HPS-621U2A IPMI Setup User's Manual

1st Ed –27 October 2022

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 © 2022 Avalue Technology Inc., ALL RIGHTS RESERVED.

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

Trademark Acknowledgement

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

Disclaimer

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

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

Life Support Policy

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

As used herein:

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

A Message to the Customer

Avalue Customer Services

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

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

Technical Support

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

first.

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

Product Warranty

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

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

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

Content

Glossary & Abbreviation6					
1. HA	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	-			
2.4	HOME> FRU INFORMATION	21			
2.5	HOME> LOGS & REPORTS	22			
2.6	HOME> SETTINGS				
2.7	HOME> REMOTE CONTROL				
2.8	HOME>IMAGE REDIRECTION	87			
2.9	HOME> POWER CONTROL				
2.10	HOME> MAINTENANCE	90			
2.11	HOME> SIGN OUT				
APPE	NDIX-A BMC HARDWRE: AST2500				
APPE	NDIX-B IPMI COMMANDS SUPPORT TABLE				
APPE	NDIX-C IPMI OEM COMMANDS LIST	108			
	NDIX-D SENSOR TABLE				
APPE	APPENDIX-E DEFAULT CONFIGURATION111				
APPENDIX-F FIRMWARE UPDATE112					
APPENDIX-G SMART FAN CONFIGURATION145					
APPENDIX-H SYSTEM EVENT LOG(SEL)149					
APPENDIX-I IPMI TO GET BIOS POST CODE156					
APPE	APPENDIX-J REMOTE CONTROL-JVIEWER158				

Glossary & Abbreviation

Glossary & Abbreviation	Explanation	
BMC	Baseboard Management Controller, this is the common abbreviation for	
	an IPMI Baseboard Management Controller	
IBMC	Integrated Baseboard Management Controller, this is the name for the	
IDIVIC	2nd generation of BMC hardware, we use AST2500 on Platform	
IMM	Integrated Management Module, this means the same as BMC	
IPMI	Intelligent Platform Management Interface, a standardized system	
	management interface	
IPMB	Intelligent Platform Management Bus, I2C based bus	
SOL	Serial Over LAN, Host serial port traffic redirected over a LAN connection	
SOL	for remote control and management	
SDR	Sensor Data Record, A data record that provides platform management	
SDK	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	
	Internal Error. A signal from the Intel Architecture processors indicating	
IERR	an internal error condition	
DEDD	Parity Error. A signal on the PCI bus that indicates a parity error on the	
PERR	bus	
	System Error. A signal on the PCI bus that indicates a 'fatal' error on the	
SERR	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.

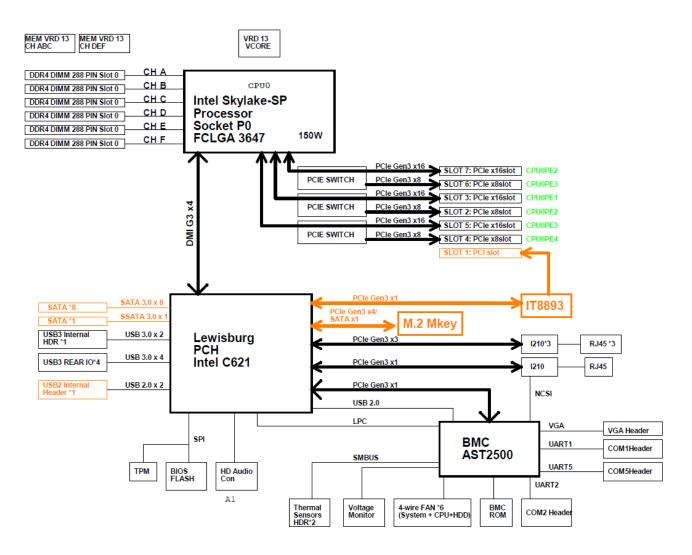


Figure 1-1 System block diagram

1.2 PLATFORM AND BMC COMPONENTS

Table 1-1 Main component related to BMC

- CPU(SkyLake) + PCH(Lewisburg C621)	
AST2500	
BIOS side: 32MB	
BMC side: 64MB	
512MB	
RMII1: Share NIC I210	
CAT24C512	
UART1: System UART	
UART2: System UART	
UART5: BMC console	
Power button	
System Reset button	
Lattice LCMXO2LF-1200C	
AMI MegaRAC 12.1	

1.3 I2C BLOCK DIAGRAM

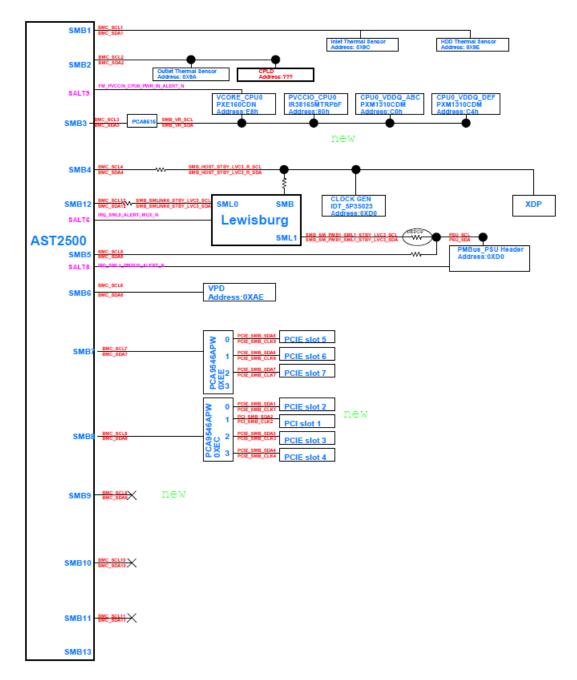


Figure 1-2 I2c block diagram

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 Number	Bus ID (channel no + bus ID + bus type)	Slave address	BMC use? (V)	Remark
1	02h	0x9C	V	Inlet Thermal Sensor
I	0211	0x9E	V	HDD Thermal Sensor
2	04h	0x9A	V	Outlet Thermal Sensor
		0xE8	V	VCORE CPU0
3	06h	0x80	V	PVCCIO CPU0
3	UON	0xC0	V	CPU0 VDDQ ABC
		0xC4	V	CPU0 VDDQ DEF
	ook	0x88	V	PCH SMB
4	08h	0xD0		CLOCK GEN IDP 5P35023
5	0Ah	0xB0	V	PMBUS
	7 0Eh	0xEE		PCA9546
		PCA9546 Channel 0		PCIE Slot 5
7		PCA9546 Channel 1		PCIE Slot 6
		PCA9546 Channel 2		PCIE Slot 7
		0xEC		PCA9546
8	10h	PCA9546 Channel 0		PCIE Slot 2
		PCA9546		PCI Slot 1

Table 1-2 Master Write-Read Bus IDs

HPS-621U2A User's Manual 11

Channel 1	
PCA9546	
Channel 2	PCIE Slot 3
PCA9546	
Channel 3	PCIE Slot 4

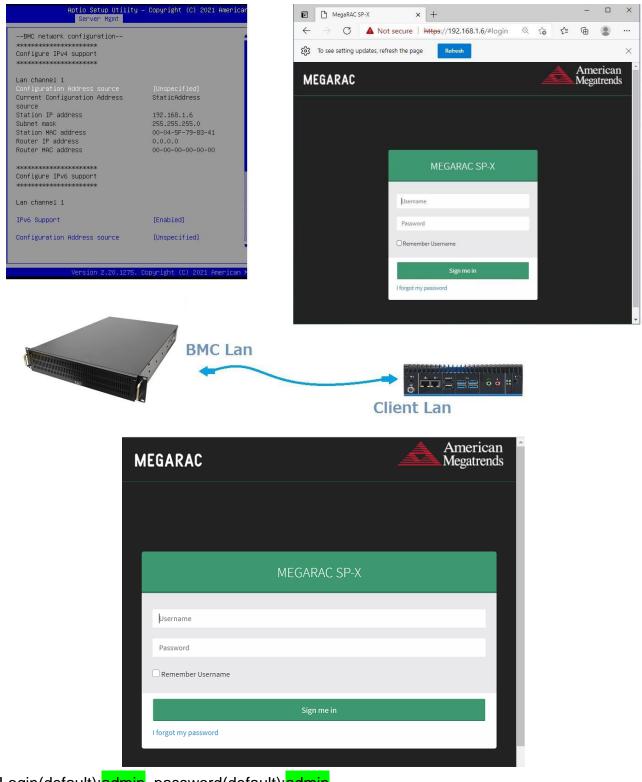
User's Manual



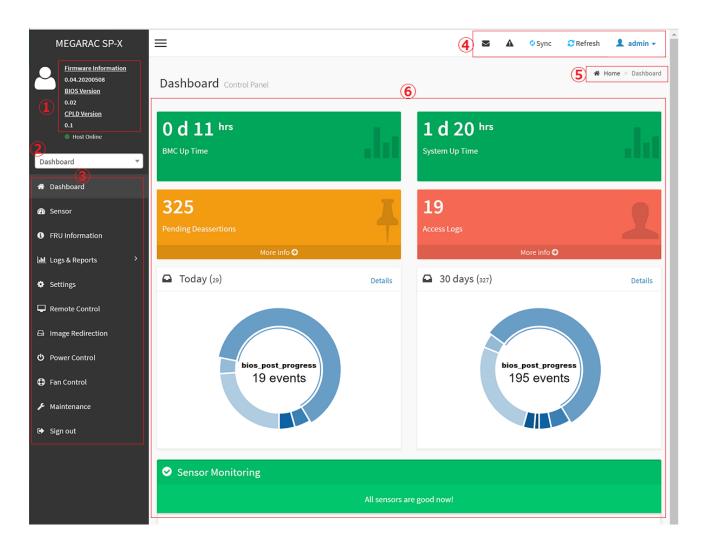
2.1 Log in

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
- 3 Menu Bar :

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

④ ▲	🗘 Sync 🛛 🔁 Refresh 🛛 💄 admin 👻		
-	Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the		
Logs and Reports page.			
A	Click the icon to view the notification received		
🗘 Sync	Click the icon to synchronize with Latest Sensor and Event Log updates.		
C Refresh	Click the icon or pressing key F5 to reload the current page.		
💄 admin 🗸	This option shows the logged-in user name and privilege. There are five kinds of privileges.		
	User: Only valid commands are allowed.		
	Operator: All BMC commands are allowed except for the configuration commands that can change		
	the behavior of the out-of-hand interfaces.		
	Administrator: All BMC commands are allowed.		
	No Access: Login access denied.		
	OEM: All OEM commands are allowed		
5 The location of the main page			

6 Main page that show content and configuration options

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

2.2 HOME>DASH BOARD

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

Dashboard Control Panel					
OdOhrs BMC Up Time	1 d 20 hrs System Up Time	226 Pending Deassert	ions More Info O	2 Access Logs More info	2
Today (226)	Details 🖸 30 days (226)	Details	Sensor Monitoring		
				All sensors are good now!	
bios_post_progress 157 events	bios_post_progress 157 events				

Item	Description
BMC Up Time	Timer that keep on accumulated while BMC on. Flash BMC f/w will reset this to
выс ор пше	zero.
System Up Time	Timer that keep on accumulated while System on. Flash BMC f/w will reset this to
System op Time	zero.
Pending Deassertions	It lists all the asserted events which are waiting for deassert state. Click more info
rending beassertions	to view the event logs

User's Manual

Access Logs	Click more info to view the Audit Log page		
Tedeu	This list event logs occurred by the different sensors today, click details link to		
Today	view the event logs		
20 Davia	This list event logs occurred by the different sensors within 30 days, click details		
30 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.

Sensor Reading Live reading of all se	nsors		倄 Home > Sensor Reading
			0
Critical Sensors (0)			
	ØAI	threshold sensors are normal	
Discrete Sensor States (1)			
Sensor Name		State	
↔ CPU THERMTRIP		No state defined	
□ Normal Sensors (40)			
Sensor Name	Reading	Behavior	
J⊷ +V12S_CPU1	12.30 Volts		
-∕v• +V5A	4.95 Volts		
J⊷ +V3.3A	3.25 Volts		
J⊷ +V1.8A	1.81 Volts	V	
J⊷ +VNN_PCH_AUX	0.99 Volts		
J⊷ +V1.05A	1.04 Volts		
J⊷ +V1.2A_BMCDDR	1.21 Volts		
	1.14 Volts		
J⊷ +V1S_VCCIO_P1AD	1 Volts		
-√⊷ +V5SB	5.10 Volts		
Jv+ +V12S	12.30 Volts		

User's Manual

J⊷ +V3.3S	3.35 Volts	
-∕⊷ +V3.0A_BAT	3.05 Volts	
-∕⊷ +VCCIN_CPU1	1.79 Volts	
-∕⊷ +VCCSA_CPU1	0.89 Volts	
J⊷ P1VDDR-123	1.22 Volts	
J⊷ P1VPP-123	2.57 Volts	
小 P1VDDR-456	1.22 Volts	
J⊷ P1VPP-456	2.57 Volts	
J⊷ +V1S_VCCIO_CPU1	1.01 Volts	<u> </u>
P1+VCCIN_T	38 °C	·
I P1+VCCSA_T	37 °C	
P1 DDR-123 T	35.00 °C	
P1 VPP_123_T	32.00 °C	
P1 DDR-456 T	38 °C	<u> </u>
P1VPP_456_T	32 °C	·
P1 VCCIO_T	32 °C	/W
CPU1_FAN	2100.00 Rpm	
SYS_FAN1	3500.00 Rpm	
SYS_FAN2	3550.00 Rpm	
SYS_FAN3	1600.00 Rpm	
l Outlet T	25.00 °C	
linlet T	25.00 °C	
CPU1T	31 °C	<u> </u>
PCH T	37 °C	<u>_</u>
I DIMM3 T	32 °C	<u> </u>
DIMM6 T	30 °C	·

Slot3_GPU_T	33 °C	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
Slot5_GPU_T	29 °C	~~~~·	
Dischlad Cancers (0)			
□ Disabled Sensors (9)			
X DIMM1 T	🗙 DIMM2 T	X DIMM4 T	🗙 DIMM5 T
X Slot1_GPU_T	X Slot2_GPU_T	¥ Slot4_GPU_T	X Slot6_GPU_T
X Slot7_GPU_T			

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.

+V12S_CPU1 Sensor Info	ormation	
1	12	2.3 Volts
	Upper Non-Recove	erable NA
	Upper Critical	12.6 Volts
22	Upper Non-Critica	I NA
Volts	Lower Non-Critica	I NA
	Lower Critical	11.4 Volts
	Lower Non-Recove	erable NA
0.00		Change Thresholds
	Time (HH:MM:SS)	

2.3.2 Home> Sensor Detail>Sensor Thresholds

This page allow user to configure threshold settings, click save button to apply changes.

Change Threshold Values	
Sensor Name	
+V12S_CPU1	
Upper Non-recoverable	
NA	
Upper Critical	
12.6	
Upper Non-critical	
NA	
Lower Non-critical	
NA	
Lower Critical	
11.4	
Lower Non-recoverable	
NA	

2.4 HOME> FRU INFORMATION

This page display FRU information that be stored in eeprom

FRU Field Replacable Units				Ø
Available FRU Devices				
FRU Device ID 0 ~				
FRU Device Name Atmel_AT24C512C				
Chassis Information	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	Mon Jun 14 16:00:00 2021	Product Manufacturer	Avalue Technology
Chassis Serial Number	Board Manufacturer	Avalue Technology	Product Name	HPM-621DE
Chassis Extra	Board Product Name	HPM-621DE	Product Part Number	HPM-621DEA-A1R
	Board Serial Number	99000016830011	Product Version	A1
	Board Part Number	HPM-621DEA-A1R	Product Serial Number	99000016830011
	FRU File ID		Asset Tag	
	Board Extra		FRU File ID	
			Product Extra	

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

2.5 HOME> LOGS & REPORTS

2.5.1 Home> Logs & Reports >IPMI Event Log

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

Event Log All sensor event logs Filter by Date Start Date O - End Date O Filter by type All Events ✓ All Sensors ~ UTC Offset: GMT - 7:0 ADownload Event Logs 20 Event Log: 226 out of 226 event entries BID: 226 Unknown sensor of type OEM_RECORD logged a oem timestamped Ø8 hours ago ID: 225 Unknown sensor of type os_boot logged a c boot completed @8 hours ago BID: 224 BIOS sensor of type bios_post_progress logged a progress Ø8 hours ago ID: 223 BIOS sensor of type bios_post_progress logged a progress @8 hours ago ID: 222 BIOS sensor of type bios_post_progress logged a progress @8 hours ago ID: 221 BIOS sensor of type bios_post_progress logged a progress O8 hours ago **Event Logs Statistics**

ltem	Option	Description
Filter by Date	 Start Date End Date All Events System Event Records OEM Event Record BIOS Generated Events 	Click field of "Start Date" or "End Date" to select the duration of filter IPMI event logs can be
Filter by type	 SMI Handler Events System Management Software Events System Software – OEM Events Remote Console Software Events Terminal Mode Remote Console software Events 	filtered by this selected event type.
Filter by sensor	 All Sensors +V12S_CPU1 	IPMI event logs can be filtered by this selected sensor.

2.5.2 Home> Logs & Reports >System Event Log

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

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	
192 2022 ID: 1 May 24th 2022, 9:26:29 am AMI00045F798341 kernel: kernel [7.240000] Helper Module Driver Version 1.2 -	
D: 2 May 24th 2022, 9:26:29 am AMI00045F798341 kernel: kernel [7.240000] Copyright (c) 2009-2015 American Megatrends Inc	
0	

Item	Option		Description
Filter by Dete	 Start Date 	ie	Click field of "Start Date" or "End Date" to
Filter by Date	 End Date 	e	select the duration of filter
	Alert		
	Critical		
	• Error		
Event Cotogony	 Notificati 	on	System event logs can be filtered by this
Event Category	Warning		selected event category.
	 Debug 		
	Emerger	су	
	 Informati 	on	

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:	Ø
Filter by Date Start Date O - End Date O	
Audit Log: 5 out of 5 event entries	
May 2022	
DI: 4 May 24th 2022, 10:43:49 am AMI00045F798341 spx_restservice: spx_restservice [1559 : 1559 INF0]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 INF0]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 Dete	Start Date	Click field of "Start Date" or "End Date" to select the
Filter by Date	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

Filter by Date Start Date O	Video Log All video event logs		Ø
	Filter by Date Start Date O - End Date O		
	0	Video 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
Filter by Date	•	End Date	duration of filter

2.6 HOME> SETTINGS A Home > Settings Settings Configure BMC options Ω = Т 0 Captured BSOD Date & Time External User Services KVM Mouse Setting Ŀ E Log Settings Media Redirection Settings Network Settings PAM Order Settings \succ Platform Event Filter Services SMTP Settings SSL Settings k System Firewall User Management Video Recording

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		

24 HPS-621U2A User's Manual

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.		
	E-mail message is one of alert and set SMTP for e-mail transmission across IP		
SMTP 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		
Video Recording	Configure the events that will trigger auto video recording function of the KVM		
	server.		

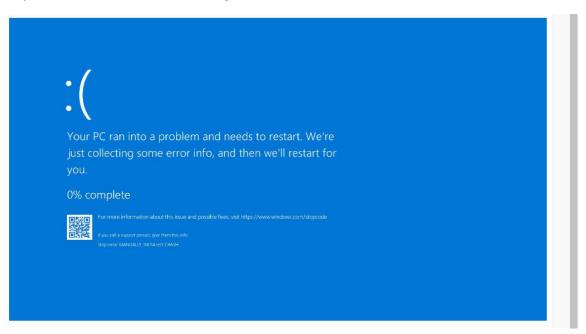
2.6.1 Home> Settings >Capture BSOD

This page displays a snapshot of the blue screen captured at the time when/if the host system crashed since the last reboot.

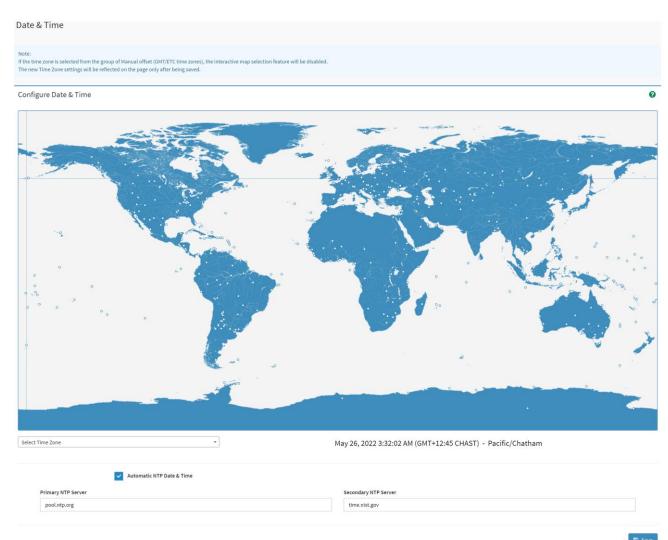
Note: KVM service should be-enabled to display the BSOD. This can be configured under 'Settings ->Services->KVM'.



BMC captured last BSOD screen if system occurred BSOD.

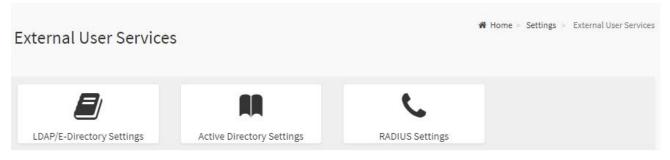


2.6.2 Home> Setting >Date & Time

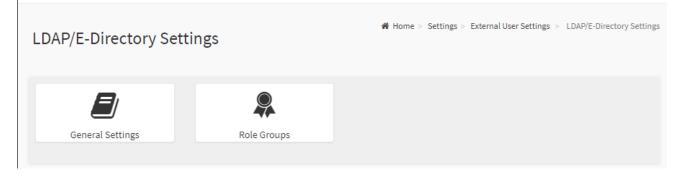


Item	Description		
Select Time Zone	Choose the Time Zone either by using the drop-down option or by		
Select Time Zone	hovering over the map and double-clicking on a location name.		
	You can select to have the time automatically synchronized to a NTP		
Automatic NTP Date & Time	server (or two) ,which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

2.6.3 Home> Setting >External User Services



2.6.3.1 Home> Settings >LDAP/E-Directory Settings



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

eneral LDAP Settings	
	0
Enable LDAP/E-Directory Authentication	
Encryption Type	
✓ No Encryption	
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	~
	🖺 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	
	Evenne	server.	
Bind DN	Example: cn=manager,ou=login,	Note:Bind DN is a string of 4 to 253 alpha-numeric	
		characters.	
	dc=domain,dc=com	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.	
Attribute of User Login	● cn	Select Attribute of User Login to find the	
	● 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'

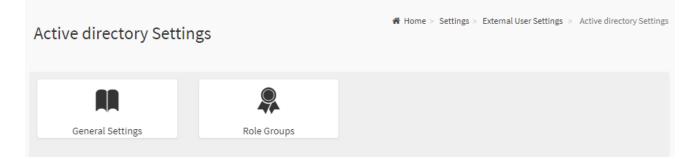
To add a Role Group, select a free box and click on it

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	
	G
Enable Active Directory Authentication	
Secret Username	
Secret Password	
User Domain Name	
Domain Controller Server Address 1	
Domain Controller Server Address 2	
Domain Controller Server Address 3	
	🖺 Save

Item	Option	Description	
Enable Active Directory Authentication		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					
Domain Controller		Enter the IP address of Active Directory server. At least on			
Server Address 2		Domain Controller Server Address must be configured.			
Domain Controller		IPv4/IPv6 formats 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'

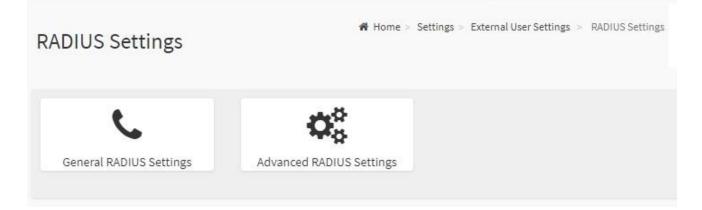
To add a Role Group ,click on a free box and configure its privilege and access.

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

Seneral RADIUS Settings	
	0
Enable RADIUS Authentication	
Server Address	
Port 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

34 HPS-621U2A 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
Operator		Attributes for the radius users on the server.
		Example:
User		Add Vendor-Specific attribute
		cd /usr/share/freeradius
OEM		vim dictionary.adtest
Proprietary		(Add content below)
No Access		# dictionary.adtest
		VENDOR ADTest 58
		# Standard attribute
		BEGIN-VENDOR ADTest
		ATTRIBUTE ADTest-group 1 string
		END-VENDOR ADTest
		vim dictionary
		(Add this line)

		\$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
SEL Log Settings Policy	Advanced Log Settings	

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

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

Item	Option	Description
Les Poliey	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

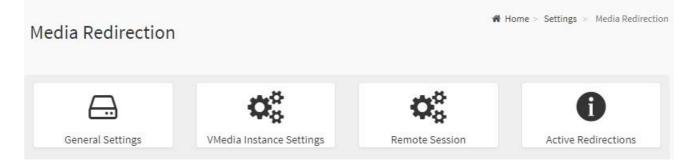
2.6.5.2 Home>	Settings>Log	Settings>Advanced	Log Settings
---------------	--------------	-------------------	--------------

Advanced Log Settings	
	?
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	ve 🛛

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.
	• UDP	Port type is supported with the enable of Remote Log. User can select
Port Type	• TCP	either UDP/TCP as per the requirement.
		If Local log is selected ,specify the size of the file in bytes.
		Size ranges from 3 to 65535
File Size		Log files are rotated when the size is larger than the mentioned
		bytes , with regards for the last rotation time interval(1 minute).
		When logged information exceeds the specified file size, the old log
Rotate Count		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	
Remote Server		Specify the port number to log system events	
Port		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 Audit Log to view all audit 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

eneral Settings	
	0
 Remote Media Support 	
V Mount CD/DVD	
Server Address for CD/DVD Images	
Server IP or Host name	
Path in server	
eg. /opt/bmc/nfs	
Share Type for CD/DVD	
nfs cifs	
Domain Name	
Jsername	
Password	
Same settings for Harddisk Images	
V Mount Harddisk	
Server Address for Harddisk Images	
Server IP or Host name	
Path in server	
eg. /opt/bmc/nfs	
Share Type for Harddisk	
Domain Name	
Jsername	
Password	
Retry Interval	
15	
Retry Count	
3	
	🖺 Save

User's Manual

Item	Option	Description
Remote Media Support		 To enable or disable Remote Media support ,check or uncheck this box. If it is selected ,then the following remote media types will be displayed CD/DVD Hard disk User can configure different settings for the different remote media types. Configuration options will be displayed for each media type, or the same options can be applied to both.
Mount CD/DVD	>	To enable or disable Mount CD/DVD support ,check or uncheck this box.
Server Address for CD/DVD image Path in server		 Address of the server where remote videos are to be stored. We support the following: IPv4/IPv6 format. FQDN(Fully qualified domain name) format Path must be alpha-numeric and the following special characters are only allowed: '/', '\', '-', '-', '-', ':'
Share Type for CD/DVD	nfscifs	Share Type of the remote media server : either NFS or Samba(CIFS).
Domain Name Username Password		If Share Type is Samba(CIFS) , then enter user credentials to authenticate the server. Note: Domain Name field is optional.
Same settings for Harddisk images	~	If the option is checked , then the server information entered for CD/DVD media type will be applied to the Hard disk remote media type as well.
Mount Harddisk	 ✓ 	To enable or disable Mount Harddisk support ,check or uncheck this box.
Server Address for Harddisk images		Address of the server where remote videos are to be stored. We support the IPv4/IPv6 format and FQDN(Fully qualified domain name) format
Path in server		Path must be alpha-numeric and the following special characters are only allowed:
Share Type for Harddisk	nfscifs	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		
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 in	stances
1	~
Remote KVM Hard disk instand	ces
1	~

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

42 HPS-621U2A 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
V 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

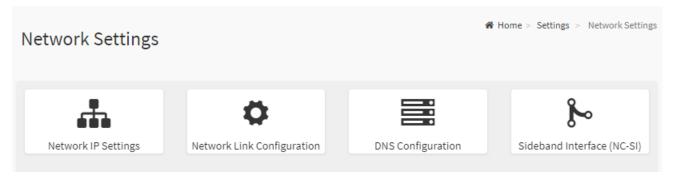
Item	Option	Description
KVM Single Port	~	Check this option to enable Single Port Application support in
Application		BMC
Keyboard Language		Select the Keyboard Language
Potry Count	1 to 20	Number of times to be retried when a KVM failure occurs.
Retry Count	1 10 20	Retry count ranges from 1 to 20
Retry Time	5 to 30	Number of seconds to wait for subsequent retries. Time
Interval(Seconds)	5 10 50	interval ranges from 5 to 30 seconds
Server Monitor OFF Feature Status	~	Check this option to enable the Server Monitor OFF feature
Automatically OFF Server Monitor, When KVM Launches		Check this option to enable Automatically OFF Server Monitor when KVM is launched
Save	🖺 Save	Click button to save the changes made

2.6.6.4 Home>Settings>Media Redirection>Active Redirections

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

Active Redirections			Home > Settings > Media Redirection > Active Redirectio		
No Media has been n	edirected.				6

2.6.7 Home>Settings>Network Settings



- Enable LAN	
AN Interface	
eth0	
IAC Address	
00:04:5F:79:83:41	
Enable IPv4	
Enable IPv4 Enable IPv4 DHCP	
Enable IPv4 DHCP	
Enable IPv4 DHCP Pv4 Address	
Enable IPv4 DHCP Pv4 Address 192.168.1.6	
Enable IPv4 DHCP Pv4 Address 192.168.1.6 Pv4 Subnet	

2.6.7.1 Home>Settings>Network Settings>Network IP Settings

Network IP Settings

IPv6 Index 0 IPv6 Address ::

0

VLAN ID 0 VLAN Priority 0

Subnet Prefix Length

Enable VLAN

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

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

2.6.7.2 Home>Settings>Network Settings>Network Link Configuration

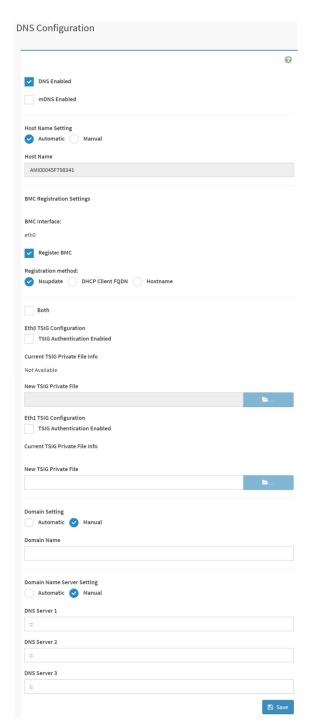
	Ø
LAN Interface	
eth0	~
✓ Auto Negotiation	
Link Speed	
1000 Mbps	
Duplex Mode	
FULL Duplex	
NCSI Interface	
Enabled	

Network Link Configuration

User's Manual

Item	Option	Description
LAN Interface	eth0	Select the network interface for which the Link speed and
LAN Interface	ento	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 Croad	• 100	network interface. Speed can be 10/100/1000 Mbps.
Link Speed	• 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
	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
Registration method	 Nsupdate DHCP client FQDN Hostname 	Nsupdate-Register with the DNS server using the nsupdate application DHCP client FQDN-Register with the DNS server using DHCP option 81 Hostname-Register with the DNS server using DHCP option 12 Note: Hostname option should be selected if the DHCP server does not support option 81 and Hostname method registration does not support IPv6 Domain interface.
Both	✓	Check this box to modify TSIG authentication for both interfaces.
TSIG		Check this box to enable TSIG Authentication – if registering
Authentication		DNS via nsupdate only.
Enabled(Eth0)		
New TSIG Private File(Eth0)	b	Browse for a new TSIG private file to be uploaded to the BMC
TSIG Authentication Enabled(Eth1)	✓	Check this box to enable TSIG authentication – if registering DNS via nsupdate only
New TSIG Private File(Eth1)	b	Browse for a new TSIG private file to be uploaded to the BMC.
Domain Sotting	Automatic	Select whether the domain interface will be configured
Domain Setting	 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

Sideband Interface (NC-SI)

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

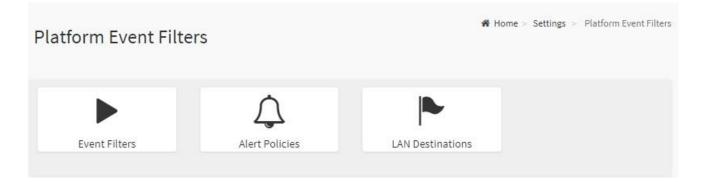
Item	Option	Description
NCSI Mode	Auto Failover ModeManual Switch Mode	Select the NCSI mode
NCSI Interface	eth0	Choose the interface name for which to configure NCSI settings
Package ID		Choose the package ID to be configured for the selected interface.
Channel Number		Choose the channel number to be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

2.6.8 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	ers						Home > Settings > Platform Event Filters	> Event Filters
⊖ All ● Con	ifigured O 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	0
	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	0	PEF ID: 12 (Enabled) when All Sensors switches to any severity run Alert (12) & none	۵
	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	~
Vent Filter Action Alert	
Power Action	
None	~
Alert Policy Group Number	
1	~
Raw Data	
Generator ID 1	
255	
Generator ID 2	
255	
Generator Type Slave Software	
Slave Address/Software ID	
Channel Number	
	~
IPMB Device LUN 0	~
	Ŷ
Sensor type	
All Sensors	~
Sensor name	
All Sensors	~
Event Options	
All Events	~
Event trigger	
255	
Event Data 1 AND Mask	
0	
Event Data 1 Compare 1	
0	
Event Data 1 Compare 2	
0	
Event Data 2 AND Mask	
0	
Event Data 2 Compare 1	
0	
Event Data 2 Compare 2	
0	
Event Data 3 AND Mask	
event Data 3 AND Mask	
Event Data 3 Compare 1	
0	
Event Data 3 Compare 2	
0	
Delete	🖹 Save

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 	Select the type of sensor that will trigger the event filter action.	
	+V5A	Chappe event ention to be either All events or Senser	
Event Options	All EventsSensor Events	Choose event option to be either All events or Sensor specific events	
Event trigger	0-255	This field is used to give Event/Reading type vale. Value ranges from 0 to 255	
Event Data 1 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255	
Event Data 1 Compare1	0-255	This field is used to indicate whether each bit position's	
Event Data 1 Compare2	0-255	comparison is an exact comparison or not, Value ranges from 0 to 255	
Event Data 2 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255	
Event Data 2 Compare1	0-255	This field is used to indicate whether each bit position's	
Event Data 2 Compare2	0-255	comparison is an exact comparison or not, Value ranges from 0 to 255	
Event Data 3 AND Mask	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255	
Event Data 3 Compare1	0-255	This field is used to indicate whether each bit position's	
Event Data 3 Compare2	0-255	comparison is an exact comparison or not, Value ranges from 0 to 255	
Save	🖺 Save	Click button to save the changes made	

2.6.9.2 Home>Settings>Platform Event Filters>Alert Policies

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

Alert Poli	cies								Home > Settings > Platform Event Filters > A	Alert Policies
Ţ	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	0	Ţ	Group: 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Ţ	Group: 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	8
¢	Group: 5 (<i>Disabled</i>) Always send alert to this destination LAN Channe: 1 Sent To: 0	°	Group: 6 (<i>Disabled</i>) Always send alert to this destination LM Channel: 1 Sent To: 0	8	Ţ	Group: 7 (<i>Disabled</i>) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Ĵ	Group: 8 (Disabled) Always send alert to this destination LM Channel: 1 Sent To: 0	0
¢	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	8	Ĵ	Group: 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	8	Ĵ	Group: 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	8
¢	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	8	Ţ	Group: 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Ţ	Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	8

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

lert Policies	
Alert Policies	8
Policy Group Number	
1	~
Enable this alert	
Policy Action	
Always send alert to this destination	~
LAN Channel	
1	~
Destination Selector	
	~
Event Specific Alert String	
Alert String Key	
	~
Delete	🖺 Save

56 HPS-621U2A User's Manual

User's Manual

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

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

2.6.9.3 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.

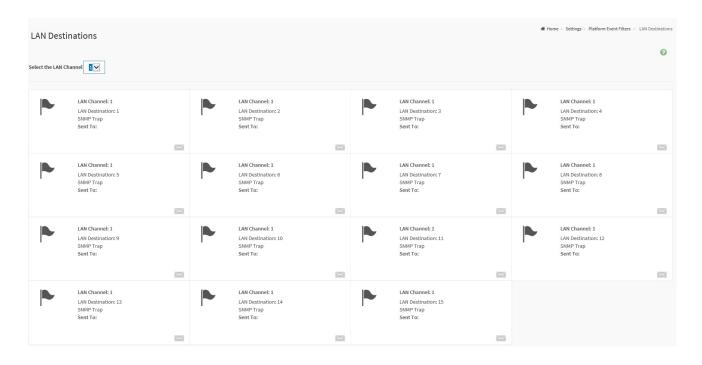
Click x icon to delete an entry from the list.

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						Ø
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		na
	0	
Service Name		
web		
✓ Active		
Interface Name		
both	~	
Secure port		
443		
Timeout		
1800		
Maximum Sessions		
20		
	Save	

Home>Settings>Services> Service Configuration

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

		Port value ranges form 1 to 65535			
		Note : Port 80 is blocked for TCP/UDP protocols			
	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		Displays the maximum number of allowed appaigns for the convice			
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

MTP 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
Primary Server IP		Server address will support the following
Frindly Server in		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 Secure		Specify the SMTP secure port
SMTP port		Default port is 465
		Port value ranges from 1 to 65535
		Check the option 'Enable' to enable SMTP Authentication.
		Note: Support SMTP Server Authentication Types are:
		CRAM-MD5.
Primary SMTP		LOGIN
Authentication		PLAIN
Addientication		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 SSLTLS Enable		Check the option to enable the SMTP SSLTLS protocol
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 SSL certificate	L Upload SSL certificate	

2.6.12.1 Home>Settings>SSL Settings> View SSL Certificate

This page displays the Current Certificate Information.

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)	
lssuer 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	

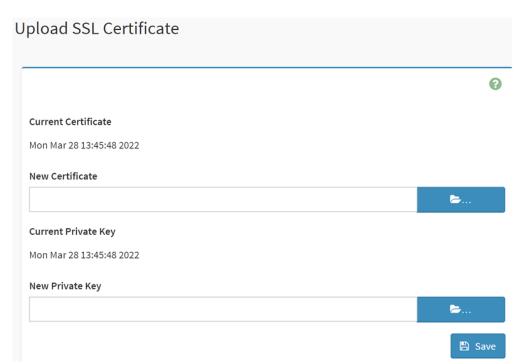
2.6.12.2 Home>Settings>SSL Settings>Generate SSL Certificate

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	
	ge •	generated	
Organizaion Unit(OU)		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



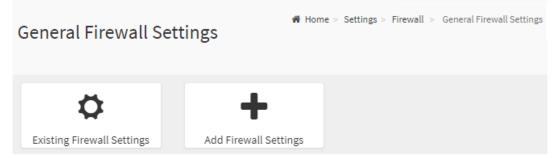
Item	Option	Description
Current Certificate		The information of the Current Certificate and date/time of
Current Certificate		its upload will be displayed(read-only)
		Browse and navigate to the new certificate file.
New Certificate	b	Certificate file should be of pem type.
		Information for the current private key and date/time when
Current Private Key		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	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	
	0

ltem	Option	Description
Block All	IPv4IPv6Both	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	0	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

	?
IP Single (or) Range Start	
IP Range End	
optional	
Enable Timeout	
Start Date	
YYYY/MM/DD	
Start Time	
	0
End Date	
YYYY/MM/DD	
End Time	
	J
Rule	
Allow	~

Item	Option	Description
IP Single (or) Range Start		This field is used for entering an IP address or the start of a range of IP addresses. IP address must follow the IPv4 format.
IP Range End		This field is used to indicate the IP address or end of an IP address range
Enable Timeout		This option is used to enable or disable timeout
Start Date	1	The firewall rule will become effective from this date
Start Time	O	The firewall rule will become effective from this time

End Date	#	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 Firewall Rules
0	+	
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	
Allow	,

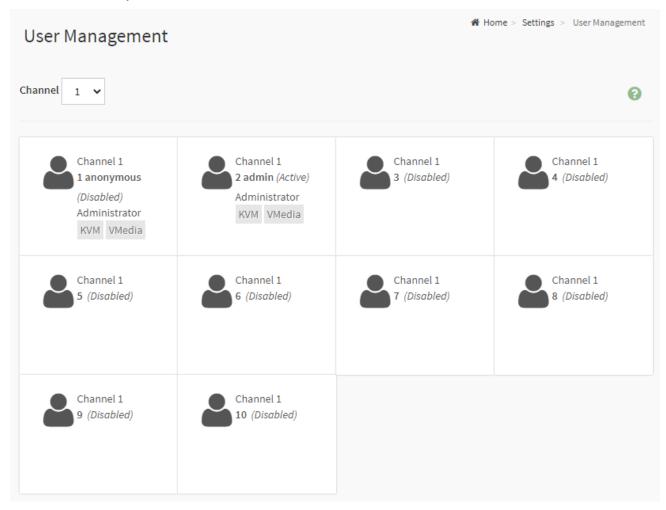
Item	Option	Description
		This field is used to specify the Port or start of a range of Port
IP Single (or)		Addresses.
Range Start		Port value ranges from 1 to 65535.
		Note: Port 80 is blocked for TCP/UDP protocols
ID Dongo End		This field is used to configure the Port or end of a range of
IP Range 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

User's Manual

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

Jsername	
anonymous	
Change Password	
assword Size	
16 bytes	
assword	
Confirm Password	
nable User Access	
Channel 1	
Channel 2	
Channel 8	
rivilege(Channel 1)	
Administrator	
Privilege(Channel 2)	
Administrator	
Privilege(Channel 8)	
Administrator	
V KVM Access	
VMedia Access	
SNMP Access	
NMP Access level	
NIMP ACCESS IEVEL	
NMP Authentication Protocol	
INMP Authentication Protocol	
NMP Privacy Protocol	
imail Format	
AMI-Format	
mail ID	
xisting SSH Key	
Not Available	
Jpload SSH Key	
	b

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.

76 HPS-621U2A User's Manual

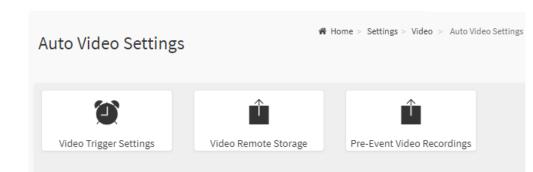
User's Manual

	• 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)	 User Administrator Operator None OEM 	Select the privilege level for each channel to be assigned to this user for access to the BMC through the netowrk
Privilege(Channel 2)	 User Administrator Operator None OEM 	 interface. There are 5 levels of Network Privileges User Administrator Operator
Privilege(Channel 8)	 User Administrator Operator None OEM 	 None OEM
KVM Access	✓	This checkbox is used to assign the KVM privilege for the user
VMedia Access		This checkbox is used to assign the VMedia privilege for the user
SNMP Access		Check the box to enable SNMP access for the user.
SNMP Access level		Choose the SNMP Access level option for user from the SNMP Access level (SHA or MD5) drop-down list. Either it can be Read Only or Read Write.
SNMP		Choose an SNMP Authentication Protocol for this user.

Authentication		Note: Password field becomes mandatory whenever the
Protocol		authentication protocol is changed.
		Choose the Encryption algorithm to be used for the SNMP
SNMP Privacy Protocol		settings from the SNMP Privacy protocol (AES or DES)
Protocol		drop-down list.
		AMI-Format: The subject of this mail format is 'Alert from
	 AMI-Format 	(your Host name)'. The mail content shows sensor
Email Format	 AMI-Format Fixed 	information, ex: Sensor type and Description.
Email Format		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.)
Existing SSH Key		If available, the uploaded SSH key information will be
Existing SSH Key		displayed(read-only)
		Use Browse button to navigate to the new public SSH key
Upload SSH Key	b	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	~	check/uncheck this ention to add/remove Critical Events trigger
(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
Fan state changed Events		Events trigger
Watabdag Timor Evanta	>	check/uncheck this option to add/remove Watchdog Timer Events
Watchdog Timer Events		trigger
Chassis Power On Events	>	check/uncheck this option to add/remove Chassis Power On
Chassis Power On Events		Events trigger
Chassis Power Off Events	~	check/uncheck this option to add/remove Chassis Power Off
		Events trigger
Chassis Reset Events	~	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
Bro Event Video Beerding	~	check/uncheck this option to add/remove Pre-Event Video
Pre-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

	0
This page is used to configure the Pre-Event video recording options. F default.	Pre-Event video recording is disabled by
To enable the Pre-Event video recording, go to the <u>Triggers Configurat</u>	t <mark>ion</mark> page.
Video Quality	
Very Low	```
Compression Mode	
High	,
Frames Per Second	
1	
/ideo Duration	
10	

🖺 Save

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

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

2.6.15.5 Home>Settings>Video Recording>Sol Settings

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

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

Option	Description	
		🖺 Save
Date and Tim	e Event	
LPC Reset Eve	ents	
Chassis Reset	Events	
Chassis Powe	r Off Events	
Chassis Powe	r On Events	
Watchdog Tin	ner Events	
Fan state cha	nged Events	
Non Recovera	ble 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
Fan state changed Events	>	check/uncheck this option to add/remove Fan state changed
		Events trigger
Watchdog Timer Events	>	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 Power Off Events	~	check/uncheck this option to add/remove Chassis Power Off
		Events trigger
Chassis Reset Events	>	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
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
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
Log Size (KB)		128KB.

User's Manual

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

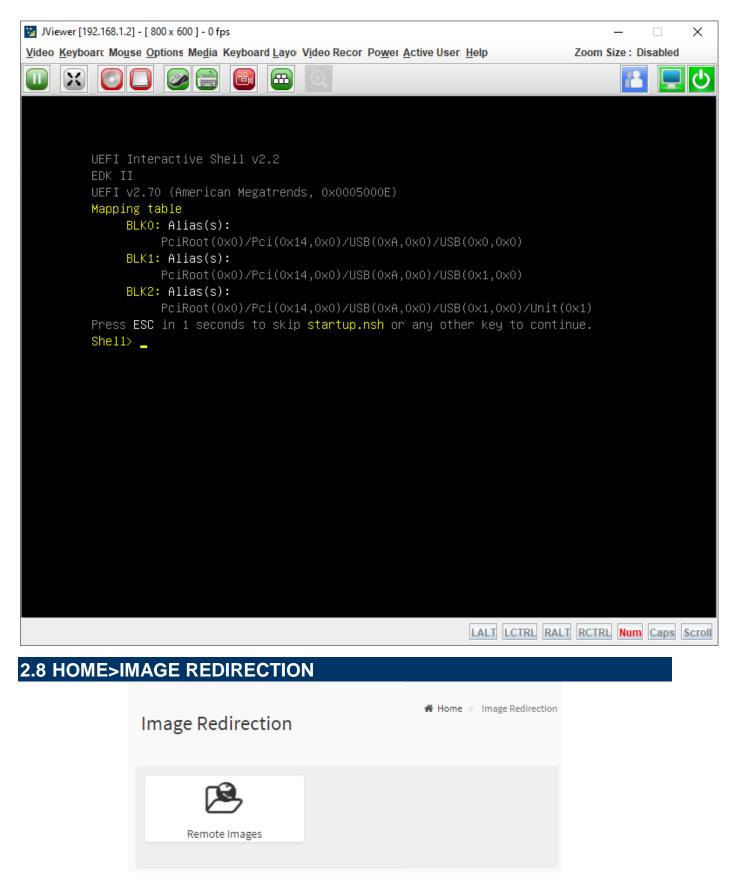
Sol Recorded video		Home > Settings > Video > Sol > Sol Recorded video
		0
S.No 🗢	File Name 🗢	File Information 🖨

2.7 HOME> RE	EMOTE CONTROL	
	Remote Control Remote KVM	
	H5Viewer	
	C Launch H5Viewer	
	JViewer	
	Launch JViewer	

2.7.1 Home>Remote Control >H5Viewer

Stop KVM										CD Imag	Browse File (0 K	B) Start Medi
Video 🗸 🛛 Mouse	Options	Keyboard 🗸	Send Keys 🕶	Hot Keys 🕶	Video Record 🗸	Power +	Active Users 🕶	Help 🕶			Zoom	100 % 🖵 🕻
			D.									
									_			
	.) O	Hi 💽		💼 文	-					5:44 PM 5/31/2022	
									LWIN RWIN		RALT RCTRL NU	M CAPS SC

2.7.2 Home>Remote Control >JViewer



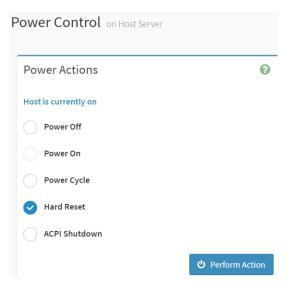
2.8.1 Home >Image Redirection>Remote Media

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
	Power Off	Select this option to power off the server
	Power On	Select this option to power on the server
Power Control	Power Cycle	Select this option to first power off, and then reboot the system
Power Control		(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

User's Manual

Perform Action	() Perform Action	Click button to perform the selected power action above
Perform Action	O Perform Action	immediately

2.10 HOME> MAINTENANCE

Jaintenance			# Home > Maintenance
Backup Configuration	Firmware Image Location	Firmware Information	Firmware Update
Preserve Configuration	Restore Configuration	S Restore Factory Defaults	_// Bios Post Code
System Administrator	Ju Download Service Data		

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.

Backup Configuration	
	0
Check All	
SNMP	
KVM	
Network & Services	
IPMI	
NTP	
Authentication	
SYSLOG	
	🛓 Download

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

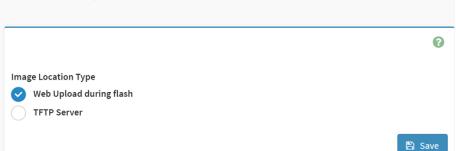
Download

_	
	Downlos
	Downloa

2.10.2 Home>Maintenance >Firmware Image Location

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

Firmware Image Location



ltem	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

Active Firmware	•
Build Date	
Mar 29 2022	
Build Time	
13:25:12 UTC	
-irmware version	
0.04.20200508	
3IOS version	
0.02	
CPLD version	

Item	Description
Build Date	Give the build date of the active BMC image

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

2.10.4 Home>Maintenance >Firmware Update

Choose the firmware image to be updated

Firmware Update

 Note:

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

 • BMC Firmware update supports the following components.

 • BOOT and APP

 • BIOS

 • ME

 • CPLD

Select Firmware Image

 Choose File

 No file chosen

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

	8
lick here to go to Firmware Update or Restore Fac	tory Defaults
Check All	
SDR	
FRU	
SEL	
IPMI	
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
IPMI	~	Checked this option to preserve IPMI configuration
Network	~	Checked this option to preserve Network configuration
NTP	~	Checked this option to preserve NTP configuration
SNMP	~	Checked this option to preserve SNMP configuration
SSH	✓	Checked this option to preserve SSH configuration
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	
	🕒

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

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

		8
	lowing checked configurations will be preserved through the restore operation. You can make as to the list in the preserve configuration page.	
SI	DR	
FF	RU	
SI	EL	
IP	РМІ	
N	etwork	
N	TP	
SI	NMP	
SS	SH	
K	VM	
Au	uthentication	
Sy	yslog	
W	/eb	

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

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

2.10.8 Home>Maintenance >System Administrator

ystem Administrator	0
Username	
sysadmin	
 Enable User Access 	
Change Password	
Password	
Confirm Password	
	🖺 Save

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

2.10.9 Home>Maintenance >Bios Post code

Collect all post from Bios.

BIOS Post	t Code All BIOS post code		♣ Home > Maintenance > 1
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	Ф Тор
3	0xA3	DXE-IDE Enable	101
	0xA3	DXE-IDE Enable	C End
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	

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.

Download Service Data Download Service Data
Download Service Data
Click the button, and BMC starts to collect data. After collection, data will be downloaded automatically.
🛓 Download Service Data

2.11 HOME> SIGN OUT

192.168.1.6 says

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

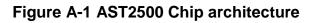
OK Cancel

APPENDIX-A BMC HARDWRE: AST2500

AST2500 is the 6th generation of Integrated Remote Management Processor introduced by ASPEED Technology Inc. It's a vastly integrated SOC device playing as a service processor to support various functions required for highly manageable server platforms. Instead of supporting PCI bus, AST2500 is designed to dedicatedly support PCIE Gen2 1x bus interface, which can make PCB layout simpler and fit systems that are going without PCI bus support.

PLL (x4) JTAG for ICE DDR3/DDR4 ARM1176JZFS SPI Master Coprocessor SRAM AHB - MBus Controller 32KB Bridge (4KB Cache) (16+16KB Cache) (x3)M-Bus AHB Bus USB2.0 Hub Hash SD/SDIO/ 1Gbps MAC MIC Video eMMC APB **USB1.1 USB2.0** (x2) Engine Engine Bridge Host Host (x2) USB1.1 HID Crypto (x2) **APB Bus** SCU /irtua MSI UART soc P2A VGA 2D E2M DMA & MCTP SMBus UART (x5) Display Bridge Controlle Engine Bridge (x14) (x1 Timer WDT PECI (x8) (x3) вмс Devic SGPIO PWN FanTach GPIO (x8) (x16) (228) (80) ADC JTAG SuperIO P-Bus MailBox ACPI (16) Master AHB Bus SPI SPI1 Pass-through Master PCIE to PCI LPC SPI eSPI VBIOS Master/Slave Bridge A SPI Slave PCI-Express SPI1 Interface LPC/eSPI Gen2 1x Interface

The chip architecture is showed below:



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

800-MHz ARM1176JZF-S 32-bit RISC CPU

Embedded one more 32-bit Coprocessor RISC CPU except the ARM. Max. 200MHz.

Built-in PCIE 2.0 Bridge Controller & PCIe Gen 2 PHY

Built-in PCI-Express 2.0 Root Complex or End Point Controller & PCI-Express Gen 2 PHY

VGA Display Controller

Graphics Display Controller

Video Compression Engine

Two 10/100/1000 Ethernet controllers with NC-SI support

16-bit DDR3L/DDR4 800MHz interface

36KB internal SRAM

System Control Unit

AHB controller

Interrupt Controller

Firmware SPI Memory Controller

SPI Master Controller

SD/SDIO/eMMC Host controller

USB2.0 Vitual Hub Controller

64-bit 2D Graphics Accelerator

14 sets of multi-function I2C/SMBus bus controller

Support up to 228 GPIO pins

Support up to 80 SGPIO input ports

Slave serial GPIO monitor

16 fan tachometers

8 PWMs

KCS interface

5 sets of 16550 UART controllers. 921.K baud-rate. Support Hardware UART debug

Built-in 8 sets of 32-bit timer modules

2 sets of USB 2.0 for keyboard, mouse, and storage devices

3 sets of 32-bit Watchdog timer

64 bytes Battery backed SRAM

LPC Bus Interface

eSPI interface

System SPI Flash Controller

Super I/O controller

Hash & Crypto Engine Memory Integrity Check(MIC)Engine 16 sets of 10 bits ADC channel pins Intel PECI 3.1 Compliant JTAG master MCTP controller MSI controller X-DMA controller The more information can refer to the Datasheet of AST2500.

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 Support	Арр	0Bh	0	V	
Get Configurable Commands	Арр	0Ch	0	V	
Get Configurable Command Sub-functions	Арр	0Dh	0	V	
Set Command Enables	Арр	60h	0		
Get Command Enables	Арр	61h	0	V	
Set Command Sub-function Enables	Арр	62h	0		
Get Command Sub-function Enables	Арр	63h	0		
Get OEM NetFn IANA Support	Арр	64h	0	V	
BMC Watchdog Timer Commands					
Reset Watchdog Timer	Арр	22h	М	V	
Set Watchdog Timer	Арр	24h	М	V	
Get Watchdog Timer	Арр	25h	М	V	
BMC Device and Messaging Commands					
Set BMC Global Enables	Арр	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	М	V	
Enable Message Channel Receive	Арр	32h	0	V	
Get Message	Арр	33h	М	V	
Send Message	Арр	34h	M	V	not support Send Raw
Read Event Message Buffer	Арр	35h	0	V	
Get BT Interface Capabilities	Арр	36h	Õ	V	
Get System GUID	Арр	37h		v	

Get Channel Authentication Capabilities App 38h O V Get Session Challenge App 39h O V Activate Session App 38h O V Set Session Privilege Level App 38h O V Class Session App 38h O V Get AuthCode App 38h O V Get Channel Access App 48h V Started mode" Get Channel Access App 43h O V Started mode" Get User Access Command App 43h O V Not support user session limit Get User Name App 48h O V Starte Payload App Get User Name Command App 48h O V Starte Payload App Get User Payload Activation Status App 48h O V Starte Payload Access App Get Channel Payload Support App 48h O V						
Capabilities Product Product Product Product Get Session Challenge App 3Ah V Set Session Privilege Level App 3Bh V Set Session Privilege Level App 3Bh V Set Session Privilege Level App 3Bh V Set Session Info App 3Ch V Set Session Info App 3Dh V Set Channel Access App 4Dh M V Set Channel Access App 4Ah V Set User Access Command App 4Ah V V Set User Payload Access App 4Ah V Set User Payload Access App <		Ann	38h	0	V	
Activate Session App 3Ah O V Set Session Privilege Level App 3Bh O V Get Session InfO App 3Bh O V Get Session InfO App 3Bh O V Get AutrOcde App 3Bh O V Set Channel Access App 4Dh M V Get Channel Indo Command App 4Ah V Shared mode* Get Channel Indo Command App 4Ah V V Set User Access Command App 4Ah V V Set User Name Command App 4Ah V V Set User Paysond Command App 4Ah V D Set User Payload Activation Status App 4Ah V D Set User Payload Activation Status App 4Ah V D Get Payload Activation Status App 4Ah V D Get Channel Payload Support App					•	
Set Session Privilege Level App 3Bh O V Close Session App 3Ch O V Get Session Info App 3Dh O V Get AuthCode App 3Fh O V Set Channel Access App 4Dh M V "Only support: disabled, always availible, shared mode" Get Channel Access App 42h O V State and access Command App 44h V State access Command App 44h V Statuser Access Command App 48h V Statuser Password Command App 48h V Statuser Pasyload App 48h V Statuser Pasyload Access App 48h V Statuser Pasyload Access <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
Close Session App 3Ch O V Get Session Info App 3Dh O V Get AuthCode App 3Dh O V Get AuthCode App 3Dh O V Set Channel Access App 4Dh M V Get Channel Info Command App 42h O V Set User Access Command App 42h O V Set User Name App 45h O V Set User Name Command App 48h O V Set User Password Command App 48h O V Get Payload App 48h O V Get Payload Access App 48h O V Get Payload Access App 48h O V Get Payload Access App 42h O V Get Channel Payload Access App 42h O V						
Cet Session Info App 3Dh O V Get AuthCode App 3Dh O V Set Channel Access App 40h M V shared mode' Get Channel Access App 41h M V shared mode' Get Channel Access Command App 42h O V Not support user session limit Get User Access Command App 44h O V Not support user session limit Get User Name App 45h O V Activate Payload App Get User Payload App 48h O V Activate Payload Activation Status App 48h O V Get Payload Activation Status App 48h O V Get Channel Payload Access App 44h O V Get Channel Payload Access App 44h O V Get Channel Payload Access App 44h O V Get Channel Payload Access App 44h O V Get Channel Payload Access App 55h O <td></td> <td>Арр</td> <td></td> <td>-</td> <td></td> <td></td>		Арр		-		
Get AuthCode App 3Fh O V "only support: disabled, always availible, shared mode" Get Channel Access App 40h M V shared mode" Get Channel Info Command App 42h V Not support: disabled, always availible, shared mode" Get User Access Command App 42h V Not support user session limit Get User Name Command App 48h V Not support user session limit Get User Pacess Command App 48h V Get Payload Activation Status App 48h V Get Payload Access App 48h V Get Channel Payload Version App 58h V Get Channel Payload Version App 55h V <		Арр	3Ch	0		
Set Channel Access App 40h M V "Only support: disabled, always availible, shared mode" Get Channel Info Command App 41h M V shared mode" Get Channel Info Command App 43h O V Not support: disabled, always availible, shared mode" Get User Access Command App 44h O V Not support: disabled, always availible, shared mode" Get User Name App 44h O V Not support: disabled, always availible, shared mode" Get User Name App 44h O V Studies Payload Studies Payload Access App Get Payload Activation Status App 44h O V Studies Payload Access App Get Channel Payload Access App 44h O V Studies Payload Access App 46h O V Get Channel Payload Access App 44h O V Studies Payload Access App 46h O V Get Channel Delyned Support App 55h O V Studies Payload Access App 56h V Sterenene Payload Access App 56h	Get Session Info	Арр	3Dh			
Set Channel Access App 401 M V shared mode" Get Channel Info Command App 42h O V Not support user session limit Get User Access Command App 44h O V Not support user session limit Get User Name Command App 44h O V Set User Race Command App Apt 46h O V Set User Paysword Command App 48h O V Get User Name Command App 48h O V Set User Payload Access App 48h O V Get Payload Access App 48h O V Set User Payload Access App 48h O V Get Channel Payload Access App 48h O V Set User Payload Access App 58h O V Get Channel Payload Access App 58h O V Set Channel Cipher Suites App 58h V Set Orannel Security Keys App 58h V Set System Info Parameters App 58h V <td< td=""><td>Get AuthCode</td><td>Арр</td><td>3Fh</td><td>0</td><td>V</td><td></td></td<>	Get AuthCode	Арр	3Fh	0	V	
Get Channel Access App 41h M V Get Channel Info Command App 42h O V Set User Access Command App 43h O V Set User Name App 45h O V Get User Name App 45h O V Get User Name App 46h O V Set User Name Command App 46h O V Activate Payload App 47h O V Activate Payload Access App 48h O V Get Payload Access App 46h O V Get Channel Payload Access App 46h O V Get Channel Odd Access App 46h O V Get Channel Odd Access App 56h O V Get Channel Payload Access App 56h O V Get Channel Cipher Suites App 56h O V Suspend/Resume Payload App 56h O V <td>Set Channel Access</td> <td>Арр</td> <td>40h</td> <td>М</td> <td>V</td> <td></td>	Set Channel Access	Арр	40h	М	V	
Get Channel Info Command App 43h O V Set User Access Command App 43h O V Not support user session limit Get User Access Command App 44h O V Set User Name Command App Get User Name Command App 46h O V Set User Password Command App Activate Payload App 48h O V Set User Payload Activation Status App 48h O V Set User Payload Access App 48h O V Get Channel Payload Support App 48h O V Get Channel Payload Support App 56h V Suspend/Resume Payload App 55h O V Set Channel Security Keys App 55h O <td>Get Channel Access</td> <td>Ann</td> <td>/1h</td> <td>М</td> <td>V</td> <td></td>	Get Channel Access	Ann	/1h	М	V	
Set User Access Command App 43h O V Not support user session limit Get User Name App 45h O V Get User Name App 45h O V Get User Name Command App 45h O V Set User Password Commad App 47h O V Activate Payload App 48h O V Get Payload Activation Status App 48h O V Get Payload Activation Status App 48h O V Get Payload Access App 48h O V Get Channel Payload Access App 44h O V Get Channel Payload Access App 54h O V Get Channel OEM Payload App 55h O V Inder Channel OEM Payload Inc App 55h O V Suspend/Resume Payload App Get System Interface App 55h O V Get System Interface App Get System Info Parameters						
Get User Access Command App 44h O V Set User Name App 45h O V Get User Name Command App 45h O V Set User Password Command App 47h O V Activate Payload App 48h O V Deactivate Payload Activation Status App 48h O V Get Payload Activation Status App 48h O V Get Payload Activation Status App 48h O V Get Channel Payload Access App 46h O V Get Channel Payload Access App 46h O V Get Channel Payload Access App 46h O V Get Channel Cher Suites App 50h O V Get Channel Cher Suites App 55h O V Get System Interface App 57h O V Chassis Supported Capasilities Chassis 00h M V Chassis Chassis <td></td> <td></td> <td></td> <td></td> <td></td> <td>Not ourport upor oppoign limit</td>						Not ourport upor oppoign limit
Set User Name App 45h O V Get User Name Command App 47h O V Set User Pasword Command App 47h O V Activate Payload App 48h O V Get Payload Activation Status App 48h O V Get Payload Activation Status App 48h O V Get Payload Actess App 48h O V Get Channel Payload Access App 48h O V Get Channel OEM Payload App 48h O V Get Channel OEM Payload App 58h O V Get Channel Cipher Suites App 58h O V Set Channel Security Keys App 58h O V Get System Info Parameters App 58h V Only 01h(KCS) is supported Get System Info Parameters App 58h V Chassis Control Chassis <						
Get User Name Command App 46h O V Set User Password Command App 47h O V Activate Payload App 48h O V Deactivate Payload App 48h O V Get Payload Activation Status App 48h O V Get Payload Access App 46h O V Get Channel Payload Mersion App 56h O V Get Channel Security Keys App 56h O V Get System Interface App 58h V Only 01h(KCS) is supported Capabilities Chassis 02h V Only 01h(KCS) is supported Capasis Device Commands Get Chassis 02h V Only 01h(CxCS) is supported						
Set User Password Command App 47h O V Activate Payload App 48h O V Get Payload Activation Status App 49h O V Get Payload Instance Info App 49h O V Get Datal Instance Info App 49h O V Get Otannel Payload Access App 40h O V Get Channel Payload Access App 47h O V Get Channel Payload Access App 47h O V Get Channel Payload Access App 47h O V Get Channel Cipher Suites App 52h M V Get Channel Cipher Suites App 54h O V Suspend/Resume Payload App 55h O V Suspend/Resume Payload Set System Into Parameters App 58h O V Chassis Device Commands Get Chassis Capabilities Chassis O3h O Chansis Capabilities Chassis Get System Into Parameters App						
Activate Payload App 48h O V Deactivate Payload App 48h O V Get Payload Activation Status App 4Ah O V Get Payload Activation Status App 4Ah O V Get Payload Access App 4Bh O V Get Channel Payload Access App 4Dh O V Get Channel Payload Version App 4Eh O V Get Channel Payload Version App 4Fh O V Get Channel Payload Version App 55h O V Get Channel Payload Version App 55h O V Get Channel Payload App 55h O V Suspend/Resume Payload App 55h O V Get System Interface App 57h O V Only 01h(KCS) is supported Get System Interface App 58h O V Chassis Dabilities Chassis Obh V Get Chassis Capabilities Chassis 00h M <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
Deactivate Payload App 49h O V Get Payload Activation Status App 44h O V Get Payload Instance Info App 48h O V Get User Payload Access App 46h O V Get Channel Payload Access App 46h O V Get Channel Payload Cursion App 4Fh O V Get Channel CEM Payload App 4Fh O V Get Channel Cipher Suites App 55h O V Master Write-Read App 55h O V Suspend/Resume Payload App 55h O V Set Channel Security Keys App 56h O V Get System Info Parameters App 58h O V Get Chansis Capabilities Chassis 00h M V Chassis Control Get System Info Parameters App 58h O V Chassis Capabilities Get Chassis Status Chassis 01h M V Chassis 02h M </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
Get Payload Áctivation Status App 4Ah O V Get Payload Instance Info App 4Bh O V Set User Payload Access App 4Ch O V Get Channel Payload Access App 4Ch O V Get Channel Payload Access App 4Ch O V Get Channel Payload Version App 4Fh O V Get Channel Payload Version App 5Ch V Get Channel Cipher Suites App Suspend/Resume Payload App 5Ch O V Get Channel Cipher Suites App 5Ch V Get Channel Security Keys App 5Ch O V Get Channel Security Keys App 5Ch V Chassis Supported Get System Info Parameters App 5Sh O V Chassis Capabilities Chassis Oth V Get Chassis Capabilities Chassis Oth V Get Chassis Capabilities Chassis Oth V Control command is combined to Chassis Get System Info Parameters App 59h O V Contr	,					
Get Payload Instance Info App 4Bh O V Set User Payload Access App 4Ch O V Get User Payload Access App 4Dh O V Get Channel Payload Access App 4Eh O V Get Channel Payload Version App 4Eh O V Get Channel OEM Payload App 56h O V Master Write-Read App 52h M V Get Channel Cipher Suites App 55h O V Suspend/Resume Payload App 55h O V Set System Interface App 57h O V Only 01h(KCS) is supported Capabilities App 58h O V Chassis Device Commands Get Chansis Status Chassis 00h M V Chassis Capabilities Get Chassis Capabilities Chassis 03h O Control command is combined to Chassis Get Chassis Reset Chassis 04h V V Control command in IPMI v1.5 Chass						
Set User Payload Access App 4Ch O V Get User Payload Access App 4Dh O V Get Channel Payload Version App 4Eh O V Get Channel Payload Version App 4Eh O V Get Channel Payload Version App 4Fh O V Get Channel Cipher Suites App 50h O V Master Write-Read App 55h O V Get Channel Cipher Suites App 55h O V Suspend/Resume Payload App 55h O V Get System Info Parameters App 57h O V Get System Info Parameters App 58h O V Chassis Device Commands Get Chassis Oth M V Chassis Oth V Get Chassis Status Chassis 03h O This command is combined to Chassis Chassis Capabilities Chassis 03h O V Chassis Cohl O Get Chassis Status Chassis 05h V </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
Get User Payload Access App 4Dh O V Get Channel Payload Support App 4Eh O V Get Channel Payload Version App 4Fh O V Get Channel Payload Version App 4Fh O V Get Channel Payload Version App 55h O V Get Channel Cipher Suites App 55h O V Get Channel Cipher Suites App 55h O V Suspend/Resume Payload App 55h O V Get System Interface App 57h O V Only 01h(KCS) is supported Get System Info Parameters App 58h O V Chassis Device Commands Get Chassis Device Commands Chassis Oh V Chassis Control Chassis Get System Info Parameters App 59h O V Chassis Control Chassis Get Chassis Status Chassis Ohassis Oh V Chassis Control command in IPMI v1.5 Chassis Control Chassis <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
Get Channel Payload Support App 4Eh O V Get Channel OEM Payload App 50h O V Master Write-Read App 52h M V Get Channel Cipher Suites App 52h M V Get Channel Cipher Suites App 55h O V Suspend/Resume Payload App 55h O V Get System Interface App 57h O V Get System Info Parameters App 58h O V Get Chassis Capabilities Chassis 00h V Only 01h(KCS) is supported Get System Info Parameters App 59h O V Chassis Capabilities Chassis Get Chassis Capabilities Chassis 00h M V Chassis Capabilities Chassis 02h V Chassis Capabilities Chassis 04h V Control command is combined to Chassis Chassis Capabilities Chassis 03h O V Set Chassis Capabilities Chassis 06h V						
Get Channel Payload Version App 4Fh O V Get Channel OEM Payload App 50h O V Master Write-Read App 52h M V Get Channel Cipher Suites App 52h O V Suspend/Resume Payload App 55h O V Encryption App 56h O V Set Channel Security Keys App 56h O V Get System Interface App 57h O V Only 01h(KCS) is supported Capabilities App 58h O V Chassis Device Commands O Get Chassis Capabilities Chassis 00h M V Chassis Device Commands O Get Chassis Capabilities Chassis 02h M V Chassis Control Chassis Chassis Reset Chassis 03h O This command is combined to Chassis Chassis Capabilities Chassis 05h V Set Power Restore Policy Chassis Get System Restart Cause Chassis						
Get Channel OEM Payload Info App 50h O V Master Write-Read App 50h O V Get Channel Cipher Suites App 54h O V Suspend/Resume Payload App 55h O V Set Channel Security Keys App 56h O V Get System Interface App 57h O V Only 01h(KCS) is supported Capabilities Set System Info Parameters App 58h O V Get Chassis Capabilities Chassis 00h M V Get Chassis Capabilities Chassis 00h M V Chassis Capabilities Chassis 03h O This command is combined to Chassis Chassis Capabilities Chassis 03h O V Chassis Capabilities Chassis 05h V Set Chassis Control command in IPMI v1.5 Chassis Capabilities Chassis 05h O V Set Power Restore Policy Chassis 06h V Set System Restart Cause Chassis						
InfoAppSunOVMaster Write-ReadApp52hMVGet Channel Cipher SuitesApp55hOVSuspend/Resume PayloadApp55hOVSet Channel Security KeysApp56hOVGet System InterfaceApp57hOVCapabilitiesApp57hOVSet System Info ParametersApp58hOVGet System Info ParametersApp58hOVChassis Device CommandsGet ChassisOhNVGet Chassis StatusChassisOhassisOhVChassis ResetChassisOhassisOhVChassis ResetChassisOhassisOhVChassis CapabilitiesChassisOhVControl command is combined to ChassisChassis ResetChassisOhassisOhVSet Control command in IPMI v1.5Chassis IdentifyChassisOhassisOhVSupportedGet System Restart CauseChassisOhVSupportedSet System Boot OptionsChassisOhVSupportedSet System Boot OptionsChassisOhVSupportedSet Power Cycle IntervalChassisOhVSupportedSet Power Cycle IntervalChassisOhVSupportedSet Power Cycle IntervalChassisOhVSupportedSet Power Cycl		Арр	4Fh	0	V	
Info Master Write-Read App 54h O V Get Channel Cipher Suites App 54h O V Suspend/Resume Payload App 55h O V Set Channel Security Keys App 56h O V Get System Interface App 57h O V Only 01h(KCS) is supported Set System Info Parameters App 58h O V Set System Info Parameters App Get Chassis Capabilities Chassis Ohn W V Get Chassis Capabilities Chassis Get Chassis Capabilities Chassis Ohn M V Chassis Capabilities Chassis Get Chassis Status Chassis Ohn M V Chassis Capabilities Chassis Chassis Reset Chassis O3h O This command is combined to Chassis Chassis Identify Chassis O4h V Set Power Restore Policy Chassis Get System Restart Cause Chassis O5h V Supported Supported Set System Boot Options Chassis O7h		۸nn	50h	0	V	
Get Channel Cipher Suites App 54h O V Suspend/Resume Payload Encryption App 55h O V Set Channel Security Keys App 56h O V Get System Interface App 57h O V Only 01h(KCS) is supported Set System Info Parameters App 58h O V Only 01h(KCS) is supported Get System Info Parameters App 58h O V Only 01h(KCS) is supported Get Chassis Device Commands App 59h O V Only 01h(KCS) is supported Get Chassis Status Chassis 00h M V Only 01h(KCS) is supported Get Chassis Status Chassis 01h M V Only 01h(KCS) Chassis Status Chassis 02h M V Chassis Capabilities Chassis Reset Chassis 03h O This command is combined to Chassis Chassis Identify Chassis 04h V Set Power Restore Policy Chassis Get System Restart Cause Chassis 07h V		лүү		0	v	
Suspend/Resume Payload Encryption App 55h O V Set Channel Security Keys App 56h O V Get System Interface App 57h O V Only 01h(KCS) is supported Get System Info Parameters App 58h O V Only 01h(KCS) is supported Get System Info Parameters App 59h O V Only 01h(KCS) is supported Get System Info Parameters App 59h O V Only 01h(KCS) is supported Get Chassis Capabilities Chassis 00h M V Only 01h(KCS) is supported Get Chassis Capabilities Chassis 00h M V Only 01h (KCS) is supported Chassis Capabilities Chassis 01h M V Only 01h (KCS) Chassis Capabilities Chassis 02h M V Ontrol command is combined to Chassis Chassis Capabilities Chassis 03h O V Set Chassis Capabilities Chassis Set Power Restart Cause Chassis 07h O V Supported Supported	Master Write-Read	Арр	52h	Μ	V	
Suspend/Resume Payload EncryptionApp55hOVSet Channel Security KeysApp56hOVGet System Interface CapabilitiesApp57hOVOnly 01h(KCS) is supportedGet System Info ParametersApp58hOVChassis SupportedGet System Info ParametersApp59hOVChassis Device Commands </td <td>Get Channel Cipher Suites</td> <td>Арр</td> <td>54h</td> <td>0</td> <td>V</td> <td></td>	Get Channel Cipher Suites	Арр	54h	0	V	
EncryptionAppSinOVSet Channel Security KeysApp56hOVGet System InterfaceApp57hOVOnly 01h(KCS) is supportedCapabilitiesApp57hOVChassis SupportedSet System Info ParametersApp58hOVGet System Info ParametersApp59hOVGet Chassis Device CommandsImage: CommandsImage: CommandsImage: CommandsGet Chassis Device CommandsImage: CommandsImage: CommandsImage: CommandsGet Chassis CapabilitiesChassis00hMVChassis Device CommandsImage: CommandsImage: Command Image: Command Ima	Suspend/Resume Payload	Ann	FFh	0	V	
Get System Interface App 57h O V Only 01h(KCS) is supported Set System Info Parameters App 58h O V Only 01h(KCS) is supported Get System Info Parameters App 59h O V Only 01h(KCS) is supported Get System Info Parameters App 59h O V Only 01h(KCS) is supported Get Chassis Device Commands Get Chassis Capabilities Chassis 00h M V Get Chassis Status Chassis 01h M V Ontrol command is combined to Chassis Chassis Reset Chassis 02h M V Ontrol command is combined to Chassis Chassis Identify Chassis 03h O This command is combined to Chassis Chassis Identify Chassis 04h O V Set Power Restore Policy Chassis 06h O V Get System Boot Options Chassis 08h O V Supported Set System Boot Options Chassis 08h O V Set Front Panel Button Chassis 08h O	Encryption	Арр	551	0	v	
Get System Interface CapabilitiesApp57hOVOnly 01h(KCS) is supportedSet System Info ParametersApp58hOVGet System Info ParametersApp59hOVChassis Device CommandsGet Chassis CapabilitiesChassis00hMVGet Chassis StatusChassis02hMVChassis ResetChassis02hMVChassis ResetChassis03hOThis command is combined to Chassis Control command in IPMI v1.5Chassis IdentifyChassis04hOVSet Power Restore PolicyChassis06hOGet System Boot OptionsChassis07hOVGet System Boot OptionsChassis09hOVSet Power Cycle IntervalChassis08hOVSet Power ResciverS/E00hMVGet POH CounterChassis08hOVSet Power Cycle IntervalChassis08hOVGet POH CounterS/E00hMVGet Event ReceiverS/E00hMVGet Event ReceiverS/E00hM <td>Set Channel Security Keys</td> <td>Арр</td> <td>56h</td> <td>0</td> <td>V</td> <td></td>	Set Channel Security Keys	Арр	56h	0	V	
CapabilitiesAppSritOVVSet System Info ParametersApp58hOVGet System Info ParametersApp59hOVChassis Device CommandsGet Chassis CapabilitiesChassis00hMVGet Chassis StatusChassis02hMVChassis ControlChassis02hMVChassis ResetChassis03hOThis command is combined to ChassisChassis IdentifyChassis04hVSet Chassis CapabilitiesChassis06hOSet Power Restore PolicyChassis06hOGet System Boot OptionsChassis08hOVSet System Boot OptionsChassis08hOVSet Power Cycle IntervalChassis08hOVSet Power Cycle IntervalChassis08hOVSet Power Cycle IntervalChassis08hOVSet Power Cycle IntervalChassis08hOVGet POH CounterChassis07hOVSet Event ReceiverS/E00hMVSet Event ReceiverS/E00hMVPerf AdAlertingOVImage: Command			C 74	~		Only 01h(KCS) is supported
Set System Info Parameters App 58h O V Get System Info Parameters App 59h O V Chassis Device Commands		Арр	570	0	V	
Get System Info Parameters App 59h O V Chassis Device Commands Chassis 00h M V Get Chassis Capabilities Chassis 00h M V Get Chassis Status Chassis 01h M V Chassis Control Chassis 02h M V Chassis Reset Chassis 03h O This command is combined to Chassis Chassis Identify Chassis 04h O V Set Chassis Capabilities Chassis 05h O V Set Power Restore Policy Chassis 06h O V Get System Restart Cause Chassis 07h O V Supported Set System Boot Options Chassis 08h O V Supported Set Front Panel Button Chassis 08h O V Set From Panel Button Chassis 0Ah O Earleystem Receiver C/Lassis 0Fh O V Set Event Receiver S/E 01h M V Get POH Counter <td></td> <td>Арр</td> <td>58h</td> <td>0</td> <td>V</td> <td></td>		Арр	58h	0	V	
Chassis Device Commands Image: Chassis Oth M V Get Chassis Capabilities Chassis Oth M V Get Chassis Status Chassis Oth M V Chassis Control Chassis O2h M V Chassis Reset Chassis O2h M V Chassis Reset Chassis O3h O This command is combined to Chassis Control command in IPMI v1.5 Chassis Identify Chassis O4h O V Set Chassis Capabilities Chassis O5h O V Set Power Restore Policy Chassis O7h O V Get System Restart Cause Chassis O8h O V Set System Boot Options Chassis O9h O V Set Front Panel Button Chassis O8h O V Set Power Cycle Interval Chassis O8h O V Set Power Cycle Interval Chassis O8h O V Set Power Cycle Interval Chassis OFh O V Set Power Cycle Interval Chassis OFh O V Set Event Receiver S/E O1h M V Set Event Receiver S/E O1h M V Set Event Receiver S/E O1h M V	Get System Info Parameters		59h	0	V	
Get Chassis Capabilities Chassis 00h M V Get Chassis Status Chassis 01h M V Chassis Control Chassis 02h M V Chassis Reset Chassis 03h O This command is combined to Chassis Chassis Identify Chassis 04h O V Set Chassis Capabilities Chassis 05h O V Set Power Restore Policy Chassis 06h O V Get System Restart Cause Chassis 07h O V Only 01h (cycle,hardware reset), 04h,8h,9 Set System Boot Options Chassis 08h O V Supported Set System Boot Options Chassis 08h O V Supported Set Front Panel Button Chassis 09h O V Set Power Cycle Interval Chassis 0Ah O Get POH Counter Chassis 0Bh O V Set Event Receiver S/E 00h M V Get Event Receiver S/E 01h M V						
Get Chassis StatusChassis01hMVChassisControlChassis02hMVChassisControlChassis03hOThis command is combined to ChassisChassis ResetChassis03hOVChassis IdentifyChassis04hOVSet Chassis CapabilitiesChassis05hOVSet Power Restore PolicyChassis06hOGet System Restart CauseChassis07hOVSet System Boot OptionsChassis08hOVGet System Boot OptionsChassis09hOVSet Front Panel ButtonChassis08hOVEnablesChassis07hOVSet Power Cycle IntervalChassis09hOVSet Power Cycle IntervalChassisGet POH CounterChassis07hOVSet Event ReceiverS/E00hMVGet Event ReceiverS/E01hMVPlatform Event (a.k.a. "Event Message")S/E02hMVPEF and Alerting CommandsS/E02hMV	Get Chassis Capabilities	Chassis	00h	М	V	
ChassisControlChassis02hMVChassis ResetChassis03hOThis command is combined to Chassis Control command in IPMI v1.5Chassis IdentifyChassis04hOVSet Chassis CapabilitiesChassis05hOVSet Chassis CapabilitiesChassis06hOVGet System Restart CauseChassis07hOVGet System Boot OptionsChassis08hOVSet Front Panel ButtonChassis09hOVSet Power Cycle IntervalChassis08hOVSet Event ReceiverS/E00hMVGet Event ReceiverS/E00hMVPlatform Event (a.k.a. "Event Message")S/E02hMVPEF and Alerting CommandsS/E02hMV						
Chassis ResetChassis03hOThis command is combined to Chassis Control command in IPMI v1.5Chassis IdentifyChassis04hOVSet Chassis CapabilitiesChassis05hOVSet Power Restore PolicyChassis06hOVGet System Restart CauseChassis07hOVSet System Boot OptionsChassis08hOVGet System Boot OptionsChassis09hOVSet Front Panel ButtonChassis09hOVSet Power Cycle IntervalChassis08hOVSet Power Cycle IntervalChassis0FhOVGet POH CounterChassis0FhOVSet Event ReceiverS/E00hMVGet Event ReceiverS/E00hMVPlatform Event (a.k.a. "Event Message")S/E02hMVPEF and Alerting CommandsONVImage: CommandsCommandsImage: CommandsImage: CommandsImage: CommandsPEF and Alerting CommandsImage: CommandsImage: CommandsImage: CommandsCommandsImage: CommandsImage: Co					V	
Chassis ResetChassisOshOControl command in IPMI v1.5Chassis IdentifyChassis04hOVSet Chassis CapabilitiesChassis05hOVSet Chassis CapabilitiesChassis06hOVGet System Restart CauseChassis07hOVOnly 01h (cycle,hardware reset), 04h,8h,SSet System Boot OptionsChassis08hOVGet System Boot OptionsChassis09hOVSet Front Panel ButtonChassis0AhOEnablesOhassis0BhOVSet Power Cycle IntervalChassis0BhOVGet POH CounterChassis0FhOVEvent CommandsImage: Command CommandsImage: Command Command Command CommandsImage: Command						This command is combined to Chassis
Chassis IdentifyChassis04h0VSet Chassis CapabilitiesChassis05h0VSet Power Restore PolicyChassis06h00Get System Restart CauseChassis07h0VOnly 01h (cycle,hardware reset), 04h,8h,SSet System Boot OptionsChassis08h0V0Get System Boot OptionsChassis08h0VGet System Boot OptionsChassis09h0VSet Front Panel ButtonChassis0Ah0VEnablesChassis0Bh0VSet Power Cycle IntervalChassis0Bh0VGet POH CounterChassis0Fh0VEvent CommandsSet Event ReceiverS/E00hMVPlatform Event (a.k.a. "Event Message")S/E02hMVPEF and Alerting Commands </td <td>Chassis Reset</td> <td>Chassis</td> <td>03h</td> <td>0</td> <td></td> <td></td>	Chassis Reset	Chassis	03h	0		
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,9 supported Set System Boot Options Chassis 08h 0 V Supported Set System Boot Options Chassis 08h 0 V Supported Set System Boot Options Chassis 09h 0 V V Get System Boot Options Chassis 09h 0 V V Set Front Panel Button Chassis 0Ah 0 V Set Power Cycle Interval Chassis 0Bh V Set Power Cycle Interval Chassis 0Bh 0 V V Set Event Receiver S/E 00h M V Get Event Receiver S/E 00h M V V Set Event (a.k.a. "Event (a.k.a. "Event Message") S/E 02h M V Platform Event (a.k.a. "Event Message") S/E 02h M V S/E S/E S/E <td>Chassis Identify</td> <td>Chassis</td> <td>04h</td> <td>0</td> <td>V</td> <td></td>	Chassis Identify	Chassis	04h	0	V	
Set Power Restore Policy Chassis 06h O Get System Restart Cause Chassis 07h O V Only 01h (cycle,hardware reset), 04h,8h,9 supported Set System Boot Options Chassis 08h O V Supported Set System Boot Options Chassis 08h O V Supported Set System Boot Options Chassis 09h O V Supported Set Front Panel Button Chassis 0Ah O V Set Power Cycle Interval Chassis 0Bh V Set Power Cycle Interval Chassis 0Fh O V Set Power Cycle Interval Chassis 0Fh O V Set Event Commands Set System Receiver S/E 00h M V Set Event Receiver S/E 01h M V Set Event (a.k.a. "Event S/E 02h M V Set S/E S/E 02h M V Set S/E S/E 02h M V Set S/E S/E 02h M V S/E 02h M V S/E S/E 02h M <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
Get System Restart CauseChassis07hOVOnly 01h (cycle,hardware reset), 04h,8h,S supportedSet System Boot OptionsChassis08hOVGet System Boot OptionsChassis09hOVSet Front Panel Button EnablesChassis0AhOSet Power Cycle IntervalChassis0BhOVGet POH CounterChassis0FhOVEvent Commands					· ·	
Set System Boot Options Chassis 08h O V Get System Boot Options Chassis 09h O V Set Front Panel Button Chassis 0Ah O V Enables Chassis 0Bh O V Set Power Cycle Interval Chassis 0Bh O V Get POH Counter Chassis 0Fh O V Event Commands					V	Only 01h (cycle,hardware reset), 04h,8h,9h
Get System Boot OptionsChassis09hOVSet Front Panel Button EnablesChassis0AhOVSet Power Cycle IntervalChassis0BhOVGet POH CounterChassis0FhOVEvent Commands </td <td>Set System Boot Options</td> <td>Chassie</td> <td>08h</td> <td>0</td> <td>V</td> <td></td>	Set System Boot Options	Chassie	08h	0	V	
Set Front Panel Button EnablesChassis0AhOSet Power Cycle IntervalChassis0BhOVGet POH CounterChassis0FhOVEvent Commands </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
EnablesCnassisOAnOSet Power Cycle IntervalChassis0BhOVGet POH CounterChassis0FhOVEvent CommandsS/E00hMVSet Event ReceiverS/E00hMVGet Event ReceiverS/E01hMVPlatform Event (a.k.a. "Event Message")S/E02hMVPEF and Alerting CommandsImage: CommandsImage: CommandsImage: Commands		01103313			v	
Set Power Cycle Interval Chassis 0Bh O V Get POH Counter Chassis 0Fh O V Event Commands V V V Set Event Receiver S/E 00h M V Get Event Receiver S/E 01h M V Platform Event (a.k.a. "Event Message") S/E 02h M V PEF and Alerting Commands V V V V		Chassis	0Ah	0		
Get POH Counter Chassis 0Fh O V Event Commands Image: Commands Image: Commands Image: Commands Image: Commands Set Event Receiver S/E 00h M V Image: Commands Image: Commands <t< td=""><td></td><td>Chassic</td><td>0Rh</td><td>0</td><td>V</td><td></td></t<>		Chassic	0Rh	0	V	
Event Commands Set Event Receiver S/E 00h M V Get Event Receiver S/E 01h M V Platform Event (a.k.a. "Event Message") S/E 02h M V PEF and Alerting Commands Image: Command Set Event Set						
Set Event Receiver S/E 00h M V Get Event Receiver S/E 01h M V Platform Event (a.k.a. "Event Message") S/E 02h M V PEF and Alerting Commands Image: Commands Image: Commands Image: Commands Image: Commands Image: Commands		01103515		0	V	
Get Event Receiver S/E 01h M V Platform Event (a.k.a. "Event Message") S/E 02h M V PEF and Alerting Commands V V V		C/E	005	Ν./	M	
Platform Event (a.k.a. "Event S/E 02h M V Message") PEF and Alerting V Commands V						
Message") S/E 0211 W V PEF and Alerting Commands Image: Command set of the se		S/⊏	UIN	IVI	V	
PEF and Alerting Commands		S/E	02h	М	V	
Commands						
IGet PEF Capabilities S/E 10h M V	Commands		1.6.			
	Get PEF Capabilities	S/E	10h	М	V	

104 HPS-621U2A User's Manual

User's Manual

Arm PEF Postpone Timer	S/E	11h	М	V	
Set PEF Configuration					Does not support parameter 15.
Parameters	S/E	12h	Μ	V	
Get PEF Configuration					Does not support parameter 15.
Parameters	S/E	13h	Μ	V	Does not support parameter 15.
Set Last Processed Event ID	S/E	14h	М	V	
Get Last Processed Event ID	S/E	15h	M	V	
Alert Immediate	S/E	16h	0	V	
PET Acknowledge	S/E	17h	0	V	
Sensor Device Commands	5/L	1711	0	v	
Get Device SDR Info	S/E	20h	0	V	
Get Device SDR	S/E	2011 21h	0	V	
Reserve Device SDR			0		
Repository	S/E	22h	0	V	
Get Sensor Reading Factors	S/E	23h	0	V	Support linear sensors only.
Set Sensor Hysteresis	S/E	23h	0	V	
Get Sensor Hysteresis	S/E	25h	0	V	
Set Sensor Threshold	S/E	26h	0	V	
Get Sensor Threshold	S/E S/E	2011 27h	0	V	
Set Sensor Event Enable	S/E S/E	2711 28h	0	V	
Get Sensor Event Enable	S/E S/E	28n 29h	0	V	
	S/E S/E		0	V	
Re-arm Sensor Events Get Sensor Event Status	S/E S/E	2Ah 2Bh	0	V	
			M	V	
Get Sensor Reading	S/E S/E	2Dh 2Eh	0	V	
Set Sensor Type			-	V	
Get Sensor Type	S/E	2Fh	0	V	
Set Sensor Reading and	S/E	30h	0	V	Sensor should be settable (just for FW
Event Status					engineer debug purpose internally)
FRU Device Commands	Charage	104	N 4	N/	
Get FRU Inventory Area Info	Storage		M	V	
Read FRU Data	Storage		M	V	
Write FRU Data	Storage	12h	М	V	
SDR Device Commands	01	0.01			
Get SDR Repository Info	Storage	20h	М	V	
Get SDR Repository	Storage	21h	0	V	
Allocation	-	0.01			
Reserve SDR Repository	Storage		M	V	
Get SDR	Storage	23h	M	V	
Add SDR	Storage			V	
Partial Add SDR	Storage		M	V	
Delete SDR	Storage		0		
Clear SDR Repository	Storage		M	V	
Get SDR Repository Time	Storage		0	V	
Set SDR Repository Time	Storage		0		
Enter SDR Repository Update	Storage		0		
Exit SDR Repository Update	Storage		0		
Run Initialization Agent	Storage	2Ch	0	V	
SEL Device Commands	01	4.01			
Get SEL Info	Storage		Μ	V	
Get SEL Allocation Info	Storage		0	V	
Reserve SEL	Storage		0	V	
Get SEL Entry	Storage		M	V	
Add SEL Entry	Storage		Μ	V	
Partial Add SEL Entry	Storage		0	V	
Delete SEL Entry	Storage		0	V	
Clear SEL	Storage		Μ	V	
Get SEL Time	Storage		М	V	
Set SEL Time	Storage		М	V	
Get Auxiliary Log Status	Storage				
Set Auxiliary Log Status	Storage	5Bh	0		

Get SEL Time UTC Offset	Storage	5Ch	0	V	
Set SEL Time UTC Offset	Storage	5Dh	Õ	V	
LAN Device Commands	g				
Set LAN Configuration	Transpo	01h	М	V	param #9, 25 are not support
Parameter	rt	• …			nonen llo of any national at
Get LAN Configuration Parameters	Transpo rt	02h	М	V	param #9, 25 are not support
Suspend BMC ARPs	Transpo rt	03h	0	V	
Get IP/UDP/RMCP Statistics	Transpo rt	04h	0		
Serial/Modem Device					
Commands					
Set Serial/Modem	Transpo	10h	М	V	
Configuration	rt				
Get Serial/Modem Configuration	Transpo rt	11h	М	V	
Set Serial/Modem Mux	Transpo rt	12h	0	V	
Get TAP Response Codes	Transpo rt	13h	0		
Set PPP UDP Proxy Transmit	Transpo rt	14h	0		
Get PPP UDP Proxy Transmit	Transpo rt	15h	0		
Send PPP UDP Proxy Packet	Transpo rt	16h	0		
Get PPP UDP Proxy Receive	Transpo rt	17h	0		
Callback	Transpo rt	19h	0		
Set User Callback Options	Transpo rt	1Ah	0		
Get User Callback Options	Transpo rt	1Bh	0		
Set Serial Routing Mux Command	Transpo rt	1Ch	0		
SOL Activating	Transpo rt	20h	0		
Set SOL Configuration Parameters	Transpo rt	21h	0	V	param #7 is not support
Get SOL Configuration Parameters	Transpo rt	22h	0	V	param #7 is not support
Command Forwarding Commands					
Forwarded Command	Transpo rt	30h	0		
Set Forwarded Commands	Transpo rt	31h	0		
Get Forwarded Commands	Transpo rt	32h	0		
Enable Forwarded Commands	Transpo rt	33h	0		
Bridge Management Commands					
Get Bridge State	Bridge	00h	0		
Set Bridge State	Bridge	01h	0		
Get ICMB Address	Bridge	02h	0		
Set ICMB Address	Bridge	03h	0		
Set Bridge ProxyAddress	Bridge	04h	0		
Get Bridge Statistics	Bridge	05h	0		

User's Manual

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)	Bhuge	5411	0	
GetEventReceptionState	Bridge	35h	0	
(optional)	Bhage	0011	0	
Other Bridge Commands				
Error Report (optional)	Bridge	FFh	0	
OEM Commands for Bridge				
NetFn				
		C0h	-	
OEM Commands	Bridge	-FE	0	
		h		

APPENDIX-C IPMI OEM COMMANDS LIST

Command	NetFn	CM D	DATA Length	DATA Value	Comments
Set Fan Mode	0x30	01h	1	0~3	Input data: 0=standard speed , 1= full speed , 2=optimal speed , 3=manual speed
Get Fan Mode	0x30	30h	0		Response data: 0=standard speed , 1= full speed , 2=optimal speed , 3=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 SOCFlash Lock	0x30	33h	1	0~1	Input data: 0=enable use socflash tool 1=disable use socflash tool
Set Fan Speed	0x30	35h	2	Byte1 : 0~4 Byte2 : 0~100	Input data: Byte 1 = fan number Byte2 = PWM duty cycle
Get Fan Speed	0x30	36h	0		Response data: Byte1 = cpu0 fan pwm duty cycle Byte2 = cpu1 fan pwm duty cycle Byte3 = sys fan 1 pwm duty cycle Byte4 = sys fan 2 pwm duty cycle Byte5 = sys fan 3 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
Get System Operation Time	0x30	40h	0		Response data Byte1 = Low Low hours Byte2 = Low hours Byte3 = High hours Byte4 = High High hours The total hours = 256*256*256*byte4 + 256*256*byte3 + 256* byte2 + byte1

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:

F		
+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

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
SYS_FAN4	1600 RPM	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

Table F-1	Dofault	Configuration
	Default	Configuration

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
	UEFI environment	AfuEfix64.efi
	OEFTenvironment	Need to disable SPS by JME1 jumper.
Local Update	Windows PE environment	AFUWINx64.EXE
		Need to disable SPS by JME1 jumper.
	IPMI command	Yafuflash.exe
Pomoto undoto		No need to disable SPS.
Remote update	IPMI Web UI	No tool required
		No need to disable SPS.

1.1 BIOS + SPS update in UEFI environment

1. Format a USB flash drive to FAT32.

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

This	s PC > USB Drive (G:) >		
^	Name Siz	e	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.

Power on system. When you hear BIOS ready beep, perss F11 to enter boot

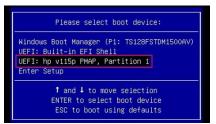
1. Format a USB flash drive to FAT32.

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

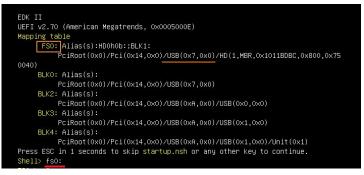
2. Download the update tool and BIOS file(xxx.bin), then save at the **root** directdory of the USB drive.

This	This PC > USB Drive (G:) >				
^	Name Size		Date r		
	EFI	521 KB	12/11, 7/19/2		
	BIOS.bin BIOS file 3	2,768 KB	1/2/2(
	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	: fs0:\			
12/11/19	04:17p	<dir></dir>	4,096	
07/19/18	06:33p		532,592	AfuEfix64.efi
01/02/20	04:46p	33	,554,432	BIOS.bin
06/16/16	02:00a		430	FlashAll.nsh
3	File(s)	34,087,454	bytes	
1	Dir(s)			
fs0:\> <u>Flas</u>	1All.nst	BIOS.bin_	input you	ır BIOS file name

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

Bergaran Alan	
Reading flash done	
– ME Data Size checking . ok	
– FFS checksumsok	
– 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	
– Update success for FDR	
– Update success for PTT –	
– Successful Update Recovery Loader to OPRx!!	
– Successful Update MFSB. –	
– Successful Update FTPR!!–	
– Successful Update MFS, IVB1 and IVB2!!	
– Successful Update FLOG and UTOK!!	
– ME Entire Image update success !!	
	s take effe

- 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:

· · · · · · · · · · · · · · · · · · ·	t <mark>ility – Copyright (C) 2020 American</mark> t Security Boot Save & Exit
BIOS Information	
BIOS Vendor	American Megatrends
Core Version	5.14
Compliancy	UEFI 2.7; PI 1.6
Project Version	0ACLA 0.45 x64
Build Date and Time	09/09/2020 14:30:17
Access Level	Administrator
BIOS Name	HPM6210B
BIOS Version	0.0B
System Language	[English]
▶ Intel RC Version	

SPS version:

Aptio Setup Utility - C Main Advanced Server Mgmt Securit	
Processor Configuration	General ME Configuration SPS version
UPI Configuration	Oper. Firmware Version 304:4.1.4.25
Memory Configuration	Backup Firmware Version N/A
IIO Configuration	Recovery Firmware Version 0A:4.1.4.25
PCI Express Configuration	ME Firmware Status #1 0x000F0245
SSATA Configuration	ME Firmware Status #2 0x88118026
Miscellaneous Configuration	Current State Operational
▶ Server ME Configuration 2	Error Code No Error

1.2 BIOS + SPS update in Windows PE environment

1. Copy update tool and BIOS file(xxx.bin) to WinPE disk.

This PC > WINPE_X64 (H:) > AfuWin64					
^	Name	Size	I		
	📑 AFUWINx64.EXE	566 KB	1		
	🗟 amifldrv64.sys	19 KB	1		
	BIOS.bin BIOS file	32,768 KB	÷		
	💿 FlashAll.bat	1 KB			

2. Plug the WinPE disk to server and close pin 2-3 of JME1.

3. Power on system. When you hear BIOS ready beep, press **F11** to enter boot menu and select the WinPE disk.



4. Switch to BIOS folder and run the command.

FlashAll.bat [BIOS file name]

11/28/2019	11:53	AM	<dir></dir>		
11/28/2019	11:53	AM	<dir></dir>		
07/19/2018	06:57	PM		579,184	AFUWINx64.EXE
03/30/2017	12:05	AM		19,432	amifldrv64.sys
01/02/2020	04:46	PM	33	,554,432	BIOS.bin
12/03/2019	05:35	PM		33	FlashAll.bat
	4 F	ile(s)	3	4,153,083	l bytes
	2 [Dir(s)	30,49	5,850,490	5 bytes free

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

AMI Firmware Update Utility v5.11.01.1745 Copyright (C)2018 American Megatrends Inc. All Rights F	eserved.
<pre>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 Updating Main Block done Updating Main Block done Updating Main Block done Verifying Main Block done Updating NVRAM Block done Updating NVRAM Block done Updating NVRAM Block done Updating NVRAM Block done Update success for FDR - Update success for PTT Successful Update Recovery Loader to OPRx!! - Successful Update TFPR!! Successful Update FTPR!! Successful Update FTPR!! Successful Update FTPR!! Successful Update FLOG and UTOK!! - ME Entire Image update success !! ARNING : System must power-off to have the changes take effec Process completed.</pre>	t!

- 6. Remove AC power and move **JME1** jumper back to pin 1-2.
- 7. Refer 1.1.1 step9 to check the BIOS and SPS version.

1.3 BIOS + SPS update using IPMI command

1. Copy BIOS file(xxx.hpm) to Yafuflash tool folder

Local Disk (C:) > Yafuflash_Win64					
^	Name	Date modified	Size		
	🗟 amifldrv64.sys	2019/11/19 下午 0	19 KB		
	bios_019.hpm	2019/11/21下午 0	32,769 KB		
	🗟 LIBIPMI.dll	2019/11/19 下午 0	632 KB		
	Yafuflash	2019/11/19下午 0	730 KB		

- 2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.
- 3. Input the command:

Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -d 2 [BIOS file name]. The default username and password are admin/admin.



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

BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IFMI Version BMC Interface(s)	PASSED 32 1 12.01.191106 2.0 KCS, USB	 BMC network configuration жизнаянски собранизации () Configure IPv4 support жизнаянски собранизации () 	3
BMC Support Nait For BMC FRB-2 Timer timeout FRB-2 Timer Policy OS Matchdog Timer OS Mtd Timer Timeout OS Mtd Timer Policy	[Enabled] [Disabled] [Enabled] [Go minutes] [Do Nothing] [Disabled] [10 minutes] [Reset]	Lan channel 1 Configuration Address source Current Configuration Address source Station IP address Subnet mask	[Unspecified] StaticAddress 192.168.1.78 255.255.255.0
BMC Configured Power Control Policy Power Control Policy	Power Restore [Unspecified]	Station MAC address Router IP address Router MAC address	00-11-22-33-44-CC 0.0.0.0 00-00-00-00-00-00
System Event Log Bmc self test log BMC network configuration View System Event Log		жжжжжжжжжжжжжжжжж Configure IPv6 support жжжжжжжжжжжжжжжж	

4. When the process ends, turn off AC power for 10 seconds.

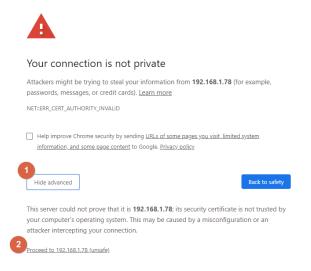


5. Refer 1.1.1 step9 to check the BIOS and SPS version.

1.4 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.

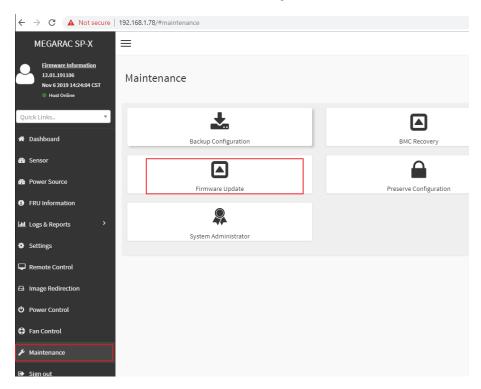
If you get a message that says "Your connection is not private", just skip it.



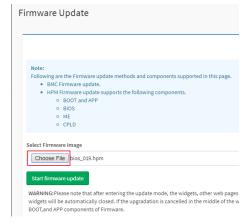
Note: BMC IP address can be configured at BIOS menu.

BMC Self Test Status	PASSED		
BMC Device ID	32	––BMC network configuration––	
BMC Device Revision BMC Firmware Revision	1 12.01.191106	****	
IPMI Version	2.0	Configure IPv4 support	
BMC Interface(s)	KCS, USB	****	3
BMC Support	[Enabled]		
Wait For BMC	[Disabled]	Lan channel 1	
RB-2 Timer	[Enabled]	Configuration Address source	
RB-2 Timer timeout	[6 minutes]	Current Configuration Address	StaticAddress
RB-2 Timer Policy	[Do Nothing]	source	
3S Watchdog Timer 3S Wtd Timer Timeout	[Disabled] [10_minutes]	Station IP address	192.168.1.78
JS Wid Timer Policy	[Reset]		
55 With Filler Forrey	[Neset]	Subnet mask	255.255.255.0
BMC Configured Power		Station MAC address	00-11-22-33-44-CC
Control Policy	Power Restore	Router IP address	0.0.0
Power Control Policy	[Unspecified]	Router MAC address	00-00-00-00-00-00

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**.

Note: Following are the Firmware update mc • BMC Firmware update. • HPM Firmware update supports • BOOT and APP • BIOS • ME • CPLD		192.168.1.78 say Are you sure you v		ок	Cancel
Select Firmware Image					
Choose File bios_019.hpm					
Start firmware update					
Uploaded signImage Public Key Info)				
New signImage Public Key					
Choose File No file chosen			Upload .		
	Preparing to t	flash			
✓ Update All					
List of Components					
# Component Name	Existing Version	Uploaded Version	Upgrade		
2 BIOS	0.0.0	1.0.35651584	~		
Proceed					

5. The message appears, "The device has been updated successfully.". Click **OK**.

Note: Following are the Firmware update methods and components supported in this • BMC Firmware update. • HPM Firmware update supports the following components. • BOOT and APP • BIOS	192.168.1.78 says The device has been updated successfully.	ОК
◦ ME ◦ CPLD		
Choose File bios_019.hpm		
Start firmware update		

6. Server will reset after few seconds, refer 1.1.1 step9 to check the BIOS and SPS version.

1.5 BIOS + SPS update using IPMI command

1. Copy BIOS file(xxx.hpm) to Yafuflash tool folder

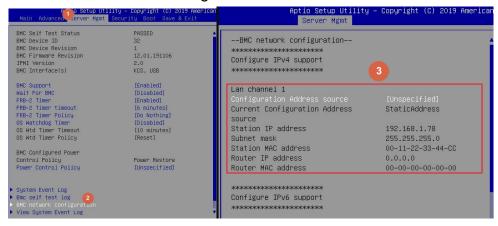
Local Disk (C:) → Yafuflash_Win64					
^	Name	Date modified	Size		
	amifldrv64.sys	2019/11/19 下午 0	19 KB		
	bios_019.hpm	2019/11/21 下午 0	32,769 KB		
	LIBIPMI.dll	2019/11/19下午 0	632 KB		
	Yafuflash	2019/11/19 下午 0	730 KB		

- 2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.
- 3. Input the command:

Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -d 2 [BIOS file name]. The default username and password are admin/admin.



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



4. When the process ends, turn off AC power for 10 seconds.

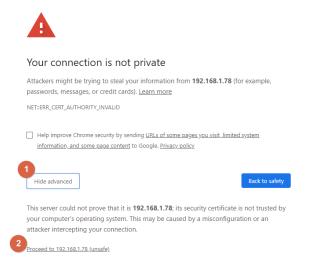


5. Refer 1.1.1 step9 to check the BIOS and SPS version.

1.6 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.

MC Self Test Status MC Device ID MC Device Revision MC Firmware Revision FMI Version MC Interface(s)	PASSED 32 1 12.01.191106 2.0 KCS, USB	 BMC network configuration xecelectedeeelectedeelectedeelectedeelectedeeelectedeelectedee	3
BMC Support Wait For BMC	[Enabled] [Disabled]	Lan channel 1	<u> </u>
FRB-2 Timer	[DISabled]	Configuration Address source	[Unspecified]
FRB-2 Timer timeout	[6 minutes]	Current Configuration Address	StaticAddress
RB-2 Timer Policy	[Do Nothing]	SOURCE	ofur fendul ess
OS Watchdog Timer	[Disabled]		100 100 1 70
DS Wtd Timer Timeout	[10 minutes]	Station IP address	192.168.1.78
OS Wtd Timer Policy	[Reset]	Subnet mask	255.255.255.0
BMC Configured Power		Station MAC address	00-11-22-33-44-CC
Control Policy	Power Restore	Router IP address	0.0.0
Power Control Policy	[Unspecified]	Router MAC address	00-00-00-00-00-00

- ← → C ▲ Not secure | 192.168.1.78/#maintenance MEGARAC SP-X \equiv Firmware Information 12.01.191106 Maintenance Nov 6 2019 14:24:04 CST Host C Quick Links.. ~ * 🖶 Dashboard Backup Configuration BMC Recovery Sensor Δ 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**.

Note: Following are the Firmware update me BMC Firmware update. HPM Firmware update supports BOOT and APP BIOS ME CPLD		192.168.1.78 say		OK Cancel
Select Firmware Image				
Choose File bios_019.hpm				
Start firmware update				
Uploaded signImage Public Key Info				
Ved Nov 6 01:23:50 2019				
New signImage Public Key				
Choose File No file chosen			Upload .	
	Preparing to	o flash		
✓ Update All				
List of Components				
# Component Name	Existing Version	Uploaded Version	Upgrade	
2 BIOS	0.0.0	1.0.35651584	~	
Proceed				

5. The message appears, "The device has been updated successfully.". Click **OK**.

Note: Following are the Firmware update methods and components supported in this • BMC Firmware update. • HPM Firmware update supports the following components. • BOOT and APP • BIOS	192.168.1.78 says The device has been updated successfully.	ок
ME CPLD Select Firmware Image		
Choose File bios_019.hpm Start firmware update		

6. Server will reset after few seconds, refer 1.1.1 step9 to check the BIOS and SPS version.

2. BIOS

Update Method	OS	ТооІ
Local Update	UEFI environment	AfuEfix64.efi
	Windows PE environment	AFUWINx64.EXE

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)	<
Allocation unit size 4096 bytes	~
	<u> </u>
Restore device defaults	

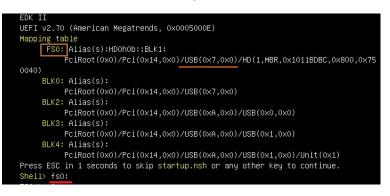
2. Download the tool and BOIS file(xxx.bin) and save at the **root** directdory of the USB drive.

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.



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



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



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

AMI Firmware Update Utility v5.11.01.1744 Copyright (C)2018 American Megatrends Inc. All Rights Reserved. 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 Updating Main Block done Verifying Main Block done Updating Main Block done Verifying Main Block done Updating NVRAM Block done Verifying NVRAM Block done Verifying NVRAM Block done Verifying NVRAM Block done Process completed.	WARNING!! DO NOT turn off the system power, if the BIOS update process has not been finished yet. <null string=""> </null>	
- ME Data Size checking . ok - FFS checksums ok - Check RomLayout ok. Erasing Boot Block done Updating 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	│ AMI Firmware Update Utility v5.11.01.1	744
FS0:\>	 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 Verifying NVRAM Block done 	

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

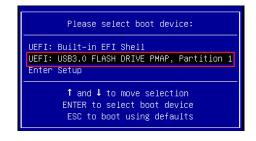
	Utility – Copyright (C) 2020 American (mt Security Boot Save & Exit
BIOS Information	30 J2 30 J2 J3 45
BIOS Vendor	American Megatrends
Core Version	5.14
Compliancy	UEFI 2.7; PI 1.6
Project Version	0ACLA 0.45 x64
Build Date and Time	09/09/2020 14:30:17
Access Level	Administrator
BIOS Name	HPM6210B
BIOS Version	0.0B
System Language	[English]
▶ Intel RC Version	

2.2 BIOS update in Windows PE environment

1. Copy update tool and BIOS file(xxx.bin) to WinPE disk.

•	Name	Size	Date modified	
	📑 AFUWINx64.EXE	566 KB	7/19/2018 6:57 PM	
	amifldrv64.sys	19 KB	3/30/2017 12:05 AM	
	BIOS.bin BIOS fil	e 32,768 KB	1/2/2020 4:46 PM	
	💿 FlashMain.bat	1 KB	12/5/2019 5:45 PM	

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



3. Switch to BIOS folder and run the command.

FlashMain.bat [BIOS file name]

11/28/2019	11:53		<dir></dir>		
11/28/2019	11:53	AM	<dir></dir>		
07/19/2018	06:57	PM		579,184	AFUWINx64.EXE
03/30/2017	12:05	AM		19,432	amifldrv64.sys
12/05/2019	05:45	PM		29	FlashMain.bat
01/02/2020	04:46	PM	33	,554,432	BIOS.bin
	4	File(s)	34	4,153,077	7 bytes
	2 1	Dir(s)	30,49	5,850,496	5 bytes free
					<u></u>
C:\AfuWin64	>Elash	Main ha	t BTOS	hin B	IOS file name

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

AMI Firmware Update Utili Copyright (C)2018 American Megatrenc	
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 Updating Main Block done Updating Main Block done Erasing NVRAM Block done Updating NVRAM Block done Verifying NVRAM Block done Verifying NVRAM Block done Process completed.	×

128 HPS-621U2A User's Manual

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

· · · · · · · · · · · · · · · · · · ·	t <mark>ility – Copyright (C) 2020 American</mark> M Security Boot Save & Exit
BIOS Information	
BIOS Vendor	American Megatrends
Core Version	5.14
Compliancy	UEFI 2.7; PI 1.6
Project Version	0ACLA 0.45 x64
Build Date and Time	09/09/2020 14:30:17
Access Level	Administrator
BIOS Name	HPM6210B
BIOS Version	0.0B
System Language	[English]
▶ Intel RC Version	

3. BMC

Update Method	OS	ТооІ
	DOS environment	Yafuflash.exe.
Local Update	WinPE environment	Yafuflash.exe
Domoto undoto	IPMI Web UI	No tool required
Remote update	IPMI command	Yafuflash.exe

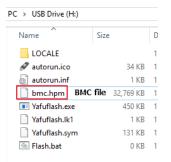
Please refer readme for tool detail information.

3.1 BMC update in DOS environment

1. Download **Rufus** to create a DOS USB drive, <u>https://rufus.ie/</u>.

🖋 Rufus 3.8.1580 (Portable)		-		×
Deixe Descention				
Drive Properties ——				- 1
Device				
NO_LABEL (H:) [3.9GB]	0			\sim
Boot selection				
Disk or ISO image (Please select)	~	\oslash	SELECT	
2 Non bootable	rst	em		_
FreeDOS Disk or ISO image (Please select)		EFI-CSN	1)	~ ?
				_
 Show advanced drive properties 				
Format Options ——				_
Volume label				
3.9GB				
File system	Cluster size	2		
FAT32 ~	4096 byte	s (Defau	lt)	\sim
 Show advanced format options 				
Chatura				
Status —				-
READY	(
🚯 (i) 🚁 💷 🛛 🦉	START		CLOSE	
1 device found				

2. Save BMC file to **root** dictory of the DOS USB drive.



3. Plug the USB drive to the Server and boot to BIOS setup. Switch to **Boot** tab and change **CSM Support** to [**Enable**], **Boot mode select** to [**LEGACY**].

Boot Configuration		
Setup Prompt Timeout	1	
Bootup NumLock State	[0n]	
Quiet Boot	[Enabled]	

Switch to Save & Exit tab and then Save changes and Reset.



4. When you hear BIOS ready beep, press **F11**, and select the DOS USB drive to boot.

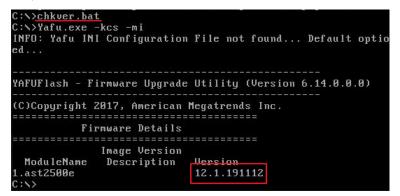
5. Input **flash.bat** [**BMC file name**] and press enter. Please wait. This process may take 40 minutes.

LOCALE		<dir></dir>	11-28-19	3:08p
AUTOEXEC	BAT	96	11-28-19	3:08p
AUTORUN	INF	206	11-28-19	3:08p
AUTORUN	ICO	34,494	11-28-19	3:08p
BMC	HPM 33	,554,991	11-25-19	3:03p
YAFU	EXE	460,378	11-19-19	5:52p
YAFU	LK1	160	11-19-19	5:52p
YAFU	SYM	133,488	11-19-19	5:52p
FLASH	BAT	25	11-29-19	11:55a
	8 file(s)	34,1	83,838 byt	es
	1 dir(s)	3,70	2 Mega byt	es free

6. When the update process finishs, BMC will reset.

•
PLEHSE DU MUI USE IHIS FLHSH IUUL FRUM IHE REDIRECTIUM CUNSULE.
Uploading Firmware Image : 100% done
Skipping [boot] Module
Skipping [conf] Module
Flashing [bkupconf] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Flashing [root] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Flashing [osimage] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Flashing [www] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Flashing [lmedia] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Flashing [ast2500e] Module
Flashing Firmware Image : 100% done
Verifying Firmware Image : 100% done
Resetting the firmware
C:N>_

7. After BMC reset, run chkver.bat to check BMC firmware version.



8. Reboot to BIOS and restore the CSM support and Boot mode select settings.

Main Advanced Server	Agmt Security Boot Save & Exit
Boot Configuration	
Setup Prompt Timeout	1
Bootup NumLock State	[0n]
Quiet Boot	[Enabled]
CSM Support	[Disable]
Boot mode select	[UEFI]

Save changes and exit.

3.2 BMC update in WinPE environment

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

This F	PC → WINPE_X64 (J:) → Yafufl	ash_Win64
^	Name	Size
	🚳 amifldrv64.sys	19 KB
	bmc.hpm BMC file	32,769 KB
٠	💿 chkver.bat	1 KE
e	💿 Flash.bat	1 KE
e	🚳 LIBIPMI.dll	632 KE
т	Yafuflash.exe	730 KE

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: Built-in EFI Shell UEFI: USB3.0 FLASH DRIVE PMAP, Partition 1 Enter Setup
↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

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

Flash.bat [BMC file]

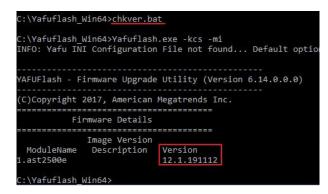
12/06/2019	11:51 AM	<dir></dir>	
12/06/2019	11:51 AM	<dir></dir>	
11/19/2019	05:52 PM	19,432	amifldrv64.sys
12/06/2019	11:50 AM	22	chkver.bat
12/06/2019	11:50 AM	30	Flash.bat
11/19/2019	05:52 PM	647,168	LIBIPMI.dll
11/19/2019	05:52 PM	747,520	Yafuflash.exe
11/25/2019	03:03 PM	33,554,991	bmc.hpm
	6 File(s) 34,969,163	3 bytes
	2 Dir(s)	30,669,848,570	5 bytes free
C:\Yafuflas	h_Win64>Flas	h.bat bmc.hpm	BMC file name

Please wait. This may take few minutes.

4. When the update process finishs, BMC will reset.

WARNING	! FTRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
	PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*******	*****
Uploadin	g Firmware Image : 100% done
Skipping	[boot] Module
Skipping	[conf] Module
	[bkupconf] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
	[root] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
	[osimage] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
	[www] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
	[lmedia] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
	[ast2500e] Module
	Firmware Image : 100% done
	g Firmware Image : 100% done
Resettin	g the firmware

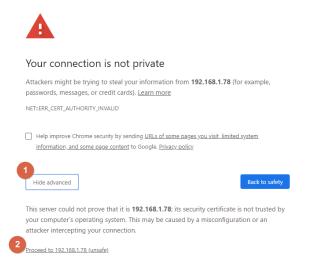
5. After BMC reset, run chkver.bat to check BMC firmware version.



3.3 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.

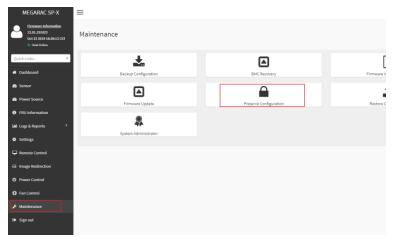
If you get a message that says "Your connection is not private", just skip it.



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

MC Self Test Status MC Device ID MC Device Revision MC Firmware Revision FMI Version MC Interface(s)	PASSED 32 1 12.01.191106 2.0 KCS, USB	 BMC network configuration xecelectedeeelectedeelectedeelectedeelectedeeelectedeelectedee	3
BMC Support Wait For BMC	[Enabled] [Disabled]	Lan channel 1	<u> </u>
FRB-2 Timer	[DISabled]	Configuration Address source	[Unspecified]
FRB-2 Timer timeout	[6 minutes]	Current Configuration Address	StaticAddress
RB-2 Timer Policy	[Do Nothing]	SOURCE	ofur fendul ess
OS Watchdog Timer	[Disabled]		100 100 1 70
DS Wtd Timer Timeout	[10 minutes]	Station IP address	192.168.1.78
OS Wtd Timer Policy	[Reset]	Subnet mask	255.255.255.0
BMC Configured Power		Station MAC address	00-11-22-33-44-CC
Control Policy	Power Restore	Router IP address	0.0.0
Power Control Policy	[Unspecified]	Router MAC address	00-00-00-00-00-00

2. Click the Maintenance tab, then Preserve Configuration.



Check all and Save.

	6
Click here to go to Firmware Update or Restore Factory Defaults	
✓ Check All	
✓ SDR	
✔ FRU	
✓ SEL	
V IPMI	
V Network	
V NTP	
✓ SNMP	
✓ SSH	
🗸 кли	
✓ Authentication	
✓ Syslog	
✓ Web	

3. Click the link to go to Firmware Upate.

P	Preserve Configuration	
	Click here to go to Firmware Update or Restore Factory Defaults	(
	✓ Check All	

4. Choose File to select BMC file.

Note:	
	ng are the Firmware update methods and components supported in this pa
	3MC Firmware update.
• •	IPM Firmware update supports the following components.
	BOOT and APP
	 BIOS ME
	o CPLD
	- GLD
Select Fir	mware Image

5. Click the Start firmware update button, then scroll down and click Proceed.

		Preparing to flash		
~	Update All			
List	t of Components			
#	Component Name	Existing Version	Uploaded Version	Upgrade
1	BOOT	12.1.0	12.1.0	~
2 Proc	APP	12.1.191023	12.1.191127	×

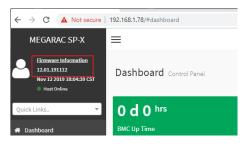
The message appears, "Are you sure you want to flash?". Click **OK**.

ponents supported in this	192.168.1.78 says Are you sure you want to flash?		
components.		ОК	Cancel

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

7	SNMP	192.168.1.78 says
8	SSH	Firmware reset has been called. Close the current session, and open a new session after a couple of minutes.
9	КУМ	ок
10	AUTHENTICATION	
11	SYSLOG	Overwrite 新行語計中解
12	WEB	overwrite
unloaded si	animage Public Key Info	

7. Reboot the server and then login to check the BMC firmware version.



3.4 BMC update using IPMI tool

1. Save **BMC** file to **Yafuflash** folder.

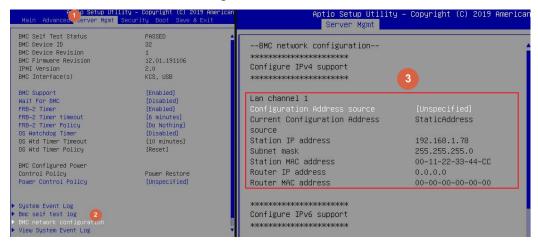
Loc	al Disk (C:) > Yafuflash_Win64			
	Name	Date modified	Size	Туре
	amifldrv64.sys	2019/11/19下午0	19 KB	System
*	🗟 LIBIPMI.dll	2019/11/19 下午 0	632 KB	Applica
A	📧 Yafuflash	2019/11/19下午 0	730 KB	Applica
*	bmc.hpm BMC file name	2019/11/28 下午 0	32,769 KB	HPM Fi
*				

- 2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.
- 3. Input the command:

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



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



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

The update process will start.

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

VARNING! FIRMWARE HEGRADE MUST NOT BE INTERRIPTED ONCE IT IS STARTED
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED. PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.

Uploading Firmware Image : 31%

5. When the update process finishs, BMC will reset.

**********	*****************
	BE INTERRUPTED ONCE IT IS STARTED. SH TOOL FROM THE REDIRECTION CONSOLE.
ploading Firmware Image : 100% kipping [boot] Module lashing [bkupconf] Module erifying Firmware Image : 100% erifying Firmware Image : 100% lashing [root] Module lashing Firmware Image : 100% erifying Firmware Image : 100% lashing [osimage] Module lashing Firmware Image : 100% erifying Firmware Image : 100% lashing [media] Module lashing Firmware Image : 100% lashing Firmware Image : 100% lashing Firmware Image : 100% lashing Firmware Image : 100%	done done done done done done done

6. Reboot the server. Check BMC firmware version by following fommand. Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -mi

C:\Yafuflash_Win64>Yafuflash.exe -nw -ip <u>192.168.1.78</u> -U <u>admin</u> -P <u>admin</u> -mi INFO: Yafu INI Configuration File not found Default options will not be applied
Creating IPMI session via network with address 192.168.1.78Done
YAFUFlash – Firmware Upgrade Utility (Version 6.14.0.0.0)
(C)Copyright 2017, American Megatrends Inc.
Firmware Details
Image Version ModuleName Description Version 1.ast2500e 12.1.191112

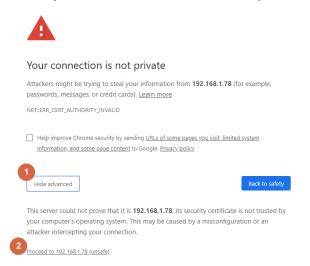
4. CPLD

Update Method	OS	ТооІ
Domoto undoto	IPMI Web UI	No tool required
Remote update	IPMI command	Yafuflash.exe

4.1 CPLD update using Web UI

1. Open 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.

	lity – Copyright (C) 2019 American Security Boot Save & Exit	Aptio Setup Utility Server Mgmt	y – Copyright (C) 2019 Americ
BMC Self Test Status BMC Device ID BMC Device Revision BMC Firmware Revision IPMI Version BMC Interface(s)	PASSED 32 1 12.01.191106 2.0 KCS, USB	BMC network configuration *************************** Configure IPv4 support *****	3
BMC Support Wait For BMC FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Watchdog Timer	[Enabled] [Disabled] [Enabled] [6 minutes] [Disabled] [10 minutes]	Lan channel 1 Configuration Address source Current Configuration Address source Station IP address	[Unspecified] StaticAddress 192.168.1.78
OS Wtd Timer Policy BMC Configured Power Control Policy Power Control Policy	[Reset] Power Restore [Unspecified]	Subnet mask Station MAC address Router IP address Router MAC address	255.255.255.0 00-11-22-33-44-CC 0.0.0.0 00-00-00-00-00-00
System Event Log Bmc self test log 2 BMC network configuration View System Event Log		жакжакжакжакжакжака Configure IPv6 support жакажакакакакакакакака	

- ← → C ▲ Not secure | 192.168.1.78/#maintenance MEGARAC SP-X \equiv Firmware Information 12.01.191106 Maintenance Nov 6 2019 14:24:04 CST Host (Quick Links.. . 1 A Dashboard Backup Configuration BMC Recovery Sensor Δ 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 CPLD file.



4. Click the Start firmware update button, then scroll down and click Proceed.

		Preparing to	flash	
~	Update All			
Lis	t of Components			
#	Component Name	Existing Version	Uploaded Version	Upgrade
1	CPLD	12.1.191112	1.0.35651584	~
Proc	seed			

The message appears, "Are you sure you want to flash?". Click **OK**.

	192.168.1.78 says		
nponents supported in this	Are you sure you want to flash?		
components.		ок	Cancel

5. The message appears, "The device has been updated successfully". Click **OK**.

	192.168.1.78 says	
	The device has been updated successfully.	
_		ОК

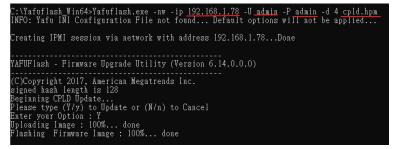
6. Shutdown the server and turn off AC power for 10 seconds.

4.2CPLD update using IPMI tool

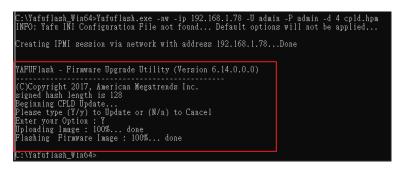
1. Save CPLD file to Yafuflash folder.

Loc	al Disk (C:) > Yafuflash_Wir	164	
	Name	Size	Da
*	🗟 amifldrv64.sys	19 KB	20
7	cpld.hpm CPLD file	494 KB	20
×	LIBIPMI.dll	632 KB	20
*	Yafuflash	730 KB	20
*			

- 2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.
- 3. Input the command: Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -d 4 [CPLD file name]. The default username and password are admin/admin.



4. After the process finishing, shutdown the server and turn off AC power for 10 seconds.



APPENDIX-G SMART FAN CONFIGURATION

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

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

Where:

Function code 0x30 is the OEM function code, and default Privilege Level is User. If you use "ipmiutil" tool in Windows OS, replace "0x30" with "00 20 C0".
 Cmd Command code. This message byte specifies the operation that it to be executed.
 Data Zero or more bytes of data, as required by given command.

OEM Command table

Description	Function code	Cmd	Data/Response data	
	0x30	0x01	[Mode] 0 = standard mode 1 = full mode 2 = optimal mode 3 = manual mode	
Set fan mode			100 100 100 100 90 90 90 90 90 90 90 90 90	STANDARD OPTIMAL FULL

Get fan mode	0x30 0x30		The response data is the fan mode. 0 = standard mode 1 = full mode 2 = optimal mode 3 = manual mode
Set fan PWM $0x30$ $0x35$ $[Fan] [PWM]$ $Fan:$ $0 = CPU1_FAN1$ $1 = CPU2_FAN1$ $2 = SYS_FAN1$ $3 = SYS_FAN2$ $4 = SYS_FAN3$ PWM:		Fan: 0 = CPU1_FAN1 1 = CPU2_FAN1 2 = SYS_FAN1 3 = SYS_FAN2 4 = SYS_FAN3	
Get fan 0x30 0x36 The response data represent each fan PWM. Byte1 = cpu0 fan pwm duty cycle Byte2 = cpu1 fan pwm duty cycle Byte3 = sys fan 1 pwm duty cycle Byte4 = sys fan 2 pwm duty cycle Byte5 = sys fan 3 pwm duty cycle Byte5 = sys fan 3 pwm duty cycle		Byte1 = cpu0 fan pwm duty cycle Byte2 = cpu1 fan pwm duty cycle Byte3 = sys fan 1 pwm duty cycle Byte4 = sys fan 2 pwm duty cycle	

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

Example

Locally set PWM of SYS_FAN3 to 0x20 by "ipmiutil" in Windows OS.

Step 1. Run Command Prompt as Administrator.

Step 2. Get fan mode

C:\ipmiutil-3.1.5-win32≻ipmiutil cmd 00 20 c0 30	
ipmiutil cmd ver 3.15	
This is a test tool to compose IPMI commands.	
Do not use without knowledge of the IPMI specification	•
BMC version 0.6, IPMI version 2.0	X
respData len=1:00 Response data	30 = Get mode
send_icmd ret = 0 UU = standard mode	oo accimoac
ipmiutil cmd, completed successfully	

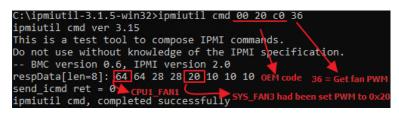
Step 3. Set fan mode to manual mode



Step 4. Set fan PWM

C:\ipmiutil-3.1.5-win32>ipmi	util cmd <u>00 20 c0</u> 35 4 20
ipmiutil cmd ver 3.15	
This is a test tool to compo	se IPMI commands.
Do not use without knowledge	of the IPMI specification, PWM = 0x20
BMC version 0.6, IPMI ver	sion 2.0
respData[len=1]: 00	
send icmd ret = 0	OEM code 35 = Set PWM 4 = SYS FAN3
ipmiutil cmd, completed succ	essfully

Step 5. Get fan PWM

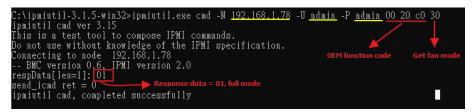


Remotely set PWM of CPU1_FAN1 to 0x10 by "ipmiutil" in Windows OS.

Step 1. Run Command Prompt as Administrator.

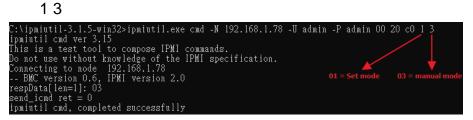
Step 2. Get fan mode

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0 30



Step 3. Set fan mode to manual mode

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0



Step 4. Set fan PWM

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0 35 0 10



Step 5. Get fan PWM

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0

36

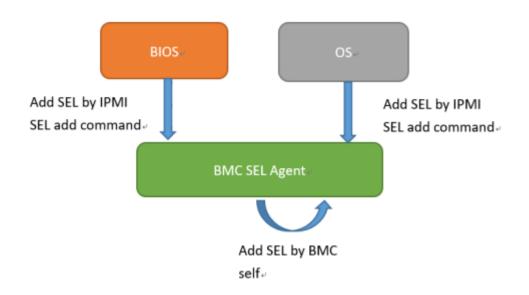


APPENDIX-H SYSTEM EVENT LOG(SEL)

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 U Note: There are various websites that convert the raw number to a date/time.	
8, 9	Generator ID (GID)	 D) RqSA and LUN if event was generated from IPMB. Software ID if event was generated from system software. Byte 1 [7:1] – 7-bit I2C slave address, or 7-bit system software ID [0] – 0b = ID is IPMB slave address, 1b = System software ID Software ID values: 0001h – BIOS POST for POST errors, RAS configuration/state, timestamp synch, OS boot e 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. 	
10	EvM Rev (ER)	[1:0] – IPMB device LUN if byte 1 holds slave address. 00b otherwise. Event message format version. 04b = IPMI v2.0 (default) 03b = IPMI v1.0	
11	Sensor Type (ST)	Sensor type code for sensor that generated the event.	
12	Sensor # (SN)	Number of sensor that generated the event (from SDR).	
13	Event Dir/Event Type (EDIR)	Event Dir [7] - 0b = Assertion event, 1b = Deassertion event. Event Type Type of trigger for the event; for example, critical threshold going high, state asserted, and so on Also indicates class of the event; for example, discrete, threshold, or OEM. The Event Type field encoded using the Event/Reading Type Code. [6:0] - Event Type Codes 01h = Threshold (states = 0x00-0x0b) 02h-0ch = Discrete 6Fh = Sensor-specific 70-7Fh = OEM	
14	Event Data 1 (ED1)		
15	Event Data 2 (ED2)	See Table 2.	
16	Event Data 3 (ED3)	-/	

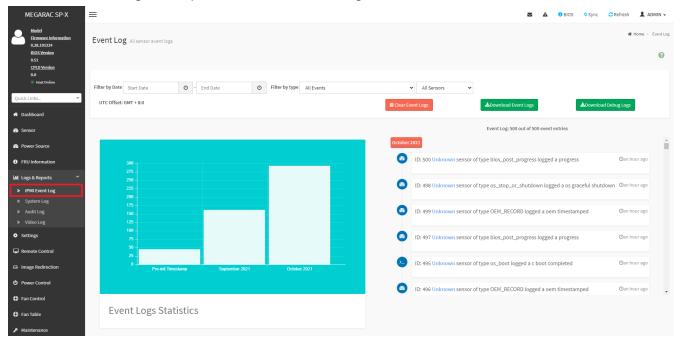
When capturing the SEL log, always collect both the text/human readable version and the hex version. Because some of the data is OEM-specific, some utilities cannot decode the information correctly. In addition, with some OEM-specific data there may be additional variables that are not decoded at all.

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 Device Revision BMC Firmware Revisi	erver Mgmt Security Boot Save & Ex	American Megatrends, Inc. dt
IPMI Version BMC Interface(s)	ı 1	▲ Press <enter> to view the System Event Log Records.</enter>
BMC Support Wait For BMC FRB-2 Timer FRB-2 Timer timeout FRB-2 Timer Policy OS Watchdog Timer OS Witd Timer Timeou OS Witd Timer Policy	[Do Nothing] [Disabled] rt [10 minutes]	++: Select Screen
BMC Configured Powe Control Policy Power Control Polic	Always Power Up	11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values
 System Event Log Bmc self test log BMC network configu View System Event L BMC User Settings BMC Warm Reset 		F3: Optimized Defaults F4: Save & Exit ESC: Exit
. Vers	ion 2.20.1275. Copyright (C) 2021 Am	merican Megatrends, Inc.
	Setup Utility – Copyright (C) 2021 rver Mgmt	American Megatrends, Inc.
No. of log entries	in SEL : 566	HEX:
DATE TIME	SENSOR TYPE	01 00 02 EE 4A 55 61 20 00 04 18 94 03 01 EE EE
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14	Chassis System ACPI Power State	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0)
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17	Chassis System ACPI Power State System Firmware Progress	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:52:09	Chassis System ACPI Power State System Firmware Progress System ACPI Power State	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown)
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:52:09 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:52:09 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State DEM (Unknown) DEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown)
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:52:09 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State DEM (Unknown) DEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:29:17 09/30/21 05:20:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event.
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:25:09 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:20:14 09/30/21 05:20:14 09/30/21 05:20:14 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:20:10 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State DEM (Unknown) DEM (Unknown) DEM (Unknown) DEM (Unknown) DEM (Unknown) DEM (Unknown) DEM (Unknown)	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Senson Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item Enter: Select
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:20:19 09/30/21 05:52:09 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) Chassis	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) System Boot/Restart Initiated	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:20:19 01/01/70 00:00:18	Chassis System ACPI Power State System Firmware Progress System ACPI Power State DEM (Unknown) DEM (Unknown) System Boot/Restart Initiated System ACPI Power State	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:17 09/30/21 05:29:17 09/30/21 05:29:17 09/30/21 05:29:17 09/30/21 05:20:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) OEM (Unknown) Chassis System Boot/Restart Initiated System ACPI Power State Physical Security	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknoun) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM System State Physical Security System Firmware Progress	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknown) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:17 09/30/21 05:29:17 09/30/21 05:25:19 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM (Unknown) Chassis System Boot/Restart Initiated System ACPI Power State Physical Security System Firmware Progress Temperature	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknoum) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
DATE TIME 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:28:14 09/30/21 05:29:17 09/30/21 05:52:09 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:00:18 01/01/70 00:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54 09/30/21 05:52:54	Chassis System ACPI Power State System Firmware Progress System ACPI Power State OEM (Unknown) OEM System ACPI Power State Physical Security System Firmware Progress Temperature Temperature	61 20 00 04 18 94 03 01 FF FF Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x94 Chassis Specific (Unknoun) Event Description: Record Type-0x02. Assertion Event. ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit

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



IPMI tool

LAN (remote)

Linux:

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

Windows:

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

D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe sel -N 192.168.1.78 -U ADMIN -P ADMIN
ipmiutil sel version 3.15
Connecting to node 192.168.1.78
BMC version 0.28, IPMI version 2.0
SEL Wer 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:

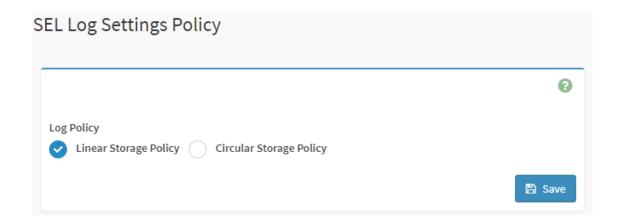
ipmitool: https://github.com/ipmitool/ipmitool ipmiutil: http://ipmiutil.sourceforge.net/

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



Memory Correctable and Uncorrectable ECC Error

ECC errors are divided into Un-correctable ECC Errors and Correctable ECC Errors.

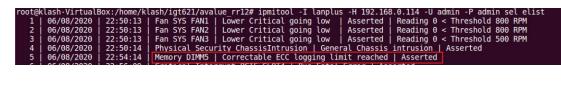
Correctable ECC errors can be detected and corrected if the chipset and DIMM support this functionality. This event in itself does not pose any direct problems because the ECC errors are still being corrected. Even though this event doesn't immediately lead to problems, it can indicate on the DIMM modules is slowly failing. If this error occurs multiple times, consider replacing the DIMM as a preventative measure.

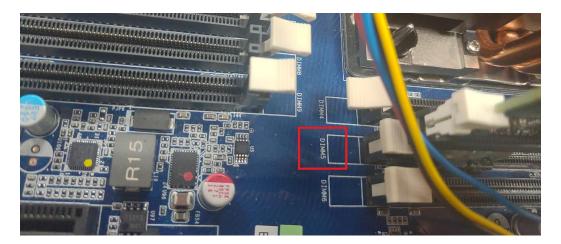
An un-correctable ECC error is a fatal issue. While correctable errors do not affect the normal operation of the system, un-correctable memory errors will immediately result in a system crash or shutdown of the system. If an un-correctable ECC error has occurred, consider replacing the DIMM as a preventative measure.

DIMM location from SEL:

1. Issus the command

ipmitool –I lanplus –H [BMC IP address] -U [user name] -P [user password] sel elist 2. The SEL log will indicate which DIMM happens error





Logs & Reports >>IPMI Event Log

ID: 11 DIMM5 sensor of type memory logged a correctable ecc logging limit reached Oin 8 hours

PCIe Errors

PCIe error events are either correctable (informational event) or fatal. In both cases information is logged to help identify the source of the PCIe error and the location.

Correctable errors include those error conditions where hardware can recover without any loss of information. Correctable errors are acceptable and normal at a low rate of occurrence. If the error continues, identify the card from SEL and check the following steps.

- a. Verify the card is inserted properly.
- b. Install the card in another slot and check if the error follows the card or stays with the slot.
- c. Update all firmware and driver.

Fatal errors are uncorrectable error conditions which render the particular Link and related hardware unreliable. For Fatal errors, a reset of the components on the Link may be required to return to reliable operation. When a fatal error is reported, identify the card from SEL and check the following steps.

- a. Verify the card is inserted properly.
- b. Install the card in another slot and check if the error follows the card or stays with the slot.
- c. Update all firmware and driver.

PCIe location from SEL:

1. Issus the command

ipmitool –I lanplus –H [BMC IP address] -U [user name] -P [user password] sel elist 2. The SEL log will indicate which PCIE happens error



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	t BIOS code O	EM command, and defa	ault Privilege Level is
User.				
	lf you use " ipm	iutil " tool in W	indows OS, replace "0x	32" with "00 20 C8".
Cmd	Command code. This message byte specifies the operation that it to be			
executed.				
Data	Zero or more b	ytes of data, a	s required by given com	nmand.

Get BIOS code Commands

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

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

Example:

Locally get BIOS code by "ipmitool" in Linux.

Ipmitool raw 0x32 0x73 0

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

The latest BIOS code is e3.

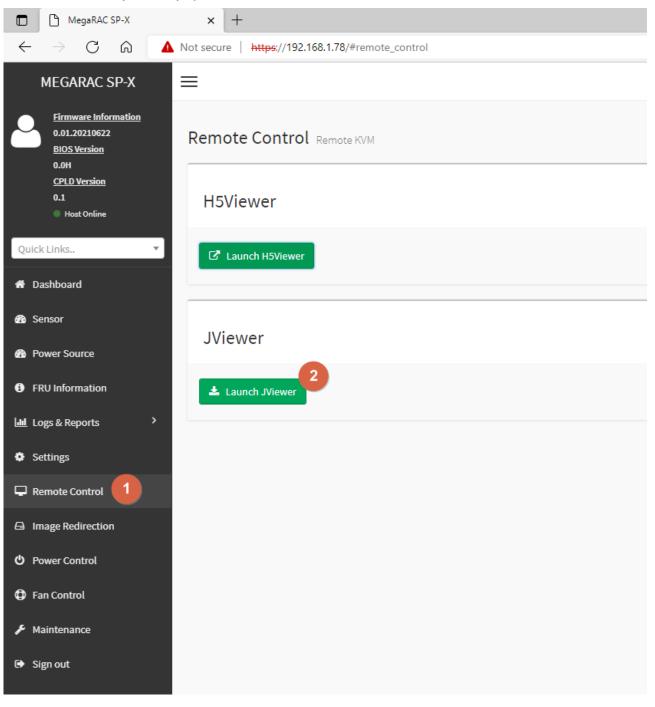
Remotely get BIOS code by "ipmiutil" in windows:

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

D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.77 -U admin -P admin <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 b5 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 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 94 95 96 ef 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 99 92 92 92 92 ad 78 b1 a0 ee ee ee 84 aa e3 send_icmd ret = 0 ipmiutil cmd, completed successfully

APPENDIX-J REMOTE CONTROL-JVIEWER

1. Select the "Remote Control" page and the click [Launch Jviewer]. The broswer will start to download jviewer.jnlp.



2. When the download completed, run jviewer.jnlp (notice: you need to install java as well.)

MegaRAC SP-X	imes Security level settings in the Java $ imes$ $ $ +	
\leftarrow \rightarrow C \bigcirc	A Not secure https://192.168.1.78/#remote_control	
MEGARAC SP-X	=	
Eirmware Information 0.01.20210622 BIOS Version 0.0H	Remote Control Remote KV/M	
CPLD Version 0.1 Hoat Online	H5Viewer	
Quick Links	C Launch H5Viewer	
A Dashboard		Security Warning X
🚯 Sensor	JViewer	Do you want to Continue?
Power Source	JViewei	The connection to this website is untrusted.
FRU Information	Launch JViewer	Website: https://192.168.1.78.443
Logs & Reports >		Note: The certificate is not valid and cannot be used to verify the identity of this website. More information
Settings		Continue Cancel
Remote Control		

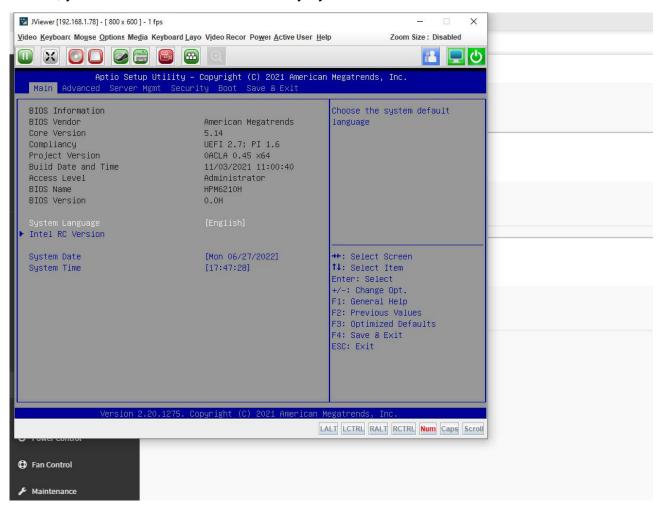
If the message shows up, please refer the java website to add the certificate.

MegaRAC SP-X	× +	
← → C ⋒ 4	Not secure https://192.168.1.78/#remote_control	
MEGARAC SP-X	=	
Eirmware Information 0.01.20210622 BIOS Version 0.0H	Remote Control Remote KVM	
CPLD Version 0.1 Host Online	H5Viewer	Java Application Blocked X
Quick Links 🔻	C Launch H5Viewer	Application Blocked by Java Security
Dashboard		For security, applications must now meet the requirements for the High or Very High security settings,
🏙 Sensor	JViewer	or be part of the Exception Site List, to be allowed to run.
Power Source		
FRU Information	▲ Launch JViewer	Neme: com ami.kvm.jvizwer.JVzwer Location: https://192.168.1.78.443
└ш Logs & Reports >		Reason: Your security settings have blocked an application signed with an expired or not-yet-valid certificate from running
Settings		
🖵 Remote Control		OK
Image Redirection		
O Power Control		
Fan Control		
🗲 Maintenance		
🕞 Sign out		

3. Check the box to accept the risk.

MegaRAC SP-X	× 🖏 Settings × 🖌 Security level settings	in the Java \times +
\leftarrow \rightarrow C \bigcirc \checkmark	Not secure https://192.168.1.78/#remote_control	
MEGARAC SP-X	≡	
Eirmware Information 0.01.20210622 BIOS Version 0.0H	Remote Control Remote KVM	
CPI D Version 0.1 O Host Online	H5Viewer	
Quick Links 🔻	C [®] Launch H5Viewer	Security Warning X Do you want to run this application?
A Dashboard		Nome: com.ami.kym.jyjewer.JVjewer
🚯 Sensor		Publisher: American Megatiends Inc.
Power Source	JViewer	Locations: https://192.168.1.78.443 Launched from downloaded JNLP file
FRU Information	🛓 Launch JViewer	Running this application may be a security risk
📶 Logs & Reports >		Risk: This application will run with unswitched access which may put your computer and personal information at risk. The information provided is unseliable or unknown so it is recommended not to run this application unless you as familiar with its source
Settings		The certificate used to identify this application has expired. More information
Remote Control		Select the box below, then click Run to start the application
Image Redirection		Secret the risk and want to run this application Run Concel

4. Now, you can control machine remotely by the Console Redirection window.



Menu item	Sub menu item	Detailed explanation
	Pause redirection:	This option is used for pausing Console Redirection.
	Resume	This option can be used to resuem the Console Redirection when the session is
	Redirection	paused.
	Refresh Video:	This option can be used to update the display shown in the Console Redirection
		windows.
	Construine Constant	This option helps to take the screenshot of the host screen and save it in the
	Capture Screen	client's system.
	*Compression	This option helps to compress the Video data transfer to the specific mode.
	Mode	Note: This Feature is only specific to AST SOC.
Video	*DTC Quantization	This option helps to choose the video quality.
VIGEO	Table:	Note: This Feature is only specific to AST SOC.
		If you enable this option, the server display will be
	Turn OFF Host	blank but you can view the screen in Console Redirection. If you disable this
	Display/Host	option, the display will be back in the server screen.
	Video Output	Note: This Feature is only specific to RVAS (Pilot video engine) video driver and
		AST SOCs.
		This option is used to view the Console Redirection in full screen mode
	Full Screen:	(Maximize).
		This menu is enabled only when both the client and host resolution are same.
	Exit	This option is used to exit the console redirection screen.
	Hold Right Ctrl	This menu item can be used to act as the right-side <ctrl> key when in</ctrl>
	Кеу	Console Redirection.
	Hold Pight Alt Koy	This menu item can be used to act as the right-side <alt> key when in Console</alt>
	Hold Right Alt Key	Redirection.
	Hold Loft Ctrl Kov	This menu item can be used to act as the Left-side <ctrl> key when in</ctrl>
	Hold Left Ctrl Key	Console Redirection.
	Sub menu item	Detailed explanation
Keyboard	Pause redirection:	This option is used for pausing Console Redirection.
	Hold Left Alt Key	This menu item can be used to act as the Left-side <alt> key when in Console</alt>
		Redirection.
	Left Windows key	This menu item can be used to act as the Left-side <win> key when in Console</win>
		Redirection.
-	Right Windows	This menu item can be used to act as the right-side <win> key when in Console</win>
	Кеу	Redirection.

Ctrl+Alt+Del

The Console Redirection menu bar consists of the following menu items.

This menu item can be used to act as if you depressed the <CTRL>,<ALT> and

		 keys down simultaneously on the server that you redirecting.
	Context menu	This menu can be used to act as the context menu key, when in Console
		Redirection.
		This Menu is used to add the user configurable shortcut keys to invoke in the
	Hot Keys	host machine. The configured key evens are saved in the BMC.
	Full Keyboard	Enable this option to provide full keyboard support. This option is used to
	Support	trigger the Ctrl and Alt key directly to host from the physical keyboard.
	Chow Curroom	This menu item can be used to show or hide the local mouse cursor on the
	Show Cursor:	remote client system.
		This menu item can be used only if the mouse mode is relative.
		In this step, the mouse threshold settings on the remote server will be
		discovered. The local mouse cursor is displayed in RED color and the remote
	Mouse Calibration	cursor is part of the remote video screen. Both the cursors will be synchronized
	Mouse Calibration	in the beginning. Please use '+' or '-' keys to change the threshold settings until
		both the cursors go out of synch. Please detect the first reading on which
		cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold
		value.
		This option handles mouse emulation from local window to remote screen using
		either of the two methods. Only 'Administrator' has the right to configure this
		option.
		Absolute mouse mode: The absolute position of the local mouse is sent to
	Mouse Mode	the server if this option is selected.
Mouse		 Relative mouse mode: The Relative mode sends the calculated relative
		mouse position displacement to the server if this option is selected.
		 Other mouse mode: This mouse mode sets the client cursor in the
		middle of the client system and will send the deviation to the host. This
		mouse mode is specific for SUSE Linux installation and accessing mouse
		in UEFI screen.
		Note: AMI MegaRAC SP-X suggests users to use Linux version of OS
		except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse
		mode.
		Client cursor will be hidden always. If you want to enable, use Alt + C to
		access the menu.
		You can see client and host cursor in JViewer if mouse is moved faster/ in
		circle. Mouse sync will depend on so many factors like network, client
		machine video packet receive and rendering, BMC CPU utilization etc. In
		Normal use case scenario you will have mouse sync better compare to
		heavy video/stress testing. High resolution and media redirection will have

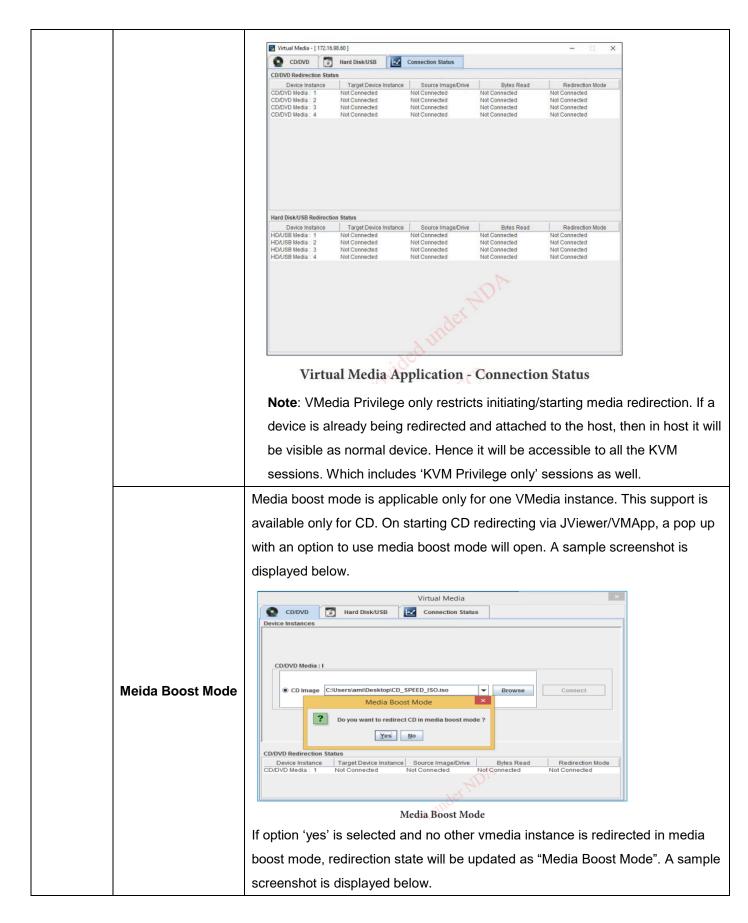
		directly impact in video rendering due to that client and host cursor can be
		viewed while moving the cursor.
		Hardware cursor will work only if aspeed video driver is installed in host.
		To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.
		The Bandwidth Usage option allows you to adjust the bandwidth. You can select
		one of the following:
	Bandwidth	Auto Detect - This option is used to detect the network bandwidth usage of the
	(Except RAVS	BMC automatically.
	video driver)	• 256 Kbps 256 Kbps
	video di iver)	• 512 Kbps 512 Kbps
		1 Mbps 1 Mbps
		• 10 Mbps 10 Mbps
	Keyboard/Mouse	This option allows you to encrypt keyboard inputs and mouse
	Encryption:	movements sent between the connections.
Options	Zoom	 Note: This option is available only when you launch the Java Console . Zoom In – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%. Zoom Out – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%. Actual Size - By default this option is selected By default this option is selected. Fit to Client Resolution - If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen. The host video will be scaled down and rendered in the KVM console. In this case, the host mouse cursor will appear smaller than the rendered in the KVM console. So the client and host mouse cursors might not be in perfect sync. Fit to Host Resolution - If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution. Note: This option can be configured from PRJ in MDS.
	Send IPMI Command	This option opens the IPMI Command dialog. Enter the raw IPMI command
		in Hexadecimal field as Hexadecimal value and click Send . The Response
		will be displayed as shown in the screenshot below.

	GUI Languages	Choose the desired GUI language.
	Block Privilege Request	Full privileged sessions can use this option to block incoming request from partial privileged sessions by setting an auto response as either "Allow only Video" or "Deny Access". Options Media Keyboard Layout Video Record Pc Bandwidth Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command GUI Languages Image: Send IPMI Command Image: Send IPMI Command Image: Send IPMI Command
Media	Virtual Media Application	The virtual media application will allow you to redirect different media to the host system. The application supports CD/DVD, Hard Disk/USB devices as well as image files. A sample screenshot of Virtual Media Application is given below.

User's Manual

Virtual Media - [172.16.98.60]
CD/DVD THard Disk/USB
Device Instances
CD/DVD Media : 1
○ D Connect
© G
CD/DVD Media : II
CD Image D Connect
⊖ G
CD/DVD Media : III
CD Image Browse Browse
G Connect
Aune
CD/DVD Redirection Status Device Instance Target Device Instance Source Image/Drive Bytes Read Redirection Mode
CD/DVD Media: 1 Not Connected Not Connected Not Connected Not Connected CD/DVD Media: 2 Not Connected Not Connected Not Connected Not Connected CD/DVD Media: 3 Not Connected Not Connected Not Connected Not Connected
CD/DVD Media : 4 Not Connected Not Connected Not Connected Not Connected
Note:
If there are two device panels for each device, and when you click the
Connect button, then the redirected device panel will be disabled.
Unmounting device will make the driver disconnect device when using Auto
Attach. Hence, when unmounting one USB key, the other USB key will be
disconnected and then reconnected.
The Virtual media application can be launched as a standalone application from
the StandAlone connection dialog. It can also be launched from the JViewer,
using the Virtual Media menu. When launched from JViewer, this application wil
work like a child dialog of the JViewer.
Note:
AST SOC:- Configured number of devices will be emulated in Windows
/Linux Host.
Macintosh OS X Clients: The package XQuartz should be present in
the Macintosh OS X clinet machines for the V-Media redirection to work.
Otherwise it may lead to problems in loading the VMedia libraries. If the
package is not already installed, download and install from the following
link. https://www.xquartz.org/
Each of the supported devices is listed in a separate tab. Each tab in the
application is described below.
CD/DVD Media: This tab can be used to start or stop the redirection of a
physical DVD/ CD-ROM drive and DVD/CD image file of ISO/NRG file format.

Hard disk/USB: This tab can be used to start or stop the redirection of a Hard
Disk/USB key image and USB key image such as img/ima.
Note: For redirecting Hard disk drives, you should have administrator
privilege (root user in the case of Linux clients).
For Windows 7 and above, the web browser from which the KVM redirection
will be initiated, should be launched using "Run as Administrator" option. If
there are multiple instances of the web browser open simultaneously, ensure
that all the instances are launched using the "Run as Administrator" option.
For Windows client, if the logical drive of the physical drive is dismounted
then the logical device is redirected with Read/Write Permission else it is
redirected with Read permission only. The USB/Hard disk drive can be
redirected as whole physical drive or individual logical drives.
For MAC client, External USB Hard disk redirection is only supported. The
External Hard disk Drives should be unmounted from the client before being
redirected.
For Linux client, fixed hard drive is redirected only as Read Mode. It does not
support write mode. The USB/Hard disk drive will be redirected as whole
physical drive.
For Hard disk image redirection, only the file extension is validated. The
Harddisk/USB key device/image will be redirected to the host as it is. The
BMC will not validate the harddisk medium, the host OS will take care of this.
This is applicable for all the media redirection client applications.
If the feature Redirect Devices Always in READ and WRITE Mode is
enabled, then the internal hard disk drives in the client machine will not be
listed. This information will be displayed in the status bar of the Virtual Media
application.
If files with hidden attribute are visible in the file open dialog, then the file can
be opened and redirected.
If the file is not visible in the file open dialog, the user shall mention the path
of the image file in the file name field of the file open dialog and then open the
image.
Continuously clicking connect/disconnect buttons without giving any delay
in-between may cause failure in media redirection, since the host may take
few seconds to connect/disconnect the media device.
SPX Stack Media redirection supports only Basic Hard disk Redirection.
Connection Status: This tab provides a collective view of the redirection
status of various virtual media devices.
The connection status tab is shown below.



		CD/DVD Redirection Status Device Instance Target Device Instance Source Image/Drive Bytes Read Redirection Mode CD/DVD Media : 1 Virtual CD/DVD : 0 C:Wsers\amilDesktop 16 KB Media Boost Mode
		A Media Boost Mode
		Note: If media boost mode is selected, the processes related to media
		redirection will have high priority than other processes. This will improve
		media performance but other processes will have limited access to CPU
		cycle.
		If CD/DVD instance is started with media boost mode, the next CD/DVD
		instance will be started without any pop-up message.
		This option is used to detect keyboard layout automatically. If the client and host
		keyboard layouts are same, then for all the supported physical keyboard
		layouts, you must select this option to avoid typo errors. If the host and client
	Auto Detect	languages differ, user can choose the host language layout in the menu and
		thereby can directly use the physical keyboard.
		This feature is fully compatible when host and client has the same keyboard
		language layout. If the client and host language layouts differ, some special
		characters will not be compatible.
		Host Platform: This feature contains two options Windows and Linux.
		When working with Windows host, Windows option should be selected.
		Similarly when working with Linux host, Linux option should be selected. This
		option should be selected properly for the Physical keyboard layout cross
Keyboard		mapping to work properly. By default, Windows will be selected.
Layout		List of Host Physical Keyboard languages supported in SPX JViewer.
		1. English –US
	Physical	2. English – UK
	Keyboard	3. French
		4. French (Belgium)
		5. German (Germany)
		6. German (Switzerland)
		7. Japanese
		8. Spanish
		9. Italian
		10. Danish
		11. Finnish
		12. Norwegian (Norway)
		13. Portuguese (Portugal)

	44 Que diale
	14. Swedish
	15. Dutch (Netherland)
	16. Dutch (Belgium)
	17. Turkish – F
	18. Turkish – Q
	This option allows you to select the keyboard layout. It will show the dialog as
	similar to Windows On-screen keyboard. If the client and host languages are
	different, you can select the soft keyboard that corresponds to the host keyboard
	layout from the list shown in JViewer, and use it to avoid typo errors.
	Note: Different Linux systems follow different keyboard layouts. So the
	softkeyboard displayed uses standard windows keyboard layout irrespective
	of the host OS.
	We have list of List of Soft Physical Keyboard languages supported in SPX
	JViewer.
	1. English –US
	2. English – UK
	3. Spanish
	4. French
	5. German (Germany)
	6. Italian
	7. Danish
Soft Keyboard :	8. Finnish
	9. German (Switzerland)
	10. Norwegian (Norway)
	11. Portuguese (Portugal)
	12. Swedish
	13. Hebrew
	14. French (Belgium)
	15. Dutch (Netherland)
	16. Dutch(Belgium)
	17. Russian (Russia)
	18. Japanese (QWERTY)
	19. Japanese (Hiragana)
	20. Japanese (Katakana)
	21. Turkish – F
	22. Turkish – Q
	Note: Soft keyboard is applicable only for JViewer Application not for other
	application in the client system.

	Start Record	This option is to start recording the screen.
	Stop Record	This option is used to stop the recording.
		To set the settings for video recording.
Video Record	Settings	 Procedure Note: Before you start recording, you have to enter the settings. Click Video Record > Settings to open the settings page as shown in the screenshot below. If Video Record I are setting and the setting are shown in the screenshot below. If Video Length 20 are seconds are setting are setting are shown in the screenshot below. If Video to be Saved are seconds are setting are setting
		 Record the process. To stop the recording, click Video Record > Stop Record.
	Reset Server	To reboot the system without powering off (warm boot).
	Immediate	To immediately power off the server.
	Shutdown	
Power	Orderly	To initiate operating system shutdown prior to the shutdown.
	Shutdown :	
	Power On Server	To power on the server.
	Power Cycle	To first power off, and then reboot the system (cold boot).
	Server	
Active Users		Click this option to displays the active users and their system ip address.
Help	JViewer	Displays the copyright and version information.

		The lower right of Console Redirection windows displays all the quick buttons.
		These quick buttons helps you to perform these functions by just clicking them.
		This key is used to play the Console redirection after being paused.
		This key can be used for pausing Console Redirection.
		This button is used to view the Console Redirection in full screen mode.
	×	Note: Set your client system resolution same to host system resolution so
		that you can view the server in full screen.
		This quick button is used to show or hide the soft keyboard.
Quick	B	This quick button is used to record the video.
Buttons		This quick button is used to show or hide the mouse cursor on the remote client
Bullons	S	system.
	2	Active Users
	D	This quick button will work like toggle button if icon is in green color server
		status is power on by clicking the button immediate shutdown action will be
		triggered in host If the icon is in red color server status is power off. Click the
		button to power on the host.
	•	This quick button displays the available hotkeys.
	00	These quick buttons will pop up a virtual media where you can configure the
		media.