

Server Management Board

E8098

First Edition V1 March 2013

Copyright © 2013 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

Notice	s	vi	
Safety	, informa	tion viii	
About	this gui	de ix	
ASMB	7-iKVM s	specifications summaryxi	
Chap	ter 1:	Product introduction	
1.1	Welcon	ne!1-2	
1.2	Package contents1-2		
1.3	Features 1-3		
1.4	System requirements1-4		
1.5	Networ	k setup 1-5	
Chap	ter 2:	Installation	
2.1	Before	you proceed2-2	
2.2	Hardwa	are installation2-2	
2.3	Firmwa	re update and IP configuration2-4	
	2.3.1	Firmware update2-4	
	2.3.2	Configure BMC IP source static IP2-6	
	2.3.3	Configure BMC IP source DHCP 2-7	
2.4	BIOS c	onfiguration2-8	
	2.4.1	Running the BIOS BMC configuration2-8	
	2.4.2	BMC network configuration 2-8	
	2.4.3	System Event Log2-10	
	2.4.4	IPv6 BMC Network Configuration2-11	
2.5	Runnin	g the ASMC7 utility2-13	
	2.5.1	Configuring the LAN controller2-15	
	2.5.2	Configuring the user name and password 2-16	
Chap	ter 3:	ASUS Host Management Controller Set-up	
3.1	ASUS H	lost Management Controller Setup 3-2	
	3.1.1	Installing and launching the ASUS Host Management Controller Setup utility	
	3.1.2	Command fields	
	3.1.3	Initial	
	3.1.4	View	
	3.1.5	Set	

Contents

	3.1.6	Monitor	3-8
	3.1.7	Help	3-9
Cha	pter 4:	Web-based user interface	
4.1	Web-ba	ased user interface	4-2
	4.1.1	Loging in the utility	
	4.1.2	Using the utility	
4.2	FRU In	formation	
4.3	Server	Health	
	4.3.1	Sensor Readings (with Thresholds)	
	4.3.2	Event Log	
4.4	Config	uration	4-6
	4.4.1	Active Directory	
	4.4.2	DNS	
	4.4.3	LDAP	
	4.4.4	Mouse Mode	4-12
	4.4.5	Network	4-12
	4.4.6	Network Bond	4-13
	4.4.7	NTP	4-13
	4.4.8	PEF	4-14
	4.4.9	RADIUS	4-21
	4.4.10	Remote Session	4-21
	4.4.11	Services	4-22
	4.4.12	SMTP	
	4.4.13	SSL	4-23
	4.4.14	Users	4-28
4.5	Remote	e Control	4-30
	4.5.1	Console Redirection	4-30
	4.5.2	Server Power Control	4-38
	4.5.3	Chassis Identify Command	4-38
	4.5.4	Power Button	4-39
4.6	Mainte	nance	4-40
	4.6.1	Firmware Update	4-40
	4.6.2	Restore Factory Default	

Contents

Арр	endix: Reference information	
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
ASU	IS contact information	1

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 http://csr.asus.com/english/REACH.htm.

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 <u>http://csr.asus.com/english/Takeback.htm</u> 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: Installation

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 (ASMB7-iKVM only)

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

Appendix: Reference Information

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 make sure 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></key1+key2+key3>	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+).
	Example: <ctrl>+<alt>+<d></d></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 the DOS prompt, type the command line: format a:

ASMB7-iKVM specifications summary

Chipset	Aspeed 2300
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.



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



1.1 Welcome!

Thank you for buying an ASUS® ASMB7-iKVM server management board!

The ASUS ASMB7-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 ASMB7-iKVM plugging in a 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 ASMB7-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

* A power supply supported PMBus and PSMI is necessary.

** Specifications are subject to change without notice.

1.4 System requirements

Before you install the ASMB7-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 the ASUS website (www.asus.com) for an updated list of server motherboards that support the ASMB7-iKVM.

** See the Appendix for details.

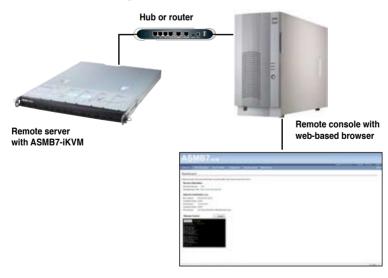
1.5 Network setup

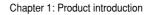
The ASMB7-iKVM server management board installed on the remote server connects to a local/central server via direct LAN connection or through a network hub. Below are the supported server management configurations.

Remote server with ASMB7-iKVM

Direct LAN connection

LAN connection through a network hub





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.



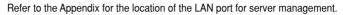
2. Orient and press the Management Card in place.





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.



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.

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



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

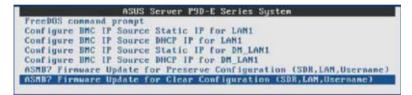
2.3 Firmware update and IP configuration

You need to update the ASMB7-iKVM firmware and configure IP source before you start using the ASMB7-iKVM board.

2.3.1 Firmware update

To update the firmware:

- 1. Insert the support CD into the optical drive.
- 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, the main menu appears. Select **ASMB7-iKVM Firmware Update** for Clear Configuration, and press <Enter> to enter the sub-menu.



6. A confirmation message appears, asking whether you want to update the firmware or not. Select <Yes> to update.



The firmware updating process starts.

7. When the update process is completed, the following screen appears.

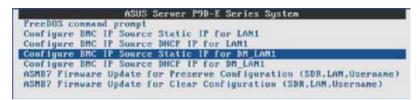
Preserving Enu Variables... done Uploading Firnware Image : 100%... done Flashing Firnware Image : 100%... done Verifying Firnware Image : 100%... done Setting Enu variables ... done Resetting the firnware..... Please wait for 70 seconds to initialize firnware Delay 70 Seconds Press any key to continue



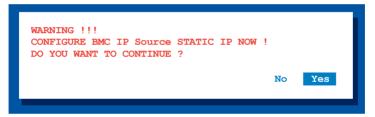
You may update firmware from the web-based user interface. Refer to page 4-13 for details.

2.3.2 Configure BMC IP source static IP

- 1. Repeat the step 1-4 in the previous sub-section.
- On reboot, the main menu appears. Select Configure BMC IP Source Static IP for LAN1 (or DM_LAN1), and press <Enter> to enter the sub-menu.



3. A confirmation message appears, asking if you want to configure the BMC IP source static IP now. Select <Yes> to continue.



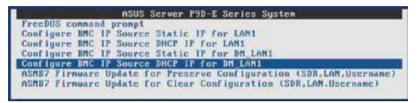
4. When the configuration is completed, the below screen appears.



5. Go to BIOS menu to set the IP. Refer to section 2.4 for IP settings in BIOS menu.

2.3.3 Configure BMC IP source DHCP

- 1. Repeat the step 1-4 in the previous sub-section.
- On reboot, the main menu appears. Select Configure BMC IP Source DHCP for LAN1 (or DM_LAN1), and press <Enter> to enter the sub-menu.



3. A confirmation message appears, asking if you want to configure the BMC IP source DHCP now. Select <Yes> to continue.



4. When the configuration is completed, the below screen appears.



5. Then you can get IP from DHCP server.

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.



- 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

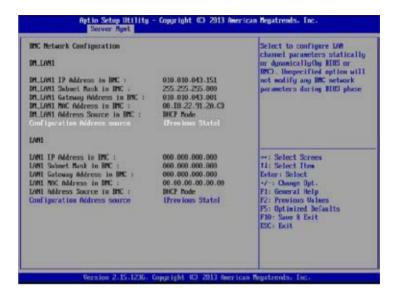
To configure the BMC in the BIOS:

- 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.





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.



SEL Components [Disabled]

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



The following items become configurable when you set **SEL Components** to [Enabled].

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.

Aptio Setup Utility – Nein Advanced Server Ngmt Event	Copyright (D) 2011 America Logs Boot Monitor Secur	
ENC Firmware Version : OS Hatchdog Timer OS Hitd Timer Timeout OS Hitd Timer Policy > Dysten Event Log > ENC Hetwork Configuration > Thys ENC Network Configuration	1.08 [Disobled] [Cominutes] [Reset]	Configure IPV6 BHC network parameters
Aptio Setup Utility - Server Hemt JPv6 EMC Network Configuration	Copyright (C) 2011 American	Select to configure LAN channel parameters statically
IPv6 EMC DALLANT: DM_LANT IP Address in EMC : -> 2002:108:01F101: DM_LANT Prefix Length in EMC : DM_LANT Bateway Address in EMC : -> 010:010:010:010:01 DM_LANT MAC Address in EMC : IPv6 EMC Mathematical in EMC : IPv6 EMC Mathmatical in EMC : IPv	64 00.E0.18.65.00.30 DHCP Made	or dynamicslly(by 8305 or 896)

IPv6 BMC DM_LAN1 IP Address Source [Previous State]

2002:DBB:0:F101:0:0:31:4049

2 14 1219 Dopumidht (C)

0:400:0:0:0:B0A1:3940:0

Lant MAC Address in BMC : 00.00.00.00.00.00 Lant Address Source in BMC : DHCP Mode JPV6 EMC Lant IP Address Source (Previous State)

Lani Prefix Length in BMC : 100 Lani Gateway Address in BMC :

->

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]

F1: General Help

F10: Save & Exit ESC: Exit

F2: Previous Values F5: Optimized Defaults



The following items are available when you set IPv6 BMC DM_LAN1 IP Address Source to [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 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 Lan1 IP Address Source to [Static].

IPv6 BMC Lan1 IP Address

Allows you to set the IPv6 BMC Lan1 IP address.

IPv6 BMC Lan1 IP Prefix Length

Allows you to set the IPv6 BMC Lan1 IP Prefix length.

IPv6 BMC Lan1 Default Gateway

Allows you to set the IPv6 BMC Lan1 Gateway IP address.

2.5 Running the ASMC7 utility

The ASMC7 utility allows you to update the ASMB7-iKVM firmware, configure the LAN setting 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 ASMC7 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.
- 5. On reboot, the main menu appears. Select **FreeDOS command prompt**, and then press <Enter> .



 When the c:> prompt appears, type ASMC7 -?, then press <Enter> to display the ASMC7 Utility Help Menu. The screen appears as shown.

nsus	Server Management Card Utility 7.00 Help Menu
sage:	
	-kcs[snic/bt/pci_snic] NetFn command data
	-bmc_ip_source source[1:Static, 2:DHCP]
	-bmc_ip_ip_addr[10.10.10.20]
	-bnc_nask (p_nask[255.255.255.81
	-bnc_gateway ip_addr[10.10.10.254]
	-ipv6_source source[1:Static, 2:DHCP]
	-ipv6_ipv6_addr[2001:0db8:1234:5678:8769:e1cb:aabb:ccdd] -ipv6_prefix_prefix_length[64]
	-pet_ip_mac_ip_addr[18.18.18.28] mac_addr[818283848586]
	-bmc_ip_s_lan1_source[1:Static, 2:DHCP1
	-bnc_ip_lan1_ip_addr[18.18.18.28]
	-bmc_mank_lan1 ip_mank[255.255.255.8]
	-bmc_g_lan1 ip_addr[10.10.10.254]
	-ipv6_s_lan1 source[1:Static, 2:DHCP]
SHC7	-ipe5_lan1_ip_addr[2881:84b8:1234:5678:8769:e1cb:aabb:ccdd]
	-ipv6_prc_lan1 prcfix_length[64]
SHC7	-pet_ip_m_lan1_ip_addr[10.10.18.20] mac_addr[818283848586]

Press any key to see next page.

(Press any key to see the next page) (ESC key to break)
ASHC7 -adm_name_new_name_string
ASMC7 -user_name_new_name_string
ASHC7 -adm_password new_adm_password
ASMC7 -user_password new_user_password
ASHC7 -sol_baud 57688[9688/19288/38488/57688/115288]
ASMC7 -bmc_info
ASHC7 -fru -view fru_id
ASMC7 -fru -load fru file
ASMC7 -fru -save fru_id fru_file
ASHC7 -sel -clear
0:55

ASMC7 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 connection to the ASMB7-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 ASMC7 utility from the support CD following the instructions in the previous section.
- 2. Set IP source:
 - (a) Type ASMC7 -bmc_ip_source 1 if you want to set a static IP address.
 - (b) Type ASMC7 -bmc_ip_source 2 if you want to get IP from DHCP server.
- Type ASMC7 -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:\>ASMC7 -bmc_ip 10.10.10.243
Detect MotherBoard -> (29PE-D16 Series)
Detect KOS 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 (a) subnet mask and (b) gateway address if necessary.
 - (a) Type ASMC7 -bmc_mask xxx.xxx.xxx (your subnet mask encoded in hexadecimal system)
 - (b) Type ASMC7 -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 ASMC7 utility.

To change the user name and password:

- 1. Follow steps 1-5 on page 2-11.
- 2. When the C:> prompt appears, type ASMC7 -user_name xxxxx, then press <Enter> to change the user name.



- 3. Type ASMC7 -user_password xxxxxxx, then press <Enter> to change the password.
- 4. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.

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

ASUS Host Management Controller Set-up

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.
- 2. At the prompt, type **ASMC7**, then press <Enter> to display the ASMC7 Utility Help Menu. The screen appears as shown.

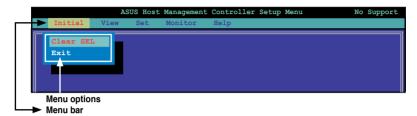


3. The main utility screen appears. Press <Enter>.



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.

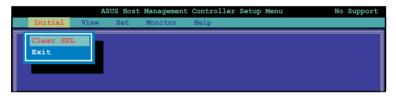


3.1.3 Initial

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):

1. 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 Host M	Management Controller Setup Menu No Su	npport
Initial View Set	Monitor Help	
Systen Event Log: (Hex) 01 00 02 09 4E 98 45 20 00 04 02 3A 01 50 19 09 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 (Threshold) Event Datal : 50h Event Value : 19h (0.2 v) Threshold : 09h 1.0 v) Offset: Lower Non-critical - going low	,
↑↓►4: Select Menu ESC	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.

Initial View Set M	onitor Help
Sensor Data Record: (Hex)	Record ID : 0001h
	SDR Version : 51h
01 00 02 09 4E 98 45 20	Record Type : 01h (Full Sensor Record)
00 04 02 3A 01 50 19 09	Owner ID/Lun : 20h/08h
	Sensor Number : 31h (CPU1 Temperature)
01 00 02 09 4E 98 45 20	Sensor Initial: 7Fh
00 04 02 3A 01 50 19 09	Capabilities : 68h
	Sensor Type : 81h (Temperature)
01 00 02 09 4E 98 45 20	Event Type : 01h (Threshold)
00 04 02 3A 01 50 19 09	Assert Mask : 0280h
	Deassert Mask : 3200h
01 00 02 09 4E 98 45 20	Reading Mask : 1010h
00 04 02 3A 01 50 19 09	Nominal Read : 20h (40 °C)
	Upper Critical: 50h (80 °C)
	Upper Warning : 50h (80 °C)
1/28	Lower Warning : 18h (24 °C)
	Lower Critical: 18h (16 °C)
	ID String : CPU1 Temperature

- 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.

	Aggement Controller Setup Menu No Support mitor Relp Device ID : 20h Device Revision : 01h (No SDR) Firmware Revision : 1.04 IPMI Version : 2.0 Manufacturer ID : 001043h Product ID : 0043h IPMI Device Support Chassis Device -> Support IPMB Event Generator -> Support IPMB Event Generator -> Support IPMB Event Generator -> Support SDR Repository Device -> Support SDR Repository Device -> Support Sensor Device -> Support
↑↓►4: Select Menu ESC: 1	Exit Up/Down KCS

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.



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>.

	AS	US Host	t Management	: Controller Setup Menu	No Support
Initial	View	Set	Monitor	Help	
		-	Set Host	Interface	
			[] BT [] PCI	Interface Interface Interface Interface Interface	
↑↓ ▶ ∢: Se	lect Mei	u Es	SC: Exit	Up/Down	KCS

You can select from the following interfaces:

KCS Interface	-	Keyboard Controller Style
SMIC Interface	-	Server Management Interface Chip
BT Interface	-	Block Transfer
PCI Interface	-	Peripheral Component Interconnect
KCS2 Interface	-	Keyboard Controller 2 Style

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.

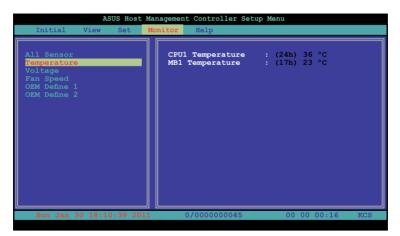
3.1.6 Monitor

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

			ment Controlle:	r Setup Menu	No Support
Initial V	iew Se	t Monito	er Help		
		Tem Vol Fan OEM	Sensor perature tage Speed Define 1 Define 2		

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.



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

3.1.7 Help

The **Help** command displays the available utility options, utility version, and copyright information.

	AS	SUS Host	t Management	Controller	Setup Menu	No Support
Initial	View	Set	Monitor	Help		
				Help About		



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 ASMB7-iKVM support CD. You can also download JRE from <u>http://www.oracle.com/</u>technetwork/java/javase/downloads/index.html

4.1.1 Loging in the utility

- 1. Ensure that the LAN cable of the computer is connected to the LAN port of the remote server.
- 2. 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.

ASMB7 avve	
	And a second sec

4.1.2 Using the utility

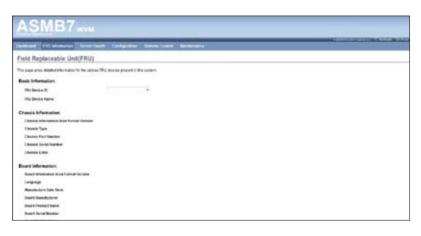
The web-based graphics user interface displays when you login in the utility successfully.



- 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.



4.3 Server Health

This section contains the data related to the server health, such as the Sensor Readings, Event log and System and Audit Log. Click each function key to start using its specific functions

	Annual Research in	aller Berris Looks	C. Buddener	
lensor Readings	1.00110	A NAMES AND A COLUMN	No be wight to be particular server	Inter Oast II
workers a	AND A	Local braining in	and the second second second second	
CPUT Tense dure	20214	6810	CPU1 Temperature: All * C	Tel State St
W) Technologie	for hubble	Ted Automa	Charl Indexes in C	
All Targer date	nome	30°C	Threadwalls for this context	LAS DRUGT 12
Pullarie	Roma	1010		
00841	TUT B	1.008 11/10	Loss the Assessment LIME 211	Associate Restances (200): 4
1.81	NOTIA	100048	100000000000 010	Uniter California (UC)
121	10114	11,004,1088	Leventile Onited LPCD 1110	Same New United Article
év .	tooma .	8.121498		
5.2/	1000	3.312 9.992		
3.55	some	2.429 1989	- STRATINER YORK OF \$10 DATING TO BUSINE	
647	hores	1294 1010		
20,144	home .	2116 104	144 (st)	
10.7 (1.00)	That Avenue he	TER hallofter	144.141	
107,740	NO NORMA	Tel Automation	10.000	
187,746	tores and the second se	2540.00%		
extrait	multiplications.	168 Audidia	VK.00	
SPU1_8004	Presence Sender(0.0140	144 101	
Portators	All descendent	0.800	CO2 2011	
10Pine	Toma	Tel Auditor	wt 241	
Tablifiethe	Saverol Channis Mexicon	5-8001	UNC ID	
ukangi R Cauciller	All Reported	018300	and the second sec	
	Tapported .	- Sawini	Direc (0)	

4.3.1 Sensor Readings (with Thresholds)

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

mark 191 Mar	will be a half [] and a	term being (see	11 1 1 1 1		
ensor Readings					
lance and the same	and the last of the local division of the last of the	a month in such that and	The to originary full patients cannot		
- 100				terms internal difference	
Put Serve day)-2	al 12 Introduction	CPUT Temperature: 481C	10.000 No.000	
and forugenetics	terns .		Threadwards for this annual	Los Minut In 128	
(10) dege (10) (10) (10) (10) (10) (10) (10) (10) (10)	1111	101-1 100 color 1100 color 1100 color 1100 color	Law Website UK	tan horizotti tan horizotti tan horizotti	
039 039 847 932 (Mal)	111	100 MR	Barrisk Decid Dis World Aren		
Ball/Aust Ball/Aust Ball/Aust	test replaces	Not had state			
eat, ner her jaar	Instrumente Processo de l'Adresso Al Consecutivo	Total Lawrence	14 00 18 00		
Normal Street	Served Steam (Band)	na saran adar	-		
All Calculations	Taken and	Sauce .	100 m 100		

- 1. Select a sensor type category: Allows you to select the type of sensor readings to be displayed in the list.
- 2. **Status List:** Show the type of sensor readings list that you selected in the drop-down list.
- 3. Live Widget: 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.

and a local difference of the second s		- Forgante Room Control Mi		
			92	ent La
		water of the or a recently said incorplice	the locks in the locks of the light from I	th process
Areas Lag. 1			* monto: All Terrory	Carlo
90.00			States I was been and	and fun
1.000	and an a second s	Contract Contract of Contract		CL.M.M.
a Song Live , Deanselled		2PU_Feet	000000411407708	1
olgi ov. Contraftet		05,794	0140020413-14227-08	
# Line Hpl. Dearstell		CPUT factorisation	6448029FT 1527-06	
Jacquing) Generative		UPUT Rempension	exercised a reaction	
sector and		CPUT Temperature	0406041343610	
a Graphly Arentes		(Prof Temperature)	2545543943-4138-A0	
olgiule Accelet		OPUL/HWT	00000013100000	
a - Dempson - Helefer		OPUTING	contraction of part of	
a longine beauves		1988,140	0000000111020.00	
regine Dosaytes		Plant, March	Annual trabes	
stgi-se Assellet		1965,540	00000001 10 00 M	
a lineire menter	14	- PHE, END	00000041100810	

- 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.

4.4 Configuration

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

NAMES AND ADDRESS OF TAXABLE PARTY.	-	Server (1983) (Rothern a	and the second se
Active Directory Settings	A conclusion of the	10 C	
	-		
te labe benny to narwith matted in another	-	and other than to an in the	
ta i al parca de cara de la sel producer finis (a anfinis la cal	-	a he mining a constant of constances, a new place cance in the last and press Califie Post Docar or the	di Ten Inaz fa ati sana Ten Inaz ante ar ancedarati si
		5	Terter Partyrold
	1	Englished as	- Brief Street A.C.
and sold as a second		And the second se	
1	-		
1	Annes Income		# # 2
	Access New York		1
	Anna anna anna anna anna anna anna anna		*
	1 tel		1

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.

nd gant sollar "Sandton Tatour Labbugs 10 Januar House, the carend latt of soully ad press insplayer Group	and have been defined and the bolies of	r haaffi is oo goog awaatto kare isha aa jaa paa laasi ka	e beingene beselft ficker Groupe Fil antil and	
	panel from (inspect of your would fine it from a	a mandie is name general and well that have in the case in the provinci have in the		
				transmitter 5
	and the	Read and Applied 7		the state of the s
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
				+
		-		
			Address and	

- 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.
- 5. 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.

Adhie Directory Authentication	(2) Bruise	
Dare Domain Name	anus com	
fime Out	130	
Demon Contralier Server Address1	13.10.192.2	
Semain Contralier Server Address2		
Dertain Controller Server Address3		

- 2. In the Active Directory Settings Page, enter the following details.
- 3. 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.

- 4. Specify the Domain Name for the user in the User Domain Name field. e.g. asus.com
- 5. Specify the time (in seconds) to wait for Active Directory queries to complete in the Time Out field.



- 1. Default Time out value: 120 seconds.
- 2. Range from 15 to 300 allowed.
- 6. Configure IP addresses in **Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3.**
- 7. Click **Save** to save the entered settings and return to Active Directory Settings Page.
- 8. 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.

Add Role Ordup		0
Rute Group Name Rute Group Domain		
Hare Group Previoge	Administrator	
		Acit Carcel

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



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



- 1. Domain Name is a string of 255 alpha-numeric characters.
- 2. 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.



4.4.3 LDAP

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

SMB7.	term berth	1000 C	
AP Settings			1
Contract Line Street Street Street	or internet beings laker		. Advector
	origentifies lines if recently burn more a realist	a na gag and to land a belief advanced and that they wide the	e Group To est a revellate Group saled an uncellipsed of
ia interationale de carectile d'a Rob linea	adgangilipa linas dina analisia ti dang a mada	a na pag-antida iang ole in gelana (lang bis bag-aikat la	el Grup, To pet a rea Gale Grup, sati el ar una Agussi sa Nortes el contactori
ierona monte contra en Anticia	en para l'an la casa de casa d	a ma gaugo prainte la rato de la anteces Case Rea Seugo visant la	e Grup. To set convibite Grup satie ar unantyprotes Nution of configuration
interne pour la contra a la contra d	elgentillen Drugt Frei andri brit dette arteko	ante productivo sura ordeningativos (Soliti Das Song voluti) for	e Group. To set a new Gale Group, solid an uncerty and a Norther of configuration Norther of configuration
in inter more the sector de Reference	elgensföre bruck forst and best and a stade	n an gun ann an Anna Anna Anna Anna Anna Anna	e Grue, To est constant de Grue center e vouetquere s Nutres et constante en la constante de Constante e e
	ntgantilite inge ken en de ken e nok	a na pagi analifa sara niyota dayan Gant Kati Sana niyota k Kati Sana Sana Kati Kati 	er Group. To set a sever flats Group part of an uncertigential Normen di contegetori I di C
And Design of the second of th	elgandina ing kawani kata ana a saka	a da para attability una un kain aktyoni Data Bata Sura visuata Ba Anna para da para da mana da mana A da mana da ma	e Sraa, Tu pit oone Gin Sang, pant ar woodgordga Kurtop it oolgaaled

1. **Advanced Settings**: To configure LDAP Advanced Settings. Options are Enable LDAP Authentication, IP Address, Port and Search base.

- 2. 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

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

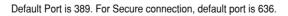
Advanced LDAP Settings		0
LDIP Juthertication	(?) Castle	
# Address	10 16 102 1	
Peri Send CR4	309	
bind CN4	chrisdmin aurilagin doridoman dzir	
Patoword		
Swarth Reve	er-valnin su-lagir de-dovaid	
		Sime Concel

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



- 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.



- 1. Search Base is a string of 255 alpha-numeric characters.
- 2. 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**.

4.4.4 Mouse Mode

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



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

4.4.5 Network

The Network page allows you to configure the network settings.

ASMB7		
Summer (Mildurane) News	and Inclusion Research Manager	
Network Betlings		
Stream report antique attention		
Littlemethics	Inclusi -	
Link Summer	2 ton	
that believes	W 85.00 V 34.00	
Publisher .	to Patrice and the	
Name of Pathons around the	21 inclusion	
(Politications	16/16/2011/07	
Subject Name	-10 10 21 10 ²	
Indust Lawrence	10.000	
Publication		
and Settings	If many	
(from in if without unstantially	E matern	
Web Andrews	The second second second second second	
Same Folg ingth	18	

- 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.

4.4.6 Network Bond

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



4.4.7 NTP

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



4.4.8 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.

Contraction of the local diversion of the local diversion of the local diversion of the local diversion of the	Contraction of the local division of the loc	Very state of the second state		
	ter het het falgerie here	Card Montena		
CF Management				
the page is contact that	The last hand and in Destants. "I land a fast	A handle, period him for he had period. These	or Wandly To and a contract (solid an arrand party of	and prove liked
1	And Total			
and a state of the	**************************************	3	4	5
				Approx 1 and 1 day cause 1
	Example	year a	Chaptering 1	Conception of the local division of the loca
	Dame	100	interesting.	
14			-	1.4
				-
			+)	
18				
27				
16				
14				
28			*	+
18				
17.				
28				
18				
m				678
		1.1	2.1	
- M.			(h)	
				(ed)

- 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.

ASMB7	IKVM			
shboard FRU Information	Server Health	Configuration	Remote Control	Maintenance
odify Event Filter er	ntry			
a his manufacture in solutions of	Caref Elling and Chief	discount in second in	a madification	
se this page to modify the existing E	Event Filter entry. Click	k Nodily to accept t	e modification.	
Event Filter Configuration		k Modify' to accept th	e modification.	
Event Filter Configuration	1		e modification.	
Event Filter Configuration PEF ID Filter Configuration	1 (2) E	nable	e modification.	
Event Filter Configuration	1 (2) E		e modification.	
Event Filter Configuration PEF ID Filter Configuration	1 (2) E	nable	e modification.	

- 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.

Manager		an Longorous Anno 1999 (1999) " An	_		
		Landon The			
and the second s					
to table a couple	e Last Max Mail Taky -	end Life Descention. To make a rough plans, aread it a fer-	beland group "School" as "Bookly". To add a here write part	The second part of and pass full	
Cost Nor	And Parks	LARDANIAN			
				1 diameter	cast baint francis in
		Particular and a second se	Trade Lot or		
1	1.0				
	-	1000 - 10000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1000 - 1		1.1 1.1	
		10			-
		4 : 6 : 14			+
		4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1			
		4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1			*
		4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1			

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

- 1. **Policy Entry #:** Displays Policy entry number for the newly configured entry (read-only).
- 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. **Channel Number:** 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		
Paica Sally #	3	
Paiko Nember	1 -	
Peiks Contiguiston	[]] Leastle	
Parky Sel	a .	
LAN Interface	OM_LAN1 +	
Destivation Selector	1	
Aunt string	🗐 Event DoepHo	
Alast Shiraj Kay	a •	
		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** as shown in the screenshot below.
- 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 **Channel Number field**, choose particular channel from the available channel 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. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th 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.

	The second		
	term balls. Terligences Ball Space Could Reserve		
Management			
to papele configure free thinks	enthis actual Celtain Trans conditions, and for tenant per 5	where its "month". To and a new web, animal as property and and another in the	
Destiller Hel?	ity LM Destrator		
And a local data in the local data	•	I undependent (Add Terration	
and the second second			_
4			-
	-		
1	1		
	1		

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:

Lod LAN Destination entry		
LAN Charriel Number	1	
LAN Deale allow	3	
Destination Tree	Sneep Teop +	
Decimation Address		
Osemanie Message	anceptrata +	
Mexage		

- 1. 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.



NOTE: 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**.

4.4.9 RADIUS

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



4.4.10 Remote Session

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

ASMB7	IIIM	Notice and the second s	
Summer Petrolemane	forest in	Anne Terrational Statements Sciences	
Configure Remote Ses	aine		
The belowing system and a matrix of		the final state for the cost estimates and any	
-	12 mater		
Balla Contaction	(C) basine		
Contrast Names (street) Binds	Lingent .	8	
11-400-1200-1200-1200-1200-1200-1200-120			
			(dee) (deet)

- 1. **KVM Encryption:** Enable/Disable encryption on KVM data for the next redirection session.
- 2. **Media Encryption:** Enable/Disable encryption on Media data for the next redirection session.
- 3. Virtual Media Attach Mode: Two types of VM attach mode are available:
- Attach Immediately attaches Virtual Media to the server upon bootup. (The option is for local F/W Update using.)
- Auto Attach Attaches Virtual Media to the server only when a virtual media session is started.
- 4. Save: To save the current changes.



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

5. **Reset:** To reset the modified changes.

4.4.11 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.

	Manager Street Street	Induces Base Land				
Nint .						
	in any other MC transies	whether and the real the take and	the owner. Innet a stription in	water haden is marely the second of	offgatalise.	
						Sector of
2	Section 1	and a	-	44	100	
-	847	athe	late	And Yose	-	
-	of cashs		a num	150		
-	to reals	indiat	11.67			
-	don-market	1004	8745	10°		
· · · · ·	446	100		40		
1	and all	the first	÷.			

4.4.12 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.

	Safe (adquere New jobs) Retaining
	anjana -
Jan. Jan	

4.4.13 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.



- 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.

the same the day is a first of the logistic case the same	Second South Lineage stice 18	and install Burgers	
Certificate Cards	preation		
min methodes in a	residences and the interaction has been a	state property a signal raise initial tax, part a second	
Colored Contribution	Transfer, 9 86 (6) 81 (910)		
teres from the pro-		Manage	
	Thursday, A standards maint		
Cancella Privaria Nets			

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

- 1. **Current Certificate:** Current certificate information will be displayed (readonly).
- 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.

ASMB7	kim i		
Samburg 100 menuto	a server for		Tanan Cost Manuary (1974) Bird State Annual
SSL Certificate Con	figuration	1	
The approximation of the second secon	L samples and the	AND LONG THE ROOM	with dentise accessed it is securitineed. Laboral 2014, aption is convert access to confluence provide tax, for one has block. Descende 2014, aprile a solution or confligues the calculated 2014, confliction in models format.
Uppent Ditt. Ger	nem 10.	Viet 10.	
Careton Renal IX			
Organizme():			
(April - ample			
face at Province(17)			
Could be a could be could be could be a could be a could be a could be a coul			
veictor		-	
day (angle	310	18 m	

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.
- 3. **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.

SMB7 IKW	
and residences line	Field Industry Associated Statement
L Certificate Configurati	on
ange in aantich serfigung 100, samilaan a ana ika 170, sadiktaile baaan in samijaa	en der 1841 Lang bei der Beland an im anstand die anstand mehr Lätter bil Langen in Langen in Der auf bei Lätter bil and der Beland bei der Be
Uppener EDE. Gammerten 100.	Shew 108
anic information	
Versee.	
Serial Notice	8156264862
Reporters Digestree	of a Const Sub-state to a Sub-st
Pathe Say	(rije m)
named From:	
Common Rankell No.	-
(representation)	Innerson Reparents Int
Organization (million)	Service Production

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.



- 1. Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- 2. 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>
- 3. For example, if your MegaRAC® SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30
- 4. Please note the <s> after <http>.You must accept the certificate before you are able to access your Generic MegaRAC® SP.

4.4.14 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.

and Antonio Sector (agent) Antonio a Antonio							
1 2 3 4 5 6 m							
	2		4				
4.	processo	(heated	construction of the	Property.			
*	10100	Evaluat	Aproxidador .	directed.			
×							
*							
					- 4		
					5.1 *		

- 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.
- 9. 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.
- 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.

4.5 Remote Control

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

ASMB7	
Samer (1910) and a first targets (hear from (because)	
Constanting Handlerschinen Inner Streader State (Streader Streader	
[Set Sees.]	
	5.05 +

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.



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
- Help

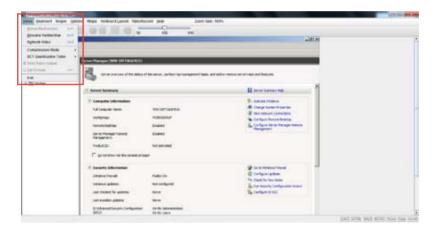
A detailed explanation of these menu items are given below.

+			Altis	
	of Tanana (MIN (011084/871)		9	
1	5	terenari pertent har namagement hala, an	whe must provide and balance.	
2	Server Servers		II to a Longer and	
	 Computer Information Marcos Dealings The Dealings on the present article 	nthrannanta matuntur Jawai matan harannat	 A statege matter B statege transit i kan m 	
	 Security Education 	Nato in Antonigant Anton Bank Lik Managaman China Antonia	E La la repuer trave E color a suban No Color travelar E color travelar E color travelar E color travelar E color travel	

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 Off Host display:** If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.
- 5. **Full Screen:** This option is used to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are same.

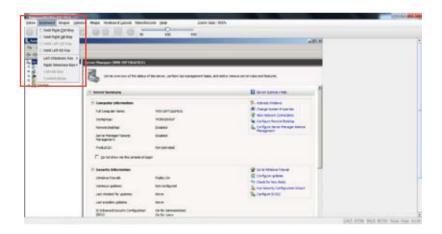


6. **Exit:** This option is used to exit the console redirection screen

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.
- 2. **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.
- 5. 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.
- 6. **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.



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 synch. Please detect the first reading on which cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold value.

			aldia	
1	Conservation of the second	file anno carlleri la tangatori lain, ari		
	- Server Servers		I martineres	
	Computer Information Vol Longuter terms information Means Statistics incompanying and terms instatistics instatistics instatistics instatistics	nticarranta valuator Salant Salant Na salanta	P. Antere means M. Dage to send to text T. This state of constant S. Configure to an interact S. Configure to an interact S	
	6 Security Education Strategy Provide Contract galaxies and Strategy For particular and Strategy For particular and strategy For particular	Fulle In An Arrigand Ann	Link Information Configuration Conf	

Options

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

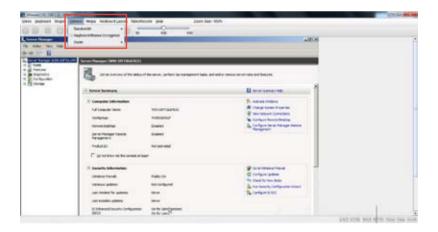
- 1. Auto Detect: This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
- 2. 256 Kbps
- 3. 512 Kbps
- 4. 1 Mbps
- 5. 10 Mbps

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

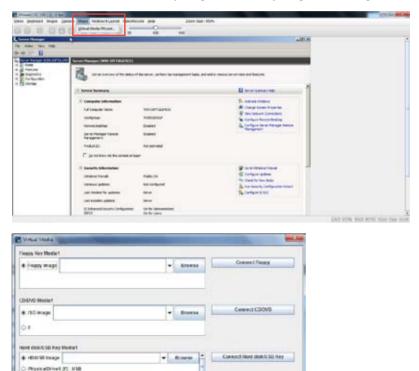
Virtual Media Wizard:

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.



Cent

iPhysicalDrived. (C.0). House Drive TargelDise Vitual Places 1 Vitual CD 1

Notical HandDick 1

Not canneded Net convected

Nationsided

14

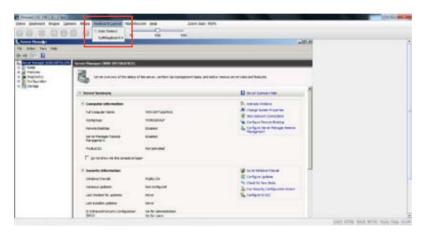
ida.

Virtual Media Wizard

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.



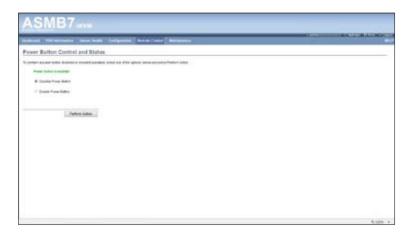
4.5.3 Chassis Identify Command

The Chassis Identify Command page allows you to perform a chassis identify command control operation. Enter identify interval in seconds, and then click **Perform Action** to start the command.



4.5.4 Power Button

The Power Button page allows you to enable or disable power button and click **Perform Action** to confirm the selection.



4.6 Maintenance

This section allows you to perform the firmware update for the remote server. You can also use **Restore Factory Defaults** to reset system settings.

agent property and the fields of the legal for loss of real
Date label that

4.6.1 Firmware Update

This section allows you to enter the update mode, and update the firmware of ASMB7. Please note that after entering update mode widgets, other web pages and services will not work. All oopen widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will reset.

ASMB7	
Sumar (Bildowing Soulhall Sufgering Area 2002) Barners	-
Firmeare Update	
Lagang branes of the stress Party Mark Mark Mark Mark Mark Mark Mark Mark	for during will should
	Env upter then

4.6.2 Restore Factory Default

This section allows you to restore all settings to factory default. Please click the **Restore Factory** to reset all settings.



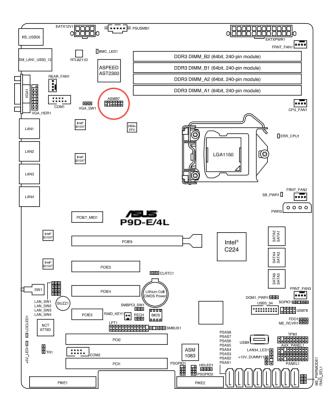
The Appendix shows the location of the LAN ports for server management and BMC connector on server motherboards. This section also presents common problems that you may encounter when installing or using the server management board.



A.1 BMC connector

The ASUS server motherboards that support the ASMB7-iKVM comes with a Baseboard Management Controller (BMC) connector.

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



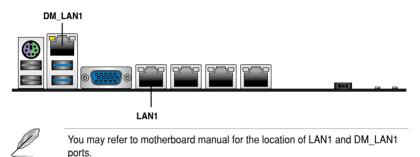


The motherboard illustration is for reference only. The motherboard layout and appearance may vary depending on the model.

A.2 LAN ports for server management

The ASUS server motherboards that support the ASMB7-iKVM comes with three 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 LAN1 and DM_LAN1 ports. You must use the LAN1 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 LAN1 and DM_LAN1 ports for server management on some server motherboards.





A.3 Troubleshooting



This troubleshooting guide provides answers to some common problems that you may encounter while installing and/or using ASUS ASMB7-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 ASMB7-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 	
	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.	
ASMB7-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_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x08: DIMM_C3, 0x08: DIMM_C2, 0x06: DIMM_D1, 0x00: DIMM_D2, 0x06: DIMM_D3, 0x0F: DIMM_D4
0xD2	CPU1_ECC2	OEM Memory ECC Sensor (For Intel DP platform only - ASUS 28 series server MB; -E6 server system)	0xC1	Discrete(0x6F) bx01: Read ECC error bx02: ECC Error occurred on a scrub bx04: Write Parity Error bx06: Error in Redundant memory bx10: Sparing Error bx20: Memory antity Error bx20: Memory antity Error bx80: Style Enable Parity	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03: DIMM_A2, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x06: DIMM_C4, 0x08: DIMM_C3, 0x08: DIMM_C4, 0x06: DIMM_D3, 0x0F: 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, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x06: DIMM_G1, 0x07: DIMM_G2, 0x06: DIMM_G3, 0x07: DIMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x14: DIMM_G3, 0x17: DIMM_C4
0xD4	CPU2_ECC2	OEM Memory ECC Sensor (For Intel DP platform only - ASUS 28 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x06: DIMM_G1, 0x00F: DIMM_G2, 0x06: DIMM_G3, 0x0F: DIMM_G2, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_E3, 0x13: DIMM_H4, 0x14: DIMM_G1, 0x15: DIMM_C4

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 Critital - going high
0x82	PSU1 Fan1	FAN	0x04	Threshold(0x01) Lower Non-oritical - going low Lower Critital - going low
0x83	PSU1 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - 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 Critital - going high
0x85	PSU2 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x86	PSU2 Fan2	FAN	0x04	Threshold(0x01) Lower Non-oritical - going low Lower Critital - 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

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 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
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 Critital - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low

0xA2	FRNT_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA3	FRNT_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA4	FRNT_FAN3	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA5	FRNT_FAN4	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA6	REAR_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA7	REAR_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA8	FRNT_FAN5	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA9	FRNT_FAN6	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xAA	FRNT_FAN7	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - 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.tw

Technical Support Telephone

+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

Online Support

Fax

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 +86-21-3407-4610 (800-820-6655) 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 +49-1805-010923 Support Fax +49-2102-959911 Online support http://support.asus.com/techserv/techserv.aspx

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

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

Technical Support

Telephone +420-596-766-891 Fax +420-596-766-329 E-mail advance.rma.eu@asus.com Online Support 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)

Address	Ul. Post Dpu 6, 02-676 Warszawa, Poland
Web site	http://pl.asus.com

Technical Support

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

ASK-Service (Russia and CIS)

Address	0.000000, 00. 00000000000, 0.10, 000000
Telephone	(495) 640-32-75
Web site	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

Conformity Conformity	ASUSTeK COMPUTER INC.	4F, No. 150, LLTE Rd., PEITOU, TAIPEI 112, TAIWAN	TAWAN A SI S COMPLITED Combu	HARKOPT STR 21-23 40800 PAT MOEN		ent Card	W/N	lirectives:	4 2010	EN 61003-3-32008 EN 560202007-411:2011		V 301 489-1 VI 9 2(2011-09) V 301 489-3 VI 4 1/2007-09)	489-4 V1 4.1(2009-05)	489-9 V1.4.1(2007-11)	489-17 V2.1.1(2009-05) 480-24 V1.6 1/2010-05)	326-2 V1 2 2 (2007-08)	325-3 VI 3.1(2007-09) 357-2 VI 4.1(2008-11)	281-1 V1.1.1 (2005-07) 281-2 V1.1.1 (2005-07)	EN 60065:2002 / A12:2011		Regulation (EC) No. 278/2009		Vec 1302.08		(EC conformity marking)	Position : CEO	Name : Jerry Shen	Den	Signature :	
EC Declaration of Conformity We, the undersigned,		City:	Country: TAWAN		declare the following apparatus:	Product name : Management Card	Model name : ASMB7-IKVM	conform with the essential requirements of the following directives:	04/108/EC-EMC Directive EN 55022-2010	EN 61000-3-2:2008-A22009 EN 55013:2001+A1:2003-A22008 EN 55013:2001+A1:2003-A22008	1					EN 302 544-2 V1.1.1(2009-01)	EN 302 623 V1.1.1(2009-01)	00	EN 60950-1 / A 12 2011	2009/125/EC-ErP Directive	8008	-	X2011/65/EU-RoHS Directive	©CE marking	,			Declaration Date: 12/04/2013	וופועווואידטוא כב ווופועווואידטוא	

DECLARATION OF CONFORMITY PerFCC Part 2 Section 2. 107(a) PerFCC Part 2 Section 2. 107(a) Responsible Party Name: Asus Computer International Address: 800 Corporate Way, Fremont, CA 94539. PhonoFax No: (510)739-3777(610)608-4555 Interby declares that the product Product Name: Management Card Model Number: ASMB74(VM Conforms to the following specifications: Conforms to the following voo conditions: (1) This device may not cared harm of a subject to the following two conditions: (1) This device may and underformed than you cause humful interformed than you are underformed to the following two conditions: Conditional interformed than you are underformed to the following two conditions: Conditional interformed than you are underived operation. Signature: Anne:
