

# HPM-621DE

# IPMI Setup User's Manual

---

1<sup>st</sup> Ed –08 June 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 UNDESIRE 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:

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

### **A Message to the Customer**

#### ***Avalue Customer Services***

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

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

#### ***Technical Support***

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

## HPM-621DE User's Manual

first.

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

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

### ***Product Warranty***

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

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

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

# Content

<b>1. HARDWARE</b> .....	<b>7</b>
1.1 SYSTEM SPEC .....	8
1.2 PLATFORM AND BMC COMPONENTS .....	9
1.3 I2C BLOCK DIAGRAM .....	10
1.4 I2CBUS ACCESS .....	11
<b>2. WEB UI</b> .....	<b>13</b>
2.1 Log in.....	14
2.2 HOME>DASH BOARD .....	16
2.3 HOME>SENSOR .....	18
2.4 HOME> FRU INFORMATION .....	21
2.5 HOME> LOGS & REPORTS .....	22
2.6 HOME> SETTINGS.....	24
2.7 HOME> REMOTE CONTROL.....	86
2.8 HOME>IMAGE REDIRECTION .....	87
2.9 HOME> POWER CONTROL.....	88
2.10 HOME> FAN CONTROL.....	89
2.11 HOME> MAINTENANCE.....	90
2.12 HOME> SIGN OUT .....	98
<b>APPENDIX-A BMC HARDWRE: AST2500</b> .....	<b>99</b>
<b>APPENDIX-B IPMI COMMANDS SUPPORT TABLE</b> .....	<b>102</b>
<b>APPENDIX-C IPMI OEM COMMANDS LIST</b> .....	<b>107</b>
<b>APPENDIX-D SENSOR TABLE</b> .....	<b>108</b>
<b>APPENDIX-E DEFAULT CONFIGURATION</b> .....	<b>111</b>
<b>APPENDIX-F FIRMWARE UPDATE</b> .....	<b>112</b>
<b>APPENDIX-G SMART FAN CONFIGURATION</b> .....	<b>145</b>
<b>APPENDIX-H SYSTEM EVENT LOG(SEL)</b> .....	<b>149</b>
<b>APPENDIX-I IPMI TO GET BIOS POST CODE</b> .....	<b>156</b>
<b>APPENDIX-J REMOTE CONTROL-JVIEWER</b> .....	<b>158</b>

## Glossary & Abbreviation

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

# 1. HARDWARE

---

# 1.1 SYSTEM SPEC

Refer to Figure 1-1. System Block Diagram.

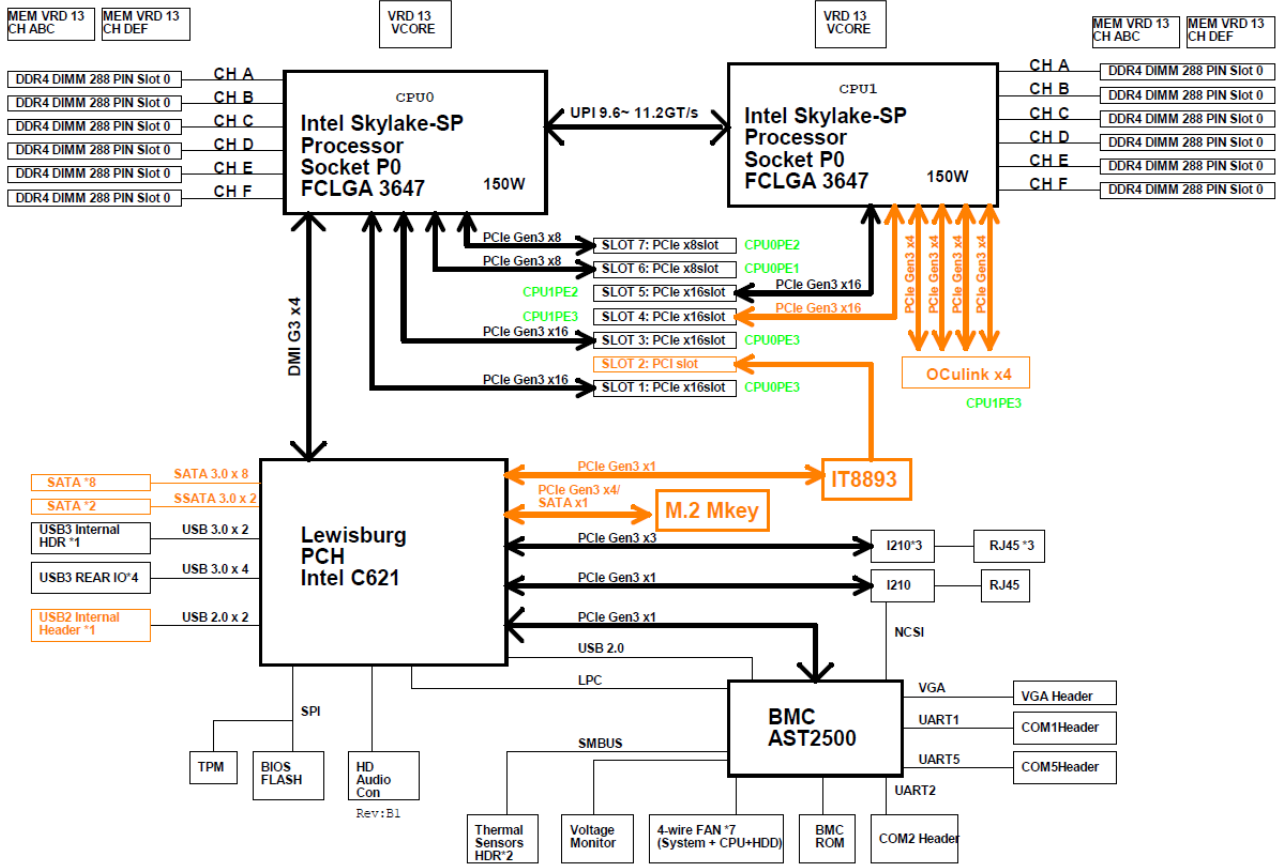


Figure 1-1 System block diagram



## 1.2 PLATFORM AND BMC COMPONENTS

**Table 1-1 Main component related to BMC**

Intel platform	- CPU(SkyLake) + PCH(Lewisburg C621)
BMC	AST2500
Flash ROM	BIOS side: 32MB BMC side: 32MB
BMC Memory	512MB
BMC LAN	RMII1: Share NIC I210
FRU device	CAT24C512
UART	UART1: System UART UART5: BMC console
LED	
Button	Power button System Reset button
CPLD	Lattice LCMXO2LF-1200C
Firmware Vendor of Code Base	AMI MegaRAC 12.1

**1.3 I2C BLOCK DIAGRAM**

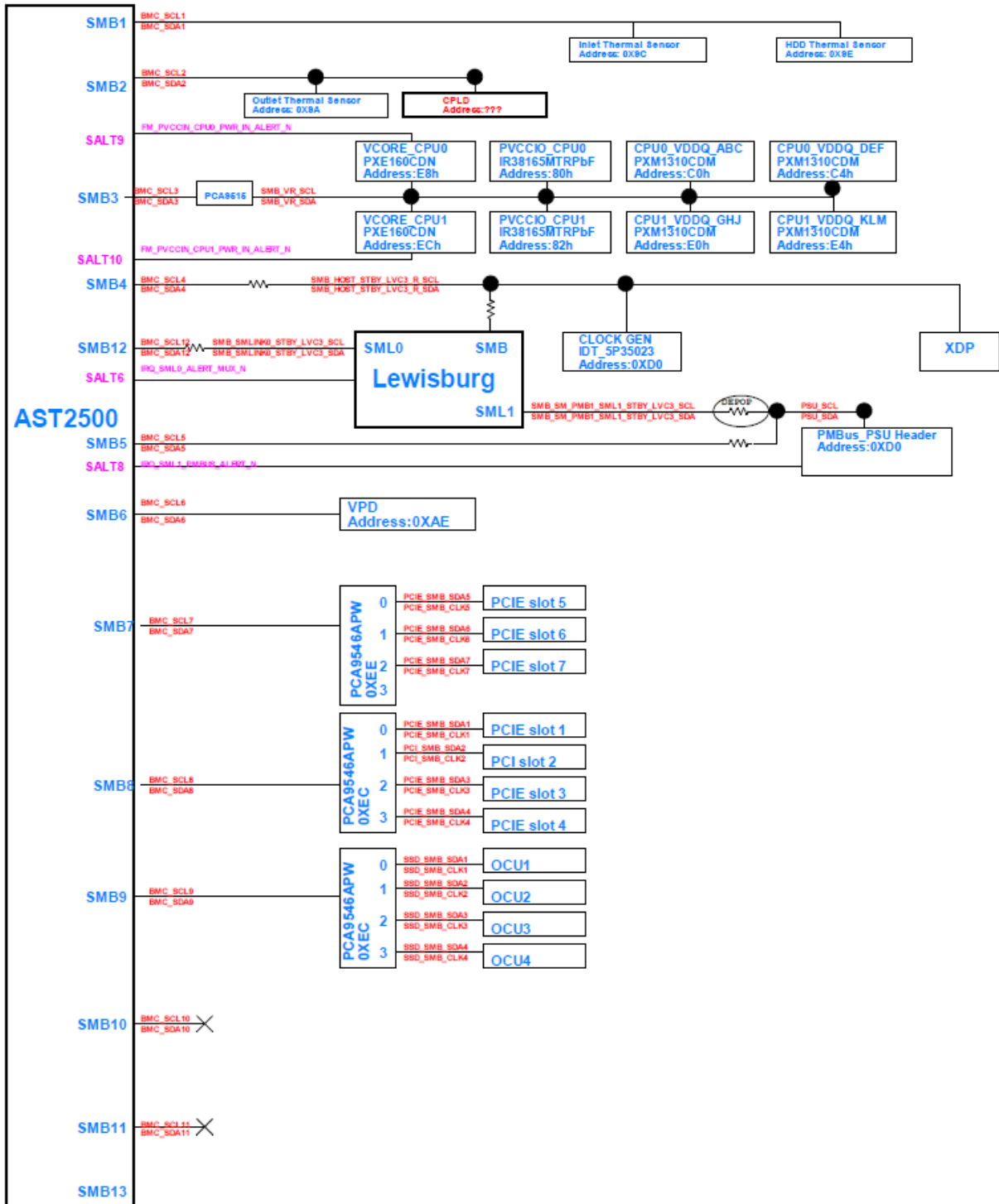


Figure 1-2 I2c block diagram

## 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.

Table 1-2 Master Write-Read Bus IDs

Physical Bus Number	Bus ID (channel no + bus ID + bus type)	Slave address	BMC use? (V)	Remark
1	02h	0x9C	V	Inlet Thermal Sensor
		0x9E	V	HDD Thermal Sensor
2	04h	0x9A	V	Outlet Thermal Sensor
3	06h	0xE8	V	VCORE CPU0
		0xEC	V	VCORE CPU1
		0x80	V	PVCCIO CPU0
		0x82	V	PVCCIO CPU1
		0xC0	V	CPU0 VDDQ ABC
		0xC4	V	CPU0 VDDQ DEF
		0xE0	V	CPU1 VDDQ GHJ
4	08h	0xE4	V	CPU1 VDDQ KLM
		0x88	V	PCH SMB
5	0Ah	0xD0		CLOCK GEN IDP 5P35023
		0xD0	V	PMBUS
7	0Eh	0xEE		PCA9546
		PCA9546 Channel 0		PCIE Slot 5
		PCA9546 Channel 1		PCIE Slot 6
8	10h	0xEC		PCA9546
		PCA9546 Channel 0		PCIE Slot 1
		PCA9546 Channel 1		PCIE Slot 2

## HPM-621DE User's Manual

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

## 2. WEB UI

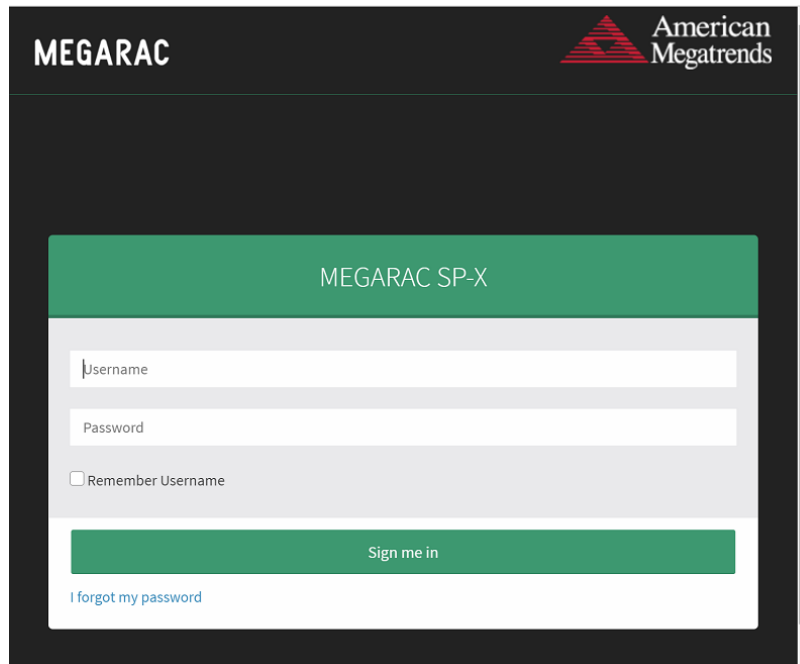
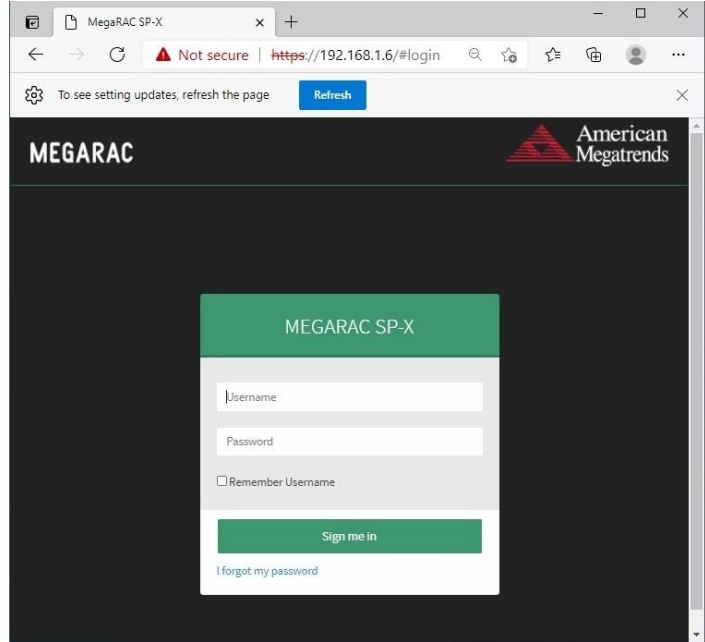
---

# HPM-621DE User's Manual

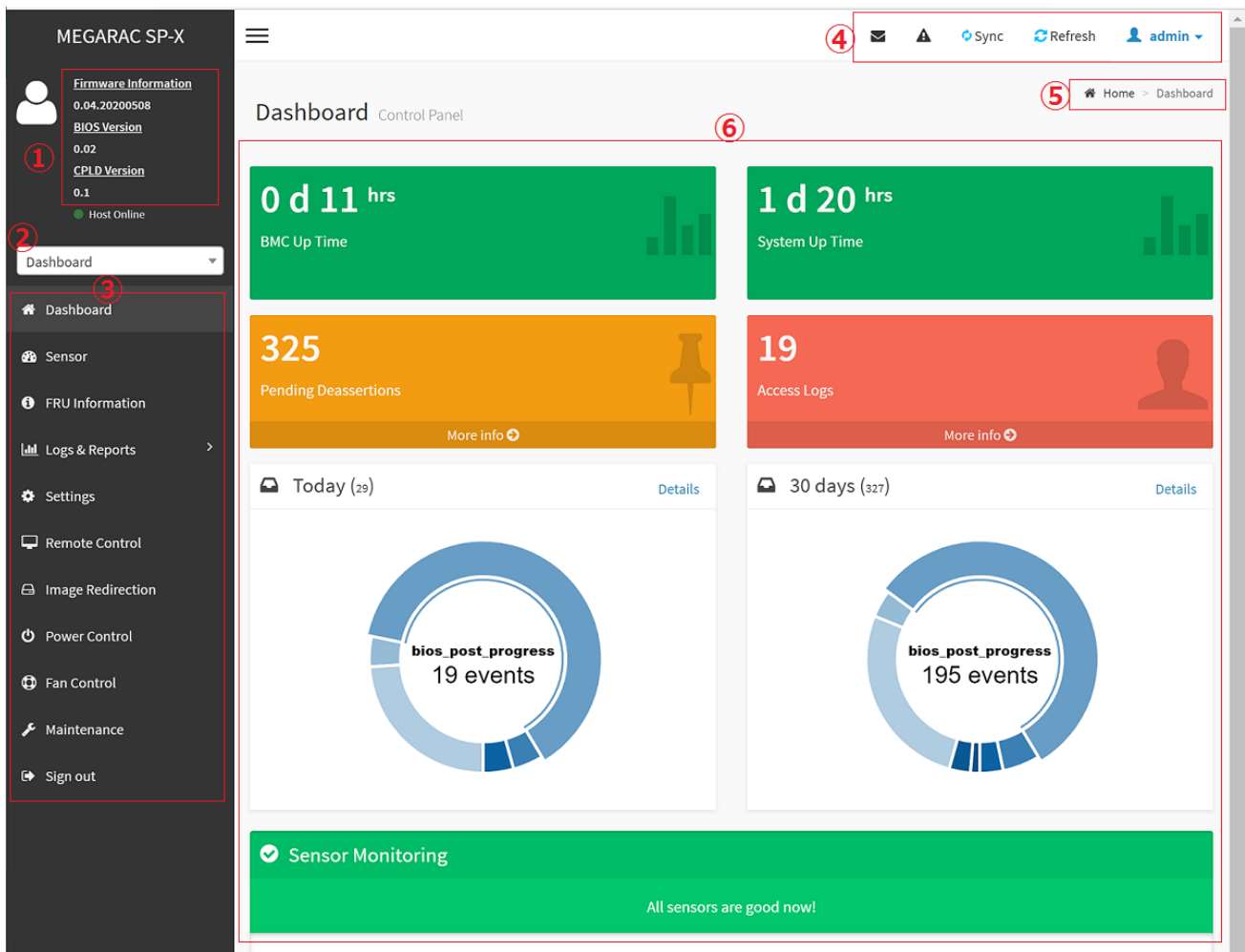
## 2.1 Log in

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

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



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



- ① Firmware Information : contains BMC/BIOS/CPLD firmware version
- ② Quick search bar : short-cut for the available menu and sub-menu pages
- ③ Menu Bar :

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

# HPM-621DE User's Manual

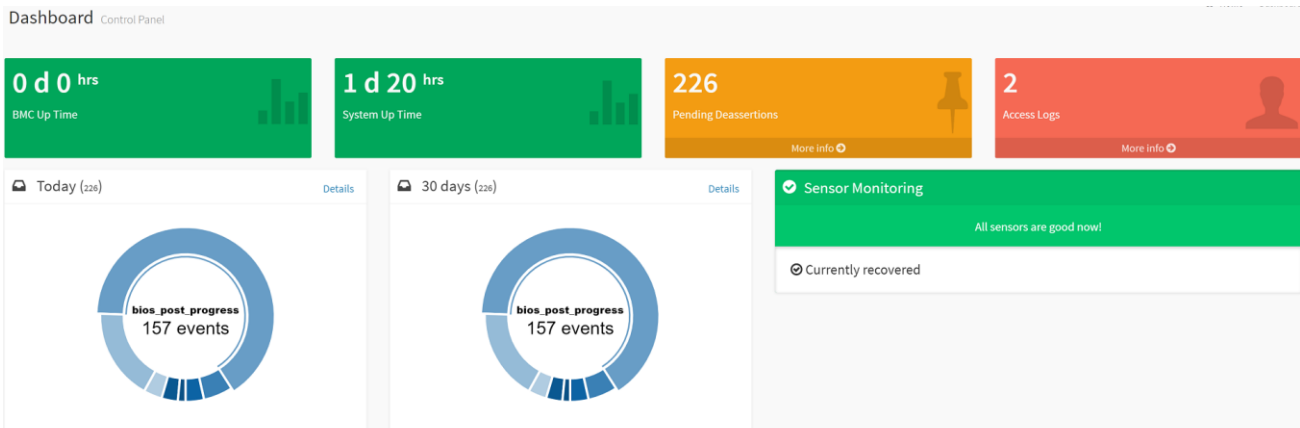


	Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the Logs and Reports page.
	Click the icon to view the notification received
	Click the icon to synchronize with Latest Sensor and Event Log updates.
	Click the icon or pressing key F5 to reload the current page.
	<p>This option shows the logged-in user name and privilege. There are five kinds of privileges.</p> <p><b>User:</b> Only valid commands are allowed.</p> <p><b>Operator:</b> All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.</p> <p><b>Administrator:</b> All BMC commands are allowed.</p> <p><b>No Access:</b> Login access denied.</p> <p><b>OEM:</b> All OEM commands are allowed</p>

- ⑤ The location of the main page
- ⑥ Main page that show content and configuration options
- ⑦ Click this icon on some main page will show more detail explanation.

## 2.2 HOME>DASH BOARD

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



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



<b>Access Logs</b>	Click more info to view the Audit Log page
<b>Today</b>	This list event logs occurred by the different sensors today, click details link to view the event logs
<b>30 Days</b>	This list event logs occurred by the different sensors within 30 days, click details link to view the event logs
<b>Sensor Monitoring</b>	Report the status of critical sensors.



↵ P1 VDDR-123	1.22 Volts	
↵ P1 VPP-123	2.50 Volts	
↵ P1 VDDR-456	1.22 Volts	
↵ P1 VPP-456	2.50 Volts	
↵ P2 VDDR-789	1.22 Volts	
↵ P2 VPP-789	2.50 Volts	
↵ P2 VDDR-101112	1.22 Volts	
↵ P2 VPP-101112	2.50 Volts	
↵ +V1S_VCCIO_CPU1	1.01 Volts	
↵ +V1S_VCCIO_CPU2	1.01 Volts	
⌵ P1 +VCCIN_T	35.00 °C	
⌵ P1 +VCCSA_T	35.00 °C	
⌵ P2 +VCCIN_T	42.00 °C	
⌵ P2 +VCCSA_T	41.00 °C	
⌵ P1 DDR-123 T	33.00 °C	
⌵ P1 VPP_123_T	31.00 °C	
⌵ P1 DDR-456 T	38.00 °C	
⌵ P1 VPP_456_T	33.00 °C	
⌵ P2 DDR-789 T	38.00 °C	
⌵ P2 VPP_456_T	36.00 °C	
⌵ P2 DDR-101112 T	43.00 °C	
⌵ P2 VPP_101112_T	42.00 °C	
⌵ P1 VCCIO_T	36.00 °C	
⌵ P2 VCCIO_T	37.00 °C	
⌵ CPU1 FAN	2300.00 Rpm	
⌵ CPU2 FAN	2400.00 Rpm	
⌵ SYS FAN1	1750.00 Rpm	
⌵ SYS FAN2	1350.00 Rpm	
⌵ SYS FAN3	1350.00 Rpm	
⌵ Outlet T	27.00 °C	
⌵ Inlet T	25.00 °C	
⌵ CPU1 T	36.00 °C	
⌵ CPU2 T	37.00 °C	
⌵ PCH T	38 °C	
⌵ DIMM4 T	33.00 °C	
⌵ DIMM10 T	36.00 °C	
⌵ Slot3_GPU_T	0.00 °C	
⌵ Slot5_GPU_T	0.00 °C	

# HPM-621DE User's Manual

Disabled Sensors (15)



## 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.

**Sensor detail** All information about this sensor

Home > Sensor Reading > Sensor detail

+V12S\_CPU1 Sensor Information

12.3 Volts

Upper Non-Recoverable	NA
Upper Critical	12.6 Volts
Upper Non-Critical	NA
Lower Non-Critical	NA
Lower Critical	11.4 Volts
Lower Non-Recoverable	NA

Change Thresholds

Sensor Events

### 2.3.2 Home> Sensor Detail>Sensor Thresholds

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

#### Sensor Thresholds

Home > Sensor Detail > Sensor Thresholds

##### Change Threshold Values ?

Sensor Name  
+V12S\_CPU1

Upper Non-recoverable

Upper Critical

Upper Non-critical

Lower Non-critical

Lower Critical

Lower Non-recoverable

Save

## 2.4 HOME> FRU INFORMATION

This page display FRU information that be stored in eeprom

**FRU** Field Replacable Units ?

---

Available FRU Devices

FRU Device ID 0 v

FRU Device Name Atmel\_AT24C512C

**Chassis Information**

Chassis Information Area Format Version 0

Chassis Type

Chassis Part Number

Chassis Serial Number

Chassis Extra

**Board Information**

Board Information Area Format Version 1

Language 25

Manufacture Date Time Mon Jun 14 16:00:00 2021

Board Manufacturer Avalue Technology

Board Product Name HPM-621DE

Board Serial Number 99000016830011

Board Part Number HPM-621DEA-A1R

FRU File ID

Board Extra

**Product Information**

Product Information Area Format Version 1

Language 25

Product Manufacturer Avalue Technology

Product Name HPM-621DE

Product Part Number HPM-621DEA-A1R

Product Version A1

Product Serial Number 99000016830011

Asset Tag

FRU File ID

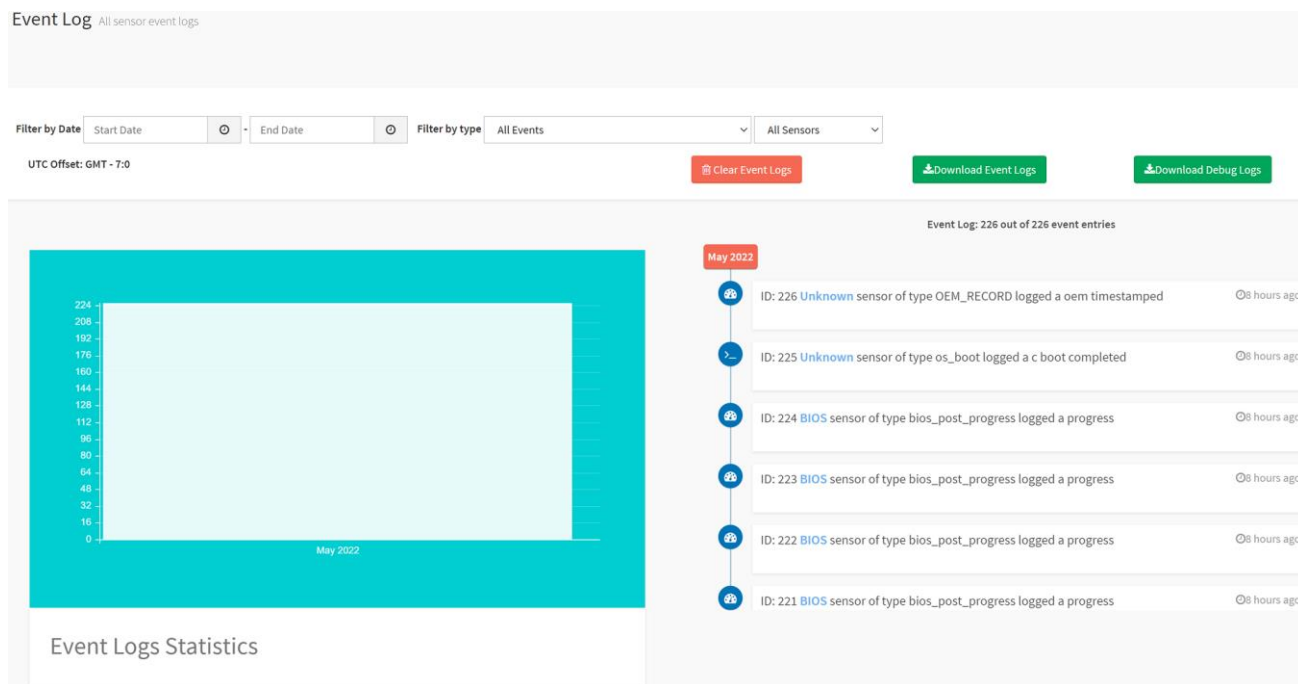
Product Extra

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

## 2.5 HOME> LOGS & REPORTS

### 2.5.1 Home> Logs & Reports >IPMI Event Log

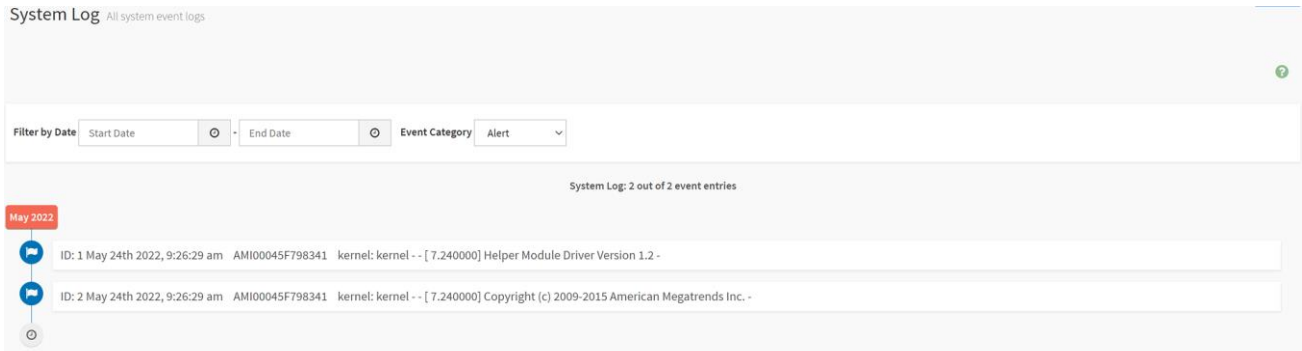
This page displays the ipmi event logs and user can filter event logs by date/type/sensor



Item	Option	Description
<b>Filter by Date</b>	<ul style="list-style-type: none"> <li>● Start Date</li> <li>● End Date</li> </ul>	Click field of “Start Date” or “End Date” to select the duration of filter
<b>Filter by type</b>	<ul style="list-style-type: none"> <li>● All Events</li> <li>● System Event Records</li> <li>● OEM Event Record</li> <li>● BIOS Generated Events</li> <li>● SMI Handler Events</li> <li>● System Management Software Events</li> <li>● System Software – OEM Events</li> <li>● Remote Console Software Events</li> <li>● Terminal Mode Remote Console software Events</li> </ul>	IPMI event logs can be filtered by this selected event type.
<b>Filter by sensor</b>	<ul style="list-style-type: none"> <li>● All Sensors</li> <li>● +V12S_CPU1</li> <li>● ....</li> </ul>	IPMI event logs can be filtered by this selected sensor.

### 2.5.2 Home> Logs & Reports >System Event Log

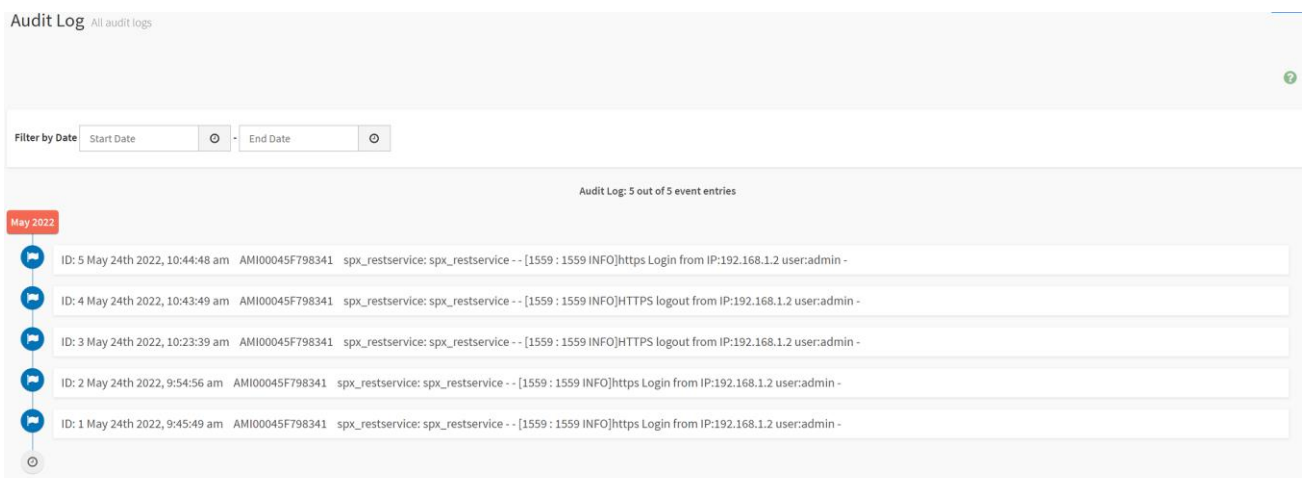
This page displays the system event logs and user can filter event logs by date/category



Item	Option	Description
<b>Filter by Date</b>	<ul style="list-style-type: none"> <li>● Start Date</li> <li>● End Date</li> </ul>	Click field of “Start Date” or “End Date” to select the duration of filter
<b>Event Category</b>	<ul style="list-style-type: none"> <li>● Alert</li> <li>● Critical</li> <li>● Error</li> <li>● Notification</li> <li>● Warning</li> <li>● Debug</li> <li>● Emergency</li> <li>● Information</li> </ul>	System event logs can be filtered by this selected event category.

### 2.5.3 Home> Logs & Reports >Audit Log

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

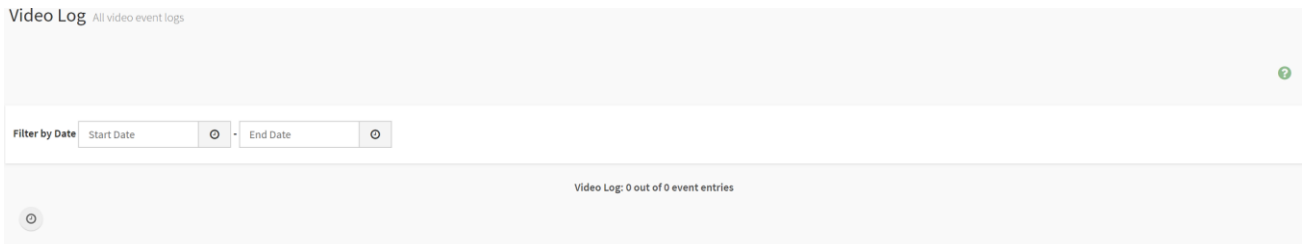


## HPM-621DE User's Manual

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

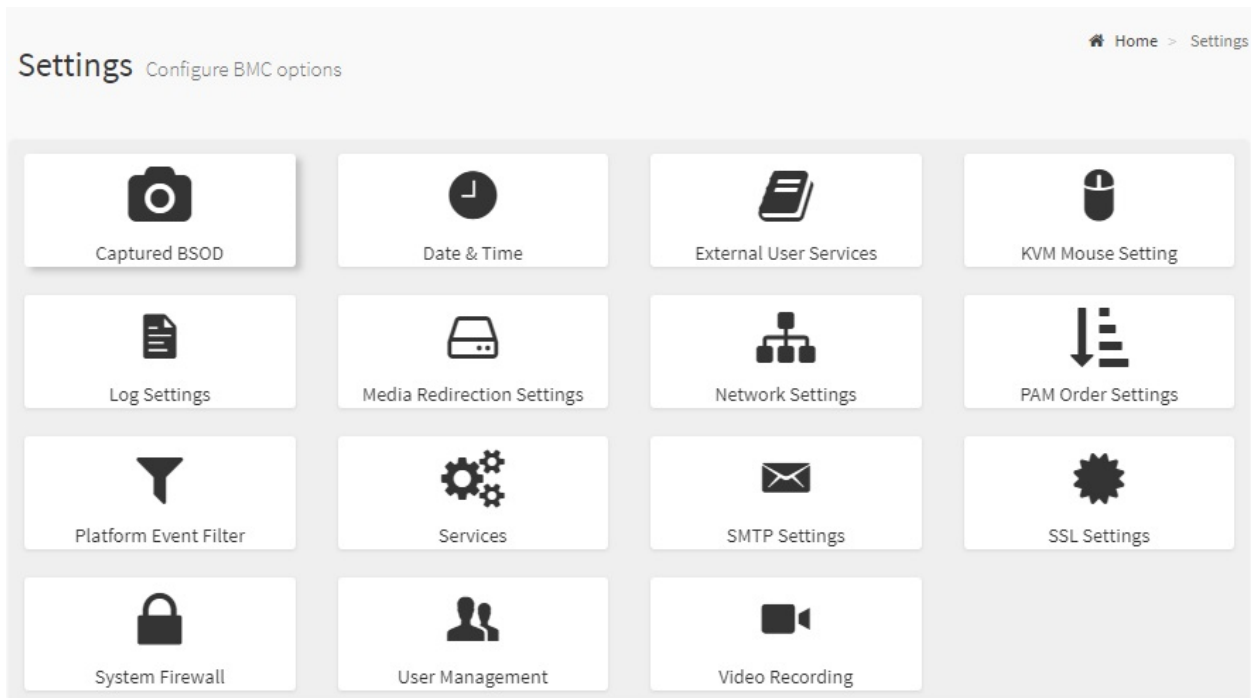
### 2.5.4 Home> Logs & Reports >Video Log

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



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

## 2.6 HOME> SETTINGS



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

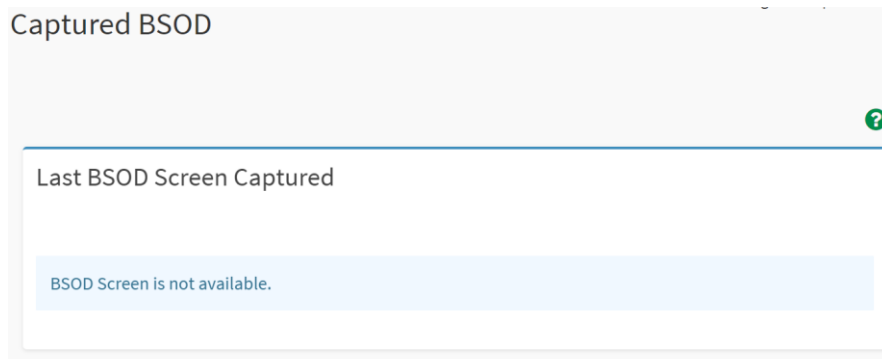


<b>Media Redirection Settings</b>	Configure the media into BMC for redirection
<b>Network Settings</b>	Configure the network settings for the available LAN channels
<b>PAM Order Settings</b>	Configure the PAM ordering for user authentication in to the BMC
<b>Platform Event Filter</b>	Configure Event Severity to trigger alert or power action
<b>Services</b>	Allow Administrator to modify services contain web/kvm/media/ssh.
<b>SMTP Settings</b>	E-mail message is one of alert and set SMTP for e-mail transmission across IP networks.
<b>SSL Settings</b>	SSL Certificate for secure transactions between webserver and browsers
<b>System Firewall</b>	Configure the firewall settings
<b>User Management</b>	Add a new user and modify or delete the existing users
<b>Video Recording</b>	Configure the events that will trigger auto video recording function of the KVM server.

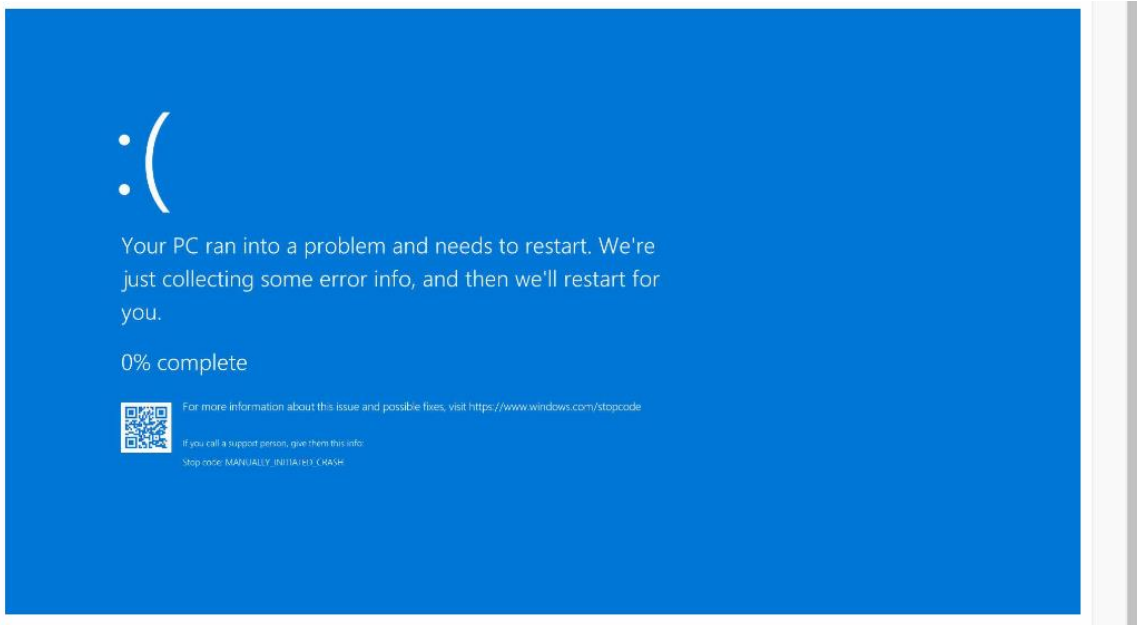
## 2.6.1 Home> Settings > Capture BSOD

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.

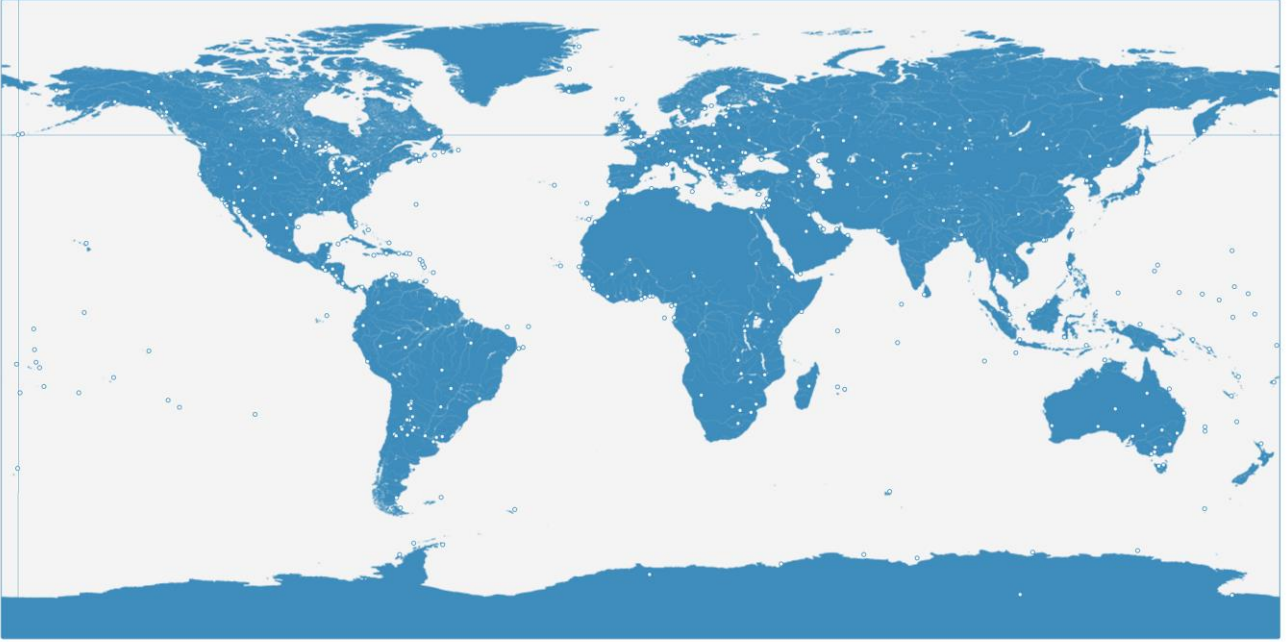


## 2.6.2 Home> Setting >Date & Time

Date & Time

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

Configure Date & Time ?



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

Automatic NTP Date & Time

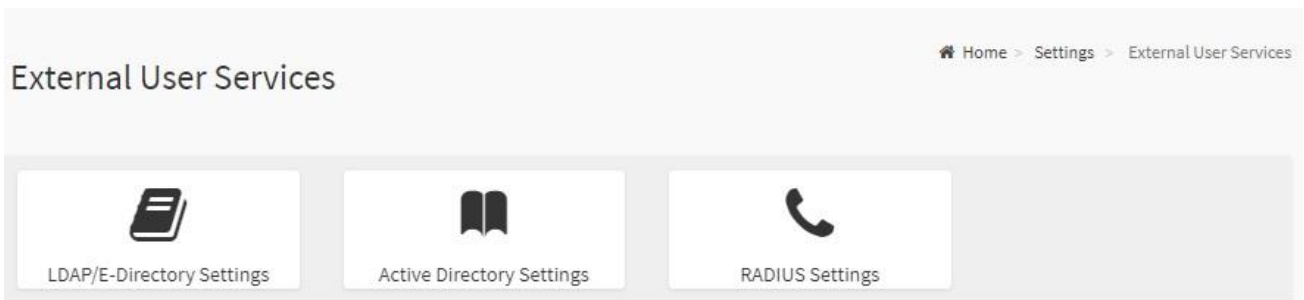
Primary NTP Server:

Secondary NTP Server:

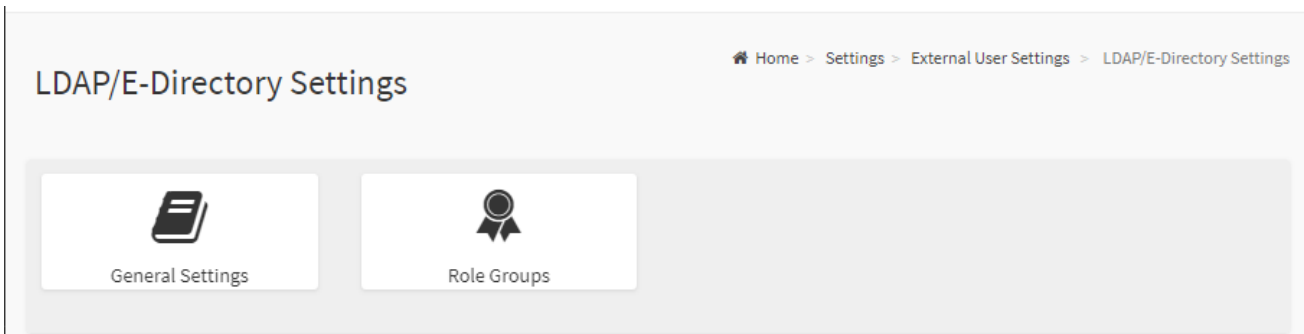
Item	Description
<b>Select Time Zone</b>	Choose the Time Zone either by using the drop-down option or by hovering over the map and double-clicking on a location name.
<b>Automatic NTP Date &amp; Time</b>	You can select to have the time automatically synchronized to a NTP server ( or two) ,which you can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

## HPM-621DE User's Manual

### 2.6.3 Home> Setting >External User Services



#### 2.6.3.1 Home> Settings >LDAP/E-Directory Settings



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

### General LDAP Settings ?

Enable LDAP/E-Directory Authentication

Encryption Type  
 No Encryption  SSL  StartTLS

Common Name Type  
 IP Address

Server Address

Port

Bind DN

Password




Search Base

Attribute of User Login

[Save](#)

Item	Option	Description
<b>Enabled LDAP/E-Directory Authentication</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Checked to enable LDAP/E-Directory settings. Note: During login prompt,use username to login as an LDAP Group member.
<b>Encryption Type</b>	<ul style="list-style-type: none"> <li>● No Encryption</li> <li>● SSL</li> <li>● StartTLS</li> </ul>	Encryption type for LDAP/E-Directory Note:Configure proper port number when SSL is enabled
<b>Common Name Type</b>	<ul style="list-style-type: none"> <li>● IP Address</li> </ul>	Select the Common Name Type as IP Address
<b>Server Address</b>	<input style="width: 100%;" type="text"/>	Enter the IP address of LDAP server in the field
<b>Port</b>		Specify the LDAP Port in the field and range from 1

## HPM-621DE User's Manual

		to 65535. Default port is 389 For SSL connections,default port is 636
<b>Bind DN</b>	Example: cn=manager,ou=login, dc=domain,dc=com	Specify the Bind DN that is used during bind operation, which authenticates the client to the server. Note:Bind DN is a string of 4 to 253 alpha-numeric characters. It must start with an alphabetical character. Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
<b>Password</b>		Enter the password in the Password field Note: <ul style="list-style-type: none"> <li>♦ at least 1 character long</li> <li>♦ not allow more than 48 characters</li> <li>♦ white space is not allowed.</li> </ul>
<b>Search Base</b>	Example: ou=login, dc=domain,dc=com	Enter the Search Base. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory Note: Search base is a string of 4 to 253 alpha-numeric characters. It must start with an alphabetical character Special Symbols like dot(.),comma(,),hyphen(-), underscore(_), equal-to(=) are allowed.
<b>Attribute of User Login</b>	<ul style="list-style-type: none"> <li>● cn</li> <li>● uid</li> </ul>	Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.
<b>Save</b>		Click button to save the changes made

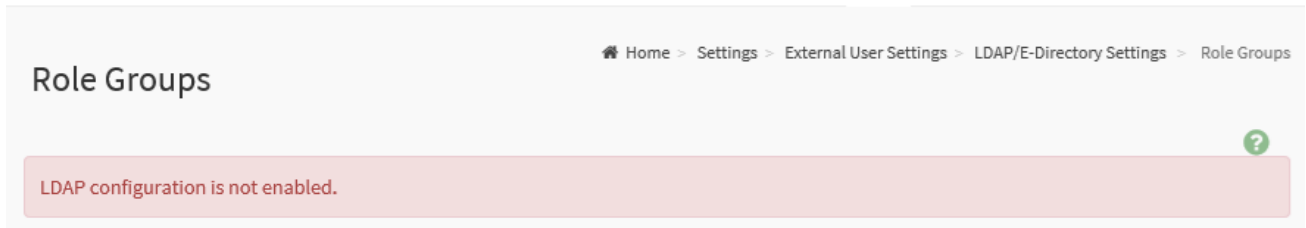
### 2.6.3.1.2 Home > Settings > External User Services > LDAP/E-Directory Settings > Role Groups

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

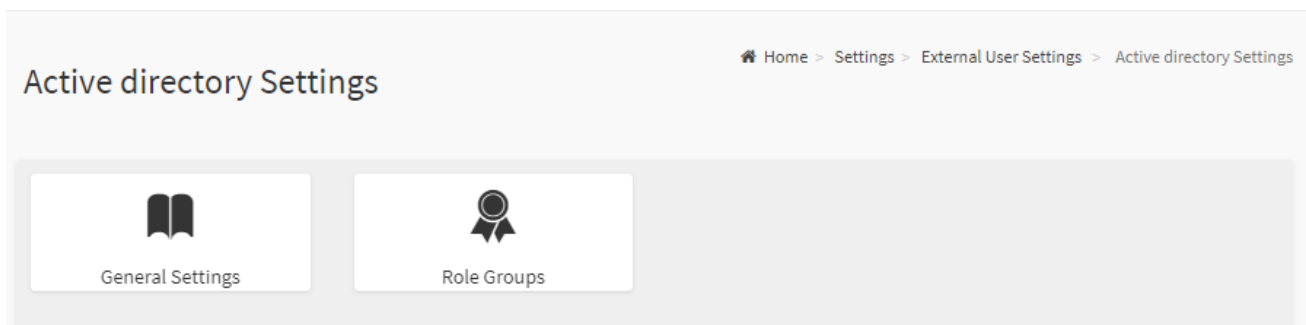
To add a Role Group, select a free box and click on it

To modify a Role Group, click on its name.

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




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



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

Item	Option	Description
<b>Enable Active Directory Authentication</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Enable/Disable Active Directory Authentication
<b>Secret Username</b>	<input type="text"/>	Specify the Username of an administrator of the Active Directory Server. <ul style="list-style-type: none"> <li>♦ A string of 1 to 64 alpha-numeric characters</li> <li>♦ Start with an alphabetical character</li> <li>♦ Case-sensitive</li> <li>♦ Special characters and spaces are not allowed</li> </ul> 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)
<b>Secret Password</b>	<input type="text"/>	Specify the Password of the administrator. <ul style="list-style-type: none"> <li>♦ At least 6 characters long</li> <li>♦ White space is not allowed</li> </ul>



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

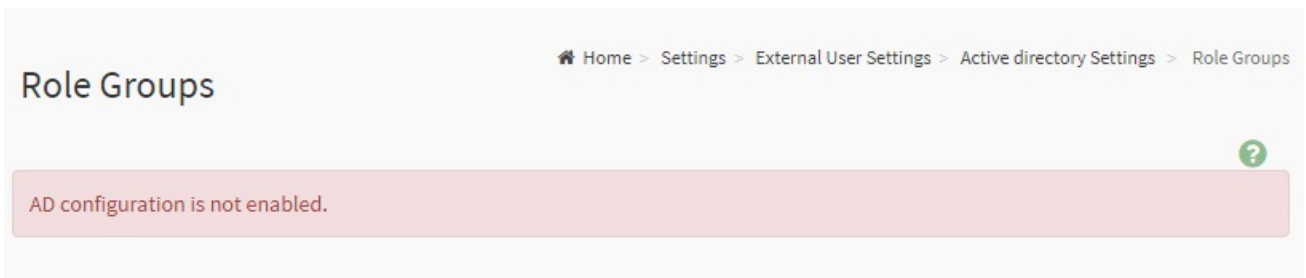
**2.6.3.2.3 Home > Settings > External User Services > Active directory Settings > Role Groups**

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

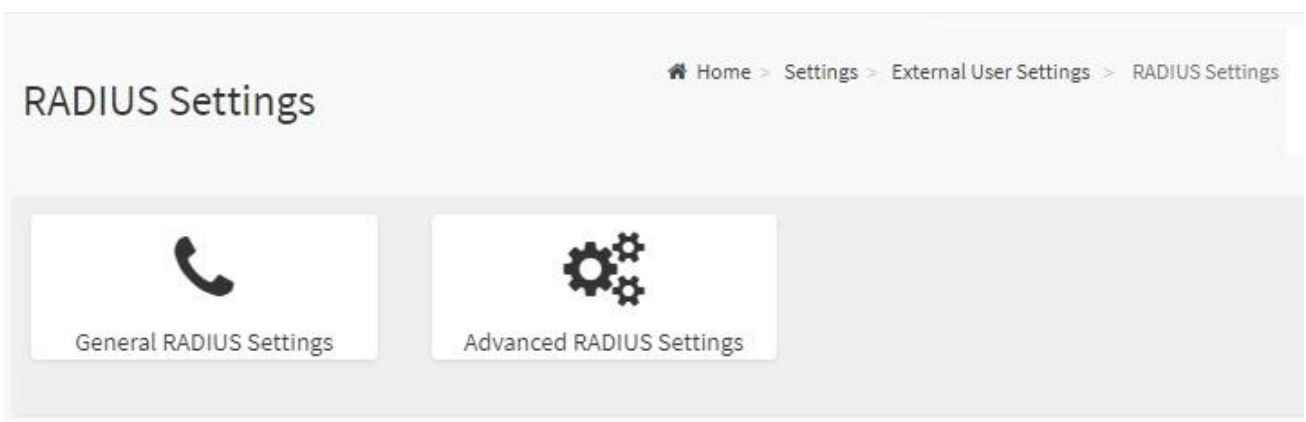
To add a Role Group ,click on a free box and configure its privilege and access.

To modify a Role Group ,click on it

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



**2.6.3.3.1 Home > Settings > External User Services > RADIUS Settings**



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

### General RADIUS Settings

?

Enable RADIUS Authentication

Server Address

Port

Secret

Enable KVM Access

Enable VMedia Access

Save

Item	Option	Description
<b>Enable RADIUS Authentication</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Enable/Disable RADIUS Authentication
<b>Server Address</b>	<input style="width: 100%;" type="text"/>	The ip address of RADIUS server Note: IP Address (both IPv4 and IPv6 format) FQDN (Fully Qualified Domain Name) format
<b>Port</b>	<input style="width: 100%; text-align: center;" type="text" value="1812"/>	The RADIUS Port number.(from 1 to 65535) Default Port is 1812
<b>Secret</b>	<input style="width: 100%;" type="text"/>	The Authentication Secret for RADIUS server <ul style="list-style-type: none"> <li>♦ not allow more than 31 characters.</li> <li>♦ must be at least 4 characters long.</li> <li>♦ white space is not allowed.</li> </ul>
<b>Enable KVM Access</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Enable/Disable access to KVM for RADIUS authenticated users
<b>Enable VMedia Access</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Enable/Disable access to VMedia for RADIUS authenticated users
<b>Save</b>	<span style="background-color: #007bff; color: white; padding: 5px 10px; border-radius: 3px;">Save</span>	Click button to save the changes made

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

### Advanced RADIUS Settings

RADIUS Authorization ?

Radius configuration is not enabled.

Administrator

Operator

User


OEM Proprietary

No Access

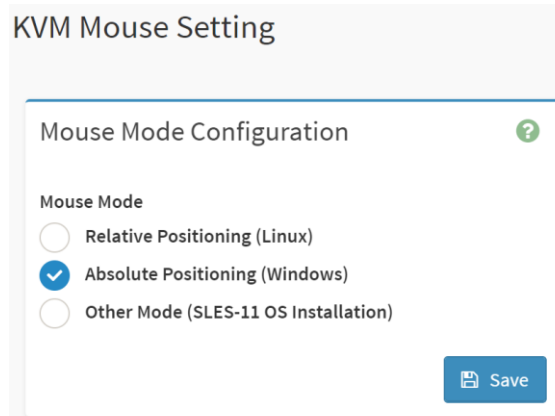
Save


Item	Option	Description
<b>Administrator</b>	<input style="width: 100%;" type="text"/>	Radius User Authorization
<b>Operator</b>	<input style="width: 100%;" type="text"/>	For authorization purposes, you should configure Vendor Specific Attributes for the radius users on the server.
<b>User</b>	<input style="width: 100%;" type="text"/>	Example: Add Vendor-Specific attribute
<b>OEM Proprietary</b>	<input style="width: 100%;" type="text"/>	cd /usr/share/freeradius vim dictionary.adtest (Add content below)
<b>No Access</b>	<input style="width: 100%;" type="text"/>	# dictionary.adtest VENDOR ADTest 58 # Standard attribute BEGIN-VENDOR ADTest ATTRIBUTE ADTest-group 1 string END-VENDOR ADTest vim dictionary (Add this line)

## HPM-621DE User's Manual

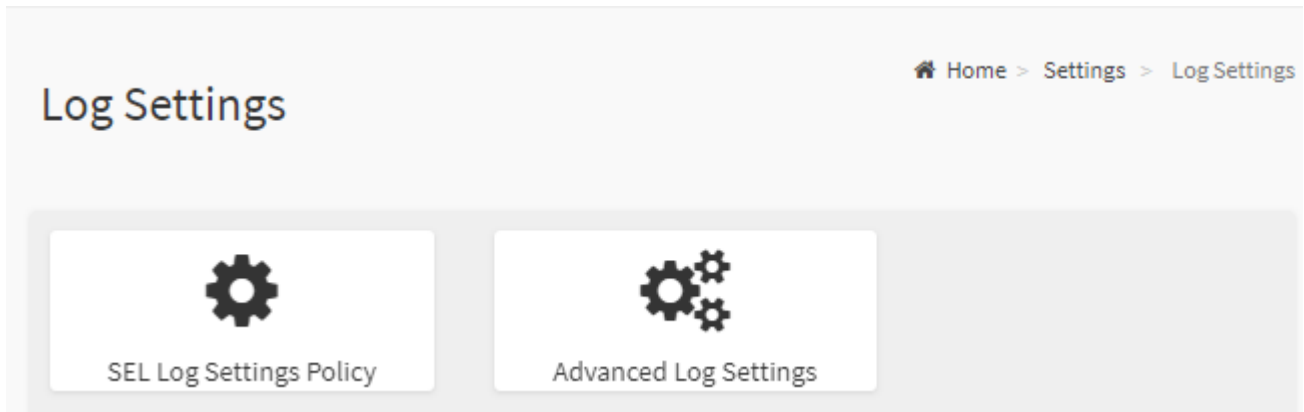
		<pre>\$INCLUDE dictionary.adtest</pre> <p>Add users: vim users (Add below content) "RadiusTest1" Cleartext-Password := "000000" Service-Type = Administrative-User, Auth-Type := System, ADTest-group := "H=4"</p> <p>NOTES: These fields will not allow more than 127 characters. '#' is not allowed.</p>
<b>Save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

### 2.6.4 Home>Settings>KVM Mouse Setting

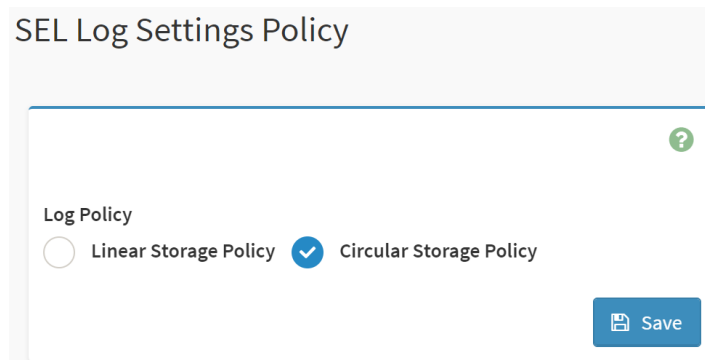


Item	Option	Description
<b>Mouse Mode</b>	<ul style="list-style-type: none"> <li>● Relative Positioning(Linux)</li> <li>● Absolute Positioning(Windows)</li> <li>● Other Mode (SLES-11 OS Installation)</li> </ul>	Select in either of three methods to calculate mouse position.
<b>Save</b>		Click button to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

2.6.5 Home>Settings>Log Settings



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



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

2.6.5.2 Home> Settings>Log Settings>Advanced Log Settings

Advanced Log Settings

?

System Log

Local Log

Remote Log

Port Type

UDP  TCP

File Size

Rotate Count

Remote Log Server

Remote Server Port

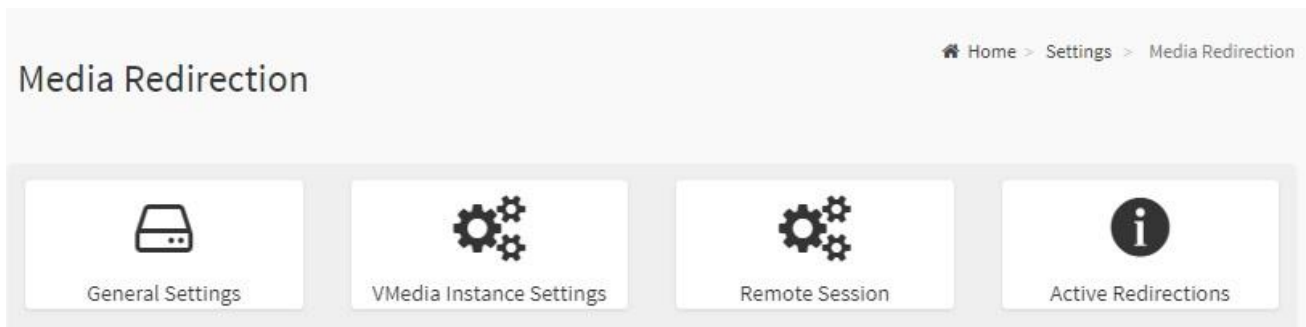
Enable Audit Log

Save

Item	Option	Description
<b>System Log</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select Enable System Log to view all system events. Entries can be filtered base on their classification levels
<b>Local Log</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select local log to save the logs locally (BMC)
<b>Remote Log</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select remote log to save the logs in a remote machine.
<b>Port Type</b>	<ul style="list-style-type: none"> <li><input checked="" type="radio"/> UDP</li> <li><input checked="" type="radio"/> TCP</li> </ul>	Port type is supported with the enable of Remote Log. User can select either UDP/TCP as per the requirement.
<b>File Size</b>	<input style="width: 100%;" type="text"/>	If Local log is selected ,specify the size of the file in bytes. <ul style="list-style-type: none"> <li>◆ Size ranges from 3 to 65535</li> <li>◆ Log files are rotated when the size is larger than the mentioned bytes , with regards for the last rotation time interval(1 minute).</li> </ul>
<b>Rotate Count</b>	<input style="width: 100%;" type="text"/>	When logged information exceeds the specified file size, the old log information automatically gets moved to back up files based on the rotate count value. If the rotate count is zero , the old log information

		gets cleared permanently each time.
<b>Remote Log Server</b>	<input type="text"/>	Specify the remote server address to log system events. Server address support the following: <ul style="list-style-type: none"> <li>♦ IP Address (Both IPv4 and IPv6 format).</li> <li>♦ FQDN (Fully qualified domain name) format</li> </ul>
<b>Remote Server Port</b>	<input type="text"/>	Specify the port number to log system events Note: If entering port number 0 , it will set port number as default. The default port number is 514
<b>Enable Audit Log</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select Enable Audit Log to view all audit events for this device.
<b>Save</b>	<input type="button" value="Save"/>	Click button to save the changes made

### 2.6.6 Home>Settings>Media Redirection



# HPM-621DE User's Manual

## 2.6.6.1 Home>Settings>Media Redirection>General Settings

### General Settings

Remote Media Support

Mount CD/DVD

Server Address for CD/DVD Images

Path in server

Share Type for CD/DVD

nfs  cifs

Domain Name

Username

Password

Same settings for Harddisk Images

Mount Harddisk

Server Address for Harddisk Images

Path in server

Share Type for Harddisk

nfs  cifs

Domain Name

Username

Password

Retry Interval

Retry Count



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

## HPM-621DE User's Manual

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

### 2.6.6.2 Home>Settings>Media Redirection>VMedia Instance Settings

#### VMedia Instance Settings

?

CD/DVD device instances


Hard disk instances

Remote KVM CD/DVD device instances

Remote KVM Hard disk instances

Power Save Mode

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

<b>instances</b>		are to be supported for Virtual Media redirection
<b>Power Save Mode</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Power Save Mode in BMC
<b>Save</b>		Click button to save the changes made

### 2.6.6.3 Home>Settings>Media Redirection>Remote Session

Remote Session ?

---

KVM Single Port Application


Keyboard Language


Retry Count

Retry Time Interval(Seconds)

Server Monitor OFF Feature Status

Automatically OFF Server Monitor, When KVM Launches



Item	Option	Description
<b>KVM Single Port Application</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Single Port Application support in BMC
<b>Keyboard Language</b>		Select the Keyboard Language
<b>Retry Count</b>	1 to 20	Number of times to be retried when a KVM failure occurs. Retry count ranges from 1 to 20
<b>Retry Time Interval(Seconds)</b>	5 to 30	Number of seconds to wait for subsequent retries. Time interval ranges from 5 to 30 seconds
<b>Server Monitor OFF Feature Status</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable the Server Monitor OFF feature
<b>Automatically OFF Server Monitor, When KVM Launches</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this option to enable Automatically OFF Server Monitor when KVM is launched
<b>Save</b>		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.

The screenshot shows the 'Active Redirections' page. At the top right, there is a breadcrumb trail: Home > Settings > Media Redirection > Active Redirections. Below the title, there is a green question mark icon. A red message box states 'No Media has been redirected.' Below this is a table with the following columns: Media Type, Media Instance, Client Type, Image Name, Redirection Status, and Client IP. Each column header has a small double-headed arrow icon next to it.

## 2.6.7 Home>Settings>Network Settings

The screenshot shows the 'Network Settings' page. At the top right, there is a breadcrumb trail: Home > Settings > Network Settings. Below the title, there are four large, light-colored buttons with icons and text labels: 'Network IP Settings' (with a network diagram icon), 'Network Link Configuration' (with a gear icon), 'DNS Configuration' (with a server rack icon), and 'Sideband Interface (NC-SI)' (with a network connection icon).

2.6.7.1 Home>Settings>Network Settings>Network IP Settings

Network IP Settings ?

---

Enable LAN

LAN Interface

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

---

Enable IPv4

Enable IPv4 DHCP

IPv4 Address

IPv4 Subnet

IPv4 Gateway

---

Enable IPv6

Enable IPv6 DHCP

IPv6 Index

IPv6 Address

Subnet Prefix Length

---

Enable VLAN

VLAN ID

VLAN Priority

[Save](#)

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

## HPM-621DE User's Manual

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

### 2.6.7.2 Home>Settings>Network Settings>Network Link Configuration

Network Link Configuration

?

LAN Interface

eth0

Auto Negotiation

Link Speed


1000 Mbps

Duplex Mode

FULL Duplex

NCSI Interface

Enabled

Item	Option	Description
<b>LAN Interface</b>	eth0	Select the network interface for which the Link speed and duplex mode are to be configured.
<b>Auto Negotiation</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is enabled to allow the device to perform automatic configuration, allowing it to achieve the best possible mode of operation (speed and duplex) over a link.
<b>Link Speed</b>	<ul style="list-style-type: none"> <li>● 10</li> <li>● 100</li> <li>● 1000</li> <li>● (Auto Negotiation)</li> </ul>	Link speed options are dependent on the capabilities of the network interface. Speed can be 10/100/1000 Mbps. Note: Link speed of 1000Mbps is not applicable when Auto Negotiation is set to OFF
<b>Duplex Mode</b>	<ul style="list-style-type: none"> <li>● Full duplex</li> <li>● Half duplex</li> </ul>	Select any one of the following duplex modes. Half duplex Full duplex
<b>NCSI Interface</b>		NCSI interface Enable/Disable
<b>Save</b>		Click button to save the changes made

2.6.7.3 Home>Settings>Network Settings>DNS Configuration

DNS Configuration ?

DNS Enabled  
 mDNS Enabled

---

**Host Name Setting**  
 Automatic  Manual

Host Name

---

**BMC Registration Settings**

BMC Interface:  
 eth0

Register BMC

Registration method:  
 Nupdate  DHCP Client FQDN  Hostname

Both

**Eth0 TSIG Configuration**  
 TSIG Authentication Enabled

Current TSIG Private File Info  
 Not Available

New TSIG Private File  
 ...

**Eth1 TSIG Configuration**  
 TSIG Authentication Enabled

Current TSIG Private File Info

New TSIG Private File  
 ...

---

**Domain Setting**  
 Automatic  Manual

Domain Name

---

**Domain Name Server Setting**  
 Automatic  Manual

DNS Server 1

DNS Server 2

DNS Server 3

Save

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



<b>Setting</b>	<ul style="list-style-type: none"> <li>● Manual</li> </ul>	automatically.
<b>Host Name</b>	<input type="text"/>	If Automatic is selected ,the this field automatically display the hostname. Otherwise,please enter the desired hostname for the device.
<b>Register BMC</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable Register BMC
<b>Registration method</b>	<ul style="list-style-type: none"> <li>● Nupdate</li> <li>● DHCP client FQDN</li> <li>● Hostname</li> </ul>	<p>Nupdate-Register with the DNS server using the nupdate application</p> <p>DHCP client FQDN-Register with the DNS server using DHCP option 81</p> <p>Hostname-Register with the DNS server using DHCP option 12</p> <p>Note: Hostname option should be selected if the DHCP server does not support option 81 and Hostname method registration does not support IPv6 Domain interface.</p>
<b>Both</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to modify TSIG authentication for both interfaces.
<b>TSIG Authentication Enabled(Eth0)</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable TSIG Authentication – if registering DNS via nupdate only.
<b>New TSIG Private File(Eth0)</b>	<input type="text" value="..."/>	Browse for a new TSIG private file to be uploaded to the BMC
<b>TSIG Authentication Enabled(Eth1)</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check this box to enable TSIG authentication – if registering DNS via nupdate only
<b>New TSIG Private File(Eth1)</b>	<input type="text" value="..."/>	Browse for a new TSIG private file to be uploaded to the BMC.
<b>Domain Setting</b>	<ul style="list-style-type: none"> <li>● Automatic</li> <li>● Manual</li> </ul>	Select whether the domain interface will be configured manually or automatically.
<b>Domain Name</b>	<input type="text"/>	Displays the domain name of the device, or ,if 'Manual' was selected, specify the domain name of the device.
<b>Domain Name Sever Setting</b>	<ul style="list-style-type: none"> <li>● Automatic</li> <li>● Manual</li> </ul>	Select whether the DNS interface will be configured manually or automatically.
<b>DNS Server 1</b>	<input type="text"/>	Specify the DNS(Domain Name System) server address to be configured for the BMC.
<b>DNS Server 2</b>	<input type="text"/>	IPv4 addresss should be given in dotted decimal representation.

## HPM-621DE User's Manual

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

### 2.6.7.4 Home>Settings>Network Settings>Sideband Interface

Sideband Interface (NC-SI)

NCSI Mode

Auto Failover Mode  Manual Switch Mode

NCSI Interface

eth0

Package ID

0 (active)

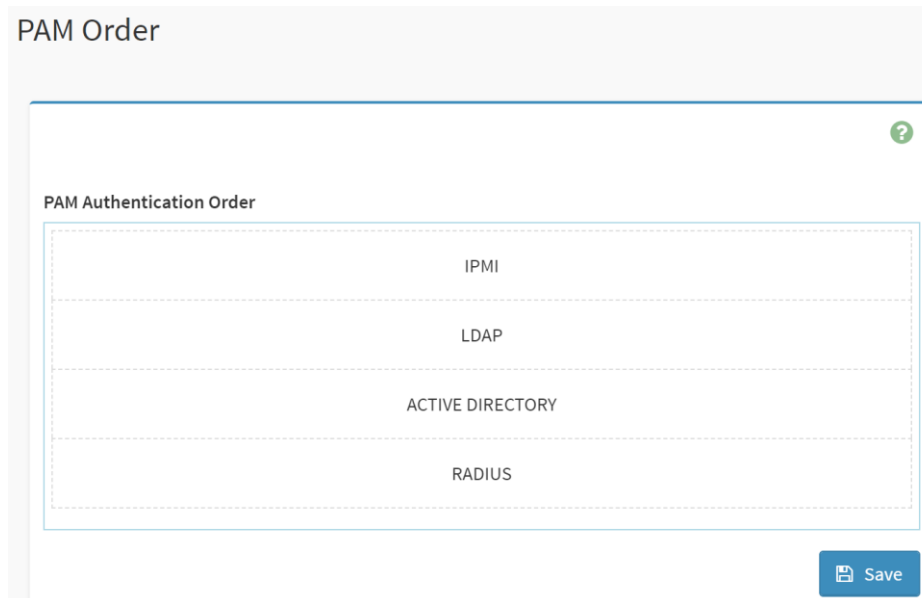
Channel Number

0 (package 0)(active)

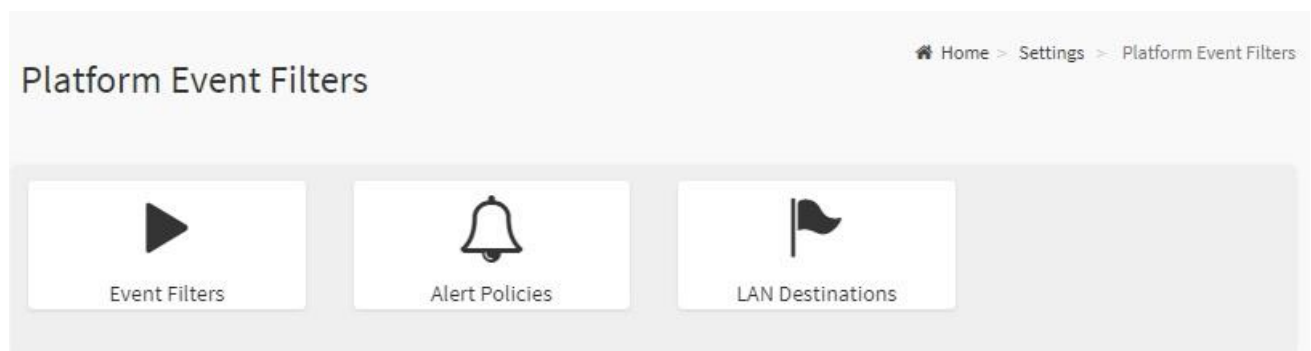
Item	Option	Description
<b>NCSI Mode</b>	<ul style="list-style-type: none"> <li>● Auto Failover Mode</li> <li>● Manual Switch Mode</li> </ul>	Select the NCSI mode
<b>NCSI Interface</b>	eth0	Choose the interface name for which to configure NCSI settings
<b>Package ID</b>		Choose the package ID to be configured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



## 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

The screenshot shows the 'Event Filters' configuration page. At the top, there is a breadcrumb trail: Home > Settings > Platform Event Filters > Event Filters. Below the title, there are radio buttons for 'All', 'Configured' (which is selected), and 'UnConfigured'. A green question mark icon is in the top right corner. The main area contains a grid of 15 event filter slots, each with a play button icon on the left and a delete 'x' icon on the right. Each slot contains the following text: 'PEF ID: [number] (Enabled)' followed by 'when All Sensors switches to any severity' and 'run Alert [number] & none'. The slots are arranged in four rows: the first three rows have four slots each, and the fourth row has three slots. The last slot in the fourth row is empty.

PEF ID	Filter Rule
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
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
PEF ID: 9 (Enabled)	when All Sensors switches to any severity run Alert (9) & none
PEF ID: 10 (Enabled)	when All Sensors switches to any severity run Alert (10) & none
PEF ID: 11 (Enabled)	when All Sensors switches to any severity run Alert (11) & none
PEF ID: 12 (Enabled)	when All Sensors switches to any severity run Alert (12) & none
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

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

Event Filter Configuration

Enable this filter

Event severity to trigger  
Any severity

Event Filter Action Alert

Power Action  
None

Alert Policy Group Number  
1

Raw Data

Generator ID 1  
255

Generator ID 2  
255

Generator Type  
 Slave  Software

Slave Address/Software ID

Channel Number  
0

IPMB Device LUN  
0

Sensor type  
All Sensors

Sensor name  
All Sensors

Event Options  
All Events

Event trigger  
255

Event Data 1 AND Mask  
0

Event Data 1 Compare 1  
0

Event Data 1 Compare 2  
0

Event Data 2 AND Mask  
0

Event Data 2 Compare 1  
0

Event Data 2 Compare 2  
0


Event Data 3 AND Mask  
0

Event Data 3 Compare 1  
0

Event Data 3 Compare 2  
0

## HPM-621DE User's Manual

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

<b>Sensor type</b>	<ul style="list-style-type: none"> <li>● All Sensors</li> <li>● Voltage</li> <li>● Temperature</li> <li>● Fan</li> <li>● Processor</li> </ul>	Select the type of sensor that will trigger the event filter action.
<b>Sensor Name</b>	<ul style="list-style-type: none"> <li>● All Sensors</li> <li>● +V12S_CPU1</li> <li>● +V5A</li> <li>● .....</li> </ul>	Choose the particular sensor from the sensor list.
<b>Event Options</b>	<ul style="list-style-type: none"> <li>● All Events</li> <li>● Sensor Events</li> </ul>	Choose event option to be either All events or Sensor specific events
<b>Event trigger</b>	0-255	This field is used to give Event/Reading type vale. Value ranges from 0 to 255
<b>Event Data 1 AND Mask</b>	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
<b>Event Data 1 Compare1</b>	0-255	This field is used to indicate whether each bit position's comparison is an exact comparison or not, Value ranges from 0 to 255
<b>Event Data 1 Compare2</b>	0-255	
<b>Event Data 2 AND Mask</b>	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
<b>Event Data 2 Compare1</b>	0-255	This field is used to indicate whether each bit position's comparison is an exact comparison or not, Value ranges from 0 to 255
<b>Event Data 2 Compare2</b>	0-255	
<b>Event Data 3 AND Mask</b>	0-255	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255
<b>Event Data 3 Compare1</b>	0-255	This field is used to indicate whether each bit position's comparison is an exact comparison or not, Value ranges from 0 to 255
<b>Event Data 3 Compare2</b>	0-255	
<b>Save</b>		Click button to save the changes made

# HPM-621DE User's Manual

































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

It shows all configured Alert policies and available slots.

You can modify or add new alert policy entry from here


Click x icon to delete an alert policy from the list

A maximum of 60 slots are available.

Alert Policies				Home > Settings > Platform Event Filters > Alert Policies
 Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 2 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 3 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 4 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 5 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 6 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 7 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 9 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 11 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 12 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 13 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		
 Group: 15 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		 Group: 1 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0		

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

Alert Policies

Alert Policies 

Policy Group Number  
1

Enable this alert

Policy Action  
Always send alert to this destination

LAN Channel  
1

Destination Selector

Event Specific Alert String

Alert String Key

Delete Save



Item	Option	Description
<b>Policy Group Number</b>	1-15	Choose a policy number that was configured in the Event filter table
<b>Enable this alert</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Check the option 'Enable' to enable the policy settings.
<b>Policy Action</b>	<ul style="list-style-type: none"> <li>● Always send alert to this destination</li> <li>● If previous successful ,skip this and continue(if configured)</li> <li>● If previous successful ,switch to another channel (if configured)</li> <li>● If previous successful ,switch to methods(if configured)</li> </ul>	<p>Choose any one of the Policy set values from the list.</p> <p>0- Always send alert to this destination</p> <p>1- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.</p> <p>2- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.</p> <p>3- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.</p> <p>4- If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.</p>
<b>LAN Channel</b>	1	Choose a LAN channel for the policy
<b>Destination Selector</b>	1-15	<p>Choose a destination from the configured destination list.</p> <p>Note: LAN Destinations have to be configured – under Configuration-&gt;PEF-&gt;LAN Destination</p>
<b>Event Specific Alert String</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	Choose the box to specify an event specific Alert String
<b>Alert String Key</b>	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.

## HPM-621DE User's Manual

<b>Delete</b>		Click button to delete the changes
<b>Save</b>		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.

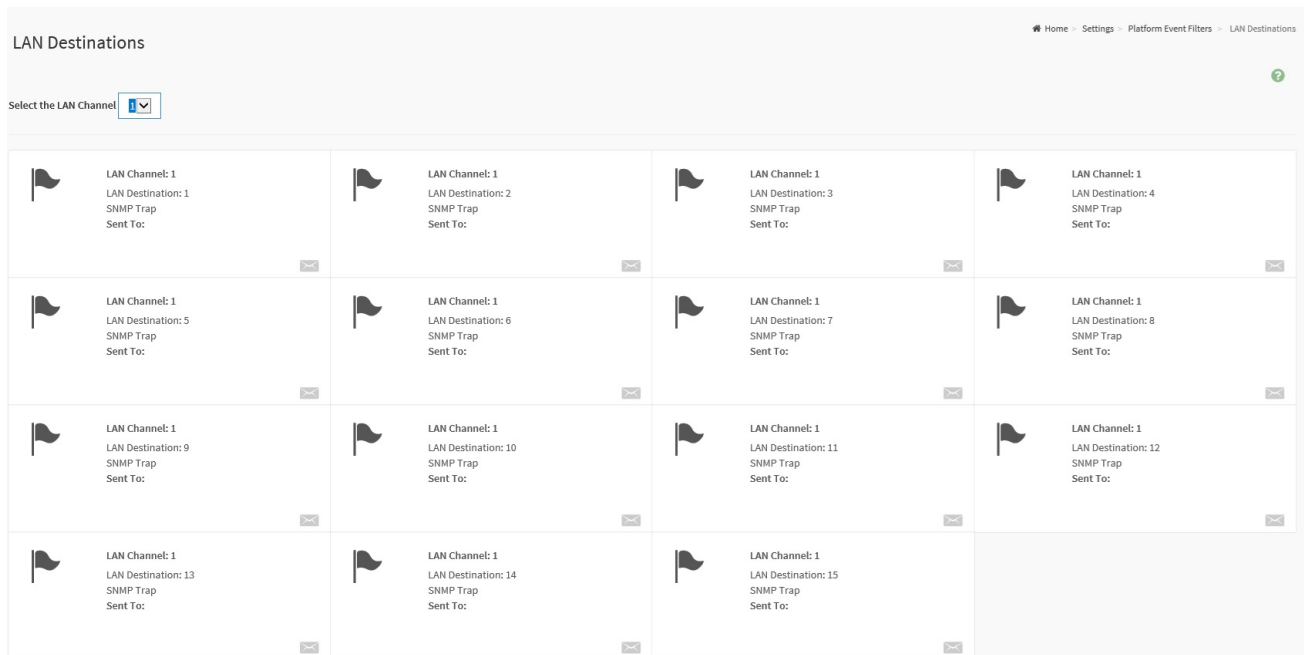
Click x icon to delete an entry from the list.

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.



LAN Destinations

Home > Settings > Platform Event Filters > LAN Destinations

Select the LAN Channel

LAN Channel: 1 LAN Destination: 1 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 2 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 3 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 4 SNMP Trap Sent To:
LAN Channel: 1 LAN Destination: 5 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 6 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 7 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 8 SNMP Trap Sent To:
LAN Channel: 1 LAN Destination: 9 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 10 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 11 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 12 SNMP Trap Sent To:
LAN Channel: 1 LAN Destination: 13 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 14 SNMP Trap Sent To:	LAN Channel: 1 LAN Destination: 15 SNMP Trap Sent To:	

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

### LAN Destination Configuration

?

LAN Channel  
1

LAN Destination  
1

Destination Type  
 SNMP Trap  E-Mail

SNMP Destination Address

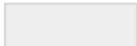

BMC Username

Email Subject

Email Message

Item	Option	Description
LAN Channel	1	Displays LAN Channel Number of the selected slot(read only)
LAN Destination	1	Displays Destination number of the selected slot(read only)
Destination Type	<ul style="list-style-type: none"> <li>● SNMP Trap</li> <li>● E-Mail</li> </ul>	Select destination type.
SNMP Destination Address	<input style="width: 50px; height: 20px;" type="text"/>	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	<input style="width: 50px; height: 20px;" type="text"/>	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	<input style="width: 50px; height: 20px;" type="text"/>	These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email


## HPM-621DE User's Manual


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

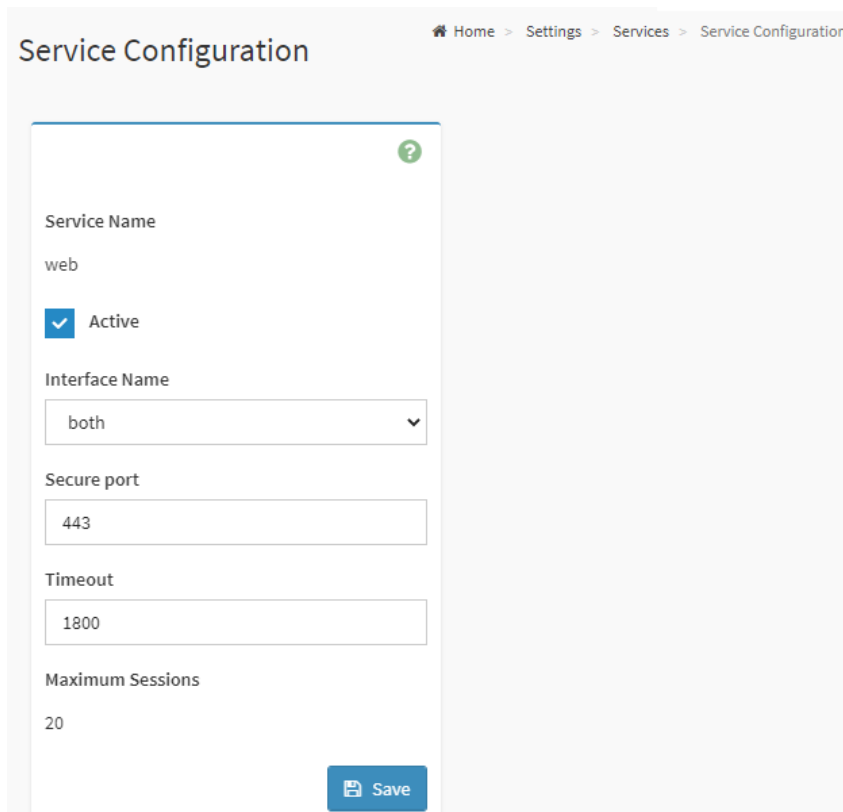
Note: To modify a service, user must be an Administrator.

Click on  icon to modify the services configuration.

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


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

Home>Settings>Services> Service Configuration




Item	Option	Description
<b>Service Name</b>	<input type="text"/>	Displays service name of the selected slot (read only)
<b>Active</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	<p>Current State</p> <p>Displays the current status of the service, either active or inactive. Check this box to activate the service.</p>
<b>Interface Name</b>	<ul style="list-style-type: none"> <li>● eth0</li> <li>● both</li> </ul>	<p>This indicate the interface on which the service is running. The user can choose any one of the available interfaces.</p> <p>Note: Service mapping to disabled interfaces will not work.</p> <ul style="list-style-type: none"> <li>◆ Status of interface can be checked/enabled,under Configuration-&gt;Network-&gt;LAN Settings.</li> <li>◆ Media and KVM interfaces are readonly when single port is enabled</li> </ul>
<b>Secure port</b>	<input type="text"/>	<p>Used to configure secure port numbers for the services.</p> <ul style="list-style-type: none"> <li>◆ Web default port is 443</li> <li>◆ KVM default port is 7582</li> <li>◆ CD Media default port is 5124</li> <li>◆ HD Media default port is 5127</li> <li>◆ SSH default port is 22</li> </ul>

## HPM-621DE User's Manual

		<ul style="list-style-type: none"> <li>Port value ranges form 1 to 65535</li> </ul> <p>Note : Port 80 is blocked for TCP/UDP protocols</p>
<b>Timeout</b>	<input type="text"/>	<p>Where supported , user can configure the session timeout value.</p> <ul style="list-style-type: none"> <li>Web and KVM timeout value ranges from 300 to 1800 seconds.</li> <li>Web timeout will be ignored if there is any ongoing KVM session</li> <li>SSH timeout value ranges from 60 to 1800 seconds</li> <li>Timeout value should be in multiples of 60 seconds.</li> </ul>
<b>Maximum Sessions</b>		Displays the maximum number of allowed sessions for the service.
<b>Save</b>		Click button to save the changes made

### Home>Settings>Services> Service Sessions

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


Click on  to terminate the particular session of the service

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


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

Home > Settings > Services > Service Sessions

## Service Sessions



Active Session - Web

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

2.6.11 Home>Settings> SMTP Settings

### SMTP Settings ?

---

**LAN Interface**

eth0
▼

**Sender Email ID**

---

**Primary SMTP Support**

**Primary Server Name**

**Primary Server IP**

**Primary SMTP port**

25

**Primary Secure SMTP port**

465

**Primary SMTP Authentication**

**Primary Username**

**Primary Password**

**Primary SMTP SSLTLS Enable**

**Primary SMTP STARTTLS Enable**

---

**Secondary SMTP Support**


Save

Item	Option	Description
<b>Lan interface</b>	eth0	Select the Lan interface to be configured
<b>Sender Email ID</b>	<div style="border: 1px solid #ccc; width: 80px; height: 20px; background-color: #f0f0f0;"></div>	Enter a valid 'Sender Email ID' on the SMTP Server. Maximum allowed size for Email ID is 64 bytes, which includes username and domain name.
<b>Primary SMTP</b>	<input checked="" type="checkbox"/>	Check this option to enable SMTP support for the BMC

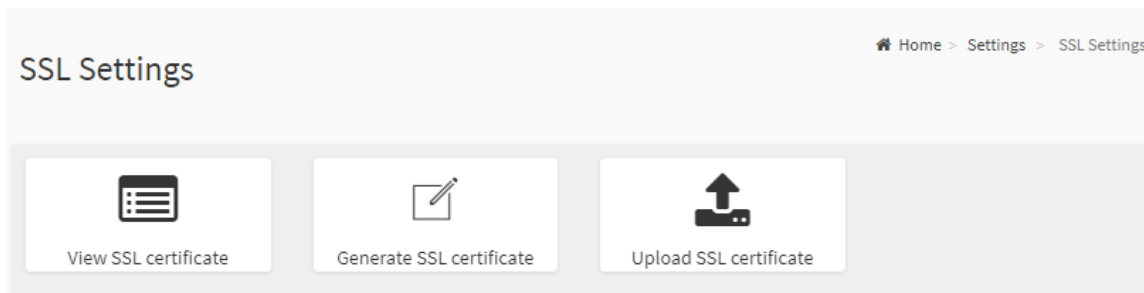
## HPM-621DE User's Manual

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



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

### 2.6.12 Home>Settings>SSL Settings



# HPM-621DE User's Manual

## 2.6.12.1 Home>Settings>SSL Settings> View SSL Certificate

This page displays the Current Certificate Information.

View SSL Certificate

---

Current Certificate Information ?

**Certificate Version**  
3

**Serial Number**  
61E7D5C8AEA9A49246ED79AD16A469FA

**Signature Algorithm**  
sha256WithRSAEncryption

**Public Key**  
(2048 bit)

---

**Issuer Common Name (CN)**  
AzurionPC

**Issuer Organization (O)**

**Issuer Organization Unit (OU)**

**Issuer City or Locality (L)**

**Issuer State or Province (ST)**

**Issuer Country (C)**

**Issuer Email Address**

---

**Valid From**  
Sep 28 15:31:28 2020 GMT

**Valid Till**  
Sep 28 15:41:29 2070 GMT

---

**Issued to Common Name (CN)**  
AzurionPC

**Issued to Organization (O)**

**Issued to Organization Unit (OU)**

**Issued to City or Locality (L)**

**Issued to State or Province (ST)**

**Issued to Country (C)**

**Issued to Email Address**

2.6.12.2 Home>Settings>SSL Settings>Generate SSL Certificate

Generate SSL Certificate ?

---

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address


Valid for

Key Length

Save


Item	Option	Description
<b>Common Name(CN)</b>	<input style="width: 50px; height: 20px; background-color: #e0e0e0;" type="text"/>	Common name for which the certificate is to be generated. <ul style="list-style-type: none"> <li>◆ Maximum of 64 alpha-numeric characters</li> <li>◆ Character '#' and '\$' are not allowed.</li> </ul>
<b>Organizaion(O)</b>	<input style="width: 50px; height: 20px; background-color: #e0e0e0;" type="text"/>	Name of the organization for which certificate is to be generated. <ul style="list-style-type: none"> <li>◆ Maximum of 64 alpha-numeric characters</li> <li>◆ Character '#' and '\$' are not allowed.</li> </ul>
<b>Organizaion Unit(OU)</b>	<input style="width: 50px; height: 20px; background-color: #e0e0e0;" type="text"/>	Section or Unit of the organization for which certificate is to be generated <ul style="list-style-type: none"> <li>◆ Maximum of 64 alpha-numeric characters</li> <li>◆ Character '#' and '\$' are not allowed.</li> </ul>
<b>City or Locality(L)</b>	<input style="width: 50px; height: 20px; background-color: #e0e0e0;" type="text"/>	City or Locality. <ul style="list-style-type: none"> <li>◆ Maximum of 64 alpha-numeric characters</li> </ul>

## HPM-621DE User's Manual


		<ul style="list-style-type: none"> <li>Character '#' and '\$' are not allowed.</li> </ul>
<b>State or Province(ST)</b>	<input type="text"/>	State or Province. <ul style="list-style-type: none"> <li>Maximum of 64 alpha-numeric characters</li> <li>Character '#' and '\$' are not allowed.</li> </ul>
<b>Country(C)</b>	<input type="text"/>	Country code. <ul style="list-style-type: none"> <li>Only two characters are allowed</li> <li>Special characters are not allowed</li> </ul>
<b>Email Address</b>	<input type="text"/>	Email addresss of organization
<b>Valid for</b>	<input type="text"/>	Requested validity days for the certificate Value ranges form 1 to 3650 days
<b>Key Length</b>	2048 bits	Choose the key length bit value of the certificare.
<b>Save</b>		Click button to save the changes made

### 2.6.12.3 Home>Settings>SSL Settings>Upload SSL Certificate


#### Upload SSL Certificate





**Current Certificate**  
Mon Mar 28 13:45:48 2022



**New Certificate**  


**Current Private Key**  
Mon Mar 28 13:45:48 2022

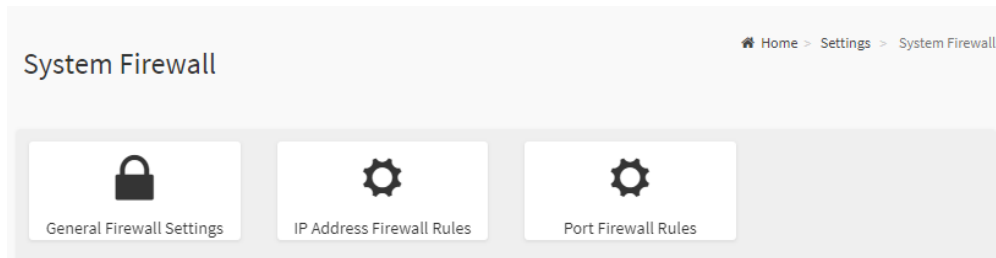
**New Private Key**  




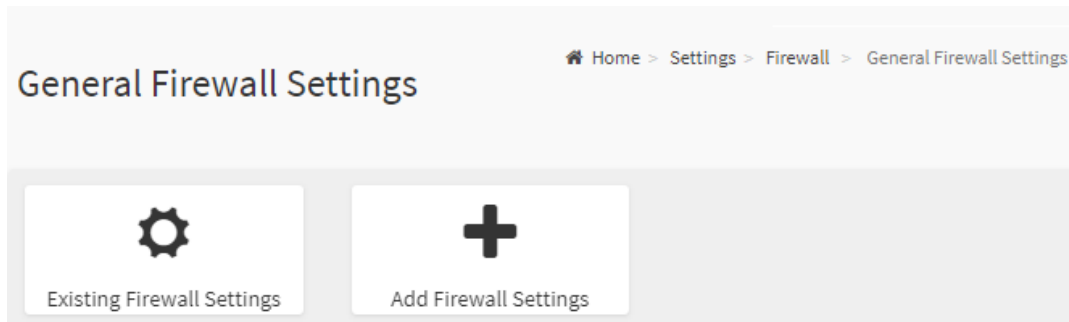
Item	Option	Description
<b>Current Certificate</b>		The information of the Current Certificate and date/time of its upload will be displayed(read-only)
<b>New Certificate</b>	<input style="width: 100%;" type="text"/> 	Browse and navigate to the new certificate file. Certificate file should be of pem type.
<b>Current Private Key</b>		Information for the current private key and date/time when it was uploaded will be displayed(read-only)

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

**2.6.13 Home>Settings>System firewall**

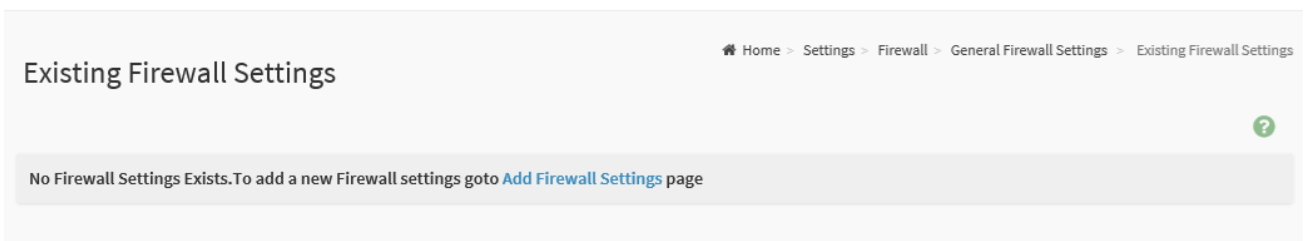


**2.6.13.1 Home>Settings> Firewall >General Firewall Settings**



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

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



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

Item	Option	Description
Block All	<ul style="list-style-type: none"> <li>● IPv4</li> <li>● IPv6</li> <li>● Both</li> </ul>	This option will block all incoming IPs and Ports
Flush All	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is used to flush all existing system firewall rules
Timeout	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is used to enable or disable firewall rules with timeout.
Start Date	<input type="text"/>	The firewall rule will become effective from this date
Start Time	<input type="text"/>	The firewall rule will become effective from this time
End Date	<input type="text"/>	The firewall rule will expire on this date
End Time	<input type="text"/>	The firewall rule will expire at this time
Save		Click button to save the changes made

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

### Add IP Rule

?

IP Single (or) Range Start

IP Range End

Enable Timeout

Start Date

YYYY/MM/DD
📅

Start Time

🕒

End Date

YYYY/MM/DD
📅

End Time

🕒


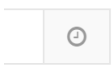

Rule

Allow
▼

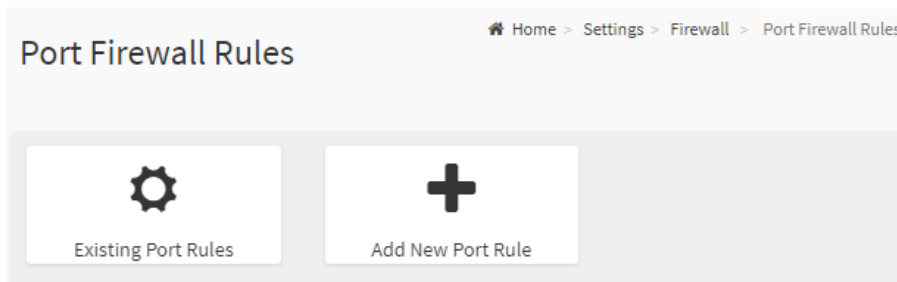
Save

Item	Option	Description
IP Single (or) Range Start	<input style="width: 80%;" type="text"/>	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	<input style="width: 80%; border-bottom: 1px dashed #ccc;" type="text"/>	This field is used to indicate the IP address or end of an IP address range
Enable Timeout	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is used to enable or disable timeout
Start Date	<input style="width: 80%;" type="text"/> 📅	The firewall rule will become effective from this date
Start Time	<input style="width: 80%;" type="text"/> 🕒	The firewall rule will become effective from this time

## HPM-621DE User's Manual

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

### 2.6.13.5 Home>Settings>System Firewall >Port Firewall Rules



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

This page display the list of existing IP firewall rules





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

### Add Port Rule

?

**Port Single (or) Range Start**

**Port Range End**

**Protocol**

TCP
▼

**Network Type**

IPv4
▼

Enable Timeout

**Start Date**

YYYY/MM/DD
📅

**Start Time**

🕒

**End Date**

YYYY/MM/DD
📅

**End Time**

🕒






**Rule**

Allow
▼

Save

Item	Option	Description
<b>IP Single (or) Range Start</b>	<input style="width: 80%;" type="text"/>	This field is used to specify the Port or start of a range of Port Addresses. Port value ranges from 1 to 65535. Note: Port 80 is blocked for TCP/UDP protocols
<b>IP Range End</b>	<input style="width: 80%;" type="text"/>	This field is used to configure the Port or end of a range of Port Addresses
<b>Protocol</b>	<ul style="list-style-type: none"> <li>● TCP</li> <li>● UDP</li> <li>● Both</li> </ul>	Select which protocol to support.
<b>Network Type</b>	<ul style="list-style-type: none"> <li>● IPv4</li> </ul>	Select which network type to support.

## HPM-621DE User's Manual

	<ul style="list-style-type: none"> <li>● IPv6</li> <li>● Both</li> </ul>	
<b>Enable Timeout</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	This option is used to configure timeout support for the new rule.
<b>Start Date</b>		Click field to select the duration of filter
<b>Start Time</b>		Click field to select the duration of filter
<b>End Date</b>		Click field to select the duration of filter
<b>End Time</b>		Click field to select the duration of filter
<b>Rule</b>	<ul style="list-style-type: none"> <li>● Allow</li> <li>● Block</li> </ul>	This field is used for allow or block this rule.
<b>Save</b>		Click button to save the changes made

### 2.6.14 Home>Settings>User management

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

The screenshot shows the 'User Management' page for 'Channel 1'. At the top, there is a breadcrumb trail: Home > Settings > User Management. Below the title, a dropdown menu is set to 'Channel 1'. A grid of 10 user slots is displayed. Slot 1 is 'anonymous (Disabled) Administrator' with 'KVM' and 'VMedia' roles. Slot 2 is 'admin (Active) Administrator' with 'KVM' and 'VMedia' roles. Slots 3, 4, 5, 6, 7, 8, 9, and 10 are all '(Disabled)'. A question mark icon is visible in the top right corner of the grid area.



Item	Option	Description
Channel	<ul style="list-style-type: none"> <li>● 1</li> <li>● 2</li> <li>● 8</li> </ul>	

2.6.14.1 Home>Settings>User management> User Management Configuration

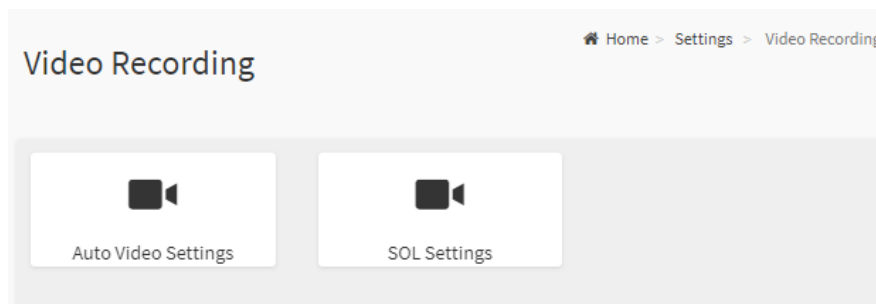
Item	Option	Description
Username	<input type="text"/>	Enter the name of the new user. <ul style="list-style-type: none"> <li>◆ String of 1 to 16 alpha-numeric characters.</li> <li>◆ Start with an alphabetical character.</li> <li>◆ Case-sensitive</li> <li>◆ '-', '_', '@' are allowed.</li> </ul>
Change Password	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to change the password.
Password Size	● 16 bytes	Select the preferred size for the password.

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

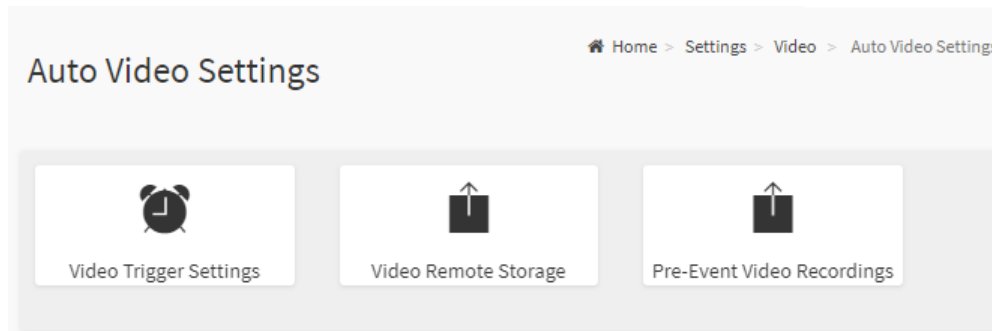
## HPM-621DE User's Manual

<b>Authentication Protocol</b>		Note: Password field becomes mandatory whenever the authentication protocol is changed.
<b>SNMP Privacy Protocol</b>		Choose the Encryption algorithm to be used for the SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.
<b>Email Format</b>	<ul style="list-style-type: none"> <li>● AMI-Format</li> <li>● Fixed Subject-Format</li> </ul>	<p>AMI-Format: The subject of this mail format is 'Alert from (your Host name)'. The mail content shows sensor information, ex: Sensor type and Description.</p> <p>Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.</p>
<b>Email ID</b>	<input type="text"/>	<p>enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.</p> <p>Maximum allowed size for Email ID is 64bytes (including username and domain name.)</p>
<b>Existing SSH Key</b>	<input type="text"/>	If available, the uploaded SSH key information will be displayed(read-only)
<b>Upload SSH Key</b>	<input type="text"/> 	<p>Use Browse button to navigate to the new public SSH key file.</p> <p>SSH key file should be of pub type.</p>
<b>Save</b>		Click button to save the changes made

### 2.6.15 Home>Settings>Video Recording



### 2.6.15.1 Home>Settings>Video Recording >Auto Video Settings

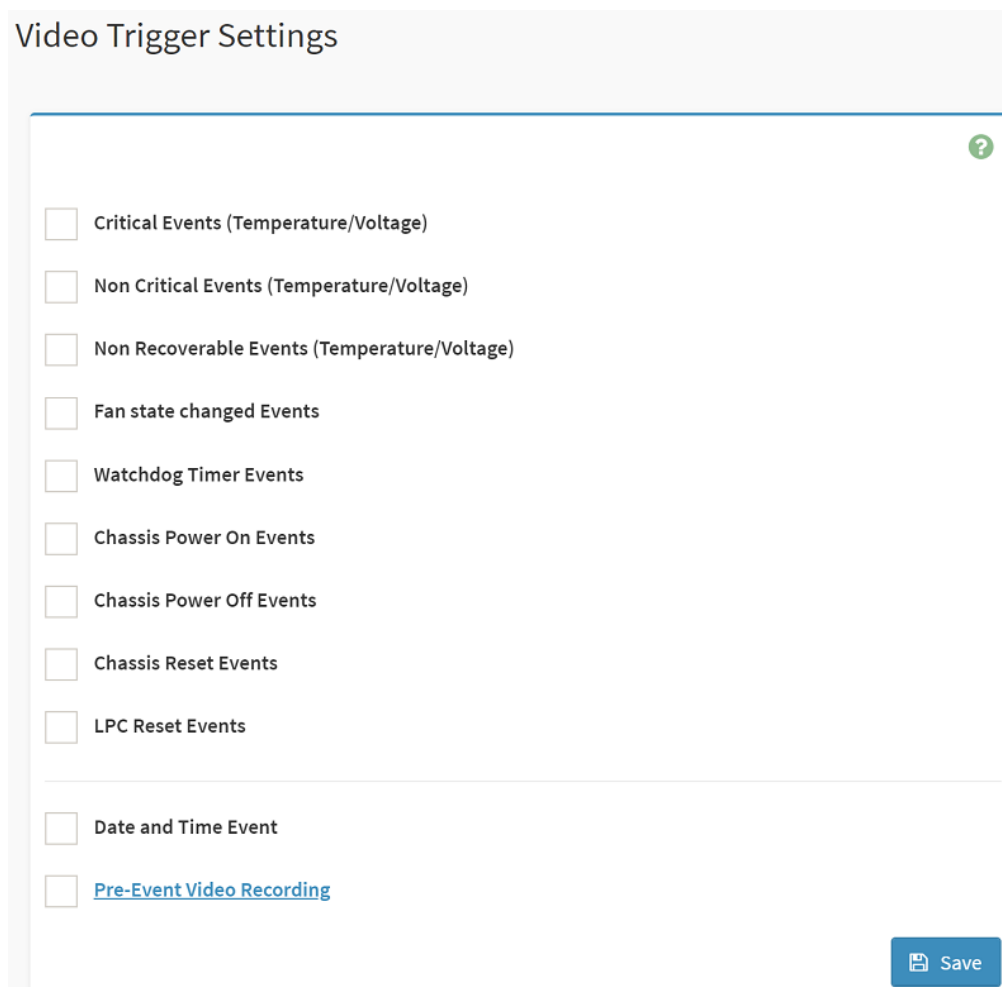


### 2.6.15.2 Home>Settings>Video Recording>Auto Video Settings>Video Trigger Settings>Video Trigger Settings


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

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

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



## HPM-621DE User's Manual

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



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

### Video Remote Storage ?

---

Record Video to Remote Server

Maximum Dumps

Maximum Duration (Sec)

Maximum Size (MB)

Server Address


Path in server

Share Type  
 NFS  CIFS

Save

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

## HPM-621DE User's Manual

	● CIFS	supported
<b>Save</b>	 Save	Click button to save the changes made

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

#### Pre-Event Video Recordings

?

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

**Video Quality**

Very Low
▼

**Compression Mode**


High
▼

**Frames Per Second**


1
▼

**Video Duration**

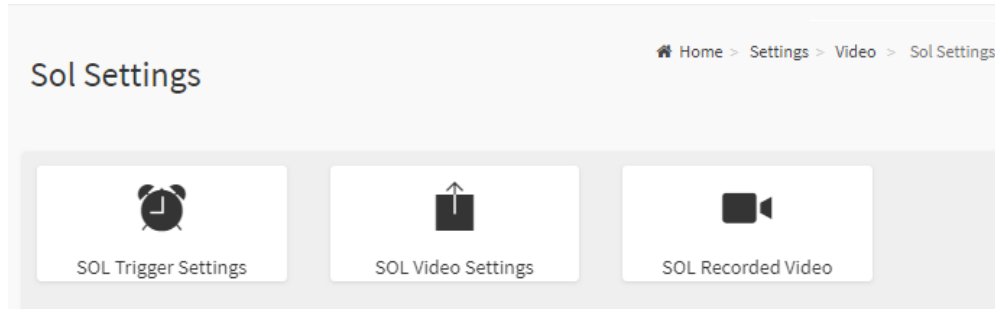
10
▼

 Save

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

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

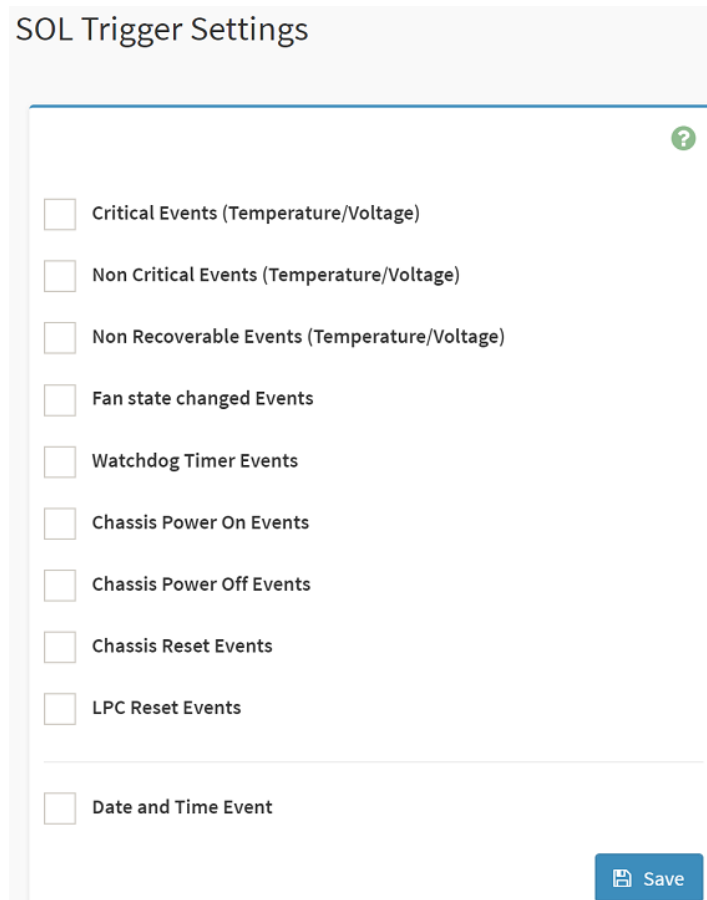
**2.6.15.5 Home>Settings>Video Recording>Sol Settings**



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


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

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



Item	Option	Description
<b>Critical Events</b>	<input checked="" type="checkbox"/>	check/uncheck this option to add/remove Critical Events trigger

## HPM-621DE User's Manual

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

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


SOL Video Settings ?

---


Log Size (KB)

Log File Count

Record Video to Remote Server



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

<b>Log File Count</b>	<input type="text"/>	Enter whether you want to have log files. Maxmum log file count is 1
<b>Record Video to Remote Server</b>	<input checked="" type="checkbox"/> <input type="checkbox"/>	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.
<b>Save</b>		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.

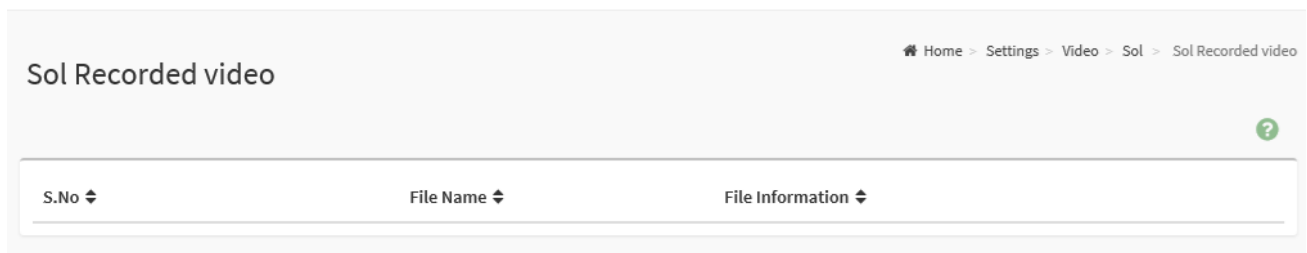
Note:

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.



## 2.7 HOME> REMOTE CONTROL

Remote Control Remote KVM

---

H5Viewer

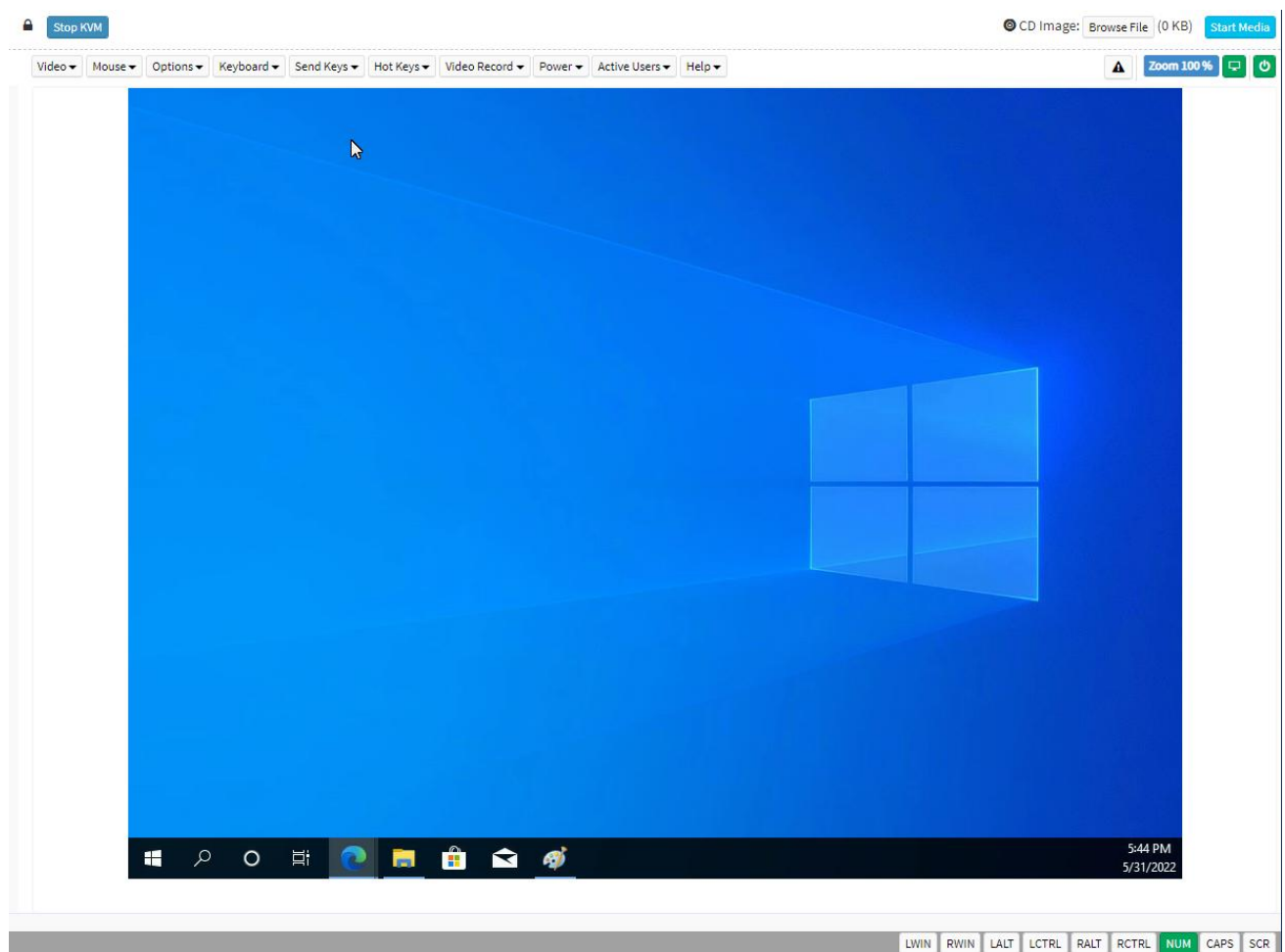
[Launch H5Viewer](#)

---

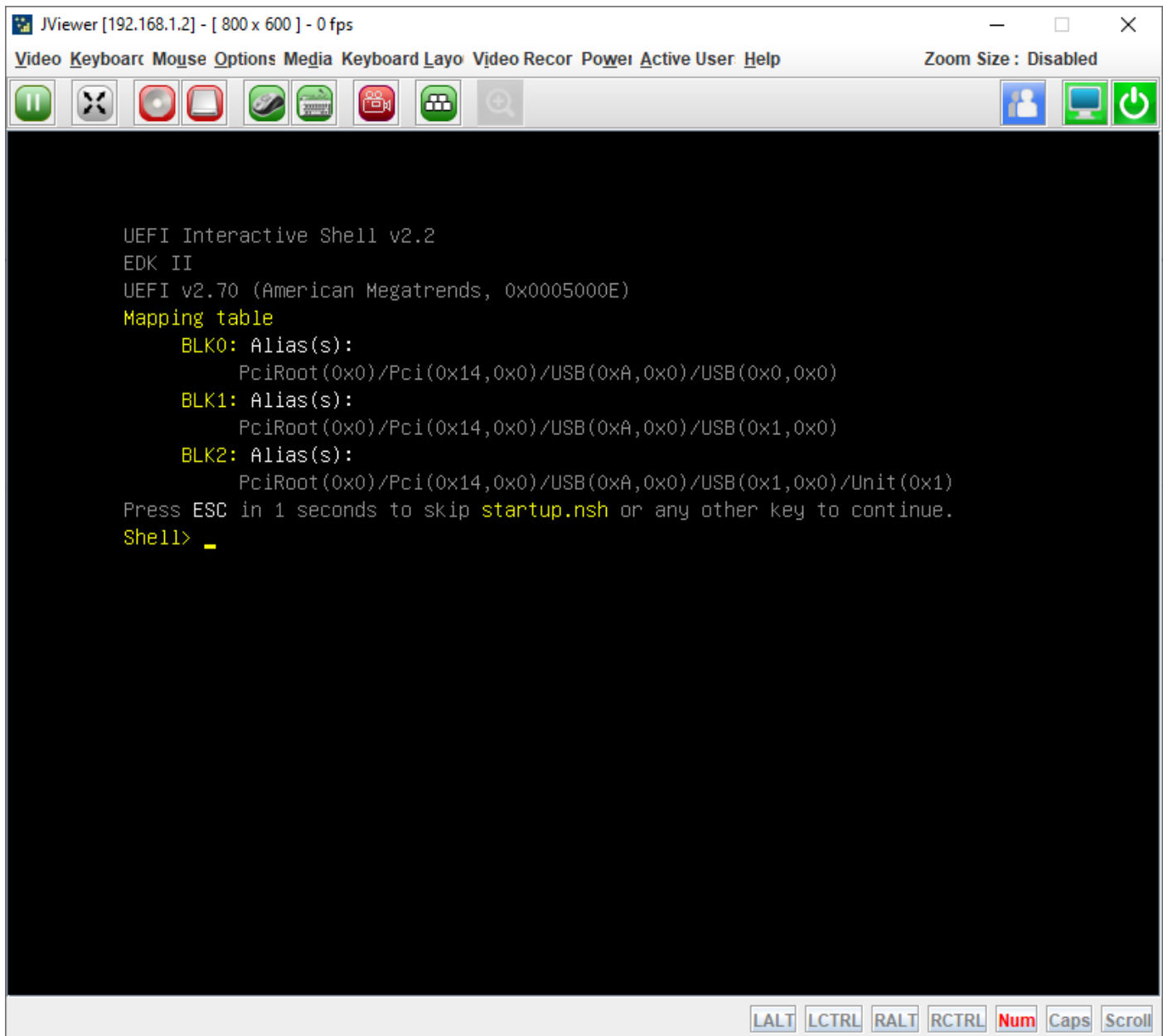
JViewer

[Launch JViewer](#)

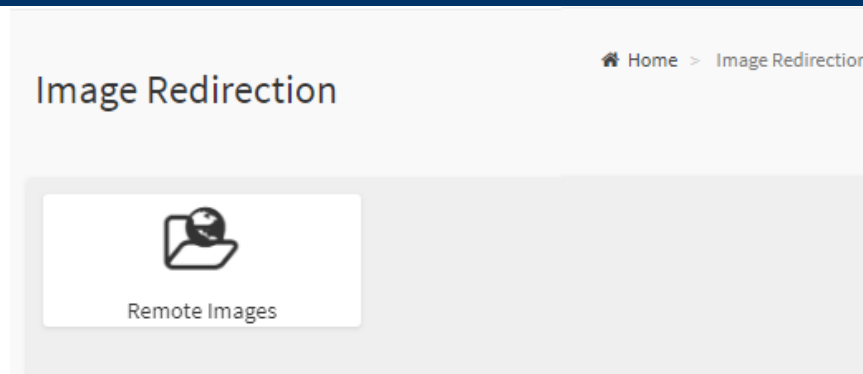
### 2.7.1 Home>Remote Control >H5Viewer



## 2.7.2 Home>Remote Control >JViewer

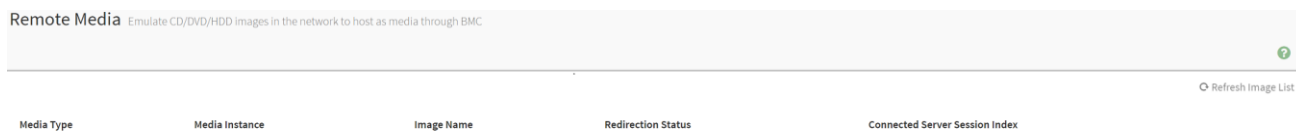


## 2.8 HOME>IMAGE REDIRECTION



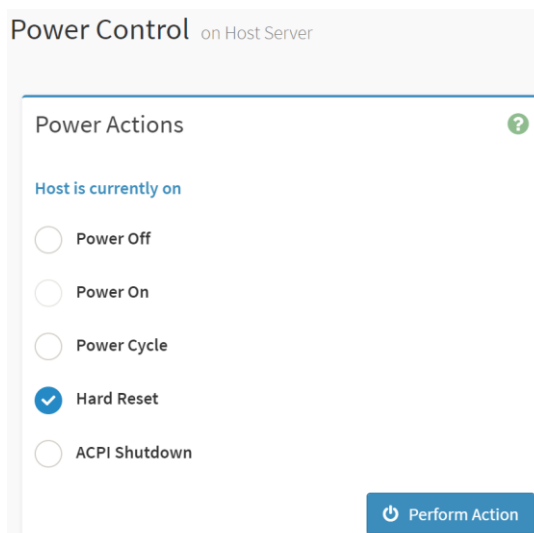
### 2.8.1 Home >Image Redirection>Remote Media

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




## 2.9 HOME> POWER CONTROL

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



Item	Option	Description
Power Control	✔ Power Off	Select this option to power off the server
	✔ Power On	Select this option to power on the server
	✔ Power Cycle	Select this option to first power off, and then reboot the system (cold boot)
	✔ Hard Reset	Select this option to reboot the system without powering off (warm boot)
	✔ ACPI Shutdown	Select this option to initiate operating system shutdown prior to the shutdown



<b>Perform Action</b>		Click button to perform the selected power action above immediately
-----------------------	---	---

## 2.10 HOME> FAN CONTROL

 If user first open Fan Control page ,this icon means host is currently on this fan mode.

### Fan Control


Fan Mode ?


Current FAN Mode is Stantard speed

Standard Speed

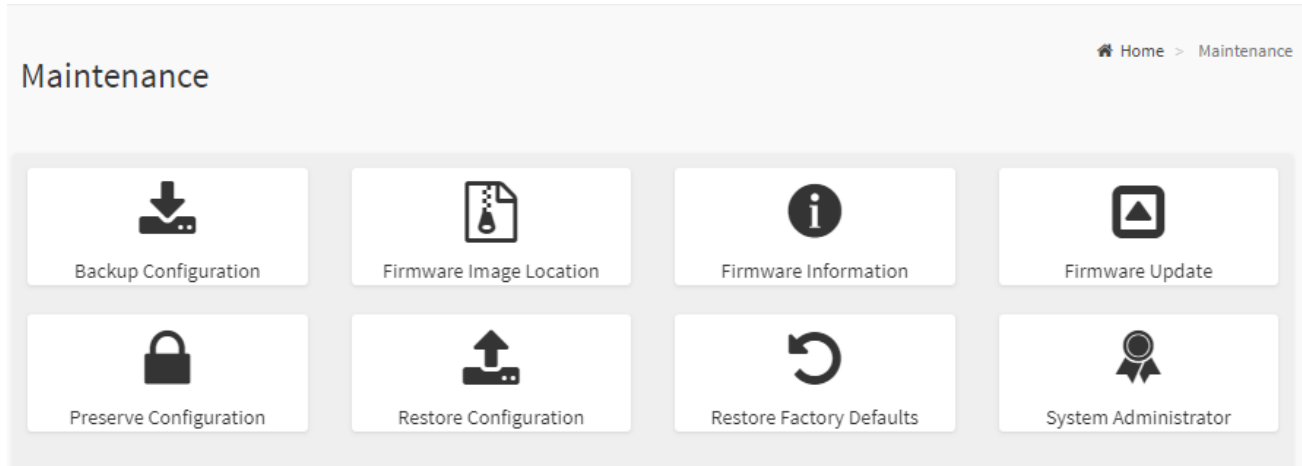
Full Speed

Optimal Speed



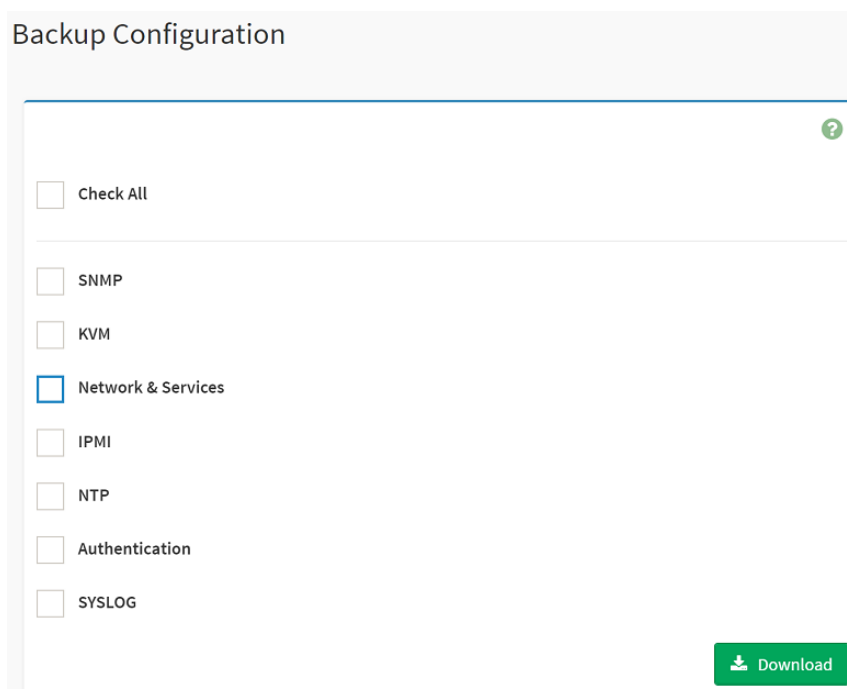
Item	Option	Description
<b>Fan Mode</b>	<input checked="" type="radio"/> Standard Speed	Select this option to set fan mode as standard speed
	<input checked="" type="radio"/> Full Speed	Select this option to set fan mode as full speed
	<input checked="" type="radio"/> Optimal Speed	Select this option to set fan mode as optimal speed
<b>Perform Action</b>		Click button to perform the selected fan mode above immediately

## 2.11 HOME> MAINTENANCE




### 2.11.1 Home>Maintenance >Backup Configuration

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

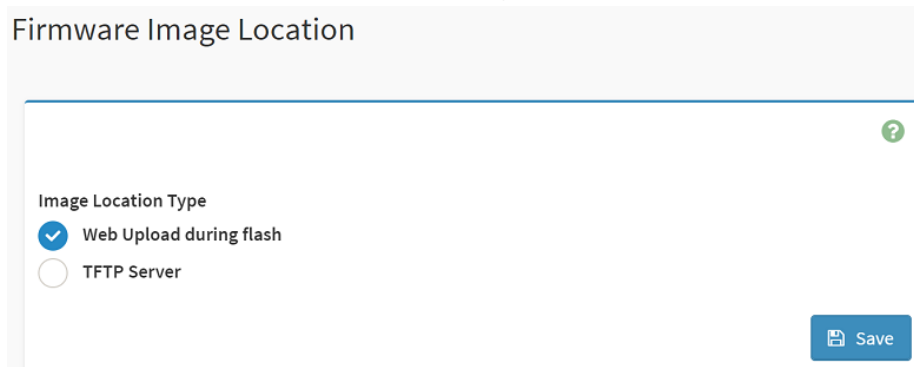



Item	Option	Description
Check All	<input checked="" type="checkbox"/> <input type="checkbox"/>	Set all following check box as checked
SNMP	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup SNMP configuration
KVM	<input checked="" type="checkbox"/> <input type="checkbox"/>	Select this option to backup KVM configuration
Network & Services	<input checked="" type="checkbox"/>	Select this option to backup Network & Services configuration

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

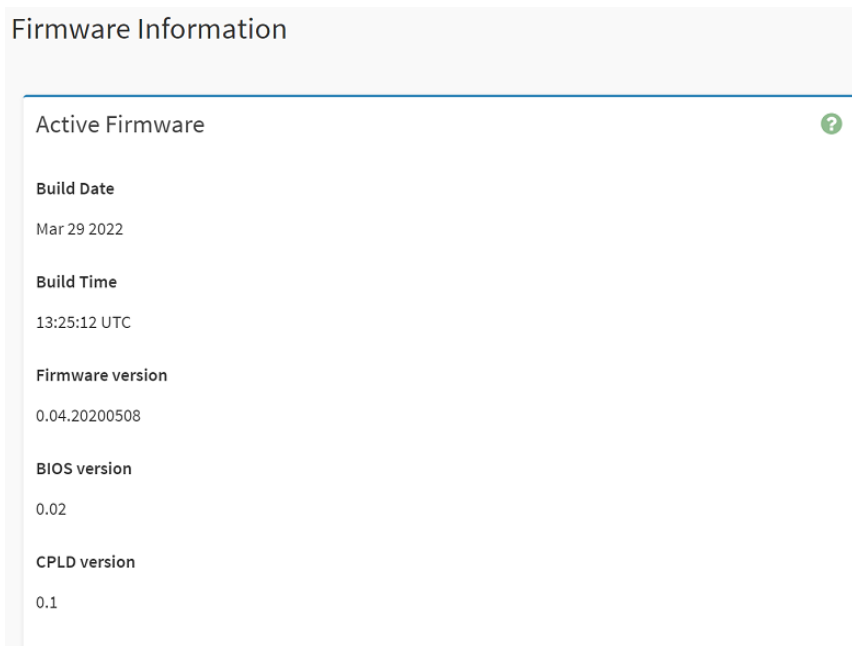
### 2.11.2 Home>Maintenance >Firmware Image Location

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



Item	Option	Description
<b>Image Location Type</b>	<ul style="list-style-type: none"> <li>● Web Upload during flash</li> <li>● TFTP Server</li> </ul>	Type of location to transfer the fw image into the BMC either Web Update during flash or TFTP Server
<b>Save</b>		Click button to save the changes made

2.11.3 Home>Maintenance >Firmware Information



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

### 2.11.4 Home>Maintenance >Firmware Update

Choose the firmware image to be updated

#### Firmware Update

?

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

- BMC Firmware update.
- HPM Firmware update supports the following components.
  - BOOT and APP
  - BIOS
  - ME
  - CPLD

**Select Firmware Image**

Choose File No file chosen

Start firmware update

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

Item	Option	Description
Choose File	<span style="border: 1px solid #ccc; padding: 2px 10px;">Choose File</span>	Click the button to choose firmware file for update
Start firmware update	<span style="background-color: #00a651; color: white; padding: 5px 15px; border-radius: 3px; cursor: pointer;">Start firmware update</span>	After choose firmware file,click the button to start firmware update.

2.11.5 Home>Maintenance >Preserve Configuration

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

### Preserve Configuration

?

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

Check All

---

SDR

FRU

SEL

IPMI

Network

NTP

SNMP

SSH

KVM


Authentication

Syslog

Web

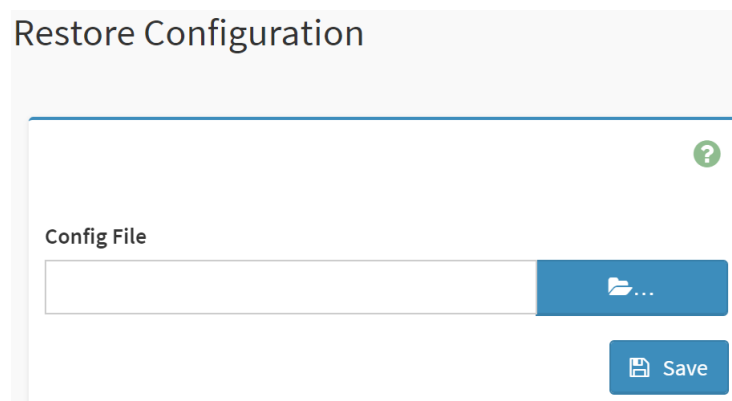
Save


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


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

### 2.11.6 Home>Maintenance >Restore Configuration

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



Item	Option	Description
<b>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 configuration
------	--	---

### 2.11.7 Home>Maintenance >Restore Factory Defaults

This option is used to restore the factory defaults of the device firmware.


This section lists the configuration items that will be preserved during restore factory default configuration.

#### Restore Factory Defaults

?


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

- SDR
- FRU
- SEL
- IPMI
- Network
- NTP
- SNMP
- SSH
- KVM
- Authentication
- Syslog
- Web

 Save


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



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

### 2.11.8 Home>Maintenance >System Administrator

#### System Administrator




**Username**  
sysadmin

Enable User Access

Change Password

**Password**

**Confirm Password**

 Save

## HPM-621DE User's Manual

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

## 2.12 HOME> SIGN OUT

192.168.1.6 says

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

OK

Cancel

## APPENDIX-A BMC HARDWARE: 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.

The chip architecture is showed below:

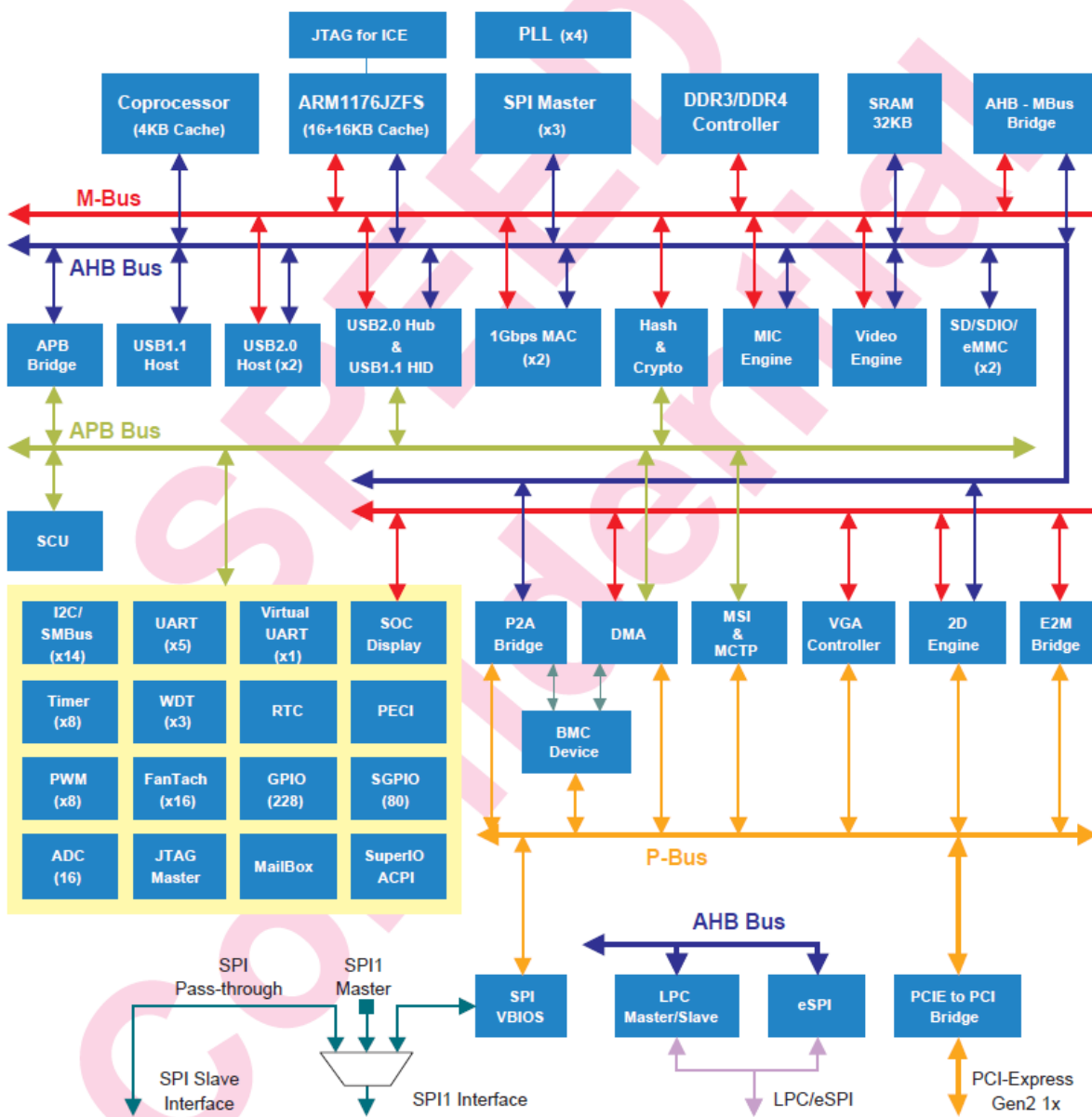


Figure A-1 AST2500 Chip architecture

## HPM-621DE User's Manual

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

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

## HPM-621DE User's Manual

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



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

## HPM-621DE User's Manual

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

## APPENDIX-C IPMI OEM COMMANDS LIST

Command	NetFn	CM D	DATA Length	DATA Value	Comments
Set Fan Mode	0x30	01h	1	0~3	<b>Input data:</b> 0=standard speed , 1= full speed , 2=optimal speed , 3>manual speed
Get Fan Mode	0x30	30h	0		<b>Response data:</b> 0=standard speed , 1= full speed , 2=optimal speed , 3>manual speed
Set FRU Lock	0x30	31h	1	0~1	<b>Input data:</b> 0=disable FRU eeprom write protect 1=enable FRU eeprom write protect
Set SOCFash Lock	0x30	33h	1	0~1	<b>Input data:</b> 0=enable use socflash tool 1=disable use socflash tool
Set Fan Speed	0x30	35h	2	Byte1 : 0~4 Byte2 : 0~100	<b>Input data:</b> Byte 1 = fan number Byte2 = PWM duty cycle
Get Fan Speed	0x30	36h	0		<b>Response data:</b> 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		<b>Response data</b> Byte1 = Low version Byte2 = High version
Get CPLD Version	0x30	39h	0		<b>Response data</b> Byte1 = Low version Byte2 = High version
Get System Operation Time	0x30	40h	0		<b>Response data</b> 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:

+V12S_CPU1	12.30 Volts	ok
+V5A	4.80 Volts	ok
+V3.3A	3.25 Volts	ok
+V1.8A	1.78 Volts	ok
+VNN_PCH_AUX	0.99 Volts	ok
+V1.05A	1.05 Volts	ok
+V1.2A_BMCDDDR	1.19 Volts	ok
+V1.15A_BMC	1.14 Volts	ok
+V1S_VCCIO_P2AD	1.01 Volts	ok
+V1S_VCCIO_P1AD	1 Volts	ok
+V12S_CPU2	12.30 Volts	ok
+V5SB	4.90 Volts	ok
+V12S	12.40 Volts	ok
+V5S	5 Volts	ok
+V3.3S	3.30 Volts	ok
+V3.0A_BAT	3.05 Volts	ok
+VCCIN_CPU1	1.80 Volts	ok
+VCCSA_CPU1	0.89 Volts	ok
+VCCIN_CPU2	1.80 Volts	ok
+VCCSA_CPU2	0.89 Volts	ok
P1 VDDR-123	1.22 Volts	ok
P1 VPP-123	2.50 Volts	ok
P1 VDDR-456	1.22 Volts	ok
P1 VPP-456	2.50 Volts	ok
P2 VDDR-789	1.22 Volts	ok

P2 VPP-789	2.50 Volts	ok
P2 VDDR-101112	1.22 Volts	ok
P2 VPP-101112	2.50 Volts	ok
+V1S_VCCIO_CPU1	1.01 Volts	ok
+V1S_VCCIO_CPU2	1.03 Volts	ok
P1 +VCCIN_T	33 degrees C	ok
P1 +VCCSA_T	32 degrees C	ok
P2 +VCCIN_T	35 degrees C	ok
P2 +VCCSA_T	37 degrees C	ok
P1 DDR-123 T	31 degrees C	ok
P1 VPP_123_T	28 degrees C	ok
P1 DDR-456 T	35 degrees C	ok
P1 VPP_456_T	31 degrees C	ok
P2 DDR-789 T	35 degrees C	ok
P2 VPP_456_T	32 degrees C	ok
P2 DDR-101112 T	38 degrees C	ok
P2 VPP_101112_T	37 degrees C	ok
P1 VCCIO_T	32 degrees C	ok
P2 VCCIO_T	33 degrees C	ok
CPU1 FAN	2200 RPM	ok
CPU2 FAN	2250 RPM	ok
SYS FAN1	1700 RPM	ok
SYS FAN2	1050 RPM	ok
SYS FAN3	1300 RPM	ok
Outlet T	26 degrees C	ok
Inlet T	24 degrees C	ok
CPU1 T	34 degrees C	ok
CPU2 T	34 degrees C	ok
PCH T	35 degrees C	ok
DIMM1 T	no reading	ns
DIMM2 T	no reading	ns
DIMM3 T	no reading	ns
DIMM4 T	31 degrees C	ok
DIMM5 T	no reading	ns

## HPM-621DE User's Manual

DIMM6 T	no reading	ns
DIMM7 T	no reading	ns
DIMM8 T	no reading	ns
DIMM9 T	no reading	ns
DIMM10 T	31 degrees C	ok
DIMM11 T	no reading	ns
DIMM12 T	no reading	ns
CPU THERMTRIP	0x00	ok
Slot1_GPU_T	no reading	ns
Slot2_GPU_T	no reading	ns
Slot3_GPU_T	28 degrees C	ok
Slot4_GPU_T	no reading	ns
Slot5_GPU_T	29 degrees C	ok
Slot6_GPU_T	no reading	ns
Slot7_GPU_T	no reading	ns

## **APPENDIX-E DEFAULT CONFIGURATION**

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

**Table F-1 Default Configuration**

<b>Parameter Name</b>	<b>Default Value</b>
<b>User IDs</b>	<b>(User/Password/Privilege/Channels)</b>
USER ID 1:	NULL/NULL/User/LAN
USER ID 2:	root/root/Administrator/LAN
<b>LAN Channel</b>	
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
<b>SOL</b>	
SOL Enable	Enable SOL payload
Payload Authentication/Authentication	Force encryption/ Authentication controlled by remote software
SOL Privilege Level Limit	Administrator
SOL non-volatile bit rate	115200 bps
SOL volatile bit rate	115200 bps
<b>Power Restore Policy</b>	chassis always powers up after AC on

## APPENDIX-F FIRMWARE UPDATE

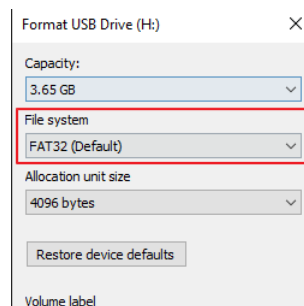
If necessary, the system firmware can be updated at local machine or remote console. Please refer the following instructions.

### 1. BIOS + SPS

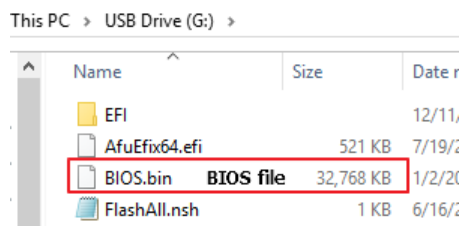
Update Method	OS	Tool and Jumper settings
Local Update	UEFI environment	AfuEfix64.efi <b>Need to disable SPS by JME1 jumper.</b>
	Windows PE environment	AFUWINx64.EXE <b>Need to disable SPS by JME1 jumper.</b>
Remote update	IPMI command	Yafuflash.exe <b>No need to disable SPS.</b>
	IPMI Web UI	No tool required <b>No need to disable SPS.</b>

#### 1.1 BIOS + SPS update in UEFI environment

1. Format a USB flash drive to FAT32.



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

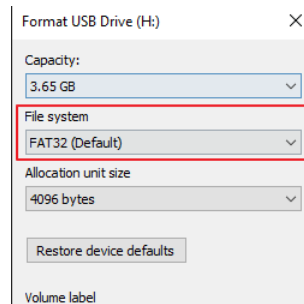


3. Plug the USB drive to the Server and close pin 2-3 of JME1.

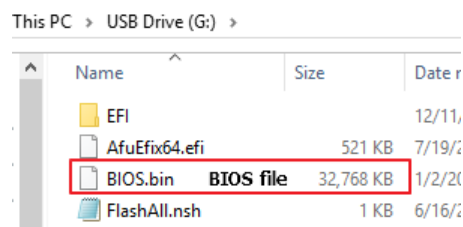


Power on system. When you hear BIOS ready beep, perss **F11** to enter boot

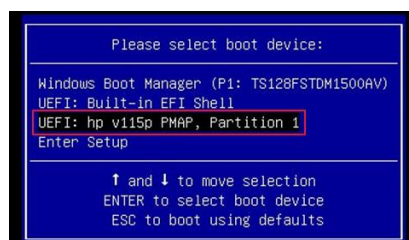
1. Format a USB flash drive to FAT32.



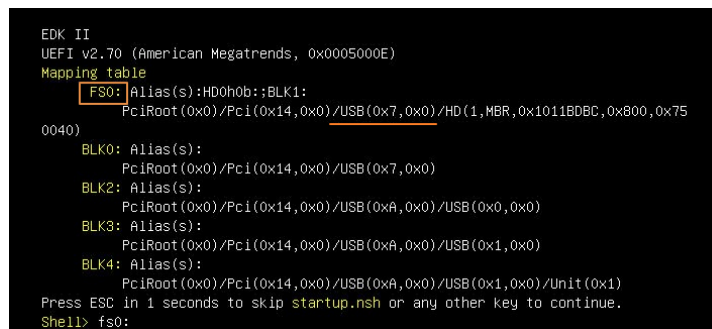
2. Download the update tool and BIOS file(xxx.bin), then save at the **root** directdory of the USB drive.



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



## HPM-621DE User's Manual

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

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

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

fs0:\> FlashAll.nsh BIOS.bin      input your BIOS file name
```

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

```
Reading flash ..... done
- ME Data Size checking . ok
- FFS checksums ..... ok
- Check RomLayout ..... ok.
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
Erasing Main Block ..... done
Updating Main Block ..... done
Verifying Main Block ..... done
Erasing NVRAM Block ..... done
Updating NVRAM Block ..... done
Verifying NVRAM Block ..... done
- Update success for FDR
- Update success for PTT.. -
- Successful Update Recovery Loader to OPRx!!
- Successful Update MFSB. -
- Successful Update FTFR!!-
- Successful Update MFS, IVB1 and IVB2!!
- Successful Update FLOG and UTOK!!
- ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!

Process completed.
FS0:\>
```

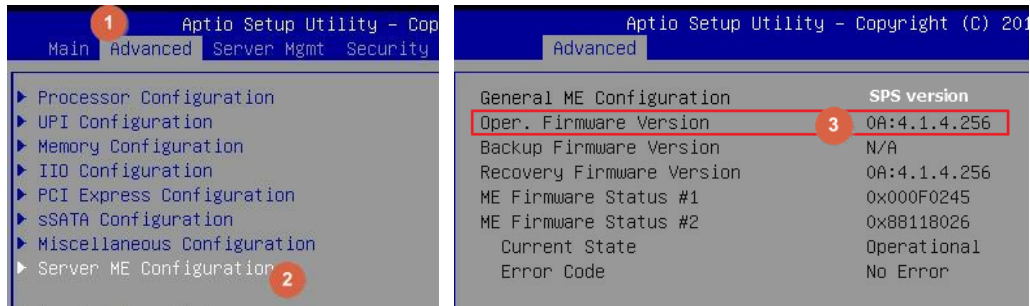
8. Remove AC power and move **JME1** jumper back to pin 1-2.
9. Power on, then boot to BIOS to check if BIOS version and SPS version are correct.

BIOS version:

```
Aptio Setup Utility - Copyright (C) 2020 American
Main Advanced Server Mgmt Security Boot Save & Exit

BIOS Information
BIOS Vendor                American Megatrends
Core Version                5.14
Compliance                 UEFI 2.7; PI 1.6
Project Version            OACLA 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
```

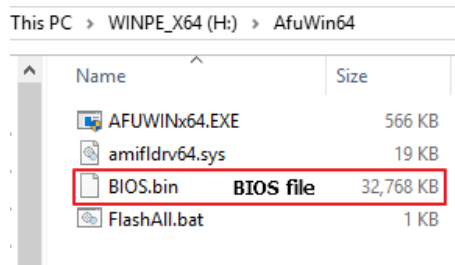
SPS version:



# HPM-621DE User's Manual

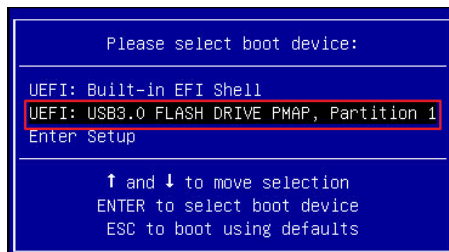
## 1.2 BIOS + SPS update in Windows PE environment

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



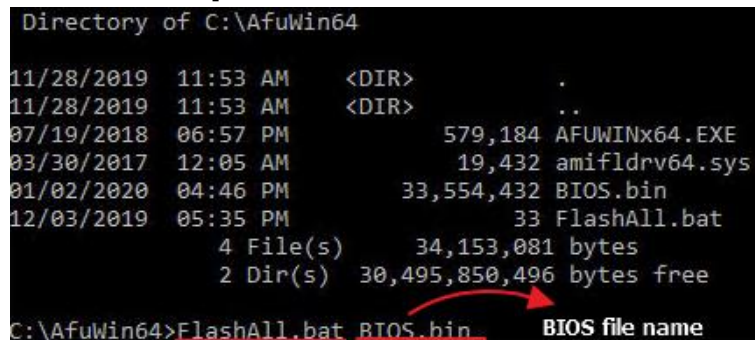
2. Plug the WinPE disk to server and close pin 2-3 of **JME1**.

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]**



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

```
Administrator: X:\windows\system32\cmd.exe
-----+-----
                AMI Firmware Update Utility v5.11.01.1745
                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
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 !!
WARNING : System must power-off to have the changes take effect!

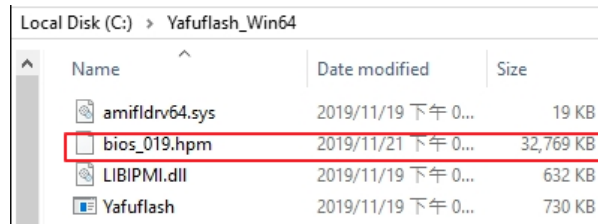
Process completed.
C:\AfuWin64>
```

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.

## HPM-621DE User's Manual

### 1.3 BIOS + SPS update using IPMI command

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



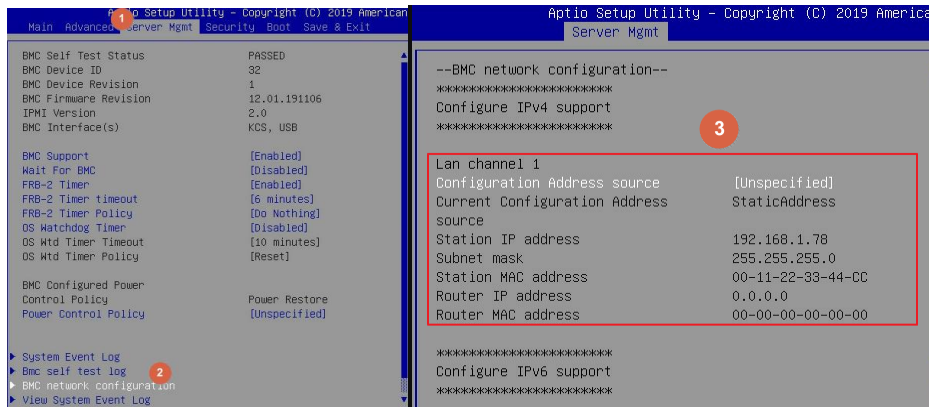
#### 2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.

#### 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.

```
C:\Windows\System32\cmd.exe - Yafuflash.exe -nw -ip 192.168.1.78 -U admin -P admin -d 2 bios_019.hpm
C:\Yafuflash_Win64>Yafuflash.exe -nw -ip 192.168.1.78 -U admin -P admin -d 2 bios_019.hpm
INFO: Yafu INI Configuration File not found... Default options will not be applied...
Creating IPMI session via network with address 192.168.1.78...Done
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
(C)Copyright 2017, American Megatrends Inc.
signed hash length is 128
Beginning BIOS Update...
Please type (Y/y) to Update or (N/n) to Cancel
Enter your Option :
```

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



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

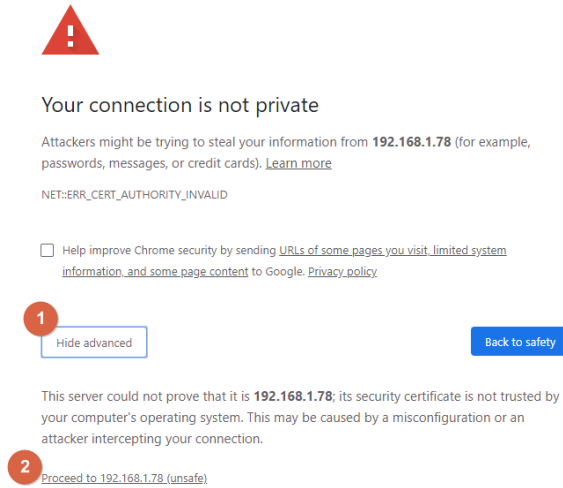
```
C:\Yafuflash_Win64>Yafuflash.exe -nw -ip 192.168.1.78 -U admin -P admin -d 2 bios_019.hpm
INFO: Yafu INI Configuration File not found... Default options will not be applied...
Creating IPMI session via network with address 192.168.1.78...Done
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
(C)Copyright 2017, American Megatrends Inc.
signed hash length is 128
Beginning BIOS Update...
Please type (Y/y) to Update or (N/n) to Cancel
Enter your Option : y
Uploading Image : 100%... done
Flashing Firmware Image : 100%... done
Verifying Firmware Image : 100%... done
```

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

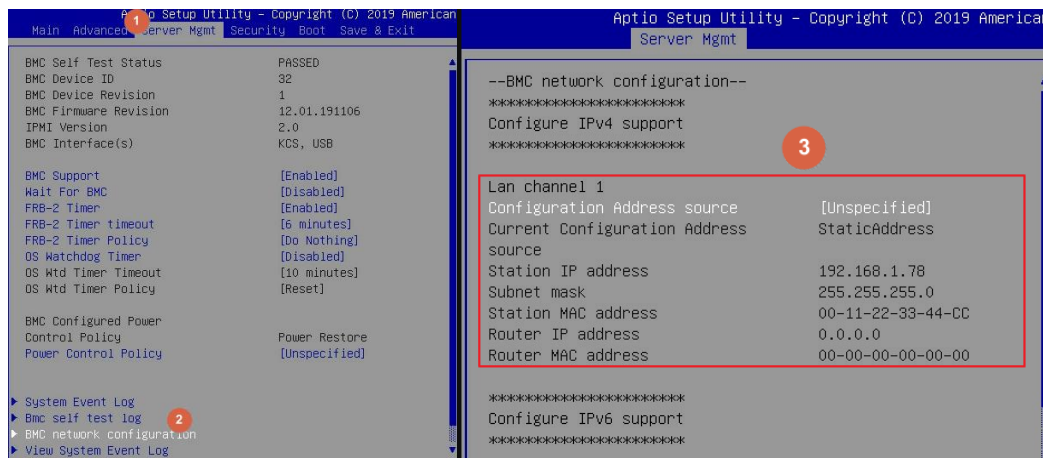
## 1.4 BIOS + SPS update using IPMI Web UI

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.

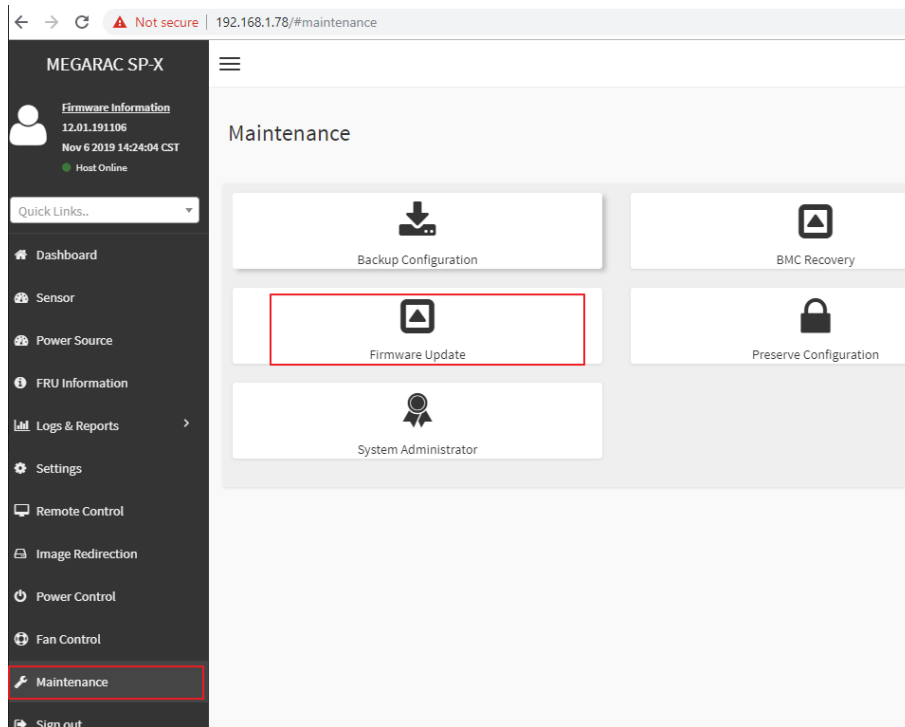


Note: BMC IP address can be configured at BIOS menu.

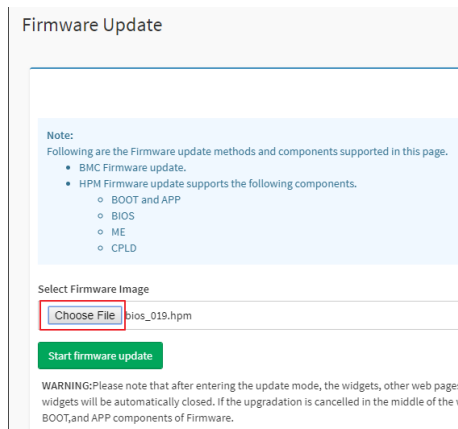


# HPM-621DE User's Manual

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



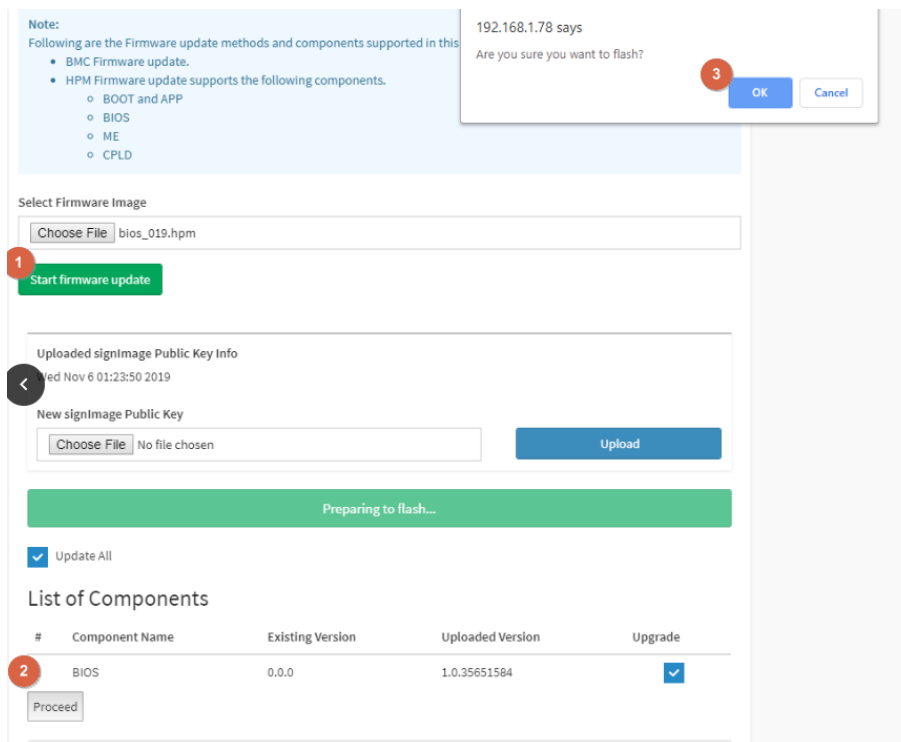
3. **Choose File** to select BIOS file(xxx.hpm).



4. Click the **Start firmware update** button, then **Proceed**. The message appears,



“Are you sure you want to flash?”. Click **OK**.



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

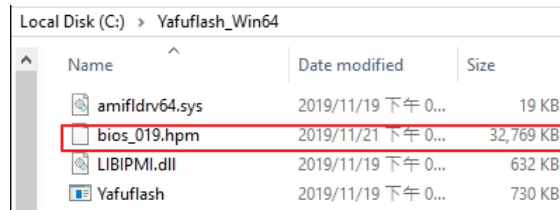


6. Server will reset after few seconds, refer 1.1.1 step9 to check the BIOS and SPS version.

# HPM-621DE User's Manual

## 1.5 BIOS + SPS update using IPMI command

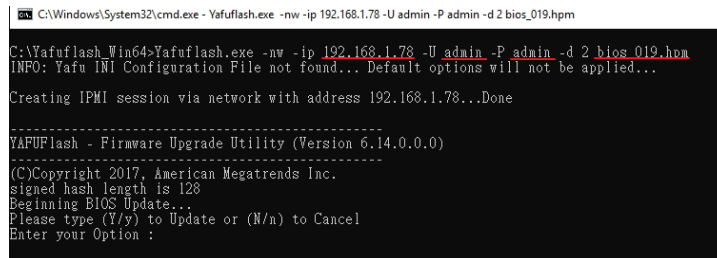
1. Copy BIOS file(xxx.hpm) to Yafuflash tool folder



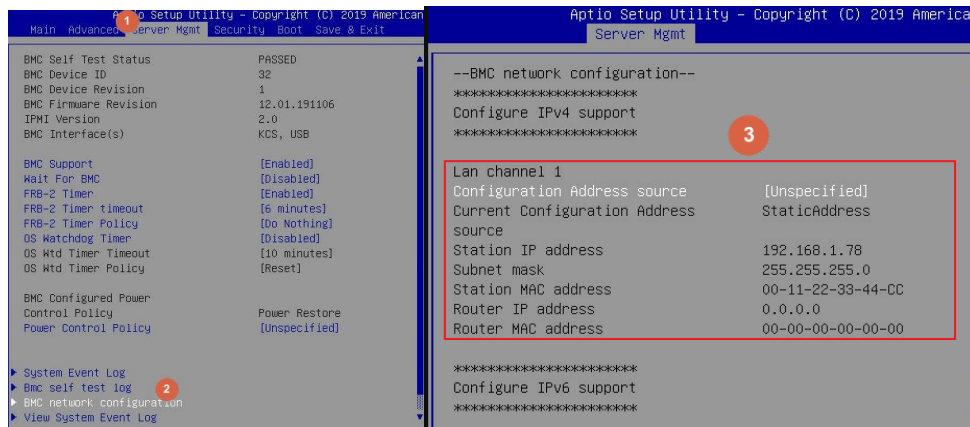
2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.

3. Input the command:

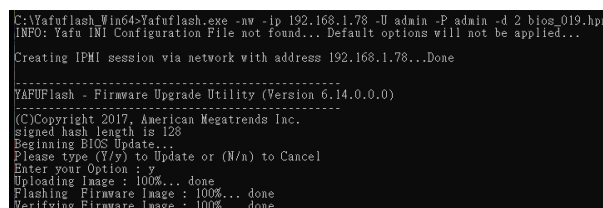
Yafuflash.exe -nw -ip [BMC IP address] -U [user name] -P [user password] -d 2 [BIOS file name]. The default username and password are admin/admin.



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



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

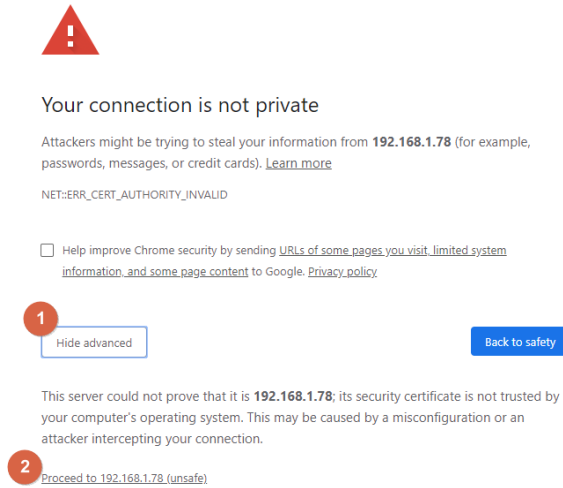


5. Refer 1.1.1 step9 to check the BIOS and SPS version.

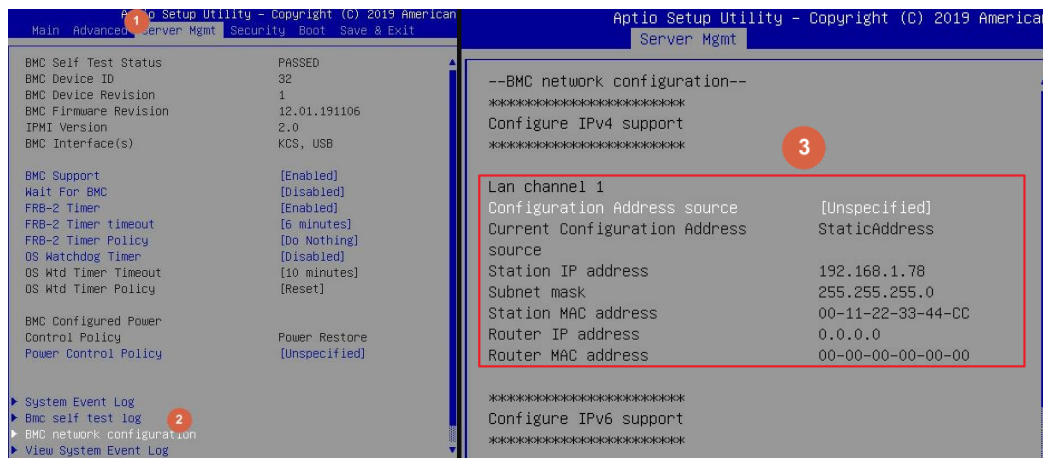
## 1.6 BIOS + SPS update using IPMI Web UI

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

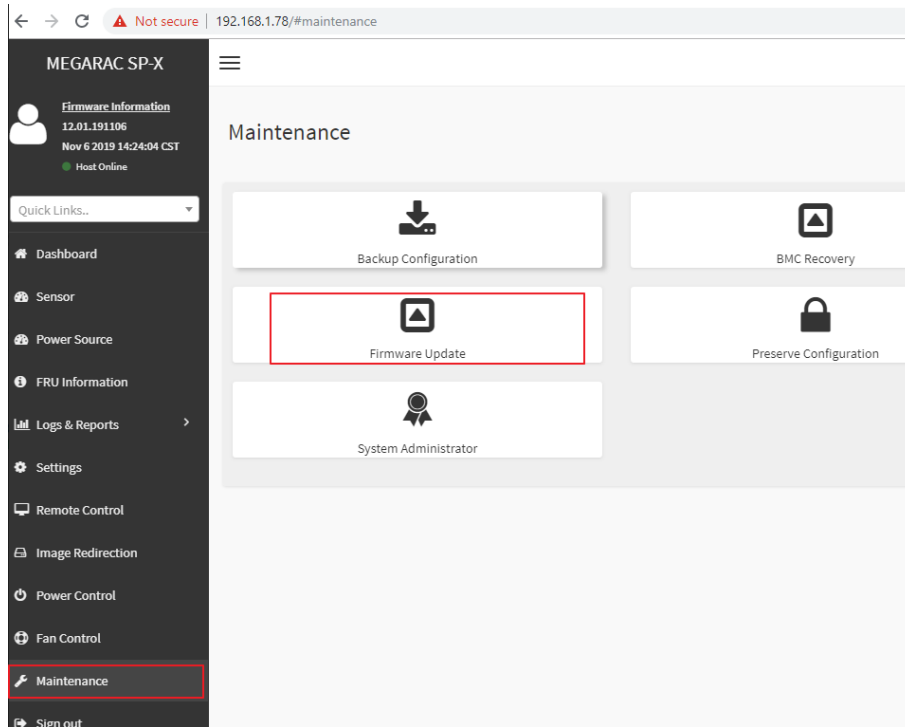
If you get a message that says “Your connection is not private”, just skip it.



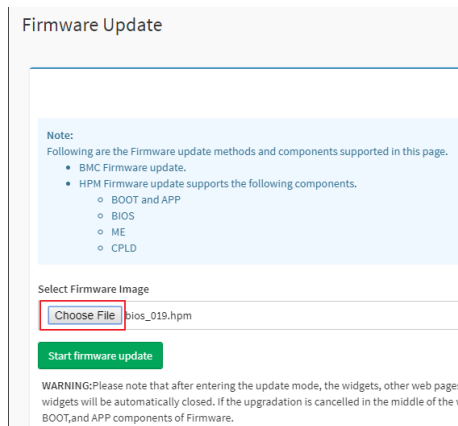
Note: BMC IP address can be configured at BIOS menu.



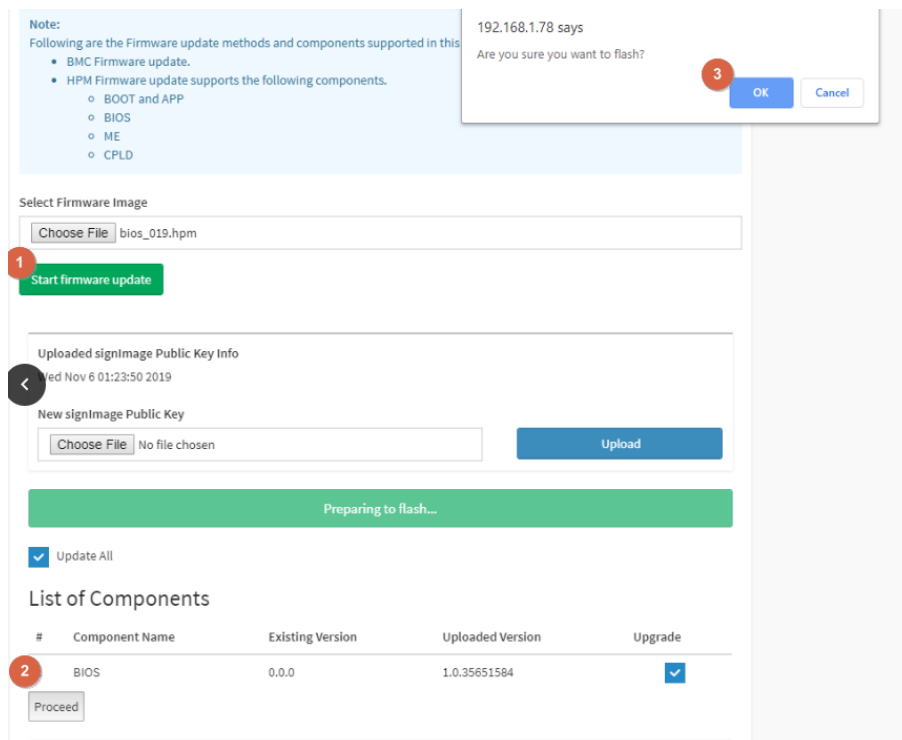
2. Click the **Maintenance** tab, then **Firmware Update**.



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



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



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



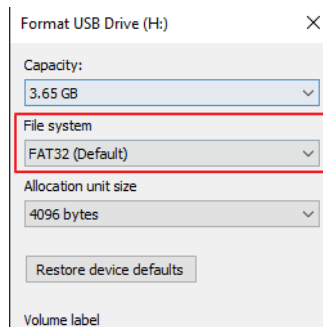
6. Server will reset after few seconds, refer 1.1.1 step9 to check the BIOS and SPS version.

## 2. BIOS

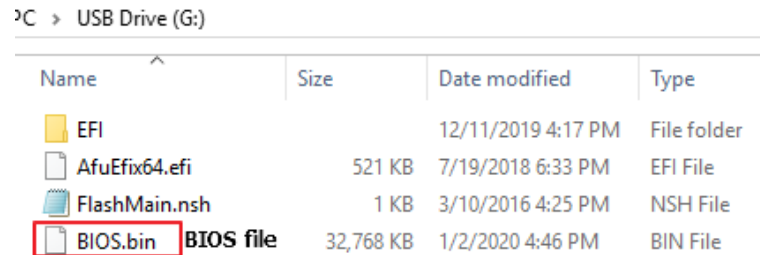
Update Method	OS	Tool
Local Update	UEFI environment	AfuEfix64.efi
	Windows PE environment	AFUWINx64.EXE

### 2.1 BIOS update in UEFI environment

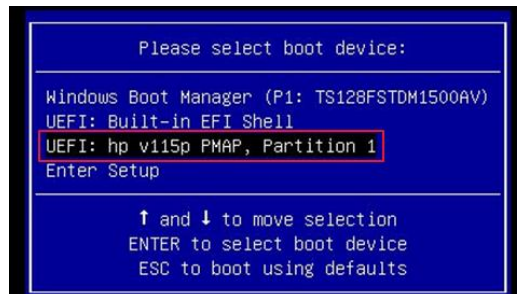
1. Format a USB flash drive to FAT32.



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



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



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

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

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

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

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

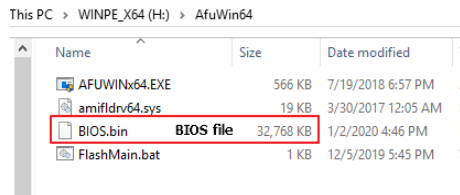
```
WARNING!!
DO NOT turn off the system power,
if the BIOS update process has not been finished yet.
<null string>
-----+-----
|              AMI Firmware Update Utility v5.11.01.1744              |
|              Copyright (C)2018 American Megatrends Inc. All Rights Reserved.              |
|-----+-----|
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
Erasing Main Block ..... done
Updating Main Block ..... done
Verifying Main Block ..... done
Erasing NVRAM Block ..... done
Updating NVRAM Block ..... done
Verifying NVRAM Block ..... done
Process completed.
FS0:\> _
```

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

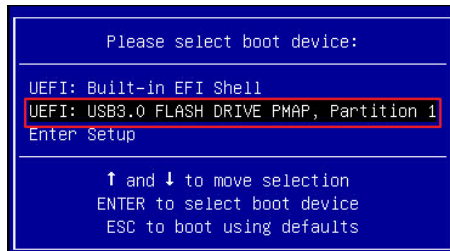
```
Aptio Setup Utility - Copyright (C) 2020 American
Main Advanced Server Mgmt Security Boot Save & Exit
BIOS Information
BIOS Vendor American Megatrends
Core Version 5.14
Compliance UEFI 2.7; PI 1.6
Project Version 0ACLA 0.45 x64
Build Date and Time 09/09/2020 14:30:17
Access Level Administrator
BIOS 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.

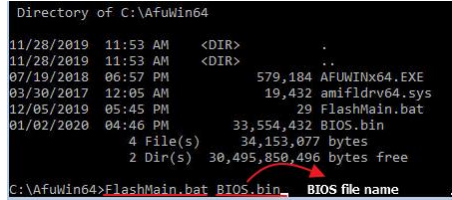


2. Power on Server. When you hear BIOS ready beep, press **F11** to enter boot menu and select the WinPE disk.

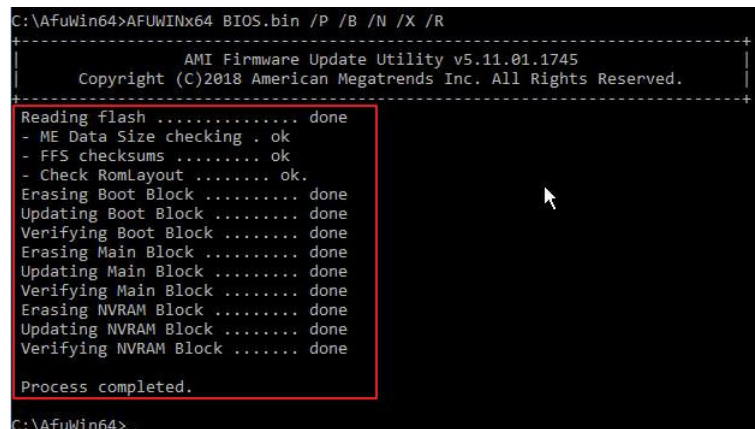


3. Switch to BIOS folder and run the command.

**FlashMain.bat [BIOS file name]**



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





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

```
Aptio Setup Utility - Copyright (C) 2020 American
Main Advanced Server Mgmt Security Boot Save & Exit
BIOS Information
BIOS Vendor                American Megatrends
Core Version                5.14
Compliance                 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
```

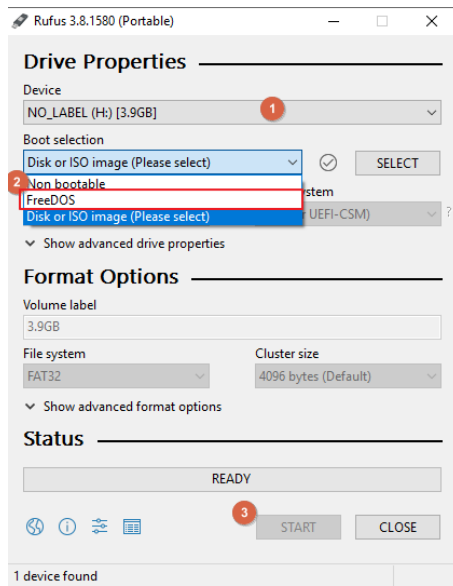
### 3. BMC

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

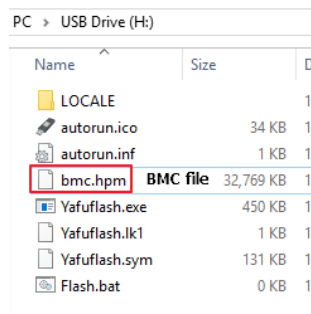
Please refer readme for tool detail information.

#### 3.1 BMC update in DOS environment

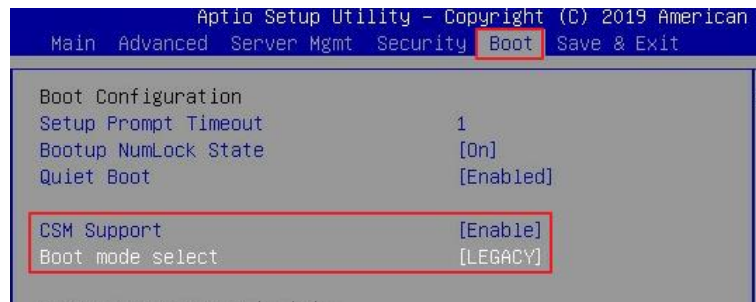
1. Download **Rufus** to create a DOS USB drive, <https://rufus.ie/>.



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]**.



- 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.

```

Directory of C:\
LOCALE          <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)      34,183,838 bytes
1 dir(s)       3,702 Mega bytes free
C:\>flash.bat bmc.hpm

```

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

```
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
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 [osimgel] 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 [lmedial] 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:\>
```

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

```
C:\>chkver.bat
C:\>Yafu.exe -kcs -mi
INFO: Yafu INI Configuration File not found... Default option
ed...

-----
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0)
-----
(C)Copyright 2017, American Megatrends Inc.
-----
Firmware Details
-----
Image Version
ModuleName Description Version
1.ast2500e 12.1.191112
C:\>
```

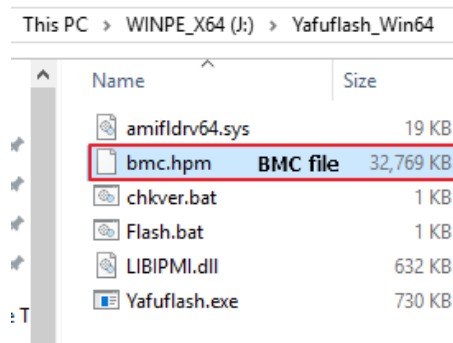
8. Reboot to BIOS and restore the **CSM support** and **Boot mode select** settings.



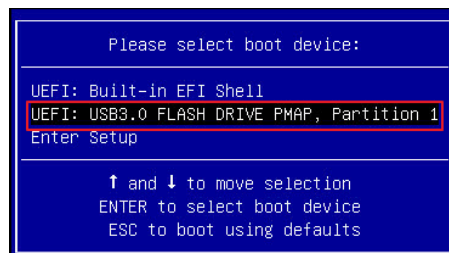
Save changes and exit.

### 3.2 BMC update in WinPE environment

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



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



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

#### Flash.bat [BMC file]

```

12/06/2019 11:51 AM <DIR> .
12/06/2019 11:51 AM <DIR> ..
11/19/2019 05:52 PM      19,432 amifldr64.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 bytes
        2 Dir(s)    30,669,848,576 bytes free

C:\Yafuflash_Win64>Flash.bat bmc.hpm
    
```

Please wait. This may take few minutes.

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

```
*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Uploading Firmware Image : 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 [vmm] 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:\Yafuflash_Win64>
```

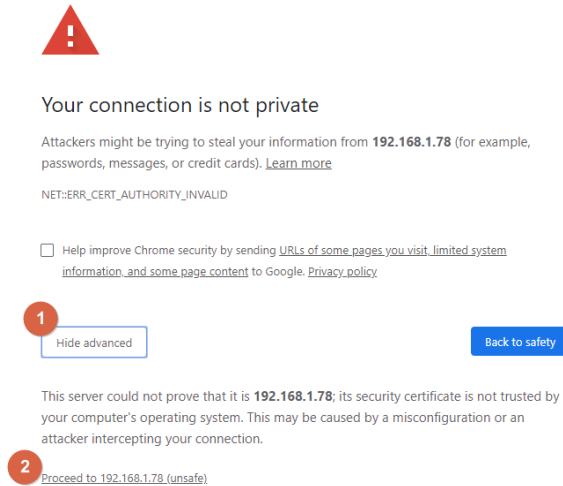
5. After BMC reset, run **chkver.bat** to check BMC firmware version.

```
C:\Yafuflash_Win64>chkver.bat
C:\Yafuflash_Win64>Yafuflash.exe -kcs -mi
INFO: Yafu INI Configuration File not found... Default optio
-----
YAFUFlash - Firmware Upgrdae Utility (Version 6.14.0.0)
-----
(C)Copyright 2017, American Megatrends Inc.
=====
Firmware Details
=====
      Image Version
ModuleName  Description  Version
1.ast2500e
C:\Yafuflash_Win64>
```

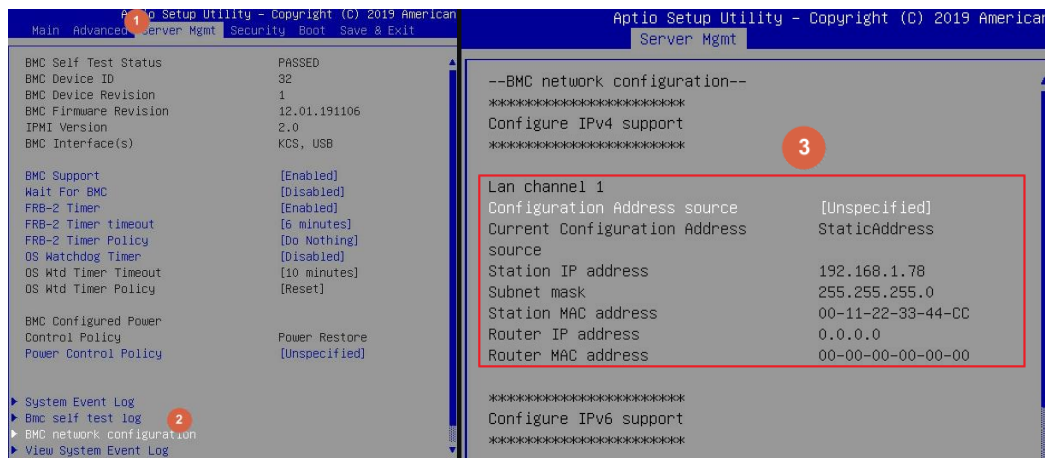
### 3.3 BMC update using Web UI

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

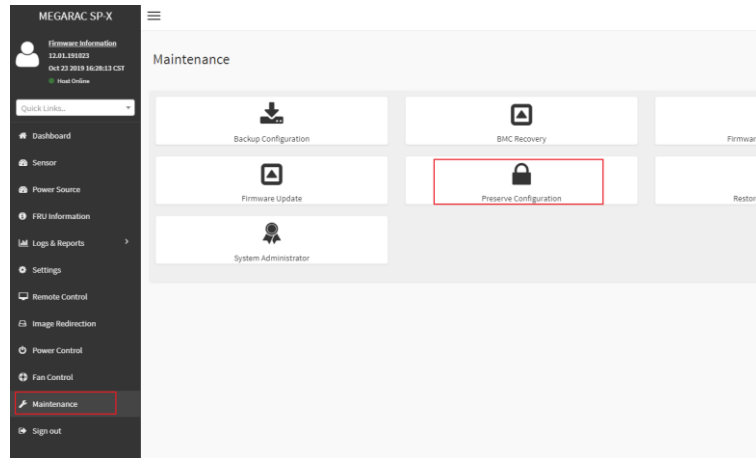
If you get a message that says “Your connection is not private”, just skip it.



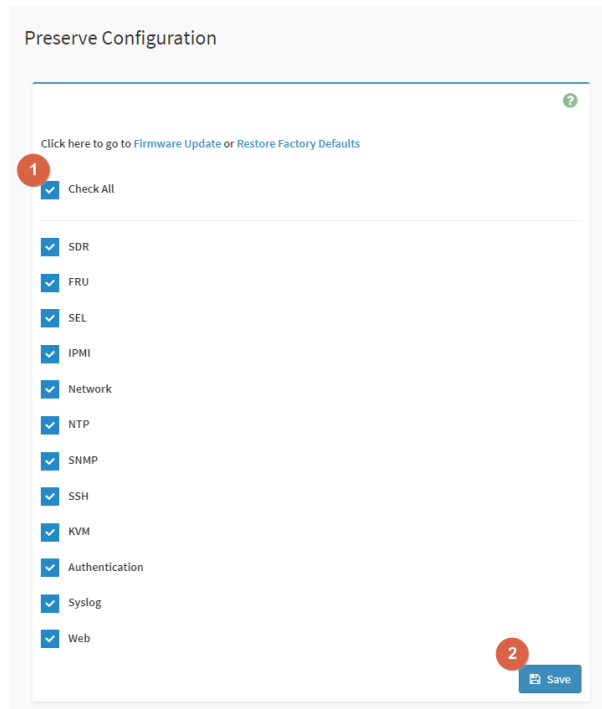
Note: BMC IP address can be configured at BIOS menu.



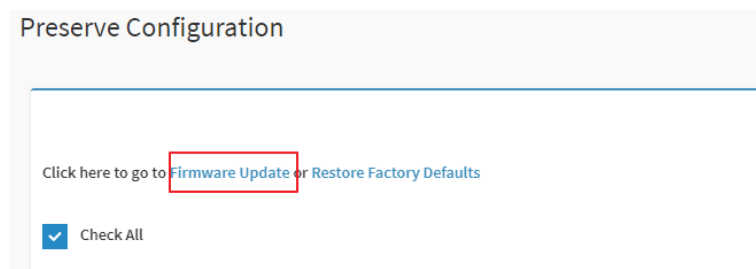
2. Click the **Maintenance** tab, then **Preserve Configuration**.



**Check all and Save.**

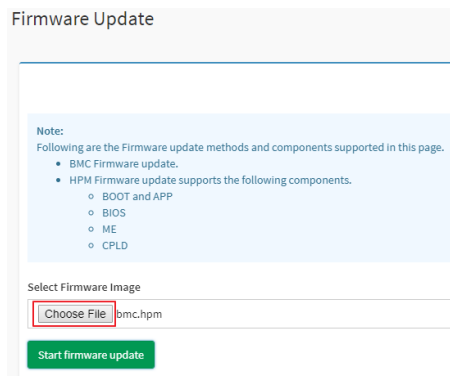


3. Click the link to go to **Firmware Update**.

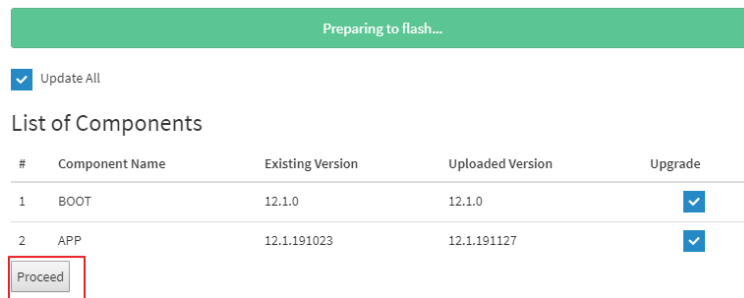




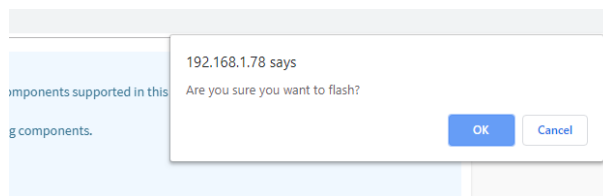
4. Choose File to select BMC file.



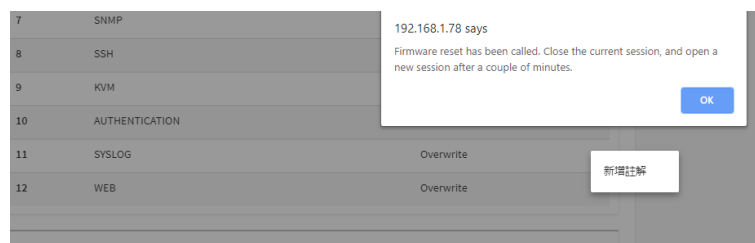
5. Click the **Start firmware update** button, then scroll down and click **Proceed**.



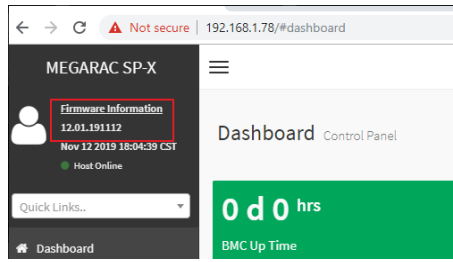
The message appears, “Are you sure you want to flash?”. Click **OK**.



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

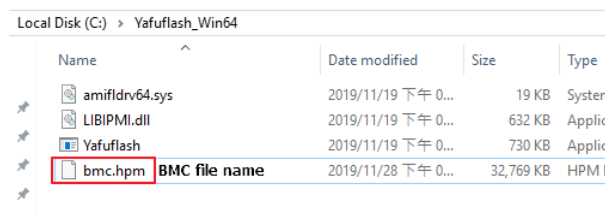


7. Reboot the server and then login to check the BMC firmware version.



### 3.4 BMC update using IPMI tool

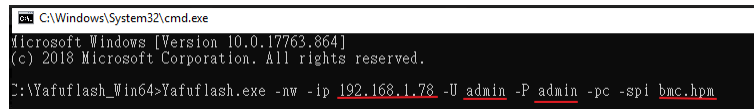
1. Save BMC file to Yafuflash folder.



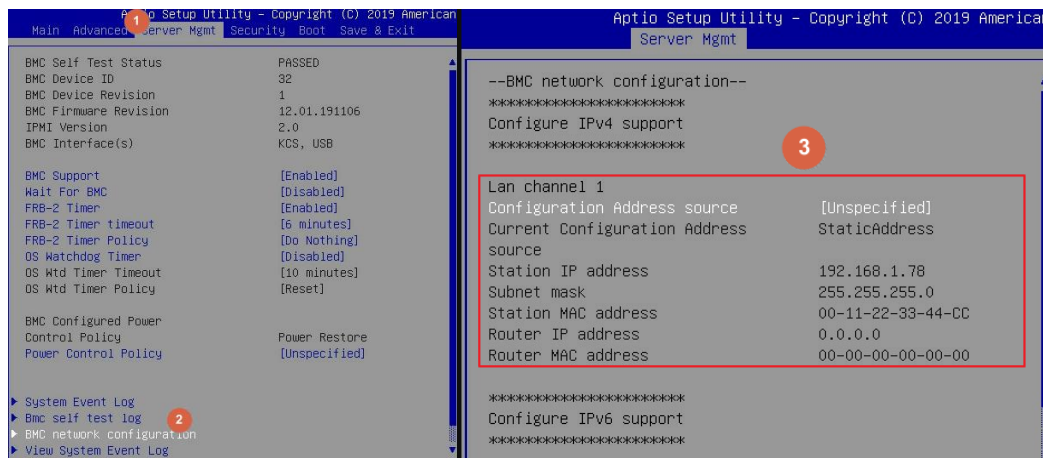
2. Open Command Prompt (admin) and change directory to Yafuflash tool folder.

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.

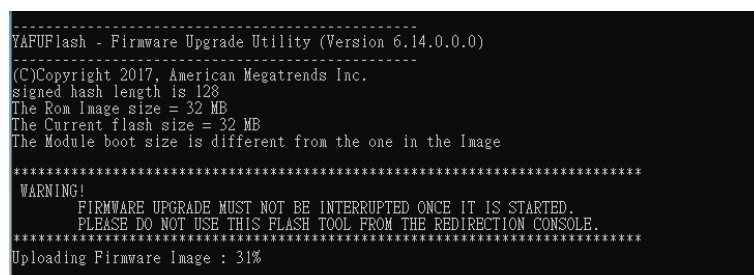


Note: BMC IP address can be configured at BIOS menu.



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

The update process will start.



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

```
C:\Windows\System32\cmd.exe
*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
PLEASE DO NOT USE THIS FLASH TOOL FROM THE REDIRECTION CONSOLE.
*****
Uploading Firmware Image : 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.....
```

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 192.168.1.78 -U admin -P admin -mi
INFO: Yafu INI Configuration File not found... Default options will not be applied...

Creating IPMI session via network with address 192.168.1.78...Done

-----
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
-----
(C)Copyright 2017, American Megatrends Inc.

=====
Firmware Details
=====
      Image Version
ModuleName  Description  Version
-----
l.ast2500e  12.1.191112
```

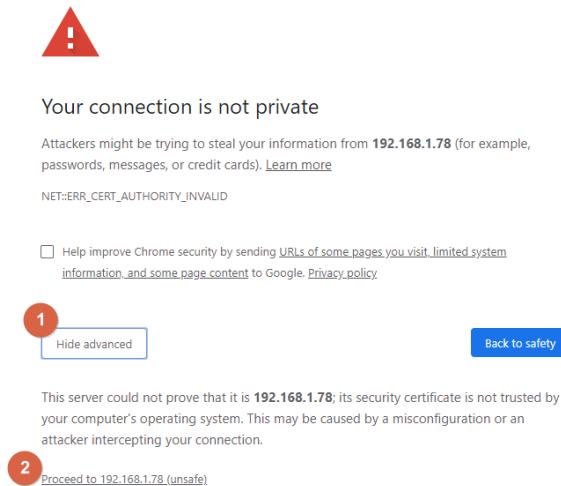
## 4. CPLD

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

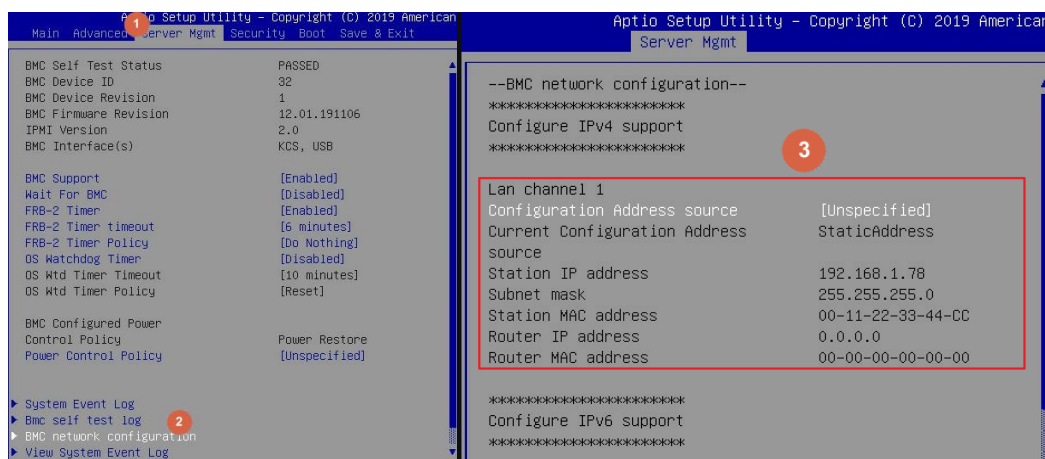
### 4.1 BMC update in DOS environment

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

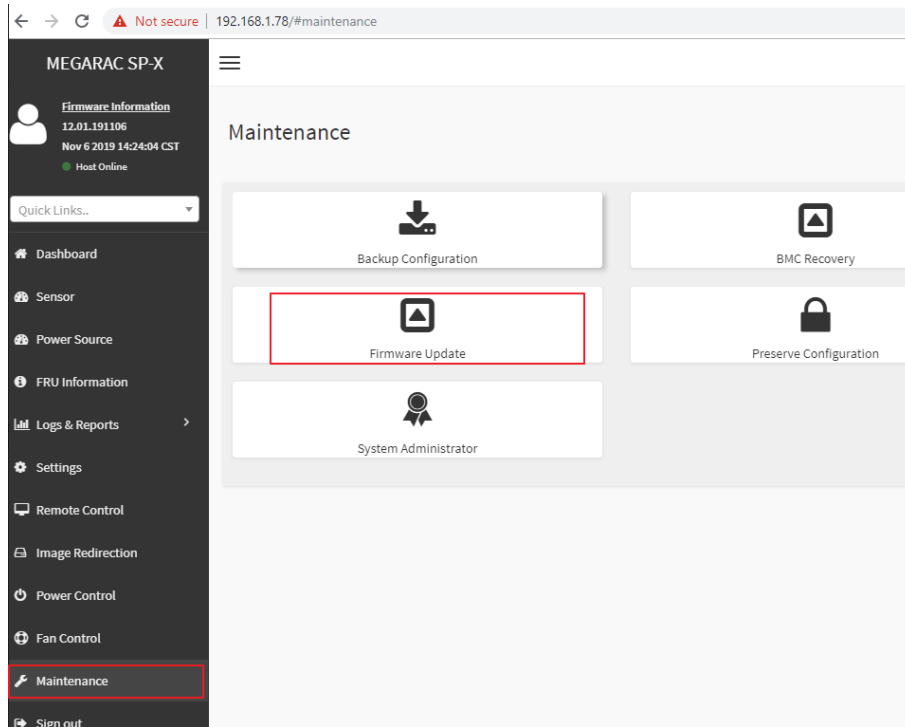
If you get a message that says **“Your connection is not private”**, just skip it.



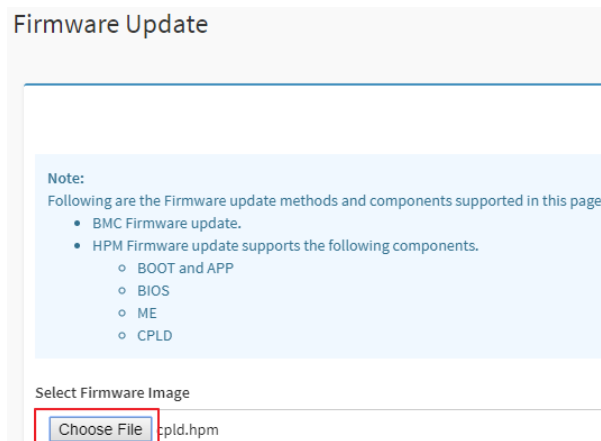
Note: BMC IP address can be configured at BIOS menu.



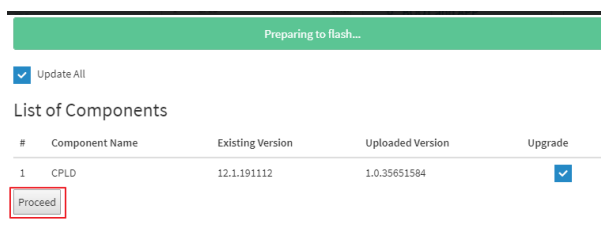
2. Click the **Maintenance** tab, then **Firmware Update**.



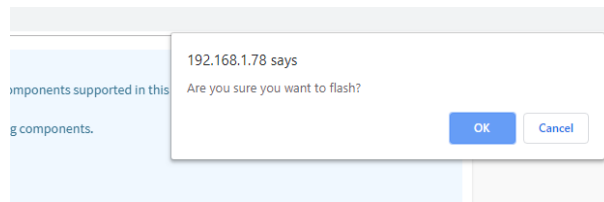
3. Choose **File** to select CPLD file.



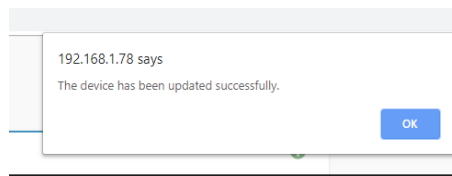
4. Click the **Start firmware update** button, then scroll down and click **Proceed**.



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



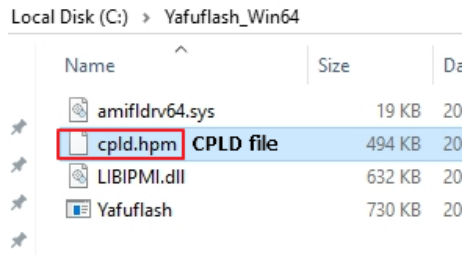
5. The message appears, "The device has been updated successfully". Click **OK**.



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

## 4.2 CPLD update using IPMI tool

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



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.

```
C:\Yafuflash_Win64>Yafuflash.exe -nw -ip 192.168.1.78 -U admin -P admin -d 4 cpld.hpm
INFO: Yafu INI Configuration File not found... Default options will not be applied...

Creating IPMI session via network with address 192.168.1.78...Done

-----
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
-----
(C)Copyright 2017, American Megatrends Inc.
signed hash length is 128
Beginning CPLD Update...
Please type (Y/y) to Update or (N/n) to Cancel
Enter your Option : Y
Uploading Image : 100%... done
Flashing Firmware Image : 100%... done
```

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

```
C:\Yafuflash_Win64>Yafuflash.exe -nw -ip 192.168.1.78 -U admin -P admin -d 4 cpld.hpm
INFO: Yafu INI Configuration File not found... Default options will not be applied...

Creating IPMI session via network with address 192.168.1.78...Done

-----
YAFUFlash - Firmware Upgrade Utility (Version 6.14.0.0.0)
-----
(C)Copyright 2017, American Megatrends Inc.
signed hash length is 128
Beginning CPLD Update...
Please type (Y/y) to Update or (N/n) to Cancel
Enter your Option : Y
Uploading Image : 100%... done
Flashing Firmware Image : 100%... done

C:\Yafuflash_Win64>
```



## 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																									
<b>Set fan mode</b>	0x30	0x01	[Mode] 0 = standard mode 1 = full mode 2 = optimal mode 3 = manual mode																									
			<table border="1"> <caption>Duty Cycle Data</caption> <thead> <tr> <th>Temperature (°C)</th> <th>STANDARD PWM (%)</th> <th>OPTIMAL PWM (%)</th> <th>FULL PWM (%)</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>40</td> <td>50</td> <td>100</td> </tr> <tr> <td>35</td> <td>40</td> <td>50</td> <td>100</td> </tr> <tr> <td>45</td> <td>50</td> <td>60</td> <td>100</td> </tr> <tr> <td>75</td> <td>90</td> <td>80</td> <td>100</td> </tr> <tr> <td>85</td> <td>100</td> <td>100</td> <td>100</td> </tr> <tr> <td>100</td> <td>100</td> <td>100</td> <td>100</td> </tr> </tbody> </table>	Temperature (°C)	STANDARD PWM (%)	OPTIMAL PWM (%)	FULL PWM (%)	0	40	50	100	35	40	50	100	45	50	60	100	75	90	80	100	85	100	100	100	100
Temperature (°C)	STANDARD PWM (%)	OPTIMAL PWM (%)	FULL PWM (%)																									
0	40	50	100																									
35	40	50	100																									
45	50	60	100																									
75	90	80	100																									
85	100	100	100																									
100	100	100	100																									

## HPM-621DE User's Manual

<b>Get fan mode</b>	0x30	0x30	<p>The response data is the fan mode.</p> <p>0 = standard mode            1 = full mode            2 = optimal mode            3 = manual mode</p>
<b>Set fan PWM</b>	0x30	0x35	<p>[Fan] [PWM]</p> <p><b>Fan:</b></p> <p>0 = CPU1_FAN1            1 = CPU2_FAN1            2 = SYS_FAN1            3 = SYS_FAN2            4 = SYS_FAN3</p> <p><b>PWM:</b></p> <p>The PWM duty cycle range should be 0x1E to 0x64(30%~100%).</p>
<b>Get fan PWM</b>	0x30	0x36	<p>The response data represent each fan PWM.</p> <p>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</p>

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
respData[len=1]: 00
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

Step 3. Set fan mode to manual mode

```
C:\ipmiutil-3.1.5-win32>ipmiutil cmd 00 20 c0 1 3
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
respData[len=1]: 03
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

Step 4. Set fan PWM

```
C:\ipmiutil-3.1.5-win32>ipmiutil cmd 00 20 c0 35 4 20
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
respData[len=1]: 00
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

Step 5. Get fan PWM

```
C:\ipmiutil-3.1.5-win32>ipmiutil cmd 00 20 c0 36
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
respData[len=8]: 64 64 28 28 20 10 10 10
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

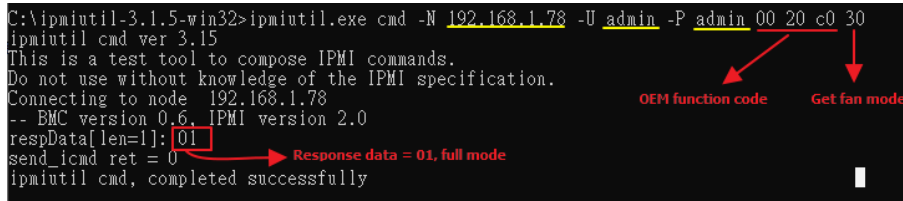
Remotely set PWM of CPU1\_FAN1 to 0x10 by “ipmiutil” in Windows OS.

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

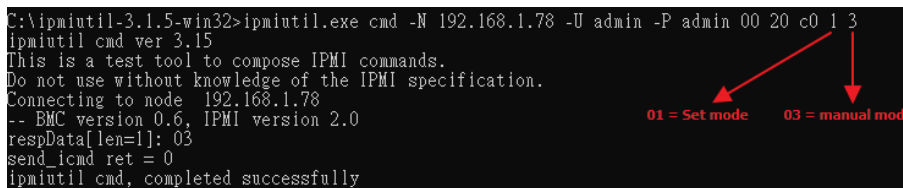
```
C:\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.78 -U admin -P admin 00 20 c0 30
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node 192.168.1.78
-- BMC version 0.6, IPMI version 2.0
respData[len=1]: 01
send_icmd ret = 0
ipmiutil cmd, completed successfully
```



Step 3. Set fan mode to manual mode

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0 1 3

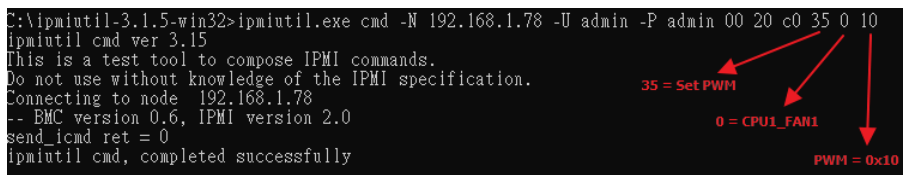
```
C:\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.78 -U admin -P admin 00 20 c0 1 3
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node 192.168.1.78
-- BMC version 0.6, IPMI version 2.0
respData[len=1]: 03
send_icmd ret = 0
ipmiutil cmd, completed successfully
```



Step 4. Set fan PWM

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

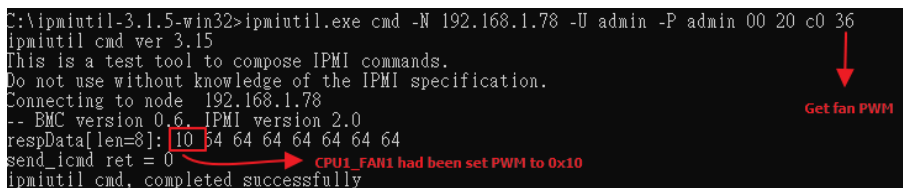
```
C:\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.78 -U admin -P admin 00 20 c0 35 0 10
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node 192.168.1.78
-- BMC version 0.6, IPMI version 2.0
send_icmd ret = 0
ipmiutil cmd, completed successfully
```



Step 5. Get fan PWM

ipmiutil.exe cmd -N [BMC IP] -U [user name] -P [user password] 00 20 c0 36

```
C:\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.78 -U admin -P admin 00 20 c0 36
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 192.168.1.78
-- BMC version 0.6, IPMI version 2.0
respData[len=8]: 10 64 64 64 64 64 64 64
send_icmd ret = 0
ipmiutil cmd, completed successfully
```

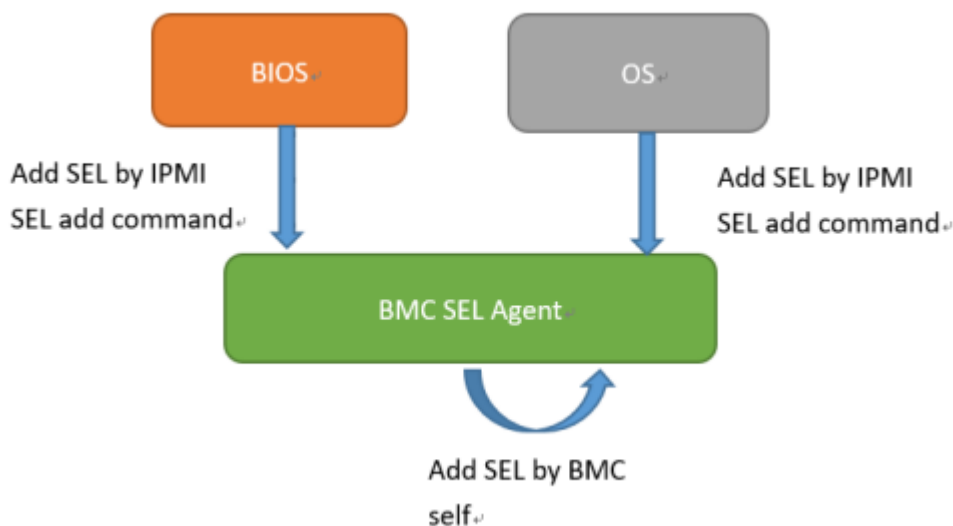


## APPENDIX-H SYSTEM EVENT LOG(SEL)

### System Event Log (SEL)

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

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



**SEL format**

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

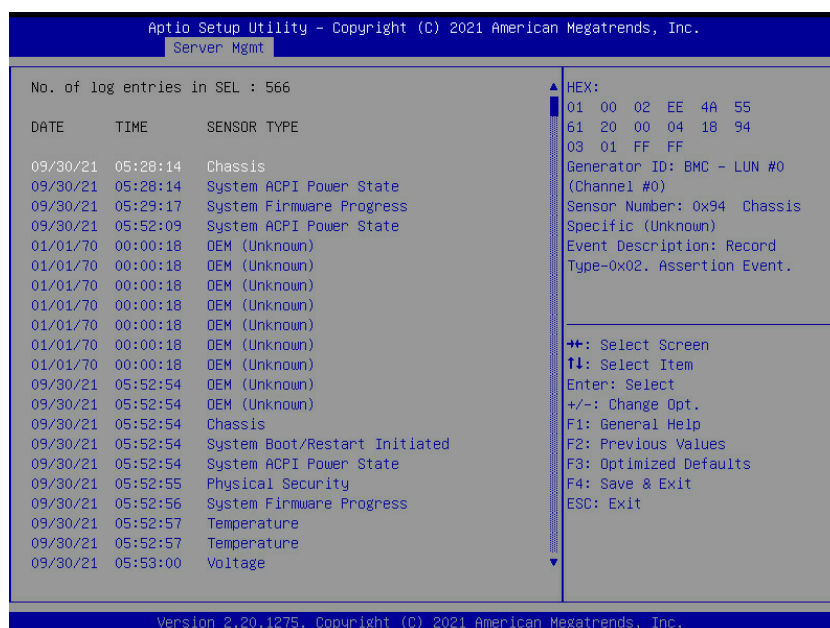
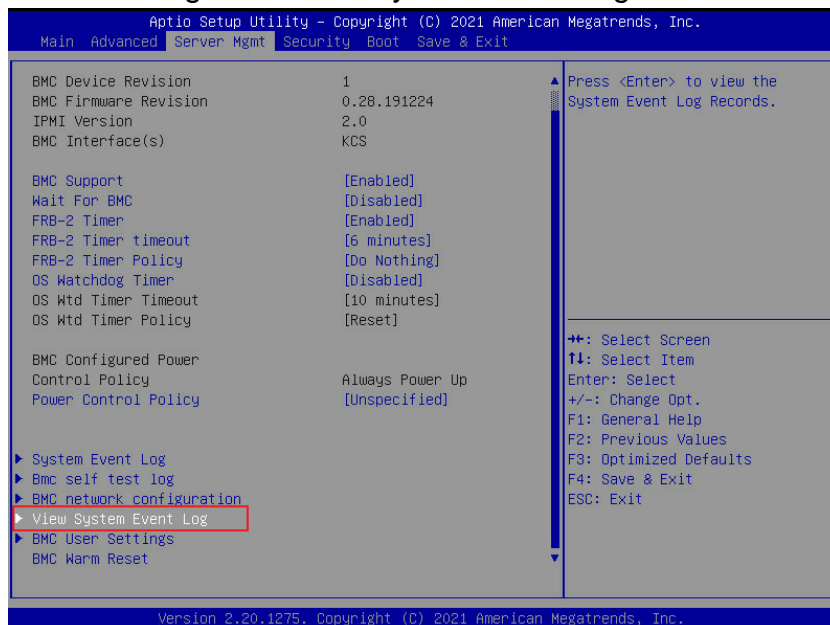
Byte	Field	Description
1, 2	Record ID (RID)	ID used for SEL record access.
3	Record Type (RT)	[7:0] – Record type 02h = System event record (default) C0h-DFh = OEM timestamped, bytes 8-16 OEM defined (see Table 3) E0h-FFh = OEM non-timestamped, bytes 4-16 OEM defined (see Table 4)
4-7	Timestamp (TS)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

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

### 3 ways to check SEL log

➤ BIOS setup

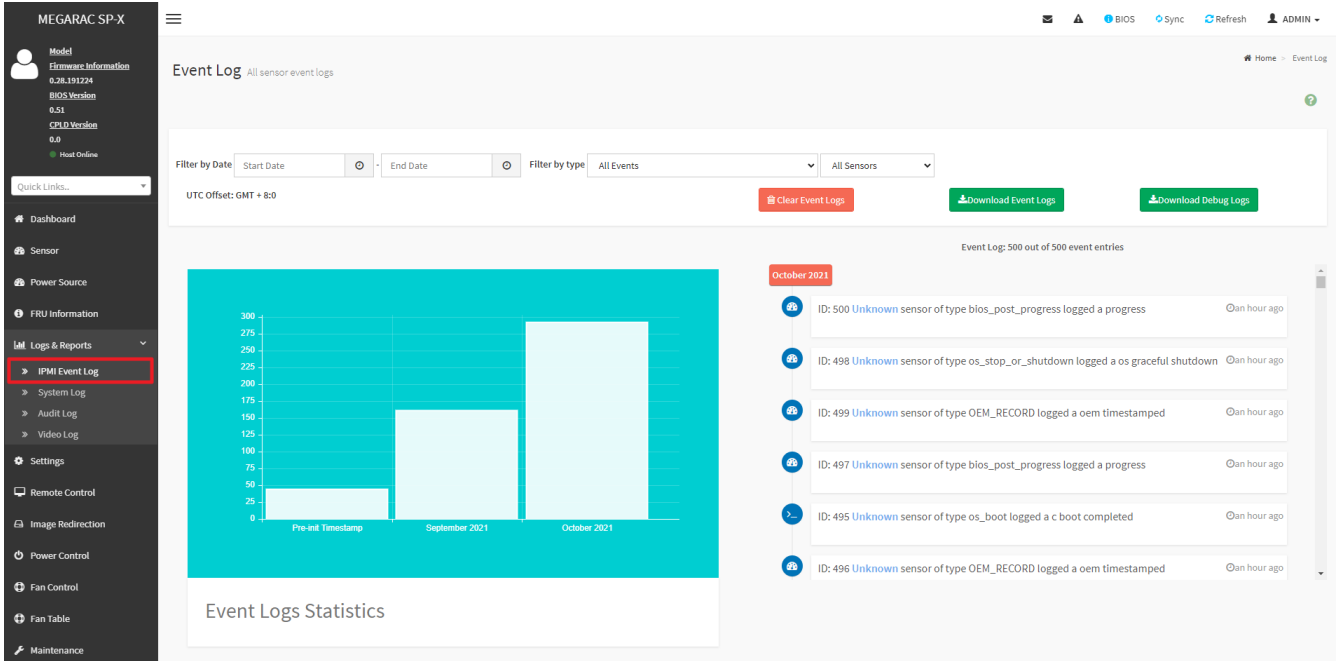
1. Power on and enter BIOS setup
2. Go to Server Mgmt => View System Event Log



# HPM-621DE User's Manual

## ➤ BMC Web

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



## ➤ IPMI tool

LAN (remote)

Linux:

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

Windows:

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

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



KCS(local)

Linux:

ipmitool sel elist

Windows:

ipmiutil.exe sel

**IPMI tools:**

ipmitool: <https://github.com/ipmitool/ipmitool>

ipmiutil: <http://ipmiutil.sourceforge.net/>

**Log Policy:**

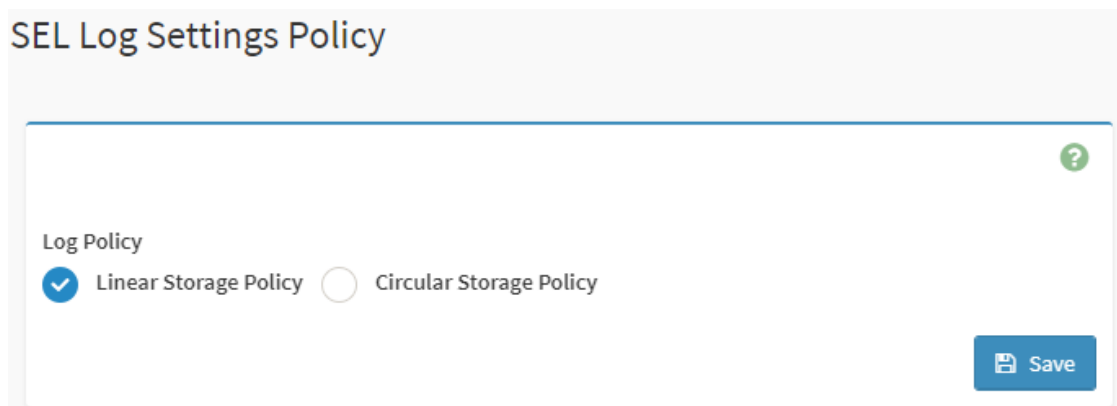
Linear Storage Policy

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

Circular Storage Policy

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

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



## Memory Correctable and Uncorrectable ECC Error

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

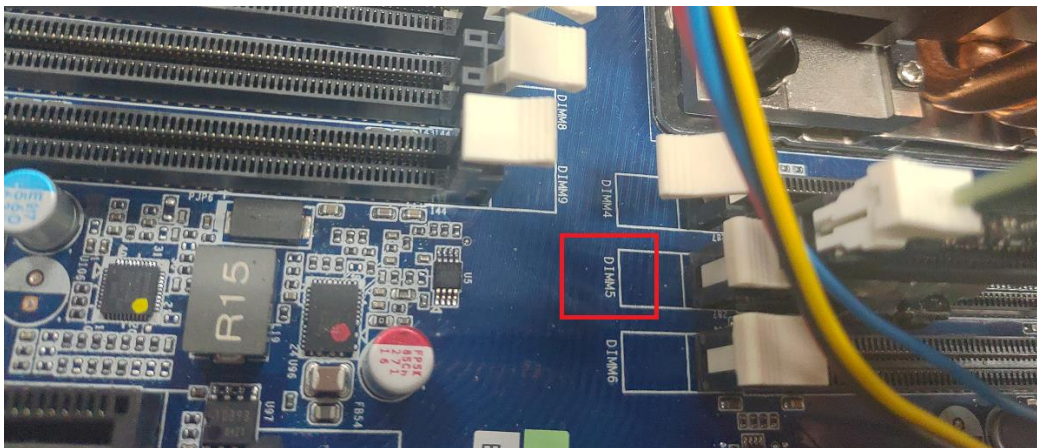
Correctable ECC errors can be detected and corrected if the chipset and DIMM support this functionality. This event in itself does not pose any direct problems because the ECC errors are still being corrected. Even though this event doesn't immediately lead to problems, it can indicate on the DIMM modules 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. Issue 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

```
root@klash-VirtualBox:~/home/klash/igt621/avalue_rr12# ipmitool -I lanplus -H 192.168.0.114 -U admin -P admin sel elist
1 06/08/2020 22:50:13 Fan SYS FAN1 Lower Critical going low Asserted Reading 0 < Threshold 800 RPM
2 06/08/2020 22:50:13 Fan SYS FAN2 Lower Critical going low Asserted Reading 0 < Threshold 800 RPM
3 06/08/2020 22:50:13 Fan SYS FAN3 Lower Critical going low Asserted Reading 0 < Threshold 500 RPM
4 06/08/2020 22:50:14 Physical Security ChassisIntrusion | General Chassis intrusion | Asserted
5 06/08/2020 22:54:14 Memory DIMM5 | Correctable ECC logging limit reached | Asserted
6 06/08/2020 22:55:00
```



### Logs & Reports >>IPMI Event Log

 ID: 11 DIMM5 sensor of type memory logged a correctable ecc logging limit reached 🕒 in 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.

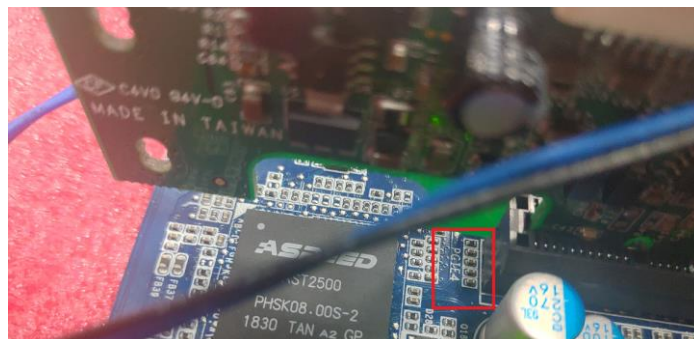
PCIe location from SEL:

1. Issue 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

1	06/08/2020	22:50:13	Fan SYS FAN1	Lower Critical going low	Asserted	Reading 0 < Threshold 800 RPM
2	06/08/2020	22:50:13	Fan SYS FAN2	Lower Critical going low	Asserted	Reading 0 < Threshold 800 RPM
3	06/08/2020	22:50:13	Fan SYS FAN3	Lower Critical going low	Asserted	Reading 0 < Threshold 500 RPM
4	06/08/2020	22:50:14	Physical Security ChassisIntrusion	General Chassis intrusion	Asserted	
5	06/08/2020	22:54:14	Memory DIMMS	Correctable ECC logging limit reached	Asserted	
6	06/08/2020	22:56:09	Critical Interrupt PCIE SLOT4	Bus Fatal Error	Asserted	
7	06/08/2020	22:56:11	OS Stop/Shutdown	Run-time critical stop	Asserted	
8	06/08/2020	22:56:12	OEM record de	000137	012401000001	
9	06/08/2020	22:56:12	OEM record de	000137	020000000001	



Logs & Reports >>IPMI Event Log

×
ID: 69 [PCIE\\_SLOT4](#) sensor of type critical\_interrupt logged a bus fatal error

⌚ in 8 hours

## APPENDIX-I IPMI TO GET BIOS POST CODE

### OEM Message format

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

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

Where:

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

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

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

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

### Get BIOS code Commands

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

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

**Example:****Locally get BIOS code by “ipmitool” in Linux.**

```
ipmitool raw 0x32 0x73 0
```

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

The latest BIOS code is e3.

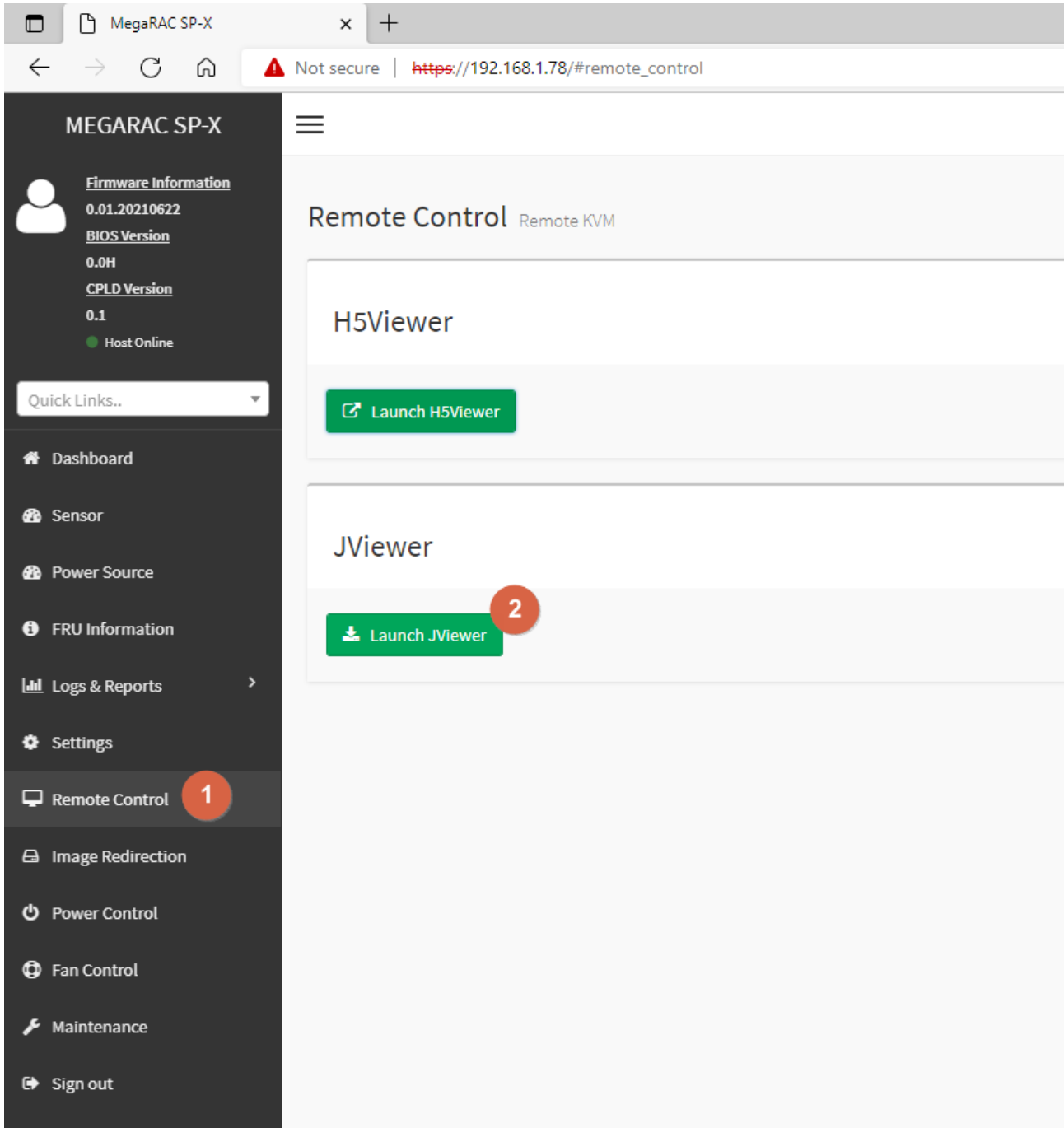
**Remotely get BIOS code by “ipmiutil” in windows:**

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

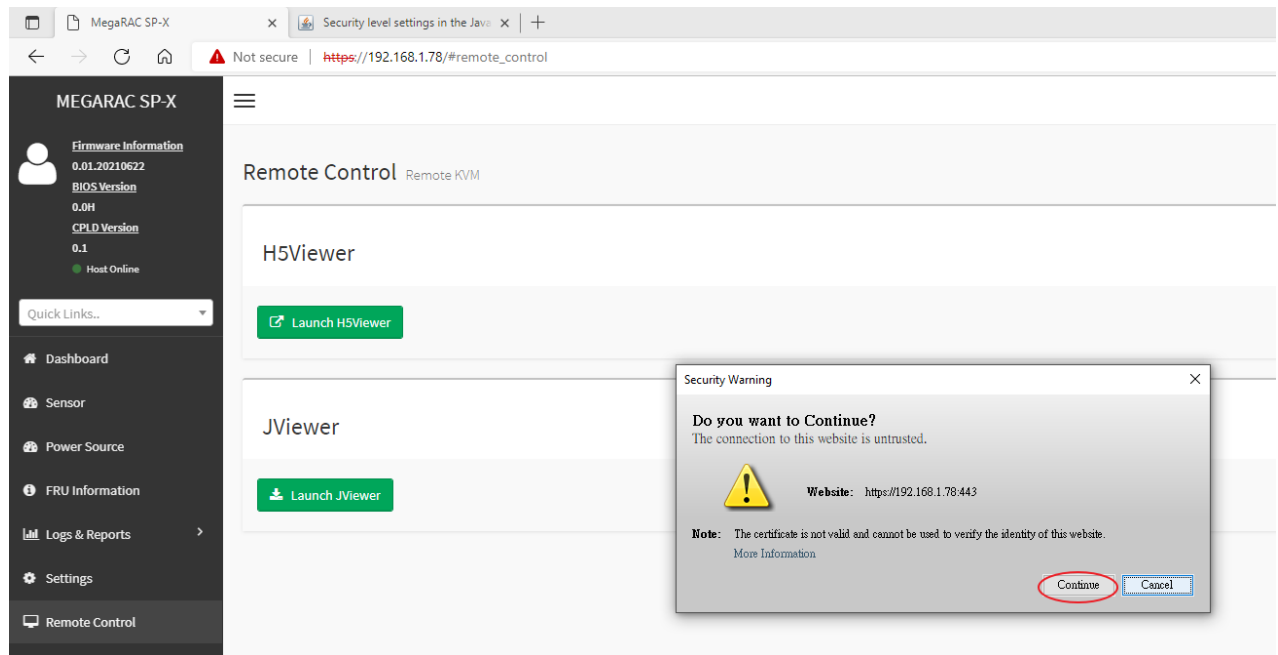
```
D:\Tools\BMC\ipmiutil-3.1.5-win32>ipmiutil.exe cmd -N 192.168.1.77 -U admin -P admin 00 20 C8 73 0
ipmiutil cmd ver 3.15
This is a test tool to compose IPMI commands.
Do not use without knowledge of the IPMI specification.
Connecting to node 192.168.1.77
-- BMC version 0.5, IPMI version 2.0
respData[len=160]: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

## APPENDIX-J REMOTE CONTROL-JVIEWER

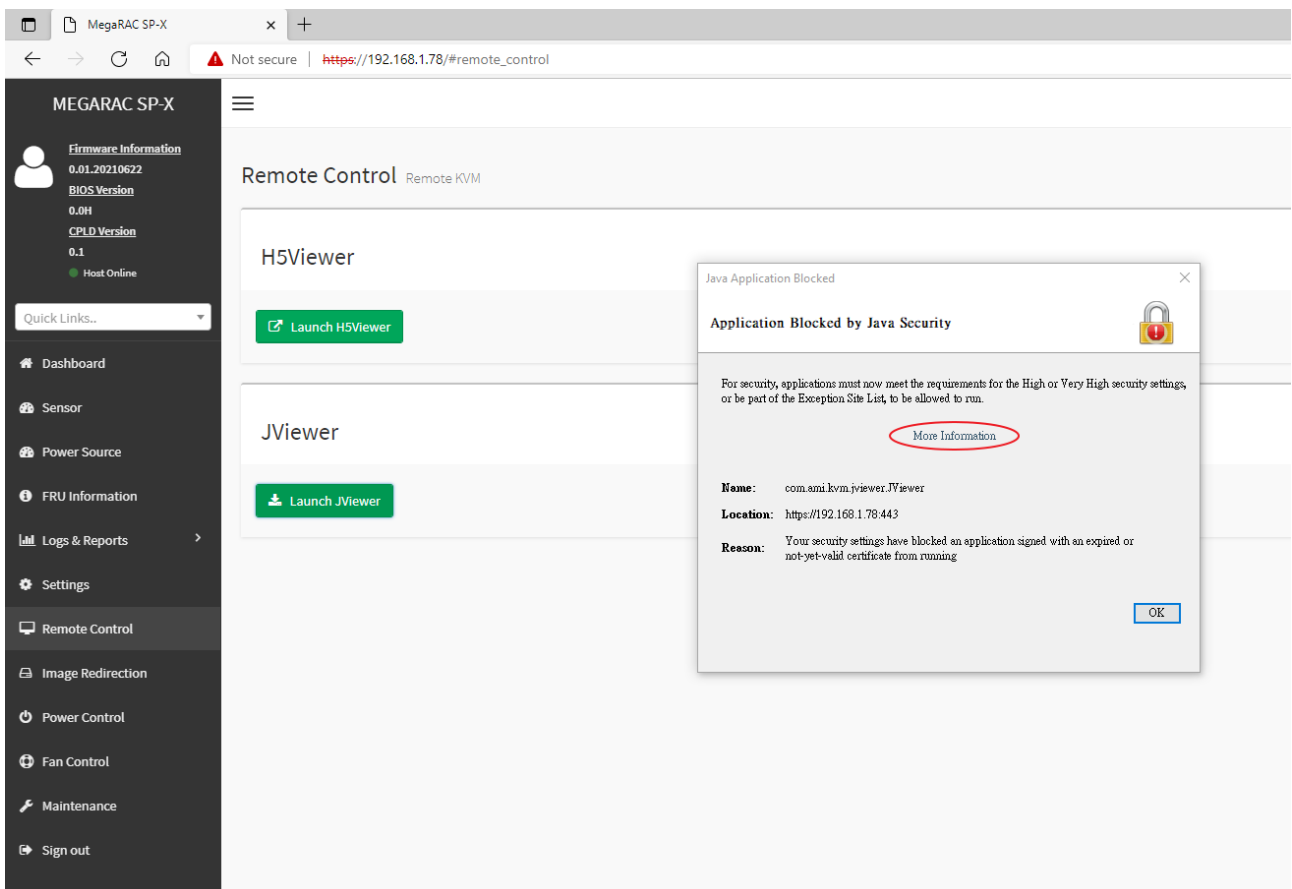
1. Select the “Remote Control” page and the click [Launch Jviewer]. The browser will start to download jviewer.jnlp.



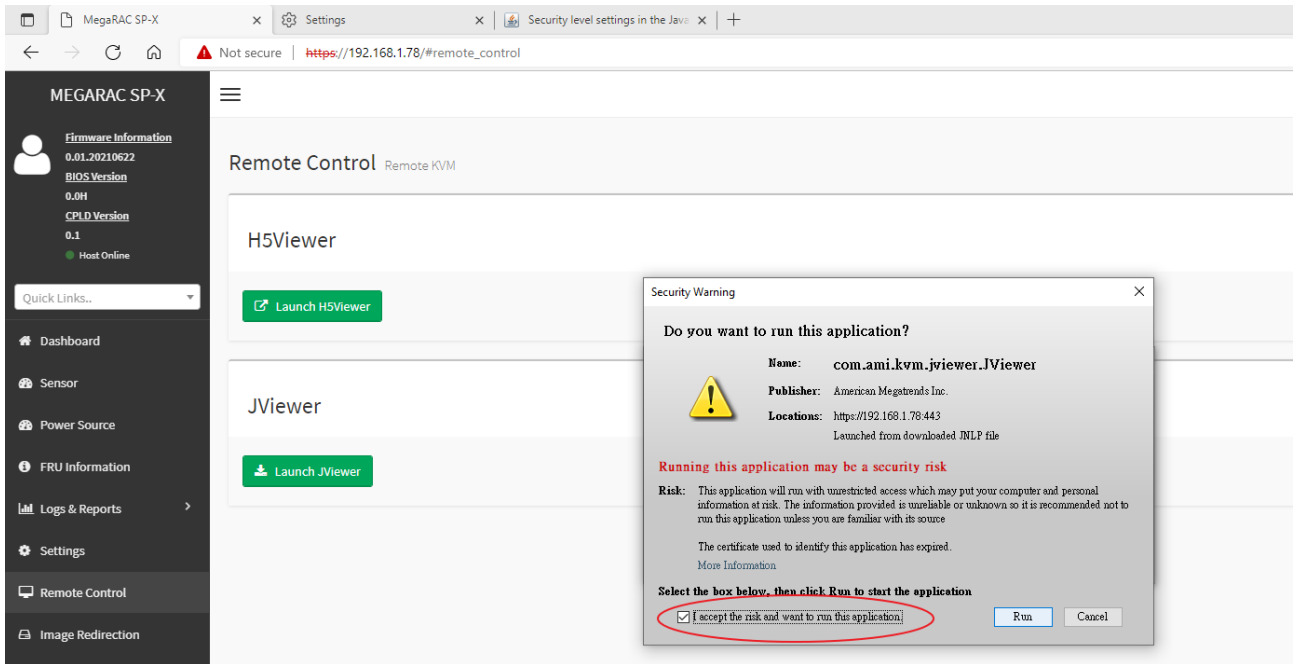
2. When the download completed, run jviewer.jnlp (notice: you need to install java as well.)



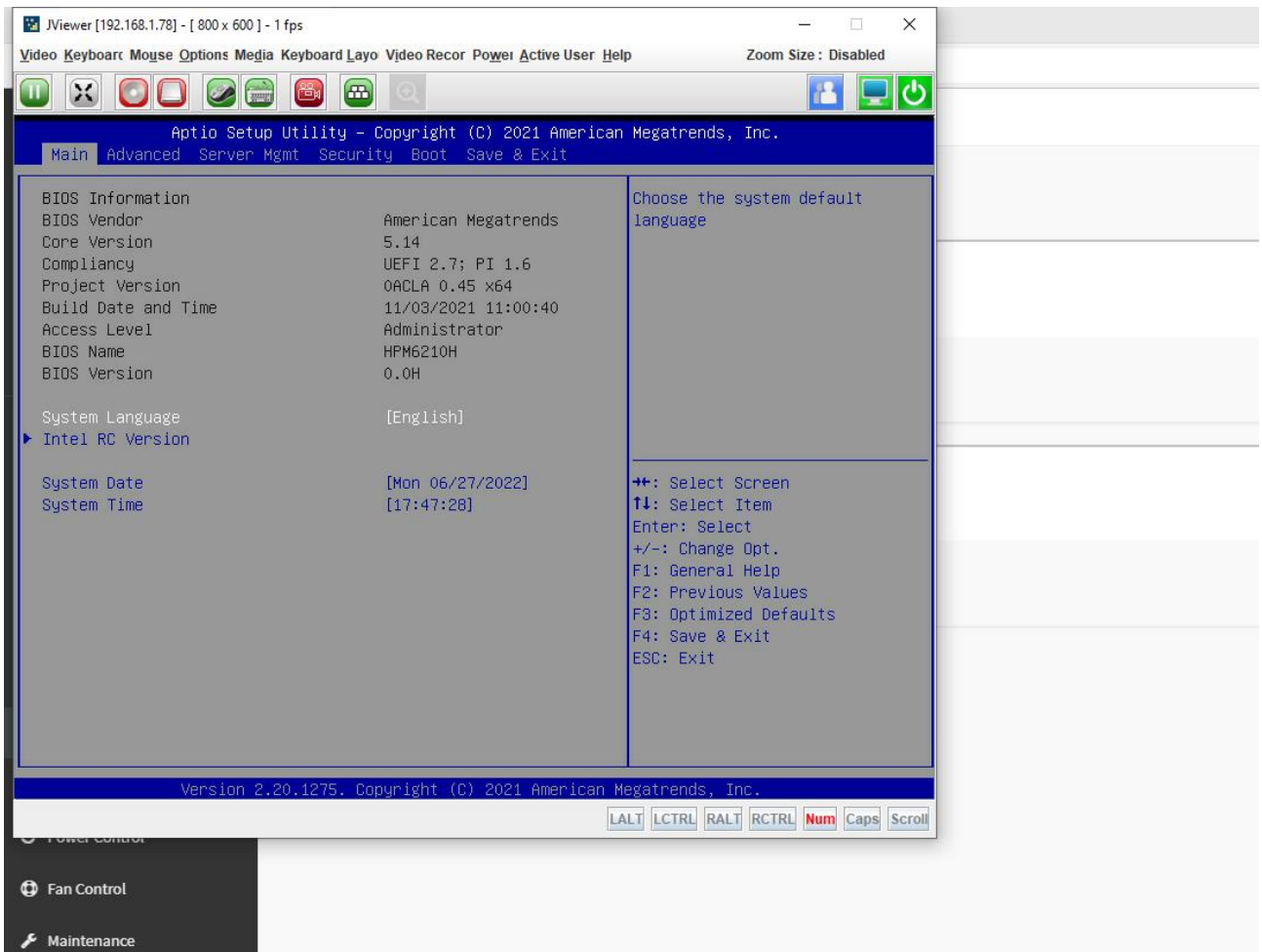
If the message shows up, please refer the java website to add the certificate.



### 3. Check the box to accept the risk.



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





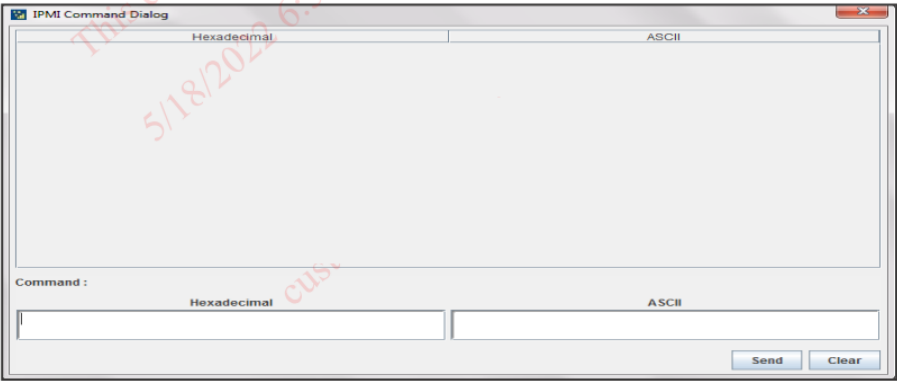
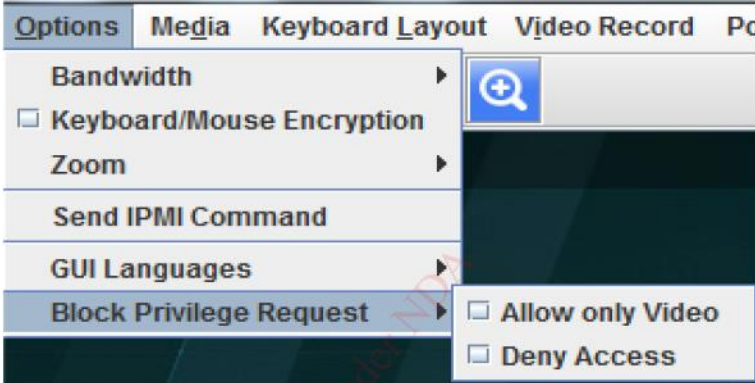
The Console Redirection menu bar consists of the following menu items.

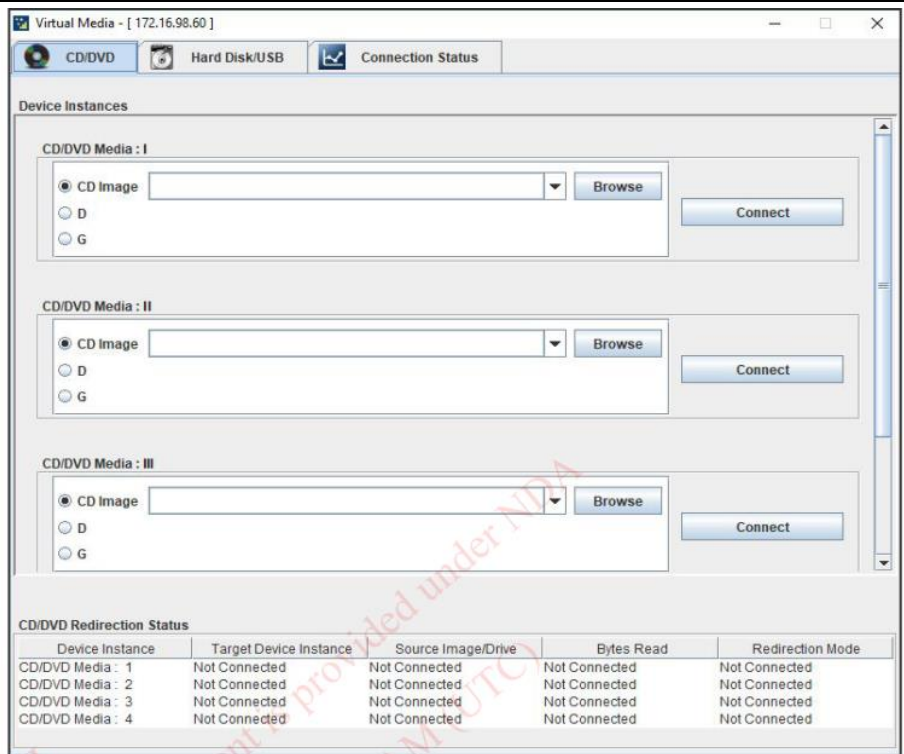
Menu item	Sub menu item	Detailed explanation
Video	<b>Pause redirection:</b>	This option is used for pausing Console Redirection.
	<b>Resume Redirection</b>	This option can be used to resume the Console Redirection when the session is paused.
	<b>Refresh Video:</b>	This option can be used to update the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

## HPM-621DE User's Manual

		<DEL> keys down simultaneously on the server that you redirecting.
	<b>Context menu</b>	This menu can be used to act as the context menu key, when in Console Redirection.
	<b>Hot Keys</b>	This Menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key evens are saved in the BMC.
	<b>Full Keyboard Support</b>	Enable this option to provide full keyboard support. This option is used to trigger the Ctrl and Alt key directly to host from the physical keyboard.
<b>Mouse</b>	<b>Show Cursor:</b>	This menu item can be used to show or hide the local mouse cursor on the remote client system.
	<b>Mouse Calibration</b>	<p>This menu item can be used only if the mouse mode is relative.</p> <p>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 cursor is part of the remote video screen. Both the cursors will be synchronized 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.</p>
	<b>Mouse Mode</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Absolute mouse mode:</b> The absolute position of the local mouse is sent to the server if this option is selected.</li> <li>• <b>Relative mouse mode:</b> The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.</li> <li>• <b>Other mouse mode:</b> 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.</li> </ul> <p><b>Note:</b> 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.</p> <p>Client cursor will be hidden always. If you want to enable, use <b>Alt + C</b> to access the menu.</p> <p>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</p>

		<p>directly impact in video rendering due to that client and host cursor can be viewed while moving the cursor.</p> <p>Hardware cursor will work only if aspeed video driver is installed in host.</p> <p>To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.</p>
<b>Options</b>	<b>Bandwidth (Except RAVS video driver)</b>	<p>The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following:</p> <p><b>Auto Detect</b> - This option is used to detect the network bandwidth usage of the BMC automatically.</p> <ul style="list-style-type: none"> <li>• 256 Kbps 256 Kbps</li> <li>• 512 Kbps 512 Kbps</li> <li>• 1 Mbps 1 Mbps</li> <li>• 10 Mbps 10 Mbps</li> </ul>
	<b>Keyboard/Mouse Encryption:</b>	<p>This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.</p>
	<b>Zoom</b>	<p>Note: This option is available only when you launch the Java Console .</p> <p><b>Zoom In</b> – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%.</p> <p><b>Zoom Out</b> – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%.</p> <p><b>Actual Size</b> - By default this option is selected By default this option is selected.</p> <p><b>Fit to Client Resolution</b> - 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.</p> <p><b>Fit to Host Resolution</b> - If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.</p> <p><b>Note:</b> This option can be configured from PRJ in MDS.</p>
	<b>Send IPMI Command</b>	<p>This option opens the IPMI Command dialog. Enter the raw IPMI command in Hexadecimal field as Hexadecimal value and click <b>Send</b>. The Response will be displayed as shown in the screenshot below.</p>

		
	<p><b>GUI Languages</b></p>	<p>Choose the desired GUI language.</p>
	<p><b>Block Privilege Request</b></p>	<p>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”.</p>  <p><b>Note:</b> This menu option is available only for Full permission session and partially privileged sessions will not have this option in the menu. Either of the options can only be selected. Both options cannot be selected together. To disable “Block Privilege Request“ none of the options should be selected in the menu.</p> <p>If “Allow only Video” is selected, then the slave session will be notified as “KVM Master Session blocked incoming request” and it will always receive “Video Only” (Partial Permission).</p> <p>If “Deny Access” is selected, then the slave session will be notified as “KVM Master Session blocked incoming request” and the incoming KVM session will be closed.</p>
<p><b>Media</b></p>	<p><b>Virtual Media Application</b></p>	<p>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.</p> <p>A sample screenshot of Virtual Media Application is given below.</p>



**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 will work like a child dialog of the JViewer.

**Note:**

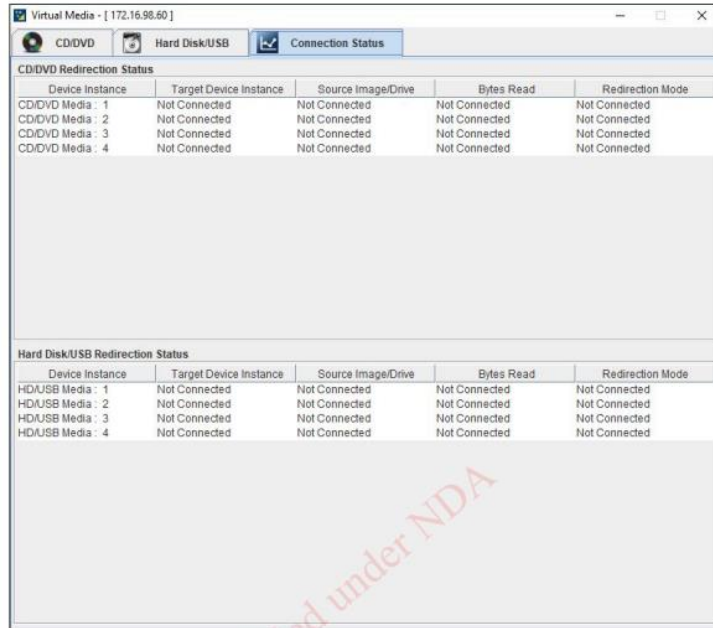
**AST SOC:-** Configured number of devices will be emulated in Windows /Linux Host.

**Macintosh OS X Clients:** The package XQuartz should be present in the Macintosh OS X client 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.

		<p><b>Hard disk/USB:</b> 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.</p> <p><b>Note:</b> For redirecting Hard disk drives, you should have administrator privilege (root user in the case of Linux clients).</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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 <b>all the media redirection client applications</b>.</p> <p>If the feature <b>Redirect Devices Always in READ and WRITE Mode</b> 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.</p> <p>If files with hidden attribute are visible in the file open dialog, then the file can be opened and redirected.</p> <p>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.</p> <p>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.</p> <p>SPX Stack Media redirection supports only Basic Hard disk Redirection.</p> <p><b>Connection Status:</b> This tab provides a collective view of the redirection status of various virtual media devices.</p> <p>The connection status tab is shown below.</p>
--	--	--

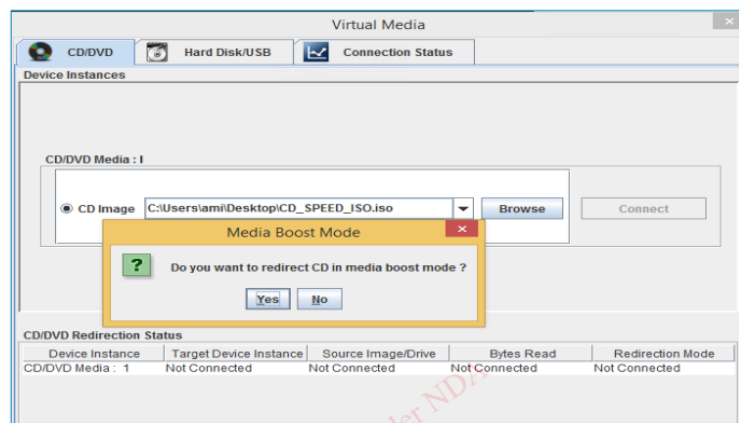


**Virtual Media Application - Connection Status**

**Note:** VMedia Privilege only restricts initiating/starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions. Which includes 'KVM Privilege only' sessions as well.


**Media Boost Mode**

Media boost mode is applicable only for one VMedia instance. This support is available only for CD. On starting CD redirecting via JViewer/VMAApp, a pop up with an option to use media boost mode will open. A sample screenshot is displayed below.



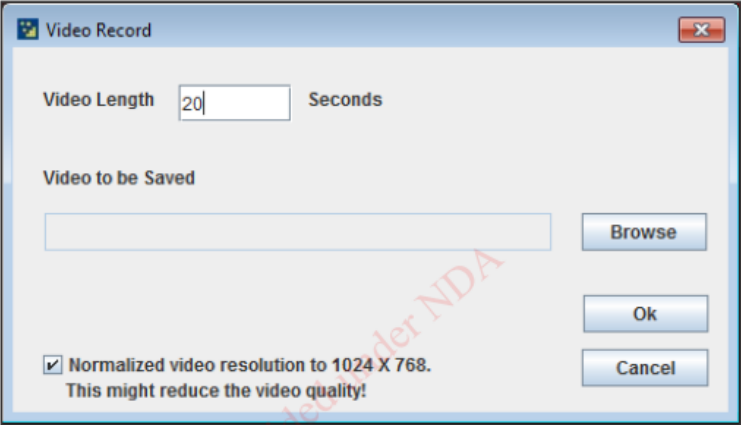
**Media Boost Mode**











If option 'yes' is selected and no other vmedia instance is redirected in media boost mode, redirection state will be updated as "Media Boost Mode". A sample screenshot is displayed below.

		 <p style="text-align: center;"><b>Media Boost Mode</b></p> <p><b>Note:</b> 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.</p> <p>If CD/DVD instance is started with media boost mode, the next CD/DVD instance will be started without any pop-up message.</p>
<p><b>Keyboard Layout</b></p>	<p><b>Auto Detect</b></p>	<p>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 languages differ, user can choose the host language layout in the menu and thereby can directly use the physical keyboard.</p>
	<p><b>Physical Keyboard</b></p>	<p>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.</p> <ul style="list-style-type: none"> <li>• 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 mapping to work properly. By default, Windows will be selected.</li> </ul> <p>List of Host Physical Keyboard languages supported in SPX JViewer.</p> <ol style="list-style-type: none"> <li>1. English –US</li> <li>2. English – UK</li> <li>3. French</li> <li>4. French (Belgium)</li> <li>5. German (Germany)</li> <li>6. German (Switzerland)</li> <li>7. Japanese</li> <li>8. Spanish</li> <li>9. Italian</li> <li>10. Danish</li> <li>11. Finnish</li> <li>12. Norwegian (Norway)</li> <li>13. Portuguese (Portugal)</li> </ol>



		<p>14. Swedish          15. Dutch (Netherland)          16. Dutch (Belgium)          17. Turkish – F          18. Turkish – Q</p>
	<p><b>Soft Keyboard :</b></p>	<p>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.</p> <p><b>Note:</b> Different Linux systems follow different keyboard layouts. So the softkeyboard displayed uses standard windows keyboard layout irrespective of the host OS.</p> <p>We have list of List of Soft Physical Keyboard languages supported in SPX JViewer.</p> <ol style="list-style-type: none"> <li>1. English –US</li> <li>2. English – UK</li> <li>3. Spanish</li> <li>4. French</li> <li>5. German (Germany)</li> <li>6. Italian</li> <li>7. Danish</li> <li>8. Finnish</li> <li>9. German (Switzerland)</li> <li>10. Norwegian (Norway)</li> <li>11. Portuguese (Portugal)</li> <li>12. Swedish</li> <li>13. Hebrew</li> <li>14. French (Belgium)</li> <li>15. Dutch (Netherland)</li> <li>16. Dutch(Belgium)</li> <li>17. Russian (Russia)</li> <li>18. Japanese (QWERTY)</li> <li>19. Japanese (Hiragana)</li> <li>20. Japanese (Katakana)</li> <li>21. Turkish – F</li> <li>22. Turkish – Q</li> </ol> <p>Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system.</p>

<b>Video Record</b>	<b>Start Record</b>	This option is to start recording the screen.
	<b>Stop Record</b>	This option is used to stop the recording.
	<b>Settings</b>	<p>To set the settings for video recording.</p> <p><b>Procedure</b></p> <p><b>Note:</b> Before you start recording, you have to enter the settings.</p> <ol style="list-style-type: none"> <li>Click <b>Video Record &gt; Settings</b> to open the settings page as shown in the screenshot below.</li> </ol> <div style="text-align: center;">  <p><b>Video Record Settings Page</b></p> </div> <ol style="list-style-type: none"> <li>Enter the <b>Video Length</b> in seconds.</li> <li><b>Browse</b> and enter the location where you want the video to be saved.</li> <li>Enable the option Normalized video resolution to 1024X768.</li> <li>Click <b>OK</b> to save the entries and return to the Console Redirection screen.</li> <li>Click <b>Cancel</b> if you don't wish to save the entries.</li> <li>In the Console Redirection window, click <b>Video Record &gt; Start Record</b>.</li> <li>Record the process.</li> <li>To stop the recording, click <b>Video Record &gt; Stop Record</b>.</li> </ol>
<b>Power</b>	<b>Reset Server</b>	To reboot the system without powering off (warm boot).
	<b>Immediate Shutdown</b>	To immediately power off the server.
	<b>Orderly Shutdown :</b>	To initiate operating system shutdown prior to the shutdown.
	<b>Power On Server</b>	To power on the server.
	<b>Power Cycle Server</b>	To first power off, and then reboot the system (cold boot).
<b>Active Users</b>		Click this option to displays the active users and their system ip address.
<b>Help</b>	<b>JViewer</b>	Displays the copyright and version information.

<b>Quick Buttons</b>		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. <b>Note:</b> 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.
		This quick button is used to record the video.
		This quick button is used to show or hide the mouse cursor on the remote client system.
		Active Users
		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.
		These quick buttons will pop up a virtual media where you can configure the media.