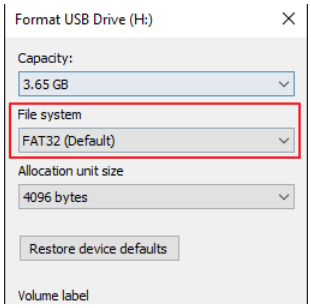
If necessary, the system firmware can be updated at local machine or remote console. Please refer the following instructions.

1. BIOS + SPS

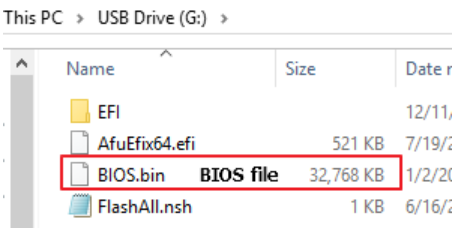
Update Method	OS	Tool and Jumper settings
Local Update	UEFI environment	AfuEfix64.efi **Need to disable SPS by JPFLASHSEC1 jumper.**
Remote Update	IPMI Web UI	No tool required **No need to disable SPS.**

1.1 BIOS + SPS update in UEFI environment

1. Format a USB flash drive to FAT32.

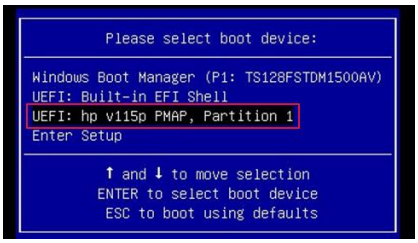


2. Download the update tool and BIOS file(xxx.bin), then save at the **root** directdory of the USB drive.



3. Plug the USB drive to the Server and close pin 2-3 of JPFLASHSEC1.

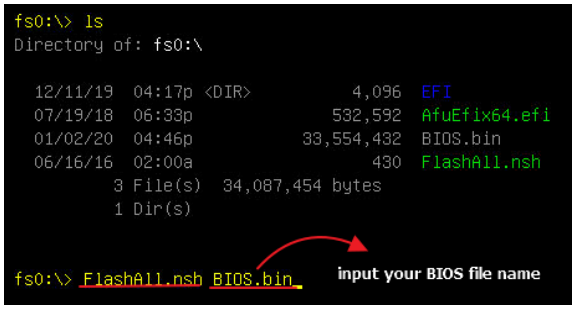
4. Power on system. When you hear BIOS ready beep, perss **F11** to enter boot menu and select the USB drive to boot.



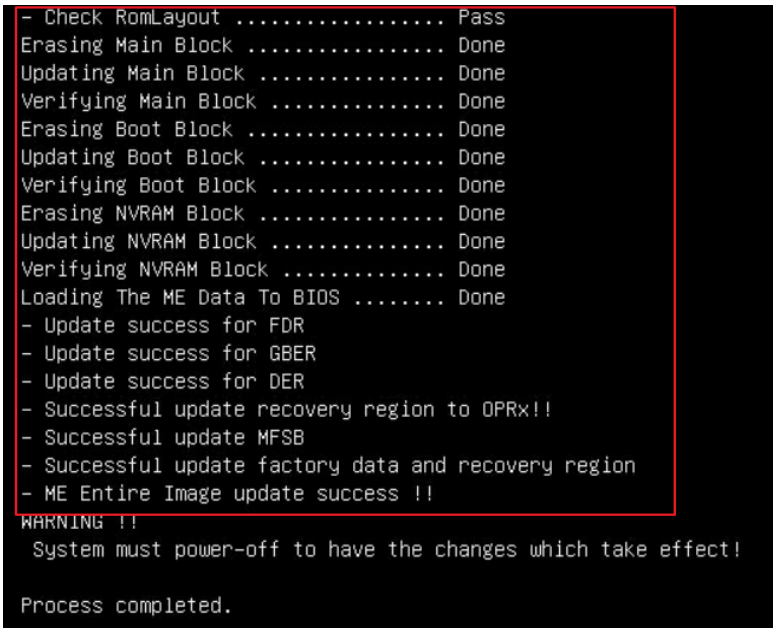
5. Type **fs*:** to enter the USB drive, for example **fs0:**.



6. Type **FlashAll.nsh [BIOS file name]** to update BIOS.



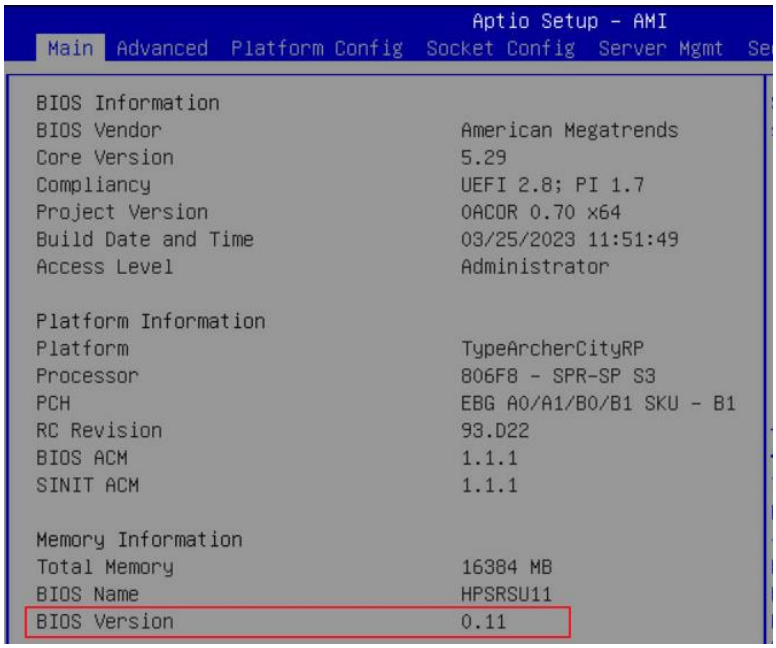
7. When the process ends, make sure all regions are done successfully without any error.



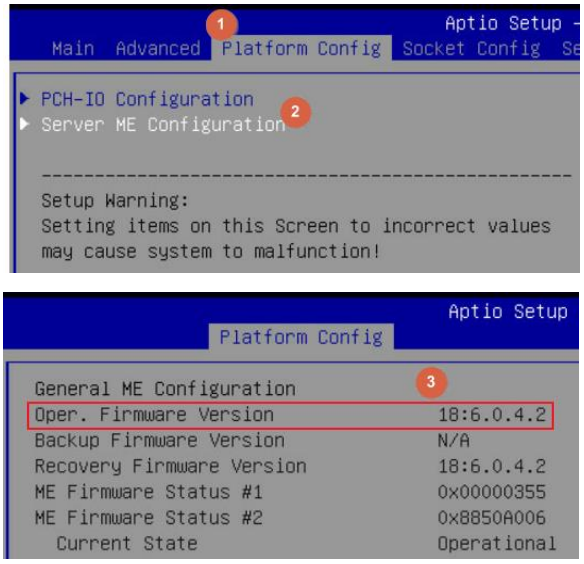
8. Remove AC power and move **JPFLASHSEC1** jumper back to pin 1-2.

9. Power on, then boot to BIOS to check if BIOS version and SPS version are correct.

BIOS version:



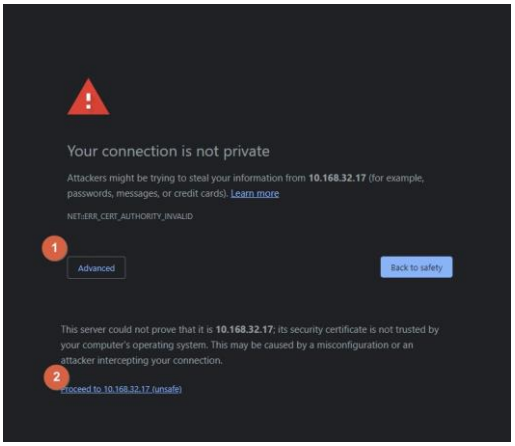
SPS version:



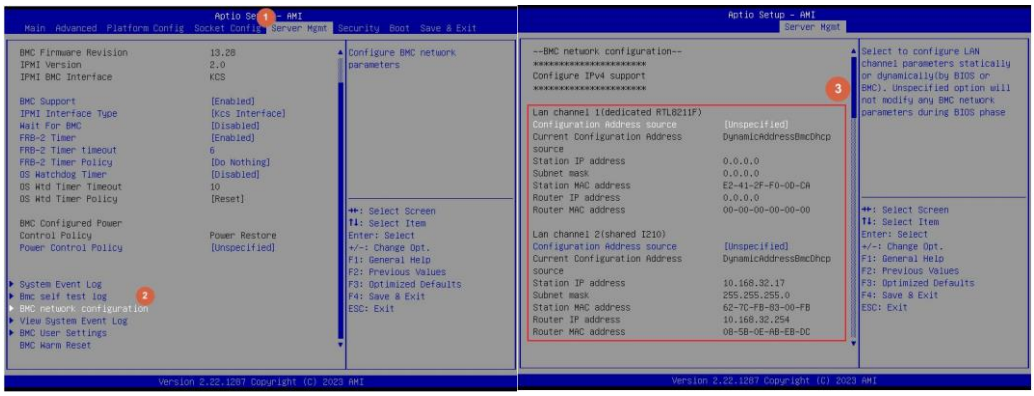
1.2 BIOS + SPS update using IPMI Web UI

1. Open web browser. Enter BMC IP address and log in. The default username and password are admin/admin.

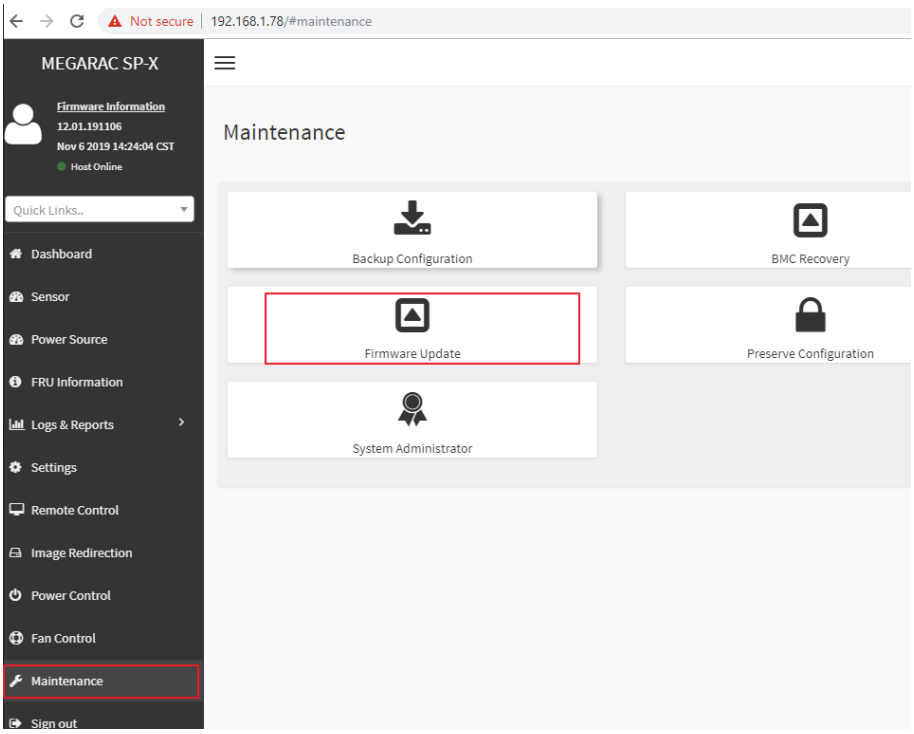
If you get a message that says "**Your connection is not private"**, just skip it.



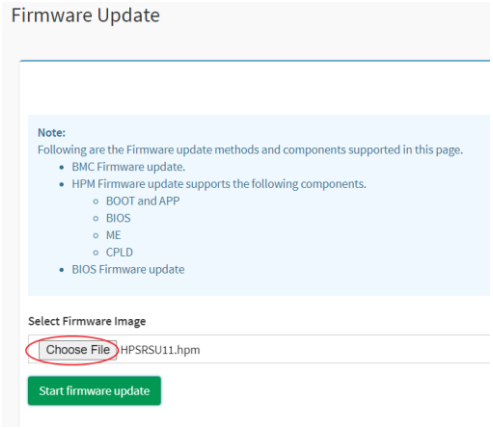
Note: BMC IP address can be configured at BIOS menu.



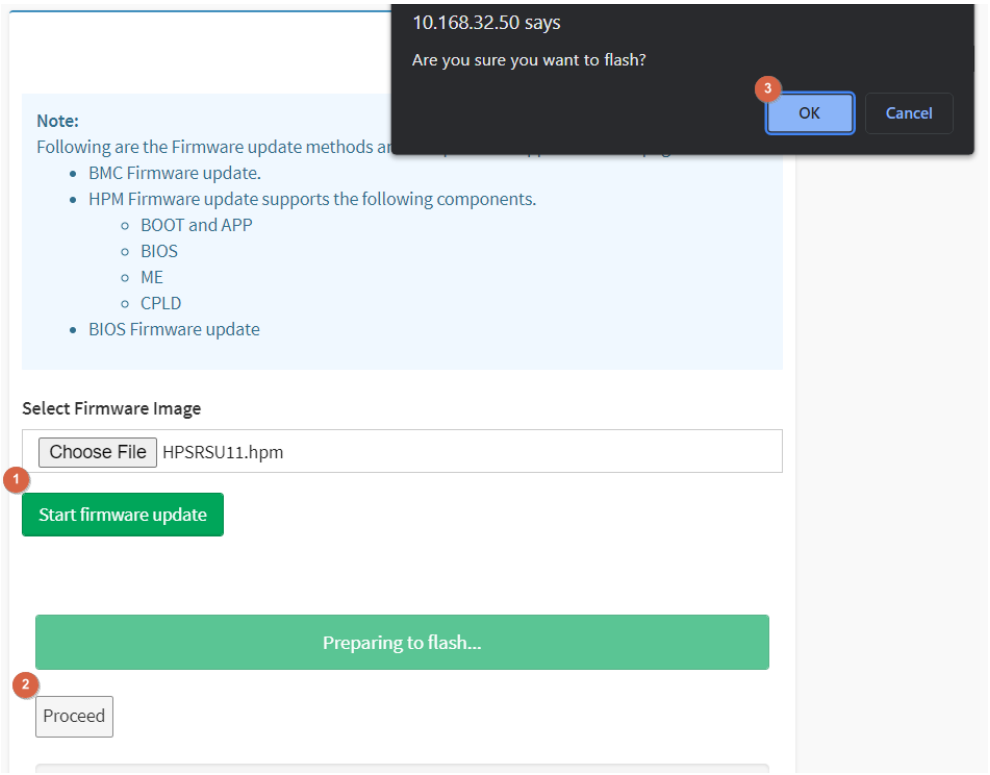
2. Click the **Maintenance** tab, then **Firmware Upate**.



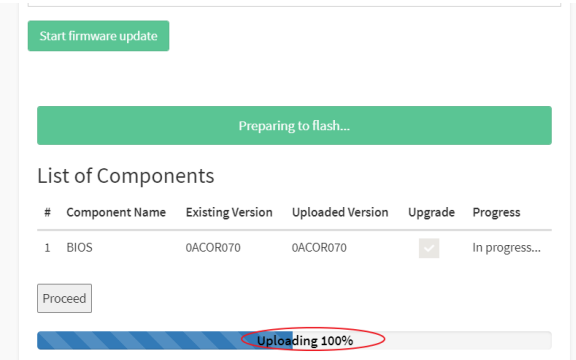
3. **Choose File** to select BIOS file(xxx.hpm).



4. Click the **Start firmware update** button, then **Proceed**. The message appears, "Are you sure you want to flash?". Click **OK**.



5. When "Uploading 100%", click **Preceed** again.



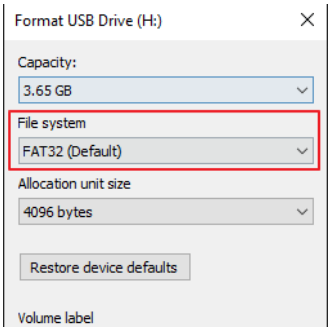
6. After finish the processs, BMC will reset after few seconds. Refer 1.1.1 step9 to check the BIOS and SPS version.

2. BIOS

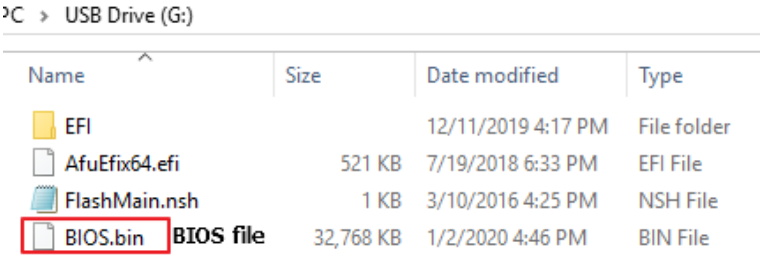
Update Method	OS	Tool
Local Update	UEFI environment	AfuEfix64.efi

2.1 BIOS update in UEFI environment

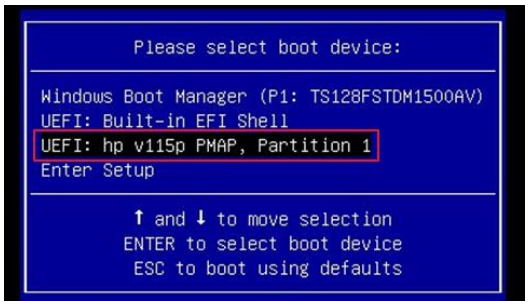
1. Format a USB flash drive to FAT32.



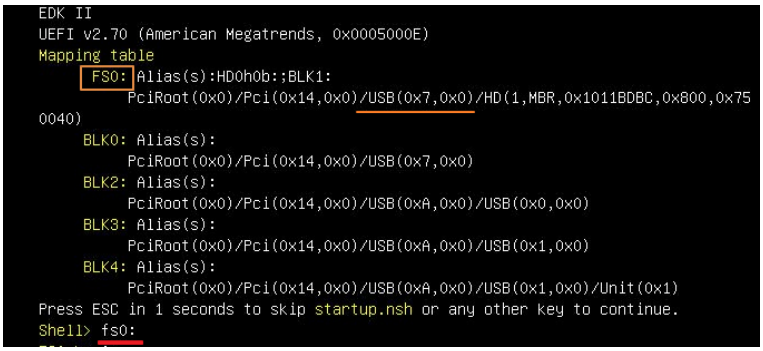
2. Download the tool and BOIS file(xxx.bin) and save at the **root** directdory of the USB drive.



3. Power on system. When you hear BIOS ready beep, perss **F11** to enter boot menu and select the USB drive to boot.



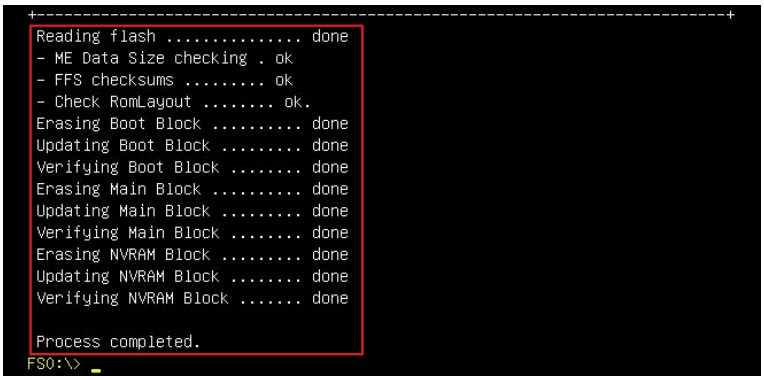
4. Type **fs*:** to enter the USB drive, for example **fs0:**



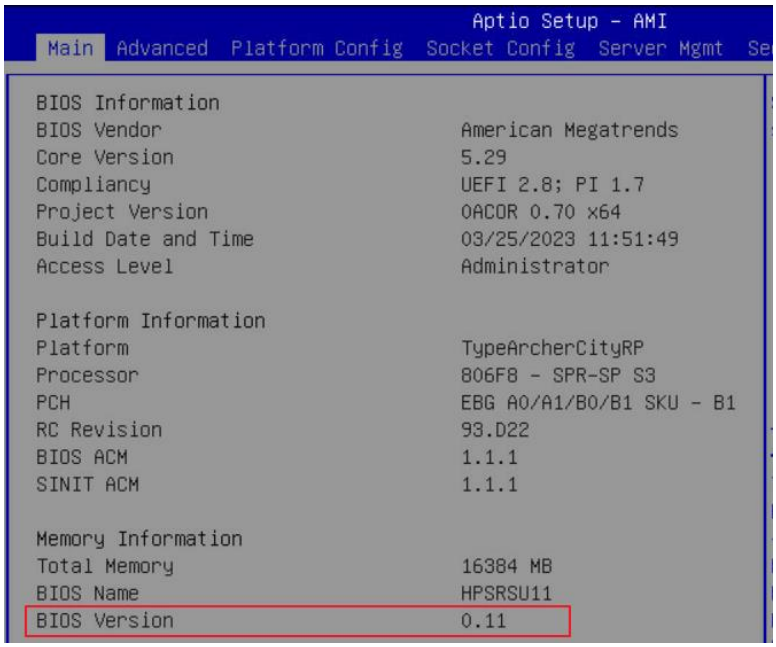
5. Type **FlashMain.nsh [BIOS file name]** to update BIOS.



6. When the process ends, make sure all regions are done successfully without any error.



7. Reboot to BIOS to check if BIOS version is correct.

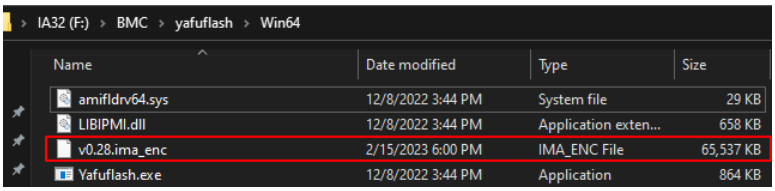


3. BMC

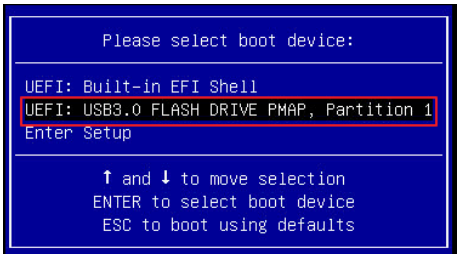
Update Method	OS	Tool
Local update	WinPE Environment	Yafuflash.exe
Remote update	IPMI Web UI	No tool required
	IPMI command	Yafuflash.exe

3.1 BMC update in WinPE environment

1. Copy update tool and BMC file to WinPE disk.

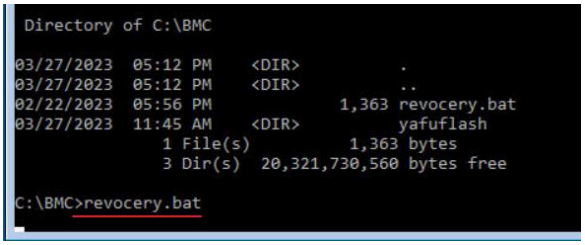


2. Plug the WinPE disk to the Server and power on. When you hear BIOS ready beep, press **F11** to enter boot menu and select the WinPE disk to boot.



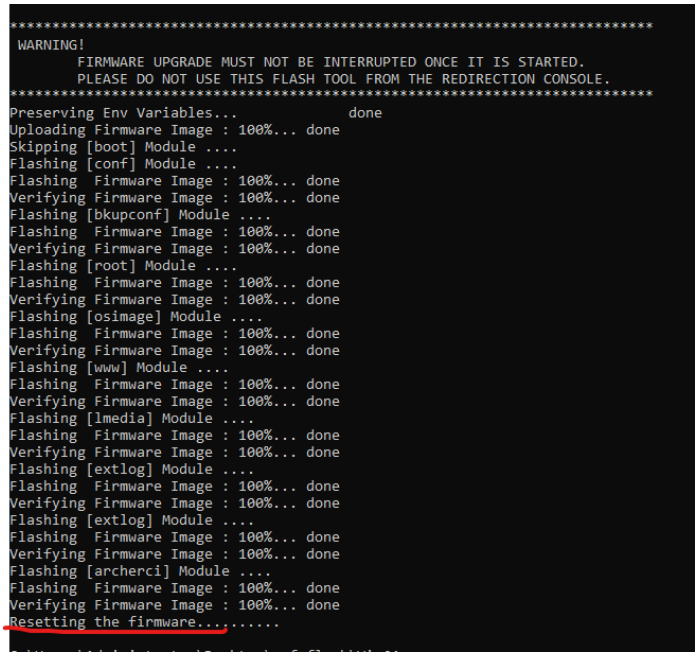
3. Switch to the ipmi tool folder and run the command.

revocery.bat

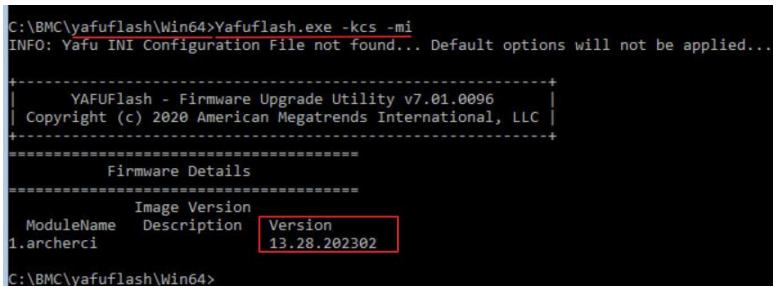


Please wait. This may take few minutes.

4. When the update process is finished, the BMC will be reset.



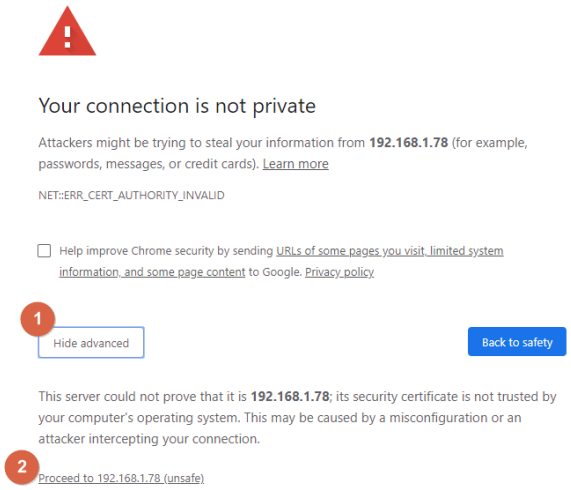
5. After BMC reset, enter **yafuflash\Win64** floder and run the command "Yafuflash -kcs -mi" to check BMC firmware version.



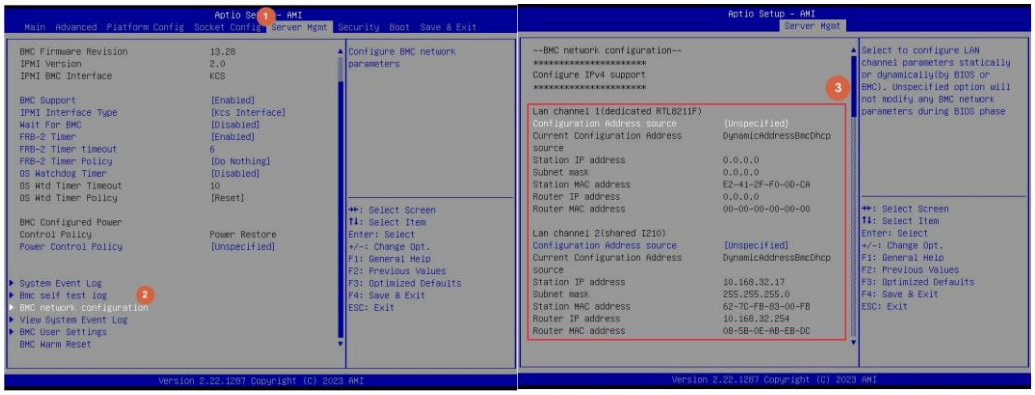
3.2 BMC update using Web UI

1. Open web browser. Enter BMC IP address and log in. The default user name and password are admin/admin.

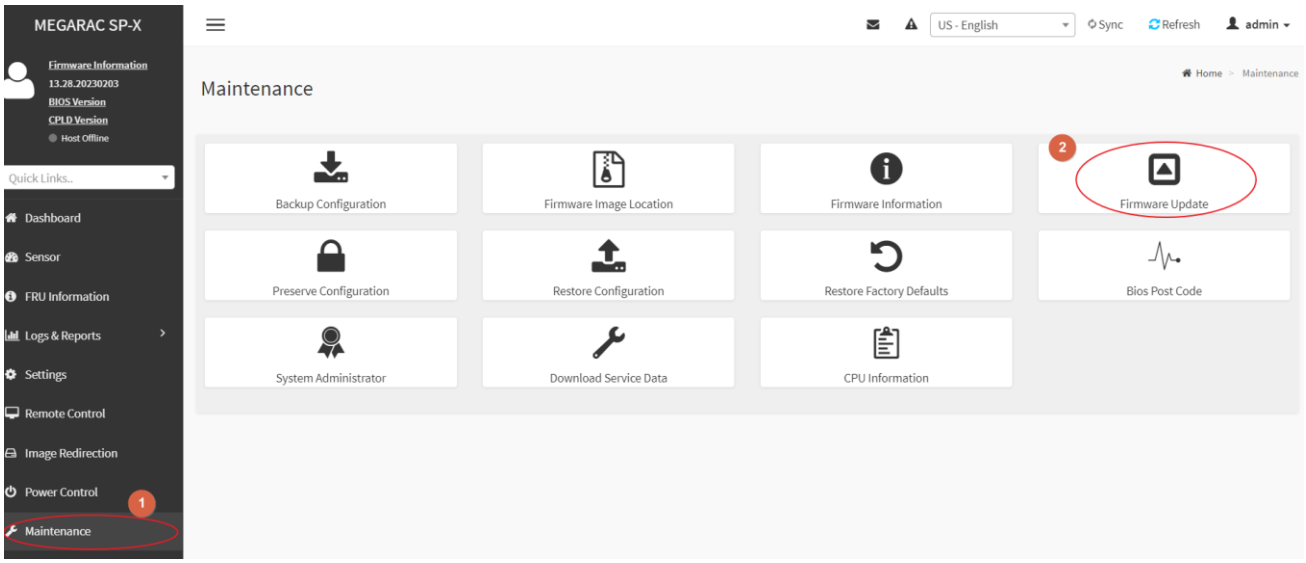
If you get a message that says "**Your connection is not private"**, just skip it.



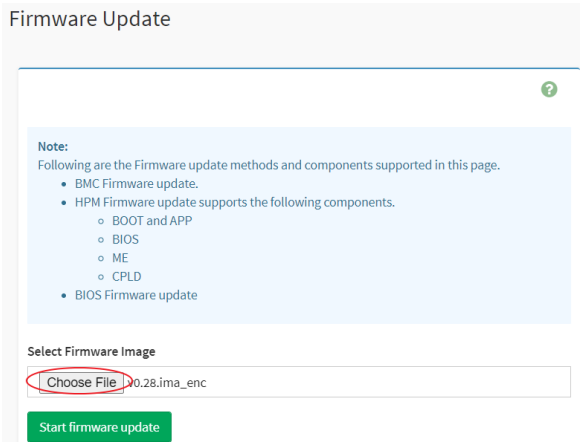
Note: BMC IP address can be configured at BIOS menu.



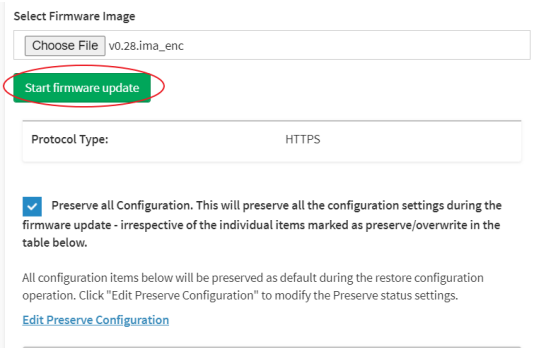
2. Click **Maintenance** and go to **Firmware Upate**.



3. **Choose File** to select BMC file.

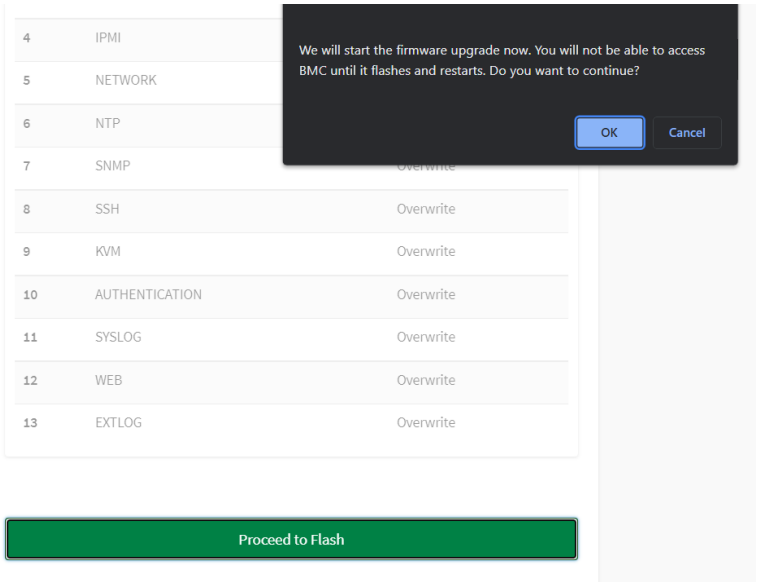


4. Click the **Start firmware update** button, then scroll down and check **Preserve all Configuration** if you'd like to preserve all configuration.

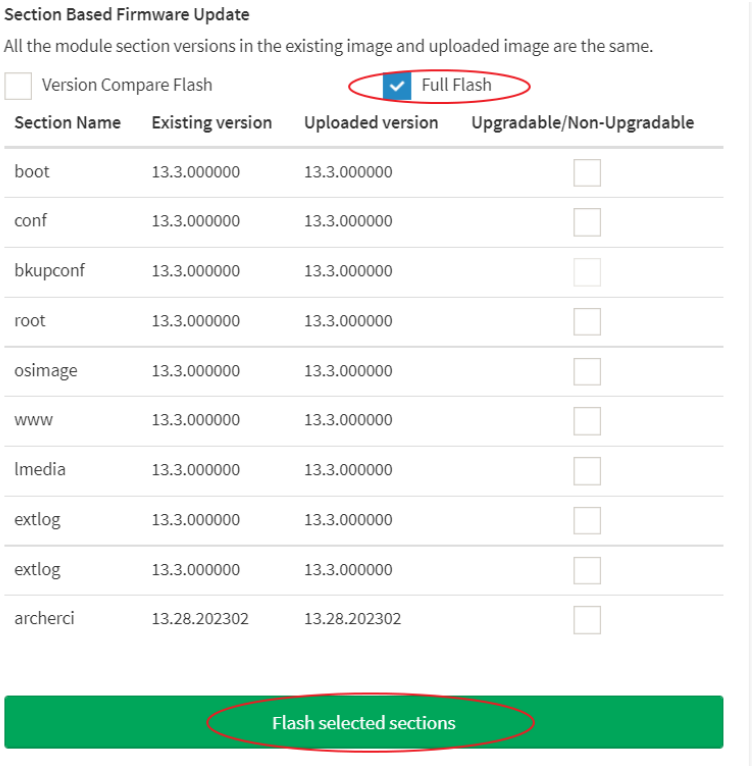


Click **Preceed to Flash**

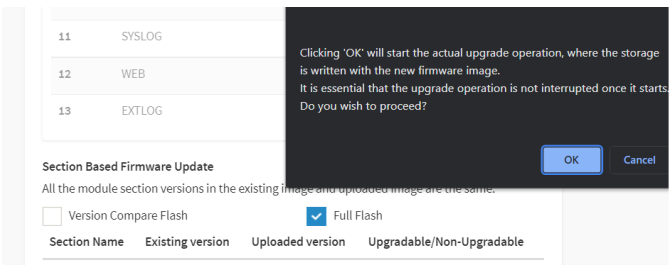
The message box appears. Click **OK**.



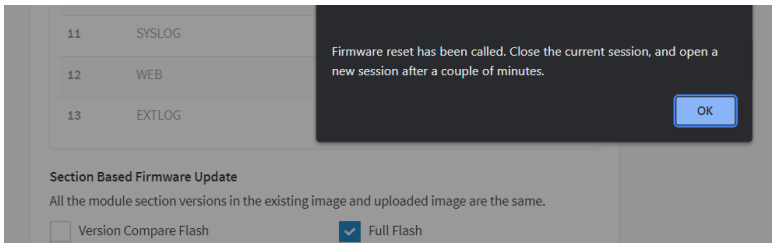
Select **Full Flash**, and click **Flash selected sections.**



When the message box shows up, click **OK** again.



5. The message appears, "Firmware reset has been called. Close this current session, and open a new session after a copule of minutes.". Click **OK**.

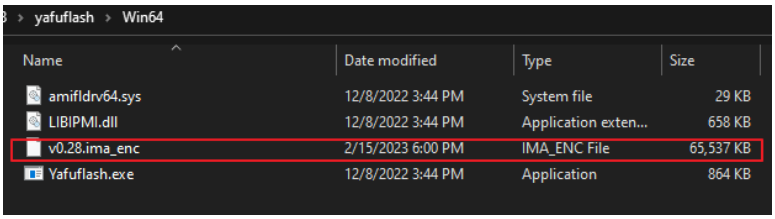


6. Login to check the BMC firmware version.



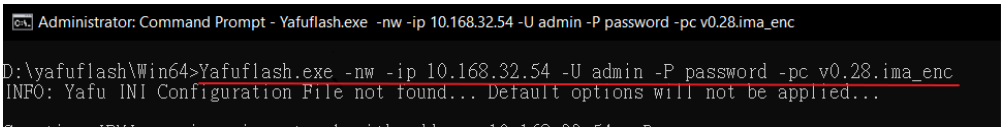
3.3 BMC update using IPMI tool

1. Make sure BMC file is saved in Win64 folder.

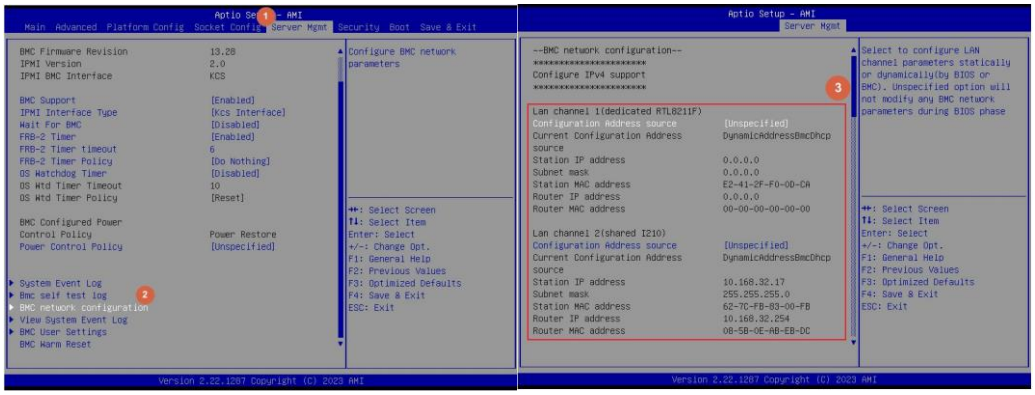


2. Open Command Prompt (admin).

3. Input the command:
Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -pc [BMC file name]. The default username and password are admin/admin.



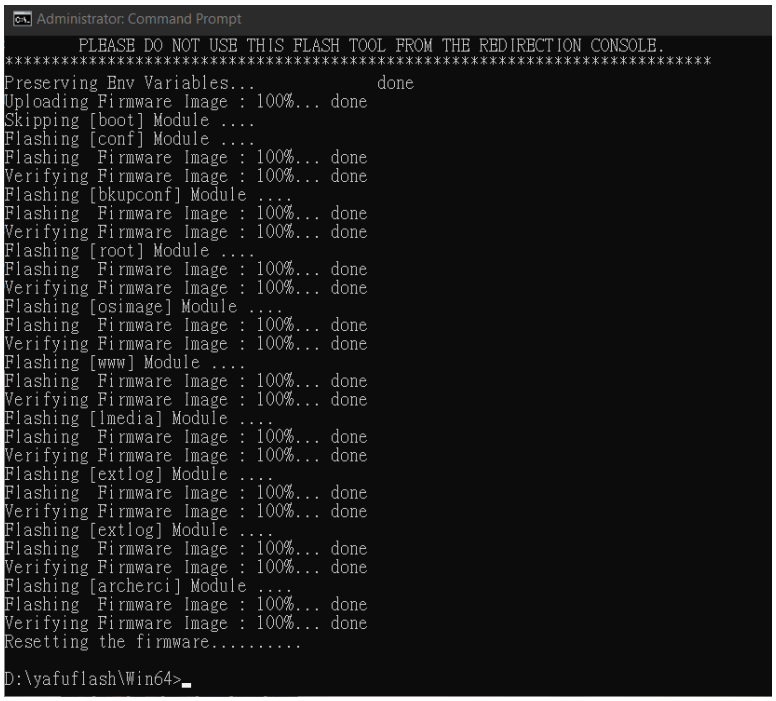
Note: BMC IP address can be configured at BIOS menu.



4. When the following screen shows, please wait few seconds.
The update process will start.

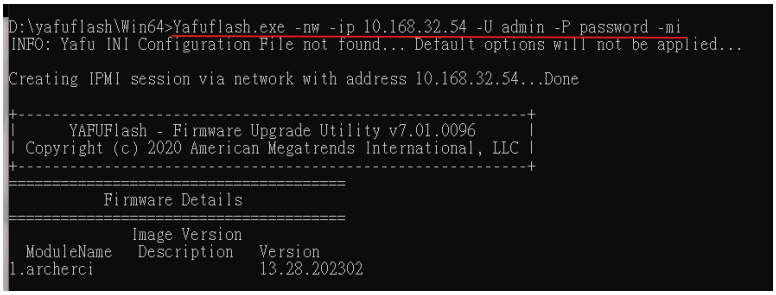


5. When the update process is finished, the BMC will be reset.



6. Wait few mintes for BMC reset. Check BMC firmware version by following fommand.

Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -mi



APPENDIX-G SMART FAN CONFIGURATION

The OEM command bytes are organized according to the following format specification:

Byte 1	Byte 2	Byte 3:N
Function code	Cmd	Data

Where:

Function code **0x30** is the OEM function code.

Cmd Command code. This message byte specifies the operation that it to be executed.

Data Zero or more bytes of data, as required by given command.

OEM Command table

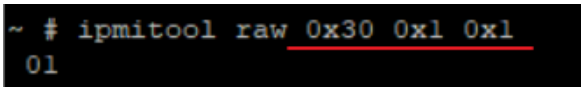
Description	Function code	Cmd	Data/Response data
Set Fan Mode	0x30	0x01	**Input data:** 0=standard speed , 1=manual speed
Get Fan Mode	0x30	0x30	**Response data:** 0=standard speed , 1=manual speed
Set fan PWM	0x30	0x35	[Fan] [PWM] Fan: 0 = CPU1_FAN1 1 = SYS_FAN1 2 = SYS_FAN2 3 = SYS_FAN3 4 = SYS_FAN4 5 = SYS_FAN5 6 = SYS_FAN6 PWM: The PWM duty cycle 0x64 =100%
Get fan PWM	0x30	0x36	The response data represent each fan PWM. Byte1 = CPU1_FAN1pwm duty cycle Byte2 = SYS_FAN1pwm duty cycle Byte3 = SYS_FAN2 pwm duty cycle Byte4 = SYS_FAN3 pwm duty cycle Byte5 = SYS_FAN4 pwm duty cycle Byte6 = SYS_FAN5 pwm duty cycle Byte7 = SYS_FAN6 pwm duty cycle

The OEM commands can be run at local or remote console. Please refer next section.

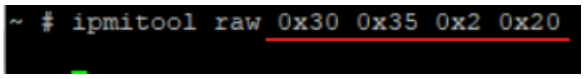
Example

Locally set PWM of SYS_FAN2 to 0x20 by "ipmitool" in Linux OS.

Step 1. Set fan mode as Manual mode



Step 2. Set fan PWM

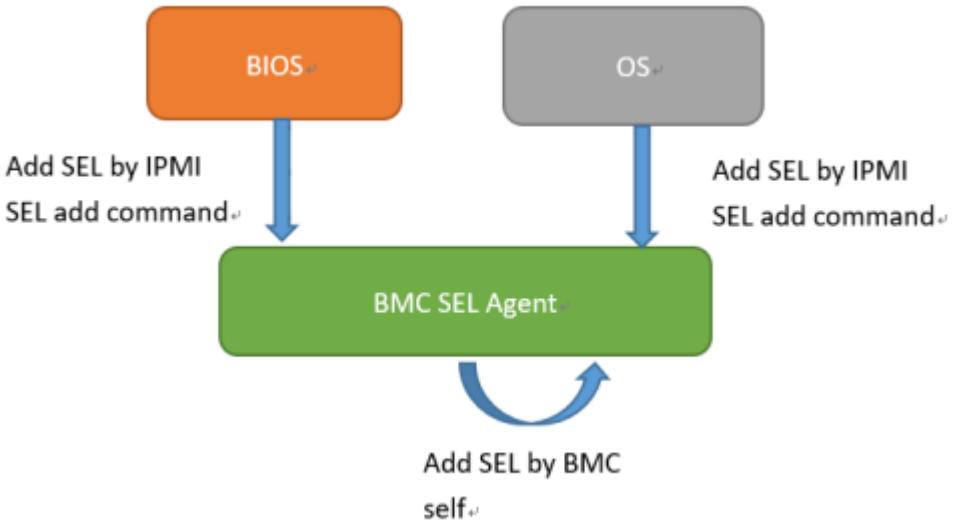


APPENDIX-H SYSTEM EVENT LOG(SEL)

System Event Log (SEL)

The BMC provides a centralized, non-volatile repository for critical, warning, and informational system events called the System Event Log (SEL). By having the BMC manage the SEL and logging functions, it helps to ensure that "post-mortem" logging information is available if a failure occurs that disables the system. The SEL is saved in BMC flash and SEL size is 16k to 64k.

The BMC allows access to the SEL from in-band and out-band mechanisms. There are various tools and utilities that can be used to access the SEL including the BMC web UI, BIOS and multiple open sourced IPMI tools.



SEL format

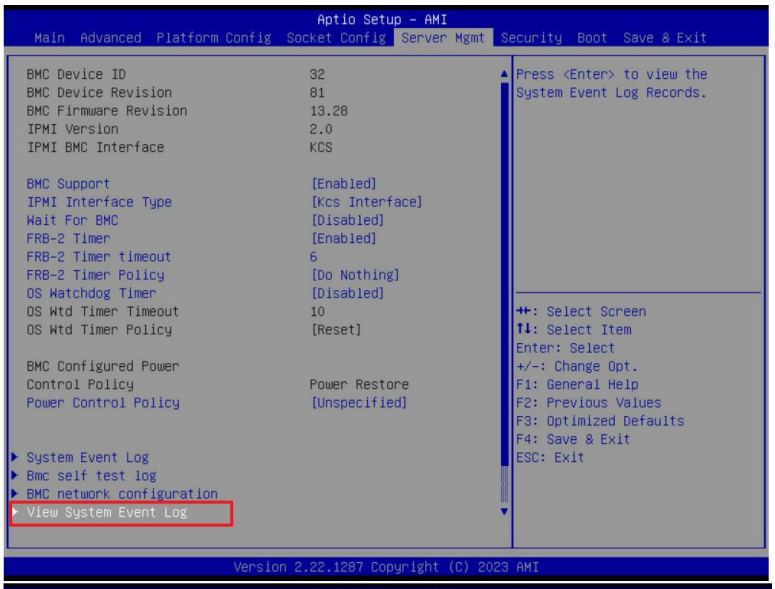
The System Event Log (SEL) record format is defined in the IPMI specification. The following section provides a basic definition for each of the field in a SEL. For more details, see the IPMI specification.

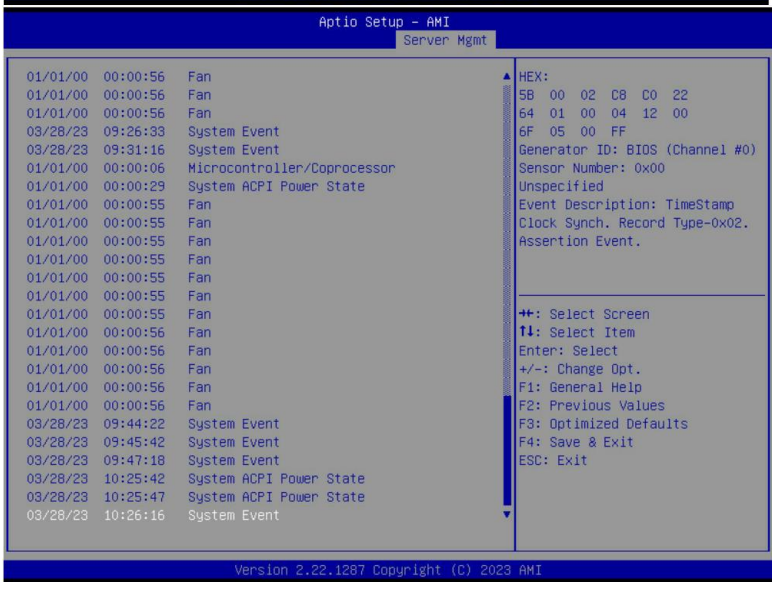
Byte	Field	Description
1, 2	Record ID (RID)	ID used for SEL record access.
3	Record Type (RT)	[7:0] – Record type 02h = System event record (default) C0h-DFh = OEM timestamped, bytes 8-16 OEM defined (see Table 3) E0h-FFh = OEM non-timestamped, bytes 4-16 OEM defined (see Table 4)
4-7	Timestamp (TS)	Time when the event was logged. The least significant byte is first. For example, TS:[29][76][68][4C] = 4C687629h = 1281914409 = Sun, 15 Aug 2010 23:20:09 UTC Note: There are various websites that convert the raw number to a date/time.
8, 9	Generator ID (GID)	RqSA and LUN if event was generated from IPMB. Software ID if event was generated from system software. *Byte 1* [7:1] – 7-bit I2C slave address, or 7-bit system software ID [0] – 0b = ID is IPMB slave address, 1b = System software ID Software ID values: 0001h – BIOS POST for POST errors, RAS configuration/state, timestamp synch, OS boot events 0033h – BIOS SMI handler 0020h – BMC firmware (default) 002Ch – Intel ME firmware 0041h – Server management software 00C0h – HSC firmware – HSBP A 00C2h – HSC firmware – HSBP B *Byte 2* [7:4] – Channel number. Channel that event message was received over. 0h if the event message was received from the system interface, primary IPMB, or internally generated by the BMC. [3:2] – Reserved. Write as 00b. [1:0] – IPMB device LUN if byte 1 holds slave address. 00b otherwise.
10	EvM Rev (ER)	Event message format version. 04h = IPMI v2.0 (default) 03h = IPMI v1.0
11	Sensor Type (ST)	Sensor type code for sensor that generated the event.
12	Sensor # (SN)	Number of sensor that generated the event (from SDR).
13	Event Dir/Event Type (EDIR)	*Event Dir* [7] – 0b = Assertion event, 1b = Deassertion event. *Event Type* Type of trigger for the event; for example, critical threshold going high, state asserted, and so on. Also indicates class of the event; for example, discrete, threshold, or OEM. The Event Type field is encoded using the Event/Reading Type Code. [6:0] – Event Type Codes 01h = Threshold (states = 0x00-0x0b) 02h-0ch = Discrete 6Fh = Sensor-specific 70-7Fh = OEM
14	Event Data 1 (ED1)	See Table 2.
15	Event Data 2 (ED2)	
16	Event Data 3 (ED3)	

When capturing the SEL log, always collect both the text/human readable version and the hex version. Because some of the data is OEM-specific, some utilities cannot decode the information correctly. In addition, with some OEM-specific data there may be additional variables that are not decoded at all.

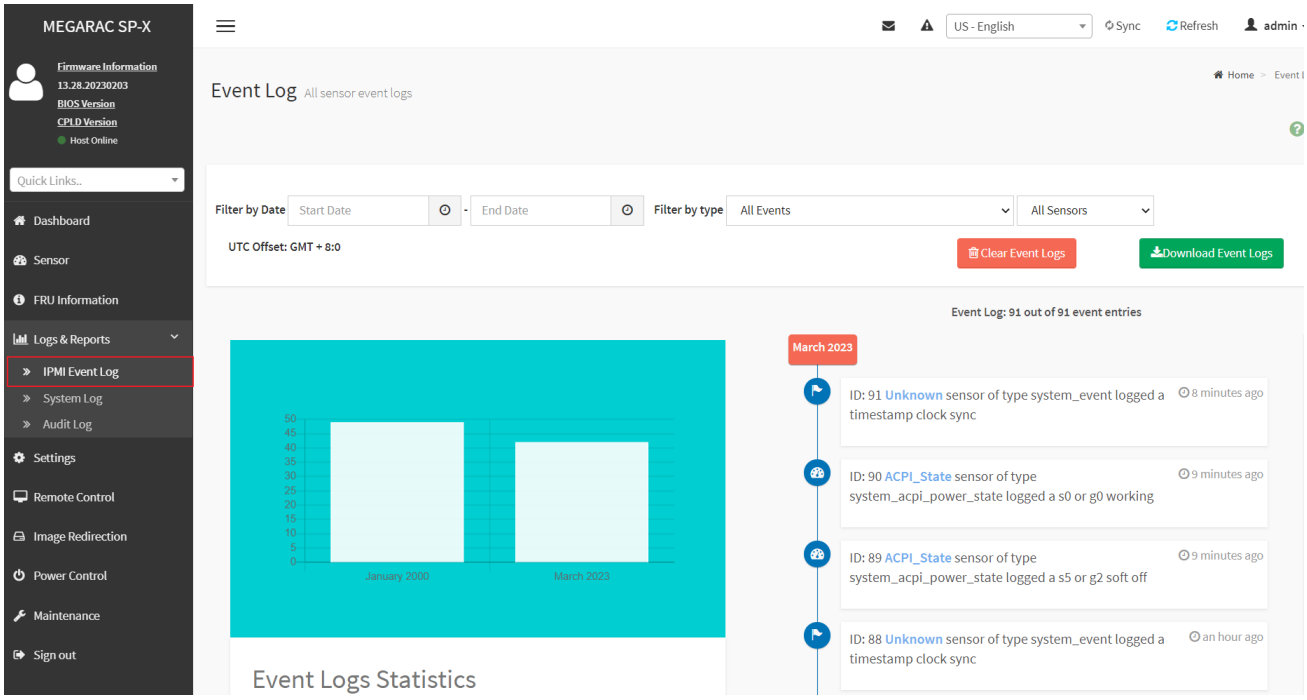
3 ways to check SEL log

- BIOS setup
    1. Power on and enter BIOS setup
    2. Go to Server Mgmt => View System Event Log





- BMC Web
  1. Login BMC web UI
  2. Go to Logs & Reports >> IPMI Event Log



- **IPMI tool**

LAN (remote)

Linux:

ipmitool –I lanplus –H [BMC IP address] -U [user name] -P [user password] sel elist

Windows:

ipmiutil.exe sel -N [BMC IP address] -U [user name] -P [user password]

```
D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe sel -N 192.168.1.78 -U ADMIN -P ADMIN
ipmiutil sel version 3.15
Connecting to node  192.168.1.78
-- BMC version 0.28, IPMI version 2.0
SEL Ver 37 Support 0f, Size = 3639 records (Used=426, Free=3213)
RecId Date/Time_____ SEV Src_ Evt_Type___ Sens# Evt_detail - Trig [Evt_data]
0001 09/30/21 13:28:14 INF BMC  Chassis #94  - 03 [01 ff ff]
0002 09/30/21 13:28:14 INF BMC  ACPI Power State #99  S0/G0 Working 6f [00 ff ff]
0003 09/30/21 13:29:17 INF BMC  System Firmware #00  prog, Reserved 6f [02 92 ff]
0004 09/30/21 13:52:09 INF BMC  ACPI Power State #99  S4/S5 soft-off, no specific state 6f [06 ff ff]
```

KCS(local)

Linux:

ipmitool sel elist

Windows:

ipmiutil.exe sel

IPMI tools:

ipmitool: https://github.com/ipmitool/ipmitool

ipmiutil: http://ipmiutil.sourceforge.net/

Log Policy:

Linear Storage Policy

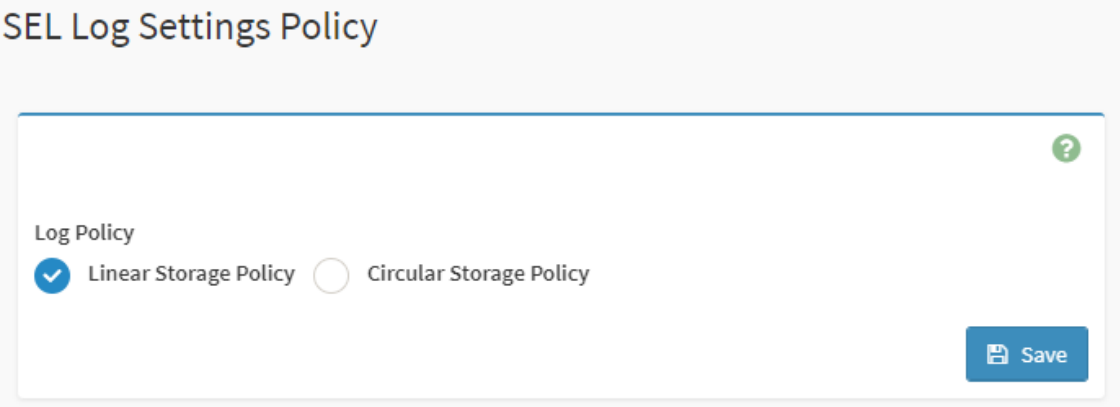
BMC will not overwrite log but inform user when the log size reach 70% and 100%.

Circular Storage Policy

BMC will overwrite log using FIFO (first-in-first-out) algorithm when log is full.

You can configure the log policy in Web-UI, and default setting is [Linear Storage Policy]

Settings➔ Log Settings➔ SEL Log Settings Policy



APPENDIX-I IPMI TO GET BIOS POST CODE

OEM Message format

The OEM command bytes are organized according to the following format specification:

Byte 1	Byte 2	Byte 3:N
Function code	Cmd	Data

Where:

Function code **0x32** is the Get BIOS code OEM command, and default Privilege Level is User.

If you use "**ipmiutil**" tool in Windows OS, replace "0x32" with "00 20 C8".

Cmd Command code. This message byte specifies the operation that it to be executed.

Data Zero or more bytes of data, as required by given command.

Get BIOS code Commands

This command is used the read BIOS code. The BIOS Code response length is 256 bytes for each block and total BIOS Code length supported to a maximum value of 512 Bytes.

NetFn	0x32
Command	0x73
Request Data	0h = Read first 256 bytes of Current BIOS code 1h = Read first 256 bytes of Previous BIOS code.

Example:

Locally get BIOS code by "ipmitool" in Linux.

Ipmitool raw 0x32 0x73 0

```
root@test-Default-string:/home/test# ipmitool raw 0x32  0x73 0
 02 03 04 05 06 19 a1 a3 a3 a7 a9 a7 a7 a7 a8 a9
 a9 aa ae af e1 e4 e3 e5 b0 b0 b0 b1 b1 b4 b2 b3
 b3 b3 b6 b6 b6 b6 b6 b6 b7 b7 be b7 b7 b8 b8 b8
 b8 b9 b9 b9 bb bb bb bb bb bb bb bb bb b7 bc bc
 bc bc bc bf e7 e8 e9 eb ec ed ee 4f 61 9a 78 68
 70 79 d1 d3 d4 91 92 94 94 94 94 94 94 94 94 94
 94 94 94 95 96 ef 92 92 92 99 91 d5 92 92 92 92
 97 98 9d 9c 92 b4 b4 b4 b4 b4 b4 b4 b4 b4 b4 a0
 a2 a2 a0 a2 a2 a2 a2 a2 a2 a2 a2 99 92 92 92 ad
 78 b1 a0 84 aa e3 e3 e3
```

The latest BIOS code is e3.

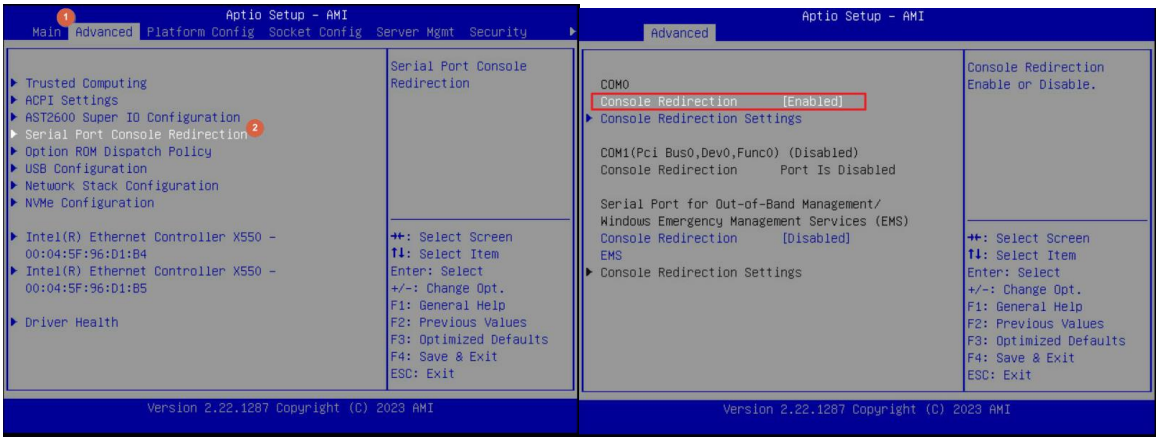
Remotely get BIOS code by "ipmiutil" in windows:

ipmiutil.exe cmd –N [BMC IP] -U [user name] -P [user password 00 20 c8 73 0

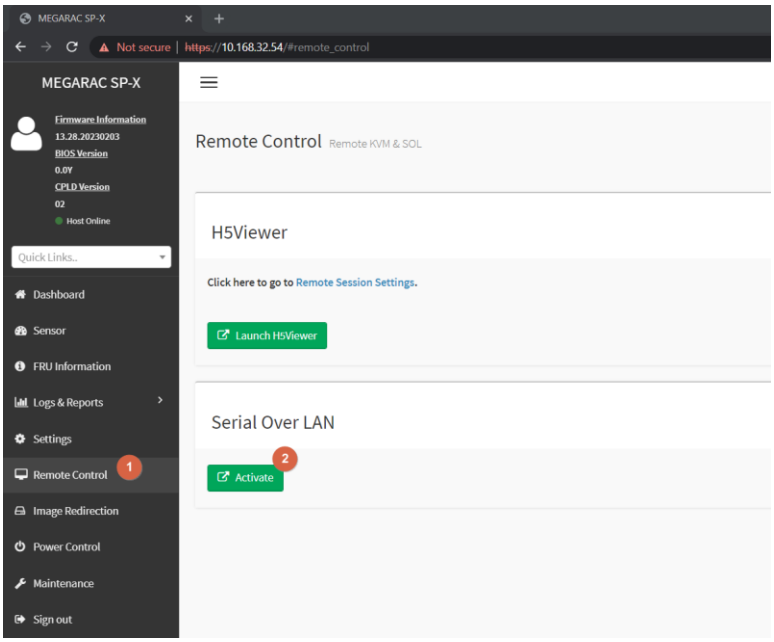
```
D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.77 -U admin -P admin 00 20 C8  73 0
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node  192.168.1.77
-- BMC version 0.5, IPMI version 2.0
respData[len=160]: 02 03 04 05 06 19 a1 a3 a3 a7 a9 a7 a7 a7 a8 a9 aa ae af e1 e4 e3 e5 b0 b0 b0 b1 b1 b
4 b2 b3 b3 b3 b6 b6 b6 b6 b6 b6 b7 b7 be b7 b7 b7 b8 b8 b8 b8 b8 b8 b9 b9 ba b9 bb bb bb bb bb bb bb bb bb
bb b9 b7 bc bc bc bc bc bc bf e6 e7 e8 e9 eb ec ed ee 4f 61 9a 78 68 70 79 d1 d3 d4 91 92 94 94 94 94 94
 94 94 94 94 94 94 94 95 96 ef 92 92 92 99 91 d5 92 92 92 92 97 98 9d 9c 92 a0 b4 b4 b4 b4 b4 b4 b4 b
4 b4 a2 a2 a0 a2 a2 a2 a2 a2 a2 a2 a2 99 92 92 92 ad 78 b1 a0 ee ee ee 84 aa e3 e3
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

APPENDIX-J REMOTE CONTROL-Serial Over LAN

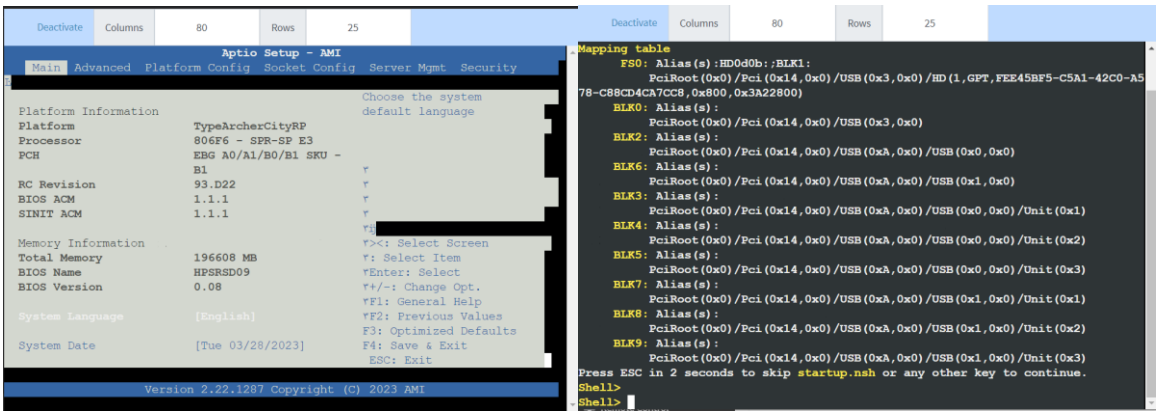
1. Enable **Serial Port Console Redirection** in BIOS setup menu.



2. Select the "Remote Control" page and the click [Serial Over LAN]. The broswer will start to run **Serial Over LAN**.

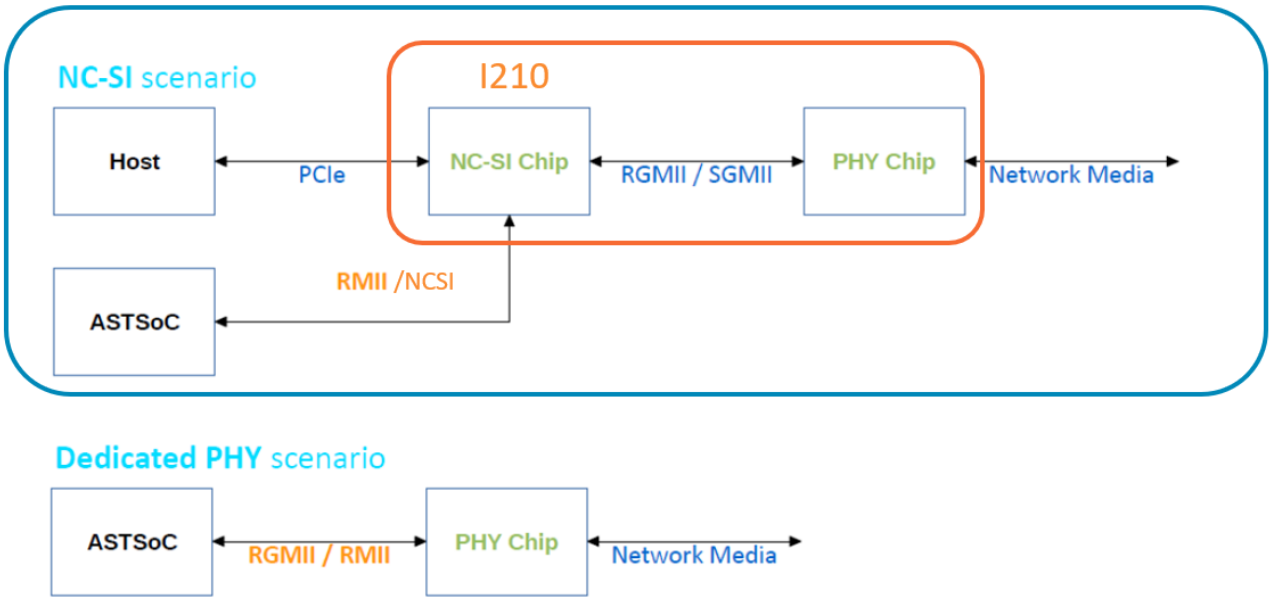


3. Access BIOS and UEFI shell in serial console.



APPENDIX-K Dedicated vs Shared IPMI port

Dedicated PHY scenario vs NC-SI(Shared) scenario

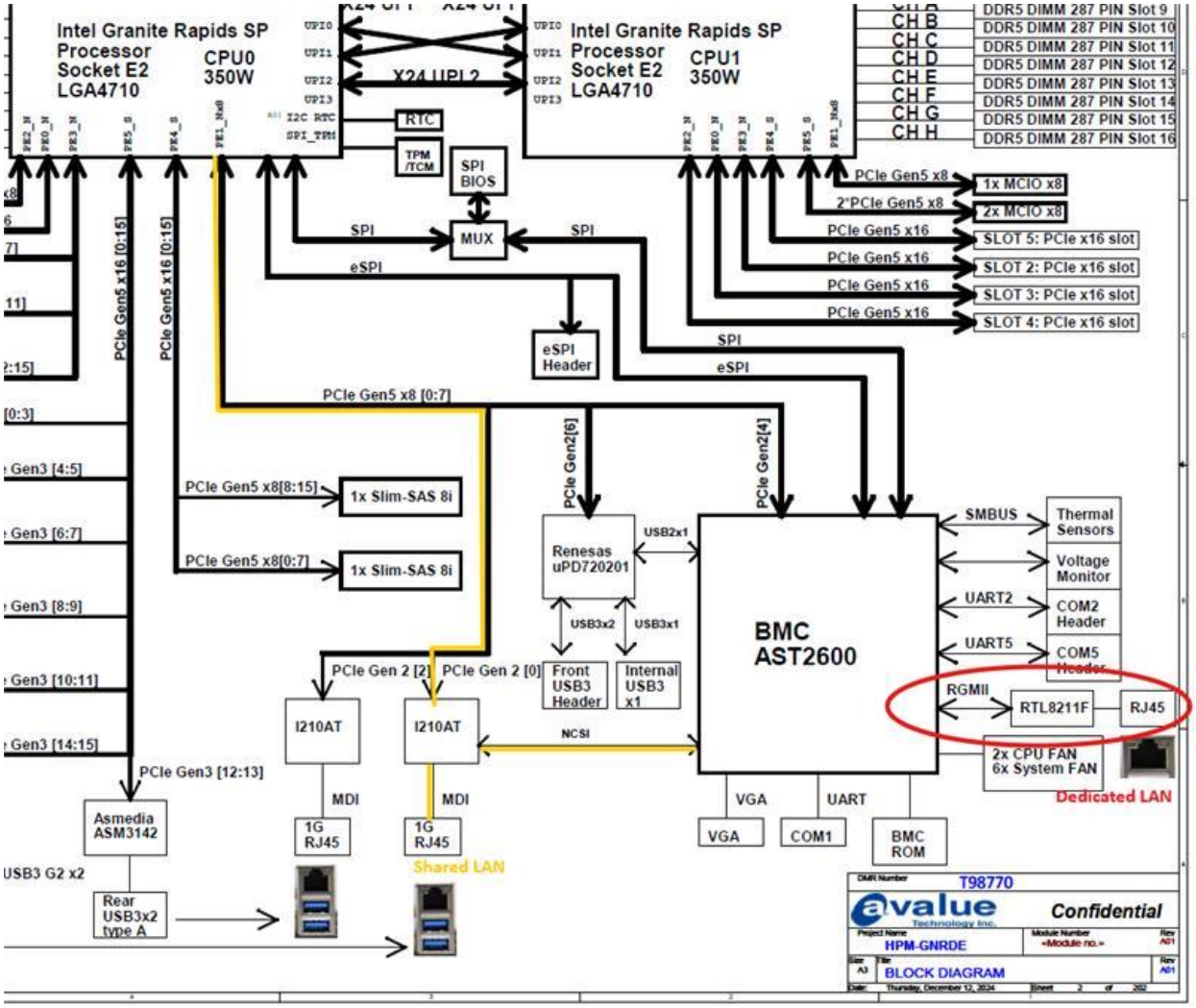


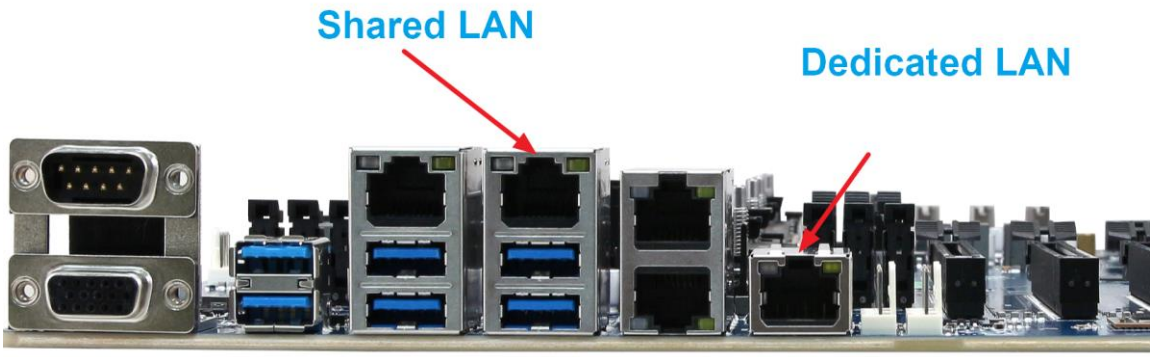
Network Controller Sideband Interface (NC-SI)

NC-SI, is an electrical interface and protocol defined by the Distributed Management Task Force (DMTF). The NC-SI enables the connection of a baseboard management controller (BMC) to network interface controllers (NICs) in a server computer system for the purpose of enabling out-of-band system management. This allows the BMC to use the network connections of the NIC ports for the management traffic, in addition to the regular host traffic.

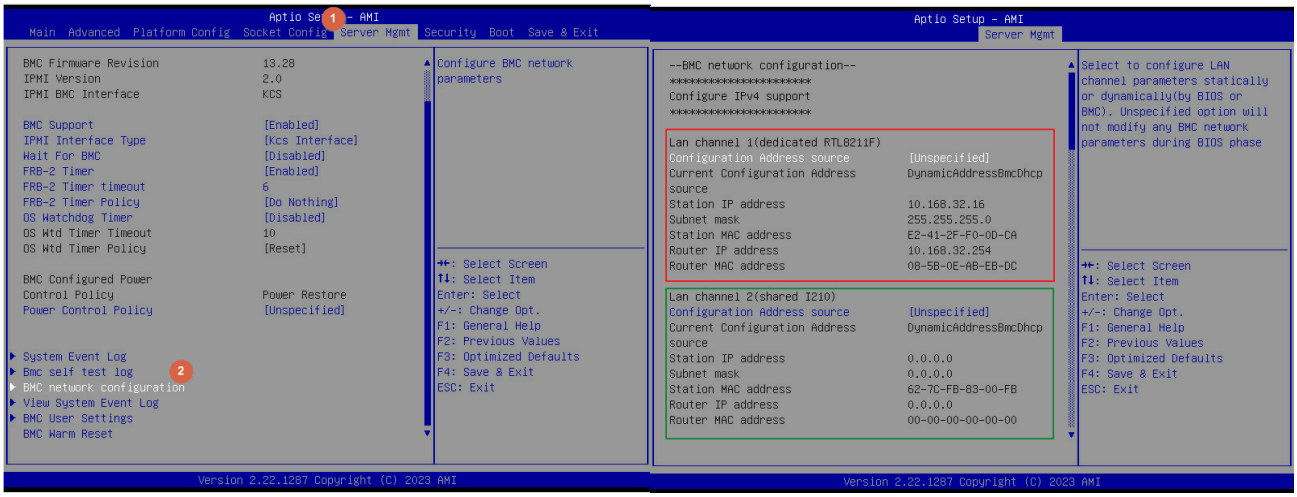
The NC-SI defines a control communication protocol between the BMC and NICs.

HPM-ERSDE

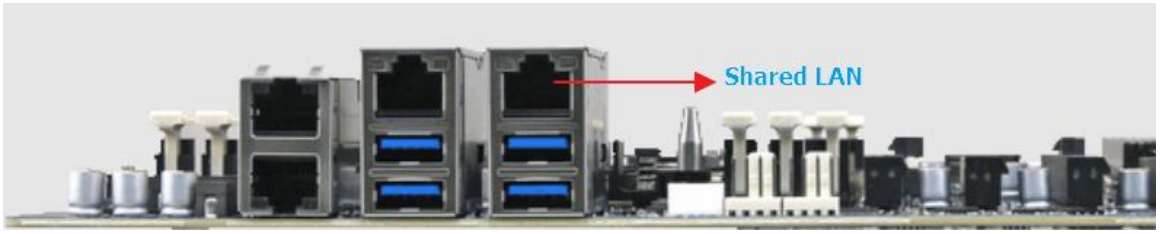

Intel Granite Rapids SP Processor Socket E2 LGA4710
CPU0 350W
Intel Granite Rapids SP Processor Socket E2 LGA4710
CPU1 350W
X24 UPI 2
RTC
TPM /TCM
SPI BIOS
MUX
SPI
eSPI
eSPI Header
DDR5 DIMM 287 PIN Slot 9
DDR5 DIMM 287 PIN Slot 10
DDR5 DIMM 287 PIN Slot 11
DDR5 DIMM 287 PIN Slot 12
DDR5 DIMM 287 PIN Slot 13
DDR5 DIMM 287 PIN Slot 14
DDR5 DIMM 287 PIN Slot 15
DDR5 DIMM 287 PIN Slot 16
CH B
CH C
CH D
CH E
CH F
CH G
CH H
PCIe Gen5 x8
1x MCIO x8
2*PCIe Gen5 x8
2x MCIO x8
PCIe Gen5 x16
SLOT 5: PCIe x16 slot
SLOT 2: PCIe x16 slot
SLOT 3: PCIe x16 slot
SLOT 4: PCIe x16 slot
PCIe Gen5 x16 [0:15]
PCIe Gen5 x8 [0:7]
PCIe Gen5 x8[8:15]
1x Slim-SAS 8i
PCIe Gen5 x8[0:7]
1x Slim-SAS 8i
PCIe Gen2[6]
PCIe Gen2[4]
Renesas uPD720201
USB2x1
USB3x2
USB3x1
Front USB3 Header
Internal USB3 x1
BMC AST2600
SMBUS
Thermal Sensors
Voltage Monitor
UART2
COM2 Header
UART5
COM5 Header
RGMII
RTL8211F
RJ45
2x CPU FAN
6x System FAN
Dedicated LAN
PCIe Gen 2 [2]
PCIe Gen 2 [0]
I210AT
I210AT
NCSI
MDI
MDI
1G RJ45
1G RJ45
Shared LAN
PCIe Gen3 [12:13]
Asmedia ASM3142
USB3 G2 x2
Rear USB3x2 type A
VGA
UART
VGA
COM1
BMC ROM
T98770
Confidential
HPM-GNRDE
BLOCK DIAGRAM


Shared LAN
Dedicated LAN

Both dedicated LAN and shared LAN can be configured in BIOS setup menu.



HPM-621 shared LAN



Q&A

1. Which one is recommended for BMC management?
   A dedicated LAN is usually a local area network dedicated to server management. By establishing a private LAN connection between the server and the management computer, the administrator can access and manage the server without worrying about collisions or interference with other network traffic.

   If you have a limited budget or space for network cabling, NC-SI may be a good option as it uses the existing network infrastructure. However, if you have security concerns, a dedicated LAN may be a better choice.

   In summary, the choice between NC-SI and a dedicated LAN for BMC management depends on your specific needs, budget, and security requirements.

2. What is the bandwidth of dedicated LAN?
   Bandwidth of dedicated LAN which is RTL8211F is 1000Mbps.