

ASMB8-iKVM

Server Management Board

User Guide

 E10970 Revised Edition V2 October 2015

Copyright © 2015 ASUSTeK COMPUTER INC. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTEK COMPUTER INC. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Contents

Notices	vi
Safety information	viii
About this guide	ix
ASMB8-iKVM specifications summary	xi

Chapter 1: Product Introduction

Welcome!	
Package contents	1-2
Features	1-3
System requirements	1-4
Network setup	1-5
	Welcome! Package contents Features System requirements Network setup

Chapter 2: Hardware Information

3.1.4

3.1.5

3.1.6

3.1.7

2.1	Before	you proceed	2-2
2.2	Hardwa	are installation	2-2
2.3	Firmwa	are update and IP configuration	2-4
	2.3.1	Firmware update	2-4
	2.3.2	Configure BMC IP source static IP	2-5
	2.3.3	Configure BMC IP source DHCP	2-6
2.4	BIOS c	onfiguration	2-7
	2.4.1	Running the BIOS BMC configuration	2-7
	2.4.2	BMC network configuration	2-8
	2.4.3	System Event Log	2-9
	2.4.4	IPv6 BMC Network Configuration	2-10
2.5	Runnin	g the ASMC8 utility	2-12
	2.5.1	Configuring the LAN controller	2-14
	2.5.2	Configuring the user name and password	2-15
Chap	oter 3: AS	US Host Management Controller Set-up	
3.1	ASUS I	Host Management Controller Setup	3-2
	3.1.1	Installing and launching the ASUS Host Management Controller Setup utility	3-2
	3.1.2	Command fields	3-3
	3.1.3	Initial	

Contents

Chapte	er 4: Web	-based User Interface	
4.1	Web-bas	ed user interface	4-2
	4.1.1	Logging in the utility	4-2
	4.1.2	Using the utility	4-3
4.2	FRU Info	rmation	4-4
4.3	Server He	ealth	4-5
	4.3.1	Sensor Readings (with Thresholds)	4-5
	4.3.2	Event Log	4-6
	4.3.3	Audit Log	4-6
	4.3.4	BSOD Screen	4-7
4.4	Configura	ation	4-8
	4.4.1	Active Directory	4-8
	4.4.2	DNS	.4-11
	4.4.3	Event Log	.4-11
	4.4.4	LDAP/E-Directory	.4-12
	4.4.5	Mouse Mode	.4-15
	4.4.6	Network	.4-15
	4.4.7	Network Bond	.4-16
	4.4.8	NTP	.4-16
	4.4.9	PEF	.4-17
	4.4.10	RADIUS	.4-24
	4.4.11	Remote Session	.4-24
	4.4.12	Services	. 4-25
	4.4.13	SMTP	. 4-25
	4.4.14	SSL	. 4-26
	4.4.15	Users	.4-31
	4.4.16	Virtual Media	. 4-33
4.5	Remote C	Control	. 4-34
	4.5.1	Console Redirection	. 4-34
	4.5.2	Server Power Control	. 4-42
	4.5.3	Java SOL	. 4-42
	4.5.4	Chassis Identify Command	. 4-42
	4.5.5	Power Button Control	.4-43
4.6	Auto Vide	eo Recording	.4-44
	4.6.1	Triggers Configuration	. 4-44
	4.6.2	Recorded Video	.4-44

Contents

4.7 Maintenance	
4.7.1 Preserve Configurat	ion4-45
4.7.2 Restore Configuration	on
4.7.3 Reset BMC	
4.7.4 Reset iKVM	
4.7.5 BIOS POST Code	
4.8 Firmware Update	
4.8.1 Firmware Update	
4.8.2 BIOS Update	4-47

Appendix

A.1	BMC connector	A-2
A.2	LAN ports for server management	A-3
A.3	Troubleshooting	A-4
A.4	Sensor Table	A-5
ASUS c	ontact information	A-11

Notices

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with manufacturer's instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- · Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Canadian Department of Communications Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This class B digital apparatus complies with Canadian ICES-003.

REACH

Complying with the REACH (Registration, Evaluation, Authorization, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS website at <u>http://csr.asus.com/english/REACH.htm</u>.

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for detailed recycling information in different regions.



DO NOT throw the motherboard in municipal waste. This product has been designed to enable proper reuse of parts and recycling. This symbol of the crossed out wheeled bin indicates that the product (electrical and electronic equipment) should not be placed in municipal waste. Check local regulations for disposal of electronic products.



DO NOT throw the mercury-containing button cell battery in municipal waste. This symbol of the crossed out wheeled bin indicates that the battery should not be placed in municipal waste.

Safety information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the server.
- When adding or removing devices to or from the server, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing server before you add a device.
- Before connecting or removing signal cables from the server, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area. If you are
 not sure about the voltage of the electrical outlet you are using, contact your local power
 company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.

Operation safety

- Before installing any component to the server, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter technical problems with the product, contact a qualified service technician or your retailer.

About this guide

This user guide contains the information you need when installing and configuring the server management board.

How this guide is organized

This guide contains the following parts:

Chapter 1: Product Introduction

This chapter describes the server management board features and the new technologies it supports.

Chapter 2: Hardware Information

This chapter provides instructions on how to install the board to the server system and install the utilities that the board supports.

Chapter 3: ASUS Host Management Controller Set-up

This chapter tells you how to use the ASUS Host Controller Set-up that the server management board supports.

Chapter 4: Web-based user interface (ASMB8-iKVM only)

This chapter tells you how to use the web-based user interface that the server management board supports.

Appendix

The Appendix shows the location of the LAN ports for server management and BMC connector on server motherboards. This section also presents common problems that you may encounter when installing or using the server management board.

Where to find more information

Refer to the following sources for additional information and for product and software updates.

1. ASUS websites

The ASUS website provides updated information on ASUS hardware and software products. Refer to the ASUS contact information.

2. Optional documentation

Your product package may include optional documentation, such as warranty flyers, that may have been added by your dealer. These documents are not part of the standard package.

Conventions used in this guide

To ensure that you perform certain tasks properly, take note of the following symbols used throughout this manual.



DANGER/WARNING: Information to prevent injury to yourself when trying to complete a task.



CAUTION: Information to prevent damage to the components when trying to complete a task.



IMPORTANT: Instructions that you MUST follow to complete a task.



NOTE: Tips and additional information to help you complete a task.

Typography

Bold text	Indicates a menu or an item to select.
Italics	Used to emphasize a word or a phrase.
<key></key>	Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key.
	Example: <enter> means that you must press the Enter or Return key.</enter>
<key1> + <key2> + <key3></key3></key2></key1>	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+).
	Example: <ctrl> + <alt> + </alt></ctrl>
Command	Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets.
	Example: At DOS prompt, type the command line:
	format A:/S

ASMB8-iKVM specifications summary

Chipset	Aspeed 2400
Internal RAM	224 MB for system 32 MB for video
Internal ROM	32 MB
Timers	32-bit Watchdog Timer
Main features	IPMI 2.0-compliant and supports KVM over LAN Web-based user interface (remote management) Virtual media Network Bonding support
Form factor	22 mm x 17 mm

* Specifications are subject to change without notice.



Product Introduction

1

This chapter describes the server management board features and the new technologies it supports.

1.1 Welcome!

Thank you for buying an ASUS® ASMB8-iKVM server management board!

The ASUS ASMB8-iKVM is an Intelligent Platform Management Interface (IPMI) 2.0-compliant board that allows you to monitor, control, and manage a remote server from the local or central server in your local area network (LAN). With ASMB8-iKVM in your server motherboard, you can completely and efficiently monitor your server in real-time. The solution allows you to reduce IT management costs and increase the productivity.

Before you start installing the server management board, check the items in your package with the list below.

1.2 Package contents

Check your server management board package for the following items.

- ASUS ASMB8-iKVM Card
- Support CD
- User guide



If any of the above items is damaged or missing, contact your retailer.

1.3 Features

1. IPMI 2.0

- System interface (KCS)
- LAN interface (support RMCP+)
- System Event Log (SEL)
- Sensor Data Record (SDR)
- Field Replaceable Unit (FRU)
- Remote Power on/off, reboot
- Serial Over LAN (SOL)
- Authentication Type: RAKP-HMAC-SHA1
- Encryption (AES)
- Platform Event Filtering (PEF)
- Platform Event Trap (PET)
- Watchdog Timer

2. Private I2C Bus

• Auto Monitoring sensors (temperature, voltage, fan speed and logging events)

3. PMBus*

Support Power supply for PMBus device

4. PSMI*

Support Power supply for PSMI bus device

5. Web-base GUI

- Monitor Sensor, show SDR, SEL, FRU, configure BMC, LAN
- Support SSL (HTTPS)
- Multiple user permission level
- Upgrade BMC firmware

6. Update Firmware

- DOS Tool
- Web GUI (Windows® XP/Vista/2003/2008, RHEL5.2, SLES10SP2)

7. Notification

- PET
- SNMP Trap
- e-Mail

8. KVM over Internet

Web-based remote console

9. Remote Update BIOS

Use Remote floppy to update BIOS

10. Remote Storage (Virtual Media)

Support two remote storage for USB/CD-ROM/DVD and image

11. Remote Install OS

Use remote storage to remote install OS

12. Support MIB file

• A management information base (MIB) is a database used for managing the entities in a communications network. Most often associated with the Simple Network Management Protocol (SNMP).

* A power supply supported PMBus and PSMI is necessary.

** Specifications are subject to change without notice.

1.4 System requirements

Before you install the ASMB8-iKVM board, check if the remote server system meets the following requirements:

- ASUS server motherboard with Baseboard Management Controller (BMC) connector*
- LAN (RJ-45) port for server management**
- Microsoft[®] Internet Explorer 5.5 or later; Firefox



- Visit <u>www.asus.com</u> for an updated list of server motherboards that support the ASMB8-iKVM.
- ** See the Appendix for details.

1.5 Network setup

The ASMB8-iKVM server management board installed on the remote server connects to a local/central server via direct LAN connection or through a network hub. Below are the supported server management configurations.

Direct LAN connection

LAN connection through a network hub







Hardware Information

This chapter provides instructions on how to install the board to the server system and install the utilities that the board supports.

2.1 Before you proceed

Take note of the following precautions before you install the server management board to the remote server system.

- Unplug the server system power cord from the wall socket before touching any component.
 - Use a grounded wrist strap or touch a safely grounded object or to a metal object, such as the power supply case, before handling components to avoid damaging them due to static electricity.
 - Hold components by the edges to avoid touching the ICs on them.
 - Whenever you uninstall any component, place it on a grounded antistatic pad or in the bag that came with the component.
 - Before you install or remove any component, ensure that the power supply is switched off or the power cord is detached from the power supply. Failure to do so may cause severe damage to the motherboard, peripherals, and/or components.

2.2 Hardware installation

To install the server management board:

1. Locate the Baseboard Management Card header on the motherboard.



 Orient and press the Management Card in place.





The motherboard illustration is for reference only. The motherboard layout and appearance may vary depending on the model, but the installation steps remain the same.

- 3. Press the board firmly until it is completely seated in place.
- 4. Insert the LAN cable plug to the LAN port for server management.



Refer to the Appendix for the location of the LAN port for server management.

5. For direct LAN configuration, connect the other end of the LAN cable to the local/central server LAN port.

For connection to a network hub or router, connect the other end of the LAN cable to the network hub or router.

 Ensure the VGA, USB, PS/2 cables are corrected, then connect the power plug to a grounded wall socket.



Every time after the AC power is re-plugged, you have to wait for about 70 seconds for the system power up.

2.3 Firmware update and IP configuration

You need to update the ASMB8-iKVM firmware and configure IP source before you start using the ASMB8-iKVM board.

2.3.1 Firmware update

To update the firmware:

- 1. Insert the support CD into the optical drive.
- 2. Restart the remote server then press during POST to enter the BIOS setup.
- 3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].
- 4. When finished, press <F10> to save your changes and exit the BIOS setup.
- On reboot, select ASMB8-iKVM Firmware Update for Clear Configuration from the main menu and press <Enter> to enter the sub-menu.



6. From the confirmation message, select <Yes> to update the firmware.



7. Wait for the firmware updating process to finish.



You may update the firmware from the web-based user interface. Refer to the **Firmware Update** section for more information.

2.3.2 Configure BMC IP source static IP

- 1. Insert the support CD into the optical drive.
- 2. Restart the remote server then press during POST to enter the BIOS setup.
- 3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].
- 4. When finished, press <F10> to save your changes and exit the BIOS setup.
- On reboot, select Configure BMC IP Source Static IP for Shared LAN (or DM_LAN1) from the main menu and press <Enter> to enter the sub-menu.



6. Select <Yes> from the confirmation window.



7. Wait for the configuration to finish. When done, press any key to continue.



 Go to BIOS menu to set the IP. For more information, refer to the IP settings in BIOS menu section.

2.3.3 Configure BMC IP source DHCP

- 1. Insert the support CD into the optical drive.
- 2. Restart the remote server then press during POST to enter the BIOS setup.
- 3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].
- 4. When finished, press <F10> to save your changes and exit the BIOS setup.
- 5. On reboot, select **Configure BMC IP Source DHCP for Shared LAN (or DM_LAN1)** from the main menu and press <Enter> to enter the sub-menu.

ASUS Server Z10PA-D8 Series System
FreeDOS command prompt
Configure BMC IP Source Static IP for Shared LAN
Configure BMC IP Source DHCP IP for Shared LAN
Configure BMC IP Source Static IP for DM_LAN1
Configure BMC IP Source DHCP IP for DM LAN1
ASMB8 Firnware Update for Preserve Configuration (SDR, LAN, Username)
ASMB8 Firnware Update for Clear Configuration (SDR, LAN, Username)

6. Select <Yes> from the confirmation window.



7. Wait for the configuration to finish. When done, press any key to continue.



8. The DHCP server will assign and IP for you.

2.4 BIOS configuration

You need to adjust the settings in the BIOS setup of the remote server for correct configuration and connection to the central server.

Ø	•	Update the remote server BIOS file following the instructions in the motherboard/ system user guide. Visit the ASUS website (www.asus.com) to download the latest BIOS file for the motherboard.

 The BIOS setup screens shown in this section are for reference purposes only, and may not exactly match what you see on your screen.

2.4.1 Running the BIOS BMC configuration

To configure the BMC in the BIOS:

- 1. Restart the remote server, then press during POST to enter the BIOS setup.
- 2. Go to the **Server Mgmt** menu, then select the **BMC network configuration** sub-menu. Use this sub-menu to configure the BMC settings.
- 3. When finished, press <F10> to save your changes and exit the BIOS setup.

2.4.2 BMC network configuration

Allows you to set the BMC LAN Parameter settings.

EMC Network Configuration DM_LAN1 DM_LAN1 IP Address in EMC : 192.168.254.020 DM_LAN1 Subnet Mask in EMC : 255.255.255.020 DM_LAN1 Gateway Address in EMC : 000.000.000.000 DM_LAN1 Gateway Address in EMC : 00.21.23.3020	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC)
DM LANI MAC Address in EMC : 00.E1.E2.3A.3B.3C Configuration Address Source [Previous State] Shared LAN Shared LAN Subnet Mask in EMC : 192.168.254.020 Shared LAN Subnet Mask in EMC : 255.255.250.00	
Shared LAN Gateway Address in EMC 000.000.000.000 Shared LAN MAC Address in EMC : 00.E1.E2.3A.20 Shared LAN MAC Address in EMC : 00.E1.E2.3A.3B.3C Configuration Address Source [Previous State]	<pre>: Select Screen 1 : Select Item Enter: Selectv +/-: Change Opt. F1: General Help F2: Previous Values F5: Optimized Defaults F10: Save & Exit ESC: Exit</pre>

Configuration Source [Previous State]

Allows you to select the IP address source type. Set the LAN channel parameters statically or dynamically.



The following items are available when you set Configuration Source to [Static].

Station IP Address

Allows you to set the BMC IP address.

Subnet Mask

Allows you to set the BMC subnet mask. We recommend that you use the same Subnet Mask you have specified on the operating system network for the used network card.

Gateway IP Address

Allows you to set the Gateway IP address.

2.4.3 System Event Log

Allows you to view all the events in the BMC event log. It will take a maximum of 15 seconds to read all the BMC SEL records.

Aptio Setup Utility - (Serv	Copyright (C) 2013 Americ er Mgmt	an Megatrends, Inc.
Enabling/Disabling Options: SEL Components	[Disabled]	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC)
Erasing Settings	[No]	
When SEL is Full	[Do Nothing]	
NOTE: All values changed here do until computer is restarted	not take effect d.	
		: Select Screen : : Select Itam Enter: Selectv +/- : Change Opt. F1: General Help F2: Previous Values F5: Optimized Defaults F10: Save & Exit ESC: Exit
Manadar 0 15 1006 0	enumiente (C) 2012 American	Marcal and Area Ware

SEL Components [Disabled]

Allows you to enable or disable all features of system event log during booting.



Erase SEL [No]

Allows you to select how to erase SEL. Configuration options: [No] [Yes, On next reset] [Yes, On every reset]

When SEL is Full [Do Nothing]

Allows you to select what to do to a full SEL. Configuration options: [Do Nothing] [Erase Immediately]

2.4.4 IPv6 BMC Network Configuration

Displays the LAN channel parameters and allows you to configure the IPv6 BMC LAN settings.

IPv6 BMC DM_LAN1 IP Address Source [Previous State]

Allows you to select the IP address source type and set the LAN channel parameters statically or dynamically.

Configuration options: [Previous State] [Static] [Dynamic-Obtained by BMC running DHCP]



The following items are available when you set IPv6 BMC DM_LAN1 IP Address Source to $[\mbox{Static}].$

IPv6 BMC DM_LAN1 IP Address

Allows you to set the IPv6 BMC DM_LAN1 IP address.

IPv6 BMC DM_LAN1 IP Prefix Length Allows you to set the IPv6 BMC DM_LAN1 IP Prefix length.

IPv6 BMC DM_LAN1 Default Gateway Allows you to set the IPv6 BMC DM_LAN1 Gateway IP address.

IPv6 BMC Shared LAN IP Address Source [Previous State]

Allows you to select the IP address source type and set the LAN channel parameters statically or dynamically. Configuration options: [Previous State] [Static][Dynamic-Obtained by BMC running DHCP]



The following items are available when you set IPv6 BMC Shared LAN IP Address Source to [Static].

IPv6 BMC Shared LAN IP Address Allows you to set the IPv6 BMC Shared LAN IP address.

IPv6 BMC Shared LAN IP Prefix Length Allows you to set the IPv6 BMC Shared LAN IP Prefix length.

IPv6 BMC Shared LAN Default Gateway Allows you to set the IPv6 BMC Shared LAN Gateway IP address.

2.5 Running the ASMC8 utility

The ASMC8 utility allows you to update the ASMB8-iKVM firmware, configure the LAN settings for the remote server, and change the user name/password in DOS environment. This utility is available from the support CD that came with the package.

To run the ASMC8 utility:

- 1. Insert the support CD into the optical drive.
- 2. Restart the remote server then press during POST to enter the BIOS setup.
- 3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].
- 4. When finished, press <F10> to save your changes and exit the BIOS setup.
- On reboot, select FreeDOS command prompt from the main menu then press <Enter>.

ASUS Server Z10PA-D8 Series System		
FreeDOS command prompt		
Configure BMC IP Source Static IP for Shared LAN		
Configure BMC IP Source DHCP IP for Shared LAN		
Configure BMC IP Source Static IP for DM LAN1		
Configure BMC IP Source DHCP IP for DM LAN1		
ASMB8 Firnware Update for Preserve Configuration (SDR, LAN, Username)		
ASMB8 Firnware Update for Clear Configuration (SDR, LAN, Username)		

 From the C:> prompt, type ASMC8 -? then press <Enter> to display the ASMC8 Utility Help Menu (as shown below).



Press any key to see next page.

ASMC8 Help Menu options

Options	Description	
-kcs[smic/bt/pci_smic] NetFn command data	Send IPMI command	
-bmc_ip_source source[1: Static, 2: DHCP]	Set the IP source	
-bmc_ip [ip_addr] (e.g., bmc_ip 10.10.10.20)	Write the BMC IP address for dedicated LAN	
-bmc_mask [ip_mask] (e.g., bmc_mask 255.255.255.0)	Write the subnet mask for dedicated LAN	
-bmc_gateway [ip_addr] (e.g., bmc_gateway 10.10.10.254)	Write the gateway address for dedicated LAN	
-pet_ip_mac[ip_addr][mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	Write the PET destination IP and MAC addresses for dedicated LAN	
-bmc_ip_s_lan1 source[1: Static, 2: DHCP]	Set the IP source for shared LAN	
-bmc_ip_lan1 [ip_addr] (e.g., bmc_ip 10.10.10.20)	Write the BMC IP address for shared LAN	
-bmc_mask_lan1 [ip_mask] (e.g., bmc_mask 255.255.255.0)	Write the subnet mask for shared LAN	
-bmc_g_lan1 [ip_addr] (e.g., bmc_gateway 10.10.10.254)	Write the gateway address for shared LAN	
-pet_ip_m_lan1 [ip_addr] [mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	Write the PET destination IP and MAC addresses for shared LAN	
-adm_name new_name_string	Change the administration name	
-user_name new_name_string	Change the user name	
-adm_password new_adm_password	Change the administration password	
-user_password new_user_password	Change the user password	
-sol_baud [baud rate] (e.g., sol_baud 57600)	Set the communication Baud rate	
-bmc_info	Displays the BMC and PET IP and MAC addresses	
-fru -view fru_id	Displays the system FRU information	
-fru -load fru_file	Update system FRU data from file	
-fru -save fru_id fru_file	Save system FRU data to file	
-sel -clear	Clear system event log	

2.5.1 Configuring the LAN controller

Before you can establish a connection to the ASMB8-iKVM board, you must configure the LAN port for server management used by the remote server to connect to the local/central server.

To configure the LAN port of the remote server:

- 1. Run the ASMC8 utility from the support CD following the instructions in the previous section.
- 2. Set IP source:
 - a. Type ASMC8 -bmc_ip_source 1 if you want to set a static IP address.
 - b. Type ASMC8 -bmc_ip_source 2 if you want to get IP from DHCP server.
- Type ASMC8 -bmc_ip xxx.xxx.xxx then press <Enter> to assign any IP address to the remote server LAN port (if necessary). The screen displays the request and response buffer.



Write the remote server IP address in a piece of paper for reference.

```
c:\>ASMC8 -bmc_ip 10.10.10.243
Detect MotherBoard -> (Z10PA-D8 Series)
Detect KCS Interface
New BMC IP : 10.10.10.243
c:\>
```

When finished, the utility returns to the DOS prompt.



Make sure that the assigned IP address for both remote and local/central servers are in the same subnet. You can use the network settings utility in your OS to check.

- 4. Configure your subnet mask and gateway address if necessary.
 - a. Type ASMC8 -bmc_mask xxx.xxx.xxx (your subnet mask encoded in hexadecimal system)
 - b. Type ASMC8 -bmc_gateway xxx.xxx.xxx (your gateway address encoded in hexadecimal system)
- 5. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.
- 6. Adjust the local/central server network settings, if necessary.

2.5.2 Configuring the user name and password

You may change your user name and password from the $\ensuremath{\mathsf{ASMC8}}$ utility.

To change the user name and password:

- 1. Insert the support CD into the optical drive.
- 2. Restart the remote server then press during POST to enter the BIOS setup.
- 3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].
- 4. When finished, press <F10> to save your changes and exit the BIOS setup.
- 5. On reboot, select **FreeDOS command prompt** from the main menu then press <Enter>.
- 6. From the C:> prompt, type ASMC8 -user_name xxxxx then press <Enter> to change the user name.

c:\>ASMC8 -user_name super Detect MotherBoard -> (Z10PA-D8 Series) Detect KCS Interface
Change User Name to super c:\>

- 7. Type ASMC8 -user_password xxxxxxx, then press <Enter> to change the password.
- 8. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.

Chapter 2: Hardware In	formation
------------------------	-----------



ASUS Host Management Controller Set-up

This chapter shows you how to set-up the ASUS Host Management Controller that the server management board supports.

3.1 ASUS Host Management Controller Setup

The ASUS Host Management Controller Setup utility provides precise configuration and basic functions including System Event Log (SEL) generation and System Data Record (SDR) reading in DOS mode.

This utility also supplies configuration sequences for the type of host interface as well as direct real-time monitoring of system information including CPU temperature(s), fan speeds and system voltages.

3.1.1 Installing and launching the ASUS Host Management Controller Setup utility

To install the ASUS Host Management Controller Setup utility:

- 1. Boot the server in DOS mode using the support CD.
- At the prompt, type ASMC8, then press <Enter> to display the ASMC8 Utility Help Menu. The screen appears as shown.



3. From the main utility screen, press <Enter>.


3.1.2 Command fields

The utility menu bar has five commands: Initial, View, Set, Monitor and Help. You can select a command using the left or right arrow button on the keyboard. After selecting a command, use the down arrow key to display available options. Select a command, then press <Enter> to execute.



3.1.3 Initial

The Initial command allows you to clear the SEL information or exit the utility.

Go to **Initial** command, then select **Clear SEL** to empty all System Event Log information for a refresh set of data records. Use the **Clear SEL** command when creating a new log that begins at an exact time for precise system monitoring.

Select Exit to close the utility and return to the DOS prompt.



3.1.4 View

The View command displays the Baseboard Management Controller (BMC) data record including the System Event Log (SEL), the System Data Record (SDR), and general BMC information.



To view the System Event Log (SEL):

 Select BMC SEL from the View command option, then press <Enter>. A complete list of system event records appear on the left pane. The right pane displays the SEL information.

The number on the left bottom of the window shows the system event displayed in the right window pane over the total number of system events in the remote host.

- 2. Use the down arrow key to display the next sensor event.
- 3. Press <Esc> to return to the main screen.

ASUS Ho	st Management Controller Setup Menu
Initial View Set	Monitor Help
Systen Event Log: (Hex) 01 00 02 09 4E 98 45 20 00 04 02 3A 01 50 19 05 1/202	Record ID : 0001h Record Type : 02h (System Event Record) Date & Date : Fri Jan 21 20:43:00 2011 General ID : 2008h EvM Rev : 04h (IPMI 1.5) Sensor Type : 02h (Voltage) Sensor Number: 3Ah (+1.1V IOH) Event Dir : 01h ('Hreshold) Event Datal : 50h Event Value : 19h (0.2 V) Threshold : 09h 1.0 V) Offset: Lower Non-critical - going low
🛛 🖾 🖣: Select Menu 🛛 E	SC: Exit Up/Down KCS

To view the System Data Record (SDR):

1. Select **BMC SDR** from the **View** command option, then press <Enter>. A complete list of data records appears on the left pane. The right pane displays the sensor data information.

The number on the bottom left of the screen indicates the data record displayed in the right window pane over the total number of sensor data records in the remote host.

ASUS	S Host Management Controlle	r Setup Menu
Initial View	Set Monitor Help	
Sensor Data Record: ((Hex) Record ID	: 0001h
	SDR Version	: 51h
	5 20 Record Type	01h (Full Sensor Record)
	09 Owner ID/Lun	20h/08h
	Sensor Number	31h (CPU1 Temperature)
	5 20 🛛 Sensor Initia	L: 7Fh
	09 Capabilities	68h
	Sensor Type	81h (Temperature)
	5 20 Event Type	: 01h (Threshold)
	09 Assert Mask	0280h
	Deassert Mask	3200h
	5 20 Reading Mask	1010h
	09 Nominal Read	20h (40 °C)
	Upper Critica	L: 50h (80 °C)
	Upper Warning	: 50h (80 °C)
	Lower Warning	: 18h (24 °C)
	Lower Critica	L: 18h (16 °C)
	ID String	CPU1 Temperature
🛛 🖾 🕶 Select Menu	ESC: Exit Up/Down	KCS

- 2. Use the down arrow key to display the next sensor data record.
- 3. Press <Esc> to return to the main screen.

To view the BMC information:

- 1. Select **BMC Info** from the **View** command option, then press <Enter>. A list of BMC information appears on the left pane.
- 2. Use the down arrow button to select a BMC information. The BMC information is displayed in the right pane.



3. Press <Esc> to return to the main screen.

3.1.5 Set

The Set command controls the host interface type and the correct BMC time.

ASU	S Host	Management	Controller Setup Menu
Initial View	Set	Monitor	Help
	Host BMC	Interface Timer	

To select the host interface:

- 1. Select **Host Interface** from the **Set** command option, then press <Enter>. The screen displays the host interfaces supported by the server management board.
- 2. Use the down arrow button to select a host interface, then press <Enter>.



You can select from the following interfaces:

(

3. When finished, press <Esc> to return to the main screen.

To set the BMC Timer:

- 1. Select BMC Timer from the Set command option, then press <Enter>.
- 2. Set the BMC IPMI timer to the current system time.
- 3. When finished, press <Esc> to return to the main screen.

3.1.6 Monitor

The **Monitor** command displays real-time data on the remote server system and CPU temperatures, voltages, and fan speeds.

ASUS Host 1	Management	Controller Setup Menu
Initial View Set	Monitor	Help
	All Sent Tempera Voltage Fan Spec OEM Defin	sor ture eed ine 1

To display a remote server information:

- 1. Select a sensor from the **Monitor** command options, then press <Enter>. A list of server information appears on the left pane.
- 2. Use the down arrow button to select a monitor information. The selected monitor information details are displayed in the right pane.

ASUS Host Ma	nagement Controller Setur	9 Menu
Initial View Set M All Sensor Temperature Voltage Fan Speed OEM Define 1 OEM Define 2	CPU1 Temperature MB1 Temperature	: (24h) 36 °C : (17h) 23 °C
Sun Jan 30 18:10:39 2011	0/000000045	00 00 00:16 KCS

3. Press <Esc> to return to the main screen.

3.1.7 Help

The $\ensuremath{\text{Help}}$ command displays the available utility options, utility version, and copyright information.







Web-based User Interface

This chapter tells you how to use the web-based user interface that the server management board supports.

4.1 Web-based user interface

The web-based user interface allows you to easily monitor the remote server's hardware information including temperatures, fan rotations, voltages, and power. This application also lets you instantly power on/off or reset the remote server.

To enter the Web-based user interface:

- 1. Enter the BIOS Setup during POST.
- 2. Go to the Advanced Menu > Runtime Error Logging > CPU II0 Bridge Configuration > Launch Storage OpROM, then press <Enter>.
- 3. Set Launch Storage OpROM to [Enabled].
- 4. Go to the Server Mgmt Menu > BMC network configuration > Configuration Address source, then press <Enter>.
- 5. Enter the IP Address in BMC, Subnet Mask in BMC and Gateway Address in BMC.
- 6. Press <F10> to save your changes and exit the BIOS Setup.



You should install JRE on remote console first before using web-based management. You can find **JRE** from the folder **JAVA** of the ASMB8-iKVM support CD. You can also download JRE from <u>http://www.oracle.com/technetwork/java/javase/downloads/index.</u> <u>html</u>

4.1.1 Logging in the utility

- 1. Ensure that the LAN cable of the computer is connected to the LAN port of the remote server.
- Open the web browser and type in the same IP address as the one in the remote server.
- 3. The below screen appears. Enter the default user name (admin) and password (admin). Then click Login.

ASMB8 KVM
Usemane: Pessword:
Logm
Required Devenior Settings 1. Allow popular form this site 🖉
2 Allow file download throm thin site. (How to 📳) 3. Enable jourcount for this case. 🚳
4. Enable coolies for this site G It is recommoded not to use Reflection, lack and Fonsard options of the browser.

4.1.2 Using the utility

The web-based graphics user interface displays when you login in the utility successfully.



- 1. Menu bar: Click a menu to display available function lists.
- 2. **Function list:** Click each function key to start using its specific functions.
- 3. Function title: Displays the function title.
- 4. **Help menu:** Click to display the brief description of the selected function.

4.2 FRU Information

This section contains detailed information for various FRU deviced present in this system.

ASMB	Birtym								
American Megatrends Inc.									
Dealbarred COULAGener		Conference	Deres Control	Aver 184 - Provider		Flowers Haden		• admin (Administrator) C	Refresh 🕏 Print 🖉 Logout
Dashboard Pro Informa	ion Server nealor	Configuration	Remote Control	Auto video Recording	Maintenance	Pinnware Opdate			HELP
Field Replaceable	Unit(FRU)								^
This page gives detailed inform	tion for the various FRU	devices present in thi	is system.						
Basic Information:									
ERII Device ID									
COU Device ID									
PRO Device Name									
Chassis Information:									
Chassis Information Are	Format Version								
Chassis Type									
Chassis Part Number									
Chassis Serial Number									
Chassis Extra									
Board Information:									
Board Information Area	ormat Version								
Language									
Manufacture Date Time									
Board Manufacturer									
Board Product Name									
Board Serial Number									
Board Part Number									
FRU File ID									
Board Extra									
Product Information:									
Product Information Are	Format Version								
Language									
Manufacturer Name									
Product Name									
Product Part Number									
Product Version									
Product Serial Number									
Asset Tag									~

4.3 Server Health

This section contains the data related to the server health such as the Sensor Readings, Event log, and BSOD Screen. Click each item to start using its specific functions.

ASMB	8.KVM					
Dashboard FRU Informat	ion Server Health	Configuration Remote	Control Auto Video Recording	Maintenance	Somin(Administra Firmware Update	HELP
Sensor Readings All sensor related information w All Sensors	Sensor Readings Event Log Il be d Audit Log BSOD Screen	le click on a record to toggle (O	N / OFF) the live widget for that particul	r sensor.		Sensor Count: 22 sensors
Sensor Name A CPU1 Temperature	Status 🗅	Current Reading 🔺				
VCORE1	Normal	Not Available Not Available	CPU1 Temperature: No	Available		NORMAL
+VCORE1 +3.3V +5V	Normal Normal Normal	Not Available Not Available Not Available Not Available	CPU1 Temperature: No Thresholds for this sensor	Available		NORMAL Live Widget Off On

4.3.1 Sensor Readings (with Thresholds)

The Sensor Readings page displays the system sensor information, including readings and status.

ASMB	В ікум			
Dashboard FRU Informatic	n Server Health Configuration	Remote Control Auto Vid	Recordina Maintenance Firmeere Undate	admin (Jordinovice) C. Kerresh & Print - Lopout HELP
Senso dings Al sessor a comation vill All Sensors V	be displayer 2 circ circ on a record	to toggle (ON / OFF) the live widget t	The perioder sense.	Sensor Count: 27 sensor
Sensor Nome (4)	Status A	Current Reading		
NM Capabilities	Supported	Supported		SUBBORTED
CPU1 Temperature	Normal	67 ° C	NM Capabilities: Supported	SOPPORTED
CPU2 Temperature	Not Available	Not Available	Threabolds for this sensor	Live Widget NA1
+VCORE1	Normal	1.782 Valts		
+VCORE2	Not Available	Not Available	Lover Non-Recoverable (LNR) NIA	Upper Non-Recoverable (UNR): N/A
+3.3V	Normal	3.264 V005	Lewer Critical (LC): NIA	Upper Critical (UC) NIA
100	Normal	4,992,900	Lower Non-Critical (LNC): NIA	Upper Non Critical (UNC): N/A
-0.00	Normal	4 883 Male		Threshold Settings
*9700	Norma	4.992 V00		
-1 70.00	Normal	3.312 VMD		
-2.3V38	Normal	5.312 Yes	Graphical view of this sensor s events	
1000 15 000	Net Australia	Nat Available		
Chassisisterion	Capacity Changin Intrusion	0,0001	UNR (0)	
4V000_00_00U1	Normal	1.2 1/10/10		
10000 00 0000	hist Auximia	hist Austinitia		
CRU EAN1	Normal	1440 8214	LNC (0)	
CPU FAN2	Not Available	Not dvailable		
EBNT FAN1	Not Available	Not Available		
FIRNT FAN2	Not Available	Not Available	uc (0)	
FRNT_FAN3	Not Available	Not Available		
FRNT_FAN4	Not Available	Not Available		
REAR_FAN1	Not Available	Not Available	Other (0)	
REAR_FAN2	Not Available	Not Available		
FRNT_FAN5	Not Available	Not Available	Discrete (0)	
+VCCI0	Normal	1.072 Volts	8 5 10 15 21	
TR3 Temperature	Normal	42 ° C	Number of Entries	
TR4 Temperature	Normal	56 ° C		View this Event Log
TR1 Temperature	Normal	45 ° C		

- 1. Select a sensor type category: Allows you to select the type of sensor readings to be displayed in the list.
- 2. **Status List:** Shows the type of sensor readings list that you selected in the drop-down list.
- 3. View this event log: Click to enable or disable the Live Widget function.

4.3.2 Event Log

The Event Log page displays a table of system event log.

ASI	MB8.	KV M							
	_	_	_			_			🕯 admin (schwarzen) - C. Refresh - 🔍 Print - 🔎 Log
Deshboerd I	FRU Information S	ierver Health	Configuration	Remote Control	Auto Video Recording	Maistenance	Firmware Update		HE
Event Log	9								
Events necessite	d by the system will be in	and here Doubl	in dick on a second to	o can the description					
Crema generation		· · · · · · · · · · · · · · · · · · ·							
All Events		×	 filter by: All Ser 	nsors 🗸					Event Log: 21 event entries, 1 page(s)
· BMC Times		UTC Offset: 0	OMT-05-001						<< < 1 > >>
EventID	Time Stamp A		Ser	nvor Name A		Sector	or Type A	Description A	
21	02/07/2105 01:2	19.57		Unknown		M	icrocontroller / Coprocessor	Transition to Running - Asserted	
20	02/07/2105 01:2	8.57		Unknown		M	icrocontroller / Coprocessor	Transition to Running - Asserted	
19	02/07/2106 01:2	18.57		Unknown		M	icrocontroller / Coprocessor	Transition to Running - Asserted	
18	02/07/2106 01:2	28.57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
17	02/07/2106 01:2	10.57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
16	02/07/2105 01:2	88.57		Unknown		M	icrocontroller / Coprocessor	Transition to Running - Asserted	
15	04/17/2014 15:2	10:37		Watchdog2		W	atchdog 2	Timer Expired - Asserted	
14	02/07/2105 01:2	28.57		Unknown		M	icrocontroller / Coprocessor	Transition to Running - Asserted	
13	02/07/2105 01:2	28.57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
12	02/07/2105 01:2	28.57		Unknown		M	crecentralier / Coprocessor	Transition to Running - Asserted	
11	02/07/2106 01:2	28.57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
10	02/07/2106 01:2	28.57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
9	02/07/2105 01:2	18 57		Unknown		M	crocontroller / Coprocessor	Transition to Running - Asserted	
8	04/16/2014 15:4	15:26		Watchdog2		W	atchdog 2	Timer Expired - Asserted	
1	01/01/2012 001	37.56		Unknown		M	crocomolier / Coprocessor	Trensition to Running - Asserted	
	0101/2012 001	37:37		Unknown			crocomposer / Coprocessor	Transition to Power Off - Assened	
*	02072105012	10.00		University		10	crocone one / Coprocessor	Transition to Porning - Asserted	
•	0207/2105 01 2	10.50		Unknown		10	crocompaine / Coprocessor	Transition to Running - Assented	
2	02072100012	10.00		University of the second secon			Concerning / Concerning	Transition to Postming - Assetted	
1	02/07/2105 01:2	10.50		Unknown		10	crocontroller / Coprocessor	Transform to Running - Asserted	
									Save Event Logs Clear All Event Logs

- 1. Select an event log category: Allows you to select the type of events to be displayed in the list.
- 2. Clear Event Log: Click to clear the event log.

4.3.3 Audit Log

The Audit Log page displays a table of audit event log.

Audit Logs This space assays logs of audit events for this device (if the options have been configured). Audit Log UTC Offset (GUT-6 Event 01-3 This States 2-3 Description 3-3 Event 01-3 This States 2-3 Description 3-3 1 Jain 10006 15 tocalhoid Webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 2 Jain 10016 15 tocalhoid Webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 3 Jain 10016 15 tocalhoid Webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 4 Jain 10016 11 tocalhoid Webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 5 Jain 10016 11 tocalhoid Webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 6 Jain 1012 154 tocalhoid webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 17) 7 Jain 112 154 16 tocalhoid webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 13) 7 Jain 1112 154 16 tocalhoid webgic (D14 IRFO/NCED0ULuser admin login successfully thim 102 105 254 13)	iboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	HELF
Less of a substrate single displays logg displays logg displays logg displays l	dit Lo	gs							
Andel Log Direct Column Column Colum	page disp	mays logs of audit ever	its for this device (if th	e options have beer	n configured).				
Aust Log UTC 001462 (0017-0) File 10 - 3 Ten States - 4 2 Jan 1 60/06 11 Incendent - 3 2 Jan 1 60/06 12 Ten States - 4 2 Jan 1 60/06 17 Ten States - 4 3 1 0 60/07 Ten States - 4 4 Jan 1 60/06 17 Ten States - 4 5 Jan 1 100/05 11 Ten States - 4 5 Jan 1 100/05 11 Ten States - 4 7 Jan 1 100/05 11 Ten States - 4 7 Jan 1 100/05 11 Ten States - 4 4 Jan 1 100/05 11 Ten States - 4 7 Jan 1 100/05 11 Ten States - 4 7 Jan 1 100/05 11 Ten States - 4 7 Jan 1 100/05 10 Ten States - 4 8 Jan 1 100/05 10 Ten States - 4 9 Ten States - 4 Ten States - 4 7 Jan 1 115/01 Ten States - 4									
Event D 1 Monthmen Description 1 1 Jun 1 98.05% Iscamber J webg/ [D14 #P00/KBQ/J user John 102 149.254.13 2 Jun 1 98.05% Iscamber J webg/ [D14 #P00/KBQ/J user John 102 149.254.13 2 Jun 1 98.05% Iscamber J webg/ [D14 #P00/KBQ/J user John 102 149.254.13 3 Jun 1 98.05% Iscamber J webg/ [D14 #P00/KBQ/J user John 102 149.254.13 4 Jun 1 90.05% Iscamber J webg/ [D14 #P00/KBQ/J logot fmm 122 149.254.13 5 Jun 1 103.94 Iscamber J webg/ [D14 #P00/KBQ/J logot fmm 122 149.254.13 6 Jun 1 1132.41 Iscamber J webg/ [D14 #P00/KBQ/J logot fmm 152 149.254.13 7 Jun 1 1151.01 Iscamber J webg/ [D14 #P00/KBQ/J logot fmm 152 149.254.13	Audit	Log							UTC Offset: (GMT+08:00)
Event D 1 Time Stamp 1 Description 3 1 Jain 1.0019-15 localhoid webge [D14 #PO]VEBDUI vare admin login successfully from 192:108.254.13 2 Jain 1.0019-15 localhoid webge [D14 #PO]VEBDUI vare admin login successfully from 192:108.254.13 3 Jain 1.0019-11 localhoid webge [D14 #PO]VEBDUI vare admin login successfully from 192:108.254.13 5 Jain 1.0029-13 localhoid webge [D14 #PO]VEBDUI logar from 192:108.254.13 6 Jain 1.0029-13 localhoid webge [D14 #PO]VEBDUI logar from 192:102.214.214.21 6 Jain 1.1029-43 localhoid webge [D14 #PO]VEBDUI vare admin login successfully from 192:108.254.13 7 Jain 1.112:101 localhoid webge [D14 #PO]VEBDUI vare admin login successfully from 192:108.254.13									This Filter: 7 event entries
Centol 3- Time Stamp -> HostRame -> Description -> 1 Jain 1 0.0616 Biochholt weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 2 Jain 1 0.0616.14 weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 3 Jain 1 0.0616.14 weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 4 Jain 1 0.0616.14 weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 5 Jain 1 0.0616.14 weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 6 Jain 1 1.0516.14 weitige (2014 R=V)(HeBOUL user admin login successfully from 192.140.254.13 7 Jain 1 1.0524.13 iscaRhoal 7 Jain 1 1.0524.01 weitige (2014 R#Op/0EBOUL user admin login successfully from 192.140.254.13									
1 Jun 1 0804 19 Needhold welge, ID 04 800/BEG04 user admin login successfully min 1916 24-11 32 2 Jun 1 0815 27 Needhold welge, ID 04 800/BEG04 user admin login successfully min 1916 24-11 32 3 Jun 1 0815 27 Needhold welge, ID 04 800/BEG04 user admin login successfully min 1916 24-11 32 4 Jun 1 0915 11 Isoaheid welge, ID 04 800/BEG04 user admin login successfully min 1916 24-12 5 Jun 1 1003 89 Isoaheid welge, ID 04 400/BEG04 user admin login successfully min 1916 24-12 14 6 Jun 1 1003 84 Isoaheid welge, ID 04 400/BEG04 user admin login successfully min 192 108 24-13 7 Jun 1 112 101 Isoaheid welge, ID 14 400/BEG04 user admin login successfully tem 192 108 24-13	vent ID	∆ Time :	Stamp 🔺		HostName A	Description A			
2 Jah 1 (167:52.2) Included webp: (2) 11 (197:01 # 0-0) # 0-0 #	1	Jan 1	08:06:16		localhost	webgo: [3014]	NFO]WEBGUI user	admin login successfully from 192.168.254.13	
Jahr 1 (e/e/e/1) Inclinioni webgic (D/H 40/0)(mixed) Last 4 down down down down down down down down	2	Jan 1	08:15:23		localnost	webgo: (3014)	NFOIWEBGUI IOGOU	t from : 192.168.254.13 User : admin	
3 Jan 1 102.05.05 Localizat erabge 102.05.01 # 0700CDDU Local activity tipes increased by them 105.05.05.01 5 Jan 1 102.05.01 Localizat erabge 102.01 # 0700CDDU Local activity tipes increased by them 105.05.05.01 7 Jan 1 112.101 Localizat webge [D014 ##000CEDDUL user admin login successfully from 192.106.224.13	3	Jan 1	08:49:17		localhoat	webgo: [3014]	NFOWEBGUI user	admin login successfully from 192.168.254.13	
s ann in 1929-1939 in collecter were an in the second and in the second and the s	-	Jali I	40-00-50		localitost	webg0, [30141	NFOJWEBGOI IOGOL	1 10111 192. 106.254. 15 USEL 400 450 054 42	
7 Jan 1 115101 Incalhod webge (2014 MPC)/K280U user admin login successfully from 192.108.224.13	6	Jan 1	10:20:42		localhost	webgo: [3014]	NEOIWEBCI II Ioon	#from : 192 169 254 12 user : admin	
	7	Jan 1	11:51:01		localhost	webgo: [3014]	NFOIWEBGUI user	admin login successfully from 192 108 254 13	

4.3.4 BSOD Screen

This page displays the snapshot of the blue screen captured if the host system crashed since last reboot.

AS	MR8							
O Arren Lange		IKVM						i admini (Januara and Califordi 🖉 Brite 🖉 Lacord
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	HELP
Blue Sci	reen of Death							
This page disp	lays the snapshot of th	e blue screen captur	ed if the host system	crashed since last rebo	vot.			
						SOD SCREEN IS	NOT AVAILABLE.	

4.4 Configuration

This section allows you to configure the system settings. Click each function key to start using its specific functions

Dashboard FRU Information Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	 admin (Administrator) C Refresh & Print P Lopout HELD
Blue Screen of Death	Active Directory DNS					
This page displays the snapshot of the blue screen captur	Event Log	ashed since last rebo	set.			
	Mouse Mode					
	Network					
	Network Bond					
	PEF					
	RADIUS					
	Remote Session					
	Services					
	SSL					
	System Firewall					
	Users Maturel Martin					
	VIII. NY GA					

4.4.1 Active Directory

An active directory does a variety of function including the ability to provide the information on objects, helps organize these objects for easy retrieval and access, allows access by users and administrators, and allows the administrators to set security up for the directory. To open Active Directory Settings page, click **Configuration** > **Active Directory** from the main menu. A sample screenshot of Active Directory Settings Page is shown in the screenshot below.

AS	MB8	ікум									
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recordina	Maintenance	Firmware Update		÷	ómin (Administrator) – C. Ro	sfresh 😵 Print 🖝 Logeut HELP
Active E	Directory Settin	ngs									
The 'Active Di	rectory' is currently disable	led. To enable Active	Directory and conf	lgure its settings. Click	on 'Advanced Settings' butto	n. iom the list and clici	: Delete Role Group or Mos	dify Role Group. To add a new Ro	de Group, select an unconfigure	d skt and click Add Role G	Advanced Settings
	9									Number o	f configured Role groups: 0
Role Gr	rose ID A		Stoup Name 3			Gr	NID Domain A			Group Privilege -3	
	1		~							~	
	2		-								
	3		~				*			*	
	4		~							*	
	5										
									Add Role Group	Modify Role Group	Delete Role Group

- 1. **Role Group ID**: The name that identifies the role group in the Active Directory. Role Group Name is a string of 255 alpha-numeric characters. Special symbols hyphen and underscore are allowed.
- 2. Add Role Group: To add a new role group to the device.
- 3. **Modify Role Group:** To modify that role group. Alternatively, double click on the configured slot.
- 4. Delete Role Group: To delete an existing Role Group.
- Advanced Settings: This option is used to configure Active Directory Advanced Settings. Options are Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.

Procedure:

Entering the details in Advanced Active Directory Settings Page

1. Click on Advanced Settings to open the Advanced Active Directory Settings page.

AS	MB	8								
Dashboard	FRU Informatio	on Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	• 20m	n (Administrator	I C Kerrech & White P Looput HELP
Active D		ettings								
To Configure	Active Directory Sec	ver Settings, dick 'Adva	sced Settings'							Advanced Settings
The list below	shows the current	Advanced Active D	Directory Setting:	5				 	×	Role Group.
		Active Directory Author	intration		X	Enable				umber of configured Role groups: 0
Rose Ca	1	Secret Username			Icel	4				3
	2 3	Secret Password				5.000				
	4 5	Domain Controller Se	ver Address1		10	10.192.2				
		Domain Controller Ser	ver Address2							
		Domain Controller Ser	ver Address3							Delete Role Group
								Savo	Cancel	
1										-

- 2. In the Active Directory Settings Page, enter the following details.
 - Active Directory Authentication: To enable/disable Active Directory, check or uncheck the Enable checkbox respectively.



If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

- Secret Username: Key in a username.
- Secret Password: Key in a password.
- User Domain Name: For the user in the User Domain Name field. e.g. asus.com
- IP addresses: Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address 3.
- 3. Click **Save** to save the settings and return to Active Directory Settings Page or click **Cancel** to cancel the entry and return to Active Directory Settings Page.

To add a new Role Group

1. In the Active Directory Settings Page, select a blank row and click **Add Role Group** to open the Add Role group Page as shown in the screenshot below.

AS	MB	Вікум							
Dashboard	FRU Informatic	n Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	 admin (Administration) C Refrech & Print - Logout HELP
Active D									
To Configure A	Active Directory Ser	er Settings, click 'Advar	iced Settings'					 	
The list below	shows the current	Add Role Group						6	Role Group.
		Role Group Name					1		imber of configured Role groups: 0
Role Gr	oup ID is	Role Group Domain							5
	2	Role Group Privilege			Admi	nistrator 🗸			
	3	Extended Privileges			- KA	M 🗆 VMedia			
	5							Add Cancel	

2. In the **Role Group Name** field, enter the name that identifies the role group in the Active Directory.



- Role Group Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen and underscore are allowed.
- 3. In the Role Group Domain field, enter the domain where the role group is located.



- Domain Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.
- 4. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.
- 5. Click Add to save the new role group and return to the Role Group List.
- 6. Click **Cancel** to cancel the settings and return to the Role Group List.

To Modify Role Group

- 1. In the Advanced Directory Settings Page, select the row that you wish to modify and click **Modify Role Group**.
- 2. Make the necessary changes and click **Save**.

To Delete a Role Group

In the Advanced Directory Settings Page, select the row that you wish to delete and click **Delete Role Group**.

4.4.2 DNS

The page allows you to manage DNS settings of the device.

ASMB8	IKVM	
Dashboard FRU Information	Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	+ admin (Administratory) C Refresh SP Print SE Legout HELP
DNS Server Settings Manage DNS settings of the device		
DNS Service	☑ Enable	
Multicast DNS mDNS Settings	C EANNE	
Host Configuration Host Settings Host Name	Automatic:	
Register BMC DM_LAN1	R Register BMC * Naciodate OPC/P Client FQDN · Hostname	
LANI	Repister BMC Nsupdate DHCP Client FODN Hostname	
TSIG Configuration TSIG Authentication Current TSIG Private File New TSIG Private File	Declaration	
Domain Name Configuration Domain Settings Domain Name	[LANL_v4 V]	
Domain Name Server Configuration DNS Server Settings	LANT	
IP Priority DNS Server1	⊕ IPv4 ○ IPv6 .	
DNS Server2		
DNS Server3		
		Save Reset

4.4.3 Event Log

This page is used to configure the System Event log information .



4.4.4 LDAP/E-Directory

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC[®] card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the MegaRAC[®] card. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

To open LDAP Settings page, click **Configuration > LDAP** from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below. LDAP Settings Page

AS	MB8	ikvm									
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		•••	lmn (Edministrator) – C. Rel	vesh & Print P Logout HELP
LDAP/E-	Directory Set	tings									
LDAP/E-Direct	ory is currently disabled	To enable LDAPIE	Directory and config	ure its settings. Click o	n 'Advanced Settings' button.					1	Advanced Settings
The list below	shows the current list of	configured Kole Gro	rups. It you would like	e to denote or modify a	role group, select the name in	om the list and click	Denete More Group or Mod	atly Hole Group. To add a new Hole Group, se	rect an uncompany	d slot and click Add Hate G Number of	configured Role groups: 0
Note Co	MBID 7		Group Name a			Group	5 Search Base			Group Privilege	
			-								
			~								
	1		~				*				
			*								
	5										
											Dalata Dala Decus

- 1. **Advanced Settings:** To configure LDAP Advanced Settings. Options are Enable LDAP Authentication, IP Address, Port and Search base.
- Add Role Group: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.
- 3. Modify Role Group: To modify the particular role group.
- 4. Delete Role Group: To be delete a role group from the list.

Procedure

Entering the details in Advanced LDAP Settings Page

 In the LDAP Settings Page, click Advanced Settings. A sample screenshot of LDAP Settings page is given below.

									HELP
LDADIE									
LUAPIE									
LOAP/E-Direc		bled. To enable LDAP/							Advanced Settings
The list below	shows the current							8	Role Group.
		Advanced LDAP/E	t-Directory Settin	ĝs					imber of configured Role groups: 0
Role Gr	oup ID is 1	LDAP/E-Directory Au	thentication		₩ Er	vable			Δ
	2	SSL			S Er	side			
	3	Server Address			10.10	1.192.1			
	6	Port			389				
		Bind DN			cn+s	ucks us=rocks dc	=domain		0.0.0.0
		Password							Cop Delete Kole Group
		Search Base			cn±0	ucks tw=rocks dc	≕login ×		
		Attribute of User Logi	°		cn	~			
								Save Cancel	

2. To enable/disable LDAP Authentication, check or uncheck the **Enable** checkbox respectively.



During login prompt, use username to login as an Idap Group member.

3. Enter the IP address of LDAP server in the IP Address field.



- IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports IPv4 Address format and IPv6 Address format.
- 4. Specify the LDAP Port in the Port field.



Default Port is 389. For Secure connection, default port is 636.

- 5. Enter the **Search Base**. The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.
- 6. Click Save to save the settings.
- 7. Click **Cancel** to cancel the modified changes.

To add a new Role Group

- 1. In the LDAP Settings Page, select a blank row and click **Add Role Group** to open the Add Role group Page as shown in the screenshot below.
- 2 In the Role Group Name field, enter the name that identifies the role group.
- 3. In the **Role Group Search Base** field, enter the path from where the role group is located to Base DN.



- Search Base is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.
- 4. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.
- 5. Click Add to save the new role group and return to the Role Group List.
- 6. Click Cancel to cancel the settings and return to the Role Group List.

To Modify Role Group

- 1. In the LDAP Settings Page, select the row that you wish to modify and click **Modify Role Group**.
- 2. Make the necessary changes and click **Save**.

To Delete a Role Group

In the LDAP Settings Page, select the row that you wish to delete and click **Delete Role Group**.

4.4.5 Mouse Mode

The Mouse Mode page allows you to select the mouse mode.



Save: Select the desired mouse mode, and then click Save to apply the setting.

4.4.6 Network

The Network page allows you to configure the network settings.

Dashboard FRU Information Server Hea	Configuration Remote Control Auto Video Recording Main	tenance Firmware Update	admin (idoutions) C Refresh & Print & Lopout HELP
Network Settings			
Manage network settings of the device.			
LAN Interface	DM_LAN1 V		
LAN Settings	Z Enable		
MAC Address	00.E1.E2.3A.3B.3C		
IPv4 Configuration Obtain an IP address automatically			
IPv4 Address	192.168.254.20		
Subnet Mosk	255.255.255.0		
Default Gateway	0.0.0.0		
IPv6 Configuration IPv6 Settings	C Enable		
Obtain an IP address automatically	☑ Use DHCP		
IPv6 Address Subset Evely levels			
Default Gateway			
VLAN Configuration VLAN Settings	Enable		
VLAN ID	0		
VLAN Priority	0		
			Save Reset

- 1. MAC Address: Select whether to obtain the IP address automatically or manually configure one.
- 2. IP Address/Subnet Mask/Default Gateway: If you configure a static IP, enter the requested address, subnet mask and gateway in the given field.

4.4.7 Network Bond

This page allows you to enable or disable networking bonding feature and configure the default interfaces.

AS	MB8	ikvm									
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		• admin (Administrator)	C Refresh w Print	HELP
Networ The following	k Bonding Co	nfiguration	inding for the device.								
Network	Bonding		Cnable								
Auto Co	efiguration		M Enable								
								 		Save F	Reset

4.4.8 NTP

This page allows you to configure the NTP server or view and modify the device's Date and Time settings.

AS	MB8	ікум									
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		 admin (Edministree) 	uor) ⊂ Refresh 🕬	HELP
NTP Setti	ings										
Here you can eit	ther configure the NT	P server or view and	modify the device's l	Date & Time settings.							
Date:	A	pell	✓ 17	2014 🗸							
Time: (hh/mm/aa)		19 32	05								
Timezone:	G	MT-5	~								
Primary N	TP Server: pi	ol.ntp.org									
Secondary	NTP Server: tir	ne.nist.gov									
🗹 Autom	atically synchronize (Date & Time with NTR	^o Server								
										Refresh Save	Reset

4.4.9 PEF

Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert. A PEF implementation is recommended to provide at least 16 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc.

To open PEF Management Settings page, click **Configurations > PEF** from the main menu. A sample screenshot of PEF Management Settings Page is shown in the screen shot below.

\SMB8ikvm											
shboard FRU Information	Server Health Configuration Remote Co	ntrol Auto Video Recording Maintenanc	e Firmware Update	🗘 admin (Administrator) - C. Refresh - 😂 Print 👘							
EF Management											
e this page to configure Event Filte	r, Alert Policy and LAN Destination. To delete or modify a	entry, select it in the list and click "Delete" or "Modify	". To add a new entry, select an unconfigured slot and click "Add".								
Ever	2 Miton	3	4	5							
				Anfigured Event Filter count:							
PEFID A	Filter Configuration - A	Event Filter Action ->	Event Severity A	Sensor Name - A							
	Enabled	(Alart)	Unspecieo	Any Any							
3	Enabled	(Alert)	Unspecified	Attr							
4	Enabled	(Alert)	Unspecified	Any							
5	Enabled	(Alert)	Unspecified	Any							
6	Enabled	[Alert]	Unspecified	Any							
7	Enabled	[Alert]	Unspecified	Any							
8	Enabled	(Alert)	Unspecified	Any							
9	Enabled	(Alert)	Unspecified	Any							
10	Enabled	(Alert)	Unspecified	Any							
11	Enabled	(Alert)	Unspecified	Any							
12	Enabled	[Alet]	Unspecified	Any							
13	Enabled	(Abert)	Unspecified	Any							
14	Enabled	(Alert)	Unspecified	Aty							
15	Enabled	[Alet]	Unspecified	Any							
95											
17		~	*	*							
18											
19											
20	*	*	*	*							
21											
22	-	-	*								
23	-	~									
-	-										
24	-		-								
27	-										
28	-	~									
29	~										
				Add Modify Delete							

- 1. PEF ID: This field displays the ID for the newly configured PEF entry (read-only).
- 2. Filter configuration: Check box to enable the PEF settings.
- 3. Event Filter Action: Check box to enable PEF Alert action. This is a mandatory field.
- 4. Event Severity: To choose any one of the Event severity from the list.
- 5. Sensor Name: To choose the particular sensor from the sensor list.
- 6. Add: To add the new event filter entry and return to Event filter list.
- 7. Modify: To modify the existing entries.
- 8. Cancel: To cancel the modification and return to Event filter list.

Procedure:

- 1. Click the Event Filter Tab to configure the event filters in the available slots
- To Add an Event Filter entry, select a free slot and click Add to open the Add event Filter entry Page. A sample screenshot of Add Event Filter Page is in seen the screenshot below.

FRU Informa	tion Server Health Configuration Remote Conf	trol Auto Video Recording Maintenance Firmware Update	admin (Idministrator) C. Refresh 10 Pr
Filter	Add Event Eilter entry		8
			nfigured Event Filte
4FID ∆	Event Fifter Configuration		A 100 A
	PEF ID	16	
	Filter Configuration	Enable	
	Event Severity	Unspecified V	
	Filter Action configuration		
	Event Filter Action	Maart North	
	Viet Date: Name	None V	
	Generator ID continuation	1 4	
	Generator ID Data	Rever Data	
	Generator ID 1	0x0	
	Generator ID 2	0x0	
	Event Generator	Stave type Software type	
	Slave Address/Software ID		
	Channel Number	0 ~	
	IPMB Device LUN	0 ~	
	Sensor configuration		
	Sensor Type	All Sensors V	
	Sensor Name	All Sensors V	
	Event Options	All Events V	
			~
	a care		

- 3. In the Event Filter Configuration section,
 - PEF ID displays the ID for configured PEF entry (read-only).
 - In filter configuration, check the box to enable the PEF settings.
 - In Event Severity, select any one of the Event severity from the list.
- 4. In the Filter Action configuration section,
 - Event Filter Action is a mandatory field and checked by default, which enable PEF Alert action (read-only).
 - Select any one of the Power action either Power down, Power reset or Power cycle from the drop down list
 - Choose any one of the configured alert policy number from the drop down list.

Alert Policy has to be configured - under Configuration->PEF->Alert Policy.

- 5. In the Generator ID configuration section,
 - Check Generator ID Data option to fill the Generator ID with raw data.
 - Generator ID 1 field is used to give raw generator ID1 data value.
 - Generator ID 2 field is used to give raw generator ID2 data value.



In RAW data field, to specify hexadecimal value prefix with '0x'.

Alert Policy Tab

This page is used to configure the Alert Policy and LAN destination. You can add, delete or modify an entry in this page.

				admin (Administrator)	Refresh & Print
ard FRU Inform	ation Server Health 0	Configuration Remote Control Auto Video Reco	rding Maintenance Firmware Update		
Managemer	ıt				
nana in contours Ex	and Eliter allert Entry and Later	Destination. To delate or modify a entry relevant in the last and	civit "Dalata" or "Modify". To add a new antivy salart an upperformed and and rick "Add		
w 1	Alert Po 🔿 LAV	V Destination		5	6
				Contr	aured A day cos
Dalley Ealer #	Dalica Number	Dalicy Configuration	Delicy Set	LAN Interface	Destination Select
84		Disbeo	Annalys serve well to the destination	DACTORN 1	v
33	1	Disabled	Always send alort to this destination	DM_LANI	•
34	1	Disabled	Always send alort to this destination	BALCAN	
.0	1	Utabled	Aways send akin to this destination	DAGOAN	
20		Distored	Avage send alert to this dectration	DM_DANI	
37		Disabled	Anneys seems are used when an analyzed and a second	Dis Lower	
20		Disabled	Anneys stern and shall be the destination	Dis Lower	
40		Disabled	Abuses send dort to this destination	DM LANS	
41	4	Disabled	Abusing pand alart to this destination	DM LANS	
42	1	Disabled	Always send alert to this destination	DM LAN1	
40	1	Disabled	Always send alert to this destination	DM LAN1	
44	1	Disabled	Always send alert to this destination	DM_LAN1	0
45	1	Disabled	Always send alort to this destination	DM_LAN1	٥
46	4	Disabled	Always send alert to this destination	DM_LAN1	0
47	4	Disabled	Always send alert to this destination	DM_LAN1	0
48	1	Disabled	Always send alert to this destination	DM_LAN1	0
49	4	Disabled	Always send alert to this destination	DM_LAN1	0
50	1	Disabled	Aways send alort to this destination	DM_LAN1	0
51	4	Disabled	Always send alert to this destination	DM_LAN1	0
52	4	Disabled	Always send alert to this destination	DM_LAN1	0
53	1	Disabled	Ahrays send alert to this destination	DM_LAN1	0
64	1	Disabled	Always send alert to this destination	DM_LAN1	0
55	1	Disabled	Always send alert to this destination	DM_LAN1	0
56	1	Disabled	Always send alert to this destination	DM_LAN1	0
57	1	Disabled	Always send alert to this destination	DM_LAN1	0
58	1	Disabled	Always send alert to this destination	DM_LAN1	0
59	1	Disabled	Always send alort to this destination	DM_LAN1	
		Disabled	Always cend alort to this dectination	DM_LAN1	•

The fields of PEF Management - Alert Policy Tab are explained below.

- 1. **Policy Entry #:** Displays Policy entry number for the newly configured entry (readonly).
- 2. Policy Number: Displays the Policy number of the configuration.
- 3. Policy Configuration: To enable or disable the policy settings.
- 4. Policy Set: To choose any one of the Policy set values from the list.

0 - Always send alert to this destination.

1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.

2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.

3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

- 5. LAN Interface: To choose a particular channel from the available channel list.
- 6. **Destination Selector:** To choose a particular destination from the configured destination list.



LAN Destination has to be configured - under Configuration->PEF->LAN Destination.

- 7. Add: To save the new alert policy and return to Alert Policy list.
- 8. Modify: To modify the existing entries.
- 9. Cancel: To cancel the modification and return to Alert Policy list.

Procedure:

Add Alert Policy entry		X
Policy Entry # Policy Number Policy Configuration		
Policy Set LAN Interface	0 - DM_LAN1 -	
Destination Selector Alert String Alert String Key	1 Event Specific 0	
		Add Cancel

- In the Alert Policy Tab, select the slot for which you have to configure the Alert policy. That is, In the Event Filter Entry Page, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
- 2. Select the slot and click Add to open the Add Alert Policy Entry Page.
- 3. Policy Entry # is a read only field.
- 4. Select the **Policy Number** from the list.
- 5. In the **Policy Configuration** field, check **Enable** if you wish to enable the policy settings.
- 6. In the **Policy Set** field, choose any of the Policy set from the list.
- 7. In the LAN Interface field, choose a particular LAN interface from the available list.
- 8. In the **Destination Selector field**, choose particular destination from the configured destination list.



LAN Destination has to be configured under Configuration->PEF->LAN Destination. If you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the fourth slot (LAN Destination Number 4) in the LAN Destination tab.

- 9. In the Alert String field, enable the check box if the Alert policy entry is Event Specific.
- 10. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
- 11. Click Add to save the new alert policy and return to Alert Policy list.
- 12. Click Cancel to cancel the modification and return to Alert Policy list.
- 13. In the Alert Policy list, to modify a configuration, select the slot to be modified and click **Modify**.
- 14. In the Modify Alert Policy Entry Page, make the necessary changes and click Modify.
- 15. In the Alert Policy list, to delete a configuration, select the slot and click **Delete**.

PEF Management LAN Destination Page

This page is used to configure the Event filter, Alert Policy and LAN destination. A sample screenshot of PEF Management LAN Destination Page is given below.

Dashboard FRU Information Server Health	Configuration Remote Control Auto Video Recording Maintenance Fi	rmware Update	- + admin (Account) ⊂ Refresh = Privit - Capad HELS					
PEF Management								
Use this page to configure Event Filter, Alert Policy and L Event Filter, Alert Policy	AN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add	d a new entry, select an unconfigured slot and click 'Add'.						
LAN Interface: DM_LAN1 V			Configured LAN Destination count: 0					
LAN Destination 3	Destination Type -3	Destination Address 3						
2								
3								
6								
7	~							
10								
11								
10								
	*	*						
1								
			Send Test Alert Add Modify Delete					
L								

The fields of PEF Management - LAN Destination Tab are explained below.

- 1. **LAN Destination:** Displays Destination number for the newly configured entry (read-only).
- Destination Type: Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields - destination Email address, subject and body of the message needs to be filled. The SMTP server information also has to be added - under Configuration->SMTP. For SNMP Trap, only the destination IP address has to be filled.
- 3. **Destination Address:** If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:
- IPv4 address format.

- IPv6 address format.

If Destination type is Email Alert, then give the email address that will receive the email.

- 4. Subject & Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address 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.
- 5. Add: To save the new LAN destination and return to LAN destination list.
- 6. Cancel: To cancel the modification and return to LAN destination list.

Procedure:

Add LAN Destination entry		
LAN Channel Number	1	
LAN Destination	1	
Destination Type	Snmp Trap 👻	
Destination Address		
Username	anonymous 👻	
Message		
		Add Cancel

- In the LAN Destination Tab, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to configure the 4th slot of LAN Destination Page.
- 2. Select the slot and click Add. This opens the Add LAN Destination entry.
- 3. In the LAN Destination field, the destination for the newly configured entry is displayed and this is a read only field.
- 4. In the **Destination Type field**, select the one of the types.
- 5. In the **Destination Address field**, enter the destination address.



If Destination type is Email Alert, then give the email address that will receive the email.

- 6. Select the User Name from the list of users.
- 7. In the Subject field, enter the subject.
- 8. In the Message field, enter the message.
- 9. Click Add to save the new LAN destination and return to LAN destination list.
- 10. Click Cancel to cancel the modification and return to LAN destination list.
- 11. In the LAN Destination Tab, to modify a configuration, select the row to be modified and click **Modify**.
- 12. In the **Modify LAN Destination Entry** page, make the necessary changes and click Modify.
- 13. In the LAN Destination Tab, to delete a configuration, select the slot and click Delete.

4.4.10 RADIUS

This page is used to enable or disable RADIUS authentication and enter the required information to access the RADIUS server.

AS	MB8	ікум								
Deshboard	FRU Information	Server Health Co	orfiguration R	emote Control	Auto Video Recording	Maintenance	Firmware Update		• admin (Admonstrator) C Rel	nich & Mint in Lagout HELP
RADIUS	Settings									
The RADIUS authentication	Authentication is current should be enabled.	By disabled. To enable RAI	OIUS Authenticatio	n and onler the req	aired information to access th	e RADIUS server. P	hoss the Save butten to save y	our changes. To configure the Advanced settings, P	ADIUS Server	Advanced Settings
RAD	US Authentication	Enable								
Port		1812								
Serv	er Address									
Secr	et									
Exte	nded privileges	KVM V	VMedia							
										Save Reset

4.4.11 Remote Session

The Remote Session page allows you to enable or disable encryption on KVM or data during the redirection session.

ASMB8ikvm								
Dashboard FRU Information	Server Health Configuration	Remote Control	Auto Video Recordina	Maintenance	Firmware Update		• admin (Administratory) C	Refresh & Print & Logout HLLP
Configure Remote Se This page is used to configure visual Single Port Application Keyboard Language © Local Monitor OFF Automatically OFF Local II	ISSion redia configuration settings Denote Auto Datect (AD) Sontor, When JViewer Launches							
								Save Reset

- 1. Single Port Application: Tick to enable.
- 2. Keyboard Language: Select the keyboard language from the drop down list box.
- 3. Local Monitor OFF: Tick to enable or disable.
- 4. Automatically OFF Local Monitor, When JViewer Launches: Tick to enable or disable.
- 5. Save: Click to save the current changes.



It will automatically close the existing remote redirection either KVM or Virtual media sessions, if any.

6. Reset: Click to reset the modified changes.

4.4.12 Services

This page lists services running on the BMC. It shows current status and other basic information about the services. Press **Modify** to modify the services configuration.

AS	MB8	ikvm							
C.A. Contraction	+ adhiol (Administrator) ⊂ Rahredh 🗘 Print 🛹 Lopour								
Deshboard		Server Health Configuration		cording Maintenance					
Service									
OCTAICO									
Below is a to	t of services running on t	te BMC. It shows current status and othe	r basic information about the services. Se	rect a slot and press "Modify" b	ution to modify the services configuration	e.			
								Number of Services: 7	
8 A	Service Name	a Current State a	Interfaces A	Nonsecure Port A	Secure Port A	Timeout A	Maximum Sessions A	Active Sessions a	
1	VIED	Active	both	80	443	1800	20	Mater	
2	kym	Active	both	7578	7582	1800	4	View	
3	có-media	Active	both	5120	5124	NA	1	Mater	
4	16 media	Active	both	5122	5126	NA	1	Vitor	
5	hd-media	Active	both	5123	5127	NA	1	Vine	
6	667	Active	NA	NA	22	600	NA	Man	
7	teinet	Inactive	NA	23	NA	600	N/A	Mana	
								Modify	

4.4.13 SMTP

The SMTP page allows you to configure SMTP mail server. Enter the IP address of the mail server, and then click **Save** to apply the settings.

ASMB8	ASMB8.KVM							
Dashboard FRU Information	Server Health Configuration	Remote Control Auto	Video Recording Maintenance	Firmware Update	• admin (r	dolocenses) C. Refresh to Print # Logout HELP		
SMTP Settings Manapa SMTP setings of the device. LAN Channel Number Sender Address Mochine Name Primary SMTP Server SMTP Server SMTP Support	1]						
Server Address Support Server requires Author User Name Possword	ntication							
Secondary SMTP Server SMTP Support Port Server Address SMTP Server requires Author User Name Password	Enable 25							
						Save Reset		

4.4.14 SSL

The Secure Socket Layer protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions.

To open SSL Certificate Configuration page, click **Configuration > SSL** from the main menu. There are three tabs in this page.

AS	MB8							
							🕯 admin (Administration) - 🗢	Refresh 🗟 Print 🔎 Logout
Dashboard								
SSL Ce This page View Sol Uplos Curre New C Curre New F	rtificate Confi Disartgue 65 od 5 view th d SSL Gene at Certificate Certificate At Privacy Key Minacy Key	guration 2 cicl centers 3 cicl centers West Occ 31 19/00/00 196/2 West Occ 31 19/00/00 196/2	or can be accented in a secured mode. Uppad for in Browse	51, eption is used to	upload the certificate and private	wy lie wia the BAC. Generate SSI op	filer is used to generate the GSL conflicting t	asond on configuration details.
								Upload

- 1. **Upload SSL** option is used to upload the certificate and private key file into the BMC.
- 2. Generate SSL option is used to generate the SSL certificate based on configuration details.
- 3. View SSL option is used to view the uploaded SSL certificate in readable format.

Desking Collision for		1 4 10 do 10 10	Planna II adam	 admin (Administrator) C Refresh S Print = Logost
Dashboard Tico Information Set	Iver Health Connguration Remote Contr	Auto video Recording Maintenance	I immetre Opaste	HELP
SSL Certificate Configur	ation			
This page is used to configure SSL certificat View SSL option is used to view the uploads	to into the BMC. Using this, the device can be access of SSL contribute in readable format.	t in a secured mode. Uplead SSL option is used to	upload the certificate and private key file into the BMC. Gener	ate SSL option is used to generate the SSL certificate based on configuration details.
Upload SSL Generate 8	SSL View SSL			
Current Certificate	Wed Dec 31 19:00:00 1969			
New Certificate	Br	WT0		
Current Privacy Key	Wed Dec 31 19:00:00 1969			
New Privacy Key	Br			
				Upload
1				

The fields of SSL Certificate Configuration – Upload SSL tab are explained below.

- 1. Current Certificate: Current certificate information will be displayed (read-only).
- 2. New Certificate: Certificate file should be of pem type
- 3. Current Privacy Key: Current privacy key information will be displayed (read-only).
- 4. New Privacy Key: Privacy key file should be of pem type
- 5. Upload: To upload the SSL certificate and privacy key into the BMC.



Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

A	SM	B 8	ікум							
Deathlean	a cour	1	Surray Marchele	Conferentian	Derester Constant	Anto Vision Donordino	Malatana	Courses Harlete	🕯 admin (Administrator) C Refrech 🔍 Print 🖃	Logout MICL D
Dashooal	a FRUI	mormation	Server meanin	Connguration	Remote Control	Auto video Recording	Maintenance	Filmware Opdate		neur
SSL C	ertifica	te Confi	guration							
This case	in used to co	otoure 991 c	etificate into the DM	C Using this, the dev	ice can be accessed in	a secured mode United 99	option is used to u	months cartificate and minute kay	the into the BMC. Generate 991 option is used to generate the 991 partiticate based on configuration de	
View SSL	option is use	d to view the u	ploaded SSL certifi	ale in readable forma	d.	a source more openedation	- open in a sea in a	point int control of and points of y	an na cano, contrato con questo e soco la goneran en con, contratos encos en cangunator en	
Upl	oad SSL	Gem	rate SSL	View SSL						
C0	mmon Nam	2(CN)								
01	panization(C	9								
On	panization U	nn(OU)								
Cit	y or Locality	r(L)								
Ste	te or Provin	ce(ST)								
0	untry(C)									
Err	ail Address									
Va	ld for			days						
Ke	y Length		512	∨ bits						
									Generate	

The fields of SSL Certificate Configuration - Generate SSL tab are explained below.

- 1. Common Name(CN): Common name for which certificate is to be generated.
 - Maximum length of 64 characters.
 - Special characters '#' and '\$' are not allowed.

- 2. **Organization(O):** Organization name for which the certificate is to be generated.
 - Maximum length of 64 characters.
 - Special characters '#' and '\$' are not allowed.
- Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.
 - Maximum length of 64 characters.
 - Special characters '#' and '\$' are not allowed.
- 4. City or Locality(L): City or Locality of the organization (mandatory).
 - Maximum length of 64 characters.
 - Special characters '#' and '\$' are not allowed.
- 5. State or Province(ST): State or Province of the organization (mandatory).
 - Maximum length of 64 characters.
 - Special characters '#' and '\$' are not allowed.
- 6. Country(C): Country code of the organization (mandatory).
 - Only two characters are allowed.
 - Special characters are not allowed.
- 7. Email Address: Email Address of the organization (mandatory).
- 8. Valid for: Validity of the certificate.
 - Value ranges from 1 to 3650 days.
- 9. Key Length: The key length bit value of the certificate.
- 10. Generate: To generate the new SSL certificate.



HTTPs service will get restarted, to use the newly generated SSL certificate.
Dashboard FRU Information Server Health	Configuration Remote Control Auto Video Recording Maintenance Firmware Undate	IFT P
	Remote Control Maintenance	
SSL Certificate Configuration		^
This page is used to configure SSL certificate into the BMC.	Using this, the device can be accessed in a secured mede. Uplead SSL option is used to uplead the certificate and private key file into the BMC. Generate SSL option is used to generate the SSL certificate based on configuration	
details. View SSL option is used to view the uploaded SSL o	entificate in readable format.	
Upload SSL Generate SSL	View SSI	.
Basic Information		
Version	3	
Serial Number	9FF7DACD544345C2	
Signature Algorithm	sha WithRSAEnayption	
Public Key	(1924 bit)	
Issued From		
Common Name(CN)	AB	
Organization(O)	American Megatrands Inc	
Organization Unit(OU)	Service Processors	
City or Locality(L)	Atonto	
State or Province(ST)	Georgia	
Country(C)	US	
Email Address	Eusportigient com	
Validity Information		
Valid From	3ep 12 09:30:47 2008 0MT	
Valid To	Jan 25 06/30/47 2010 OMT	
Issued To		
Common Name(CN)	ANI.	
Organization(O)	American Megahrends Inc	
Organization Unit(OU)	Service Processors	
City or Locality(L)	Atanta	
State or Province(ST)	Georala	18

The fields of SSL Certificate Configuration – Generate SSL tab are explained below.

- 1. **Basic Information:** This section displays the basic information about the uploaded SSL certificate. It displays the following fields.
 - Version
 - Serial Number
 - Signature Algorithm
 - Public Key
- 2. **Issued From:** This section describes the following Certificate Issuer information
 - Common Name(CN)
 - Organization(O)
 - Organization Unit(OU)
 - City or Locality(L)
 - State or Province(ST)
 - Country(C)
 - Email Address
- 3. Validity Information: This section displays the validity period of the uploaded certificate.
 - Valid From
 - Valid To

- 4. **Issued To:** This section display the information about the certificate issuer.
 - Common Name(CN)
 - Organization(O)
 - Organization Unit(OU)
 - City or Locality(L)
 - State or Province(ST)
 - Country(C)
 - Email Address

Procedure

- 1. Click the Upload SSL Tab, Browse the New Certificate and New Privacy key.
- 2. Click **Upload** to upload the new certificate and privacy key.
- 3. In Generate SSL tab, enter the following details in the respective fields
 - The Common Name for which the certificate is to be generated.
 - The Name of the Organization for which the certificate is to be generated.
 - The **Overall Organization Section Unit** name for which certificate to be generated.
 - The City or Locality of the organization
 - The State or Province of the organization
 - The Country of the organization
 - The email address of the organization.
 - The number of days the certificate will be valid in the Valid For field.
- 4. Choose the Key Length bit value of the certificate
- 5. Click Generate to generate the certificate.
- 6. Click View SSL tab to view the uploaded SSL certificate in user readable format.



- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your Generic MegaRAC[®] SP securely using the following format in your IP Address field from your Internet browser: https://<your MegaRAC[®] SP's IP address here>
- For example, if your MegaRAC[®] SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30
- Please note the <s> after <http>.You must accept the certificate before you are able to access your Generic MegaRAC[®] SP.

4.4.15 Users

The User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click **Configuration > Users** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

ASM	В8ікум				
Dashboard FRU In	formation Server Health Configuration	Remote Control Auto Video Recording	Maintenance Firmware Update		Fadmin (Administrator) C Refresh S Print E Logout HELE
User Manager	nent current list of available 2 peakes or modely a us	er, select the user n 3 is and click "De	tele User' or "Mode 4 add a new user, s	elect an unconfigur 5 click "Add User"	6 Number of configured users: 2
UserID A	Username A	User Access A	Network Privilege A	SNMP Status A	Email ID -3
1	anonymous	Disabled	Administrator	Disabled	
2	admin	Enabled	Administrator	Disabled	
3	*	*	*	*	~
4	~			*	~
5		-	-		
6	*			*	*
7					
8					~
9					
10	~				~
					Add User Modily User Delete User

- 1. **User ID:** Displays the ID number of the user. Note: The list contains a maximum of ten users only.
- 2. User Name: Displays the name of the user.
- 3. User Access: To enable or disable the access privilege of the user.
- 4. Network Privilege: Displays the network access privilege of the user.
- 5. **SNMP Status:** Displays if the SNMP status for the user is enabled or Disabled.
- 6. Email ID: Displays email address of the user. Add User: To add a new user.
- 7. Add User: To add a new user.
- 8. Modify User: To modify an existing user.
- 9. Delete User: To delete an existing user.

Add a new user:

- 1. To add a new user, select a free slot and click Add User.
- 2. Enter the name of the user in the User Name field.
- 3. In the Password and Confirm Password fields, enter and confirm your new password.
- 4. Password must be at least 8 characters long. White space is not allowed. This field will not allow more than 20 characters.

- 5 Enable or Disable the User Access Privilege.
- 6. In the Network Privilege field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.
- 7. Check the SNMP Status check box to enable SNMP access for the user. NOTE: Password field is mandatory, if SNMP Status is enabled.
- 8. Choose the SNMP Access level option for user from the SNMP Access dropdown list. Either it can be Read Only or Read Write.
- Choose the Authentication Protocol to use for SNMP settings from the drop down list. NOTE: Password field is mandatory, if Authentication protocol is changed.
- 10. Choose the Encryption algorithm to use for SNMP settings from the Privacy protocol dropdown list.
- 11. In the Email ID field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content shows sensor information, ex: Sensor type and Description.

Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.

- 12. In the **New SSK Key** field, click Browse and select the SSH key file. Note: SSH key file should be of pub type.
- 13. Click Add to save the new user and return to the users list.
- 14. Click Cancel to cancel the modification and return to the users list.

Modify an existing User

- 1. Select an existing user from the list and click Modify User. This opens the Add User screen as shown in the screenshot below.
- 2. Edit the required fields.
- 3. To change the password, enable the Change Password option.
- 4. After editing the changes, click Modify to return to the users list page.

Delete an existing User

To delete an existing user, select the user from the list and click Delete User.

4.4.16 Virtual Media

The following option will allow to configure virtual media devices. Below, you can select the number of instances that are be supported for each type of virtual media devices.

ASMB8	ikvm				
Dashboard FRU Information	Server Health Configuration	Remote Control Auto Video Re	cording Maintenance Firmware Up	lato	# admin (Idministrator) C. Refresh & Print M Lopost HELP
Virtual Media Device	5				
The following option will allow to confi	igure virtual media devices. Below, you ca	n select the number of instances that are	be supported for each type of virtual media devi	es.	
Floppy devices	2 🗸				
CD/DVD devices	2 🗸				
Hard disk devices	2 🗸				
Power Save Mode	Enable				
					Save Reset

4.5 Remote Control

This section allows you to perform remote operations on the server. Click each function key to start using its specific functions

Darbhoard CDII Johannation Secure Health Configuration	Parante Control Auto Video Decordino Maintenance Elemente Hadate	Fadmin (Administrator) ⊂ Refresh 🕏 Print 🚽 Legout
Console Redirection Pro: be tuden to loand the estinction consists and manage the server remain	Scalada Tandar Sana Marana Tanas Canada Alara Sata Marana Satalang Canada Nawa Satalang Canada Nawa Satalang Canada	

4.5.1 Console Redirection

The remote console application, which is started using the WebGUI, allows you to control your server's operating system remotely, using the screen, mouse, and keyboard, and to redirect local CD/DVD, Floppy diskette and Hard disk/USB thumb drives as if they were connected directly to the server.

Dashboard FRU Information Server Health Configuration	Remote Control Auto Video Recording Maintenance Firmware Update	HELP
Console Redirection	Console Redirection Server Power Control	
Press the button to isunch the redirection console and manage the server rem	Java SOL Chaosis Identity Command	
	Power Button Control Java Console	

Browser Settings

For Launching the KVM, pop-up block should be disabled. For Internet explorer, enable the download file options from the settings.

Java Console:

This is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE should be installed in the client's system. You can install JRE from the following link. http://www.java.com/en/download/manual.jsp

The Java Console can be launched in two ways

- 1. Open the Dashboard Page and in Remote control section, click Launch for Java Console.
- 2. Open Remote Control>Console Redirection Page and click Java Console.

This will download the .jnlp file from BMC.

To open the .jnlp file, use the appropriate JRE version (Javaws) When the downloading is done, it opens the Console Redirection window.

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

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Video Record
- Power
- Active Users
- Help

A detailed explanation of these menu items are given below.



Video

This menu contains the following sub menu items.

- 1. Pause redirection: This option is used for pausing Console Redirection.
- 2. **Resume Redirection:** This option is used to resume the Console Redirection when the session is paused.
- 3. **Refresh Video:** This option can be used to update the display shown in the Console Redirection window.
- 4. **Turn ON Host display:** If you enable this option, the display will be back in the server screen.
- 5. Compression Mode: Allows you to choose the compression settings for the video.
- DCT Quantization Table: Allows you to set the quality that ranges from 0 (Worst Quality) to 7 (Best Quality).
- 7. **Turn OFF Host display:** If you enable this option, the server display will be blank but you can view the screen in Console Redirection.
- 8. **Capture Screen:** This option allows you to screen capture the console redirection screen.



9. Exit: This option is used to exit the console redirection screen

Keyboard

This menu contains the following sub menu items.

- 1. Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.
- Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.
- 3. Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.
- 4. **Hold Left Alt Key:** This menu item can be used to act as the left-side <ALT> key when in Console Redirection.
- Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.
- Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.
- Alt+Ctrl+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and keys down simultaneously on the server that you are redirecting.
- 8. **Context menu:** This menu item can be used to act as the context menu key, when in Console Redirection.
- 9. Hot Keys: This menu item can be used to add hot keys for frequently used keys.
- 10. Full Keyboard support: Tick this item for full keyboard support.



Mouse

- 1. **Show Cursor:** This menu item can be used to show or hide the local mouse cursor on the remote client system.
- 2. Mouse Calibration: This menu item can be used only if the mouse mode is relative. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote 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 sync. Please detect the first reading on which cursors go out of sync. Once this is detected, use 'ALT-T' to save the threshold value.
- 3. Mouse Mode: This menu item allows you to select the mode or type of mouse support.



Options

Band width: The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following:

- 1. Auto Detect: This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
- 2. 256 Kbps
- 3. 512 Kbps
- 4. 1 Mbps
- 5. 10 Mbps
- 6. 100 Mbps

Keyboard/Mouse Encryption: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.

Zoom: This option is available only when you launch the Java Console.

- 1. Zoom In: For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%
- 2. **Zoom Out:** For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%



Media

Virtual Media Wizard:

To add or modify a media, select and click 'Virtual Media Wizard' button, which pops out a box named "Virtual Media" where you can configure the media. A sample screenshot of Virtual media screen is given below. Virtual Media.

Floppy Key Media: This menu item can be used to start or stop the redirection of a physical floppy drive and floppy image types such as img.

CD/DVD Media: This menu item can be used to start or stop the redirection of a physical DVD/CD-ROM drive and cd image types such as iso.

Hard disc/USB Key Media: This menu item can be used to start or stop the redirection of a Hard Disk/USB key image and USB key image such as img.

Viewer [192.168.254.20] - 1 pr	_	
Video Keyboart Mouse Options Media Keyboard Layo	Video Recor Power Active User Hel	p Zoom Size : Disabled
Virtual Media Wizard.	50 100	150 👤 🖵 😃
Aptio Setup Utility - Main Advanced IntelRCSetup Serve	Copyright (C) 2013 American r Mgmt Event Logs Monitor	Megatrends, Inc. Security Boot Tool Exit
BIDS Information BIDS Vendor Core Version Dopliancy BIDS Version Build Oate Memory Information Total Memory System Language	American Megatrends 5.007 UEFI 2.3; PI 1.2 0210 x64 01/20/2014 8192 MB [English]	Choose the system default language
System Date System Time Access Level	[Thuredbg 04/17/2014] [15:01:15] Administrator	+: Select Screen 11: Select Item Enter: Select +/ Change Opt. F3: General Help F2: Previous Values F5: Obtilized Defaults F10: Save Changes & Reset ESC: Exit
Version 2.16.1243. Co	pyright (C) 2013 American M	egatrends, Inc.
		LALT LCTRL RALT RCTRL Num Cops Scroll

😢 Virtual Media		C (100	X
Floppy Key Media : I		_	^
Floppy Image	▼ Browse	Connect Floppy	
Floppy Key Media : II			
Floppy Image	▼ Browse	Connect Floppy	
CD/DVD Media : I			
CD Image	▼ Browse	Connect CD/DVD	
CD/DVD Media : II		_	
CD Image	➡ Browse	Connect CD/DVD	
O.F.			
Hard disk/USB Key Media : I		_	•

Keyboard Layout

Auto Detect: This option is used to detect keyboard layout automatically. The languages supported automatically are English – US, French – France, Spanish – Spain, German-Germany, Japanese- Japan. If the client and host languages are same, then for all the languages other than English mentioned above, you must select this option to avoid typo errors.

Soft Keyboard: This option allows you to select the keyboard layout. It will show the dialog as similar to onscreen keyboard. If the client and host languages are different, then for all the languages other than English mentioned above, you must select the appropriate language in the list shown in JViewer and use the softkeyboard to avoid typo errors. Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system. Soft keyboard is applicable only for JViewer Application not for other application in the client system.



4.5.2 Server Power Control

The Server Power Control page displays the current server power status and allows you to change the current settings. Select the desired option, and then click **Perform Action** to execute the selected action.

ASMB8 _{IKVM}	
Deshboard FRU Information Server Health Configuration Remote Control Auto Video Recording Meintenance Firmware Update	admin (schoolstate) C Refrech & Print Ecoport HELP
Power Control and Status	
The current server server status is shown below. To perform a power centrol operation, select one of the options below and press "Perform Action".	
Nosi is currently on	
Power button is enabled	
Reset Server	
Power off Server - Immediate	
Power Off Server - Orderly Shubdown	
Power On Server	
O Power Cycle Server	
	Perform Action

4.5.3 Java SOL

The Java SOL page allows lets you launch the Java SOL application.

And a second beginning to the second se	
Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	Initiatives) C Refresh & Print P Logout HELP
Java SOL	
Press the button to launch the Java SOL	
Java SOL	

4.5.4 Chassis Identify Command

The Chassis Identify Command page allows you to perform a chassis identify command control operation. You can set the Locator LED either always ON or OFF. You can also key in an identify interval in seconds then click **Perform Action** to start the command.



4.5.5 Power Button Control

The Power Button Control page allows you to enable or disable power buttons. Select an option then click **Perform Action** to confirm the selection .

ASMB8	ikvm								
Desta and Distances		C	n	1		The second s	 	admin (Administrator)	C Refresh & Print P Legout
Dashboard Pico Information	Server mealur	Comparation	Remote Condier	Auto Video Recording	Manifornance	Pititiware Opsaw			HELP
Power Button Contro	and Statu	8							
To perform a power button disabled o	v enabled operation	select one of the coti	ons below and mess P	writern Action					
Power button is enabled									
Disable Power Button									
Enable Power Button									
	6								
L P	erform Action								

4.6 Auto Video Recording

This section allows you to configure the events that will trigger the auto video recording function of the KVM server and display the list of available recorded video files on the BMC.

A	S	MB8	ікум						
Deshb	oard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	• admin (Aministrum) C. Refresh - Ø Print - P Lopout HELP
Cor	isole	Redirection				Triggers Configuration Recorded Video			
Press	Press the butter to launch the redirection conside and manage the server remotility.								
							Java Co	nsole	

4.6.1 Triggers Configuration

This page allows you to configure the events that will trigger the auto video recording function of the KVM server.



4.6.2 Recorded Video

This section displays the list of available recorded video files on the BMC and lets play, download and save, or delete a selected video.

	Padmin (/dminstrator) C Refresh 🔍 Print 🍡 Legout
Dashboard FRUInformation Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	
Video Recording	
Reference and an analysis and an analysis of the Reference of the Referenc	and some the olders. All the Wester's bodies to delate the entertaint often
being a list of available recorder when res on the bind. Select a water and circle in Pay view below in pay the water, select a water and circle ine contribution a	To save the video, Crox the "Deleve" coust to deleve the sendores video.
	Number of available Video files : 0
If → File Name →	Flie Information 4
Data Nor Available	
	Play Video Download Delete
1	
1	
1	
1	
1	

4.7 Maintenance

The Maintenance menu allows you to select specific configuration items to be preserved or to restore the default configuration for your device.

AS	MB8	iKVM							
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	• a Firmware Update	(Min (Admir	inistrator) C Refresh 60 Print 🖝 Logo HEI
Preserve This page allo Click hore to	e Configuratio ws you to select the spe go to <u>Firmware Update</u>	ecific configuration it or <u>Restore Config</u> u	ems to be preserved ration	l in the cases of "Rest	ore Configuration", and "Firmwa	Preserve Configu Restore Configur Reset BMC Reset iKVM BIOS POST Coo	ration e Configuration le	option".	Number of Preserved Items: 0
# Preserve Configuration Item								Preserve	Status
1 0DR									
2				FRU					

4.7.1 Preserve Configuration

This page allows you to select specific configuration items to be preserved in the cases of Restore Configuration and Firmware Update without Preserve Configuration option.

AS	MB8	iKVM						h (marcia	C Referable & Root	100004
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update			HELP
Preserve	Preserve Configuration									
This page allos	is you to select the spec	the computation is	ins to be preserved	In the cases of relation	Conspiration , and Pirminal	e opoate wendut P	reserve Computation option .			
Click here to	go to Einmware Update	or Restore Confe	garation							
									Number of Preserved Its	ems: 0
	Δ			Preserve Cor	figuration Item A			Preserve Status		
					SUR					
					FRU					
3					SEL					
4					PM					
5				N	stwork.					
6					NTP					
7				\$	NMP					
8					SSH .					
9					CVM					
11	0			Auto	intication					
1	1			9	yslog					
								Check All	Uncheck All Save Re	eset

4.7.2 Restore Configuration

This page allows you to restore the default configuration for your device.

Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	• admin (Administrator) C Refresh & Print of Lopout HELP						
Restore Configuration							
This page allows you is notice the instance of the construction for you device. This can allow configuration terms to be preserved by allows "form "Process Configuration". You This task Configuration terms will be preserved and allow terms of the advice							
This section lists the configuration items, that will be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items.							
₽ Δ Preserve Configuration Bren. Δ	Preserve Status 🛆						
Oats Ner Avatable							
Enter Pressive Cardgaration.							

- 1. Enter Preserve Configuration. Click to select specific configuration items to be preserved
- Restore Configuration. Selected configuration items will be preserved while all the other configuration items will be restored to their default values. If none are selected, all the configuration items will be restored to their default values, essentially restoring the device configuration to its factory defaults.

4.7.3 Reset BMC

This page allows you to run cold reset command of the device.

	/
è	

Please note that after entering **Perform Action**, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

AS	MB8	ikvm						
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	admin(Admin Firmware Update	istrator) C Refresh 🐶 Print 🖝 Logou HEL
Reset B	мс							
tun cold rese	t command of the devic	e. Press "Perform A	ction" to reset the de	vice.				
WARNING	c Please note that after (entering "Perform Ac	tion", other web pag	es and services will no	ot work. All open widgets will b	e closed automatica	lly. The device will reset and reboot	within few minutes.
								Perform Action

4.7.4 Reset iKVM

This page allows you reset the iKVM of the device.



Please note that after entering **Perform Action**, other JAVA console and virtual media will not work. All iKVM session will be closed automatically.



4.7.5 BIOS POST Code

The page shows the BIOS POST Code information of the last state.



4.8 Firmware Update

This section allows you to update the firmware of the device, or update the BIOS of the host.



4.8.1 Firmware Update

This page allows you to update the firmware of the device remotely.



Please note that after entering **Enter 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.

AS	MB8	iKVM						C •	
Uashboard	FRU Information	Server Health	Contiguration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		HELP
Firmware Update Itigszef timuse of the decise Press "Press "Press" Press" Press "Press" Press" Press									
VMARINE Process note that after extering the update mode, the weights, other web pages and sensions will not work all the open weights will be automatically rised. If the upgraduation is cancelled in the model of the work of the other weights, the other weights and the other weights and the other weights are approximately an									
# =	7		Preserve Cor	figuration Itom				Procerve Statuc A	
1				SDR				Overwrite	
2				FRU				Overwrite	
3				SEL		Overwrite			
4				IPMI				Overwrite	
5			N	etwork.				Overwrite	
6				NTP				Overwrite	
7			3	NMP				Overwrite	
8				SSH				Overwrite	
9				KVM.				Overwrite	
10	10 Automation Overvite								
11			S	yslog				Overwrite	
							Ent	er Preserve Configuration	Enter Update Mode

4.8.2 BIOS Update

This page allows you to update the BIOS of the host remotely.



Please note that after entering **Start Updating BIOS**, the widgets will not work. All open widgets will be closed automatically.

AS	MB8	iKVM						
Dashboard	FRU Information	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	• ac Firmware Update	min(Administrator) C Refresh V Print Cloqout HELP
BIOS U Upgrade BIO WARNING	Construction of minimum of m							
								Start Updating BIOS

Chapter 4:	Web-based	User	Interface
------------	-----------	------	-----------

Appendix

The Appendix shows the location of the LAN ports for server management and BMC connector on server motherboards. This section also presents common problems that you may encounter when installing or using the server management board.

A.1 BMC connector

The ASUS server motherboards that support the ASMB8-iKVM comes with a Baseboard Management Controller (BMC) connector.

Refer to the illustration below to locate the BMC connector on different server motherboards.



P

The motherboard illustration is for reference only. The motherboard layout and appearance may vary depending on the model.

A.2 LAN ports for server management

The ASUS server motherboards that support ASMB8-iKVM comes with three (3) LAN (RJ-45) ports: one for network connection and the other two for server management.

For easy identification, the LAN ports for server management are Shared LAN and DM_LAN1 ports. You must use the Shared LAN and DM_LAN1 ports for server management to connect the remote server to the local/central host (direct LAN connection) or to the network hub or router.

Refer to the illustration below to identify the Shared LAN and DM_LAN1 ports for server management on some server motherboards.





Refer to your motherboard's user guide for the location of Shared LAN and DM_LAN1 ports.

A.3 Troubleshooting



This troubleshooting guide provides answers to some common problems that you may encounter while installing and/or using ASUS ASMB8-iKVM. These problems require simple troubleshooting that you can perform by yourself. Contact the Technical Support if you encounter problems not mentioned in this section.

Problem	Solution		
The local/central server cannot connect to the ASMB8-iKVM board	 Check if the LAN cable is connected to the LAN port. 		
	 Make sure that the IP address of both the remote and local/central servers are on the same subnet. (Refer to chapter 2 for details.) Try "ping xx.xx.xx.xx" (remote server ip) on local/central server and make sure remote server could reply the ping request. 		
	 Check if the IP source is set to [DHCP]. When set to [DHCP], you'll not be able to configure the IP address. 		
All the SEL (System Event Log) cannot be displayed	The maximum SEL number is 900 events.		
The date/time shown in SEL (System Event Log) screen is incorrect	Refer to section 4.4.9 to check if the time zone is set up correctly.		
ASMB8-iKVM has network connection problems in Firewall environment	Ask MIS to add the following port numbers in Firewall: 5123 (virtual floppy) (TCP) 5120 (virtual CDROM) (TCP) 623 (IPMI) (TCP & UDP) 80 (HTTP) (TCP) 7578 (iKVM) (TCP) 443 (HTTPs) (TCP) 161 (SNMP) (UDP)		
The Java redirection screen cannot be displayed normally	Click Refresh Page button to refresh the redirection screen.		



The ASMB JAVA console only works with the onboard VGA. Other add-on video cards may not properly display the ASMB JAVA console.

A.4 Sensor Table

Memory ECC

Sensor No.	Sensor Name	Sensor Type	Sensor Type code	Sensor Value or Event Type	Event Data 3
0xD1	CPU1_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03:DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B2, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x08: DIMM_C3, 0x08: DIMM_C2, 0x06: DIMM_D1, 0x00: DIMM_D2, 0x06: DIMM_D3, 0x0F: DIMM_D4
0xD3	CPU2_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x08: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x06: DIMM_G3, 0x0F: DIMM_G2, 0x06: DIMM_G3, 0x0F: DIMM_G2, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_G3, 0x17: DIMM_C4

CPU CATERR

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0xDA	CPU_CATERR	Processor	07h	Discrete (6Fh) 0x01: IERR

Memory Error

Sensor No.	Sensor Name	Sensor Type	Sensor Type code	Sensor Value or Event Type	Event Data 3
0xDB	Memory_Train_ERR	OEM Type	0xC5	Discrete (6Fh) 0x01: Memory Train Error	[7:0] - Memory module/device 0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0a: DIMM_C3, 0x06: DIMM_D1, 0x040: DIMM_D2, 0x0e: DIMM_D3, 0x10: DIMM_B1, 0x104: DIMM_B2, 0x12: DIMM_B3, 0x16: DIMM_F1, 0x16: DIMM_F2, 0x16: DIMM_F3, 0x18: DIMM_G1, 0x19; DIMM_G2, 0x18: DIMM_G3, 0x18: DIMM_H1, 0x104: DIMM_A2, 0x1e: DIMM_H3

Backplane HD

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x68	Backplane1 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x69	Backplane1 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6A	Backplane1 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6B	Backplane1 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6C	Backplane1 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6D	Backplane1 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6E	Backplane1 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6F	Backplane1 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x78	Backplane2 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x79	Backplane2 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7A	Backplane2 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7B	Backplane2 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7C	Backplane2 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7D	Backplane2 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7E	Backplane2 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7F	Backplane2 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild

Power Supply

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x81	PSU1 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critical - going high
0x82	PSU1 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x83	PSU1 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x92	PSU1 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x93	PSU1 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x94	PSU1 AC	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x95	PSU1 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x96	PSU1 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x97	PSU1 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected
0x84	PSU2 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critical - going high
0x85	PSU2 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x86	PSU2 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x9A	PSU2 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9B	PSU2 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x9C	PSU2 AC Lost	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x9D	PSU2 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9E	PSU2 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9F	PSU2 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected

Hardware Monitor

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x31	CPU1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x32	CPU2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCC	TR1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCD	TR2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x34	VCORE1	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x35	VCORE2	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x36	+3.3V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x37	+5V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x38	+12V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x39	+1.5V_ICH (For Intel DP platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3A	+1.1V_IOH (For Intel DP platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3B	+5VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3C	VBAT	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3D	P1VTT (For Intel DP platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3E	+1.5V_P1DDR3 (For Intel platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high

(continued on the next page)

0x3F	P2VTT (For Intel DP platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x40	+3.3VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x41	+1.5V_P2DDR3 (For Iniel DP platform only ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	P1DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	+1.5V (For Intel UP platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x43	P2DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x44	P1_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x45	P2_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x46	P1_VDDNB (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x47	+1.8V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x48	+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x49	+1.1V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x4A	VTT (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0xA0	CPU_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low

(continued on the next page)

0xA2	FRNT_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA3	FRNT_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA4	FRNT_FAN3	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA5	FRNT_FAN4	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA6	REAR_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA7	REAR_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA8	FRNT_FAN5	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA9	FRNT_FAN6	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xAA	FRNT_FAN7	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x4F	Chassis Intrusion	Physical Security (Chassis Intrusion)	0x05	Discrete(0x6F) 0x01: General Chassis Intrusion 0x02: Drive Bay Intrusion

ASUS contact information

ASUSTeK COMPUTER INC.

Address Telephone Fax E-mail Web site 15 Li-Te Road, Peitou, Taipei, Taiwan 11259 +886-2-2894-3447 +886-2-2890-7798 info@asus.com.tw http://www.asus.com

Technical Support

Telephone Fax Online Support +86-21-38429911 +86-21-58668722 ext: 9101 http://support.asus.com/techserv/techserv.aspx

ASUSTeK COMPUTER INC. (Taiwan)

Address Telephone Fax E-mail Web site 15 Li-Te Road, Peitou, Taipei, Taiwan 11259 +886-2-2894-3447 +886-2-2890-7798 info@asus.com.tw http://www.asus.com.tw

Technical Support

Telephone Online Support +886-2-2894-3447 (0800-093-456) http://support.asus.com/techserv/techserv.aspx

ASUSTeK COMPUTER INC. (China)

Address

Telephone Fax Web site No.508, Chundong Road, Xinzhuang Industrial Zone, Minhang District, Shanghai, China. +86-21-5442-1616 +86-21-5442-0099 http://www.asus.com.cn

Technical Support

Telephone Online Support 400-620-6655 http://support.asus.com/techserv/techserv.aspx

ASUS contact information

ASUS COMPUTER INTERNATIONAL (America)

Address Fax Web site 800 Corporate Way, Fremont, CA 94539, USA +1-510-608-4555 http://usa.asus.com

Technical Support

Support fax General support Online support +1-812-284-0883 +1-812-282-2787 http://support.asus.com/techserv/techserv.aspx

ASUS COMPUTER GmbH (Germany and Austria)

Address Fax Web site Online contact Harkort Str. 21-23, D-40880 Ratingen, Germany +49-2102-959911 http://www.asus.de http://www.asus.de/sales

Technical Support

Telephone Support Fax Online support +49-1805-010923 +49-2102-959911 http://support.asus.com/techserv/techserv.aspx

ASUS Czech Service s.r.o. (Europe)

Address

Telephone Web site Na Rovince 887, 720 00 Ostrava – Hrabová, Czech Republic +420-596766888 http://www.asus.cz

Technical Support

Telephone Fax E-mail Online Support +420-596-766-891 +420-596-766-329 advance.rma.eu@asus.com http://support.asus.com/techserv/techserv.aspx

ASUS contact information

ASUS Holland BV (The Netherlands)

Address Marconistraat 2, 7825GD EMMEN, The Netherlands Web site http://www.asus.com

Technical Support

Telephone	+31-(0)591-5-70292
Fax	+31-(0)591-666853
E-mail	advance.rma.eu@asus.com
Online Support	http://support.asus.com/techserv/techserv.aspx

ASUS Polska Sp. z o.o. (Poland)

AddressUl. Postępu 6, 02-676 Warszawa, PolandWeb sitehttp://pl.asus.com

Technical Support

Telephone	+48-225718033
Online Support	http://support.asus.com/techserv/techserv.aspx

ASK-Service (Russia and CIS)

Address Telephone Web site г.Москва, ул. Орджоникидзе, д.10, Россия (495) 640-32-75 http://ru.asus.com

Technical Support

Telephone	008-800-100-ASUS (008-800-100-2787)
Online Support	http://vip.asus.com/eservice/techserv.aspx?SLanguage=ru

In of Conformity Science MCREDIBLE	SUSTek COMPUTER INC.	F, No. 150, LI-TE Rd., PEITOU, TAIPEI 112, TAIWAN	SUS COMPUTER GmbH	MRKORT STR. 21-23, 40890 RATINGEN	ERMANY		Aanagement card	ASMB8-IKVM	lowing directives:	EN 55024 2010	EN 61000-3-3 2008 EN 55020-2007+A11:2011		EN 301 489-1 V1.9.2(2011-09) EN 301 489-3 V1 4 1/2002-080	EN 301 489-4 V1.4.1(2009-05)	EN 301 489-7 V1.3.1(2005-11) EN 301 489-9 V1 4 1/2007-11)	EN 301 489-17 V2 2.1 (2012-09)	EN 301 489-24 V1.5.1 (2010-09) EN 302 326-2 V1 2 2(20107-06)	EN 302 326-3 V1.3.1(2007-09)	EN 301 357-2 V1.4.1(2005-11) EN 302 291-1 V1.1.1(2005-07) EN 2020 201 201 2005-07)	EN 302 291-2 V1.1.1(2005-07)		EN 60065 2002 / A12:2011		Regulation (EC) No. 278/2009	Regulation (EC) No. 617/2013	Ver. 140331		(EC conformity marking)	Bosition · CEO	Name: Jerry Shen	$\left(\right)$	A lens		Signature :		
EC Declaratio	We, the undersigned, Manufacturer:	Address: 4	Authorized representative in Europe: A	Address, City: H	Country: G	declare the following apparatus:	Product name :	Model name :	conform with the essential requirements of the fol	X2004/108/EC-EMC Directive	EN 550132001+A1:2003 EN 550132001+A1:2003+A2 2005	1999/5/EC-R&TTE Directive	EN 300 328 V1.7.1 (2006-10)	EN300 440-2 VI.4.1(2010-08)	EN301511 V9.0.2(2003-03)	EN 301 908-2 V5.2.1(2011-07)	EN 301 893 V1.6.1 (2011-11) F EN 302 544-2 V1 1 1/2004-01)	EN 302 623 V1.1.1(2009-01)		EN 50385 2002 EN 62311 2008	2006/95/EC-LVD Directive	EN 60950-1 / A12.2011	20 09/125/EC-ErP Directive	Regulation (EC) No. 1275/2008	Regulation (EC) No. 642/2009	X2011.65/EU-RoHS Directive	SCE marking						Declaration Date: 09/05/2014	Year to begin affixing CE marking: 2014		

DECLARATION OF CONFORMITY Per FCC Part 2 Section 2. 1077(a) Responsible Party Name: Asus Computer International Address: 800 Corporate Way, Fremont, CA 94539, Phone/Fax No: (510)739-3777/(510)608-4555 Phone/Fax No: (510)739-3777/(510)608-4555 Prove/Fax No: (510)739-3777/(510)608-4555 Prove/Fax No: (510)739-3777/(510)608-4555 Prove/Fax No: (510)739-3777/(510)608-4555 Phone/Fax No: (510)730-2007 Phone/Fax No: (510)730-2007 Phone/Fax No: (510)730-2007 Phone/Fax No: (510)730-2007 Phone/Fax No: (510)730-2007 Phone/Fax No: (510)730-2004 Phone/Fax No: (510)730
--