

ASMB3-IKVM Server Management Board



E3730

First Edition V1 April 2008

Copyright © 2008 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

Conter	nts	
Notices	S	v
Safety	informati	ion vi
About	this guid	e vii
ASMB3	3-IKVM sp	pecifications summary ix
Chapt	er 1:	Product introduction
1.1	Welcom	e!
1.2	Package	contents 1-2
1.3	Features	s 1-2
1.4	Board la	yout 1-4
1.5	System	requirements1-4
1.6	Network	setup 1-5
Chapt	er 2:	Installation
2.1	Before y	ou proceed 2-2
2.2	Hardwar	e installation2-2
2.3	Firmwar	e update2-5
2.4	BIOS co	nfiguration 2-6
	2.4.1	AMI BIOS setup2-6
	2.4.2	Phoenix BIOS setup2-9
2.5	Running	the KIRARARI utility2-13
	2.5.1	Updating the ASMB3-IKVM firmware 2-14
	2.5.2	Configuring the LAN controller2-15
	2.5.3	Configuring the user name and password 2-16
Chapt	er 3:	Software support
3.1	Web-bas	sed user interface 3-2
	3.1.1	Loging in the utility
	3.1.2	Home page
	3.1.3	Remote Control
	3.1.4	Virtual Media 3-7
	3.1.5	System Health3-11
	3.1.6	User Management 3-14
	3.1.7	KVM Settings 3-16

Contents

	3.1.8	Device Settings	
	3.1.9	Maintenance	
Арре	ndix:	Reference information	
A.1	LAN p	ort for server management	A-2
A.2	BMC s	ocket	A-3
A.3	Troubl	eshooting	A-4

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.

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.



This symbol of the crossed out wheeled bin indicates that the product (electrical, electronic equipment, and mercury-containing button cell battery) should not be placed in municipal waste. Check local regulations for disposal of electronic products.

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: Software support

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 IKVM LAN port for server management and BMC socket on several 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></ctrl+alt+d>
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:

ASMB3-IKVM specifications summary

Chipset	KIRA100
Internal RAM	256 Mb for system 256 Mb for video
Internal ROM	64 Mb
Timers	32-bit Watchdog Timer
System interface	Supports Keyboard Controller Style (KCS)
LAN type	10/100 Mbps Dedicated LAN
LED	1 x BMC heartbeat
Bus	2 x I2C bus 1 x LPC bus 2 x UART bus (debug only) 1 x DVO bus 1 x LAN interface
Main features	IPMI 2.0-compliant and supports KVM over LAN Web-based user interface (remote management) Virtual media
Form factor	2.66" x 1.48"

* 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® ASMB3-IKVM server management board!

The ASUS ASMB3-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 ASMB3-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 ASMB3-IKVM board
- Support CD
- User guide



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

1.3 Features

1. KVM over LAN:

Allows you to access your servers anytime and anywhere

- Remote access to your servers with full control by local keyboard, video monitor and mouse (KVM)
- Out-of-band KVM: Supports remote access even if server OS is down
- Dynamic Host Configuration Protocol (DHCP):
 - Avoids the need to manually set IP address by receiving IP address automatically (for ASMB3-IKVM board)

2. IPMI 2.0 features:

IPMI 2.0-compliant and supports

- Hardware Health Monitor
 - Sensor Data Record (SDR): Displays status and record for temperature, voltage and fan speed sensors
 - System Event Log (SEL)
- Field Replaceable Unit (FRU)
- Lan Alerting
 - Via Simple Network Management Protocol (SNMP)/Platform Event Trap (PET)
 - Via E-mail
- · Remote Power Control to power on/off and reboot a system
- Remote Management Control Protocol (RMCP+)
 - Enhances authentication and confidentiality capabilities for IPMI LAN sessions
- Advanced Encryption Standard (AES)

3. Web-based user interface (Remote Management):

- JAVA-based web browser*
- · Supports multiple viewers with different authorities
- Supports Secure Sockets Layer (SSL)
 - Uses cryptographic protocols to secure and authenticate connection between a client and a server over a network
 - Ensure data integrity and privacy
- Remote BIOS Update
- Remote Firmware Update
- * Install Java Runtime Environment (JRE) before using web-based remote management

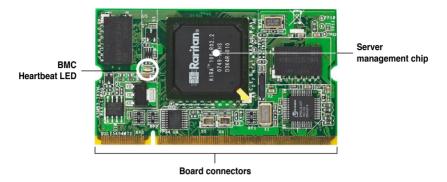
4. Virtual media:

Allows you to share the data stored in a local drive of the remote server

- Hard disk drive
- USB flash
- CD/DVD ROM
- Floppy
- Image file

1.4 Board layout

The ASUS ASMB3-IKVM comes in a BMC package. The illustration below shows the major components of the server management board.



LED indicators

The ASMB3-IKVM board comes with a BMC heartbeat LED. Refer to the table below for the LED indications.

LED	Name	Status	Description
LED1	BMC Heartbeat	Blinking	ASMB3-IKVM firmware is in execution.
		Off (for about 30 seconds)	The Heartbeat LED is off for about 30 seconds when the firmware is loading after the AC power is re-plugged.
		Off (continuously)	The ASMB3-IKVM firmware is corrupted or the server system standby-power is off.

1.5 System requirements

Before you install the ASMB3-IKVM board, check if the remote server system meets the following requirements:

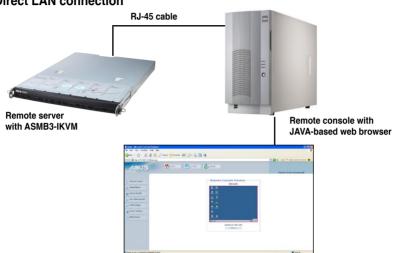
- ASUS server motherboard with Baseboard Management Controller (BMC) socket*
- IKVM LAN port for server management**
- Microsoft[®] Internet Explorer 5.5 or later; Firefox



- Visit the ASUS website (www.asus.com) for an updated list of server motherboards that support the ASMB3-IKVM.
- ** See the Appendix for details.

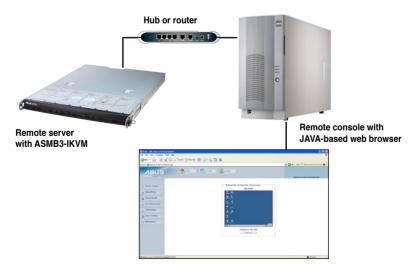
1.6 **Network setup**

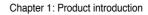
The ASMB3-IKVM server management board installed on the remote server connects to a local/central server via direct LAN connection or through a network hub. Below are the supported server management configurations.



Direct LAN connection

LAN connection through a network hub





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. Remove the remote server system cover, and then locate the Baseboard Management Controller (BMC) socket on the motherboard.



Refer to the Appendix section for the location of the BMC socket on supported motherboards.



- Position the board at a 30°-45° angle, then match the notch on the board with the break on the socket.
- Carefully push the board to the socket until its connectors (golden fingers) are fully-inserted to the socket.



4. Press the board firmly until the BMC socket retaining clips snap back and secure the board in place.



When installed, the board appears as shown.



5. Reinstall the remote server system cover, then connect the power plug to a grounded wall socket.



Everytime after the AC power is re-plugged, you have to wait for about 30 seconds for the system power up.

6. Insert the LAN cable plug to the IKVM LAN port for server management.



Refer to the Appendix for the location of the IKVM LAN port for server management on various server motherboards.

7. 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.

To uninstall the board:

1. Simultaneously push the BMC socket retaining clips outward until the board tilts up.



2. Carefully pull the board out from the BMC socket, then set aside.



2.3 Firmware update

You need to update the ASMB3-IKVM firmware before you start using the ASMB3-IKVM board.

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 **ASMB3-iKVM Firmware Update**, and press <Enter> to enter the sub-menu.

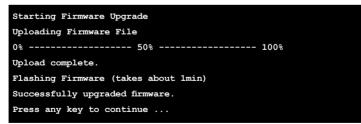


6. A confirmation message appears, asking whether you want to update the firmware or not. Press <Y> to update.

```
Are you sure you want to update ASMB3-iKVM Firmware now?
Yes or No [YN]?
```

The firmware updating process starts.

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



8. Turn off the system and **unplug the AC power cord for 5 seconds** before restarting the system



You may update firmware from the web-based user interface. Refer to page 3-25 for details.

2.4 BIOS configuration

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

- Ø
- Update the remote server BIOS file following the instructions in the motherboard/system user guide. Visit the ASUS website (www.asus.com) to download the latest BIOS file for the motherboard.
- The BIOS setup screens shown in this section are for reference purposes only, and may not exactly match what you see on your screen.

2.4.1 AMI BIOS setup

You must configure the network settings of both the remote server and the local/ central server to establish communication for remote server control and monitoring.

Running the BIOS IPMI configuration

To configure the IPMI in the BIOS:

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

IPMI Configuration

BIOS SETUP UTILITY Advanced	
IPMI Configuration BMC Firmware version: 001.001 ▶ View BMC System Event Log Clear BMC System Event Log ▶ Set LAN Configuration BMC Watch Dog Timer Action [Disabled]	View all events in the BMC Event Log. It will take a max. of 15 seconds to read all BMC SEL records.
	 ↔ Select Screen ↓ Select Item Enter Go to Sub Screen F1 General Help F10 Save and Exit ESC Exit

View BMC 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.

Advanced	BIOS SETUP UTILITY	
Total Number of Entries:	0	Use +/- to traverse
SEL Entry Number:	[N/A]	the event log.
		 Select Screen Select Item Change Option General Help Save and Exit ESC Exit
v02.58 (C)Copyri	ght 1985-2007, American Meg	atrends, Inc.

Clear BMC System Event Log

Allows you to clear the system event log. Press <Enter> to go to the sub screen, and then select **Ok** to clear BMC System Event Log.

Set LAN Configuration

Allows you to set the BMC LAN Parameter settings.

LAN Configuration.	Options
IP Address [000.0	5.255.0 Static Mode 0.000.000
	00.000.000] ←→ Select Screen t↓ Select Item +- Change Option F1 General Help F10 Save and Exit ESC Exit

IP Address Source

Allows you to select the IP address source type. When set to [Static Mode], the following three items become configurable, and you have to assign the IP address, subnet mask and gateway address for the remote server. When set to [DHCP Mode], you don't have to assign the IP address, subnet mask and gateway address for the remote server.

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 Address

Allows you to set the gateway address. We recommend that you use the same gateway address you have specified on the operating system network for the used network card.

BMC Watch Dog Timer Action [Disabled]

Allows the BMC to reset or power down the system when the operating system crashes or hangs. Configuration options: [Disabled] [Reset System] [Power Down] [Power Cycle]



It is necessary to install ASWM (ASUS System Web-based Management) for using this function.

2.4.2 Phoenix BIOS setup

Running the BIOS IPMI configuration

To configure the IPMI in the BIOS:

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



IPMI Configuration

Ph	oenixBIOS Setup Utility	
Server		
IPMI		Item Specific Help
IFMI Specification Version BMC Firmware Version Cystem Event Logging Clear System Event Log Existing Event Log number Event Log Control SYS Firmware Progress BIOS POST Firmvare Progress BIOS POST Watchdog OS Boot Watchdog Timer for loading OS (min) Time out action Date Format to show Date Separator	2.0 1.04 [Enabled] [Disabled] 34 [Disabled] [Disabled] [Disabled] [Disabled] [10] [No action] [MM DD YYYY] [/]	Enable/Disable IFMI event logging. Disabling will still log events received via the system interface.
F1 Help ↑↓ Select Item ESC: Exit →← Select Menu		

IPMI Specification Version

This item shows the auto-detected IPMI specification version.

BMC Firmware Version

This item shows the auto-detected BMC firmware version.

System Event Logging [Enabled]

Allows you to enable or disable the IPMI event logging feature. Configuration options: [Enabled] [Disabled]

Clear System Event Log [Disabled]

Enabling this item forces the BIOS to clear the system event log on the next cold boot. Configuration options: [Disabled] [Enabled]

Existing Event Log number

This item shows the auto-detected quantity of existing/remaining event logs.

Event Log Control

The following sub-items allow you to control the event logs.

SYS Firmware Progress [Disabled]

Allows you to enable or disable the POST progress log feature. Configuration options: [Disabled] [Enabled]

BIOS POST Errors [Enabled]

Allows you to enable or disable the POST error log feature. Configuration options: [Disabled] [Enabled]

BIOS POST Watchdog [Disabled]

Allows you to enable or disable the BIOS POST watchdog feature. Configuration options: [Disabled] [Enabled]

OS Boot Watchdog [Disabled]

Allows you to enable or disable the OS boot watchdog feature. Configuration options: [Disabled] [Enabled]

Timer for loading OS (min) [10]

Allows you to set the timer value for the watchdog timer. Use the numeric keypad to enter your desired value, or use the <+>/<-> key to increase/decrease the value. Valid input values range from [1] ~ [100].

Time out action [No action]

Allows you to specify what action to take if the OS fails to boot. Configuration options: [No Action] [Reset] [Power Off] [Power Cycle]

Date Format to show [MM DD YYYY]

Allows you to choose the date format to be displayed. Configuration options: [MM DD YYYY] [DD MM YYYY] [YYYY DD MM]

<u>Date Separator [/]</u> Allows you to choose which character to use in date entries. Configuration options: [.] [/]

Scroll down to display more items.

PhoenixBIOS Setup Utility	
Server	
IPMI	Item Specific Help
System Event Log System Event Log (list mode) DHCP [Enabled] IP Address [000.000.000]	Display the System Event Log.
F1 Help ↑↓ Select Item -/+ Change Values ESC: Exit →← Select Menu Enter Select ≽Sub-menu	F9 Setup Defaults F10 Save and Exit



To configure your subnet mask and gateway address, refer to **section 2.5.1** for more information on using KIRARARI utility.

System Event Log

Press <Enter> to open the System Event Log, which allows you to view log entries. Use the arrow keys to browse entry numbers.

System Event Log SEL Entry Number = 1 SEL Record ID = 0001 SEL Record Type = 02-System Event Record Timestamp = 04/17/2006 16:10:44 Generator Id = 20 00 SEL Message Rev = 04 Sensor Type = Sensor Type = 01 - Temperature Sensor Number = 32 - CPU2temperature1 SEL Event Type = 01 - Threshold Event Description = Upper Non-critical Going High, Assertion SEL Event Data = 57 80 50	Server	
SEL Record ID = 0001 SEL Record Type = 02-System Event Record Timestamp = 04/17/2006 Generator Id = 20 SEL Message Rev = 04 Sensor Type = 01 - Temperature Sensor Number = 32 - CPU2temperature1 SEL Event Type = 01 - Threshold Event Description = Upper Non-critical Going High, Assertion		System Event Log
	SEL Record ID = SEL Record Type = Timestamp = Generator Id = SEL Message Rev = Sensor Type = Sensor Number = SEL Event Type = Event Description =	02-System Event Record 04/17/2006 16:10:44 20 00 04 01 - Temperature 32 - CPU2temperature1 01 - Threshold Upper Non-critical Going High, Assertion

System Event Log (list mode)

Press <Enter> to open the System Event Log in list mode.

	System	Event Log (list mode)		
Event ID	Sensor Name	Sensor Type	Date/Time St	amp
001	CPU2temperature1		04/17/2006	16:10:44
002	CPU2temperature1	Going High, Assertion Temp ng High, Assertion	04/17/2006	16:10:44
003	CPU2temperature2		04/17/2006	16:10:44
004	CPU2temperature2		04/17/2006	16:10:44
005	DIMM_01 AMB temp		04/17/2006	16:10:44
006	DIMM_01 AMB temp Upper Critical Goi	Temp	04/17/2006	16:10:45

Choose an event ID, then press <Enter> to view the details.

PhoenixBIOS Setup Utility Server					
[0001	CPU2temperature1	Temp	04/17/2006	16:10:44]
SEL Entry SEL Record SEL Record Timestamp Generator SEL Messag Sensor Typ Sensor Typ Sensor Num SEL Event Event Desc SEL Event	: ID = Type = = Id = e Rev = e = ber = Type = ription =	04/17/2006 20 00 04 01 - Tempe 32 - CPU2t 01 - Thres	emperature1	gh, Asserti	.on
F1 Help ESC: Exit			Change Values Select ▶Sub-menu		Setup Defaults Save and Exit

<u>DHCP</u>

Allows you to enable or disable to set the IP source setting as DHCP.

IP Address

Allows you to provide information to set the BMC IP address.

2.5 Running the KIRARARI utility

The KIRARARI utility allows you to update the ASMB3-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 KIRARARI utility:

- 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 **FreeDOS command prompt**, and then press <Enter> .



- 6. When the C:> prompt appears, type CD \ASMB3\IKVM\MODEL\RS100-E5\ PI2, then press <Enter>.*
- 7. At the prompt, type kirarari.exe, then press <Enter> to display the KIRARARI Utility Help Menu. The screen appears as shown.

Usage: kirarari [options] command [parameters]	
Possible options are:	
-a	
-f Never prompt for user confirmation	
-c Calm mode (nothing printed out)	
-v Increase verbosity (can be specified multiple times)	
Possible commands are:	
info Show information about the BMC	
ver	
reset	
fw Firmware operations	
cfg Backup or restore device configuration	
serial Serial number operations	
defaults	
ip Read or set IP address	
$g\hat{\mathbf{w}}$ Read or set default gateway address	
netmask Read or set subnet mask	
mac Read or set MAC address	
ipsrc	
admin Show admin name or set name and password	
raw Execute raw commands	
test Execute some self tests	
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>_	Γ

Refer to the table on the next page for a description of the help menu options.



* The model name (for example RS100-E5) varies based on the motherboard model you purchase.

KIRARARI Help Menu options

Options	Description
kirarari reset	Reset the device for BMC card
kirarari fw	Show firmware information
kirarari fw upgrade < <filename>></filename>	Upgrade BMC firmware
kirarari ip	Show IP setting
kirarari ip set xxx.xxx.xxx.xxx	Set IP to xxx.xxx.xxx
kirarari gw	Show gateway setting
kirarari gw set xxx.xxx.xxx.xxx	Set gateway to xxx.xxx.xxx.xxx
kirarari netmask	Show net-mask setting
kirarari netmask set xxx.xxx.xxx.xxx	Set net-mask to xxx.xxx.xxx.xxx
kirarari mac	Show MAC setting
kirarari mac set xxx.xxx.xxx.xxx	Set MAC to xxx.xxx.xxx.xxx
kirarari ipsrc	Show IP source setting
kirarari ipsrc set < <static bios="" dhcp="">></static>	Set the IP source from static (no change)/ bios (assign by bios setting)/dhcp (get IP from DHCP server)
kirarari admin	Show administrator name
kirarari admin name xxxxx	Set login name of administrator to xxxxx
kirarari admin passwd xxxxx	Set login password of administrator to xxxxx

2.5.1 Updating the ASMB3-IKVM firmware

You may use KIRARARI utility to update the ASMB3-IKVM firmware.

To update the firmware:

1. Download the latest ASMB3-IKVM firmware from the ASUS website (www.asus.com), and then save the file.

S

Save the file in a USB flash or in the hard disk drive of the remote server.

- 2. Follow steps 1-6 on previous page.
- At the prompt, type kirarari fw upgrade rs100e51.bin, then press <Enter> to start updating the firmware.*
- 4. When the update process is complete, the following screen appears.

5. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.



* The file name (for example rs100e51.bin) varies based on the motherboard model you purchase and the firmware version you download from website.

2.5.2 Configuring the LAN controller

Before you can establish connection to the ASMB3-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. Follow steps 1-6 on page 2-13.
- 2. At the prompt, type **kirarari ipsrc**, then press <Enter> to see the current IP source setting.

```
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>kirarari ipsrc
IP source: Static Address
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>
```

- If the current IP source is set to DHCP address, then you don't have to assign the IP address to the remote server. If the current IP source is set to Static address, then follow below instructions to complete the IP address assignment.
- Type kirarari ip set xxx.xxx.xxx, then press <Enter> to assign any IP address to the remote server. The screen displays the request and response buffer. Write the remote server IP address in a piece of paper for reference.

```
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>kirarari ip set 192.168.0.212
Successfully set IP address to 192.168.0.212
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>
```

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.

- 5. Configure your subnet mask (a) and gateway address (b) if necessary.
 - (a) Type kirarari netmask set xxx.xxx.xxx
 - (b) Type kirarari gw set xxx.xxx.xxx
- 6. Press <Enter> to effect the configuration.
- 7. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.
- 8. Adjust the local/central server network settings, if necessary.

2.5.3 Configuring the user name and password

You may change your login name and password from the KIRARARI utility.

To change the login name and password:

- 1. Follow steps 1-6 on page 2-13.
- 2. At the prompt, type kirarari admin name xxxxx, then press <Enter> to change the login name.

```
C:\ASME3\IKVM\MODEL\RS100-E5\PI2>kirarari admin name super
Successfully set administrator username to super
C:\ASME3\IKVM\MODEL\RS100-E5\PI2>
```

- 3. Type kirarari admin passwd xxxxx, 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 tells you how to use the web-based user interface that the server management board supports.



3.1 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.



You should install JRE on remote console first before using web-based management. You can find **JRE** from the folder **JAVA** of the ASMB3-IKVM support CD. You can also download JRE from <u>http://java.sun.com/javase/downloads</u>.

3.1.1 Loging in the utility

- 1. Ensure that the LAN cable of the computer is connected to the IKVM 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 (super) and password (pass). Then click Login.

Address 🛃 http://192.168.0.212/auth.asp		🔽 🔁 Go	Links 🎽 Norton Internet Security 🚇 🗸
	Authenticate with Username and Password!		
	Username		
	Password		
	Login		



A **Change Password** screen appears asking you to change the password when you log in the utility for the first time. Type in the default password (pass) in the **Old password** column, and then type in the new password in the **New password** and **Confirm New Password** columns.

Change Password	
Old Password	
New Password	
Confirm New Password	
	Apply

3.1.2 Home page

The home page displays when you login in the utility sucessfully.

Home Console Course	Remote Console connected!
Remote Console Preview Orkin con	- 4 5

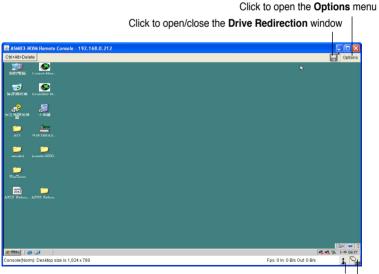
- 1. **Home:** Click this icon to return to the home page.
- 2. Console: Click this icon to open the remote server window.
- 3. Logout: Click this icon to log out the utility.
- 4. **Remote server screen:** Displays the remote server screen. Click this screen to open the remote server window.
- 5. **Refresh:** Click this icon to refresh the remote server screen.
- 6. Function keys: Click each function key to start using its specific functions.

3.1.3 Remote Control

Click **Remote Control** to open its submenu, and then click **KVM Console** to open remote server console screen.

		Home Console Console Remote Console connected
Remote Console Preview Gibliogen Gibliogen <th>KVM Console Vittus metho System Health O Viser Management KVM Settings KVM Settings</th> <th>E E E E E E E E E E E E E E E E E E E</th>	KVM Console Vittus metho System Health O Viser Management KVM Settings KVM Settings	E E E E E E E E E E E E E E E E E E E

Remote server console screen



Indicates the number of networks (users) that are connected via Console Redirection Indicates the availability of keyboard and mouse

Drive Redirection

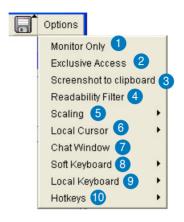
The **Drive Redirection** function allows you to share your looal drives (floppy disk drives, CD-ROM and hard disk drives) with users in the remote system. Click **Connect Drive**, and then a **Select a drive to redirect** screen appears, allowing you to select the drives you want to share in the remote system.

You have to check the box before **Enable Write support** item if you want to write data into the shared drive. For enabling this function, the **Force read-only connectors** item in the **Drive Redirection** window of the web-based utility should be unchecked. See page 3-9 for details.

🕌 ASMB3-iKN	VM Remote Console - 192.168.0.212	
	Drive Redirection	
Drive 1:	Connect Drive Connect ISO Disconnect Not connected	
Cancelled D	Drive redirection	
Drive 2:	Connect Drive Connect ISO Disconnect Not connected	
Drive Redire	ection disconnected.	
	📓 Select a drive to redirect 🛛 🔀	_
Ctrl+Alt+Delet	E C: (Hard Disk) Refresh List	Options
	OK Cancel	

You may want to share an ISO image file with users in the remote system. Click **Connect ISO**, and then a **Choose ISO image to redirect** screen appears, allowing you to select the ISO image you what to share in the remote system.

Options menu



- Monitor Only: Click to toggle the Monitor Only function on or off. If this function is switched on, the remote server console screen could be viewed only, no remote console interaction is possible.
- Exclusive Access: Click to toggle the Exclusive Access function on or off. If this function is switched on, no other users could open the remote console at the same time until you disable this function or log off.*
- 3. Screenshot to clipboard: Click to capture a screenshot of the remote server console screen.
- 4. Readability Filter: Click to toggle the Readability Filter function on or off. If this function is switched on, most of the screen details will be shown even if the scaling mode is set to higher percentage. This function is available only with a JVM 1.4 or higher.
- 5. Scaling: Click to adjust the diaplay ratio of the remote server console screen.
- 6. **Local Cursor:** Click to select the diaplay type of mouse cursor for the remote server console screen.
- 7. **Chat Window:** Click to open the chat window that allows you have conversation with the other users.
- 8. **Soft Keyboard:** Click to display the soft keyboard or select the input language and country mapping of the soft keyboard.
- 9. Local Keyboard: Click to select the input language for the remote console.
- 10. Hotkeys: Click to select the hotkey to send a command to the remote server.



* This option is available only when the **RC settings (Exclusive Access)** permission has been enabled. Refer to **3.1.6 User Management** for details.

3.1.4 Virtual Media

Click Virtual Media to open its submenu.



You may use the **Drive Redirection** funciton from the remote server console screen. Refer to page 3-5 for details.

Floppy Disk

	Hame Console Console Remote Console connected!
Remote Control	Active Image - Drive 1 Ho disk emulation set. 2
CO-ROM Image Drive Redirection Options	Active Image - Drive 2 No disk emulation set.
System Health O O User Management Extra Settings	Floppy Image Upload The option address you to updated a benary image (e.g. example ing) with anaxium size of 1.4486 bit her ASM654/VM. The image with a emulated for the total as UB device.
Device Settings	Virtual Drive Drive 1 🛛 5 Pkoppy Image File Upriced

- 1. **Floppy Disk:** Click this function key to upload the data stored in the local floppy disk image to the remote server.
- 2. Active Image Drive 1: Displays the data that has been uploaded to Drive 1 of the remote server.
- 3. Active Image Drive 2: Displays the data that has been uploaded to Drive 2 of the remote server.
- 4. Floppy Image Upload: Allows you to upload a binary image with a maximum size of 1.44 MB to the ASMB3-IKVM. This image will be emulated to the remote server as a USB floppy device.
- 5. **Virtual Drive:** Selects the drive in the remote server as a distination drive for you to upload your image data.
- 6. **Floppy Image File:** Click **Browse** to preview and select the files that you want to upload to the remote server.
- 7. **Upload:** Click to upload the file to the specified drive of the remote server.

CD-ROM Image

ACHIO I HVH		Remote Console connected
Remote Control	Active Image - Drive 1 Bodisk emulation set. 2	
Virtual Media		
CD-ROM Image	Active Image - Drive 2 No disk emulation set.	
System Health	Image on Windows Share	
Ö Üser Management	This option allows you to share a CD-ROM image	
6 KVIII Settings	over a Windows Share with a maximum size of 800MB. This image will be emulated to the host as USB device.	
Device Settings	Vistual Drive Drive 1 V	
Y Maintenance		
	Share host 6	
	Share name	
	Path to Image 8	
	9 User (optional)	

- CD-ROM Image: Click this function key to share data stored in your CD-ROM image with other users in the remote server through the Windows Share application via USB.
- 2. Active Image Drive 1: Displays the file name of the data in Drive 1 of the remote server.
- 3. Active Image Drive 2: Displays the file name of the data in Drive 2 of the remote server.
- Image on Windows Share: Allows you to decide how you want to share the data stored in your CD-ROM image with the users in the remote server.*
- 5. **Virtual Drive:** Selects the drive in the remote server that you want to share your data with.
- 6. **Share host:** Enter the IP address or the name of the system that you want to share data with via Windows Share.
- 7. **Share name:** Enter the name of the Windows Share you want to share data with in the remote server.
- 8. **Path to image:** Enter the location of source files that you want to share via Windows Share.
- User/Password (Optional): Enter the user name and password of the Windows Share. Leave blank to use guest account.
- 10. Set: Click to apply your selections.



- * Ensure that you've installed **NWLink IPX/SPX/NetBIOS compatible Transport Protocol** item for the network of the user with the CD-ROM image.
- The remote connect ISO function is for read only.

	ark Protocol that you want to install, then c lisk for this component, click Have Disk.	
Manufacturer	Network Protocol:	
Microsoft	Microsoft TCP/IP version 6	ompalible Transp
This driver is digital Tell me who driver s		Have Disk

Drive Redirection

	Console	Remote Console connected
Remote Control	Active Image - Drive 1 Bis disk enskaldion set.	
en Ploppy Disk JCD-ROM Image Drive Redirection	Active Image - Drive 2 No disk emulation set.	
D System Health 30 User Management	Drive Redirection	
KVM Settings	(frigory, CD-RCM, rentrovable statis and handstatis) with the remote system.	
Y Maintenance	6 Proce read cely connections Apply Reserve to defaults 7 nd value to equal to the default 8	

- Drive Redirection: Click this function key to make local drives accessible for other users via console redirection. This function allows you to share your local drives (floppy disk drives, CD-ROM and hard disk drives) with users in the remote system.
- 2. Active Image Drive 1: Displays the file name of the data in Drive 1 of the remote server.
- 3. Active Image Drive 2: Displays the file name of the data in Drive 2 of the remote server.
- 4. Drive Redirection: Use this window to configure Drive Redirection settings.
- 5. **Disable Drive Redirection:** Check this box to disable Drive Redirection function. When this function is disabled, local drives will not be accessible for other users in remote server.
- Force read-only connectors: Check this box to allow the data stored in local drives to be read in the remote system, but could not be overwritten to ensure data integrity and system security.
- 7. Apply: Click to apply your settings.
- 8. Reset to defaults: Click to return to the default settings.

Options

ACRED HVH		Remote Console connected
Remote Control	2 Virtual Media Options	
Virtual Media Floopy Disk	Apply. Reset to defaults 2	
CD-ROM Image Drive Redirection	3 *Stored value is equal to the default.	4
System Health		
) User Management		
KVM Settings		
Device Settings		
Y Maintenance		

- 1. **Options:** Click this function key to open the Virtual Media options.
- 2. Virtual Media Options: Check this box to disable the funciton of Virtual Media options to prevent data stored in a local drive from being accessed by the user in the remote server.
- 3. **Apply:** Click to apply the setting if you've checked the box.
- 4. Reset to defaults: Click to return to the default settings.

3.1.5 System Health

Click System Health to open its submenu.

Chassis Control

	nome Consile Consele	
Remote Control Vertual Media System Health Chassis Control System Event Log System Event Log Sys	Remote Console connected Chassis Information 2 Forer i: 0n Reveal: 0 Reveal: 0 Power Control Power Control Power Control Power Control Power Control Power Control	
Device Settings		

- 1. **Chassis Control:** Click this function key to know the power information and power management for the remote server.
- 2. Chassis Information: Allows you to know the power information for the remote server. Click **Refresh** to update the information on this window.
- 3. **Power Control:** Click **Power On** to turn on the remote server; click **Power Down** to turn off the remote server; click **Power Cycle** to turn off the remote server and turn it on later; click **Reset** to reset the remote console.



Click **Power Cycle** to turn off the remote server, and allow the remote server to be powered on automatically after about 3 minutes.

Monitor Sensors

ASMB3-IKVM					Rem	ote Console connected!
	-					
Remote Control	2 -	Monitor	ing Senso	rs		
		Sensor Type	Sensor Name	Sensor Status	Sensor Reading	
🚱 Virtual Media		Temperature	CPU1temperature	C/K	40 degrees C	
		Temperature	MB temperature 1	Above upper non-critical threshold	56 degrees C	
🕀 System Health		Votage	VCore 1	Ok	1.160 Volts	
Chassis Control	<u> </u>	Votage	+3.3V	Ok	3.248 Volts	
Monitor Sensors		Voltage	+5¥	OK	4.272 Voits	
System Event Log Alert Settings		Voltage	+12Y	OK	12.206 Volts	
no User Management		Voltage	CMOS Battery	CK	3.104 Volts	
00 oper management					0 RPM	
KVM Settings					2060 RPM	
		1.011	oyucan run z	Refresh	200011111	
Device Settings			-	(Carlos and		

- 1. **Monitor Sensors:** Click this function key to display the health monitoring information for the remote server.
- Monitoring Sensors: Allows you to see the related health monitoring information for the remote server. Click Refresh to update the information on this window.

System Event Log

		onsole		Logout		
Remote Control	Systen	n Even	t Log	Source	Description	Direction
A Meteoret Marchine	SEL record 02					Assertion Event
🔬 Virtual Media					Timer expired	
System Health	SEL record 02	04.02/2008	09:23:47	CMOS Battery	Lower Critical going high	Assertion Event
- System Hould	SEL record 02	04.02/2008	09:23:47	CMOS Bettery	Lower Non-critical going high	Assertion Event
o Chassis Control	SEL record 02	04/02/2008	09.23:41	CMOS Battery	Lower Critical going low	Assertion Event
o Monitor Sensors	SEL record 02	04/02/2008	09.23-44	CMOS Ballery	Lower Non-critical going low	Assertion Event
e System Event Log						
o Alert Settings	SEL record 02	04.02/2008	08:56:27	Watchdog 2	Timer expired	Assertion Event
ôộ User Management	SEL record 02	04.02/2008	08:56:16	CMOS Bettery	Lower Critical going high	Assertion Event
	SEL record 02	04/02/2008	08:56:16	CMOS Battery	Lower Non-critical going high	Assertion Event
KVM Settings	SEL record 02	04.02/2008	08:56:10	CMOS Battery	Lower Critical going low	Assertion Event
Bevice Settings	SEL record 02	04.02/2008	08:56:10	CMOS Battery	Lower Non-critical going low	Assertion Event
Q Dence Settings			c	lear	Refresh	
O Maintenance						

1. **System Event Log:** Click this function key to display the system health event log information for the remote server.

Alert Settings

ASMB3 IKVM													Re	ernote	Console	connected
Remote Control	IPM	I Alert	Configur		Filter List]	PolicyL	ist]	[LAN]	Destinati	on List						
🚱 Virtual Media																
System Health	IPM	I Filter	List													
	Index	Status	Filter Type	Action Polic	H Squarity	General	or ID	Sensor	Sensor No	Trigger	Offset	Data	Dat	22	Data 2	
Chassis Control Monitor Sensors	and ox	360605	Lutter (Abo	ACDON POIN	ym Seveniy	Cremerce	0110	Type	No	mggo						
System Event Log		disabled	configurable		0 unspecified	00	60	00	00	00	0000	00 00	0 00 00	00 01	00 00 00	fedic1
Alert Settings	2	disabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	0 00 00	00 00	00 00 00	ledit1
O User Management	3	disabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	00 00 0	0 00	00 00 00	India1
	4	disabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	0 00 00	0 00	00 00 00	[edit1
KVM Settings	5	disabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	0 00 00	0 00	00 00 00	(edit)
Danker Company	6	disabled	configurable		0 mspecified	00	00	00	00	00	0000	00 00	0 00 00	0 00	00 00 00	India1
Device Settings	7	dirabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	0 00 00	0 00	00 00 00	[edit]
Y Maintenance		disabled	configurable		0 unspecified		00		00	00					00 00 00	
1			configurable		0 unspecified		00		00	00					00 00 01	
			configurable		0 unspecified		00		00	00					00 00 01	a constant of the
			configurable		0 unspecified		00		00	00					00 00 01	
	12	disabled	configurable		0 unspecified	00	00	00	00	00					00 00 01	
	10	disabled	configurable		0 unspecified	00	00	00	00	00	0000	00 00	00 00 00	00 00	00 00 01	Ledis1

1. Alert Settings: Click this function key to enter the alert settings submenu for the remote server.

3.1.6 User Management

Click User Management to open its submenu.

Change Password

		Remote Console connected
Class & Control Contr	Change Password Othenward Wee Password Content there Password Content there Password	

1. Change Password: Click this function key to enter the Change Password window. After entering all the necessary information, click Apply to apply the new settings.

Users & Groups

ACMERTING					Remote Console connected
Remote Castrol Q Vermal Hodas System Hodats Change Roseword Users A Groups Permissions Q MM Settings	Herrunz rane Fulluser rane Contre Passwort Ernal address Mobile number	- select - v	Lookup		
Device Settings		 Unknown> (defeature orce user to change provide the second s			
Maintenance	Create	Hodify	Copy	Delate	
	Group Manage Existing groups New group name Create	ement - select - V	Lookup	Delate	

- 1. **Users & Groups:** Click this function key to enter the user management and group management submenus.
- 2. Users Management: Allows you to setup the related user information.
- 3. **Group Management:** Allows you to setup the group information for better user management.

Permissions

	Console Ducogout	
ASNESTRVM		Remote Console connected
Remote Control	2 User / Group Permissions	
BAARDER OF MEETING	Show permissions for	3
Virtual Media	Uber - select - 🖌 Croup Admin 🖌 Update	
System Health		
System recam	Permission	
User Management	Board Reset : Ves	
change Password	Change Password: Yes	
Jsers & Groups	Dote/Time Settings : Yes	
Permissions	Persware Update : Ves	
KVM Settings	Group Pennissions : Ves	
	PM Phylege Level : Administrator	
Device Softings	PM may use SOL payload : Vec	
Maintenance	KeyboardMouse Settings : Ves	
	Network/DynENS Settings : Ves	
	RC settings (Encoding): Ves	
	RC settings (Exclusive Access): Ves	
	BC settings (Holiveys) : Ves	
	RC settings (Monitor Mode): Ves	

- 1. **Permissions:** Click this function key to enter the user/group permissions submenu.
- 2. User / Group Permissions: Selects the user and group that you want to show the permission details.
- 3. **Update:** Click to update the permission information.



You can only set the user permission by setting group only.

3.1.7 KVM Settings

Click KVM Settings to open its submenu.

User Console

Click **User Console** to open the setup window. From the window you could configure the detailed settings for the remote server console.

ASNOTICOM		Remote Console connected
Remote Coste ol Service Restance Vertual Media System Health Q0 User Management	Renote Console Settings for User The strigge where an early sole of the setting the set of the setting the set of the setting the set of the setting	
eUser Console Cardo an UMocar Deduce Settings	Pre-configured Instruction speed Local (high collar) w Contribution To -coole w Contribution To -coole w to - high coll w *	
	Remote Console Type © Detaut Jans VI © Set Monregistral Jan Brainer Repr Project in the Associationer Repr Project in the Associationer Repr entrol in the Associationer Repr entrol in the Association of the Project Intel entrol in the Association of the Association of the Association entrol in the Association of the Association of the Association entrol in the Association of the Association of the Association of the Association entrol in the Association of the Association o	

Keyboard/Mouse

Click **Keyboard/Mouse** to open the setup window. From the window you could configure the detailed settings for the keyboard and mouse.





Set **USB Mouse Type** to [Windows > = 2000, Mac OS X] if your operating system is Windows[®]; set **USB Mouse Type** to [Other Operating Systems] if your operating system is Linux.

3.1.8 Device Settings

Click Device Settings to open its submenu.

Network

ACM03 INVM	_	Remote Console connected
Remote Control	2 Network Basic Settings	
MARKSHOUL HE STREET	Pauto configuration None 💌	
Virtual Media	Preferred host name (DHCP only)	
System Health	Paddress 192168.0.212	
	Subnet mask 255 255 0 -	
User Management	Cateway # address 0.0.0.0	
KVM Settings	Primary DNS server IP address 192.168.0.2	
Device Settings	Secondary DNS server IP address 168.95.1.1	
etwork		
evnamic DNS ecurity	3 Network Miscellaneous Settings	
ertificate	Renote Console & HTTPS port 443 -	
ate/Time uthentication	HTTP port 80 -	
ventLog	TELNET port 23	
IMP Settings	SSHport 22 -	
Maintenance		
	Bandweth Link hours "	

Scroll down to display more items.

	Anne Source Detailed	Remote Console connected
a Notived: 2)Pranasc OKS 2)Security 2)Centricats 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)DAP (2)Print 2)Print 2)Print (2)Print 2)Print (2)Print (2)Print 2)Print (2)Print (2)Print 2)Print (2)Print (Network Miscellaneous Settings Renot Groups at HTS par (40) HIT Par (80) TUAE par (20) Bashed (20) Deatabalitation [20] Charl Interface Deatabalitation [20] Ubiterities generative adaption (20) "Deatabalitation adaption [20] "Observed tabalitation adaption]	•

- 1. Network: Click this function key to enter the network submenus.
- 2. Network Basic Settings: Allows you to configure basic settings for the network.
- 3. Network Miscellaneous Settings: Allows you to configure other settings for the network.
- 4. LAN Interface Settings: Allows you to configure the LAN interface speed and LAN interface duplex mode.

Dynamic DNS

ASNOTICOM		Remote Console connected
Remote Control Vernal Meeta Sporten Health Used Management Read Settings Opender Settings O		
Vytaanse voor Genfante Datu/Teme Kevent tag I Maarenaance	Apply Reserve And Andre	

- 1. **Dynamic DNS:** Click this function key to enter the dynamic DNS submenus and configure its related settings.
- 2. Enable Dynamic DNS: Check this box to enable the dynamic DNS service.

Security

ASHBITIKVM					Remote Console connected
Remote Control	2 ^{-нт}	TP Encryption	Force HTTPS for Web a	coss "	
🔗 Virtual Media					
System Health	3 - KV	M Encryption			
	•		KVM Encryption Ott Ott	y O Force	
00 User Management					
KVM Settings	4 IP	Access Control			
Device Settings	•		Please note: 'Apply' is required, or cha		
a Notwork			Enable IP Access Control		
o Dynamic DNS			Default policy ACCEPT *		
Security		Rule #	PMask	Policy	
Date/Time				ACCEPT ~	
Authentication		Appen	d Insert Re	place Delete	
a Event Log a SNMP Settings					
Y Maintenance	5 Gra	our bacad Sucto	m Access Control		
01	0	sup bused bysee	Please note: 'Apply' is required, or cha	noes will be lost.	
			Enable Group based System Access Contr		
			ACCEDIT III .	a	

Scroll down to display more items.

ASHBUTKVM			Oroup based System Access Control "		Remo	te Console connectedi
	Rule #	Default Action ACCE Starting P 0.0.0.0		Group	Action ACCEPT	
					ACCEPT W	
		Appand	Inzert Replace	Delete		
	6 User	Blocking				
		Max. n	unities of failed logins centry for in Block time (minutes) centry for in			
		Max. rv	Control of the second sec	inte) "]
		Max. n	Block time (minutes) (empty for in	inte) " dation "]
		Mac.n	Block time (minutes) (empty for in	inte) " dation "]

- 1. Security: Click this function key to enter the security submenus.
- 2. **HTTP Encryption:** Allows you to set to use the HTTPS connection to access the web.
- 3. **KVM Encryption:** Allows you to set to use the encrypted connection.
- 4. **IP Access Control:** Allows you to configure the detailed IP access control settings.
- Group based System Access Control: Allows you to limit several user access to the network by identifying their IP addresses.
- 6. User Blocking: Allows you to set the conditions when a user will be blocked.
- 7. Login limitations: Allows you to configure the login limitations.

Certificate

ASMESTIKAM		Remote Console connected
Remote Control	2 Certificate Signing Request (CSR)	
Virtual Media	Common name	
	Organizational unit	
System Health	Organization	
0 User Management	Locality/City	
KVM Settings	StateProvince	
	Country (ISO code)	
Device Settings	Enal	
Notwork Dynamic DNS	Challenge password	
Security	Continn Challenge password	
Certificate Total	Key length (bits) 1024 💌 -	
Authentication	Create	
Event Log SNMP Settings	* Stored value is equal to the default.	
Y Maintenance		

- 1. **Certificate:** Click this function key to enter the **Certificate** submenus and configure its related settings.
- 2. Certificate Signing Request (CSR): Allows you to define the Certificate Signing Request (CSR) form. Click Create to apply the settings.

Date/Time

ASNO3 DVM	_	Remote Console connected
Semante Carinel Seman	2 Date/Time Settings und min with the settings of our secretaries the provide setting of the set of	

- 1. Date/Time: Click this function key to enter the Date/Time submenus.
- 2. **Date/Time Settings:** Allows you to configure the internal realtime clock for the remote server.

Authentication

	Authentication Settings	
Remote Control	2 S Local Authentication "	
😥 Virtual Media	O LOAP	
System Health	User LDAP Server	
	Base DN of User LDAP Server	
20 User Management	Type of external LDAP Server Genoric LDAP server 9	
KVM Settings	Name of login-name attribute	
Device Settings	Name of user-entry objecticlass	
a Natwork	User search subfilter	
o Dynamic DNS o Security	Active Directory Domain	
Certificate		
a Date/Time	O RADAIS	
DEvent Log	Server Shared Secret Auth. Are. Timeout Retries	
3 SNMP Settings	Port Port	
SY Maintenance	1. 1012 • 1013 • 1 • 3 •	
	Marg entries	

- 1. **Authentication:** Click this function key to enter the **Authentication** submenus.
- 2. Authentication Settings: Allows you to configure the authentication settings. Click Apply to apply the settings.

Event Log

/1505	Aome Console Depart	
ASMERIKVM		Remote Console connected
	2 Event Log Targets	Aemola Cotaga consisted
		~

Scroll down to display more items.

ASMESTIKVM		Remote Console connected
a) tertenak a) tertenak a) Security a) Se	Beff Logap Select * Selection * S	

- 1. Event Log: Click this function key to enter the Event Log submenus.
- 2. **Event Log Targets:** Allows you to configure the event log targets.
 - · List Logging Enabled: Check the box to enable the event log list.
 - NFS Logging Enabled: Check the box to enable the NFS log list.
 - SMTP Logging Enabled: Check the box to enable to send e-mails to the address you've specified in the Receiver Email Address column.
 - SNMP Logging Enabled: Check the box to enable to send a SNMP trap to a specified destination IP address.
- 3. **Event Log Assignments:** Allows you to select the events that will generate an event log.

SNMP Settings

ASNO3 IKVM		Remote Console connected
Remote Control Quartural Morida 3 Systems Health Quartural Management	2 SNMP Settings Control Date Appet System Control Nation N	
Checko Settings Notwork Ornamic DDS Securty Cartificate Date/Time Authentication	Clinic times to when the SLMME MR Margin Present in default * Chicred value is equal to the default.	

- 1. SNMP Settings: Click this function key to enter the SNMP submenus.
- 2. SNMP Settings: Allows you to configure the Simple Network Management Protocol (SNMP) settings.

3.1.9 Maintenance

Click Maintenance to open its submenu.

Device Information



- 1. **Device Information:** Click this function key to enter the **Device Information** submenus.
- 2. **Device Information:** Displays the detailed information of the ASMB3-IKVM board.
- 3. **Connected Users:** Displays the user name, IP address and status of the users connected to the remote system.

Event Log

Remote Control	2 Even	t Log	[Prev [Next]	
Virtual Media	Date	Event	Description	
	0418/2008	23.55.39 Renote Console	Connection to client 192 158.0.11 established.	
System Health	04/16/2008	23:55:28 Authentication	User 'super' logged in from IP address 192 168.0.11	
0 User Management	01.01.1 970	00.00.20 Board Message	Device successfully started.	
	04/16/2008	13.50.40 Authentication	User 'super' logged in from IP address 192 168.0.11	
KVM Settings	01.01.1 970	00.00.24 Doard Message	Device successfully started.	
Device Settings	04/15/2008	22.55:29 Rendle Console	Connection to client 192 168.0.11 established.	
Contra Strange	04/15/2008	22.55.11 Authentication	User 'super' logged in from IP address 192.168.0.11	
Mainfenance	04/15/2008	17:15:31 Authentication	User 'super' logged in from IP address 192.168.0.11	
Device Information	04/15/2008	17:12:18 Board Message	Device successfully started.	
Event Log			[Prev [Next]	
Update Firmware Unit Reset				
Durit's Laboration				

- 1. Event Log: Click this function key to enter the Event Log submenus.
- 2. Event Log: Displays the event log list.

Update Firmware

ASNOTIKVM		Remote Console connected
Remote Control	2 Firmware Upload	
Virtual Media	Upload	
System Health		
User Management		
KVM Settings		
Device Settings		
Mainfenance		
ivice Information		
adate Firmware		

- 1. **Update Firmware:** Click this function key to enter the **Firmware Update** submenus.
- Firmware Upload: Type in the name of the firmware you want to update or click Browse to select the firmware file. Click Upload to start updating the firmware. It might take a few minutes to complete the procedure.

Unit Reset

	none Ecceste Strank	Remote Console connected
Remote Control	Reset Keyboard/Mouse 2	
System Health	Reset Video Engine	
Contraction Settings	Reset Device	
SY Maldemance	4	
eUnit Keset		

- 1. Unit Reset: Click this function key to enter the Unit Reset submenus.
- 2. Reset Keyboard/Mouse: Click to reset keyboard/mouse.
- 3. Reset Video Engine: Click to reset the video and its controller.
- 4. Reset Device: Click to reset the IPMI firmaware.

Chapter	3:	Software	support
onaptor	۰.	continuito	oupport

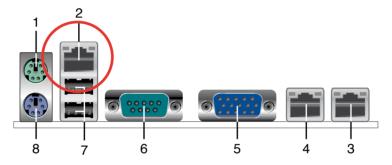
The Appendix shows the location of the IKVM LAN port for server management and BMC socket on several motherboards. This section also presents common problems that you may encounter when installing or using the server management board.



A.1 LAN port for server management

The ASUS server motherboards that support the ASMB3-IKVM comes with an IKVM LAN port. You must use the IKVM LAN port 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 illustrations below to identify the IKVM LAN port for server management on some server motherboards.



P5BV-M/RS100-E5 motherboard

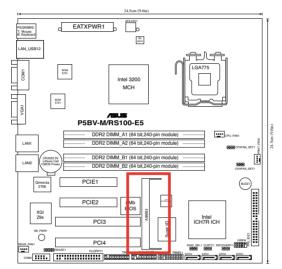


You can refer to motherboard manual for the location of IKVM LAN port.

A.2 BMC socket

The ASUS server motherboards that support the ASMB3-IKVM comes with a Baseboard Management Controller (BMC) socket.

Refer to the illustrations below to locate the BMC socket on different server motherboards.



P5BV-M/RS100-E5 motherboard

A.3

Troubleshooting

Į

This troubleshooting guide provides answers to some common problems that you may encounter while installing and/or using ASUS ASMB3-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 ASMB3-IKVM board	 Check if the LAN cable is connected to the IKVM LAN port. See section A.1 LAN port for server management for details.
	 Make sure that the IP address of both the remote and local/central servers are on the same subnet. (See chapter 2 for details.) Try "ping <romete_server_bmc_ip>" on local/ central server and make sure romete server could reply the ping request.</romete_server_bmc_ip>
	 Check if the IP source is set to [DHCP]. When set to [DHCP], you'll not be able to configure the IP address.
The cursor on the remote server console screen (refer to the screenshot on section 3.1.3) shows duplicates or becomes abnormal	 Check if the mouse setting is correct. Select different USB mouse type in drop-down menu for different operating sytems. See section 3.1.7 KVM Settings for details.
	 Click Options in the remote server console screen. From the pop-up menu, click Local Cursor, and then select Transparent or default.
	 Click Synchronize mouse in the remote server console screen. (Only for Linux operating system)
Cannot use Virtual Media to share the data stored in the CD-ROM image with the users in the remote server.	Check if you've installed NWLink IPX/SPX/NetBIOS compatible Transport Protocol item for the network. If no, follow below instruction to install the item.
	 Right-click the Network Connections icon on the Windows[®] taskbar, and then select Open Network Connections.
	 Right-click Local Area Connection, and then select Properties.
	3. Click Install button, the Select Network Connection Type screen appears.
	 Select Protocol, and then click Add Select NWLink IPX/SPX/NetBIOS
	compatible Transport Protocol, and then click OK to install.