

HPS-SRSU4A /HPS-SRSUTA IPMI Setup User's Manual

1st Ed –17 June 2023

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 © 2023 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

HPS-SRSU4A/HPS-SRSUTA User's Manual

first.

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

<http://www.avalue.com.tw/>

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

Glossary & Abbreviation	6
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.....	84
2.8 HOME>IMAGE REDIRECTION	86
2.9 HOME> POWER CONTROL.....	86
2.10 HOME> MAINTENANCE.....	88
2.11 HOME> SIGN OUT	98
APPENDIX-A BMC HARDWRE: AST2600	99
APPENDIX-B IPMI COMMANDS SUPPORT TABLE	102
APPENDIX-C IPMI OEM COMMANDS LIST	107
APPENDIX-D SENSOR TABLE	108
APPENDIX-E DEFAULT CONFIGURATION	110
APPENDIX-F FIRMWARE UPDATE	111
APPENDIX-G SMART FAN CONFIGURATION.....	128
APPENDIX-H SYSTEM EVENT LOG(SEL)	130
APPENDIX-I IPMI TO GET BIOS POST CODE	135
APPENDIX-J REMOTE CONTROL-Serial Over LAN	137
APPENDIX-K Dedicated vs Shared IPMI port.....	138

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.

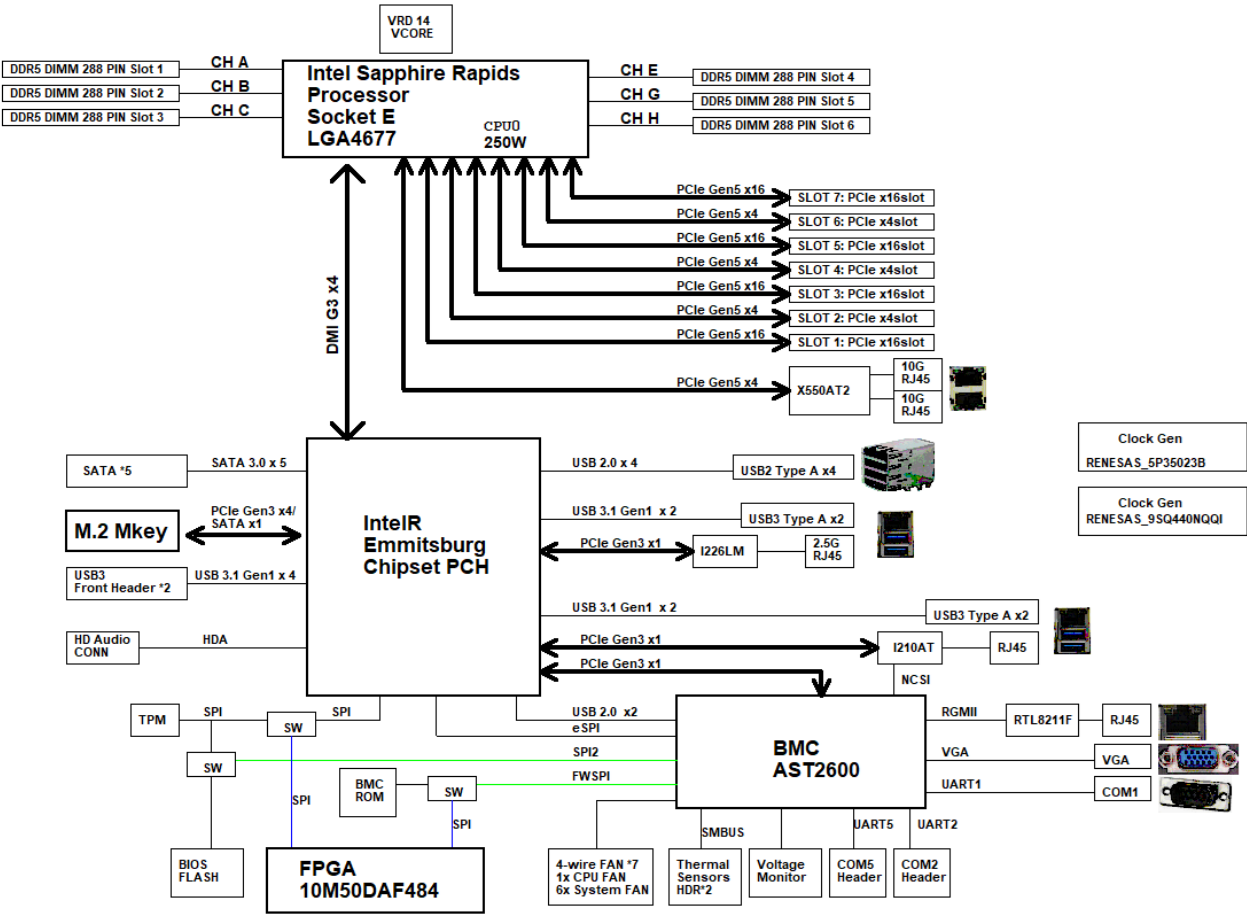


Figure 1-1 System block diagram

1.2 PLATFORM AND BMC COMPONENTS

Table 1-1 Main component related to BMC

Intel platform	- CPU(Sapphire Rapids) + PCH(Emmitsburg)
BMC	AST2600
Flash ROM	BIOS side: 32MB BMC side: 64MB
BMC Memory	512MB
BMC LAN	RGMII1: Dedicated PHY RTL8211F RMII3: Shared NIC I210AT
FRU device	CAT24C512
UART	UART1: System UART UART2: System UART UART5: BMC console
LED	BMC Heartbeat LED Off: BMC is initialization LED On: BMC is working normally
Button	Power button System Reset button
CPLD	Intel 10M50DAF484C8G
Firmware Vendor of Code Base	AMI MegaRAC 13.3

1.3 I2C BLOCK DIAGRAM

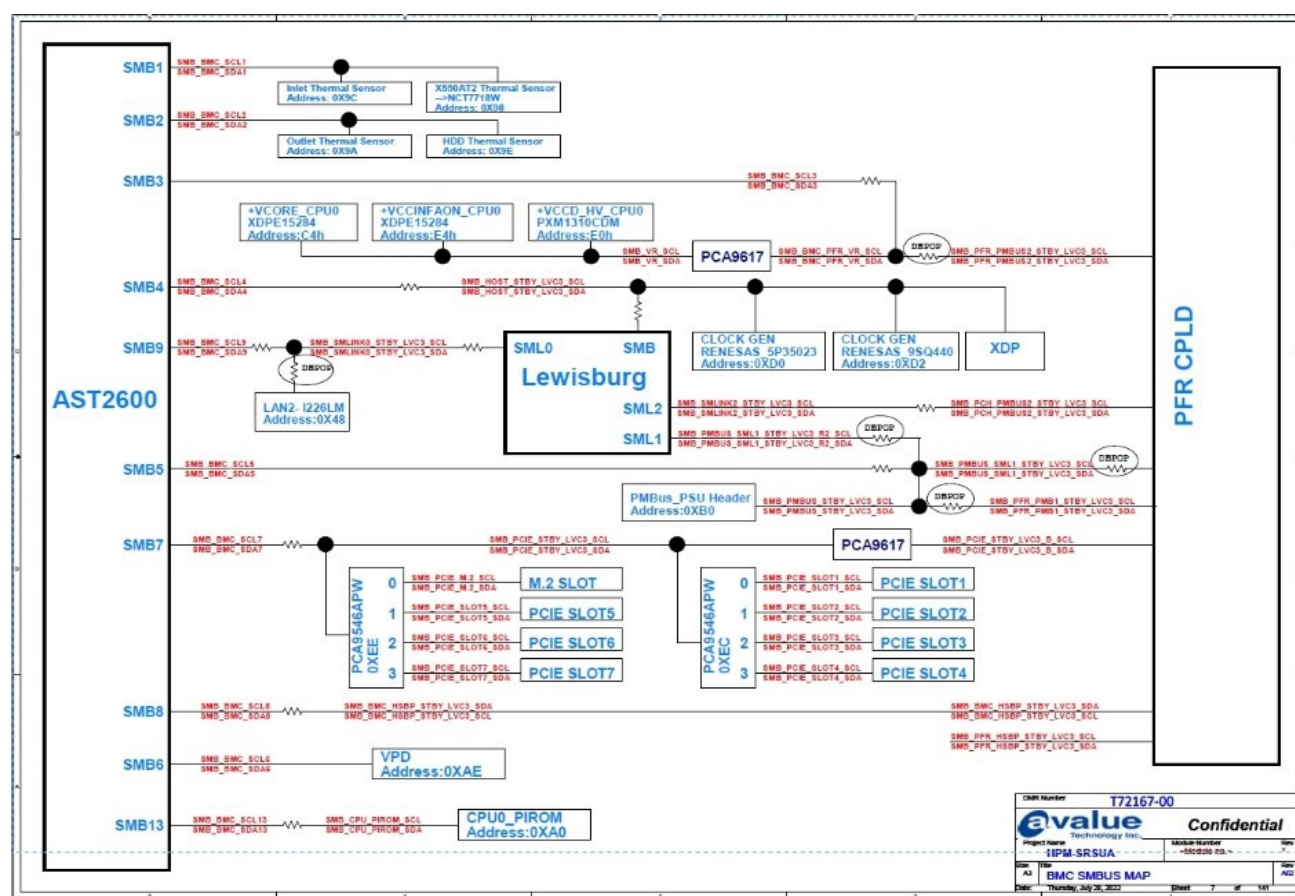


Figure 1-2 I2c block diagram

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	Bus ID (channel no + bus ID + bus type)		Slave address		BMC use? (V)	Remark
1	0x2		0x9C		V	Inlet Thermal Sensor
			0x98		V	X550AT2 Thermal Sensor
2	0x4		0x9A		V	Outlet Thermal Sensor
			0x9E		V	HDD Thermal Sensor
3	0x6		0xC4		V	VCORE CPU0
			0xE4		V	VCCINFAON CPU0
			0xE0		V	VCCD HV CPU0
4	0x8		0xD0		V	CLOCK GEN RENESAS 5P35023
			0xD2		V	CLOCK GEN RENESAS 9SQ440
5	0xA		0xB0		V	PMBus PSU Header
6	0xC		0xAE			VPD
7	0xE	0xEC	PCA9546APW Channel 0		V	PCIE Slot 1
			PCA9546APW Channel 1			PCIE Slot 2

HPS-SRSU4A/HPS-SRSUTA User's Manual

			PCA9546APW Channel 2		PCIE Slot 3
			PCA9546APW Channel 3		PCIE Slot 4
		0xEE	PCA9546APW Channel 0	V	M.2 Solt
			PCA9546APW Channel 1		PCIE Slot 5
			PCA9546APW Channel 2		PCIE Slot 6
			PCA9546APW Channel 3		PCIE Slot 7
9	0x12	0x2C			PCH
13	0x14	0xA		V	CPU0 PIROM

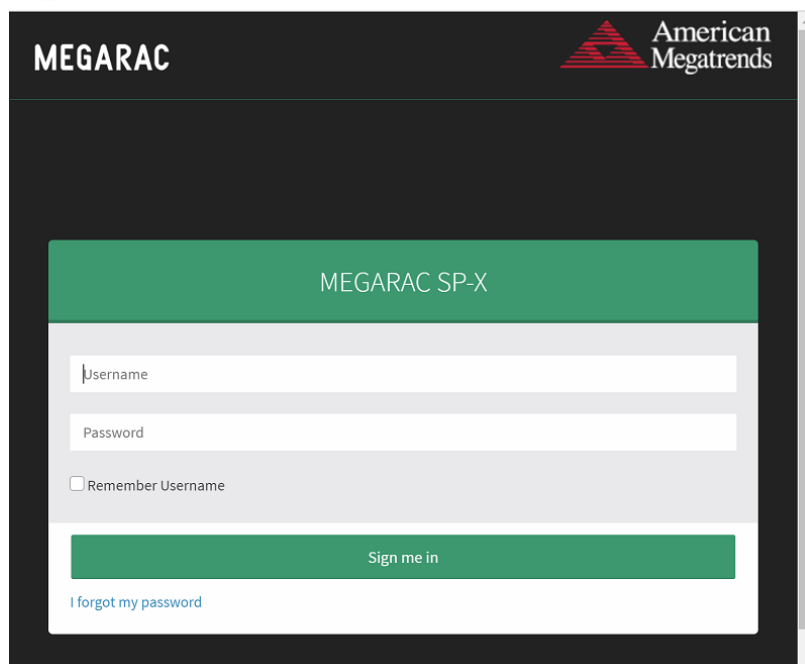
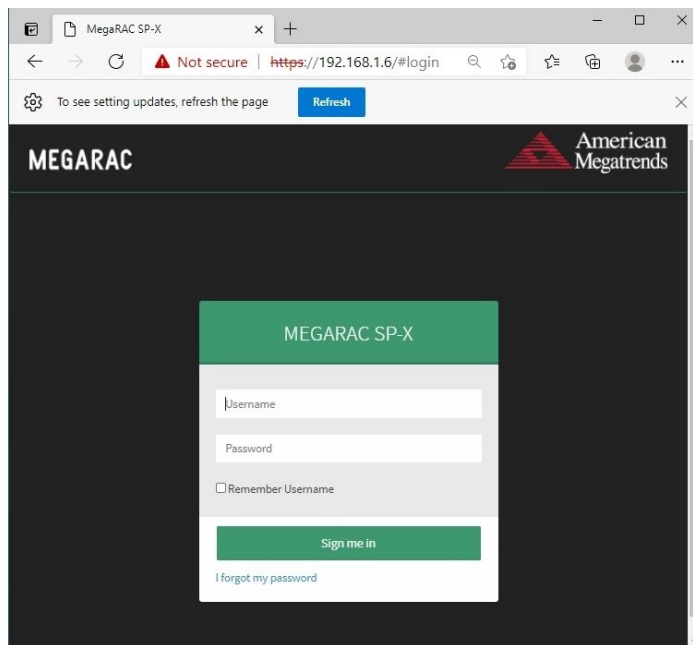
2. WEB UI

HPS-SRSU4A/HPS-SRSUTA User's Manual

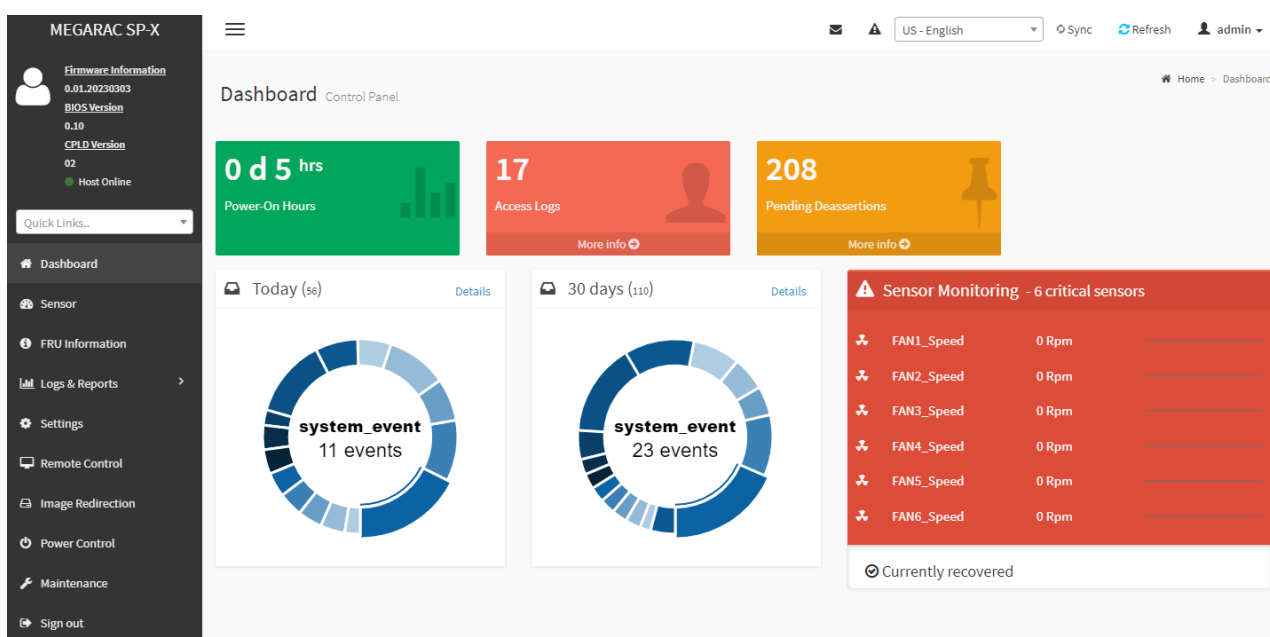
2.1 Log in

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    Sync  Refresh  admin ▾

	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.

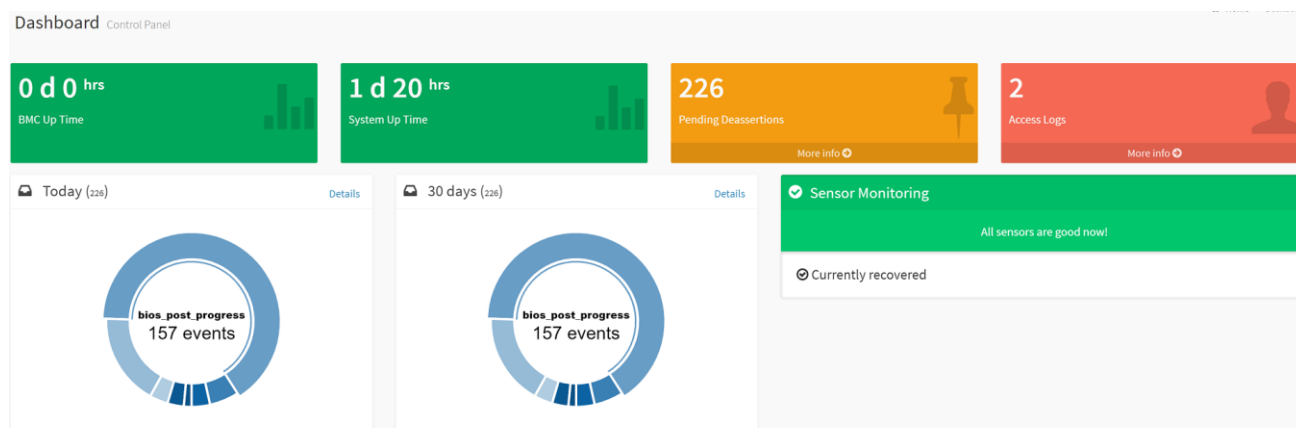
HPS-SRSU4A/HPS-SRSUTA User's Manual

 admin ▼	<p>This option shows the logged-in user name and privilege. There are five kinds of privileges.</p> <p>User: Only valid commands are allowed.</p> <p>Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.</p> <p>Administrator: All BMC commands are allowed.</p> <p>No Access: Login access denied.</p> <p>OEM: All OEM commands are allowed</p>
--	--

- 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.

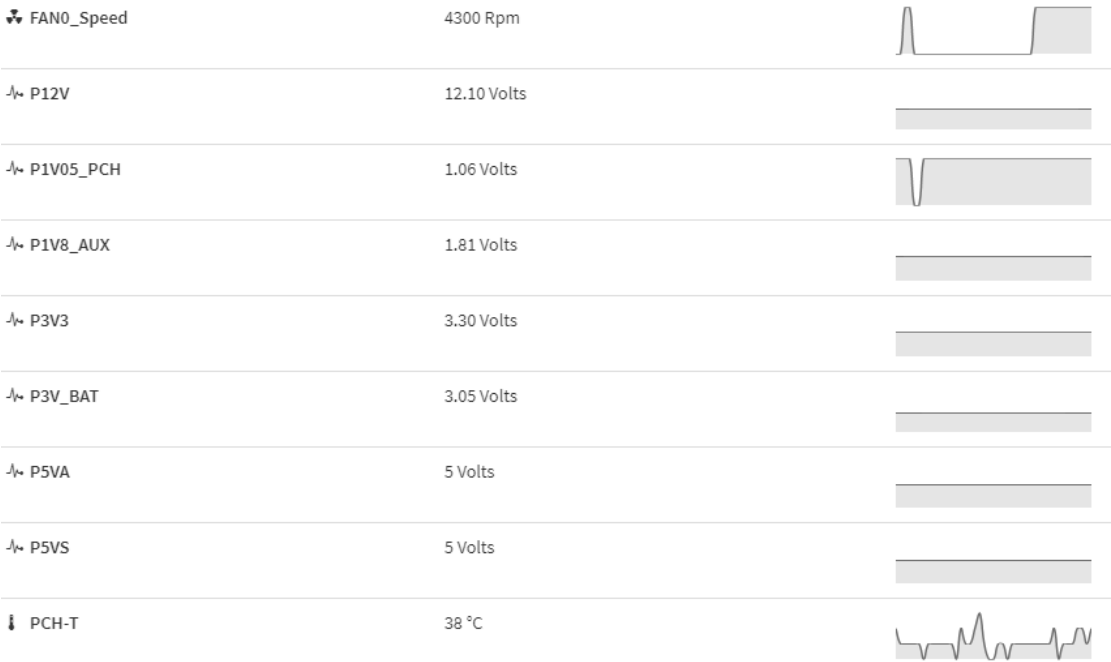
2.3 HOME>SENSOR

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	State
ACPI_State	S5/G2 'Soft Off'
BMC Watchdog	No state defined
BMC_Boot_Up	Device Enabled
CPLD_CRC_Error	No state defined
CPU_Mismatch	No state defined
CPU_Power_Fault	No state defined
CPU_Thermtrip	General Chassis Intrusion
CPU_VR_HOT	General Chassis Intrusion

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	

HPS-SRSU4A/HPS-SRSUTA User’s Manual

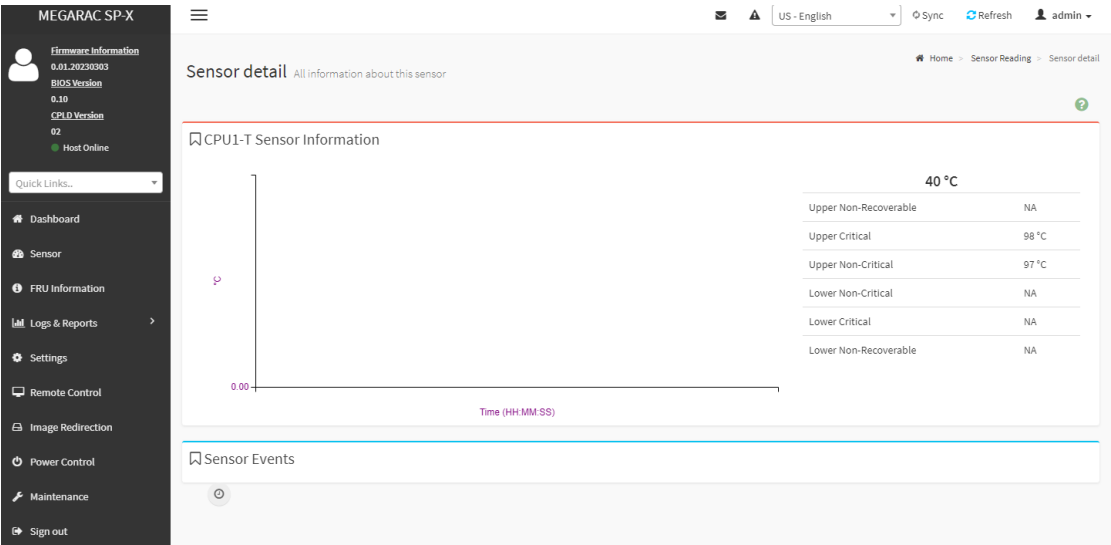


2.3.1 Home> Sensor Reading>Sensor detail

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 Field Replacable Units
Home > FRU

Available FRU Devices

FRU Device ID
0
FRU Device Name
MB_FRU

Chassis Information
Board Information
Product Information

Chassis Information Area Format Version: 0
Chassis Type:
Chassis Part Number:
Chassis Serial Number:
Chassis Extra:

Board Information Area Format Version: 1
Language: 25
Manufacture Date Time: Fri Dec 30 00:00:00 2022
Board Manufacturer: Avalue Technology
Board Product Name: HPM-SRSUA-A2
Board Serial Number: 0123456789012345678901234567890123456789
Board Part Number: 000000000001
FRU File ID: 1.0
Board Extra:

Product Information Area Format Version: 1
Language: 25
Product Manufacturer: Avalue Technology
Product Name: HPM-SRSUA-A02
Product Part Number: 0000000000000001
Product Version:
Product Serial Number: 1234567890
Asset Tag:
FRU File ID: 1.0
Product Extra:

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

Event Log All sensor event logs

Filter by Date Start Date End Date Filter by type All Events All Sensors

UTC Offset: GMT - 7:0
Clear Event Logs
Download Event Logs
Download Debug Logs

Event Log: 226 out of 226 event entries

May 2022

Event Logs Statistics

ID: 226 Unknown sensor of type OEM_RECORD logged a oem timestamped 0s hours ago
ID: 225 Unknown sensor of type os_boot logged a c boot completed 0s hours ago
ID: 224 BIOS sensor of type bios_post_progress logged a progress 0s hours ago
ID: 223 BIOS sensor of type bios_post_progress logged a progress 0s hours ago
ID: 222 BIOS sensor of type bios_post_progress logged a progress 0s hours ago
ID: 221 BIOS sensor of type bios_post_progress logged a progress 0s hours ago

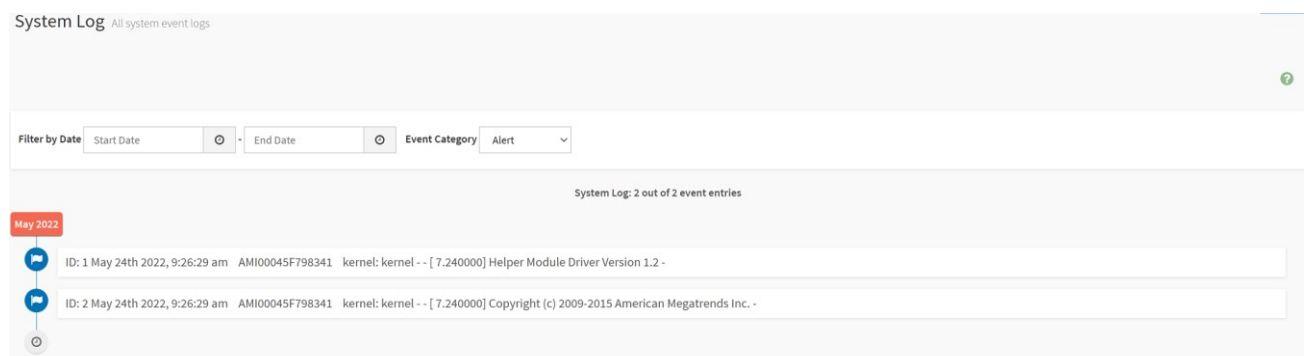
Item	Option	Description
Filter by Date	<ul style="list-style-type: none"> Start Date End Date 	Click field of "Start Date" or "End Date" to select the

HPS-SRSU4A/HPS-SRSUTA User's Manual

		duration of filter
Filter by type	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● All Sensors ● +V12S_CPU1 ● 	IPMI event logs can be filtered by this selected sensor.

2.5.2 Home> Logs & Reports >System Event Log

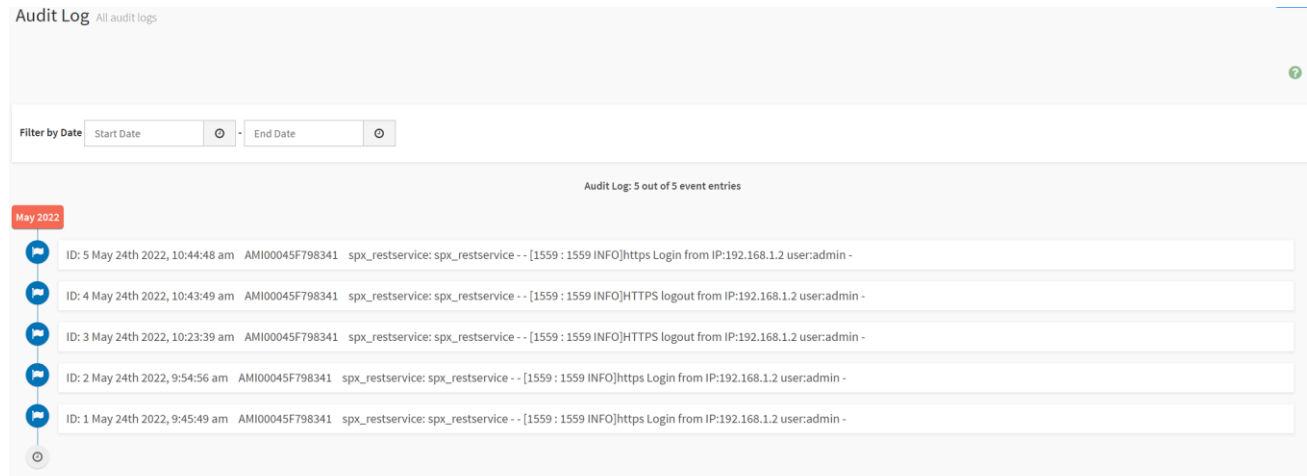
This page displays the system event logs and user can filter event logs by date/category



Item	Option	Description
Filter by Date	<ul style="list-style-type: none"> ● Start Date ● End Date 	Click field of “Start Date” or “End Date” to select the duration of filter
Event Category	<ul style="list-style-type: none"> ● 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

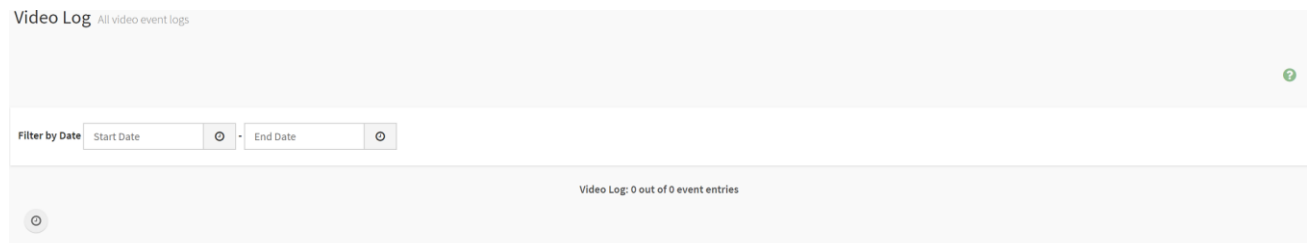
This page displays the audit logs and user can filter audit logs by date



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

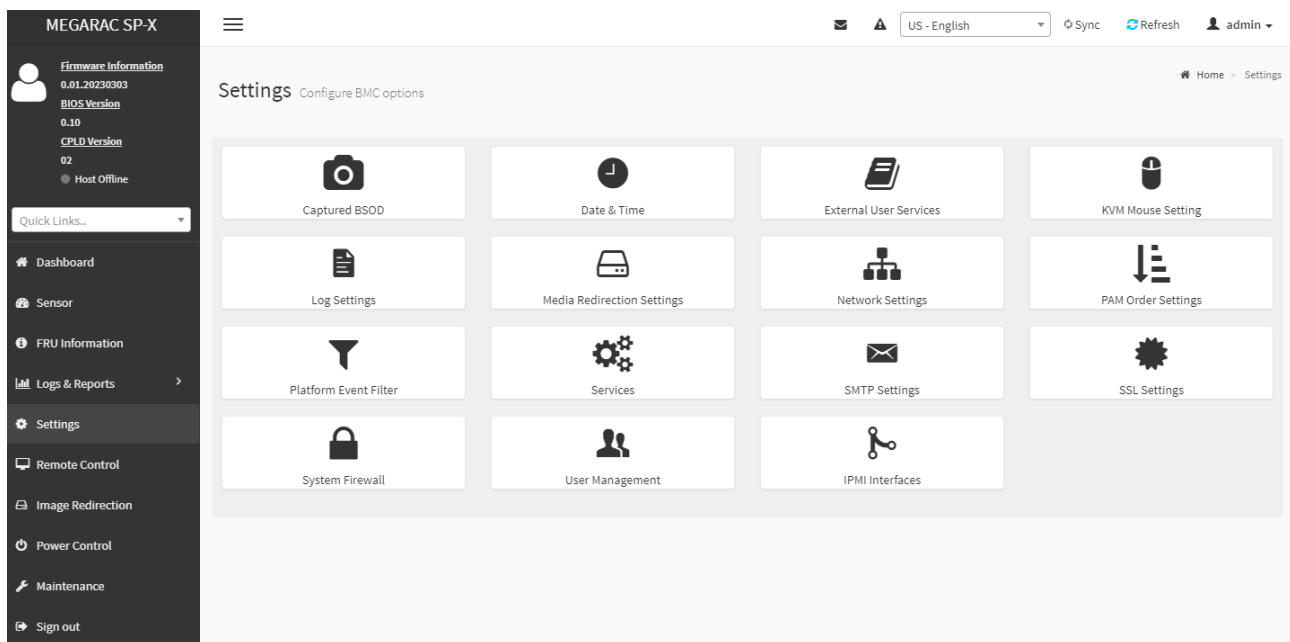
2.5.4 Home> Logs & Reports >Video Log

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



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

2.6 HOME> SETTINGS



IPMI Interfaces

This page is used to configure the IPMI Interfaces. To open IPMI interfaces page, click **Settings >**

IPMI Interfaces.

This page displays the following interfaces like **IPMI Over LAN** and **IPMI Over KCS**.

Procedure

- **IPMI Over LAN** - Check or uncheck the IPMI Over LAN interface which allows the user to perform IPMI communication over LAN.
- **IPMI Over KCS** - Check or uncheck the IPMI Over KCS interface which allows the user to perform IPMI communication over KCS.

Note: IPMI Communication will not be performed over LAN /KCS interface if it is disabled.

- **Save:** Click **Save** to save the configured interfaces.

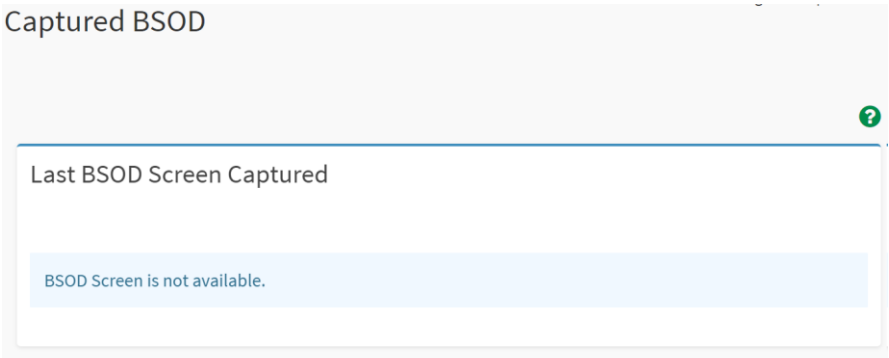
Item	Description
Captured BSOD	Captured snapshot of BSOD if the host system crashed
Date & Time	Set the date and time on the BMC
External User Services	Configure server settings to authenticate users
KVM Mouse Setting	Some settings of mouse emulation for KVM
Log Settings	Log settings for SEL log and Audit log
Media Redirection Settings	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.

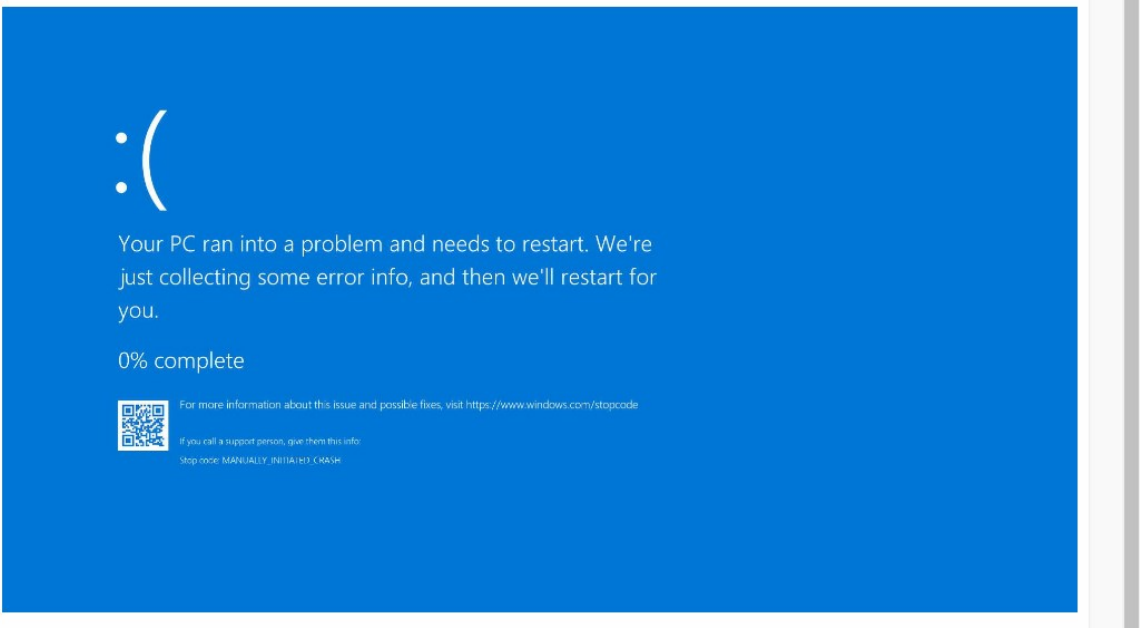
2.6.1 Home> Settings >Capture BSOD

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.

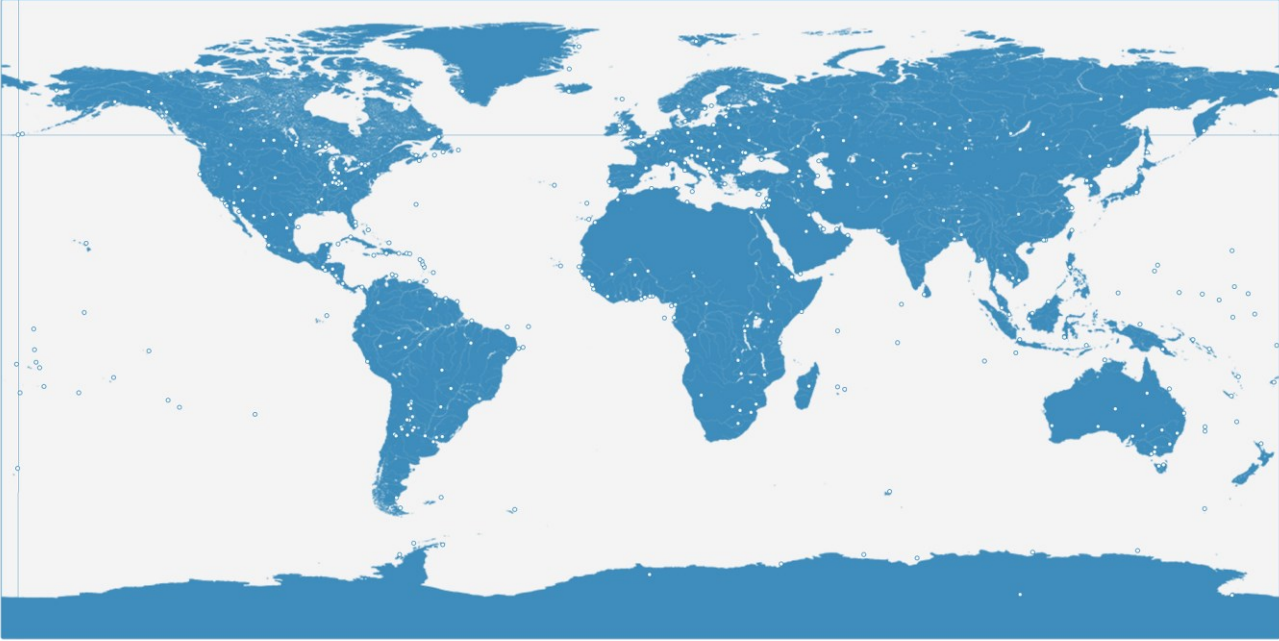


2.6.2 Home> Setting >Date & Time

Date & Time

Note:
If the time zone is selected from the group of Manual offset (GMT/ETC time zones), the interactive map selection feature will be disabled.
The new Time Zone settings will be reflected on the page only after being saved.

Configure Date & Time




Select Time Zone ▼

May 26, 2022 3:32:02 AM (GMT+12:45 CHAST) - Pacific/Chatham

☒ Automatic NTP Date & Time

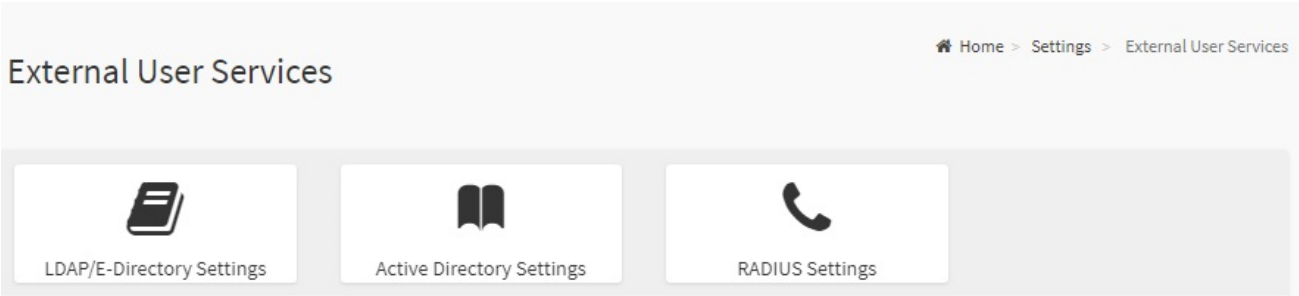
Primary NTP Server
pool.ntp.org

Secondary NTP Server
time.nist.gov

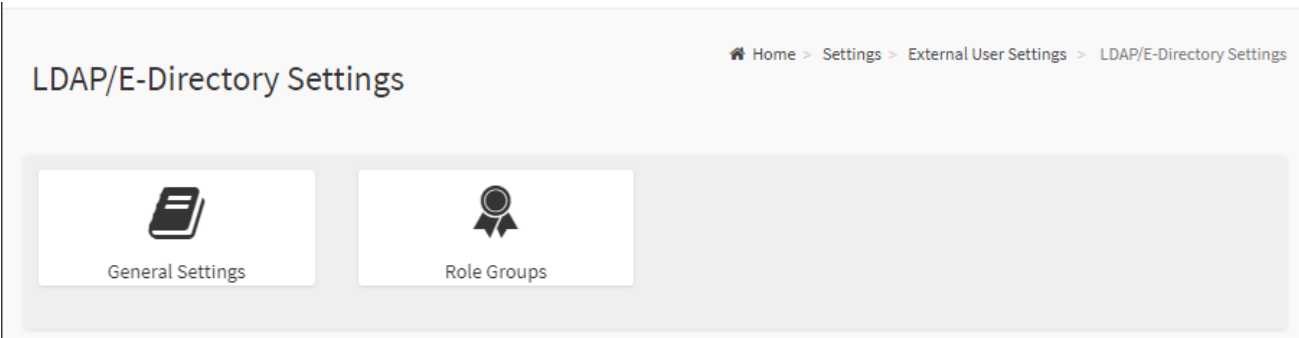
 Save

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

General LDAP Settings

☐ Enable LDAP/E-Directory Authentication

Encryption Type
☒ No Encryption ☐ SSL ☐ StartTLS

Common Name Type
☒ IP Address

Server Address


Port

Bind DN

Password




Search Base

Attribute of User Login

 Save

Item	Option	Description
Enabled LDAP/E-Directory Authentication	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked to enable LDAP/E-Directory settings. Note: During login prompt, use username to login as an LDAP Group member.
Encryption Type	<ul style="list-style-type: none"> ● No Encryption ● SSL ● StartTLS 	Encryption type for LDAP/E-Directory Note: Configure proper port number when SSL is enabled
Common Name Type	<ul style="list-style-type: none"> ● IP Address 	Select the Common Name Type as IP Address
Server Address	<input type="text"/>	Enter the IP address of LDAP server in the field
Port		Specify the LDAP Port in the field and range from 1

HPS-SRSU4A/HPS-SRSUTA User's Manual

		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: <ul style="list-style-type: none"> ♦ 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	<ul style="list-style-type: none"> ● cn ● uid 	Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.
Save		Click button to save the changes made

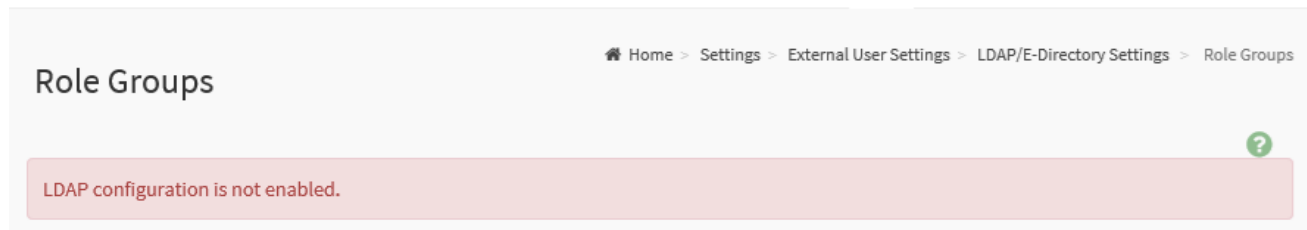
2.6.3.1.2 Home > Settings > External User Services > LDAP/E-Directory Settings > Role Groups

Note: Free/Unconfigured slots are denoted by the word 'None'

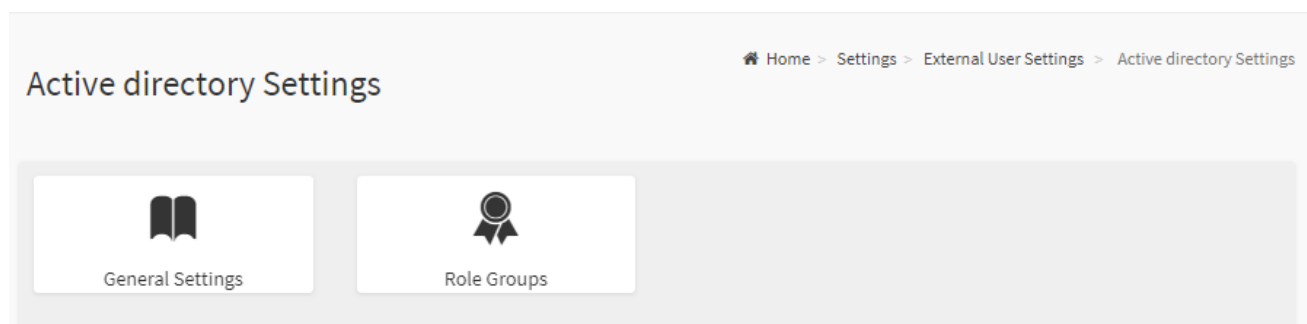
To add a Role Group, select a free box and click on it

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

General Active Directory Settings

?

☐ Enable Active Directory Authentication

Secret Username

Secret Password

User Domain Name


Domain Controller Server Address 1

Domain Controller Server Address 2

Domain Controller Server Address 3

Save

Item	Option	Description
Enable Active Directory Authentication	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Enable/Disable Active Directory Authentication
Secret Username	<div></div>	<div>Specify the Username of an administrator of the Active Directory Server.</div> <div><div><div></div></div><ul style="list-style-type: none">A string of 1 to 64 alpha-numeric charactersStart with an alphabetical characterCase-sensitiveSpecial characters and spaces are not allowed<div>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)</div></div>
Secret Password	<div></div>	<div>Specify the Password of the administrator.</div> <div><div><div></div></div><ul style="list-style-type: none">At least 6 characters longWhite space is not allowed</div>

		Note: This field will not allow more than 127 characters.
User Domain Name	<input type="text"/>	Specify the Domain Name for the user e.g. MyDomain.com
Domain Controller Server Address 1	<input type="text"/>	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	<input type="text"/>	
Domain Controller Server Address 3	<input type="text"/>	
Save		Click button to save the changes made

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

Note: Free/Unconfigured slots are denoted by the word 'None'

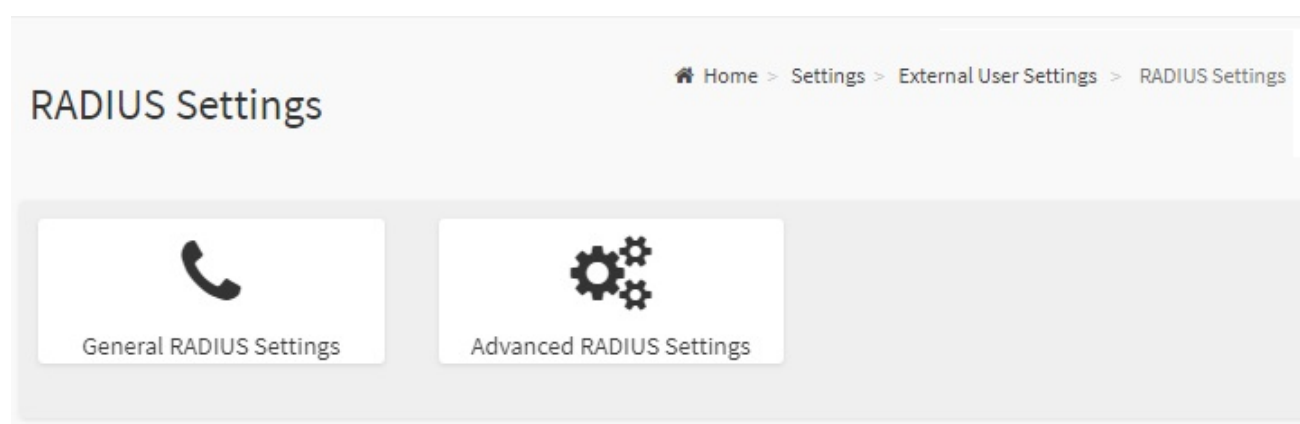
To add a Role Group ,click on a free box and configure its privilege and access.

To modify a Role Group ,click on it

To delete a Role Group, click on the X present at the right top corner 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

General RADIUS Settings

Enable RADIUS Authentication

Server Address

Port

1812

Secret

Enable KVM Access

Enable VMedia Access

Save

Item	Option	Description
Enable RADIUS Authentication	<div><div>✓</div><div></div></div>	Enable/Disable RADIUS Authentication
Server Address	<div></div>	The ip address of RADIUS server Note: IP Address (both IPv4 and IPv6 format) FQDN (Fully Qualified Domain Name) format
Port	<div></div>	The RADIUS Port number.(from 1 to 65535) Default Port is 1812
Secret	<div></div>	The Authentication Secret for RADIUS server <ul style="list-style-type: none">not allow more than 31 characters.must be at least 4 characters long.white space is not allowed.
Enable KVM Access	<div><div>✓</div><div></div></div>	Enable/Disable access to KVM for RADIUS authenticated users
Enable VMedia Access	<div><div>✓</div><div></div></div>	Enable/Disable access to VMedia for RADIUS authenticated users
Save	<div>Save</div>	Click button to save the changes made

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

Advanced RADIUS Settings

RADIUS Authorization ?

Radius configuration is not enabled.

Administrator

Operator

User


OEM Proprietary

No Access

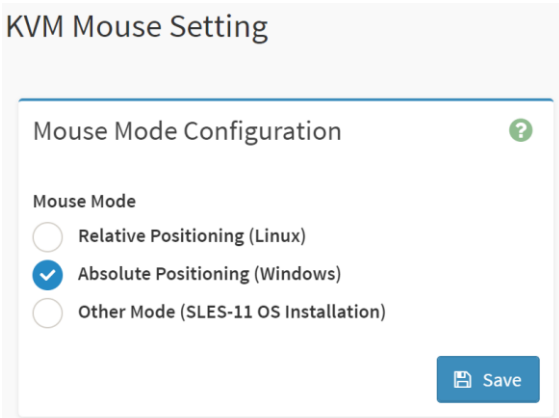
Save


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

HPS-SRSU4A/HPS-SRSUTA User’s Manual

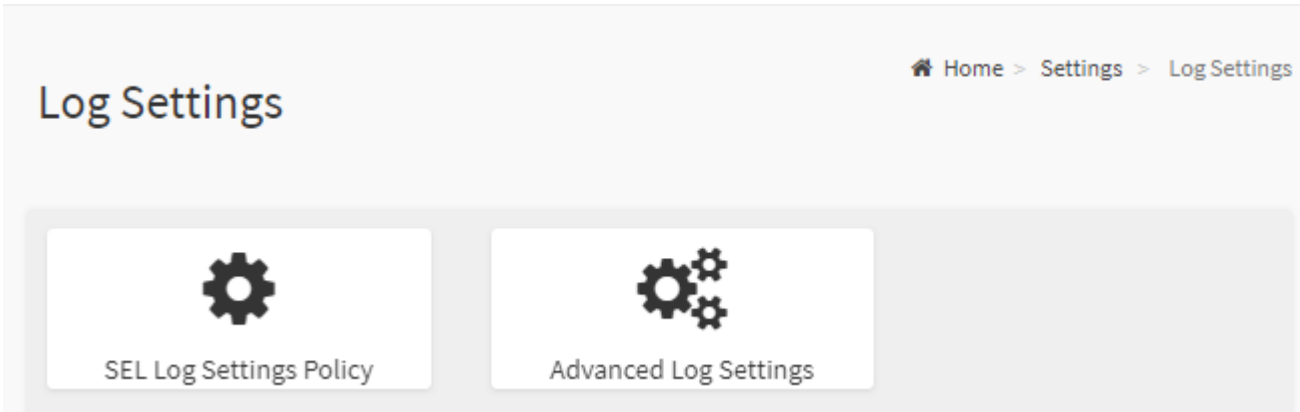
		<p>\$INCLUDE dictionary.adtest</p> <p>Add users:</p> <p>vim users</p> <p>(Add below content)</p> <p>"RadiusTest1" Cleartext-Password := "000000"</p> <p>Service-Type = Administrative-User,</p> <p>Auth-Type := System,</p> <p>ADTest-group := "H=4"</p> <p>NOTES: These fields will not allow more than 127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

2.6.4 Home>Settings>KVM Mouse Setting

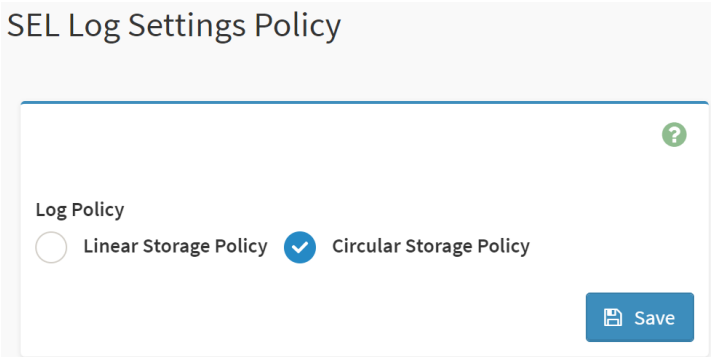



Item	Option	Description
Mouse Mode	<ul style="list-style-type: none">● Relative Positioning(Linux)● Absolute Positioning(Windows)● Other Mode (SLES-11 OS Installation)	Select in either of three methods to calculate mouse position.
Save		Click button to save the changes made

2.6.5 Home>Settings>Log Settings



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



Item	Option	Description
Log Policy	<ul style="list-style-type: none">Linear Storage PolicyCircular Storage Policy	This field is used to configure the log policy for the event log.
Save		Click button to save the changes made

2.6.5.2 Home> Settings>Log Settings>Advanced Log Settings

Advanced Log Settings

System Log

Local Log

Remote Log

Port Type

UDPTCP

File Size

50000

Rotate Count

0

Remote Log Server

Server IP or Hostname


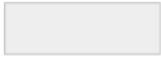

Remote Server Port

0

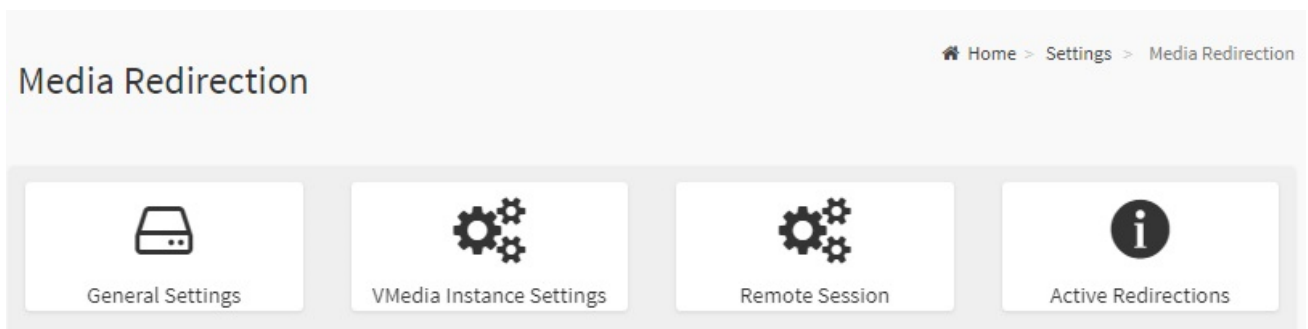
Enable Audit Log

Save

Item	Option	Description
System Log	<div><div></div><div></div></div>	Select Enable System Log to view all system events. Entries can be filtered base on their classification levels
Local Log	<div><div></div><div></div></div>	Select local log to save the logs locally (BMC)
Remote Log	<div><div></div><div></div></div>	Select remote log to save the logs in a remote machine.
Port Type	<div><div></div>UDP<div></div>TCP</div>	Port type is supported with the enable of Remote Log. User can select either UDP/TCP as per the requirement.
File Size	<div></div>	<div>If Local log is selected ,specify the size of the file in bytes.</div> <div><div></div>Size ranges from 3 to 65535</div> <div><div></div>Log files are rotated when the size is larger than the mentioned bytes , with regards for the last rotation time interval(1 minute).</div>
Rotate Count	<div></div>	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: <ul style="list-style-type: none"> ♦ 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	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select Enable Audit Log to view all audit events for this device.
Save		Click button to save the changes made

2.6.6 Home>Settings>Media Redirection



HPS-SRSU4A/HPS-SRSUTA User’s Manual

2.6.6.1 Home>Settings>Media Redirection>General Settings

General Settings

Remote Media Support

Mount CD/DVD

Server Address for CD/DVD Images

Server IP or Host name

Path in server

eg. /opt/bmc/nfs

Share Type for CD/DVD

nfs cifs

Domain Name

Username

Password

Same settings for Harddisk Images

Mount Harddisk

Server Address for Harddisk Images

Server IP or Host name

Path in server

eg. /opt/bmc/nfs

Share Type for Harddisk

nfs cifs

Domain Name

Username

Password

Retry Interval

15


Retry Count

3

Save

Item	Option	Description
Remote Media Support	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>To enable or disable Remote Media support ,check or uncheck this box.</p> <p>If it is selected ,then the following remote media types will be displayed</p> <ul style="list-style-type: none"> ♦ CD/DVD ♦ Hard disk <p>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.</p>
Mount CD/DVD	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>To enable or disable Mount CD/DVD support ,check or uncheck this box.</p>
Server Address for CD/DVD image	<input type="text"/>	<p>Address of the server where remote videos are to be stored. We support the following:</p> <ul style="list-style-type: none"> ♦ IPv4/IPv6 format. ♦ FQDN(Fully qualified domain name) format
Path in server	<input type="text"/>	<p>Path must be alpha-numeric and the following special characters are only allowed:</p> <p>'/' , '\', '-', '_', '.', ':'</p>
Share Type for CD/DVD	<ul style="list-style-type: none"> ● nfs ● cifs 	<p>Share Type of the remote media server : either NFS or Samba(CIFS).</p>
Domain Name	<input type="text"/>	<p>If Share Type is Samba(CIFS) , then enter user credentials to authenticate the server.</p> <p>Note: Domain Name field is optional.</p>
Username	<input type="text"/>	
Password	<input type="text"/>	
Same settings for Harddisk images	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>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.</p>
Mount Harddisk	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>To enable or disable Mount Harddisk support ,check or uncheck this box.</p>
Server Address for Harddisk images	<input type="text"/>	<p>Address of the server where remote videos are to be stored.</p> <p>We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format</p>
Path in server	<input type="text"/>	<p>Path must be alpha-numeric and the following special characters are only allowed:</p> <p>'/' , '\', '-', '_', '.', ':'</p>
Share Type for Harddisk	<ul style="list-style-type: none"> ● nfs ● cifs 	<p>Share Type of the remote media server : either NFS or Samba(CIFS).</p>

HPS-SRSU4A/HPS-SRSUTA User's Manual

Domain Name	<input type="text"/>	If Share Type is Samba(CIFS), then enter user credentials to authenticate the server. Note : Domain Name field is optional.
Username	<input type="text"/>	
Password	<input type="password"/>	
Retry Interval	<input type="text"/>	Specify the Retry Interval and range should be from 15 to 30.Default value will be 15
Retry Count	<input type="text"/>	Specify the Retry Count and range should be from 3 to 6. Default value will be 3
System Log	<input checked="" type="checkbox"/> <input type="checkbox"/>	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

2.6.6.2 Home>Settings>Media Redirection>VMedia Instance Settings

VMedia Instance Settings

CD/DVD device instances

1

Hard disk instances

1


Remote KVM CD/DVD device instances

1


Remote KVM Hard disk instances

1

☒ Power Save Mode

 Save

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	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Power Save Mode in BMC
Save		Click button to save the changes made

2.6.6.3 Home>Settings>Media Redirection>Remote Session

Remote Session

?

☒ KVM Single Port Application

Keyboard Language

Auto Detect (AD) ▾

Retry Count


3


Retry Time Interval(Seconds)

10

☒ Server Monitor OFF Feature Status

☐ Automatically OFF Server Monitor, When KVM Launches



Item	Option	Description
KVM Single Port Application	<input checked="" type="checkbox"/> <input type="checkbox"/>	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	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable the Server Monitor OFF feature
Automatically OFF Server Monitor, When KVM Launches	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Automatically OFF Server Monitor when KVM is launched
Save		Click button to save the changes made

2.6.6.4 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.

Active Redirections

Home > Settings > Media Redirection > Active Redirections

No Media has been redirected.

Media Type

Media Instance

Client Type

Image Name

Redirection Status

Client IP

2.6.7 Home>Settings>Network Settings

Network Settings

Home > Settings > Network Settings

Network IP Settings

Network Link Configuration

DNS Configuration

Sideband Interface (NC-SI)

2.6.7.1 Home>Settings>Network Settings>Network IP Settings

Network IP Settings

☒ Enable LAN

LAN Interface

eth0

MAC Address

00:04:5F:79:83:41

☒ Enable IPv4

☐ Enable IPv4 DHCP

IPv4 Address

192.168.1.6

IPv4 Subnet

255.255.255.0

IPv4 Gateway

0.0.0.0

☒ Enable IPv6

☒ Enable IPv6 DHCP

IPv6 Index

0

IPv6 Address

::

Subnet Prefix Length

0

☐ Enable VLAN

VLAN ID

0

VLAN Priority

0

Save

Item	Option	Description
Enabled IPv4	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Enable/Disabled IP of BMC lan is ipv4 address format
Enabled IPv4 DHCP	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	IPv4 is assigned by DHCP server or manual settings
IPv4 Address	<div><input type="text" value="192.168.1.6"/></div>	Fill out specific the static IPv4 address for lan of BMC

HPS-SRSU4A/HPS-SRSUTA User's Manual 43

HPS-SRSU4A/HPS-SRSUTA User's Manual

IPv4 Subnet Mask	<input type="text"/>	Fill out specific the static IPv4 Subnet Mask for lan of BMC
IPv4 Default Gateway	<input type="text"/>	Fill out specific the static IPv4 Default Gateway for lan of BMC
Enabled IPv6	<input checked="" type="checkbox"/> <input type="checkbox"/>	IP of BMC lan is ipv6 address format
Enabled IPV6 DHCP	<input checked="" type="checkbox"/> <input type="checkbox"/>	IPv6 is assigned by DHCP server or manual settings
IPv6 Index	<input type="text"/>	To specify a static IPv6 Index to be configured to the device
IPv6 Address	<input type="text"/>	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	<input checked="" type="checkbox"/> <input type="checkbox"/>	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	<input type="button" value="Save"/>	Click button to save the changes made

2.6.7.2 Home>Settings>Network Settings>Network Link Configuration

Network Link Configuration

?

LAN Interface

eth0

☒ Auto Negotiation

Link Speed


1000 Mbps


Duplex Mode

FULL Duplex

NCSI Interface

Enabled

 Save

Item	Option	Description
LAN Interface	eth0	Select the network interface for which the Link speed and duplex mode are to be configured.
Auto Negotiation	<input checked="" type="checkbox"/> <input type="checkbox"/>	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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Full duplex ● Half duplex 	Select any one of the following duplex modes. Half duplex Full duplex
NCSI Interface		NCSI interface Enable/Disable
Save	 Save	Click button to save the changes made

HPS-SRSU4A/HPS-SRSUTA User’s Manual

2.6.7.3 Home>Settings>Network Settings>DNS Configuration

DNS Configuration

☒ DNS Enabled

☐ mDNS Enabled

Host Name Setting

☒ Automatic ☐ Manual

Host Name

AMI00045F798341

BMC Registration Settings

BMC Interface:

eth0

☒ Register BMC

Registration method:

☒ Nupdate ☐ DHCP Client FQDN ☐ Hostname

☐ Both

Eth0 TSIG Configuration

☐ TSIG Authentication Enabled

Current TSIG Private File Info

Not Available

New TSIG Private File

...

Eth1 TSIG Configuration

☐ TSIG Authentication Enabled

Current TSIG Private File Info

...

Domain Setting

☐ Automatic ☒ Manual

Domain Name

Domain Name Server Setting

☐ Automatic ☒ Manual

DNS Server 1

::

DNS Server 2

::

DNS Server 3

::

Save

Item	Option	Description
DNS Enabled	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Check this box to enable all DNS services
mDNS Enabled	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Check this box to enable Multicast DNS
Host Name	<div><input checked="" type="radio"/> Automatic</div>	Select whether the host name will be configured manually or

Setting	<ul style="list-style-type: none"> ● Manual 	automatically.
Host Name	<input type="text"/>	<p>If Automatic is selected ,the this field automatically display the hostname.</p> <p>Otherwise,please enter the desired hostname for the device.</p>
Register BMC	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable Register BMC
Registration method	<ul style="list-style-type: none"> ● Nsupdate ● DHCP client FQDN ● Hostname 	<p>Nsupdate-Register with the DNS server using the nsupdate application</p> <p>DHCP client FQDN-Register with the DNS server using DHCP option 81</p> <p>Hostname-Register with the DNS server using DHCP option 12</p> <p>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.</p>
Both	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to modify TSIG authentication for both interfaces.
TSIG Authentication Enabled(Eth0)	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable TSIG Authentication – if registering DNS via nsupdate only.
New TSIG Private File(Eth0)	<input type="text" value="Browse..."/>	Browse for a new TSIG private file to be uploaded to the BMC
TSIG Authentication Enabled(Eth1)	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable TSIG authentication – if registering DNS via nsupdate only
New TSIG Private File(Eth1)	<input type="text" value="Browse..."/>	Browse for a new TSIG private file to be uploaded to the BMC.
Domain Setting	<ul style="list-style-type: none"> ● Automatic ● Manual 	Select whether the domain interface will be configured manually or automatically.
Domain Name	<input type="text"/>	Displays the domain name of the device, or ,if 'Manual' was selected, specify the domain name of the device.
Domain Name Sever Setting	<ul style="list-style-type: none"> ● Automatic ● Manual 	Select whether the DNS interface will be configured manually or automatically.
DNS Server 1	<input type="text"/>	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	<input type="text"/>	

HPS-SRSU4A/HPS-SRSUTA User’s Manual

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

2.6.7.4 Home>Settings>Network Settings>Sideband Interface

Sideband Interface (NC-SI)

?

NCSI Mode

Auto Failover Mode Manual Switch Mode

NCSI Interface

eth0

Package ID

0 (active)

Channel Number

0 (package 0)(active)

Save

Item	Option	Description
NCSI Mode	<ul style="list-style-type: none">Auto Failover ModeManual Switch Mode	Select the NCSI mode
NCSI Interface	eth0	Choose the interface name for which to configure NCSI settings
Package ID	<div></div>	Choose the package ID to be configured for the selected interface.
Channel Number	<div></div>	Choose the channel number to be configured for the selected interface.
Save	<div>Save</div>	Click button to save the changes made

2.6.8 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.

PAM Order

PAM Authentication Order

IPMI
LDAP
ACTIVE DIRECTORY
RADIUS

Save

2.6.9 Home>Settings>Platform Event Filter

Platform Event Filters

Home > Settings > Platform Event Filters

Event Filters

Alert Policies

LAN Destinations

2.6.9.1 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

Event Filters

Home > Settings > Platform Event Filters > Event Filters

?

☐ All

☒ Configured

☐ UnConfigured

<div><div></div><div>PEF ID: 1 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (1) & none</div><div></div></div>	<div><div></div><div>PEF ID: 2 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (2) & none</div><div></div></div>	<div><div></div><div>PEF ID: 3 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (3) & none</div><div></div></div>	<div><div></div><div>PEF ID: 4 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (4) & none</div><div></div></div>
<div><div></div><div>PEF ID: 5 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (5) & none</div><div></div></div>	<div><div></div><div>PEF ID: 6 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (6) & none</div><div></div></div>	<div><div></div><div>PEF ID: 7 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (7) & none</div><div></div></div>	<div><div></div><div>PEF ID: 8 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (8) & none</div><div></div></div>
<div><div></div><div>PEF ID: 9 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (9) & none</div><div></div></div>	<div><div></div><div>PEF ID: 10 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (10) & none</div><div></div></div>	<div><div></div><div>PEF ID: 11 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (11) & none</div><div></div></div>	<div><div></div><div>PEF ID: 12 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (12) & none</div><div></div></div>
<div><div></div><div>PEF ID: 13 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (13) & none</div><div></div></div>	<div><div></div><div>PEF ID: 14 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (14) & none</div><div></div></div>	<div><div></div><div>PEF ID: 15 <i>(Enabled)</i> when All Sensors switches to any severity run Alert (15) & none</div><div></div></div>	

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

Event Filter Configuration

?

☒ Enable this filter

Event severity to trigger
 Any severity

☒ Event Filter Action Alert

Power Action
 None

Alert Policy Group Number
 1

☒ Raw Data

Generator ID 1
 255

Generator ID 2
 255

Generator Type
☐ Slave ☐ Software

Slave Address/Software ID

Channel Number
 0

IPMB Device LUN
 0

Sensor type
 All Sensors

Sensor name
 All Sensors

Event Options
 All Events

Event trigger
 255

Event Data 1 AND Mask
 0

Event Data 1 Compare 1
 0

Event Data 1 Compare 2
 0

Event Data 2 AND Mask
 0

Event Data 2 Compare 1
 0

Event Data 2 Compare 2
 0

Event Data 3 AND Mask
 0

Event Data 3 Compare 1
 0


Event Data 3 Compare 2
 0

Delete

Save

HPS-SRSU4A/HPS-SRSUTA User's Manual

Item	Option	Description
Enable this filter	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check the option 'Enable' to enable the PEF settings
Event severity to trigger	<ul style="list-style-type: none"> 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	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable PEF Alert action.
Power Action	<ul style="list-style-type: none"> 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	<input checked="" type="checkbox"/> <input type="checkbox"/>	Enable this option to enter the Generator ID with raw data.
Generator ID 1	<input type="text"/>	Enter the raw generator ID1 data value.
Generator ID 2	<input type="text"/>	Enter the raw generator ID2 data value. Note: In the RAW data field, prefix the value with '0x' to specify hexadecimal value.
Generator Type	<ul style="list-style-type: none"> Slave Software 	Choose the event generator as Slave Address – if event is generated from IPMB
Slave Address /Software ID	<input type="text"/>	Choose System Software ID – if event is generated from system software
Channel Number	<input type="text"/>	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	<input type="text"/>	Choose the corresponding IPMB Device LUN if event is generated by IPMB

Sensor type	<ul style="list-style-type: none"> ● All Sensors ● Voltage ● Temperature ● Fan ● Processor 	Select the type of sensor that will trigger the event filter action.
Sensor Name	<ul style="list-style-type: none"> ● All Sensors ● +V12S_CPU1 ● +V5A ● 	Choose the particular sensor from the sensor list.
Event Options	<ul style="list-style-type: none"> ● 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

2.6.9.2 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.

Alert Policies

Home > Settings > Platform Event Filters > Alert Policies

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

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

Alert Policies

Alert Policies

Policy Group Number

1

☐

Enable this alert

Policy Action

Always send alert to this destination

LAN Channel

1

Destination Selector

☐

Event Specific Alert String

Alert String Key

Delete

Save

Item	Option	Description
Policy Group Number	1-15	Choose a policy number that was configured in the Event filter table
Enable this alert	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check the option 'Enable' to enable the policy settings.
Policy Action	<ul style="list-style-type: none"> ● Always send alert to this destination ● If previous successful ,skip this and continue(if configured) ● If previous successful ,switch to another channel (if configured) ● If previous successful ,switch to methods(if configured) 	<p>Choose any one of the Policy set values from the list.</p> <p>0- Always send alert to this destination</p> <p>1- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.</p> <p>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.</p> <p>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.</p> <p>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.</p>
LAN Channel	1	Choose a LAN channel for the policy
Destination Selector	1-15	<p>Choose a destination from the configured destination list.</p> <p>Note: LAN Destinations have to be configured – under Configuration->PEF->LAN Destination</p>
Event Specific Alert String	<input checked="" type="checkbox"/> <input type="checkbox"/>	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.

HPS-SRSU4A/HPS-SRSUTA User’s Manual

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

2.6.9.3 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.

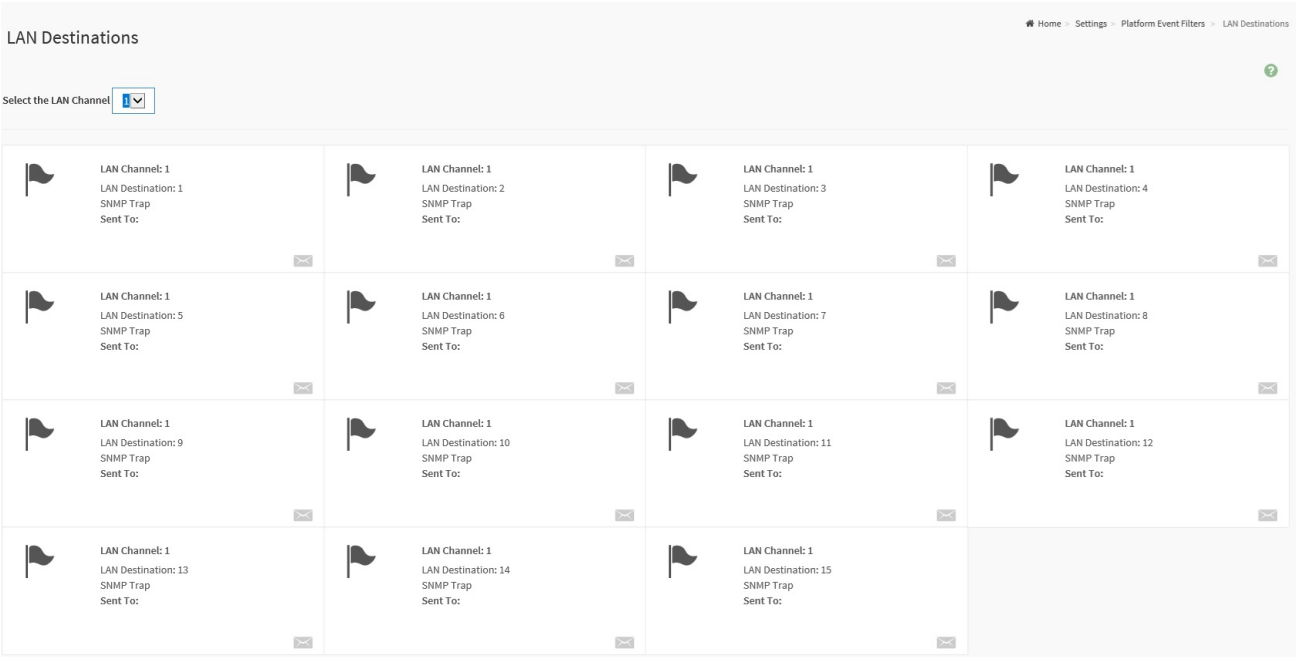
Click x icon to delete an entry from the list.

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

LAN Destination Configuration

?

LAN Channel

1

LAN Destination

1

Destination Type

☒ SNMP Trap
 ☐ E-Mail

SNMP Destination Address

BMC Username

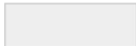

Email Subject

Email Message

Save

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	<ul style="list-style-type: none"> 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

HPS-SRSU4A/HPS-SRSUTA User's Manual


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












2.6.10 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.

Services 						
Service ↕	Status ↕	Interfaces ↕	Secure Port ↕	Timeout ↕	Maximum Sessions ↕	
web	Active	both	443	1800	20	 
kvm	Active	both	443	1800	4	 
cd-media	Active	both	443	N/A	1	 
hd-media	Active	both	443	N/A	1	 
ssh	Active	NA	22	600	N/A	 

Home>Settings>Services> Service Configuration

Service Configuration Home > Settings > Services > Service Configuration

?

Service Name

web

☒ Active

Interface Name

both

Secure port

443

Timeout

1800

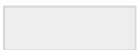

Maximum Sessions

20

Save


Item	Option	Description
Service Name	<input type="text"/>	Displays service name of the selected slot (read only)
Active	<input checked="" type="checkbox"/> <input type="checkbox"/>	Current State Displays the current status of the service, either active or inactive. Check this box to activate the service.
Interface Name	<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Status of interface can be checked/enabled,under Configuration->Network->LAN Settings. Media and KVM interfaces are readonly when single port is enabled
Secure port	<input type="text"/>	Used to configure secure port numbers for the services. <ul style="list-style-type: none"> 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

HPS-SRSU4A/HPS-SRSUTA User's Manual

		<ul style="list-style-type: none"> Port value ranges form 1 to 65535 <p>Note : Port 80 is blocked for TCP/UDP protocols</p>
Timeout		<p>Where supported , user can configure the session timeout value.</p> <ul style="list-style-type: none"> 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		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

Service Sessions

 Home >
  Settings >
  Services >
 Service Sessions



Active Session - Web

Session ID	Session Type	User ID	User Name	Client IP	Privilege	
1*	Web HTTPS	2	admin	192.168.1.2	Administrator	

2.6.11 Home>Settings> SMTP Settings

SMTP Settings

?

LAN Interface

eth0

Sender Email ID

☒ Primary SMTP Support

Primary Server Name

Primary Server IP

Primary SMTP port

25

Primary Secure SMTP port

465

☐ Primary SMTP Authentication

Primary Username

Primary Password

☐ Primary SMTP SSLTLS Enable

☐ Primary SMTP STARTTLS Enable


☐ Secondary SMTP Support

Save

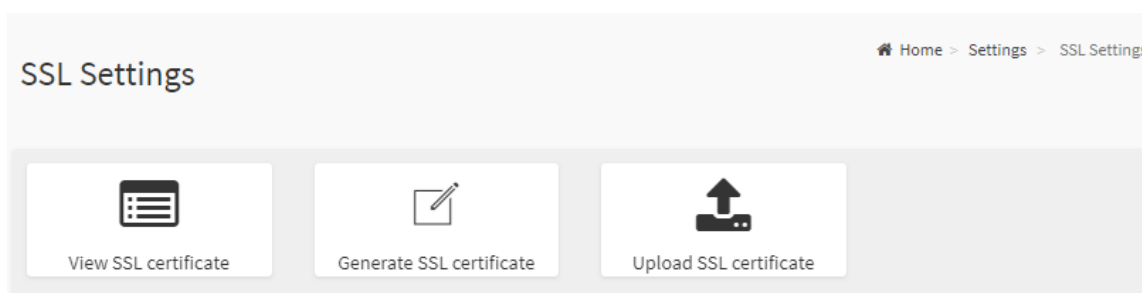
Item	Option	Description
Lan interface	eth0	Select the Lan interface to be configured
Sender Email ID	<div></div>	Enter a valid 'Sender Email ID' on the SMTP Server. Maximum allowed size for Email ID is 64 bytes,which includes username and domain name.
Primary SMTP	<div><input checked="" type="checkbox"/></div>	Check this option to enable SMTP support for the BMC

HPS-SRSU4A/HPS-SRSUTA User's Manual

Support	<input type="checkbox"/>	
Primary Server Name	<input type="text"/>	<p>Enter the 'Machine Name' of the SMTP Server. This field is for information Purpose Only.</p> <p>Machine Name is a string of 25 alpha-numeric characters maximum.</p> <p>Spaces and special characters are not allowed</p>
Primary Server IP	<input type="text"/>	<p>Enter the Server Address for the SMTP server</p> <p>Server address will support the following</p> <ul style="list-style-type: none"> ♦ IPv4/IPv6 address format ♦ Host name format
Primary SMTP port	<input type="text"/>	<p>Specify the SMTP port</p> <p>Default port is 25</p> <p>Port value ranges from 1 to 65535</p>
Primary Secure SMTP port	<input type="text"/>	<p>Specify the SMTP secure port</p> <p>Default port is 465</p> <p>Port value ranges from 1 to 65535</p>
Primary SMTP Authentication	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Check the option 'Enable' to enable SMTP Authentication.</p> <p>Note: Support SMTP Server Authentication Types are: CRAM-MD5.</p> <p>LOGIN</p> <p>PLAIN</p> <p>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'</p>
Primary Username	<input type="text"/>	<p>Enter user name required to access SMTP Accounts.</p> <p>User Name can be of length 4 to 64 alpha-numeric characters, '.', '@', '-', '_',</p> <p>It must start with an alphabetical character</p> <p>Other special characters are not allowed</p>
Primary Password	<input type="text"/>	<p>Enter the password for the SMTP User Account.</p> <p>Password must be at least 4 characters long.</p> <p>White space is not allowed</p> <p>Note: This field will not allow more than 64 characters.</p>
Primary SMTP SSLTLS Enable	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Check the option to enable the SMTP SSLTLS protocol</p>
Primary SMTP STARTTLS Enable	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Check the option to enable the SMTP STARTTLS protocol</p>

Secondary SMTP Support	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Secondary SMTP support for the BMC.
Save	 Save	Click button to save the changes made

2.6.12 Home>Settings>SSL Settings



2.6.12.1 Home>Settings>SSL Settings> View SSL Certificate

This page displays the Current Certificate Information.

View SSL Certificate

Current Certificate Information

Certificate Version

3

Serial Number

61E7D5C8AEA9A49246ED79AD16A469FA

Signature Algorithm

sha256WithRSAEncryption

Public Key

(2048 bit)

Issuer Common Name (CN)

AzurionPC

Issuer Organization (O)

Issuer Organization Unit (OU)

Issuer City or Locality (L)

Issuer State or Province (ST)

Issuer Country (C)

Issuer Email Address

Valid From

Sep 28 15:31:28 2020 GMT

Valid Till

Sep 28 15:41:29 2070 GMT

Issued to Common Name (CN)

AzurionPC

Issued to Organization (O)

Issued to Organization Unit (OU)

Issued to City or Locality (L)

Issued to State or Province (ST)

Issued to Country (C)

Issued to Email Address

2.6.12.2 Home>Settings>SSL Settings>Generate SSL Certificate

Generate SSL Certificate

?

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for

in days


Key Length

2048 bits

Save

Item	Option	Description
Common Name(CN)		Common name for which the certificate is to be generated. <ul style="list-style-type: none"> Maximum of 64 alpha-numeric characters Character '#' and '\$' are not allowed.
Organizaion(O)		Name of the organization for which certificate is to be generated. <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Maximum of 64 alpha-numeric characters Character '#' and '\$' are not allowed.
City or Locality(L)		City or Locality. <ul style="list-style-type: none"> Maximum of 64 alpha-numeric characters

HPS-SRSU4A/HPS-SRSUTA User's Manual

		<ul style="list-style-type: none"> Character '#' and '\$' are not allowed.
State or Province(ST)	<input type="text"/>	State or Province. <ul style="list-style-type: none"> Maximum of 64 alpha-numeric characters Character '#' and '\$' are not allowed.
Country(C)	<input type="text"/>	Country code. <ul style="list-style-type: none"> Only two characters are allowed Special characters are not allowed
Email Address	<input type="text"/>	Email addresss of organization
Valid for	<input type="text"/>	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		Click button to save the changes made

2.6.12.3 Home>Settings>SSL Settings>Upload SSL Certificate


Upload SSL Certificate

?

Current Certificate

Mon Mar 28 13:45:48 2022


New Certificate




Current Private Key



Mon Mar 28 13:45:48 2022

New Private Key

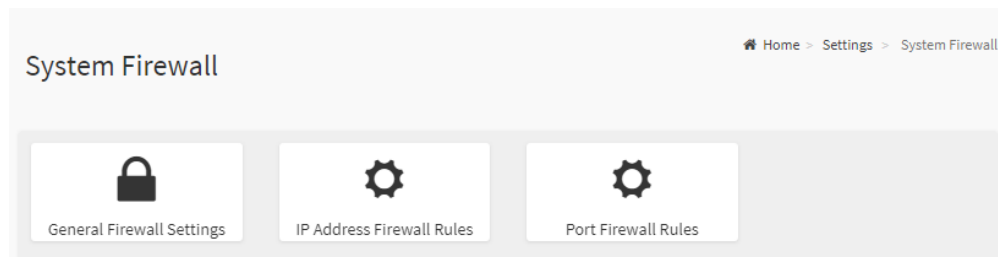




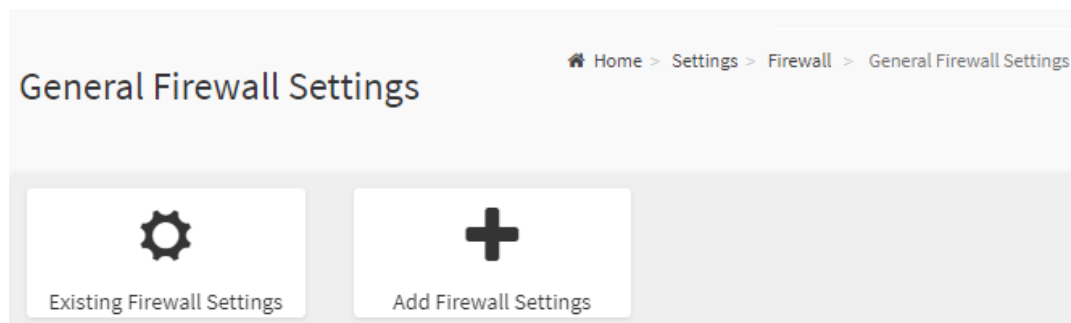
Item	Option	Description
Current Certificate		The information of the Current Certificate and date/time of its upload will be displayed(read-only)
New Certificate	<input type="text"/>	Browse and navigate to the new certificate file. Certificate file should be of pem type.
Current Private Key		Information 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

2.6.13 Home>Settings>System firewall

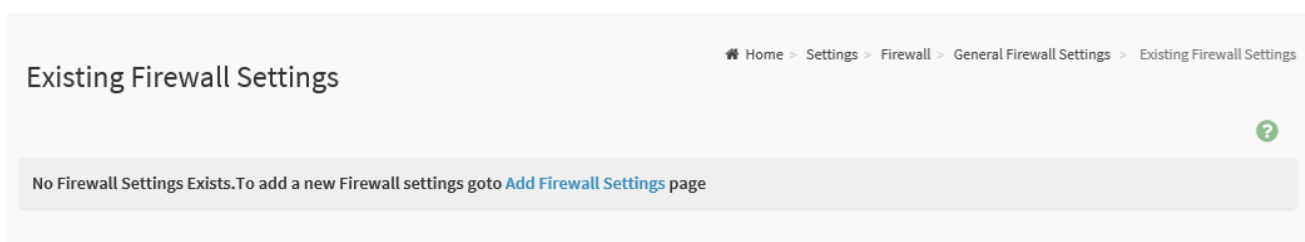


2.6.13.1 Home>Settings> Firewall >General Firewall Settings



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

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



2.6.13.3 Home>Settings> Firewall >General Firewall Setting >Add Firewall Settings

Add Firewall Settings

?

Block All

IPv4

☐ Flush All

☐ Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

YYYY/MM/DD

End Time

Save

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

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

Add IP Rule

?

IP Single (or) Range Start

IP Range End

optional

☐
Enable Timeout

Start Date

YYYY/MM/DD

Start Time

End Date

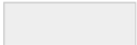
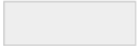

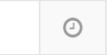
YYYY/MM/DD

End Time

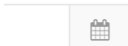
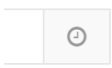

Rule

Allow

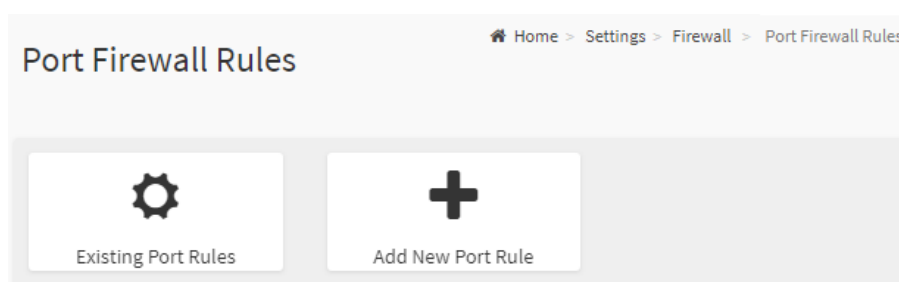
Save

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	<input checked="" type="checkbox"/> <input type="checkbox"/>	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

HPS-SRSU4A/HPS-SRSUTA User's Manual

End Date		The firewall rule will expire on this date
End Time		The firewall rule will expire at this time
Rule	<ul style="list-style-type: none">● Allow● Block	This field is used for allow or block this rule.
Save		Click button to save the changes made

2.6.13.5 Home>Settings>System Firewall >Port Firewall Rules



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

This page display the list of existing IP firewall rules



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

Add Port Rule

?

Port Single (or) Range Start

Port Range End

Protocol

TCP
▼

Network Type

IPv4
▼

☐ **Enable Timeout**

Start Date

YYYY/MM/DD
📅

Start Time

🕒

End Date

YYYY/MM/DD
📅

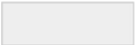
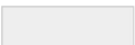
End Time

🕒






Rule

Allow
▼

Save

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	<ul style="list-style-type: none"> ● TCP ● UDP ● Both 	Select which protocol to support.
Network Type	<ul style="list-style-type: none"> ● IPv4 	Select which network type to support.

HPS-SRSU4A/HPS-SRSUTA User's Manual

	<ul style="list-style-type: none"> ● IPv6 ● Both 	
Enable Timeout	<input checked="" type="checkbox"/> <input type="checkbox"/>	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	<ul style="list-style-type: none"> ● Allow ● Block 	This field is used for allow or block this rule.
Save		Click button to save the changes made

2.6.14 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.

User Management

Home > Settings > User Management

Channel 1

Channel 1

1 anonymous

(Disabled)

Administrator

KVM

VMedia

Channel 1

2 admin (Active)

Administrator

KVM

VMedia

Channel 1

3 (Disabled)

Channel 1

4 (Disabled)

Channel 1

5 (Disabled)

Channel 1

6 (Disabled)

Channel 1

7 (Disabled)

Channel 1

8 (Disabled)

Channel 1

9 (Disabled)

Channel 1

10 (Disabled)

Item	Option	Description
Channel	<div><div></div>1</div> <div><div></div>2</div> <div><div></div>8</div>	

2.6.14.1 Home>Settings>User management> User Management Configuration

User Management Configuration

Username

anonymous

☐ Change Password

Password Size

16 bytes

Password

Confirm Password

Enable User Access

☒ Channel 1

☒ Channel 2

☒ Channel 8

Privilege(Channel 1)

Administrator

Privilege(Channel 2)

Administrator

Privilege(Channel 8)

Administrator

☒ KVM Access

☒ VMedia Access

☐ SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

Email Format

AMI-Format

Email ID

Existing SSH Key

Not Available

Upload SSH Key



Delete

Save

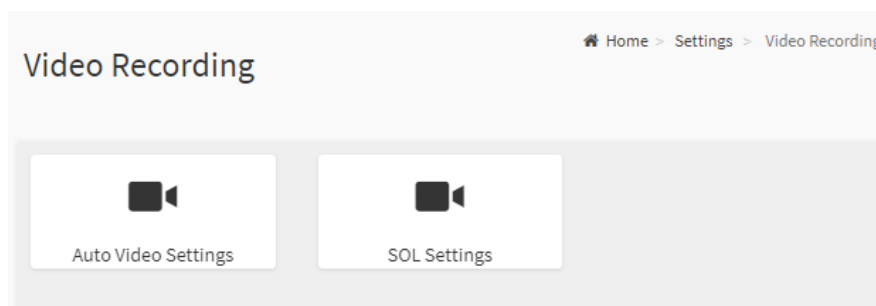
Item	Option	Description
Username	<div></div>	<div>Enter the name of the new user.</div> <div><div>♦ String of 1 to 16 alpha-numeric characters.</div><div>♦ Start with an alphabetical character.</div><div>♦ Case-sensitive</div><div>♦ '-', '_', '@' are allowed.</div></div>
Change Password	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	<div>Select this option to change the password.</div>
Password Size	<div><div>●</div>16 bytes</div>	<div>Select the preferred size for the password.</div>

	<ul style="list-style-type: none"> 20 bytes 	
Password	<div></div>	<p>Enter a strong password consisting of at least one upper case letter, alpha-numeric characters, and special characters</p> <p>Note: Password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.</p>
Confirm Password	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Confirm the password</p>
Channel 1	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Check the boxed to enabled network access for the user. Upon enabling, the corresponding IPMI messaging privilege will be assigned to the user.</p> <p>Note: It is recommended that the IPMI messaging option should be enabled as well if user is created through IPMI</p>
Channel 2	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	
Channel 8	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	
Privilege(Channel 1)	<ul style="list-style-type: none"> User Administrator Operator None OEM 	<p>Select the privilege level for each channel to be assigned to this user for access to the BMC through the network interface.</p> <p>There are 5 levels of Network Privileges</p> <ul style="list-style-type: none"> User Administrator Operator None OEM
Privilege(Channel 2)	<ul style="list-style-type: none"> User Administrator Operator None OEM 	
Privilege(Channel 8)	<ul style="list-style-type: none"> User Administrator Operator None OEM 	
KVM Access	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>This checkbox is used to assign the KVM privilege for the user</p>
VMedia Access	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>This checkbox is used to assign the VMedia privilege for the user</p>
SNMP Access	<div> <input checked="" type="checkbox"/> <input type="checkbox"/> </div>	<p>Check the box to enable SNMP access for the user.</p>
SNMP Access level		<p>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.</p>
SNMP		<p>Choose an SNMP Authentication Protocol for this user.</p>

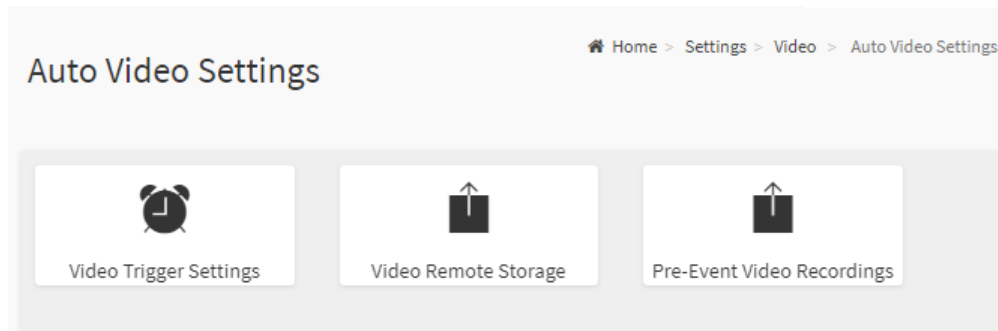
HPS-SRSU4A/HPS-SRSUTA User's Manual

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	<ul style="list-style-type: none"> ● AMI-Format ● Fixed Subject-Format 	<p>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.</p> <p>Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.</p>
Email ID	<input type="text"/>	<p>enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.</p> <p>Maximum allowed size for Email ID is 64bytes (including username and domain name.)</p>
Existing SSH Key	<input type="text"/>	If available, the uploaded SSH key information will be displayed(read-only)
Upload SSH Key	<input type="text"/> 	<p>Use Browse button to navigate to the new public SSH key file.</p> <p>SSH key file should be of pub type.</p>
Save		Click button to save the changes made

2.6.15 Home>Settings>Video Recording



2.6.15.1 Home>Settings>Video Recording >Auto Video Settings



2.6.15.2 Home>Settings>Video Recording>Auto Video Settings>Video Trigger Settings>Video Trigger Settings

You can check/uncheck a box to add/remove that trigger for your system.

Note: KVM service should be enabled to perform auto-video recording.

The date and time event should be in advance of the current system date and time.

Video Trigger Settings

?

☐ Critical Events (Temperature/Voltage)

☐ Non Critical Events (Temperature/Voltage)

☐ Non Recoverable Events (Temperature/Voltage)

☐ Fan state changed Events

☐ Watchdog Timer Events

☐ Chassis Power On Events

☐ Chassis Power Off Events

☐ Chassis Reset Events


☐ LPC Reset Events

☐ Date and Time Event

☐ [Pre-Event Video Recording](#)

Save

HPS-SRSU4A/HPS-SRSUTA User's Manual

Item	Option	Description
Critical Events (Temperature/Voltage)	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Critical Events trigger
Non Critical Events (Temperature/Voltage)	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Non Critical Events trigger
Non Recoverable Events (Temperature/Voltage)	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Non Recoverable Events trigger
Fan state changed Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Fan state changed Events trigger
Watchdog Timer Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Watchdog Timer Events trigger
Chassis Power On Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Power On Events trigger
Chassis Power Off Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Power Off Events trigger
Chassis Reset Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Reset Events trigger
LPC Reset Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove LPC Reset Events trigger
Date and Time Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Date and Time Events trigger
Pre-Event Video Recording	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Pre-Event Video Recording trigger
Save	 Save	Click button to save the changes made

2.6.15.3 Home>Settings>Video Recording>Auto Video Settings>Video Remote Storage>Video Remote Storage

Video Remote Storage

☐ Record Video to Remote Server

Maximum Dumps
2

Maximum Duration (Sec)
20

Maximum Size (MB)
5

Server Address
Server IP or Host name


Path in server
eg. /opt/bmc/videos

Share Type
☒ NFS
 ☐ CIFS

Save


Item	Option	Description
Record Video to Remote Server	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is to enable/disable Remote Video support. Note: By default ,video files will be stored in the local path of the BMC. If the remote video support is enabled, then the video files will be stored only in the remote path , and not within the BMC
Maximum Dumps	1-100	Maximum Dumps value should range from 1 to 100
Maximum Duration (Sec)	1-3600	Maximum Duration should range from 1 to 3600 sec
Maximum Size (MB)	1-500	Maximum Size should range rom 1 to 500 MB
Server Address	<input type="text"/>	Address of the server where remote videos are to be stored. We support the following: IP Address (both IPv4 and IPv6 format). FQDN(Fully qualified domain name) format.
Path in server	<input type="text"/>	Path must be alpha-numeric and the following special characters are only allowed ' / , \ , ' - , ' _ , ' : , ' : '
Share Type	<input checked="" type="radio"/> NFS	Share Type of the remote video server:NFS or Samba(CIFS) are

HPS-SRSU4A/HPS-SRSUTA User’s Manual

	<ul style="list-style-type: none">● CIFS	supported
Save	 Save	Click button to save the changes made

2.6.15.4 Home>Settings>Video Recording>Auto Video Settings>Pre-Event Video Recordings>Pre-Event Video Recordings

Pre-Event Video Recordings



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

Video Quality

Very Low

Compression Mode


High

Frames Per Second


1

Video Duration

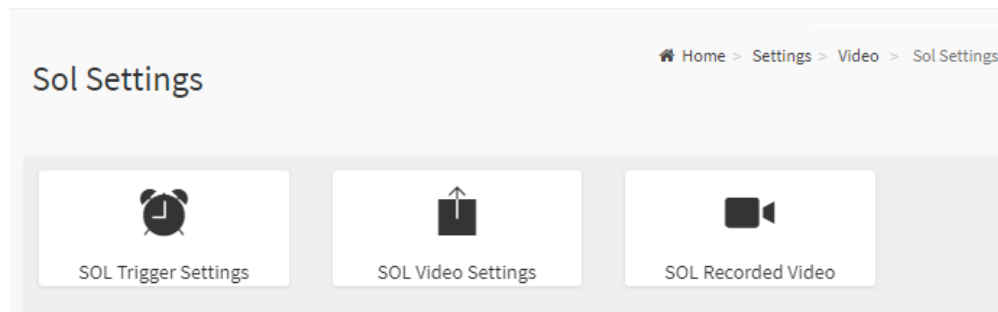
10

 Save

Item	Option	Description
Video Quality	<ul style="list-style-type: none">● Very Low● Low● Average● Normal● High	Choose the desired video quality from the options in the drop-down list
Compression Mode	<ul style="list-style-type: none">● High● Normal● Low● no	Select the Compression Mode from the options listed in the drop-down list
Frames Per Second	1-4	Choose the FPS to specify the desired number of frames per second

Video Duration	10/20/30/40/50/60	Choose the desired video duration in seconds
Save	 Save	Click button to save the changes made

2.6.15.5 Home>Settings>Video Recording>Sol Settings




2.6.15.6 Home>Settings>Video Recording>Sol Settings>SOL Trigger Settings


Configure which event on the page will trigger the SOL video recording. You can check/uncheck a box to add/remove that trigger for your system.

Note: The date and time should be in advance of the current system date and time


SOL Trigger Settings

☐ Critical Events (Temperature/Voltage)
☐ Non Critical Events (Temperature/Voltage)
☐ Non Recoverable Events (Temperature/Voltage)
☐ Fan state changed Events
☐ Watchdog Timer Events
☐ Chassis Power On Events
☐ Chassis Power Off Events
☐ Chassis Reset Events
☐ LPC Reset Events
☐ Date and Time Event

 Save

Item	Option	Description
Critical Events		check/uncheck this option to add/remove Critical Events trigger

HPS-SRSU4A/HPS-SRSUTA User's Manual

(Temperature/Voltage)	<input type="checkbox"/>	
Non Critical Events (Temperature/Voltage)	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Non Critical Events trigger
Non Recoverable Events (Temperature/Voltage)	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Non Recoverable Events trigger
Fan state changed Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Fan state changed Events trigger
Watchdog Timer Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Watchdog Timer Events trigger
Chassis Power On Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Power On Events trigger
Chassis Power Off Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Power Off Events trigger
Chassis Reset Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Chassis Reset Events trigger
LPC Reset Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove LPC Reset Events trigger
Date and Time Events	<input checked="" type="checkbox"/> <input type="checkbox"/>	check/uncheck this option to add/remove Date and Time Events trigger
Save	 Save	Click button to save the changes made

2.6.15.7 Home>Settings>Video Recording>Sol Settings>SOL Video Settings

SOL Video Settings


Log Size (KB)

128


Log File Count

1

☐ Record Video to Remote Server

 Save

Item	Option	Description
Log Size (KB)	<input type="text"/>	Enter the preferred size for the log file. Maximum log file size is 128KB.

Log File Count	<input type="text"/>	Enter whether you want to have log files. Maximum log file count is 1
Record Video to Remote Server	<input checked="" type="checkbox"/> <input type="checkbox"/>	To enable or disable Remote Video support, check or uncheck the 'Enable' checkbox respectively. Note: By default video files will be stored in local path of BMC. If remote video support is enabled then the video files will be stored only in remote path, not within BMC.
Save		Click button to save the changes made

2.6.15.8 Home>Settings>Video Recording>Sol Settings>SOL Recorded video

Below is a list of recorded video files.

Note:

By default, video files will be stored in the local path of the BMC.

If the remote video support is enabled, then the video files will be stored only in the remote path, and not within the BMC.

Click on icon to download and save the file

Click on icon to delete the selected video.

Sol Recorded video

Home >
 Settings >
 Video >
 Sol >
 Sol Recorded video

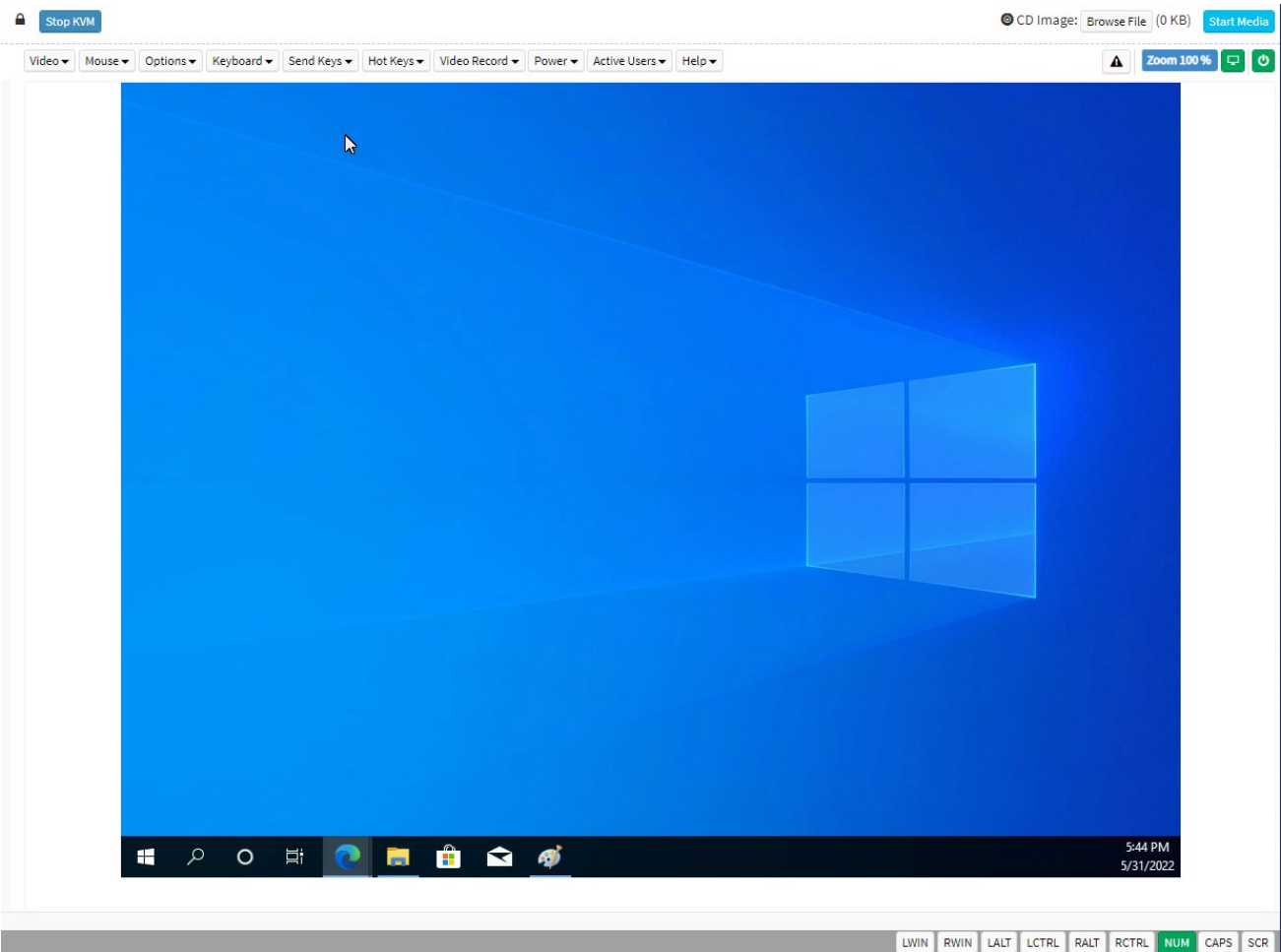
?

S.No	File Name	File Information

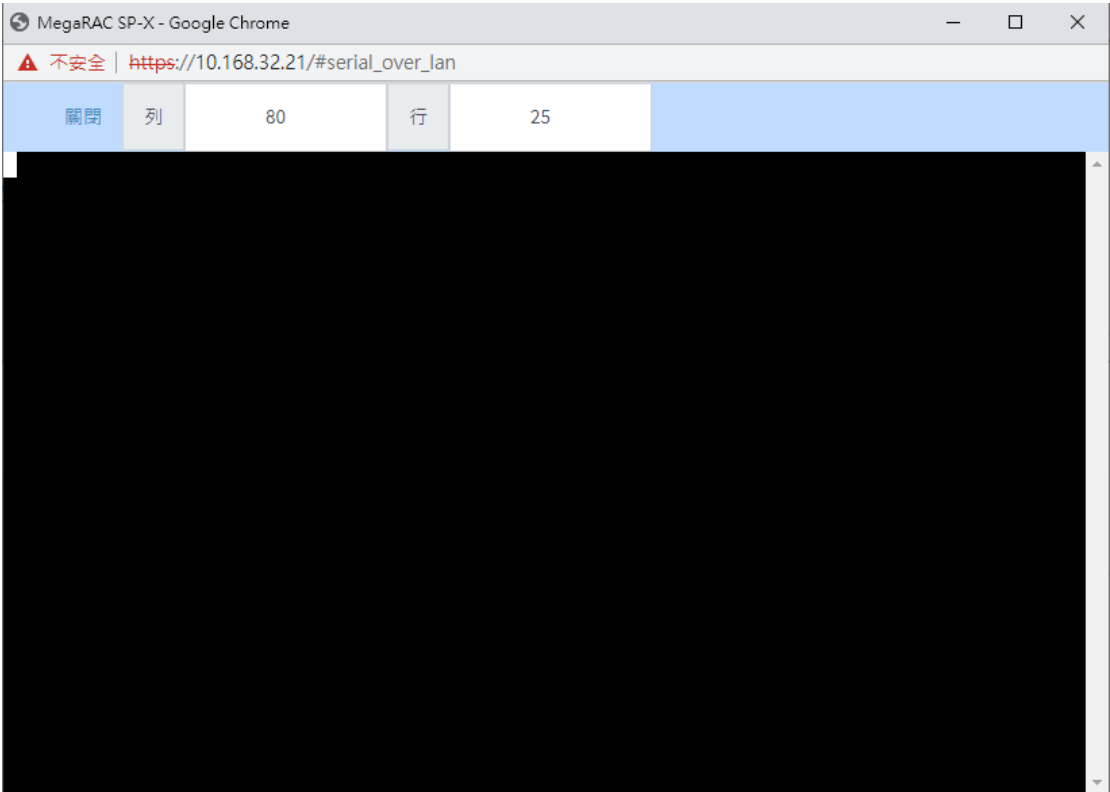
2.7 HOME> REMOTE CONTROL



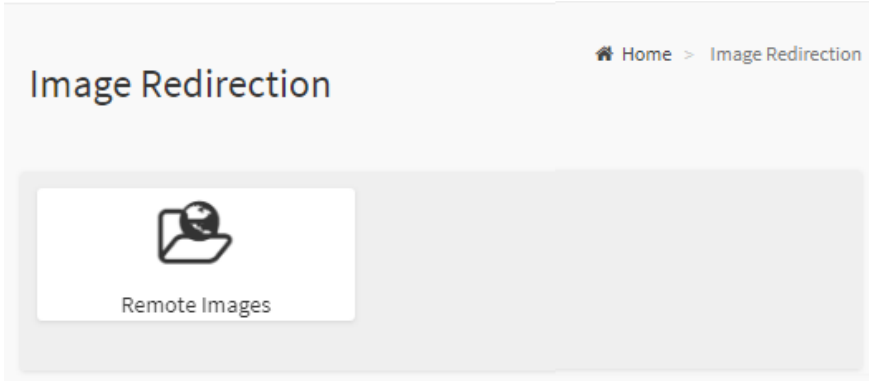
2.7.1 Home>Remote Control >H5Viewer



2.7.2 Home>Remote Control >Serial Over LAN

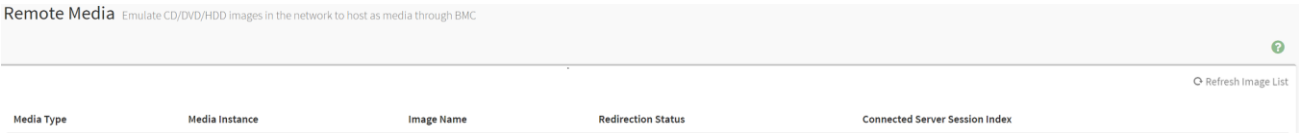


2.8 HOME>IMAGE REDIRECTION



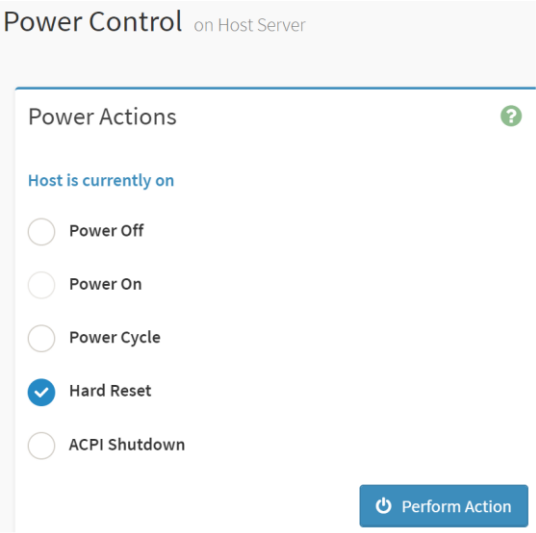
2.8.1 Home >Image Redirection>Remote Media

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

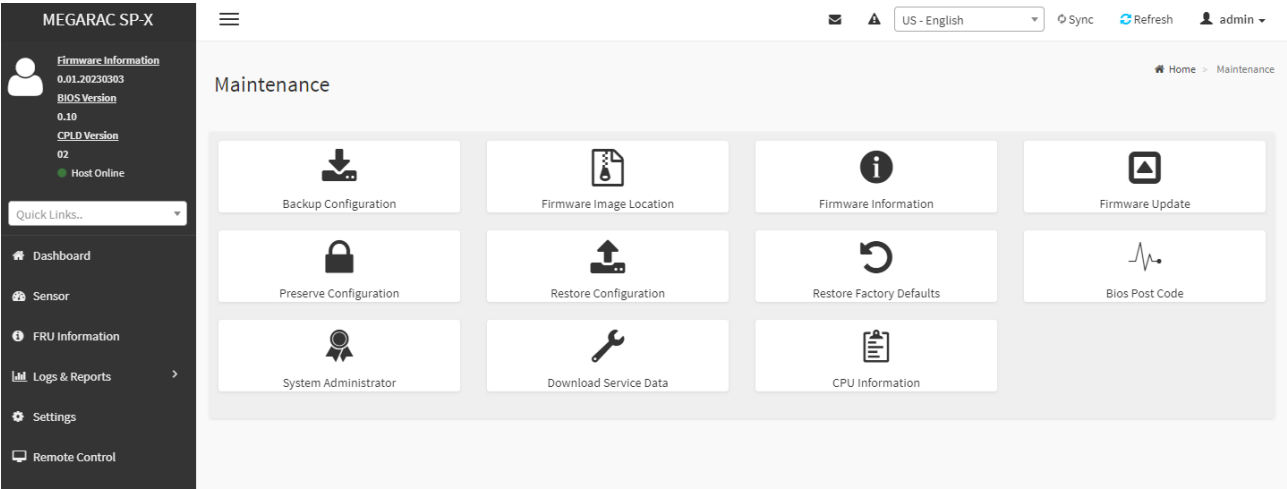
✔ If user first open Power Control page ,this icon means host is currently on this power stage.



Item	Option	Description
------	--------	-------------

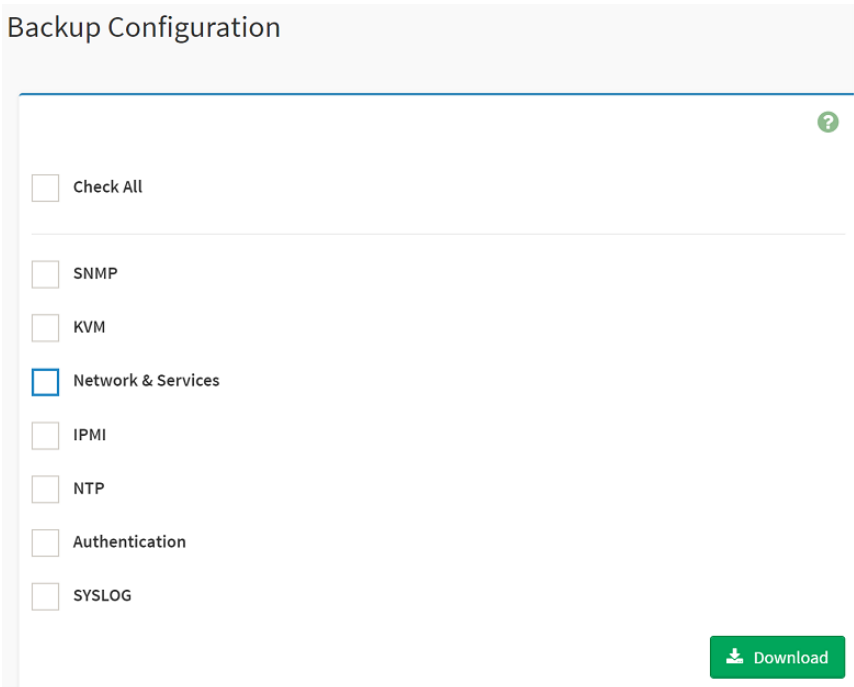
Power Control	 Power Off	Select this option to power off the server
	 Power On	Select this option to power on the server
	 Power Cycle	Select this option to first power off, and then reboot the system (cold boot)
	 Hard Reset	Select this option to reboot the system without powering off (warm boot)
	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

2.10 HOME> MAINTENANCE




2.10.1 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	<input checked="" type="checkbox"/>	Set all following check box as checked
	<input type="checkbox"/>	
SNMP	<input checked="" type="checkbox"/>	Select this option to backup SNMP configuration
	<input type="checkbox"/>	
KVM	<input checked="" type="checkbox"/>	Select this option to backup KVM configuration

	<input type="checkbox"/>	
Network & Services	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup Network & Services configuration
IPMI	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup IPMI configuration
NTP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup NTP configuration
Authentication	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup Authentication configuration
SYSLOG	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup SYSLOG configuration
Download		Click this button to backup selected config above as a file.

2.10.2 Home>Maintenance >Firmware Image Location


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


Firmware Image Location

Image Location Type

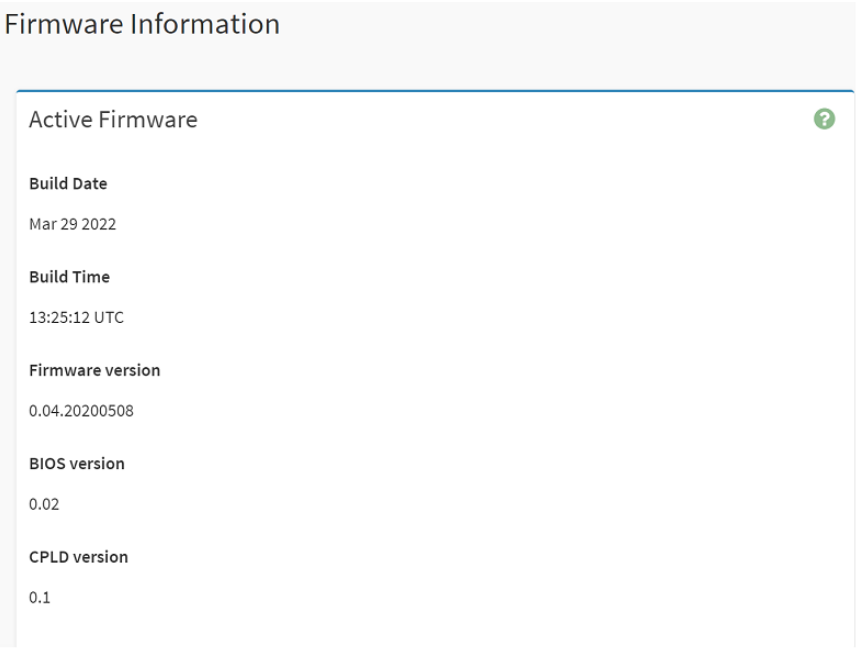
☒ Web Upload during flash

☐ TFTP Server



Item	Option	Description
Image Location Type	<ul style="list-style-type: none"> 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		Click button to save the changes made

2.10.3 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

2.10.4 Home>Maintenance >Firmware Update

Choose the firmware image to be updated

Firmware Update

Note:

Following are the Firmware update methods and components supported in this page.

BMC Firmware update.

HPM Firmware update supports the following components.

BOOT and APP

BIOS

ME

CPLD

Select Firmware Image

Choose File

No file chosen

Start firmware update

WARNING:

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

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

2.10.5 Home>Maintenance >Preserve Configuration

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

Preserve Configuration

?

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

☐ Check All

☐ SDR

☐ FRU

☐ SEL

☐ IPMI

☐ Network

☐ NTP

☐ SNMP

☐ SSH

☐ KVM


☐ Authentication

☐ Syslog

☐ Web

Save

Item	Option	Description
Check All	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Checked this option to set all following check box as checked
SDR	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Checked this option to preserve SDR configuration
FRU	<div><input checked="" type="checkbox"/></div> <div><input type="checkbox"/></div>	Checked this option to preserve FRU configuration

SEL	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve SEL configuration
IPMI	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve IPMI configuration
Network	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Network configuration
NTP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve NTP configuration
SNMP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve SNMP configuration
SSH	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve SSH configuration
KVM	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve KVM configuration
Authentication	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Authentication configuration
Syslog	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Syslog configuration
Web	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Web configuration
Save	 Save	Click the button to save the changes made


2.10.6 Home>Maintenance >Restore Configuration

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


Restore Configuration

?

Config File

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


HPS-SRSU4A/HPS-SRSUTA User’s Manual

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

2.10.7 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.

Restore Factory Defaults



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

☐

SDR

☐

FRU

☐

SEL

☐

IPMI

☐

Network

☐

NTP

☐

SNMP

☐

SSH

☐

KVM

☐

Authentication

☐


Syslog

☐

Web

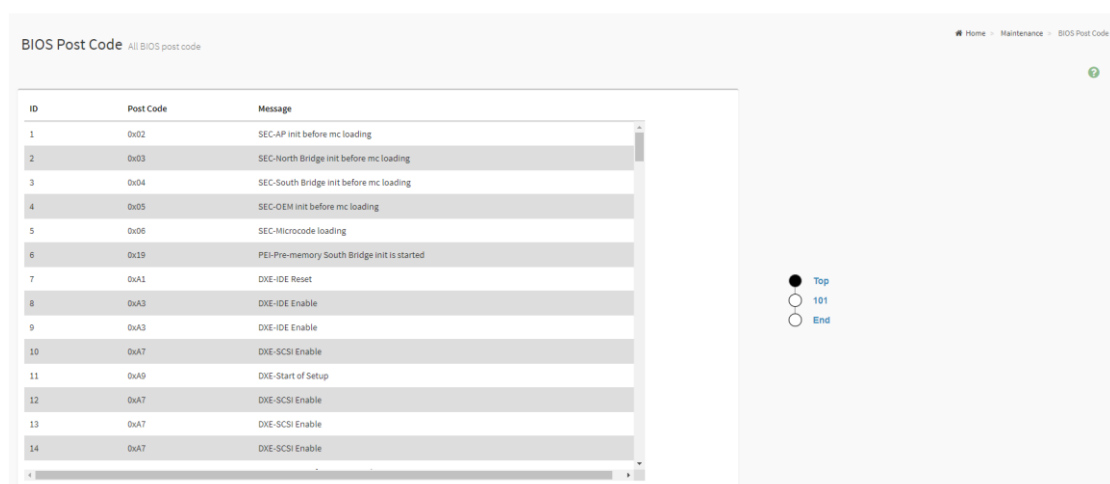
 Save

Item	Option	Description
SDR	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Checked this option to preserve SDR configuration while Restore Factory Defaults
FRU	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Checked this option to preserve FRU configuration while Restore Factory Defaults
SEL	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Checked this option to preserve SEL configuration while Restore Factory Defaults

IPMI	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve IPMI configuration while Restore Factory Defaults
Network	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Network configuration while Restore Factory Defaults
NTP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve NTP configuration while Restore Factory Defaults
SNMP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve SNMP configuration while Restore Factory Defaults
SSH	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve SSH configuration while Restore Factory Defaults
KVM	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve KVM configuration while Restore Factory Defaults
Authentication	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Authentication configuration while Restore Factory Defaults
Syslog	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Syslog configuration while Restore Factory Defaults
Web	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked this option to preserve Web configuration while Restore Factory Defaults
Save	 Save	Click the button to perform Restore Factory Defaults

2.10.8 Home>Maintenance > Bios Post code

Collect all post from Bios.



2.10.9 Home>Maintenance >System Administrator

System Administrator

?

Username

sysadmin

☒

Enable User Access

☐

Change Password

Password

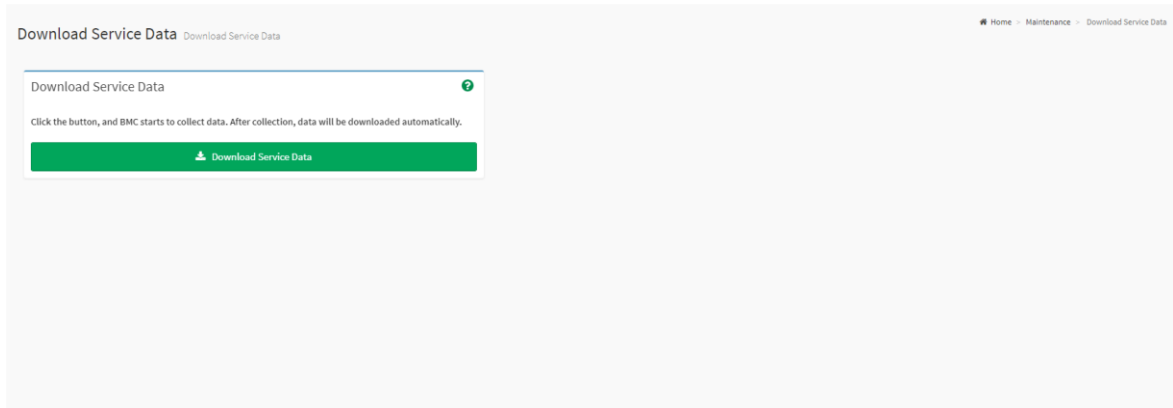
Confirm Password

Save

Item	Option	Description
Username		Username of the System Administrator is displayed(read only)
Enable User Access	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Check/Uncheck this option to enable/disabled user access for the system administrator
Change Password	<div><input checked="" type="checkbox"/> <input type="checkbox"/></div>	Check this option to change the existing password. This will enable the password fields.
Password	<div></div>	Enter the new password here. <ul style="list-style-type: none">♦ At least 8 characters long♦ While space is not allowed♦ More than 64 characters is not allowed
Confirm Password	<div></div>	Enter the same password which you have entered in the Password field to confirm it.
Save	<div>Save</div>	Click button to save the changes made

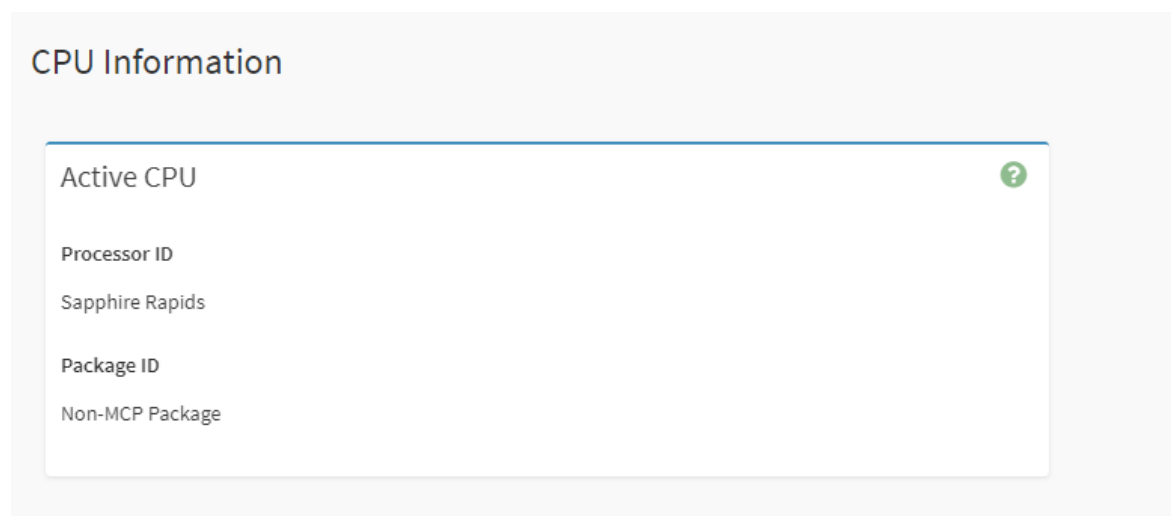
2.10.10 Home>Maintenance > Download Service Data

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.



2.10.11 Home>Maintenance > CPU Information

This page shows active CPU information.



2.11 HOME> SIGN OUT

192.168.1.6 says

Would you like to Sign out of this Session? If yes, click Ok else click Cancel.

OK

Cancel

APPENDIX-A BMC HARDWARE: AST2600

AST2600 is the 7th generation of Integrated Remote Management Processor introduced by ASPEED Technology Inc. It's 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 significantly 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 complex 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 described in the following chapters.

The chip architecture is showed below:

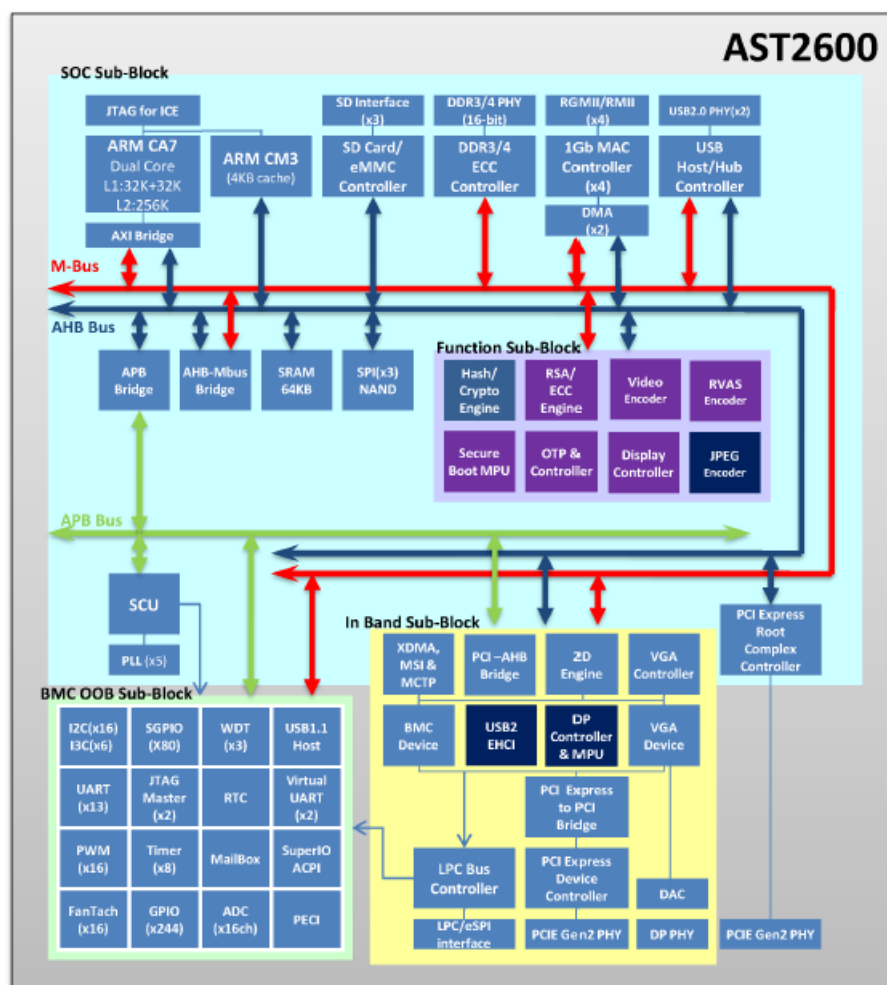


Figure A-1 AST2600 Chip Architecture

HPS-SRSU4A/HPS-SRSUTA User's Manual

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 masters: 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	CM D	M/ O	Supporte d	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 available, 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	

HPS-SRSU4A/HPS-SRSUTA User's Manual

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		

HPS-SRSU4A/HPS-SRSUTA User's Manual

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		
GetChassisDeviceld	Bridge	13h	O		
SetChassisDeviceld	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- FEh	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_FAN1 pwm duty cycle Byte2 = Outlet_FAN1 pwm duty cycle Byte3 = Outlet_FAN2 pwm duty cycle Byte4 = Intel_FAN pwm duty cycle
Get BIOS Version	0x30	37h	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:

+V12S_CPU1	12.30 Volts	ok
+V5A	4.95 Volts	ok
+V3.3A	3.25 Volts	ok
+V1.8A	1.81 Volts	ok
+VNN_PCH_AUX	0.99 Volts	ok
+V1.05A	1.04 Volts	ok
+V1.2A_BMCDDDR	1.21 Volts	ok
+V1.15A_BMC	1.14 Volts	ok
+V1S_VCCIO_P1AD	1 Volts	ok
+V5SB	5.10 Volts	ok
+V12S	12.30 Volts	ok
+V5S	5 Volts	ok
+V3.3S	3.35 Volts	ok
+V3.0A_BAT	3.05 Volts	ok
+VCCIN_CPU1	1.80 Volts	ok
+VCCSA_CPU1	0.89 Volts	ok
P1 VDDR-123	1.22 Volts	ok
P1 VPP-123	2.57 Volts	ok
P1 VDDR-456	1.22 Volts	ok
P1 VPP-456	2.57 Volts	ok
+V1S_VCCIO_CPU1	1.01 Volts	ok
P1 +VCCIN_T	37 degrees C	ok
P1 +VCCSA_T	35 degrees C	ok
P1 DDR-123 T	35 degrees C	ok
P1 VPP_123_T	32 degrees C	ok

P1 DDR-456 T	38 degrees C	ok
P1 VPP_456_T	32 degrees C	ok
P1 VCCIO_T	32 degrees C	ok
CPU1_FAN	2100 RPM	ok
Outlet_FAN1	3500 RPM	ok
Outlet_FAN2	3550 RPM	ok
Intel_FAN1	1600 RPM	ok
Outlet T	25 degrees C	ok
Inlet T	25 degrees C	ok
CPU1 T	31 degrees C	ok
PCH T	37 degrees C	ok
DIMM1 T	no reading	ns
DIMM2 T	no reading	ns
DIMM3 T	31 degrees C	ok
DIMM4 T	no reading	ns
DIMM5 T	no reading	ns
DIMM6 T	30 degrees C	ok
CPU THERMTRIP	0x00	ok
Slot1_GPU_T	no reading	ns
Slot2_GPU_T	no reading	ns
Slot3_GPU_T	31 degrees C	ok
Slot4_GPU_T	no reading	ns
Slot5_GPU_T	29 degrees C	ok
Slot6_GPU_T	no reading	ns
Slot7_GPU_T	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

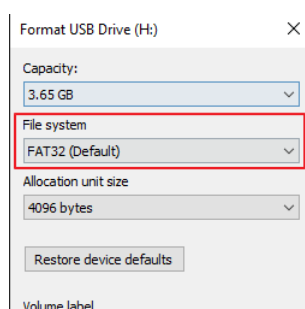
If necessary, the system firmware can be updated at local machine or remote console. Please refer the following instructions.

1. BIOS + SPS

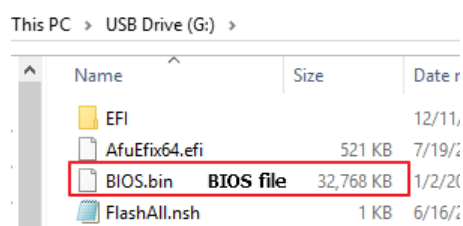
Update Method	OS	Tool and Jumper settings
Local Update	UEFI environment	AfuEfix64.efi Need to disable SPS by JME1 jumper.
Remote Update	IPMI Web UI	No tool required No need to disable SPS.

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** directory of the USB drive.



3. Plug the USB drive to the Server and close pin 2-3 of JME1.

HPS-SRSU4A/HPS-SRSUTA User's Manual

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



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

```
EDK II
UEFI v2.70 (American Megatrends, 0x0005000E)
Mapping table
FS0: Alias(s): HD0h0b:;BLK1:
PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)/HD(1,MBR,0x1011BD0C,0xB00,0x75
0040)
BLK0: Alias(s):
PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)
BLK2: Alias(s):
PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x0,0x0)
BLK3: Alias(s):
PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x1,0x0)
BLK4: Alias(s):
PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x1,0x0)/Unit(0x1)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
```

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

```
fs0:\> ls
Directory of: fs0:\

12/11/19 04:17p <DIR>          4,096  EFI
07/19/18 06:33p          532,592  AfuEfix64.efi
01/02/20 04:46p        33,554,432  BIOS.bin
06/16/16 02:00a           430  FlashAll.nsh
          3 File(s)  34,087,454 bytes
          1 Dir(s)

fs0:\> FlashAll.nsh BIOS.bin
```

input your BIOS file name

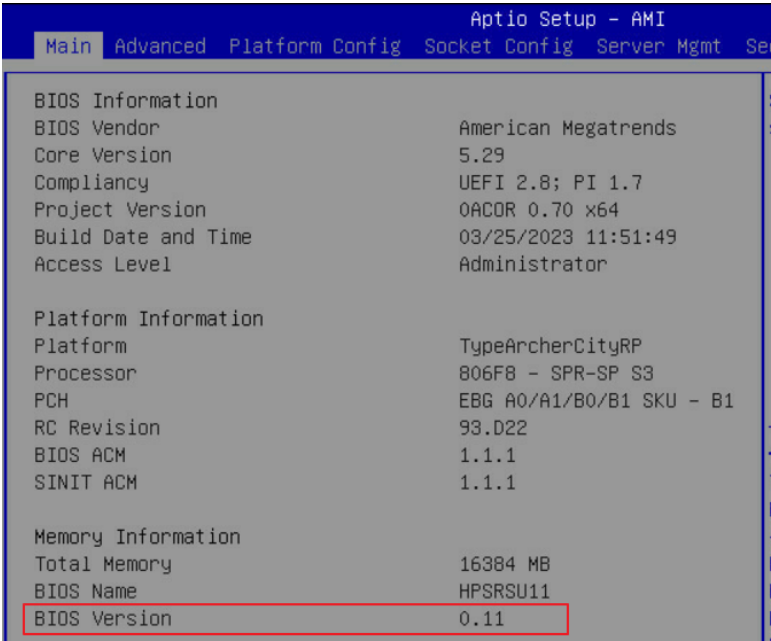
7. When the process ends, make sure all regions are done successfully without any error.

```
- Check RomLayout ..... Pass
Erasing Main Block ..... Done
Updating Main Block ..... Done
Verifying Main Block ..... Done
Erasing Boot Block ..... Done
Updating Boot Block ..... Done
Verifying Boot Block ..... Done
Erasing NVRAM Block ..... Done
Updating NVRAM Block ..... Done
Verifying NVRAM Block ..... Done
Loading The ME Data To BIOS ..... Done
- Update success for FDR
- Update success for GBER
- Update success for DER
- Successful update recovery region to OPRx!!
- Successful update MFSB
- Successful update factory data and recovery region
- ME Entire Image update success !!
WARNING !!
System must power-off to have the changes which take effect!
Process completed.
```

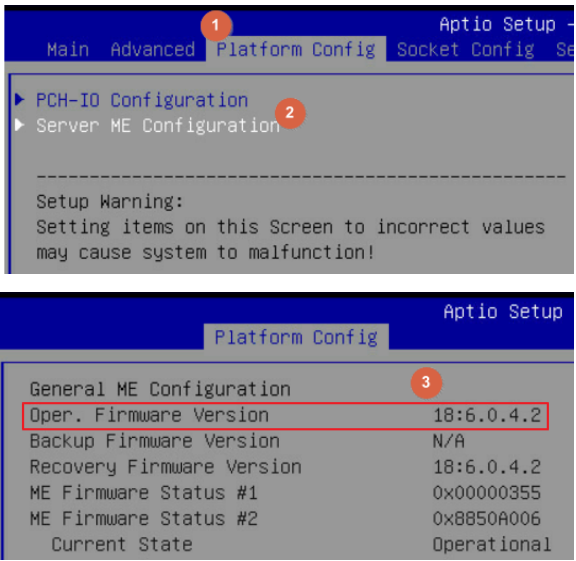
8. Remove AC power and move **JME1** jumper back to pin 1-2.
9. Power on, then boot to BIOS to check if BIOS version and SPS version are correct.

HPS-SRSU4A/HPS-SRSUTA User’s Manual

BIOS version:



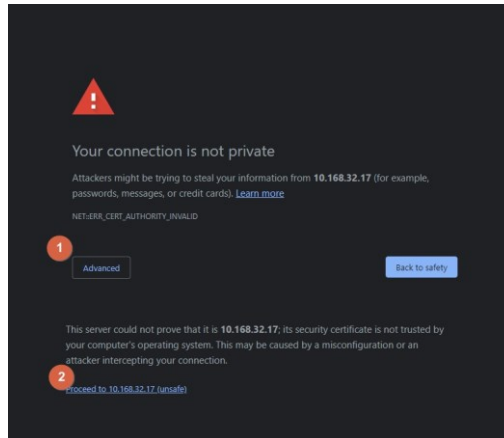
SPS version:



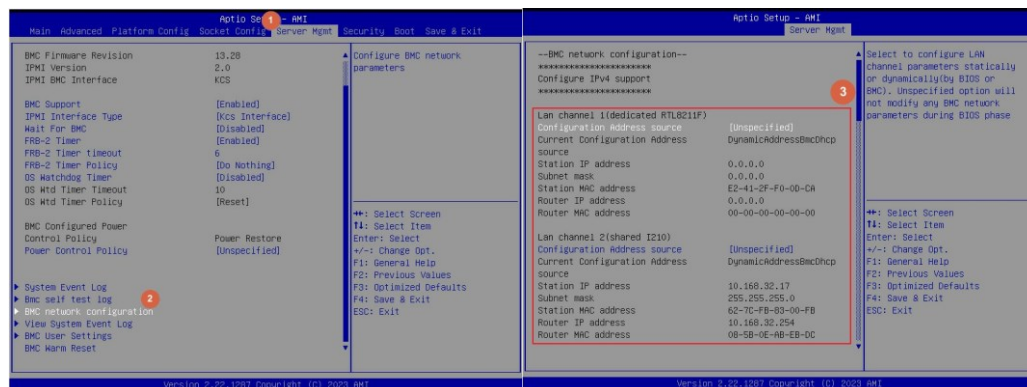
1.2 BIOS + SPS update using IPMI Web UI

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.

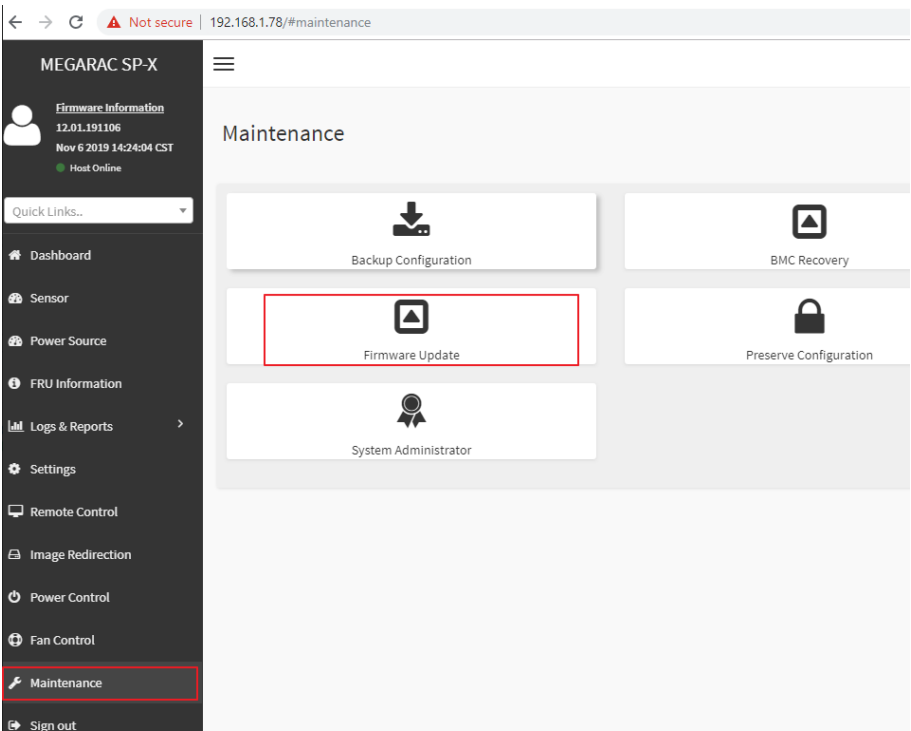


Note: BMC IP address can be configured at BIOS menu.

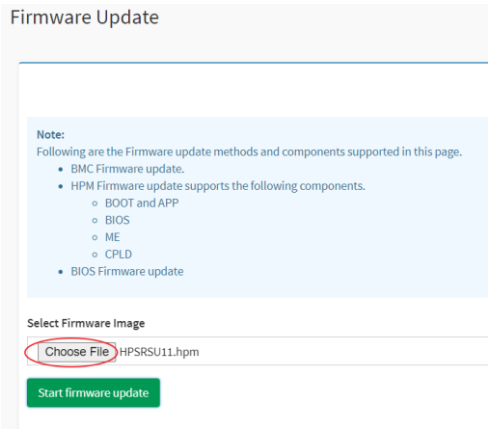


HPS-SRSU4A/HPS-SRSUTA User’s Manual

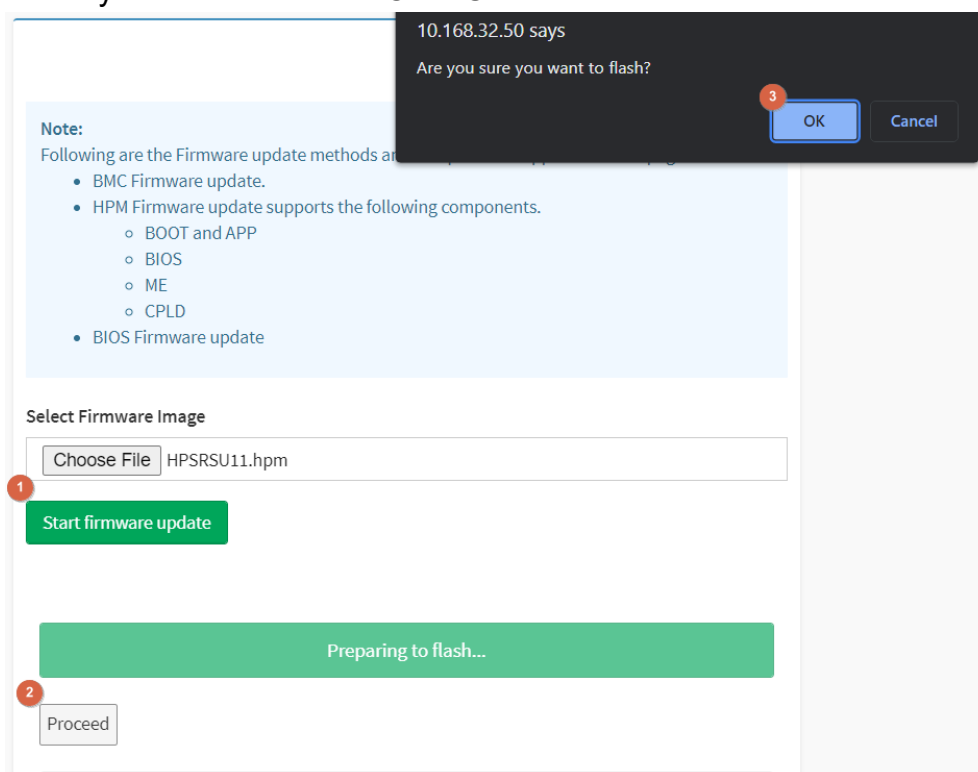
2. Click the **Maintenance** tab, then **Firmware Update**.



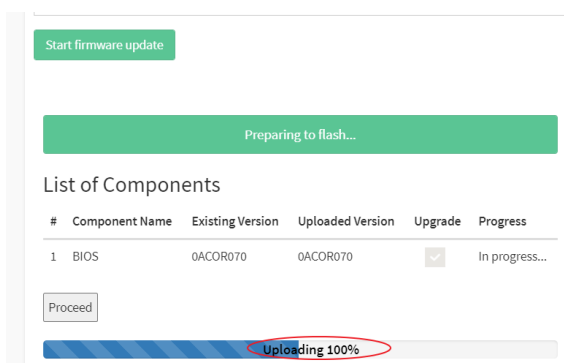
3. **Choose File** to select BIOS file(xxx.hpm).



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 **Proceed** again.



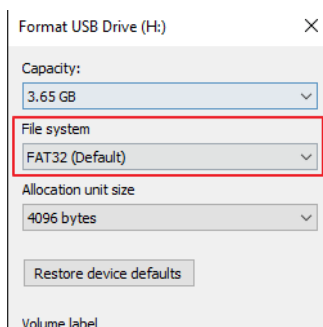
6. After finish the processs, BMC will reset after few seconds. Refer 1.1.1 step9 to check the BIOS and SPS version.

2. BIOS

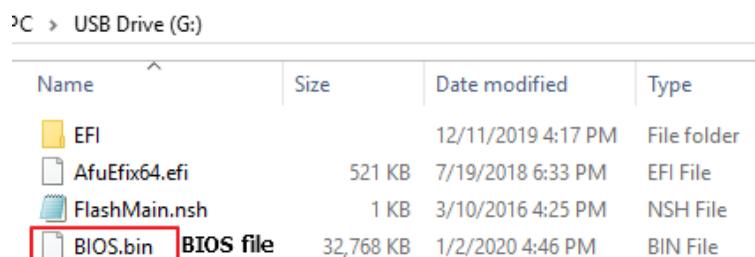
Update Method	OS	Tool
Local Update	UEFI environment	AfuEfix64.efi

2.1 BIOS update in UEFI environment

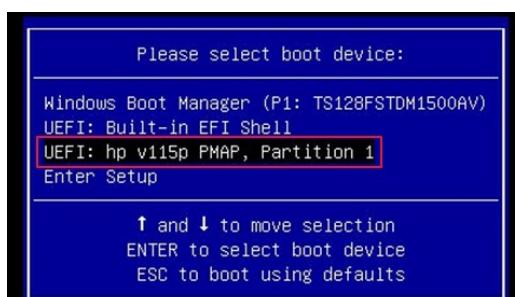
1. Format a USB flash drive to FAT32.



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:**

```
EDK II
UEFI v2.70 (American Megatrends, 0x0005000E)
Mapping table
FS0: Alias(s):HD0h0b:;BLK1:
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)/HD(1,MBR,0x1011BDBC,0x800,0x75
0040)
BLK0: Alias(s):
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0x7,0x0)
BLK2: Alias(s):
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x0,0x0)
BLK3: Alias(s):
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x1,0x0)
BLK4: Alias(s):
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0xA,0x0)/USB(0x1,0x0)/Unit(0x1)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
```

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

```
Shell> fs0:
fs0:\> FlashMain.nsh BIOS.bin Input your BIOS name
```

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

```
+-----+
| Reading flash ..... done |
| - ME Data Size checking . ok |
| - FFS checksums ..... ok |
| - Check RomLayout ..... ok. |
| Erasing Boot Block ..... done |
| Updating Boot Block ..... done |
| Verifying Boot Block ..... done |
| Erasing Main Block ..... done |
| Updating Main Block ..... done |
| Verifying Main Block ..... done |
| Erasing NVRAM Block ..... done |
| Updating NVRAM Block ..... done |
| Verifying NVRAM Block ..... done |
| Process completed. |
+-----+
FS0:\> _
```

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

```
Aptio Setup - AMI
Main Advanced Platform Config Socket Config Server Mgmt Se

BIOS Information
BIOS Vendor          American Megatrends
Core Version         5.29
Compliance           UEFI 2.8; PI 1.7
Project Version      OACOR 0.70 x64
Build Date and Time  03/25/2023 11:51:49
Access Level         Administrator

Platform Information
Platform             TypeArcherCityRP
Processor            806F8 - SPR-SP S3
PCH                  EBG A0/A1/B0/B1 SKU - B1
RC Revision          93.D22
BIOS ACM             1.1.1
SINIT ACM            1.1.1

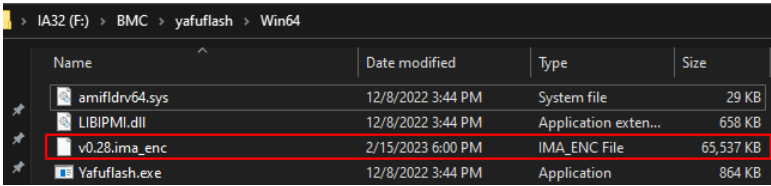
Memory Information
Total Memory         16384 MB
BIOS Name            HPSRSU11
BIOS Version         0.11
```

3. BMC

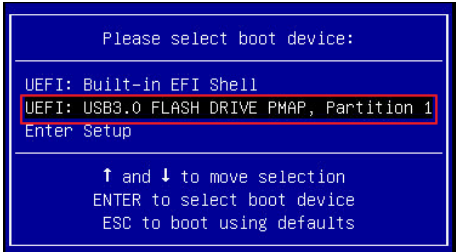
Update Method	OS	Tool
Local update	WinPE Environment	Yafuflash.exe
Remote update	IPMI Web UI	No tool required
	IPMI command	Yafuflash.exe

3.1 BMC update in WinPE environment

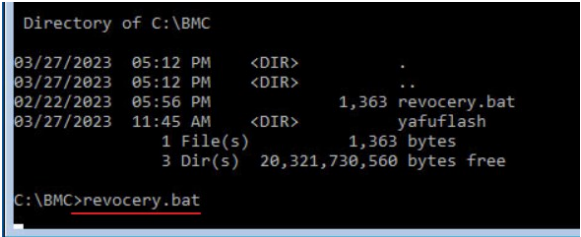
1. Copy update tool and BMC file to WinPE disk.



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.

```
*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Preserving Env Variables... done
Uploading Firmware Image : 100%... done
Skipping [boot] Module ....
Flashing [conf] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [bkupconf] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [root] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [osimage] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [www] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [lmedia] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [extlog] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [extlog] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [archerci] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Resetting the firmware.....
```

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

```
C:\BMC\yafuflash\Win64>Yafuflash.exe -kcs -mi
INFO: Yafu INI Configuration File not found... Default options will not be applied...

+-----+
| YAFUFlash - Firmware Upgrade Utility v7.01.0096 |
| Copyright (c) 2020 American Megatrends International, LLC |
+-----+

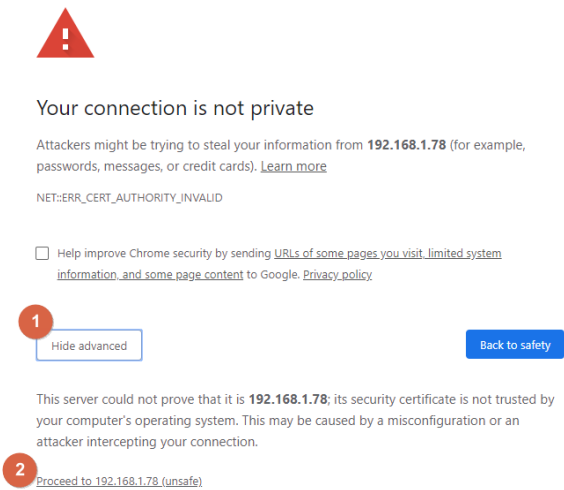
=====
Firmware Details
=====
      Image Version
Module Name  Description  Version
-----
1.archerci  13.28.202302
```

HPS-SRSU4A/HPS-SRSUTA User's Manual

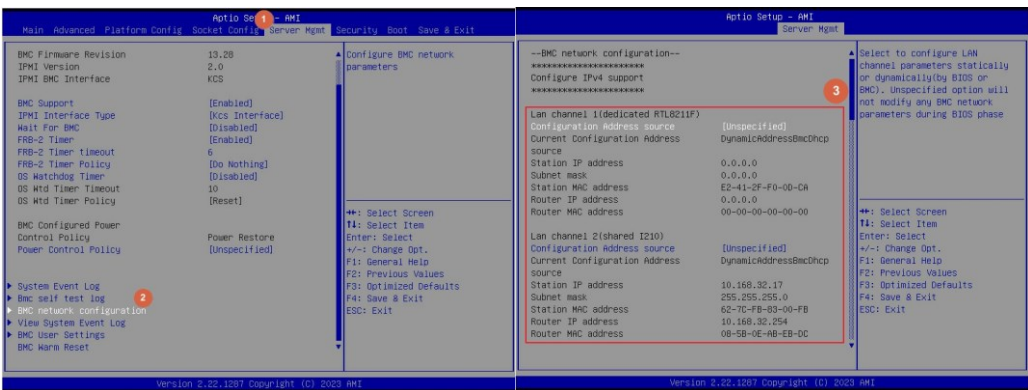
3.2 BMC update using Web UI

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

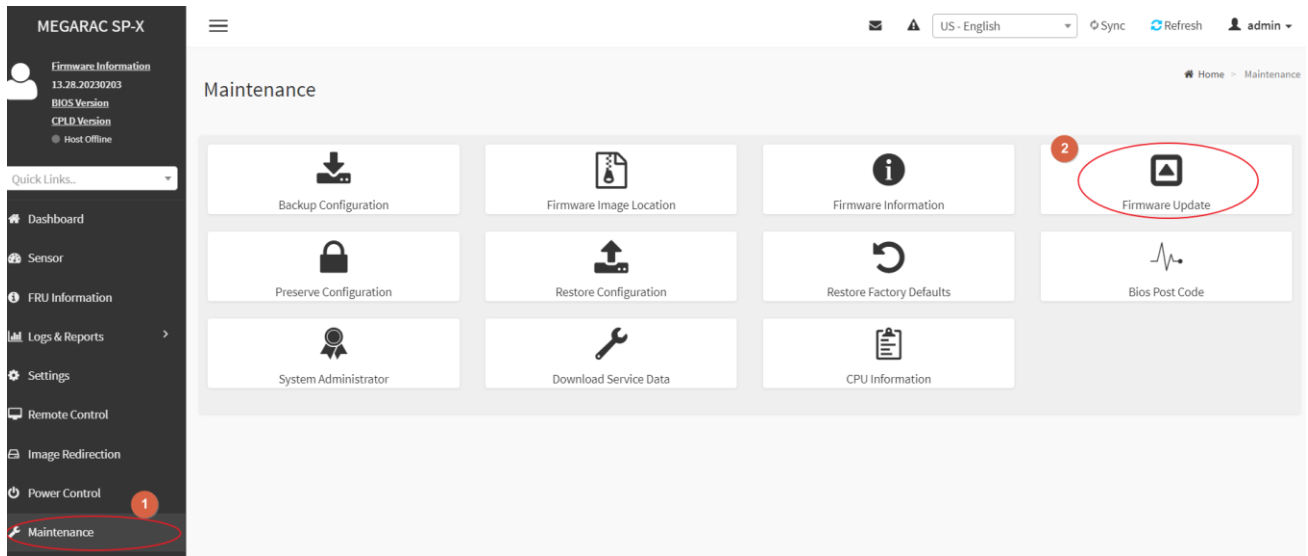
If you get a message that says “Your connection is not private”, just skip it.



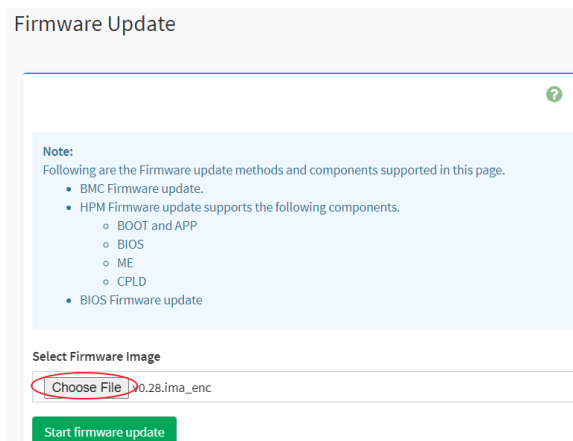
Note: BMC IP address can be configured at BIOS menu.



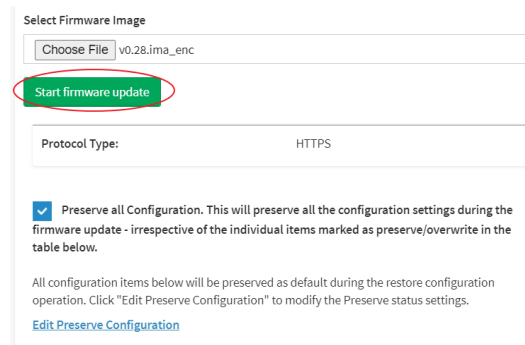
2. Click **Maintenance** and go to **Firmware Update**.



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

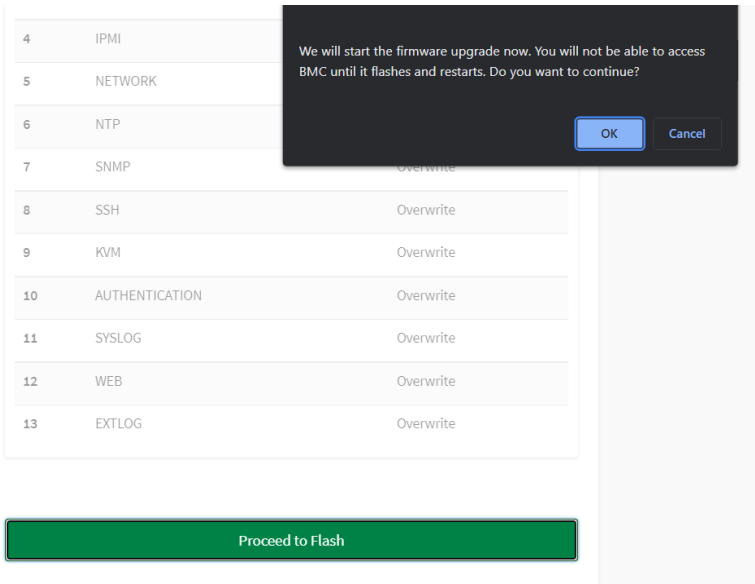


4. Click the **Start firmware update** button, then scroll down and check **Preserve all Configuration** if you'd like to preserve all configuration.

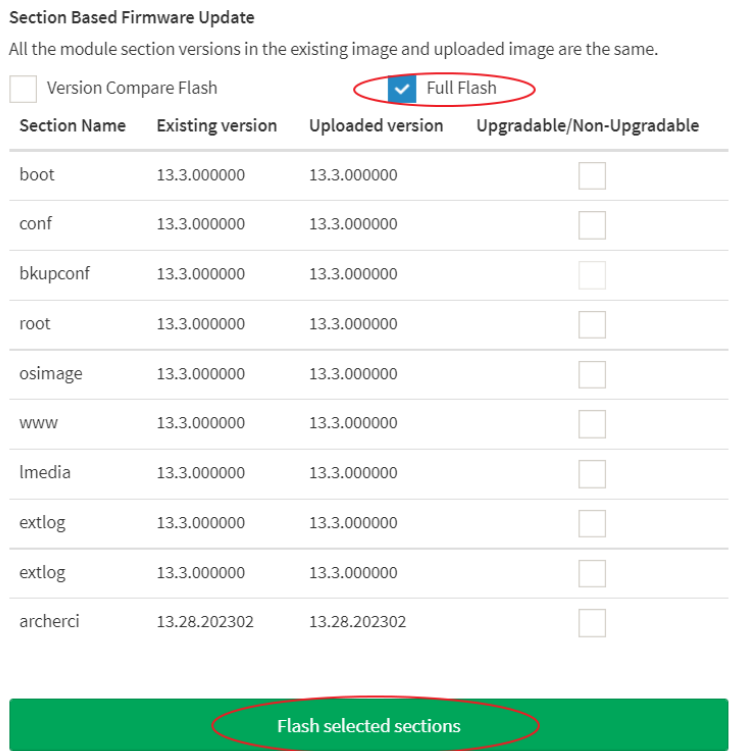


HPS-SRSU4A/HPS-SRSUTA User’s Manual

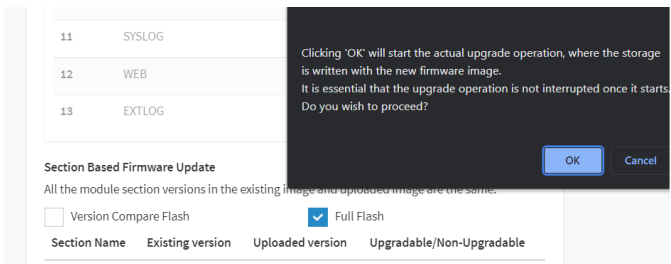
Click **Preceed to Flash**
The message box appears. Click **OK**.



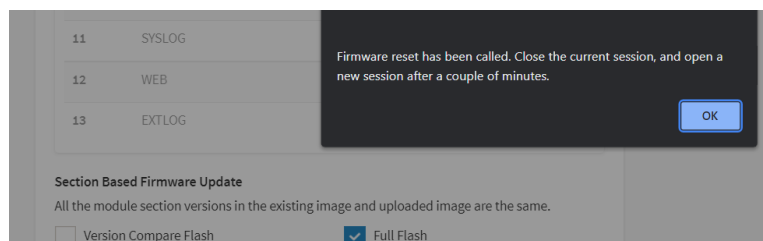
Select **Full Flash**, and click **Flash selected sections**.



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 couple of minutes.". Click **OK**.



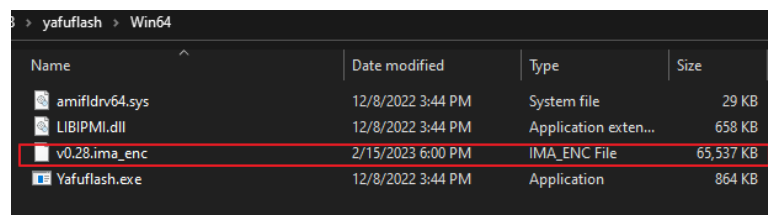
6. Login to check the BMC firmware version.



HPS-SRSU4A/HPS-SRSUTA User's Manual

3.3 BMC update using IPMI tool

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

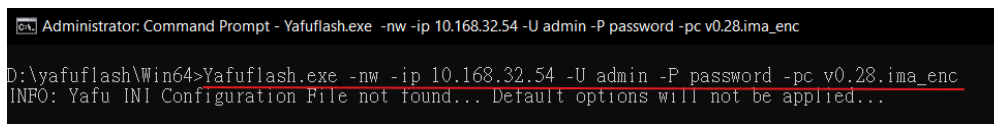


Name	Date modified	Type	Size
amifldr64.sys	12/8/2022 3:44 PM	System file	29 KB
LIBIPMI.dll	12/8/2022 3:44 PM	Application extension	658 KB
v0.28.ima_enc	2/15/2023 6:00 PM	IMA_ENC File	65,537 KB
Yafuflash.exe	12/8/2022 3:44 PM	Application	864 KB

2. Open Command Prompt (admin).

3. Input the command:

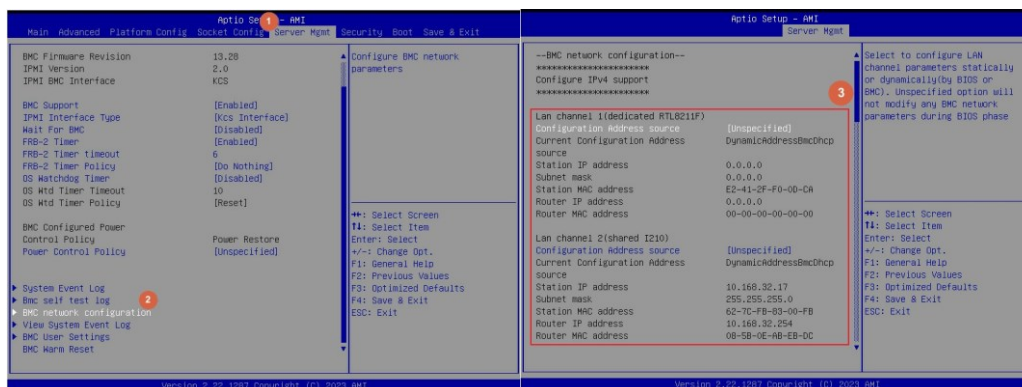
Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -pc [BMC file name]. The default username and password are admin/admin.



```
Administrator: Command Prompt - Yafuflash.exe -nw -ip 10.168.32.54 -U admin -P password -pc v0.28.ima_enc

D:\yafuflash\Win64>Yafuflash.exe -nw -ip 10.168.32.54 -U admin -P password -pc v0.28.ima_enc
INFO: Yafu INI Configuration File not found... Default options will not be applied...
```

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.



```
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
(C)Copyright 2017, American Megatrends Inc.
signed hash length is 128
The Rom Image size = 32 MB
The Current flash size = 32 MB
The Module boot size is different from the one in the Image

*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Uploading Firmware Image : 31%
```

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

```

Administrator: Command Prompt

PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Preserving Env Variables... done
Uploading Firmware Image : 100%... done
Skipping [boot] Module ....
Flashing [conf] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [bkupconf] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [root] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [osimage] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [www] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [lmedia] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [extlog] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [extlog] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Flashing [archerci] Module ....
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
Resetting the firmware.....

D:\yafuflash\Win64>

```

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

```

D:\yafuflash\Win64>Yafuflash.exe -nw -ip 10.168.32.54 -U admin -P password -mi
INFO: Yafu INI Configuration File not found... Default options will not be applied...

Creating IPMI session via network with address 10.168.32.54...Done

+-----+
|      YAFUFlash - Firmware Upgrade Utility v7.01.0096      |
| Copyright (c) 2020 American Megatrends International, LLC |
+-----+

=====
Firmware Details
=====
ModuleName      Image Version
Description      Version
l.archerci      13.28.202302

```

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 = Outlet_FAN1 2 = Outlet_FAN2 3 = Intel_FAN1 PWM: The PWM duty cycle 0x64 =100%
Get fan PWM	0x30	0x36	The response data represent each fan PWM. Byte1 = CPU1_FAN1 pwm duty cycle Byte2 = Outlet_FAN1 pwm duty cycle Byte3 = Outlet_FAN2 pwm duty cycle Byte4 = Intel_FAN1 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

```
~ # ipmitool raw 0x30 0x1 0x1  
01
```

Step 2. Set fan PWM

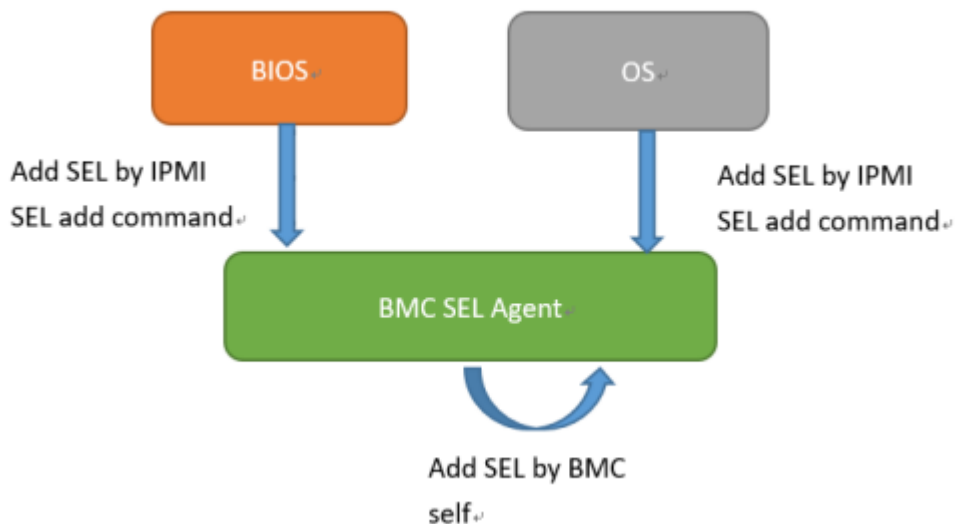
```
~ # ipmitool raw 0x30 0x35 0x2 0x20  
-
```

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.

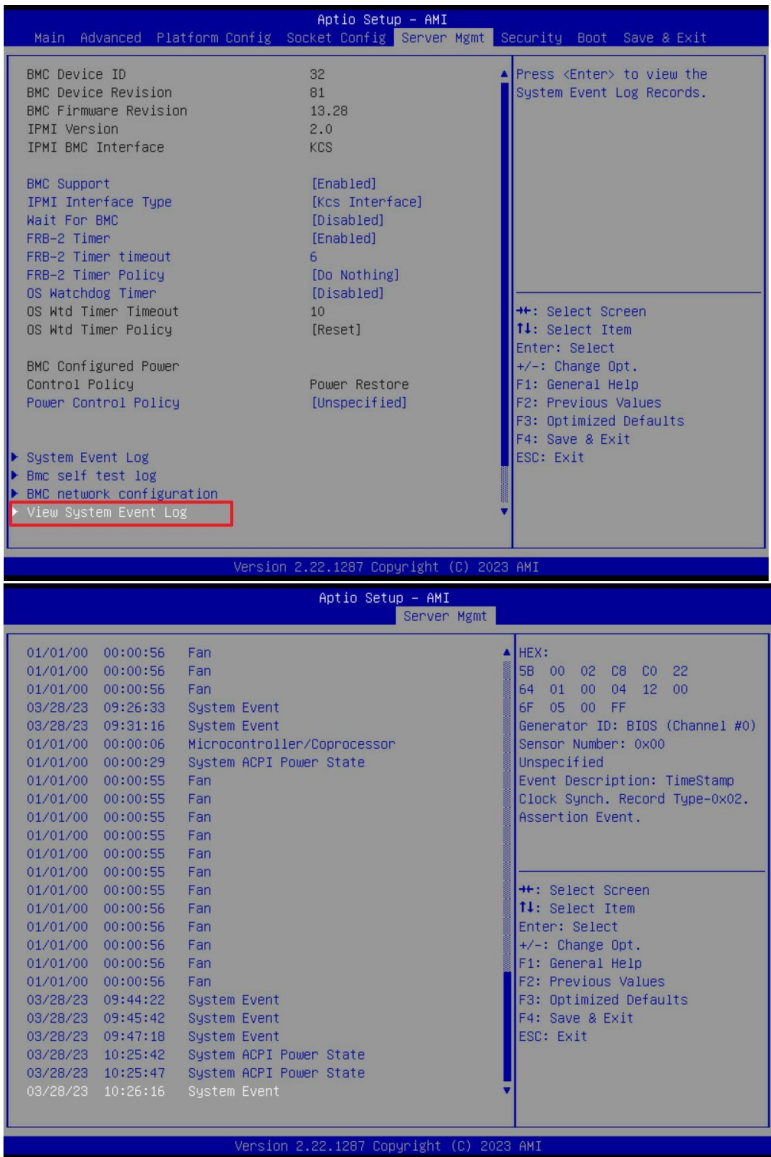
Byte	Field	Description
1, 2	Record ID (RID)	ID used for SEL record access.
3	Record Type (RT)	<p>[7:0] – Record type</p> <p>02h = System event record (default)</p> <p>C0h-DFh = OEM timestamped, bytes 8-16 OEM defined (see Table 3)</p> <p>E0h-FFh = OEM non-timestamped, bytes 4-16 OEM defined (see Table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

HPS-SRSU4A/HPS-SRSUTA User’s Manual

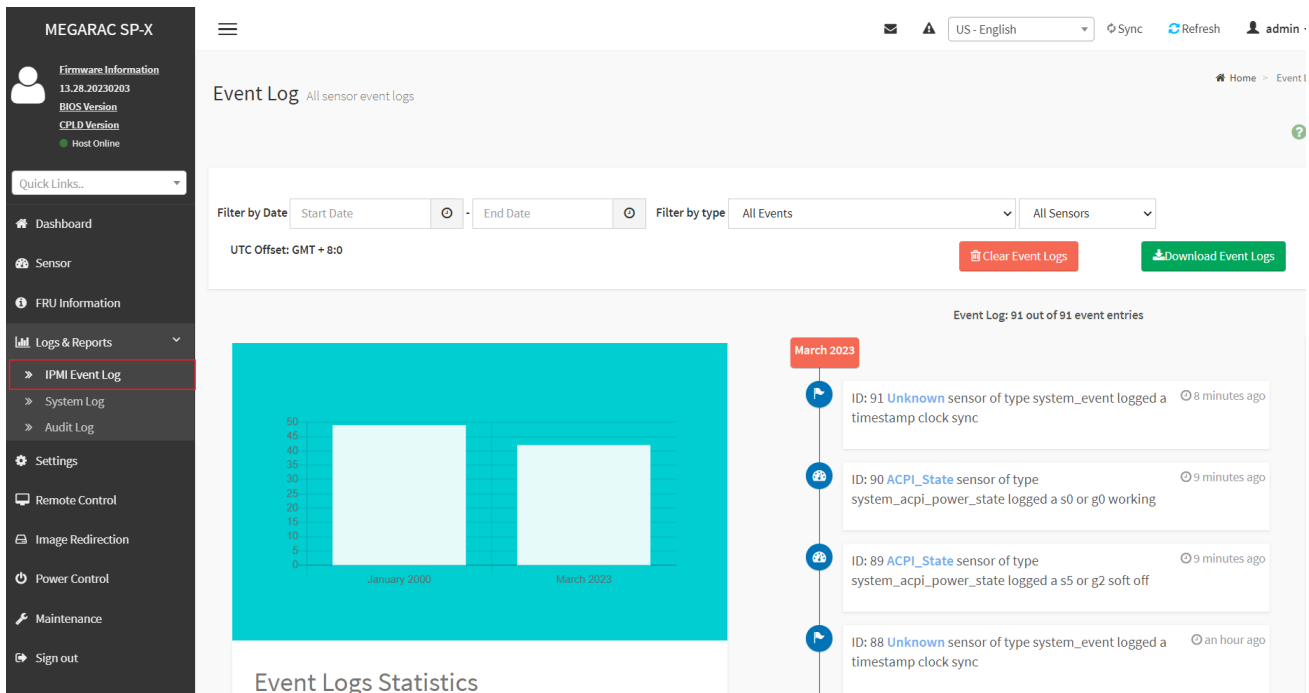
When capturing the SEL log, always collect both the text/human readable version and the hex version. Because some of the data is OEM-specific, some utilities cannot decode the information correctly. In addition, with some OEM-specific data there may be additional variables that are not decoded at all.

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]
```

HPS-SRSU4A/HPS-SRSUTA User's Manual

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

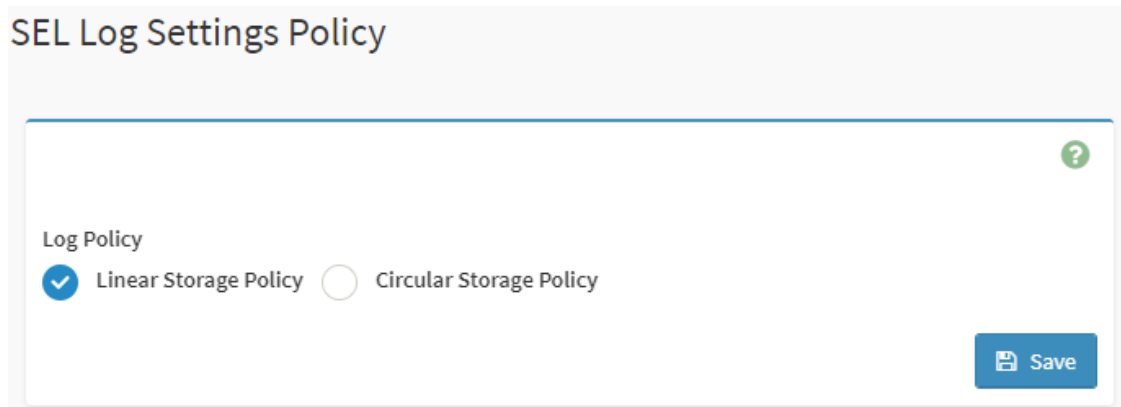
BMC will not overwrite log but inform user when the log size reach 70% and 100%.

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



The screenshot shows a web interface for configuring the SEL Log Settings Policy. The title is "SEL Log Settings Policy". Below the title is a form with a "Log Policy" section. It contains two radio button options: "Linear Storage Policy" (which is selected with a blue checkmark) and "Circular Storage Policy" (which is unselected). A green question mark icon is in the top right corner of the form. A blue "Save" button is in the bottom right corner.

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:

HPS-SRSU4A/HPS-SRSUTA User's Manual

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 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 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 a0
a2 a2 a0 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.

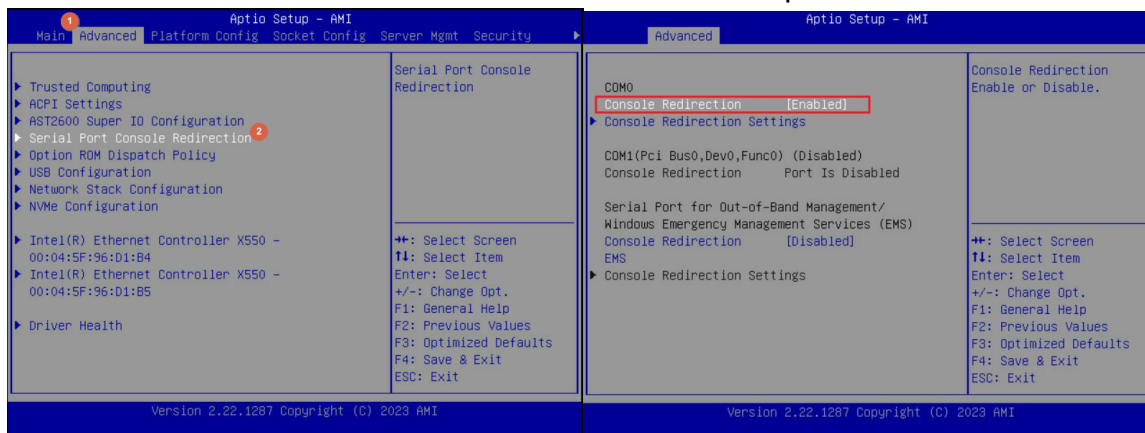
Remotely get BIOS code by “ipmiutil” in windows:

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

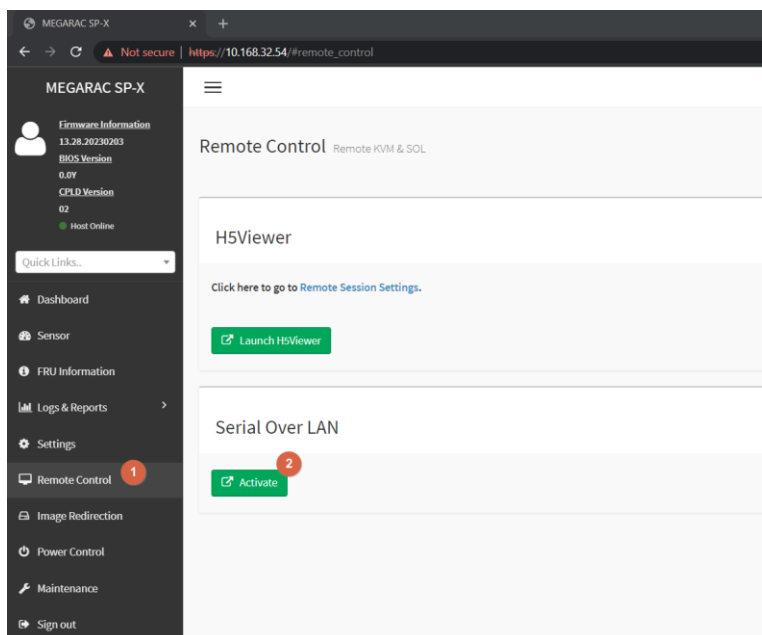
```
D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.77 -U admin -P admin 00 20 C8 73 0
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node 192.168.1.77
-- BMC version 0.5, IPMI version 2.0
respData[len=160]: 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 b9 b9 ba b9 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 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 b
4 b4 a2 a2 a0 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

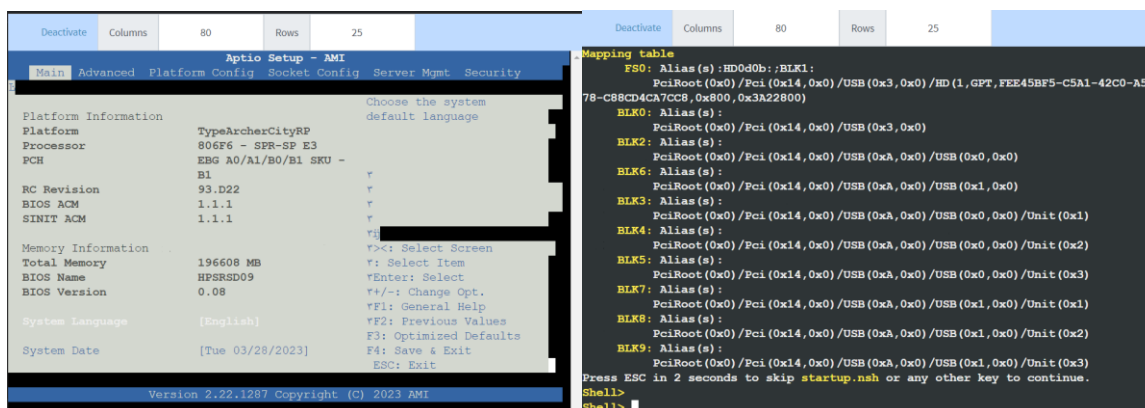
1. Enable Serial Port Console Redirection in BIOS setup menu.



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

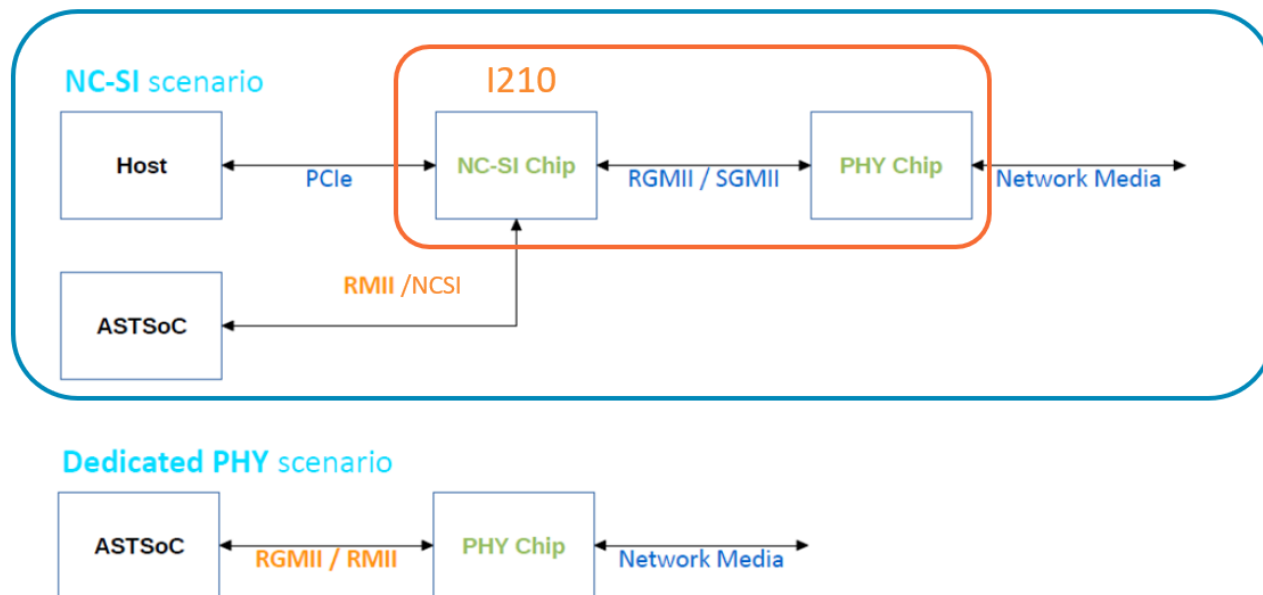


3. Access BIOS and UEFI shell in serial console.



APPENDIX-K Dedicated vs Shared IPMI port

Dedicated PHY scenario vs NC-SI(Shared) scenario

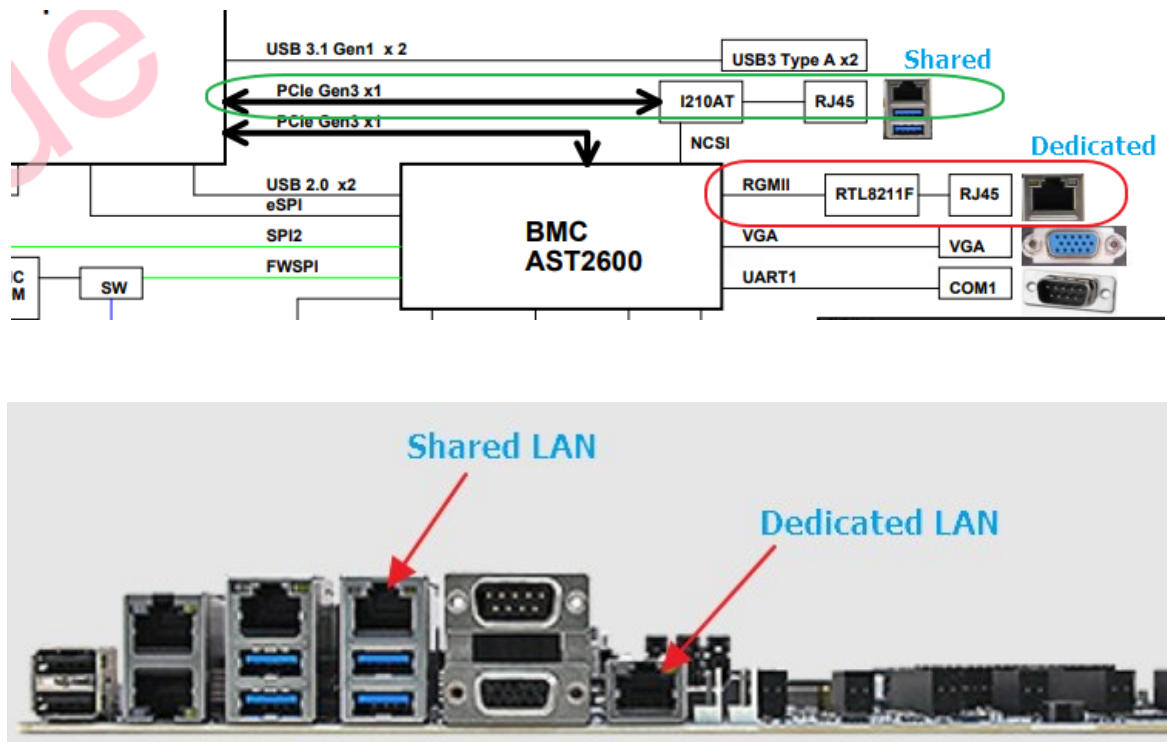


Network Controller Sideband Interface (NC-SI)

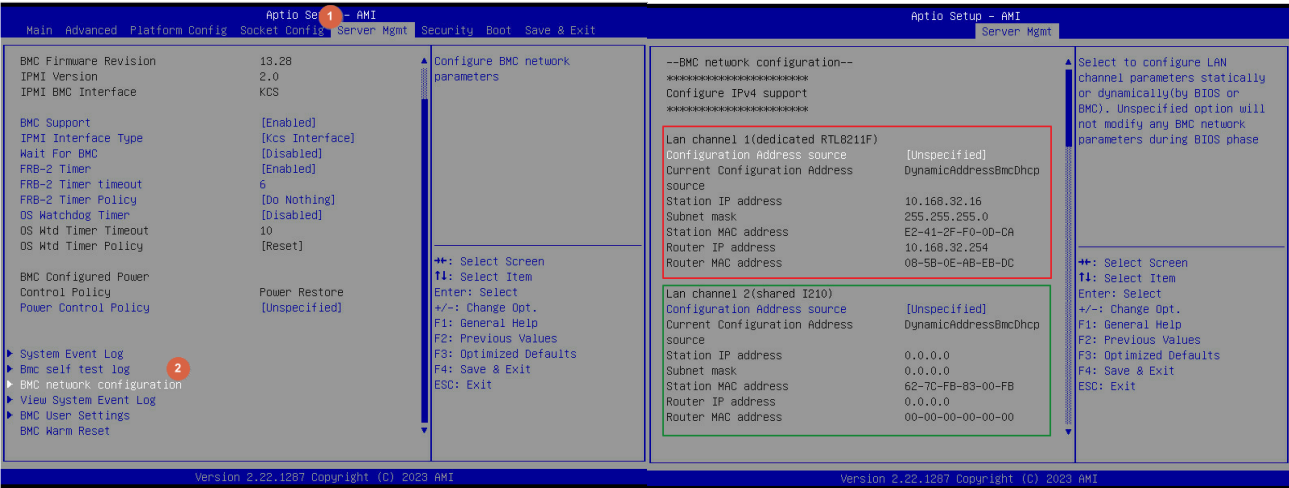
NC-SI, is an electrical interface and protocol defined by the Distributed Management Task Force (DMTF). The NC-SI enables the connection of a baseboard management controller (BMC) to network interface controllers (NICs) in a server computer system for the purpose of enabling out-of-band system management.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

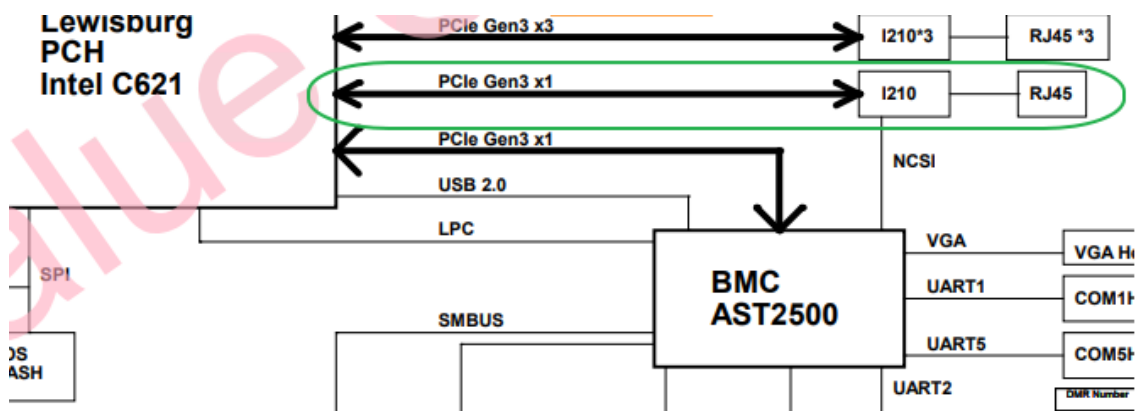
HPM-SRSUA



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.