HPM-SRSUA IPMI Setup User's

Manual

1st Ed -16 March 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, 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

We reserve 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. We assume 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. We make no representation or warranty that such application will be suitable for the specified use without further testing or modification.

Life Support Policy

Our PRODUCTS ARE NOT FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE PRIOR WRITTEN APPROVAL.

As used herein:

- 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

Customer Services

Each 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 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.

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

Technical Support

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

first.

Product Warranty

We warrant 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 authorized personnel, or which have been subject to misuse, abuse, accident or improper installation. We assume no liability under the terms of this warranty as a consequence of such events. Because of our high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If any of our 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:

- Collect all the information about the problem encountered. (For example, CPU type and speed, our 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

Gloss	ary & Abbreviation	6		
1. HAI	RDWARE	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. WE	B 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		
APPE	NDIX-A BMC HARDWRE: AST2600	99		
APPE	NDIX-B IPMI COMMANDS SUPPORT TABLE	102		
APPE	NDIX-C IPMI OEM COMMANDS LIST	107		
APPE	NDIX-D SENSOR TABLE	108		
APPE	NDIX-E DEFAULT CONFIGURATION	110		
APPE	NDIX-F FIRMWARE UPDATE	111		
APPENDIX-G SMART FAN CONFIGURATION128				
APPE	NDIX-H SYSTEM EVENT LOG(SEL)	130		
APPENDIX-I IPMI TO GET BIOS POST CODE135				
APPE	APPENDIX-J REMOTE CONTROL-Serial Over LAN137			
APPE	APPENDIX-K Dedicated vs Shared IPMI port138			

Glossary & Abbreviation

Glossary & Abbreviation	Explanation		
DMC	Baseboard Management Controller, this is the common abbreviation for		
DIVIC	an IPMI Baseboard Management Controller		
DMC	Integrated Baseboard Management Controller, this is the name for the		
DIVIC	2nd generation of BMC hardware, we use AST2600 on Platform		
IMM	Integrated Management Module, this means the same as BMC		
	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		
SOL	for remote control and management		
סחפ	Sensor Data Record, A data record that provides platform management		
	sensor type, locations, event generation, and access information		
	Ability to share a serial connector between the BMC's serial controller		
Serial Port Sharing	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		
	Vital Product Data, this is the term given to system component		
VPD	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		
IEDD	Internal Error. A signal from the Intel Architecture processors indicating		
	an internal error condition		
DEDD	Parity Error. A signal on the PCI bus that indicates a parity error on the		
	bus		
CEDD	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		

User's Manual



1.1 SYSTEM SPEC

Refer to Figure 1-1. System Block Diagram.



Figure 1-1 System block diagram

1.2 PLATFORM AND BMC COMPONENTS

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

Table 1-1 Main component related to BMC

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.

Physical	Bus ID (chan	nel no		BMC uso2	
Bus	+	s	lave address		Remark
Number	bus ID + bus	type)		(•)	
4	0.2		0x9C	V	Inlet Thermal Sensor
1	0.02		0x98	v	X550AT2 Thermal Sensor
2	0x4		0x9A	v	Outlet Thermal Sensor
2	084		0x9E	V	HDD Thermal Sensor
			0xC4	v	VCORE CPU0
3	0x6		0xE4	v	VCCINFAON CPU0
			0xE0	V	VCCD HV CPU0
				N	CLOCK GEN
4	0x8		UXDO	v	RENESAS 5P35023
4				V	CLOCK GEN
			UXD2		RENESAS 9SQ440
5	0xA		0xB0	v	PMBus PSU Header
6	0xC		0xAE		VPD
7	0xE	0xEC	PCA9546APW Channel 0	v	PCIE Slot 1
		PCAS	546APW Channel 1		PCIE Slot 2

Table 1-2 Master Write-Read Bus IDs

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

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: <u>https://<BMC IP></u> 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

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

₫

A

🗘 Sync 🛛 🔁 Refresh

sh 🔹 👤 admin 🗸

	Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the
	Logs and Reports page.
A	Click the icon to view the notification received
🗘 Sync	Click the icon to synchronize with Latest Sensor and Event Log updates.
🔁 Refresh	Click the icon or pressing key F5 to reload the current page.

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

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 Un Time	Timer that keep on accumulated while System on. Flash BMC f/w will reset this to
System op Time	zero.
Power On Hours	Power-On Hours will keep on accumulated and will be reset to zero when you
Power-On Hours	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
Today	view the event logs
20 Dave	This list event logs occurred by the different sensors within 30 days, click details
SU Days	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.

MEGARAC SP-X	≡	Sync	c CRefresh 💄 admin 🗸
Eirmware Information 0.01.20230303 BIOS Version 0.10 CPLD Version	Sensor Reading Live reading of all sensors		# Home > Sensor Reading
02 Host Online	□ Critical Sensors (0)		
Quick Links	GAll threshold :	sensors are normal	
# Dashboard	Discrete Sensor States (18)		
🚳 Sensor	Sensor Name	State	
FRU Information	& ACPL State	S5/G2 'Soft Off'	
🔟 Logs & Reports 💙	BMC Watchdog	No state defined	
Settings	BMC_Boot_Up	Device Enabled	
Remote Control	CPLD_CRC_Error	No state defined	
Image Redirection	를 CPU_Mismatch	No state defined	
O Power Control	≣ CPU_Power_Fault	No state defined	
🗲 Maintenance	GPU_Thermtrip	General Chassis Intrusion	
🕒 Sign out	킄 CPU_VR_HOT	General Chassis Intrusion	

Sensor Name	Reading	Behavior
¢ CPU1-T	35 °C	
JIMM1-T	0 °C	
JIMM2-T	0 °C	
I DIMM3-T	0 °C	
JIMM4-T	35 °C	
I DIMM5-T	0 °C	
LIMM6-T	0 °C	
FAN0_Speed	4200 Rpm	
J _{4•} P12V	12.10 Volts	
J _⊷ P1V05_PCH	1.05 Volts	
J⊷ P1V8_AUX	1.81 Volts	
-/⊷ P3V3	3.30 Volts	

♣ FAN0_Speed	4300 Rpm	
J⊭ P12V	12.10 Volts	
J⊷ P1V05_PCH	1.06 Volts	
J⊷ P1V8_AUX	1.81 Volts	
J⊭ P3V3	3.30 Volts	
J⊷ P3V_BAT	3.05 Volts	
J⊷ P5VA	5 Volts	
JM PSVS	5 Volts	
PCH-T	38 °C	

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.

MEGARAC SP-X		S - English 🔹 🗘 Sync 😂 Refresh	n 🎗 admin -
Errowarc Information 0.01.20230303 BIOS Version 0.10 CPLO Version 02 Host Online	Sensor detail All information about this sensor	🏟 Home > Sensor Re	ading > Sensor detail
Quick Links	1	40 °C	
# Dashboard		Upper Non-Recoverable	NA
øða Sensor		Upper Critical	98 °C
		Upper Non-Critical	97 °C
FRU Information	Ç.	Lower Non-Critical	NA
Logs & Reports		Lower Critical	NA
Settings		Lower Non-Recoverable	NA
Remote Control	0.00		
Image Redirection	Time (HH:MM:SS)		
එ Power Control	Sensor Events		
✗ Maintenance	٥		
🕒 Sign out			

18 HPM-SRSUA User's Manual

2.4 HOME> FRU INFORMATION

This page display FRU information that be stored in eeprom

FRU Field Replacable Units					# Home > FRU
Available FRU Devices					0
FRU Device ID					
Chassis Information	m_110	Board Information		Product Information	
Chassis Information Area Format Version	0	Board Information Area Format Version	1	Product Information Area Format Version	1
Chassis Type		Language	25	Language	25
Chassis Part Number		Manufacture Date Time	Fri Dec 30 00:00:00 2022	Product Manufacturer	Avalue Technology
Chassis Serial Number		Board Manufacturer	Avalue Technology	Product Name	0000000000000
Chassis Extra		Board Product Name	HPM-SRSUA-A2	Product Varian	00000000001
		Board Serial Number	0123456789012345678901234567890123456789	Product Serial Number	1234567890
		Board Part Number	00000000001	Asset Tag	
		FRU File ID	1.0	FRU File ID	1.0
		Board Extra		Product Extra	
FRU device ID	Select th	e device ID from	n the drop down lis	st	
FRU Device Name	The nam	e of eeprom that	store FRU informati	on	
	GS & RE	PORTS			

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 O Filter by type All Events UTC Offset: GMT - 7:0	✓ All Sensors ✓
	Event Log: 225 out of 226 event entries
224 - 206 -	ID: 226 Unknown sensor of type OEM_RECORD logged a oem timestamped OB hours ago
192 - 176 - 160 -	D: 225 Unknown sensor of type os_boot logged a c boot completed @8 hours ago
128 - 112 - 96 -	ID: 224 BIOS sensor of type bios_post_progress logged a progress O8 hours ago
60 - 64 - 48 - 32 -	ID: 223 BIOS sensor of type bios_post_progress logged a progress O® hours ago
16 0 May 2022	ID: 222 BIOS sensor of type bios_post_progress logged a progress O8 hours ago
	ID: 221 BIOS sensor of type bios_post_progress logged a progress OB hours ago
Event Logs Statistics	

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

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

System Log All system event logs	
	0
Filter by Date Start Date O - End Date O Event Category Alert ~	
System Log: 2 out of 2 event entries	
ID: 1 May 24th 2022, 9:26:29 am AMI00045F798341 kernel: kernel [7.240000] Helper Module Driver Version 1.2 -	
Di: 2 May 24th 2022, 9:26:29 am AMI00045F798341 kernel: kernel - [7.240000] Copyright (c) 2009-2015 American Megatrends Inc	

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

2.5.3 Home> Logs & Reports >Audit Log

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

Audit Log All audit logs	0
Filter by Date Start Date O - End Date O	
Audit Log: 5 out of 5 event entries	
May 2022	
ID: 5 May 24th 2022, 10:44:48 am AMI00045F798341 spx_restservice [1559 : 1559 INFO]https Login from IP:192.168.1.2 user:admin -	
ID: 4 May 24th 2022, 10:43:49 am AMI00045F798341 spx_restservice: spx_restservice [1559 : 1559 INFO]HTTPS logout from IP:192.168.1.2 user:admin -	
ID: 3 May 24th 2022, 10:23:39 am AMI00045F798341 spx_restservice: spx_restservice [1559 : 1559 INFO]HTTPS logout from IP:192.168.1.2 user:admin -	
ID: 2 May 24th 2022, 9:54:56 am AMI00045F798341 spx_restservice: spx_restservice [1559 : 1559 INFO]https Login from IP:192.168.1.2 user:admin -	
ID: 1 May 24th 2022, 9:45:49 am AMI00045F798341 spx_restservice: spx_restservice [1559 : 1559 INFO]https Login from IP:192.168.1.2 user:admin -	
0	

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

2.5.4 Home> Logs & Reports >Video Log

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

Video Log All video event logs	Ø
Filter by Date Start Date O - End Date O	
Vide	to Log: 0 out of 0 event entries

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

2.6 HOME>	SETTINGS			
MEGARAC SP-X	=		US - English	▼ Ø Sync 📿 Refresh 💄 admin マ
Eirmware Information 0.01.20230303 BIOS Version 0.10	Settings Configure BMC options			🕷 Home > Settings
02 Quick Links	Captured BSOD	Date & Time	External User Services	W KVM Mouse Setting
# Dashboard # Sensor	Log Settings	Media Redirection Settings	Network Settings	PAM Order Settings
FRU Information Information Information	Platform Event Filter	¢\$ Services	SMTP Settings	SSL Settings
Settings		1 1	₿~	
Remote Control	System Firewall	User Management	IPMI Interfaces	
C Power Control				
🗲 Maintenance				
🕒 Sign out				

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**

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.	
SMTD Sottings	E-mail message is one of alert and set SMTP for e-mail transmission across IP	
SMIP Settings	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	
IDMI Interferen	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



		B	Save
--	--	---	------

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

General Settings

2.6.3 Home> Setting >External User Services

External User Service	S	*	Home > Settings >	External User Services
LDAP/E-Directory Settings	Active Directory Settings	RADIUS Settings		
2.6.3.1 Home> Setting	gs >LDAP/E-Directory S	Settings		
LDAP/E-Directory Se	ttings	₩ Home > Settings > Exten	nal User Settings > LI	DAP/E-Directory Settings
	.			

Role Groups

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

eneral LDAP Settings	
	0
Enable LDAP/E-Directory Authentication	
Encryption Type	
✓ No Encryption SSL StartTLS	
Common Name Type	
IP Address	
Server Address	
Port	
389	
Bind DN	
E.g., cn=admin,ou=login,dc=domain,dc=com	
Password	
Whitespace not allowed	
Search Base	
E.g., ou=login,dc=domain,dc=com	
Attribute of User Login	
cn	~
	B Save

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

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

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

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

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

To modify a Role Group, click on its name.

To delete a Role Group, click on the X icon present at the right top corner for that box.



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



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

eneral 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	

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

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

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

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

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

To modify a Role Group ,click on it

To delete a Role Group, click on the X present at the right top cornet of its box.



2.6.3.3.1 Home> Settings>External User Services>RADIUS Settings



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

General RADIUS Settings	
	•
Enable RADIUS Authentication	
Server Address	
1812	
Secret	
Enable KVM Access	
Enable VMedia Access	
	🖺 Save

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

32 HPM-SRSUA User's Manual

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

Advanced RADIUS Settings	
RADIUS Authorization	0
Radius configuration is not enabled.	
Administrator	
Operator	
User	
OEM Proprietary	
No Access	
	🖺 Save

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

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

2.6.4 Home>Settings>KVM Mouse Setting

WM Mouse Setting	
Mouse Mode Configuration	0
Mouse Mode Relative Positioning (Linux) Absolute Positioning (Windows) Other Mode (SLES-11 OS Installation)	
	🖺 Save

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

2.6.5 Home>Settings>Log Settings

Log Settings		♣ Home > Settings > Log Settings
\$	\mathbf{Q}_{0}^{0}	
SEL Log Settings Policy	Advanced Log Settings	

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

SEL Log Settings Policy	
Log Policy	0
Linear Storage Policy 🖌 Circular Storage Policy	
	🖺 Save

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

2.6.5.2 Home>	Settings>Log	Settings>Advanced	Log Settings
---------------	--------------	-------------------	--------------

Advanced Log Settings
0
✓ System Log
✓ Local Log
Remote Log
Port Type UDP TCP
File Size
50000
Rotate Count
0
Remote Log Server
Server IP or Hostname
Remote Server Port
0
✓ Enable Audit Log
🖺 Save

Item	Option	Description
System Log	~	Select Enable System Log to view all system events. Entries can be
		filtered base on their classification levels
Local Log	 ✓ 	Select local log to save the logs locally (BMC)
Remote Log	✓	Select remote log to save the logs in a remote machine.
Port Type	• UDP	Port type is supported with the enable of Remote Log. User can select
	• TCP	either UDP/TCP as per the requirement.
File Size		If Local log is selected ,specify the size of the file in bytes.
		Size ranges from 3 to 65535
		Log files are rotated when the size is larger than the mentioned
		bytes , with regards for the last rotation time interval(1 minute).
Rotate Count		When logged information exceeds the specified file size, the old log
		information automatically gets moved to back up files based on the
		rotate count value. If the rotate count is zero , the old log information
		gets cleared permanently each time.
---------------	--------	---
		Specify the remote server address to log system events.
Remote Log		Server address support the following:
Server		IP Address (Both IPv4 and IPv6 format).
		FQDN (Fully qualified domain name) format
Domoto Sonvor		Specify the port number to log system events
Remote Server		Note: If entering port number 0 , it will set port number as default. The
Port		default port number is 514
Enable Audit	~	Select Enchle Audit Log to view all audit events for this device
Log		Select Enable Addit Log to view all addit events for this device.
Save	🖺 Save	Click button to save the changes made

2.6.6 Home>Settings>Media Redirection



2.6.6.1 Home>Settings>Media Redirection>General Settings

Remote Media Support Mount CD/DVD Server IA ddress for CD/DVD Images Server IP or Host name Path in server eg. /opt/bmc/nfs Share Type for CD/DVD Infs cifs Domain Name Same settings for Harddisk Images Server IP or Host name Password Server IP or Host name Password Same settings for Harddisk Images Server IP or Host name Password Server IP or Host name Password Same settings for Harddisk Images Server IP or Host name Password Server IP or Host name <th>-</th> <th></th>	-	
Remote Media Support Mount CD/DVD Images Server IP or Host name Path in server eg./opt/bmc/nfs Share Type for CD/DVD Inf cffs Domain Name Password Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Same Type for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Share Type for Harddisk Images Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Share Type for Harddisk Images Same settings for Harddisk Images Same Type for Harddisk Images Same Type for Harddisk Images Jername Jername Jername Jath in server eg./opt/bmc/nfs Share Type for Harddisk Tot IS Comain Name Jername Jername Jath in server eg./opt/bmc/nfs Share Type for Harddisk Tot IS Comain Name Jername		0
Mount CD/DVD Server Address for CD/DVD Images Server IP or Host name Path in server e.g. /opt/bmc/nfs Jsername Jsername Same settings for Harddisk Images Server IP or Host name Address for Harddisk Server IP or Host name Address for Host	 Remote Media Support 	
Server IP or Host name Path in server eg./opt/Dmc/nfs ither Type for CD/DVD infs clfs Domain Name Isername Same settings for Harddisk Images Server IP or Host name value Same settings for Harddisk Images Server IP or Host name value in in server eg./opt/Dmc/nfs iserver IP or Host name batt in server eg./opt/Dmc/nfs istare Type for Harddisk in fs clfs bornain Name istare Type for Harddisk	Mount CD/DVD	
Server IP or Host name bath in server eg./opt/bmc/nfs isher Type for CD/DVD frs	Server Address for CD/DVD Images	
Path in server eg. /opt/bmc/nfs share Type for CD/DVD	Server IP or Host name	
eg./opt/bmc/nfs share Type for CD/DVDnfscifs Domain Name Jsername Same settings for Harddisk Images Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Share Type for Harddisknfs	Path in server	
share Type for CD/DVD nfs cifs Jsername Jsername Same settings for Harddisk Images Mount Harddisk Server IP or Host name Sath in server eg./opt/bmc/nfs Share Type for Harddisk or ifs Somain Name Jsername Jser	eg. /opt/bmc/nfs	
nfs cfs Domain Name Jsername Password Same settings for Harddisk Images Server IP or Host name Path in server eg./opt/bmc/nfs Share Type for Harddisk on fs	Share Type for CD/DVD	
Domain Name Jsername 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 onsignation offs Domain Name Jsername Jsername Password Retry Interval 15 Retry Count 3	nfs cifs	
Jsername 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 onfs	Domain Name	
Jsername Password Same settings for Harddisk Images Mount Harddisk Server IP or Host name Server IP or Host name g_,opt/bmc/nfs Share Type for Harddisk of s Comain Name Jsername Jsername Jsername Jsername 15 Retry Count 3		
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 Jsername Password Setry Interval 15 Retry Count 3	Jsername	
Password Same settings for Harddisk Images Image: Comparison of the set of the		
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 nfscifs Domain Name Jsername Password Retry Interval 15 Retry Count 3	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 Jsername Jsername Password Retry Interval 15 Retry Count 3		
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 nfscifs Domain Name Jsername Password Retry Interval 15 Retry Count 3		
Mount Harddisk Server Address for Harddisk Images Server IP or Host name Path in server eg. /opt/bmc/nfs Share Type for Harddisk onfs offs cifs Domain Name Jsername Password Retry Interval 15 Retry Count 3	Same settings for Harddisk Images	
Server Address for Harddisk Images Server IP or Host name Path in server eg, /opt/bmc/nfs Share Type for Harddisk	V Mount Harddisk	
Server Address for Harddisk images Server IP or Host name Path in server eg. /opt/bmc/nfs Share Type for Harddisk		
Path in server eg. /opt/bmc/nfs Share Type for Harddisk nfs cifs Domain Name Username Password Retry Interval 15 Retry Count 3	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		
eg, /opt/omc/nis Share Type for Harddisk nfscifs Domain Name Username Password Retry Interval 15 Retry Count 3	Path in server	
Share Type for Harddisk	eg. /opt/bmc/nts	
Domain Name Username Password Retry Interval 15 Retry Count 3	Share Type for Harddisk	
Domain Name Username Password Retry Interval 15 Retry Count 3		
Username Password Retry Interval 15 Retry Count 3	Jomain Name	
Username Password Retry Interval 15 Retry Count 3		
Password Retry Interval 15 Retry Count 3	Jsername	
Password Retry Interval 15 Retry Count 3		
Retry Interval 15 Retry Count 3	Password	
Retry Interval 15 Retry Count 3		
15 Retry Count 3	Retry Interval	
3	15	
3	Retry Count	
	3	
		E) - c

User's Manual

ltem	Option	Description
		To enable or disable Remote Media support ,check or uncheck this box.
		If it is selected ,then the following remote media types will be displayed
		CD/DVD
Remote Media		Hard disk
Support		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.
	~	To enable or disable Mount CD/DVD support ,check or uncheck this
Mount CD/DVD		box.
		Address of the server where remote videos are to be stored. We support
Server Address		the following:
for CD/DVD image		 IPv4/IPv6 format.
g		 FQDN(Fully gualified domain name) format
		Path must be alpha-numeric and the following special characters are
Path in server		only allowed:
		·// ·// · · · · · · · · · · · · · · · ·
Share Type for	● nfs	
	• cifs	Share Type of the remote media server : either NFS or Samba(CIFS).
Domain Name		
		If Share Type is Samba(CIFS) , then enter user credentials to
Username		authenticate the server.
		Note: Domain Name field is optional.
Password		
1 433 WOI'U		
		If the option is checked, then the server information entered for
Same settings for		If the option is checked, then the server information entered for
Same settings for Harddisk images		If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type
Same settings for Harddisk images		If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type as well.
Same settings for Harddisk images Mount Harddisk		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. To enable or disable Mount Harddisk support ,check or uncheck this
Same settings for Harddisk images Mount Harddisk		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. To enable or disable Mount Harddisk support ,check or uncheck this box.
Same settings for Harddisk images Mount Harddisk Server Address		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. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored.
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk		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. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk images		If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type as well. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk images		If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type as well. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format Path must be alpha-numeric and the following special characters are only allowed:
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk images Path in server		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. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format Path must be alpha-numeric and the following special characters are only allowed:
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk images Path in server		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. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format Path must be alpha-numeric and the following special characters are only allowed: '/', 'V', '-', '_', '.', ''.'
Same settings for Harddisk images Mount Harddisk Server Address for Harddisk images Path in server Share Type for	 nfs nfs 	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. To enable or disable Mount Harddisk support ,check or uncheck this box. Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format Path must be alpha-numeric and the following special characters are only allowed: '7', '\', '\-, '\', '\', '\', '\', '\', '\

Domain Name		
		If Share Type is Samba(CIFS), then enter user credentials to
Username		authenticate the server.
		Note : Domain Name field is optional.
Password		
Betweelertermeel		Specify the Retry Interval and range should be from 15 to 30.Default
Retry Interval		value will be 15
Detry Count		Specify the Retry Count and range should be from 3 to 6. Default value
Retry Count		will be 3
System Log	~	Select Enable System Log to view all system events. Entries can be
System Log		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

	G
CD/DVD device instances	
1	~
lard disk instances	
1	~
Remote KVM CD/DVD device	instances
1	~
Remote KVM Hard disk insta	nces
1	~

Item	Option	Description
CD/DVD device instances	0.4	Select the number of CD/DVD devices that are to be
CD/DVD device instances	0-4	supported for Virtual Media redirection
Hand diels instances	0.4	Select the number of Hard disk devices to be supported for
Hard disk instances	0-4	Virtual Media redirection
Remote KVM CD/DVD device	0.4	Select the number of Remote KVM CD/DVD devices that are
instances	0-4	to be supported for Virtual Media redirection
Remote KVM Hard disk	0-4	Select the number of Remote KVM Hard disk devices that

40 HPM-SRSUA User's Manual

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

2.6.6.3 Home>Settings>Media Redirection>Remote Session

emote Session	
	0
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	
	🖪 Save

Item	Option	Description
KVM Single Port	~	Check this option to enable Single Port Application support in
Application		BMC
Keyboard Language		Select the Keyboard Language
Bothy Count	1 to 20	Number of times to be retried when a KVM failure occurs.
Retry Count	1 10 20	Retry count ranges from 1 to 20
Retry Time	E to 20	Number of seconds to wait for subsequent retries. Time
Interval(Seconds)	5 10 30	interval ranges from 5 to 30 seconds
Server Monitor OFF	~	Check this option to opphic the Server Meniter OFF feeture
Feature Status		Check this option to enable the Server Monitor OFF leature
Automatically OFF		Check this option to opphic Automotically OFE Server
Server Monitor, When		Meniter when K/(M is lounghed
KVM Launches		
Save	🖺 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 Redire	ctions			🖨 Home > Settings > Media F	dia Redirection > Active Redi		
						0	
No Media has been re	directed.						
Media Type 🗢	Media Instance 🗢	Client Type 🗢	Image Name 🖨	Redirection Status 🗢	Client IP 🖨		

2.6.7 Home>Settings>Network Settings



Network IP Settings	
	0
Chable LAN	
LAN Interface	
eth0	~
MAC Address	
00:04:5F:79:83:41	
Enable IPv4	
Enable IPv4 DHCP	

2.6.7.1 Home>Settings>Network Settings>Network IP Settings

IPv4 Address
192.168.1.6
IPv4 Subnet
255.255.255.0
IPv4 Gateway
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

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

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

2.6.7.2 Home>Settings>Network Settings>Network Link Configuration

	Ø
LAN Interface	
eth0	~
✓ Auto Negotiation	
Link Speed	
1000 Mbps	
Duplex Mode	
FULL Duplex	
NCSI Interface	
Enabled	

Network Link Configuration

User's Manual

ltem	Option	Description		
	ath0	Select the network interface for which the Link speed and		
LAN Interface	euro	duplex made are to be configured.		
		This option is enabled to allow the device to perform		
Auto Negotiation		automatic configuration, allowing it to achieve the best		
		possible mode of operation (speed and duplex)over a link.		
	• 10	Link speed options are dependent on the capabilities of the		
Link Speed	• 100	network interface. Speed can be 10/100/1000 Mbps.		
	• 1000	Note:Link speed of 1000Mbps is not applicable when Auto		
	 (Auto Negotiation) 	Negotiation is set to OFF		
		Select any one of the following duplex modes.		
Duplex Mode	Full duplex	Halt duplex		
		Full duplex		
NCSI Interface		NCSI interface Enable/Disable		
Save	🖺 Save	Click button to save the changes made		

2.6.7.3 Home>Settings>Network Settings>DNS Configuration



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

User's Manual

Setting	 Manual 	automatically.		
		If Automatic is selected ,the this field automatically display the		
Host Name		hostname.		
		Otherwise, please enter the desired hostname for the device.		
Register BMC		Check this box to enable Register BMC		
		Nsupdate-Register with the DNS server using the nsupdate		
		application		
		DHCP client FQDN-Register with the DNS server using		
Pagistration		DHCP option 81		
Registration		Hostname-Register with the DNS server using DHCP option		
metriod		12		
	 Hostname 	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.		
Poth	~	Check this box to modify TSIG authentication for both		
Both		interfaces.		
TSIG		Check this hay to apple TSIG Authoptication if registering		
Authentication		DNS via neurodate only		
Enabled(Eth0)				
New TSIG Private		Browse for a new TSIG private file to be uploaded to the BMC		
File(Eth0)		blowse for a new 1516 private life to be uploaded to the bind		
TSIG	~	Check this box to enable TSIG authentication – if registering		
Authentication		DNS via nsundate only		
Enabled(Eth1)				
New TSIG Private	E	Browse for a new TSIG private file to be uploaded to the BMC.		
File(Eth1)				
Domain Setting	Automatic	Select whether the domain interface will be configured		
g	Manual	manually or automatically.		
Domain Name		Displays the domain name of the device, or ,if 'Manual' was		
		selected, specify the domain name of the device.		
Domain Name	Automatic	Select whether the DNS interface will be configured manually		
Sever Setting	Manual	or automatically.		
DNS Server 1		Specify the DNS(Domain Name System) server address to be		
		configured for the BMC.		
DNS Server 2		IPv4 addresss should be given in dotted decimal		
		representation.		

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

2.6.7.4 Home>Settings>Network Settings>Sideband Interface

	8
NCSI Mode	
Auto Failover Mode Manual Switch Mode	
NCSI Interface	
eth0	~
Package ID	
0 (active)	~
Channel Number	

Item	Option	Description	
	Auto Failover Mode		
	Manual Switch Mode		
NCSI Interface	otb0	Choose the interface name for which to configure NCSI	
NCSI IIIteriace	ento	settings	
Deekene ID		Choose the package ID to be configured for the selected	
r ackage ib		interface.	
Channel Number		Choose the channel number to be configured for the	
		selected interface.	
Save	🖺 Save	Click button to save the changes made	

Sideband Interface (NC-SI)

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.

uthentication Or	ler	
	IPMI	
	LDAP	
	ACTIVE DIRECTORY	
	RADIUS	

2.6.9 Home>Settings>Platform Event Filter



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 Filte	rs						Home > Settings > Platform Event Filters >	Event Filters
⊖ All ● Conf	igured \bigcirc UnConfigured							0
	PEF ID: 1 (Enabled) when All Sensors switches to any severity run Alert (1) & none	•	PEF ID: 2 (Enabled) when All Sensors switches to any severity run Alert (2) & none	°	PEF ID: 3 (Enabled) when All Sensors switches to any severity run Alert (3) & none	•	PEF ID: 4 (Enabled) when All Sensors switches to any severity run Alert (4) & none	8
	PEF ID: 5 (Enabled) when All Sensors switches to any severity run Alert (5) & none	•	PEF ID: 6 (Enabled) when All Sensors switches to any severity run Alert (6) & none	°	PEF ID: 7 (Enabled) when All Sensors switches to any severity run Alert (7) & none	•	PEF ID: 8 (Enabled) when All Sensors switches to any severity run Alert (8) & none	0
	PEF ID: 9 (Enabled) when All Sensors switches to any severity run Alert (9) & none	•	PEF ID: 10 (Enabled) when All Sensors switches to any severity run Alert (10) & none	°	PEF ID: 11 (Enabled) when All Sensors switches to any severity run Alert (11) & none	•	PEF ID: 12 (Enabled) when All Sensors switches to any severity run Alert (12) & none	0
	PEF ID: 13 (Enabled) when All Sensors switches to any severity run Alert (13) & none	•	PEF ID: 14 (Enabled) when All Sensors switches to any severity run Alert (14) & none	◦	PEF ID: 15 (Enabled) when All Sensors switches to any severity run Alert (15) & none	۵		

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

Event Filter Configuration

	0
—	
Enable this filter	
Event severity to trigger	
Any severity	~
Event Filter Action Alert	
Power Action	
None	~
Alert Policy Group Number	
1	~
Raw Data	
Conceptor ID 1	
255	
Generator ID 2	
200	
Generator Type	
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	
Frient Data 1 Compare 2	
Event Data 2 Compare 1	
0	
Event Data 2 Compare 2	
U	
Event Data 3 AND Mask	
0	
Event Data 3 Compare 1	
0	
Event Data 3 Compare 2	
0	

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

Sensor type Sensor Name	 All Sensors Voltage Temperature Fan Processor All Sensors +V12S_CPU1 +V5A 	Select the type of sensor that will trigger the event filter action.		
	•			
Event Options	All Events	Choose event option to be either All events or Sensor		
•	Sensor Events	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	0.255	This field is used to indicate wildcarded or compared bits.		
Mask	0-255	Value ranges from 0 to 255		
Event Data 1	0-255	This field is used to indicate whether each hit position's		
Compare1	0 200	comparison is an exact comparison or not		
Event Data 1	0-255	Value ranges from 0 to 255		
Compare2	0 200			
Event Data 2 AND	0-255	This field is used to indicate wildcarded or compared bits.		
Mask	0 200	Value ranges from 0 to 255		
Event Data 2	0-255	This field is used to indicate whether each hit position's		
Compare1	0 200	comparison is an exact comparison or not		
Event Data 2	0-255	Value ranges from 0 to 255		
Compare2	0 200			
Event Data 3 AND	0-255	This field is used to indicate wildcarded or compared bits.		
Mask	0.200	Value ranges from 0 to 255		
Event Data 3	0-255	This field is used to indicate whether each hit position's		
Compare1	0.200	comparison is an exact comparison or not		
Event Data 3	0-255	Value ranges from 0 to 255		
Compare2				
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 Polic	ies						Home > Settings > Platform Event Filters > Alert Po	alicie:
Ĵ	Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	Ŷ	Group: 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0
¢	Group: 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	° _	Group: 6 (Disabled) Always send alert to this destination LNN Channel: 1 Sent To: 0	°	Group: 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 8 (<i>Disabled</i>) Always send alert to this destination LNN Channel: 1 Sent To: 0	0
Ĵ	Group: 9 (<i>Disabled</i>) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0
Ĵ	Group: 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	°	Group: 1 (<i>Disabled</i>) Always send alert to this destination LAN Channel: 1 Sent To: 0	0

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

Alert Policies	e
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	
	~

54 HPM-SRSUA User's Manual

User's Manual

Item	Option	Description		
Policy Group	4.45	Choose a policy number that was configured		
Number	1-15	in the Event filter table		
Enable this alert	✓	Check the option 'Enable' to enable the policy		
		Choose any one of the Policy set values from		
		the list.		
		0- Always send alert to this destination		
		1- If alert to previous destination was		
		successful, do not send alert to this		
	 Always send alert to this 	destination. Proceed to next entry in this		
	destination	policy set.		
	 If previous successful, skip this 	2- If alert to previous destination was		
	and comtinue(if configured)	successful, do not send alert to this		
Policy Action	 If previous successful, switch 	destination. Proceed to next entry in this		
	to another channel (if	policy set that is to a different channel.		
	 If previous successful ,switch to methodo(if configured) 	3- If alert to previous destination was		
		successful, do not send alert to this		
		destination. Proceed to next entry in this		
	to methods(il conligured)	policy set that is to a different channel.		
		4- If alert to previous destination was		
		successful, do not send alert to this		
		destination. Proceed to next entry in this		
		policy set that is to a different destination		
		type.		
LAN Channel	1	Choose a LAN channel for the policy		
		Choose a destination from the configured		
		destination list.		
Destination Selector	1-15	Note: LAN Destinations have to be		
		configured – under Configuration->PEF->LAN		
		Destination		
Event Specific Alert	 Image: A start of the start of	Choose the box to specify an event specific		
String		Alert String		
		Choose from a set of values (all linked to		
		strings that are kept in the PEF configuration		
Alert String Key	1-40	parameters), to specify which is to be sent for		
		this Alert Policy entry.		

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

2.6.9.3 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

AN Destination Configuration	
	Ø
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	SNMP TrapE-Mail	Select destination type.
SNMP Destination Address		If Destination type is SNMP Trap, then give the IP address of the system that will receive the alert. Destination address will support IPv4/IPv6 format
BMC Username		If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. Note: Email address for the user has to be configured under Settings->Users Management.
Email Subject		These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email

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

2.6.10 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							0
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	=	

ervice Configuration		_	
	0		
Service Name			
web			
✓ Active			
Interface Name			
both	~		
Secure port			
443			
Timeout			
1800			
Maximum Sessions			
20			
	0		

Home>Settings>Services> Service Configuration

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

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

Home>Settings>Services> Service Sessions

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

Click on <a>Image: 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 Ses	ssions			🖨 Home	> Settings > Services >	Service Sessions
Active Session - W	/eb					
Session ID 🖨	Session Type 🗢	User ID 🖨	User Name 🗢	Client IP 🖨	Privilege 🗢	_
1*	Web HTTPS	2	admin	192.168.1.2	Administrator	8

2.6.11 Home>Settings> SMTP Settings

ATP Settings	
	6
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		Enter a valid 'Sender Email ID' on the SMTP Server. Maximum allowed size for Email ID is 64 bytes,which includes username and domain name.
Primary SMTP	~	Check this option to enable SMTP support for the BMC

Support		
		Enter the 'Machine Name' of the SMTP Server. This field is
		for information Purpose Only.
Primary Server Name		Machine Name is a string of 25 alpha-numeric characters
		maximu.
		Spaces and special characters are not allowed
		Enter the Server Address for the SMTP server
Primony Sonyor ID		Server address will support the following
Frindry Server iP		IPv4/IPv6 address format
		Host name format
		Specify the SMTP port
Primary SMTP port		Default port is 25
		Port value ranges from 1 to 65535
Primary Soouro		Specify the SMTP secure port
SMTP port		Default port is 465
SMIP por		Port value ranges from 1 to 65535
		Check the option 'Enable' to enable SMTP Authentication.
		Note: Support SMTP Server Authentication Types are:
		CRAM-MD5.
Brimony SMTD		LOGIN
Primary SMIP		PLAIN
Aumentication		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'
		Enter user name required to access SMTP Accounts.
		User Name can be of length 4 to 64 alpha-numeric
Primary Username		characters, '.' , '@' , '-' ,'_'
		It must start win an alphabetical character
		Other special characters are not allowed
		Enter the password for the SMTP User Account.
Primary Password		Password must be at least 4 characters long.
		White space is not allowed
		Note:This field will not allow more than 64 characters.
Primary SMTP	~	Check the option to enable the SMTP SSLTLS protocol
SSLTLS Enable		
Primary SMTP	~	Check the option to enable the SMTP STARTTLS protocol
STARTTLS Enable		

User's Manual

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

2.6.12 Home>Settings>SSL Settings

SSL Settings		₭ Home > Settings > SSL Settings
View SSL certificate	Generate SSI certificate	

2.6.12.1 Home>Settings>SSL Settings> View SSL Certificate

This page displays the Current Certificate Information.

iew 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

enerate SSL Certificate	
	6
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	```

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

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

2.6.12.3 Home>Settings>SSL Settings>Upload SSL Certificate



Item	Option	Description
Current Cortificate		The information of the Current Certificate and date/time of
Current Certificate		its upload will be displayed(read-only)
New Certificate		Browse and navigate to the new certificate file.
	~	Certificate file should be of pem type.
Current Private Key		Information for the current private key and date/time when
		it was uploaded will be displayed(read-only)

New Private Key	b	Browse and navigate to the private key file. Private key file should be of pem type.
Save	🖺 Save	Click button to save the changes made

2.6.13 Home>Settings>System firewall

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

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

	e
Block All	
IPv4	
Flush All	
Timeout	
Start Date	
YYYY/MM/DD	m
Start Time	
	0
End Date	
YYYY/MM/DD	
End Time	

Item	Option	Description
Block All	 IPv4 IPv6 Both 	This option will block all incoming IPs and Ports
Flush All	~	This option is used to flush all existing system firewall rules
Timeout	~	This option is used to enable or disable firewall rules with timeout.
Start Date		The firewall rule will become effective from this date
Start Time	0	The firewall rule will become effective from this time
End Date		The firewall rule will expire on this date
End Time	O	The firewall rule will expire at this time
Save	🖺 Save	Click button to save the changes made

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

	6
IP Single (or) Range Start	
IP Range End	
optional	
Enable Timeout	
Start Date	
YYYY/MM/DD	**
Start Time	
	4
End Date	
YYYY/MM/DD	
End Time	
	J
Rule	

ltem	Option	Description
IP Single (or) Range Start		This field is used for entering an IP address or the start of a range of IP addresses. IP address must follow the IPv4 format.
IP Range End		This field is used to indicate the IP address or end of an IP address range
Enable Timeout	~	This option is used to enable or disable timeout
Start Date	Ê	The firewall rule will become effective from this date
Start Time	0	The firewall rule will become effective from this time

End Date	Ê	The firewall rule will expire on this date
End Time	0	The firewall rule will expire at this time
Rule	AllowBlock	This field is used for allow or block this rule.
Save	🖺 Save	Click button to save the changes made

2.6.13.5 Home>Settings>System Firewall >Port Firewall Rules

Port Firewall Rules	倄 Home >	Settings > Firewall > Port Fire	ewall Rules
\$	+		
Existing Port Rules	Add New Port Rule		

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

	6
Port Single (or) Range Start	
Port Range End	
optional	
Protocol	
ТСР	`
Network Type	
IPv4	
Enable Timeout	
Start Date	
YYYY/MM/DD	
Start Time	
	0
End Date	
YYYY/MM/DD	
End Time	
	0
Rule	

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

	● IPv6	
	Both	
Enable Timeout	~	This option is used to configure timeout support for the new
		rule.
Start Date		Click field to select the duration of filter
Start Time	0	Click field to select the duration of filter
End Date	**	Click field to select the duration of filter
End Time	0	Click field to select the duration of filter
Rule	AllowBlock	This field is used for allow or block this rule.
Save	🖺 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.



Item	Option	Description
	• 1	
Channel	• 2	
	• 8	

2.6.14.1 Home>Settings>User management> User Management Configuration

ser management comigaration	
	(
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	
Administrator	
KVM Access	
VMedia Access	
SNMP Access	
SNMP Access level	
NMP Authentication Protocol	
SNMP Privacy Protocol	
mail Format	
AMI-Format	
mail ID	
Existing SSH Kev	
Not Available	
Inload SSH Key	
abiana aoni neg	b
Delete	🖺 Sav

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

74 HPM-SRSUA User's Manual

User's Manual

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

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

2.6.15 Home>Settings>Video Recording

Video Recording		♣ Home > Settings > Video Recording
Auto Video Settings	SOL Settings	



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.

	6
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	

Item	Option	Description
Critical Events (Temperature/Voltage)	>	check/uncheck this option to add/remove Critical Events trigger
Non Critical Events	>	check/uncheck this option to add/remove Non Critical Events
(Temperature/Voltage)		trigger
Non Recoverable Events	>	check/uncheck this option to add/remove Non Recoverable Events
(Temperature/Voltage)		trigger
Fon state changed Events	>	check/uncheck this option to add/remove Fan state changed
Fail State Changed Events		Events trigger
Watchdog Timor Evonts	>	check/uncheck this option to add/remove Watchdog Timer Events
		trigger
Chassis Power On Events	~	check/uncheck this option to add/remove Chassis Power On
		Events trigger
Chassis Dower Off Events	~	check/uncheck this option to add/remove Chassis Power Off
		Events trigger
Chassis Posot Evonts	~	check/uncheck this option to add/remove Chassis Reset Events
		trigger
LPC Reset Events	~	check/uncheck this option to add/remove LPC Reset Events trigger
Data and Time Events	~	check/uncheck this option to add/remove Date and Time Events
Date and Time Events		trigger
Pro Event Video Decording	~	check/uncheck this option to add/remove Pre-Event Video
FIE-EVENT VIDEO RECORDING		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

	0
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	

🖺 Save Item Option Description This option is to enable/disable Remote Video support. **Record Video to Remote** Note: By default ,video files will be stored in the local path of the \checkmark Server 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 1-100 **Maximum Dumps** Maximum Dumps value should range from 1 to 100 1-3600 Maximum Duration (Sec) Maximum Duration should range from 1 to 3600 sec 1-500 Maximum Size should range rom 1 to 500 MB Maximum Size (MB) Address of the server where remote videos are to be stored. We support the following: Server Address IP Address (both IPv4 and IPv6 format). FQDN(Fully qualified domain name) format. Path must be alpha-numeric and the following special Path in server characters are only allowed `/` , `\` , `-` , `_` , `.` , `:` NFS Share Type of the remote video server:NFS or Samba(CIFS) are Share Type •

	• 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

	8
This page is used to configure the Pre-Event video recording options. I default.	Pre-Event video recording is disabled by
To enable the Pre-Event video recording, go to the <u>Triggers Configura</u>	<u>tion</u> page.
Video Quality	
Very Low	``````````````````````````````````````
Compression Mode	
High	
Frames Per Second	
1	
/ideo Duration	
10	

🖺 Save

Item	Option	Description
	Very Low	
	• Low	Choose the desired video quality from the options in the
Video Quality	Average	dron down list
	Normal	diop-down list
	● High	
Compression Mode	● High	
	Normal	Select the Compression Mode from the options listed in the
	• Low	drop-down list
	● no	
Fromos Dor Second		Choose the FPS to specify the desired number of frames per
Frames Per Second	1-4	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

	Sol Settings		♣ Home > Settings > Video > Sol Se	ttings.
SOL Trigger Settings SOL Video Settings SOL Recorded Video	SOI Trigger Settings	SOL Video 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

			🖺 Save			
	Date and Tim	e Event				
	LPC Reset Eve	ents				
	Chassis Reset	Events				
	Chassis Powe	r Off Events				
Chassis Power On Events						
	Watchdog Tin	ner Events				
	Fan state cha	nged Events				
	Non Recovera	able Events (Temperature/Voltage)				
	Non Critical E	vents (Temperature/Voltage)				
	Critical Event	s (Temperature/Voltage)				
			-			

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

(Temperature/Voltage)		
Non Critical Events	>	check/uncheck this option to add/remove Non Critical Events
(Temperature/Voltage)		trigger
Non Recoverable Events	>	check/uncheck this option to add/remove Non Recoverable Events
(Temperature/Voltage)		trigger
Fon state changed Events	>	check/uncheck this option to add/remove Fan state changed
Fan state changed Events		Events trigger
Watabdag Timor Evanta	>	check/uncheck this option to add/remove Watchdog Timer Events
		trigger
Chassis Power On Events	>	check/uncheck this option to add/remove Chassis Power On
Chassis Fower On Events		Events trigger
Chassis Power Off Events	>	check/uncheck this option to add/remove Chassis Power Off
Chassis Fower On Events		Events trigger
Chassis Poset Events	>	check/uncheck this option to add/remove Chassis Reset Events
		trigger
I PC Reset Events	~	check/uncheck this option to add/remove LPC Reset Events trigger
Date and Time Events	~	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

OL Video Settings	
0	
	0
Log Size (KB)	
128	
Log File Count	
1	
Record Video to Remote Server	

🖺 Save

Item	Option	Description
		Enter the preferred size for the log file. Maximum log file size is
		128KB.

User's Manual

Log File Count		Enter whether you want to have log files. Maxmum log file count	
		is 1	
		To enable or disable Remoe Video support, check or uncheck	
Papard Video to Pomoto		the 'Enable' checkbox respectively.	
		Note:By default video files will be stored in local path of BMC. If	
Server		remote video support is enabled then the video files will be	
		stored only in remote path, not within BMC.	
Save	🖹 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 deault , 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 dowload and save the file

Clock on icon to delete the selected video.

Sol Recorded video		Home > Settings > Video > Sol > Sol Recorded video
		0
S.No 🕈	File Name 🗢	File Information 🖨

2.7 HOME> REMOTE CONTROL

Remote Control Remote KVM & SOL	Home > Remote Control
	Θ
H5Viewer	
Click here to go to Remote Session Settings.	
C [*] Launch HSViewer	
Serial Over LAN	
C Activate	

2.7.1 Home>Remote Control >H5Viewer



3	MegaRAC	SP-X - G	oogle Chrome				_	\times
A	不安全	https:/	//10.168.32.21/#serial_0	over_lar	ı			
	關問	列	80	行	25			
								-
								-

2.7.2 Home>Remote Control >Serial Over LAN



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.

Remote Media Emulate CD/DVD/HDD images in the network to host as media through BMC								
					0			
					O Refresh Image List			
Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index				

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

User's Manual

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

2.10 HOME	E> MAINTENAN	CE		
MEGARAC SP-X	=		US - English	▼ © Sync 😌 Refresh 💄 admin 🗸
Firmware Information 0.01.20230303 BIOS Version 0.10 CRI D Version	Maintenance			₩ Home > Maintenance
02 Host Online	*	à	0	
Quick Links 🔻	Backup Configuration	Firmware Image Location	Firmware information	Firmware Update
# Dashboard		1	ن	_//~•
🚯 Sensor	Preserve Configuration	Restore Configuration	Restore Factory Defaults	Bios Post Code
6 FRU Information	.	يع		
Logs & Reports	System Administrator	Download Service Data	CPU Information	
Settings				
Remote Control				

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.

	6
Check All	
SNMP	
KVM	
Network & Services	
ІРМІ	
NTP	
Authentication	
SYSLOG	

Item	Option	Description
Check All	~	Set all following check box as checked
SNMP	>	Select this option to backup SNMP configuration
KVM	~	Select this option to backup KVM configuration

88 HPM-SRSUA User's Manual

User's Manual

Network & Services	>	Select this option to backup Network & Services configuration
ІРМІ	>	Select this option to backup IPMI configuration
NTP	~	Select this option to backup NTP configuration
Authentication	~	Select this option to backup Authentication configuration
SYSLOG	>	Select this option to backup SYSLOG configuration
Download	📩 Download	Click this button to backup selected config above as a file.

2.10.2 Home>Maintenance >Firmware Image Location

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



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

2.10.3 Home>Maintenance >Firmware Information

F	irmware Information	
	Active Firmware	0
	Build Date	
	Mar 29 2022	
	Build Time	
	13:25:12 UTC	
	Firmware version	
	0.04.20200508	
	BIOS version	
	0.02	
	CPLD version	
	0.1	

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

	0
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	
elect Firmware Image	
Choose File No file chosen	
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.

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

2.10.5 Home>Maintenance >Preserve Configuration

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

	0
lick here to go to Firmware Update or Restore	Factory Defaults
Check All	
SDR	
FRU	
SEL	
ІРМІ	
Network	
NTP	
SNMP	
SSH	
KVM	
Authentication	
Syslog	
Web	

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

SEL	✓	Checked this option to preserve SEL configuration
ІРМІ	~	Checked this option to preserve IPMI configuration
Network	>	Checked this option to preserve Network configuration
NTP	 ✓ 	Checked this option to preserve NTP configuration
SNMP	>	Checked this option to preserve SNMP configuration
SSH	~	Checked this option to preserve SSH configuration
кум	~	Checked this option to preserve KVM configuration
Authentication	>	Checked this option to preserve Authentication configuration
Syslog	~	Checked this option to preserve Syslog configuration
Web	>	Checked this option to preserve Web configuration
Save	🖺 Save	Click the button to save the changes made

2.10.6 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	
	0
Config File	
	🕒

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

Savo	E Savo	After select config file ,click the button to perform restore
Save	D Save	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.

		?
The fo	ollowing checked configurations will be preserved through the restore operation. You can make tes to the list in the preserve configuration page.	
5	SDR	
F	FRU	
S	SEL	
I	РМІ	
ľ	Network	
ľ	NTP	
S	SNMP	
S	SSH	
۲	KVM	
A	Authentication	
S	Syslog	
v	Neb	

Item	Option	Description
epp	>	Checked this option to preserve SDR configuration while Restore Factory
SDR		Defaults
EDU	>	Checked this option to preserve FRU configuration while Restore Factory
FRU		Defaults
С.	>	Checked this option to preserve SEL configuration while Restore Factory
JEL		Defaults

IDMI	>	Checked this option to preserve IPMI configuration while Restore Factory
		Defaults
Network	~	Checked this option to preserve Network configuration while Restore Factory
Network		Defaults
NTD	>	Checked this option to preserve NTP configuration while Restore Factory
		Defaults
	>	Checked this option to preserve SNMP configuration while Restore Factory
SINIVIP		Defaults
ссц	>	Checked this option to preserve SSH configuration while Restore Factory
330		Defaults
KV/M	~	Checked this option to preserve KVM configuration while Restore Factory
		Defaults
Authoptication	~	Checked this option to preserve Authentication configuration while Restore
Authentication		Factory Defaults
Syclog	~	Checked this option to preserve Syslog configuration while Restore Factory
Sysiog		Defaults
Wab	~	Checked this option to preserve Web configuration while Restore Factory
VVED		Defaults
Save	🖺 Save	Click the button to perform Restore Factory Defaults

2.10.8 Home>Maintenance > Bios Post code

Collect all post from Bios.

BIOS Post Co	de All BIOS post code		# Home >	Maintenance >	BIOS Post Code
					0
ID	Post Code	Message			
1	0x02	SEC-AP init before mc loading			
2	0x03	SEC-North Bridge Init before mc loading			
3	0x04	SEC-South Bridge init before mc loading			
4	0x05	SEC-OEM init before mc loading			
5	0x06	SEC-Microcode loading			
6	0x19	PEI-Pre-memory South Bridge Init is started			
7	0xA1	DXE-IDE Reset			
8	0xA3	DXE-IDE Enable			
9	0xA3	DXE-IDE Enable			
10	0xA7	DXE-SCSI Enable			
11	0xA9	DXE-Start of Setup			
12	0xA7	DXE-SCSI Enable			
13	0xA7	DXE-SCSI Enable			
14	0xA7	DXE-SCSI Enable			
<					

	6
Username	
sysadmin	
✓ Enable User Access	
Change Password	
Password	
Confirm Password	

2.10.9 Home>Maintenance >System Administrator

Item	Option	Description
Username		Username of the System Administrator is displayed(read only)
Enable Llear Access	>	Check/Uncheck this option to enable/disabled user access for the
Enable User Access		system administrator
Change Becowerd	>	Check this option to change the existing password. This will enable
Change Password		the password fields.
		Enter the new password here.
Descurerd		At least 8 characters long
Password		While space is not allowed
		More than 64 characters is not allowed
Confirm Decoword		Enter the same password which you have entered in the Password
Commin Password		field to comfirm it.
Save	🖺 Save	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.

0

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.

ОК	Cancel

APPENDIX-A BMC HARDWRE: AST2600

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

The chip architecture is showed below:



Figure A-1 AST2600 Chip Architecture

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

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

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

The more information can refer to the Datasheet of AST2600.

APPENDIX-B IPMI COMMANDS SUPPORT TABLE

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

Command	NetFn	CM D	M/ O	Supporte d	Comments
IPMI Device "Global"					
Commands					
Get Device ID	Арр	01h	Μ	V	
Broadcast 'Get Device ID'[1]	Арр	01h	Μ		
Cold Reset	Арр	02h	0	V	
Warm Reset	Арр	03h	0	V	
Get Self Test Results	Арр	04h	Μ	V	
Manufacturing Test On	Арр	05h	0	V	need password
Set ACPI Power State	Арр	06h	0	V	
Get ACPI Power State	Арр	07h	0	V	
Get Device GUID	Арр	08h	0	V	
Get NetFn Support	Арр	09h	0	V	
Get Command Support	Арр	0Ah	0	V	
Get Command Sub-function	۸nn	0Bb	0	V	
Support	Арр	UDII	0	v	
Get Configurable Commands	Арр	0Ch	0	V	
Get Configurable Command	۸nn	ODh	0	V	
Sub-functions	Арр	UDII	0	v	
Set Command Enables	Арр	60h	0		
Get Command Enables	Арр	61h	0	V	
Set Command Sub-function	۸nn	62h	0		
Enables	Арр	0211	0		
Get Command Sub-function	۸nn	63h	0		
Enables	Лүү	0311	0		
Get OEM NetFn IANA	Δnn	64h	0	V	
Support	лүү	0411	0	v	
BMC Watchdog Timer					
Commands					
Reset Watchdog Timer	Арр	22h	Μ	V	
Set Watchdog Timer	Арр	24h	Μ	V	
Get Watchdog Timer	Арр	25h	Μ	V	
BMC Device and Messaging					
Commands					
Set BMC Global Enables	App	2Eh	м	V	"Only Supported: SEL Logging Enable / Disable, Event message buffer
				-	Enable/disable"
Get BMC Global Enables	Арр	2Fh	М	V	
Clear Message Flags	Арр	30h	Μ	V	
Get Message Flags	Арр	31h	Μ	V	
Enable Message Channel		0.01	~		
Receive	Арр	32n	0	V	
Get Message	Арр	33h	Μ	V	
Send Message	App	34h	Μ	V	not support Send Raw
Read Event Message Buffer	App	35h	0	V	
Get BT Interface Capabilities	App	36h	Ō	V	
Get System GUID	Арр	37h	Ō	V	

102 HPM-SRSUA User's Manual

User's Manual

Get Channel Authentication	Ann	206	0	V	
Capabilities	Арр	380	0	V	
Get Session Challenge	App	39h	0	V	
Activate Session	App	3Ah	0	V	
Set Session Privilege Level	App	3Rh	0	V	
Close Session	App	20h	0	V	
	Арр	301	0	V	
Get Session Info	Арр	3Dh	0	V	
Get AuthCode	Арр	3Fh	0	V	
Set Channel Access	Арр	40h	М	V	"Only support: disabled, always availible, shared mode"
Get Channel Access	App	41h	М	V	
Get Channel Info Command	App	42h	0	V	
Set User Access Command	App	/3h	0	V	Not support user session limit
Get User Access Command	<u> </u>	4011 44h	0	V	
Set Lleer Neme	App	4411 45b	0	V	
	Арр	450	0	V	
Get User Name Command	Арр	46h	0	V	
Set User Password Command	Арр	47h	0	V	
Activate Payload	Арр	48h	0	V	
Deactivate Payload	Арр	49h	0	V	
Get Payload Activation Status	App	4Ah	0	V	
Get Payload Instance Info	App	4Bh	0	V	
Set Liser Payload Access	7.pp 	4Ch	0	V	
Cet Lleer Devleed Access	App	4011 4Db	0	V	
Get User Payload Access	Арр	4DN	0	V	
Get Channel Payload Support	Арр	4Eh	0	V	
Get Channel Payload Version	Арр	4Fh	0	V	
Get Channel OEM Payload	App	50h	0	V	
Info	Abb	5011	0	v	
Master Write-Read	App	52h	М	V	
Get Channel Cipher Suites	App	54h	0	V	
Suspend/Resume Payload	, .pp	• …	Ŭ	•	
Encryption	Арр	55h	0	V	
Set Channel Security Keye	Ann	FCh	0	V	
Set Channel Security Keys	Арр	100	0	V	
Get System Interface	App	57h	0	V	Only 01n(KCS) is supported
Capabilities				-	
Set System Info Parameters	Арр	58h	0	V	
Get System Info Parameters	Арр	59h	0	V	
Chassis Device Commands					
Get Chassis Capabilities	Chassis	00h	М	V	
Get Chassis Status	Chassis	01h	M	V	
ChassisControl	Chassie	02h	M	V	
ChassisControl	Chassis	0211	IVI	v	This command is combined to Chassis
Chassis Reset	Chassis	03h	0		Control command is combined to Chassis
			_		Control command in IPIVII V1.5
Chassis Identify	Chassis	04h	0	V	
Set Chassis Capabilities	Chassis	05h	0	V	
Set Power Restore Policy	Chassis	06h	0		
Get System Restart Cause	Chassis	07h	0	V	Only 01h (cycle,hardware reset), 04h,8h,9h supported
Set System Boot Options	Chassis	08h	0	V	
Get System Boot Options	Chassis	09h	Ō	V	
Set Front Panel Button	Chabble	0011	Ŭ	•	
Enables	Chassis	0Ah	0		
Set Dower Cycle Interval	Chassia	ODh	0	V	
Set Power Cycle Interval	Chassis		0	V	
Get POH Counter	Chassis	U⊢h	0	V	
Event Commands					
Set Event Receiver	S/E	00h	Μ	V	
Get Event Receiver	S/E	01h	Μ	V	
Platform Event (a.k.a. "Event	o /=	0.01			
Message")	S/E	02h	M	V	
PEF and Alerting					
Commande					
	0/5	105	N /	11	
Get PER Capabilities	3/E	TUN	IVI	V	

Arm PEF Postpone Timer	S/E	11h	Μ	V	
Set PEF Configuration	S/F	12h	м	V	Does not support parameter 15.
Parameters	0/L	1211	IVI	v	
Get PEF Configuration	S/F	13h	м	V	Does not support parameter 15.
Parameters	0/2	1011	101	v	
Set Last Processed Event ID	S/E	14h	Μ	V	
Get Last Processed Event ID	S/E	15h	Μ	V	
Alert Immediate	S/E	16h	0	V	
PET Acknowledge	S/E	17h	0	V	
Sensor Device Commands					
Get Device SDR Info	S/E	20h	0	V	
Get Device SDR	S/E	21h	0	V	
Reserve Device SDR	0/5	0.01	~		
Repository	S/E	ZZN	0	V	
Get Sensor Reading Factors	S/E	23h	0	V	Support linear sensors only.
Set Sensor Hysteresis	S/E	24h	0	V	
Get Sensor Hysteresis	S/E	25h	0	V	
Set Sensor Threshold	S/F	26h	Ō	v	
Get Sensor Threshold	S/F	27h	õ	V	
Set Sensor Event Enable	S/F	28h	õ	V	
Get Sensor Event Enable	S/F	29h	õ	V	
Re-arm Sensor Events	S/F	24h	õ	V	
Get Sensor Event Status	S/F	2Rh	0	V V	
Get Sensor Reading	S/E	2011 20h	M	v \/	
Set Sensor Type		2011 2Eh		V	
Cot Songer Type	S/E	2000	0	V	
Set Sensor Deading and	3/E	2511	0	v	Sanaar abould be eattable (just for EM
Set Sensor Reading and	S/E	30h	0	V	Sensor should be settable (just for FVV
Event Status					engineer debug purpose internaliy)
FRU Device Commands	Storage	10h	N/	V	
Get FRU Inventory Area Inio	Storage	100		V	
Read FRU Data	Storage	110	IVI	V	
Write FRU Data	Storage	12n	IVI	V	
SDR Device Commands	01	0.01			
Get SDR Repository Info	Storage	20h	M	V	
Get SDR Repository	Storage	21h	0	V	
Allocation	<u> </u>				
Reserve SDR Repository	Storage	22h	M	V	
Get SDR	Storage	23h	M	V	
Add SDR	Storage	24h	0	V	
Partial Add SDR	Storage	25h	M	V	
Delete SDR	Storage	26h	0		
Clear SDR Repository	Storage	27h	Μ	V	
Get SDR Repository Time	Storage	28h	0	V	
Set SDR Repository Time	Storage	29h	0		
Enter SDR Repository Update	Storage	2Ah	0		
Exit SDR Repository Update	Storage	2Bh	0		
Run Initialization Agent	Storage	2Ch	0	V	
SEL Device Commands					
Get SEL Info	Storage	40h	Μ	V	
Get SEL Allocation Info	Storage	41h	0	V	
Reserve SEL	Storage	42h	0	V	
Get SEL Entry	Storage	43h	Μ	V	
Add SEL Entry	Storage	44h	Μ	V	
Partial Add SEL Entry	Storage	45h	0	V	1
Delete SEL Entry	Storage	46h	Ō	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	0	v	
Set Auxiliary Log Status	Storage	5Rh	0		
Jost Auxiliary Log Status	Juliage	501		I	I I

User's Manual

Get SEL Time UTC Offset	Storage	5Ch	0	V	
Set SEL Time UTC Offset	Storage	5Dh	0	V	
LAN Device Commands	Clorage	0211	Ŭ		
Set I AN Configuration	Tranana				param #0, 25 are not support
Set LAN Configuration	Transpo	01h	Μ	V	param #9, 25 are not support
	- п -				10.05 · · · ·
Get LAN Configuration	Transpo	02h	М	V	param #9, 25 are not support
Parameters	rt	0211	IVI	v	
Sugnard DMC ADDa	Transpo	0.0 h	0	V	
Suspend BINC ARPS	rt	030	0	V	
	Transpo		_		
Get IP/UDP/RMCP Statistics	rt	04h	0		
Sorial/Modom Dovice	11				
Commands	-				
Set Serial/Modem	Transpo	10h	М	V	
Configuration	rt			•	
Get Serial/Modem	Transpo	116	N /	V	
Configuration	rt	1 1 1 1	IVI	v	
	Transpo	4.01	•		
Set Serial/Modem Mux	rt	12h	0	V	
	Transpo				
Get TAP Response Codes	rt	13h	0		
Set PPP UDP Proxy Transmit	Transpo	14h	0		
	rt		•		
Cot PPP LIDP Proxy Transmit	Transpo	15h	\circ		
Get FFF ODF FTOXy Hanshit	rt	1311	0		
	Transpo	4.01	0		
Send PPP UDP Proxy Packet	rt	160	0		
	Transpo				
Get PPP UDP Proxy Receive	rt	17h	0		
	11 Tanaana				
Callback	Transpo	19h	0		
Set User Callback Options	Transpo	1Ah	0		
	rt		-		
Get User Callback Options	Transpo	1Bh	0		
	rt	1 Dii)		
Set Serial Routing Mux	Transpo	10h	0		
Command	rt	TCH	0		
	Transpo				
SOL Activating	rt	20h	0		
Set SOL Configuration	Transno				param #7 is not support
Parameters	rt	21h	0	V	
	11 Tanaana				n ana na 117 ia na taona ant
Get SOL Configuration	Transpo	22h	0	V	param #7 is not support
Parameters	rt				
Command Forwarding					
Commands					
Forwarded Command	Transpo	30h	\cap		
Torwarded Command	rt	3011	0		
Cat Famula d Cammanda	Transpo	046	0		
Set Forwarded Commands	rt	310	0		
	Transpo				
Get Forwarded Commands	rt	32h	0		
Enchle Converded	Tranana				
Enable Forwarded	Transpo	33h	0		
Commands	rt				
Bridge Management					
Commands					
Get Bridge State	Bridge	00h	0		
Set Bridge State	Bridae	01h	0		
Get ICMB Address	Bridge	02h	Ō		
Set ICMB Address	Bridge	02h	$\overline{0}$		
Sot Bridge Brown Address	Bridge	0.15			1
Cet Dridge PluxyAddless	Dridge	040			
Get Bridge Statistics	Ruage	05h	U		

Get ICMB Capabilities	Bridge	06h	0	
Clear Bridge Statistics	Bridge	08h	0	
Get Bridge Proxy Address	Bridge	09h	0	
Get ICMB Connector Info	Bridge	0Ah	0	
Get ICMB Connection ID	Bridge	0Bh	0	
Send ICMB Connection ID	Bridge	0Ch	0	
Discovery Commands				
(ICMB)				
PrepareForDiscovery	Bridge	10h	0	
GetAddresses	Bridge	11h	0	
SetDiscovered	Bridge	12h	0	
GetChassisDeviceId	Bridge	13h	0	
SetChassisDeviceId	Bridge	14h	0	
Bridging Commands (ICMB)				
BridgeRequest	Bridge	20h	0	
BridgeMessage	Bridge	21h	0	
Event Commands (ICMB)				
GetEventCount	Bridge	30h	0	
SetEventDestination	Bridge	31h	0	
SetEventReceptionState	Bridge	32h	0	
SendICMBEventMessage	Bridge	33h	0	
GetEventDestination	Bridge	34h	0	
(optional)	Bhage	0411	0	
GetEventReceptionState	Bridae	35h	0	
(optional)	Bhago	0011	•	
Other Bridge Commands			_	
Error Report (optional)	Bridge	FFh	0	
OEM Commands for Bridge				
NetFn		0.01		
		C0h	~	
	Bridge	-FE	0	
		n		

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_FAN1pwm duty cycle Byte2 = SYS_FAN1pwm duty cycle Byte3 = SYS_FAN2 pwm duty cycle Byte4 = SYS_FAN3 pwm duty cycle Byte5 = SYS_FAN4 pwm duty cycle Byte6 = SYS_FAN5 pwm duty cycle Byte7 = SYS_FAN6 pwm duty cycle
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_BMCDDR	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
User's Manual

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
SYS_FAN1	3500 RPM	ok
SYS_FAN2	3550 RPM	ok
SYS_FAN3	1600 RPM	ok
Outlet T	25 degrees C	ok
Inlet T	25 degrees C	ok
CPU1 T	31 degrees C	ok
РСН Т	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.

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	Force encryption/ Authentication controlled by remote
Authentication/Authentication	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
		AfuEfix64.efi
Local Opdate	OEFTenvironment	Need to disable SPS by JME1 jumper.
Romoto Undoto		No tool required
Remote Opdate		No need to disable SPS.

1.1 BIOS + SPS update in UEFI environment

1. Format a USB flash drive to FAT32.



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

This I	PC > USB Drive (G:) >		
^	Name	Size	Date r
	EFI		12/11,
	AfuEfix64.efi	521 KB	7/19/2
	BIOS.bin BIOS file	32,768 KB	1/2/20
	FlashAll.nsh	1 KB	6/16/2

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

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



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



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

fs0:\> ls Directory o	f: fs0:\			
12/11/19 07/19/18 01/02/20 06/16/16	04:17p 06:33p 04:46p 02:00a	<dir> 33</dir>	4,096 532,592 ,554,432 430	EFI AfuEfix64.efi BIOS.bin FlashAll.nsh
3 1	File(s) Dir(s)	34,087,454	bytes	ır 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 eff	fect
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.

BIOS version:

Main Advanced Platform Config	Aptio Setup – AMI Socket Config Server Mgmt Se
BIOS Information	
BIOS Vendor	American Megatrends
Core Version	5.29
Compliancy	UEFI 2.8; PI 1.7
Project Version	0ACOR 0.70 ×64
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

SPS version:

Ма	in (advance	d Plat	form	Config	Ap Socket	tio Cor	Setu nfig	p - Se
▶ PCH ▶ Serv	-IO (ver)	Configu 1E Conf	ration igurati	on <mark>2</mark>	8				
Set Set may	up Wa ting cau:	arning: items se syst	on this em to m	Scre alfun	en to ction!	incorrec		alues	
						Ap	tio	Setu	up

Platform Conf.	ig
General ME Configuration	3
Oper. Firmware Version	18:6.0.4.2
Backup Firmware Version	N/A
Recovery Firmware Version	18:6.0.4.2
ME Firmware Status #1	0x00000355
ME Firmware Status #2	0x8850A006
Current State	Operational

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.

Main Advanced Platform Confl	Aptio Se - AMI ig Socket Config Server M	gmt Security Boot Save & Exit		Aptio Setup – AMI Server Hgmt	
Hols. Advanced. Flatform Conf. BHC Firmare Revision IPHI Version IPHI Version IPHI Interface BHC Support IPHI Interface Tupe FRB-2 Tuper Tupe FRB-2 Tuper Tolecut FRB-2 Tuper Folicy SB Hatchape Tuper FBB-2 Tuper Folicy SB Hatchape Tuper SB Hatchape Tolicy Power Control Policy Power Control Policy • System Event Log	10.00 US Server k 10.20 2.0 KCS Emabled Usca Interfacel Browbadd Formbadd Formbadd Formbadd Do Nothings To Server Do Nothings Dissiled Do Nothings Dissiled Diss	Scarity Lost Sue & Exit Configure BHC network Dargeeters *** Select Screen ***	BBC Return: configuration BBC network: configuration	Description Service Repute Description Find Description Description Service Repute Description Service Repute Description Service Repute Description Service Repute Description Service Service Description Service Service	Select to configure LAN channel parameters statically or dynamically 0% BIOS or BeC), impose list on to will not notify any BPC return, parameters during BIOS phase **: Select Screen 1: Select Time Dren: Select *-: Change Oot. F1: General Neip F2: Previous Values F3: Optimized Dereauts
 Bmc self test log BMC network configuration View System Event Log BMC User Settings BMC Karm Reset 		F4: Save & Exit ESC: Exit	Sutarit mask Station HAC address Router IP address Router MAC address	295,295,295,00 62-70:FB-83-00-FB 10.168.32,254 08-58-0E-AB-EB-DC	F#1 SAVE B EXIT
Vers) 2023 AMI			

- ← → C ▲ Not secure | 192.168.1.78/#maintenance MEGARAC SP-X \equiv Firmware Information 12.01.191106 Nov 6 2019 14:24:04 CST Maintenance Host C Quick Links.. . * 🖶 Dashboard Backup Configuration BMC Recovery Sensor Power Source Firmware Update Preserve Configuration FRU Information 9 Logs & Reports System Administrator Settings 🖵 Remote Control 🖨 Image Redirection O Power Control Fan Control ✤ Maintenance
- 2. Click the Maintenance tab, then Firmware Upate.

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



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

	Are you sure you want to flash?	3_		
Note:		Ť	OK Can	cel
Following are the Firmware update methods an				
 BMC Firmware update. 				
 HPM Firmware update supports the following the following statement of the following state	wing components.			
 BOOT and APP 				
 BIOS 				
• ME				
 CPLD 				
 BIOS Firmware update 				
elect Firmware Image				
elect Firmware Image Choose File HPSRSU11.hpm				
elect Firmware Image Choose File HPSRSU11.hpm Start firmware update				
Choose File HPSRSU11.hpm				
Choose File HPSRSU11.hpm				
ielect Firmware Image Choose File HPSRSU11.hpm Start firmware update				
ielect Firmware Image Choose File HPSRSU11.hpm Start firmware update Preparin	g to flash			
Select Firmware Image Choose File HPSRSU11.hpm Start firmware update Preparin	g to flash			
Select Firmware Image Choose File HPSRSU11.hpm Start firmware update Preparin Proceed	g to flash			

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

		Prepari			
is	st of Compon	ents			
ŧ	Component Name	Existing Version	Uploaded Version	Upgrade	Progress

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	ΤοοΙ
Local Update	UEFI environment	AfuEfix64.efi

2.1 BIOS update in UEFI environment

1. Format a USB flash drive to FAT32.

Format USB Drive (H:)	×
Capacity: 3.65 GB	~
File system	
FAT32 (Default)	\sim
Allocation unit size	
4096 bytes	\sim
Restore device defaults	
Volume label	

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

PC > USB Drive (G:)			
Name	Size	Date modified	Туре
EFI		12/11/2019 4:17 PM	File folder
AfuEfix64.efi	521 KB	7/19/2018 6:33 PM	EFI File
🧾 FlashMain.nsh	1 KB	3/10/2016 4:25 PM	NSH File
BIOS.bin BIOS file	32,768 KB	1/2/2020 4:46 PM	BIN File

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

	Please select boot device:
Windo	ws Boot Manager (P1: TS128FSTDM1500AV)
UEFI:	Built-in EFI Shell
UEFI:	hp v115p PMAP, Partition 1
Enter	Setup
	† and ↓ to move selection ENTER to select boot device ESC to boot using defaults

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



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

Shell>	fs0:	_
(-0.1)		DIOS NO TRUT VOUR BIOS DODO
1SU:\>	<u>FlashMalh.nsh</u>	BIUS.DIN_INPUT YOU 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.		
FSO:\>		

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

Main Advanced Platform Config	Aptio Setup – AMI Socket Config Server Mgmt Se
BIOS Information	
BIOS Vendor	American Megatrends
Core Version	5 29
Compliancu	UFFT 2 8: PT 1 7
Project Version	0ACOR 0 70 ×64
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
Domoto undoto	IPMI Web UI	No tool required
Remote update	IPMI command	Yafuflash.exe

3.1 BMC update in WinPE environment

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

•	IA32 (F:) \rightarrow BMC \rightarrow yafuflash \rightarrow Win64			
	Name	Date modified	Туре	Size
	📄 amifldrv64.sys	12/8/2022 3:44 PM	System file	29 KB
<i>.</i>	📓 LIBIPMI.dll	12/8/2022 3:44 PM	Application exten	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. 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.

	Please select boot device:
UEFI: Bu	uilt-in EFI Shell
UEFI: US	B3.0 FLASH DRIVE PMAP, Partition 1
Enter Se	tup
E	↑ and ↓ to move selection NTER to select boot device ESC to boot using defaults

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

revocery.bat

03/27/2023	05:12 PM	<dir></dir>	
03/27/2023	05:12 PM	<dir></dir>	
02/22/2023	05:56 PM		1,363 revocery.bat
03/27/2023	11:45 AM	<dir></dir>	yafuflash
	1 File(s)	1,363 bytes
	3 Dir(s) 20.321.7	30,560 bytes free

Please wait. This may take few minutes.

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

WARNING!
FIRMWARE OPGRADE MUST NOT BE INTERROPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
December For Visibles
Preserving Env variables done
Ching Firmware Image : 100% done
Shipping [boot] Module
Elashing Lonny module
Varifying Finnware Image - 100%. done
Flashing [hkunconf] Module
Elashing 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
Veritying Firmware Image : 100% done
Flashing [extlog] Module
Flashing Firmware Image: 100% done
Veritying Firmware image: 100% done
Flashing Exclog House
Verifying Firmware Tmage - 100%
Flashing [archerci] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Resetting the firmware

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

ait options will not be applied
+ 096 nal, LLC

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.

Aptio Sec <mark>ia - AMI</mark> Main Advanced Platform Config Socket Config Server Mamt Security Boot Save & Exit		Aptio Setup – AHI Server Hgmt			
Main Advanced Flatform con BNC Firmmere Revision IPMI embinisme IPMI BNC Interface BNC Support IPMI Interface Type Mail for BNC FRB-2 Timer Timeru FRB-2 Timer Timeru FRB-2 Timer Timeru FRB-2 Timer Timeru BNC Sofigueed Four Control Folicy Four Control Policy	<pre>10 Socket Config Derver H 13.28 2.0 KCS [Enabled] MCCs Interface] Displed] Enabled] 6 10 Nothing] [Disbled] 10 [Reset] Power Restore [Unspecified]</pre>	Recurity Excit Size & Exit Configure BHC network parameters +: Select Screen H: Select Screen H: Select Tite Enter: Select Y-: Change Dt, Fil: General Heig Fil: Fil: General Heig	BBC network.com/iguration	Cerver Hast Cerver Hast	Splect to configure LAN channel parameters statically or dynamically(by BDS or BHC). Inspectified option will not modify any BHC network parameters during BIOS phase *: Splect Screen 11: Select Item Enter: Select *: General Helo F2: FreeJons Volues
Sustem Event Log Bmc self fest log BMC network configuration View System Event Log BMC User Settings BMC Karm Reset		F3: Ortevidos Maides F3: Ostimized Defaults F4: Save & Exit ESC: Exit	Station IP address Subret mask Station MAC address Router IP address Router MAC address	10.166.32.17 255.255.255.0 62-7C-FB-83-00-FB 10.166.32.254 08-5B-0E-AB-EB-DC	F3: Optimized Defaults F4: Save & Exit ESC: Exit
ve	rsion 2.22,1287 Copyright (C) 2023 AMI	Version	2.22.1287 Copyright (C) 2	023 AMI

MEGARAC SP-X	≡		US - English	▼ © Sync CRefresh L admin -
Eirmware Information 13.28.20230203 BIOS Version CPLD Version	Maintenance			₩ Home > Maintenance
Quick Links	Backup Configuration	Firmware Image Location	Firmware Information	2 Firmware Update
🖀 Dashboard				
🍘 Sensor		1	5	
FRU Information	Preserve Configuration	Restore Configuration	Restore Factory Defaults	Bios Post Code
Leel Logs & Reports >		×		
Settings	System Administrator	Download Service Data	CPU Information	
🖵 Remote Control				
Image Redirection				
එ Power Control 1				
F Maintenance				

2. Click Maintenance and go to Firmware Upate.

3. Choose File to select BMC file.

0

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

elect Firmware Image	
Choose File v0.28.ima_enc	
Start firmware update	
Protocol Type:	HTTPS
Preserve all Configuration.	This will preserve all the configuration settings during the
table below.	the individual items marked as preserve/overwrite in the
table below. All configuration items below will I operation. Click "Edit Preserve Cor	the individual items marked as preserve/overwrite in the pe preserved as default during the restore configuration nfiguration" to modify the Preserve status settings.

Click Preceed to Flash

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

4	IPMI	We will start the firmware upgrade now. You will not be able to access
5	NETWORK	BMC until it flashes and restarts. Do you want to continue?
6	NTP	OK
7	SNMP	Overwrite
8	SSH	Overwrite
9	KVM	Overwrite
10	AUTHENTICATION	Overwrite
11	SYSLOG	Overwrite
12	WEB	Overwrite
13	EXTLOG	Overwrite
	Pr	oceed to Flash

Select Full Flash

All the module section versions in the existing image and uploaded image are the same.					
Section Name	Existing version	Uploaded version	Upgradable/Non-Upgradable		
oot	13.3.000000	13.3.000000			
onf	13.3.000000	13.3.000000			
kupconf	13.3.000000	13.3.000000			
oot	13.3.000000	13.3.000000			
osimage	13.3.000000	13.3.000000			
www	13.3.000000	13.3.000000			
media	13.3.000000	13.3.000000			
extlog	13.3.000000	13.3.000000			
extlog	13.3.000000	13.3.000000			
ircherci	13.28.202302	13.28.202302			

When the message box shows up, click $\ensuremath{\text{OK}}$ again.

All the module section versions in the existing integerand uproduce image are the same. Version Compare Flash Version Compare Flash Section Name Evicting version								
S	ection Base	d Firmware Update			ОК		Cancel	
	13	EXTLOG	Do you wish to proceed?					
	12	WEB	is written w It is essenti	ith the new firmware image. al that the upgrade operation is no	t interrupte	d one	ce it start	
	11	SYSLOG	Clicking 'O	Clicking 'OK' will start the actual upgrade operation, wher				

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

12		new session after a couple of minutes.
13	EXTLOG	СК
ection B	ased Firmware Update	

6. Login to check the BMC firmware version.

Ν	IEGARAC SP-X
	Firmware Information
\sim	13.28.20230203
	BIOS Version
	0.0Y
	CPLD Version
	02

3.3 BMC update using IPMI tool

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

8 → yafuflash → Win64			
Name	Date modified	Туре	Size
🗟 amifldrv64.sys	12/8/2022 3:44 PM	System file	29 KB
🚳 LIBIPMI.dll	12/8/2022 3:44 PM	Application exten	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.



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

Main Advanced Platform Conf	Aptio Se - AMI ig Socket Confis Server H	gmt Security Boot Save & Exit	Aptio Setup - AMI Server Ngat						
BMC Firmware Revision IPMI Version IPMI BMC Interface BMC Support	13.28 2.0 KCS [Enabled]	 Configure BMC network parameters 	BMC network configuration	Select to configure LAN channel parameters statically or dynamically(by BIOS or BHC). Unspecified option will not modify any BHC network					
IPMI Interface Type Wait For BMC FRB-2 Timer FRB-2 Timer Inmeout FRB-2 Timer Policy OS Watchdog Timer OS Wid Timer Tomeout OS Wid Timer Policy	(Kcs Interface) [Disabled] [Enabled] 6 [Do Nothing] [Disabled] 10 [Decet]		Lan channel (idedicated RTL821F) Contigunation Address source Current Configuration Address Source Station IP address Subret mask Station MC address Denter IP address	Unspecified) DynamicAddressBmcDhcp 0.0.0.0 0.0.0.0 E2-41-2F-F0-00-CA	parameters during BIOS phase				
BMC Configured Power Control Policy Power Control Policy	Power Restore [Unspecified]	++: Select Screen 11: Select Item Enter: Select +/-: Change Oct. F1: General Help	Router MAC address Lan channel 2(shared I210) Configuration Address source Current Configuration Address	00-00-00-00-00-00 [Unspecified] DynamicAddressBmcDhcp	++: Select Screen 14; Select Item Enter: Select +/-: Change Opt. F1: General Helo				
System Event Log Bnc self test log BNC network configuration View System Event Log BNC User Settings		F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	Source Station IP address Subret mask Station MAC address Router MAC address Router MAC address	10.168.32.17 255.255.255.0 62-7C-FB-83-00-FB 10.168.32.254 08-5B-0E-AB-EB-DC	F3: Optimized Defaults F4: Save & Exit ESC: Exit				

4. When the following screen shows, please wait few seconds.

The update process will start.



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

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 Plaching foot] Module
Plashing Firmware Image: 100% done Verifying Firmware Image: 100% done
Flashing [okupcon]]Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
Flashing [root] Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
riasning Losimagej Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
riasning [www]Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
riasning [imedia] Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
rlashing [extlog] Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
rlashing [exilog] Module Plashing Firmware Image : 100% done Verifying Firmware Image : 100% done
Flashing [archerci] Module Flashing Firmware Image : 100% done Verifying Firmware Image : 100% done
D:\yafuflash\Win64>_

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

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



APPENDIX-G SMART FAN CONFIGURATION

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

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

Where:

Function code
 Ox30 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	Cmd	Data/Response data					
	code							
Set Fan Mode	0x30	0x01	Input data: 0=standard speed , 1=manual speed					
Get Fan Mode	0x30	0x30	Response data: 0=standard speed , 1=manual speed					
Set fan PWM	0x30	0x35	[Fan] [PWM] Fan: $0 = CPU1_FAN1$ $1 = SYS_FAN1$ $2 = SYS_FAN2$ $3 = SYS_FAN3$ $4 = SYS_FAN3$ $4 = SYS_FAN4$ $5 = SYS_FAN5$ $6 = SYS_FAN6$ PWM: The PWM duty cycle 0x64 =100%					
Get fan PWM	0x30	0x36	The response data represent each fan PWM. Byte1 = CPU1_FAN1pwm duty cycle Byte2 = SYS_FAN1pwm duty cycle Byte3 = SYS_FAN2 pwm duty cycle Byte4 = SYS_FAN3 pwm duty cycle Byte5 = SYS_FAN4 pwm duty cycle Byte6 = SYS_FAN5 pwm duty cycle Byte7 = SYS_FAN6 pwm duty cycle					

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

Example

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

Step 1. Set fan mode as Manual mode



/ # 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)	[7:0] – Record type 02h = System event record (default) C0h-DFh = OEM timestamped, bytes 8-16 OEM defined (see Table 3) E0h-FFh = OEM non-timestamped, bytes 4-16 OEM defined (see Table 4)
4-7	Timestamp (TS)	Time when the event was logged. The least significant byte is first. For example, TS:[29][76][68][4C] = 4C687629h = 1281914409 = Sun, 15 Aug 2010 23:20:09 UTC Note: There are various websites that convert the raw number to a date/time.
8, 9	Generator ID (GID)	RqSA and LUN if event was generated from IPMB. Software ID if event was generated from system software.
		[7:1] – 7-bit I2C slave address, or 7-bit system software ID [0] – 0b = ID is IPMB slave address, 1b = System software ID Software ID values: 0001h – BIOS POST for POST errors, RAS configuration/state, timestamp synch, OS boot events 0033h – BIOS SMI handler
		0020h – BMC firmware (default) 002ch – Intel ME firmware 0041h – Server management software 00c0h – HSC firmware – HSBP A 00c2h – HSC firmware – HSBP B
		Byte 2 [7:4] – Channel number. Channel that event message was received over. 0h if the event message was received from the system interface, primary IPMB, or internally generated by the BMC. [3:2] – Reserved. Write as 00b. [1:0] – IPMB device LUN if byte 1 holds slave address. 00b otherwise.
10	EvM Rev (ER)	Event message format version. 04h = IPMI v2.0 (default) 03h = IPMI v1.0
11	Sensor Type (ST)	Sensor type code for sensor that generated the event.
12	Sensor # (SN)	Number of sensor that generated the event (from SDR).
13	Event Dir/Event Type (EDIR)	Event Dir [7] – 0b = Assertion event, 1b = Deassertion event.
		Type of trigger for the event; for example, critical threshold going high, state asserted, and so on. Also indicates class of the event; for example, discrete, threshold, or OEM. The Event Type field is encoded using the Event/Reading Type Code. [6:0] – Event Type Codes 01h = Threshold (states = 0x00-0x0b) 02h-0ch = Discrete 6Fh = Sensor-specific
44	Event Data 4 (ED4)	/0-/FN = UEM
14	Event Data 1 (ED1)	0 7-11-0
15	Event Data 2 (ED2)	See Table 2.

16 Event Data 3 (ED3)

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

3 ways to check SEL log

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



➢ BMC Web

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



IPMI tool

LAN (remote)

Linux:

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

Windows:

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

D:\Tools\BMC\ipmiutil-3.1.5-win32> <u>ipmiutil.exe_selN_192.168.1.78_U_ADMINP_ADMIN</u>
ipmiutil sel version 3.15
Connecting to node 192.168.1.78
BMC version 0.28, IPMI version 2.0
SEL Ver 37 Support Of, Size = 3639 records (Used=426, Free=3213)
RecId Date/Time SEV Src_ Evt_Type Sens# Evt_detail - Trig [Evt_data]
0001 09/30/21 13:28:14 INF BMC Chassis #94 - 03 [01 ff ff]
0002 09/30/21 13:28:14 INF BMC ACPI Power State #99 S0/G0 Working 6f [00 ff ff]
0003 09/30/21 13:29:17 INF BMC System Firmware #00 prog, Reserved 6f [02 92 ff]
0004 09/30/21 13:52:09 INF BMC ACPI Power State #99 S4/S5 soft-off, no specific state 6f [06 ff ff]

KCS(local) Linux: ipmitool sel elist Windows: ipmiutil.exe sel

IPMI tools:

ipmitool: https://github.com/ipmitool/ipmitool ipmiutil: http://ipmiutil.sourceforge.net/

Log Policy:

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

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

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

SEL Log Settings Policy	
	0
Log Policy Linear Storage Policy Circular Storage Policy	
	🖺 Save

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 OI	EM command, and defa	ault Privilege Level is
User.				
	lf you use " ipm	iutil " tool in Wi	ndows OS, replace "0x	32" with "00 20 C8".
Cmd	Command code	e. This messag	e byte specifies the op	eration that it to be
executed.				
Data	Zero or more by	ytes of data, as	required by given com	imand.

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.

Locally get BIOS code by "ipmitool" in Linux.

Ipmitool raw 0x32 0x73 0

гоот	t@te	est	-Det	faul	lt-s	stri	ing:	:/hc	ome,	/tes	st#	ipr	nita	loc	гам	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	b 0	b0	b0	b1	b1	b 4	b2	b3			
b3	b3	b6	b6	b6	b6	b6	b6	b7	b7	be	b7	b 7	b 8	b 8	b 8			
b8	b9	b9	b9	bb	bb	bb	bb	bb	bb	bb	bb	bb	b7	bc	bc			
bc	bc	bc	bf	e7	e8	e9	eb	ec	ed	ee	4f	61	9a	78	68			
70	79	d1	d3	d4	91	92	94	94	94	94	94	94	94	94	94			
94	94	94	95	96	ef	92	92	92	99	91	d5	92	92	92	92			
97	98	9d	9c	92	b4	b 4	b4	b4	b4	b4	b4	b 4	b4	b4	a0			
a2	a2	a0	a2	a2	a2	a2	a2	a2	a2	a2	99	92	92	92	ad			
78	b1	a0	84	aa	e3	e3	e3								-3100			

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 <u>00 20 C8 73 0</u> 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 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 bb b9 b7 bc bc bc bc bc bc bf e6 e7 e8 e9 eb ec ed ee 4f 61 9a 78 68 70 79 d1 d3 d4 91 92 94 94 94 94 94 94 94 94 94 94 94 94 95 96 ef 92 92 92 92 99 91 d5 92 92 92 97 98 9d 9c 92 a0 b4 b4 b4 b4 b4 b4 b4 b4 b4 4 b4 a2 a2 a0 a2 a2 a2 a2 a2 a2 a2 a2 a2 99 92 92 92 ad 78 b1 a0 ee ee ee 84 aa e3 e3 send_icmd ret = 0 ipmiutil cmd, completed successfully

APPENDIX-J REMOTE CONTROL-Serial Over LAN

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



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

S MEGARAC SP-X	× +
← → C ▲ Not secure	https://10.168.32.54/#remote_control
MEGARAC SP-X	≡
Eirmware Information 13.28.20230203 BIOS Version 0.0V CPLD Version	Remote Control Remote KVM & SOL
02 Host Online Ouick Links,	H5Viewer
A Dashboard	Click here to go to Remote Session Settings.
🏙 Sensor	C [*] Launch H5Viewer
 FRU Information 	
Logs & Reports >	Seriel Over LAN
Settings	Serial Over LAN
Remote Control	C Activate
Image Redirection	
O Power Control	
F Maintenance	
🕞 Sign out	

3. Access BIOS and UEFI shell in serial console.

Deactivate C	Columns	80	Rows	25				Deactivate	Columns	80	Rows	25		
Main Advan	iced Pla	Aptio tform Config	Setup Socket	- AMI Config Serv	er Mgmt S	Security	A .	Mapping tabl FSO: A Pc	■ lias(s):HI iRoot(0x0)	00d0b:;BLK1: /Pci(0x14,0x0)	/USB (0x	3,0x0)/HD(1,GP	r, fee45bf5-c5a1-42c0-a5	
				Choos	the syst	cem		78-C88CD4CA7	CC8,0x800,	0x3A22800)				
Platform Info	rmation			defau	t languag	je		BLK0: A	lias(s):		(
Platform		TypeArche:	rCityRP					PC	$1 \text{Root}(0 \times 0)$	/Pc1 (0x14,0x0)	/USB (Ux	3,0x0)		
Processor		806F6 - SI	PR-SP E	3				BLKZ: A	iBoot(0v0)	/Pci (0x14 0x0)	/11SB (0v	a 0v0)/IISB(0v0	0×0)	
PCH		EBG AU/AL	/B0/B1	SKU -				BLK6: A	lias(s):	/ ECE (OAL4, OAO)	, 000 (0x	A, 020 / / 000 (020 /	.0	
RC Revision		93.D22		, T				Pc	iRoot (0x0)	/Pci (0x14,0x0)	/USB (0x	A, 0x0) /USB (0x1,	,0x0)	
BIOS ACM		1.1.1		٣				BLK3: Alias(s):						
SINIT ACM		1.1.1		٣				Pc	iRoot (0x0)	/Pci(0x14,0x0)	/USB (0x	A, 0x0) /USB (0x0,	,0x0)/Unit(0x1)	
				rij				BLK4: A	lias(s):		(2000) 10	/===	0 0) (7) 1, (0, 0)	
Memory Inform	ation .			۳><:	elect Scr	reen		PC	1 = -(-)	/PC1 (0X14,0X0)	/USB (Ux	A, UXU) / USB (UXU,	(0x0)/Unit(0x2)	
Total Memory		196608 MB		r: Se	ect Item			BLKD: A	iBoot(0v0)	/Pci (0x14 0x0)	/11SB (0y	a 0v0) /IISB (0v0	$(1)^{(1)}$	
BIOS Name		0.08		*=/	: Select Change On	st.		BLK7: A	lias(s):	/101 (0A11/0A0)	,	1, 010 (010)	(one), one (one)	
DIOD VELDION		0.00		YF1:	eneral He	alp		Pc	iRoot(0x0)	/Pci (0x14,0x0)	/USB (0x	A, 0x0) /USB (0x1,	0x0)/Unit(0x1)	
System Langua				٣F2:	revious V	/alues		BLK8: A	lias(s):					
				F3: 0	timized D	Defaults		Pc	iRoot (0x0)	/Pci(0x14,0x0)	/USB (0x	A, 0x0) /USB (0x1,	,0x0)/Unit(0x2)	
System Date		[Tue 03/2]	8/2023]	F4: S	ve & Exit			BLK9: A	lias(s):		(1000 10	/=== /	0 0) (7) 11 (0 0)	
				ESC:	Exit			PC Press FSC in	2 second	/PC1 (UX14,UXU)	/USB (Ux	A, UXU) / USB (UXI,	(0x0)/Unit(0x3)	
	Vor	eion 2 22 122	7 Copur	ight (C) 2023	7MT			Shell>	2 second:	to skip start	.up.nsn	or any other ke	sy co concinue.	
	A6T	5101 2:22.120	- соруг	igne (e) 2025	DELT-			Shell>						

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.

Aptio Ser <mark>n - AMI</mark> Main Advanced Platform Config Socket Config Server Mgmt Security Boot Save & Exit			Aptio Setup – AMI Server Mgmt		
BNC Firmware Revision IPMI Version IPMI BND Interface BNC Support IPMI Interface Type Wait For BNC FRB-2 Timer Timeout FRB-2 Timer Timeout OS NatChidog Timer OS NatC	13.28 2.0 KCS [Enabled] [Kcs Interface] [Disabled] 6 [Do Nothing] [Disabled] 10 [Reset] Power Restore [Unspecified]	<pre> Configure BMC network parameters **: Select Screen 14: Select Item Enter: Select */-: Change Opt. F1: General Help P2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit </pre>	BKC network configuration ***********************************	Unspecified DynamicAddresSBncDhcp 10.168.32.16 255.255.255.0 E2-41-2F-F0-0D-CA 10.168.32.254 08-58-0E-AB-EB-DC Unspecified DynamicAddresSBncDhcp 0.0.0.0 0.0.0.0 62-70-FB-83-00-FB 0.0.0.0 00-00-00-00-00	 Select to configure LAN channel parameters statically or dynamically(by BIDS or BHC). Unspecified option will not modify any BHC network parameters during BIOS phase **: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1287 Copyright (C) 2023 AMI Version 2.22.1287 Copyright (C) 2023 AMI					

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.

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