ASMB3-IKVM

Server Management Board

E3730

First Edition V1
April 2008

Contents

Contents

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>	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.
<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>
`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 Product introduction

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

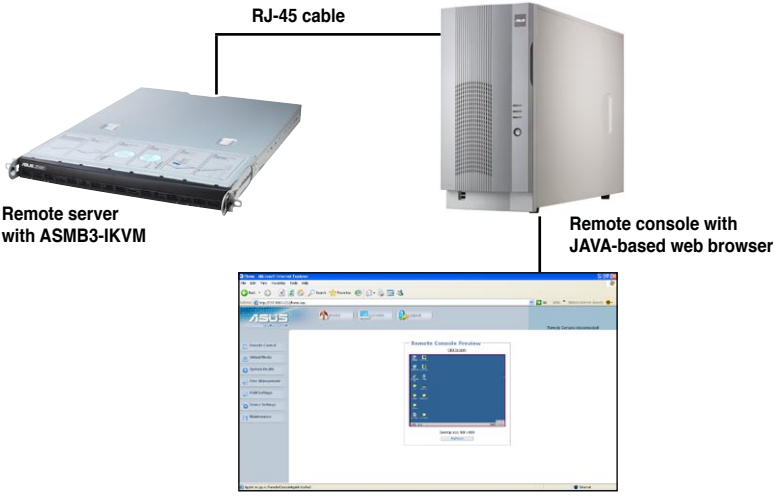
* Visit the ASUS website (www.asus.com) for an updated list of server motherboards that support the ASMB3-IKVM.

** See the Appendix for details.

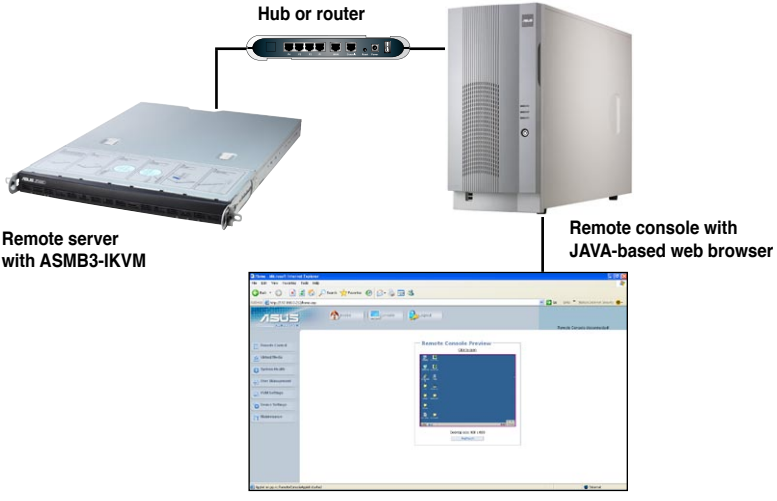
1.6 Network setup

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 Installation

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.

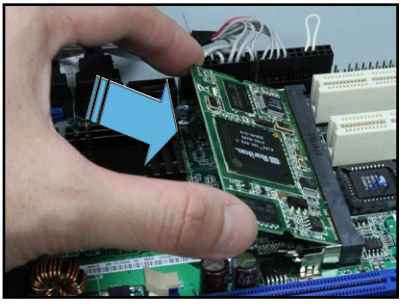
2.2 Hardware installation

To install the server management board:

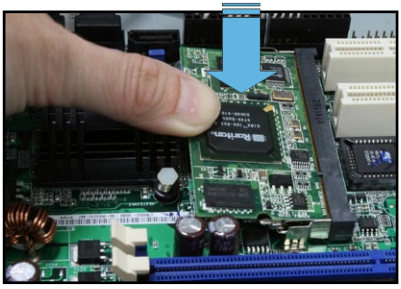
1. Remove the remote server system cover, and then locate the Baseboard Management Controller (BMC) socket on the motherboard.

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

2. Position the board at a 30º-45º angle, then match the notch on the board with the break on the socket.
3. 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.

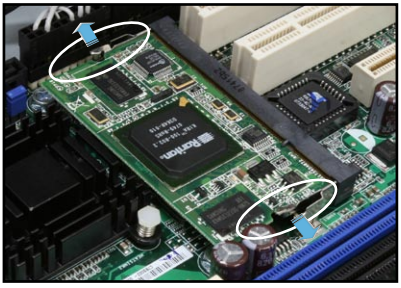
Refer to the Appendix for the location of the IKVM LAN port for server management on various server motherboards.

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

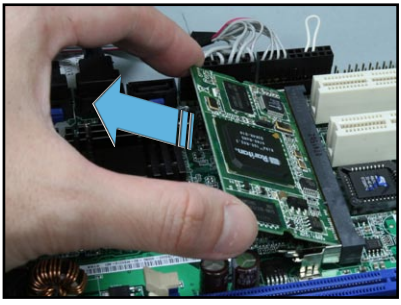
   For connection to a network hub or router, connect the other end of the LAN cable to the network hub or router.

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.

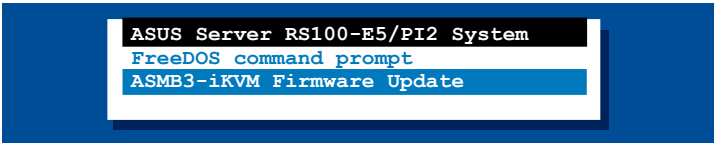


2.3 Firmware update

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.
2. Restart the remote server, then press <Del> 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.

```
Starting Firmware Upgrade
Uploading Firmware File
0% ------------------ 50% ----------------- 100%
Upload complete.
Flashing Firmware (takes about 1min)
Successfully upgraded firmware.
Press any key to continue ...
```

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.

- 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

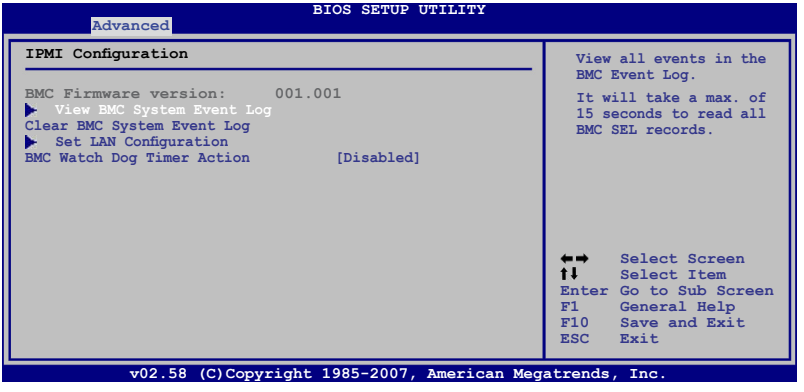
You must configure the network settings of both the remote server and the local/central server to establish communication for remote server control and monitoring.

Running the BIOS IPMI configuration

To configure the IPMI in the BIOS:

1. Restart the remote server, then press <Del> 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



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.

```
BIOS SETUP UTILITY
Advanced

Total Number of Entries:      0                    Use +/- to traverse
                                                   the event log.
SEL Entry Number:             [N/A]

                                                   ←→   Select Screen
                                                   ↑↓   Select Item
                                                   +-   Change Option
                                                   F1   General Help
                                                   F10  Save and Exit
                                                   ESC  Exit

v02.58 (C)Copyright 1985-2007, American Megatrends, 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.

```
BIOS SETUP UTILITY
Advanced

LAN Configuration.                                 Options

Current IP address in BMC:          192.168.0.212
Current Subnet Mask in BMC:         255.255.255.0  DHCP Mode
Current Gateway Address in BMC:     000.000.000.000Static Mode
Current MAC address in BMC:         00.E0.18.03.04.0C

IP Address Source                   [Static Mode]
IP Address                          [000.000.000.000]
Subnet Mask                         [000.000.000.000]
Gateway Address                     [000.000.000.000]

                                                   ←→ Select Screen
                                                   ↑↓ Select Item
                                                   +- Change Option
                                                   F1 General Help
                                                   F10 Save and Exit
                                                   ESC Exit

v02.58 (C)Copyright 1985-2007, American Megatrends, Inc.
```

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 <Del> 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.

```
                    PhoenixBIOS Setup Utility
  Main   Advanced   Server   Security   Boot   Exit

  ▶ Console Redirection                 Item Specific Help
  ▶ DMI Event Logging
  ▶ IPMI                                Additional setup menus to
                                        configure console.

  F1   Help   ↑↓  Select Item    -/+    Change Values      F9   Setup Defaults
  ESC: Exit   →←  Select Menu    Enter  Select ▶ Sub-menu  F10   Save and Exit
```

IPMI Configuration

```
                    PhoenixBIOS Setup Utility
                         Server

              IPMI                          Item Specific Help

  IPMI Specification Version      2.0
  BMC Firmware Version            1.04       Enable/Disable IPMI
  System Event Logging            [Enabled]  event logging. Disabling
  Clear System Event Log          [Disabled] will still log events
  Existing Event Log number       34         received via the system
  Event Log Control                          interface.
    SYS Firmware Progress         [Disabled]
    BIOS POST Errors              [Enabled]
  BIOS POST Watchdog              [Disabled]
  OS Boot Watchdog                [Disabled]
    Timer for loading OS (min)    [ 10]
    Time out action               [No action]
  Date Format to show             [MM DD YYYY]
  Date Separator                  [/]

  F1   Help   ↑↓  Select Item    -/+    Change Values      F9   Setup Defaults
  ESC: Exit   →←  Select Menu    Enter  Select ▶Sub-menu   F10   Save and Exit
```

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]

Date Separator [/]

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                            Display the System Event
▶ System Event Log (list mode)                Log.

  DHCP                          [Enabled]
  IP Address                    [000.000.000.000]

F1   Help   ↑↓  Select Item    -/+   Change Values      F9   Setup Defaults
ESC: Exit   →←  Select Menu    Enter Select ▶Sub-menu   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.

```
PhoenixBIOS Setup Utility
Server

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 =               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

F1   Help   ↑↓  Select Item    -/+   Change Values      F9   Setup Defaults
ESC: Exit   →←  Select Menu    Enter Select ▶Sub-menu   F10  Save and Exit
```

System Event Log (list mode)

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

```
PhoenixBIOS Setup Utility
Server

System Event Log (list mode)

Event ID    Sensor Name          Sensor Type        Date/Time Stamp
-----------------------------------------------------------------------
▶ 001       CPU2temperature1     Temp               04/17/2006  16:10:44
            Upper Non-critical Going High, Assertion
▶ 002       CPU2temperature1     Temp               04/17/2006  16:10:44
            Upper Critical Going High, Assertion
▶ 003       CPU2temperature2     Temp               04/17/2006  16:10:44
            Upper Non-critical Going High, Assertion
▶ 004       CPU2temperature2     Temp               04/17/2006  16:10:44
            Upper Critical Going High, Assertion
▶ 005       DIMM_01 AMB temp     Temp               04/17/2006  16:10:44
            Lower Non-critical Going Low, Assertion
▶ 006       DIMM_01 AMB temp     Temp               04/17/2006  16:10:45
            Upper Critical Going Low, Assertion

F1   Help   ↑↓  Select Item    -/+   Change Values     F9   Setup Defaults
ESC: Exit   →←  Select Menu   Enter  Select ▶Sub-menu   F10  Save and Exit
```

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 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 =                 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

F1   Help   ↑↓  Select Item    -/+   Change Values     F9   Setup Defaults
ESC: Exit   →←  Select Menu   Enter  Select ▶Sub-menu   F10  Save and Exit
```

DHCP

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.
2. Restart the remote server, then press <Del> 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 ................. Run in ASMI mode
    -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 ................ Show program version and information
    reset .............. Reset the device
    fw ................. Firmware operations
    cfg ................ Backup or restore device configuration
    serial ............. Serial number operations
    defaults ........... Reset device to factory settings
    ip ................. Read or set IP address
    gw ................. Read or set default gateway address
    netmask ............ Read or set subnet mask
    mac ................ Read or set MAC address
    ipsrc .............. Get or specify IP source configuration
    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>_
```

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>>	Upgrade BMC firmware
kirarari ip	Show IP setting
kirarari ip set xxx.xxx.xxx.xxx	Set IP to xxx.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>>	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.

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.
3. 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.

```
C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>kirarari fw upgrade rs100e51.bin
Starting Firmware Upgrade
Uploading Firmware File
0% ------------------ 50% ------------------ 100%
*****************************************************
Upload complete.
Flashing Firmware (takes about 1min)
Successfully upgraded firmware.

C:\ASMB3\IKVM\MODEL\RS100-E5\PI2>
```

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>
```

3. 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.
4. Type **kirarari ip set xxx.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.xxx**
   (b) Type **kirarari gw set xxx.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:\ASMB3\IKVM\MODEL\RS100-E5\PI2>kirarari admin name super
Successfully set administrator username to super
C:\ASMB3\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 Software support

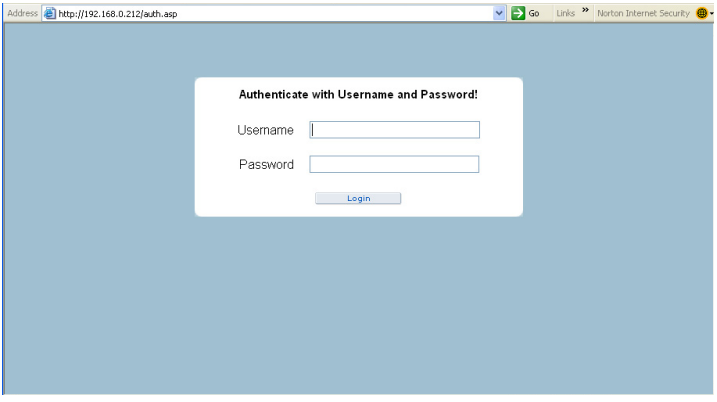
3.1 Web-based user interface

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.

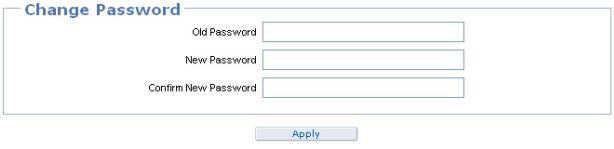
You should install JRE on remote console first before using web-based management. You can find **JRE** from the folder **JAVA** of the ASMB3-IKVM support CD. You can also download JRE from **http://java.sun.com/javase/downloads**.

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.

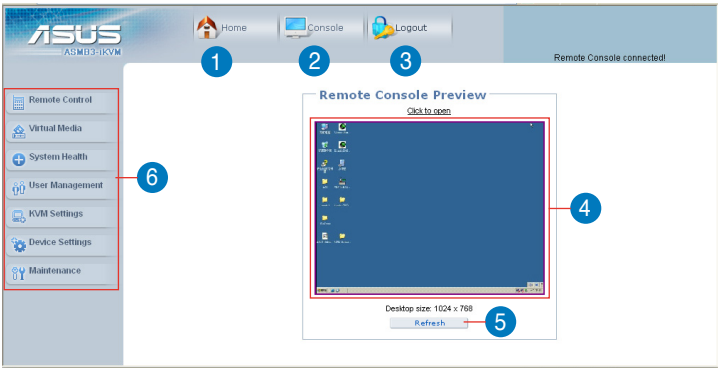


A **Change Password** screen appears asking you to change the password when you log in the utility for the first time. Type in the default password (pass) in the **Old password** column, and then type in the new password in the **New password** and **Confirm New Password** columns.



3.1.2 Home page

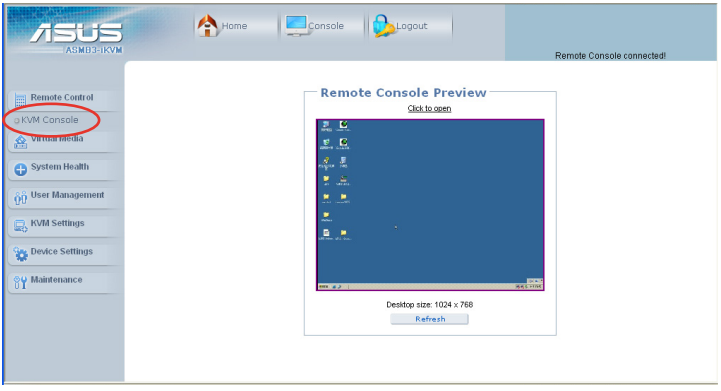
The home page displays when you login in the utility sucessfully.



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

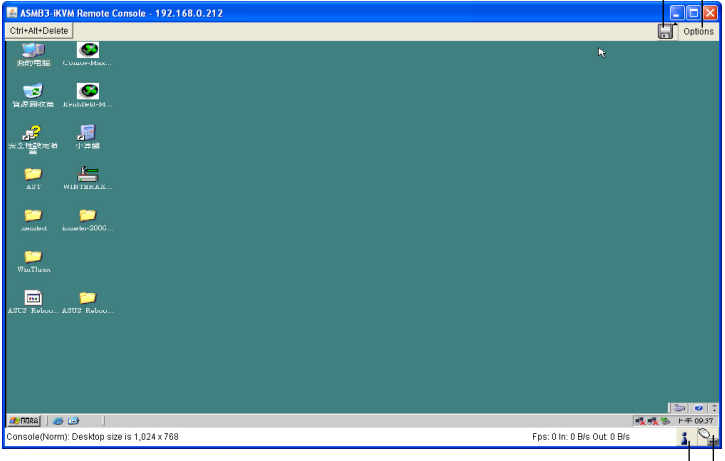
Click **Remote Control** to open its submenu, and then click **KVM Console** to open remote server console screen.



Remote server console screen

Click to open the **Options** menu

Click to open/close the **Drive Redirection** window



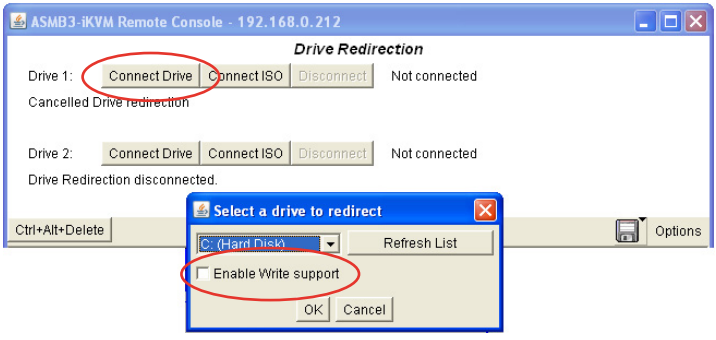
Indicates the number of networks (users) that are connected via Console Redirection

Indicates the availability of keyboard and mouse

Drive Redirection

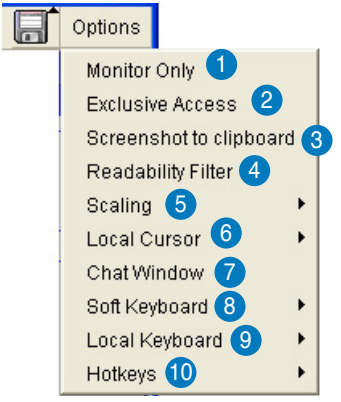
The **Drive Redirection** function allows you to share your lcoal drives (floppy disk drives, CD-ROM and hard disk drives) with users in the remote system. Click **Connect Drive**, and then a **Select a drive to redirect** screen appears, allowing you to select the drives you want to share in the remote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



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 wnat to share in the remote system.

Options menu



1. **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.
2. **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.

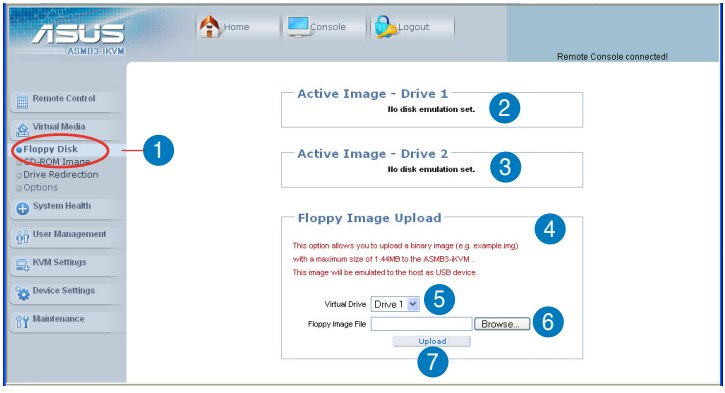
* This option is available only when the **RC settings (Exclusive Access)** permission has been enabled. Refer to **3.1.6 User Management** for details.

3.1.4 Virtual Media

Click **Virtual Media** to open its submenu.

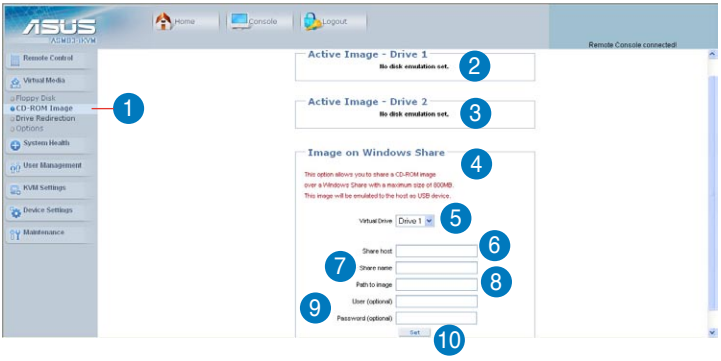
> You may use the **Drive Redirection** funciton from the remote server console screen. Refer to page 3-5 for details.

Floppy Disk



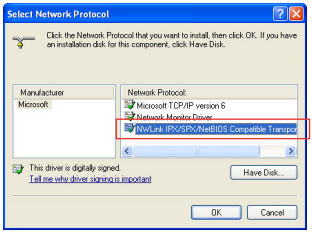
1. **Floppy Disk:** Click this function key to upload the data stored in the local floppy disk image to the remote server.
2. **Active Image - Drive 1:** Displays the data that has been uploaded to Drive 1 of the remote server.
3. **Active Image - Drive 2:** Displays the data that has been uploaded to 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

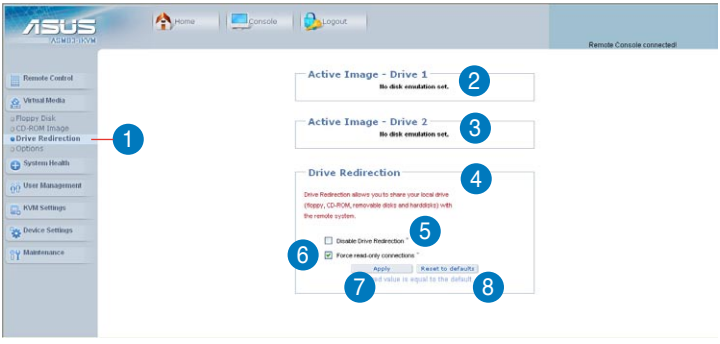


1. **CD-ROM Image:** Click this function key to share data stored in your CD-ROM image with other users in the remote server through the Windows Share application via USB.
2. **Active Image - Drive 1:** Displays the file name of the data in Drive 1 of the remote server.
3. **Active Image - Drive 2:** Displays the file name of the data in Drive 2 of the remote server.
4. **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.
9. **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.

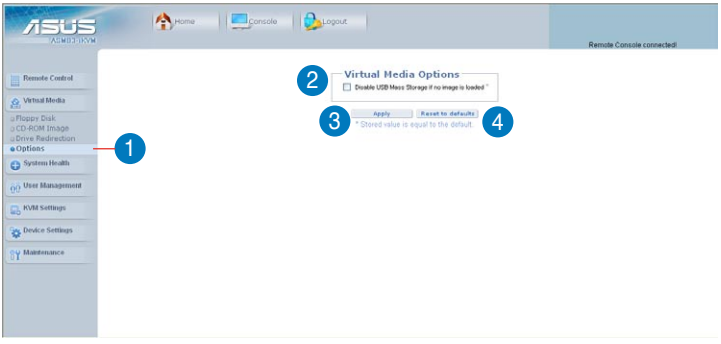


Drive Redirection



1. **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.
6. **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

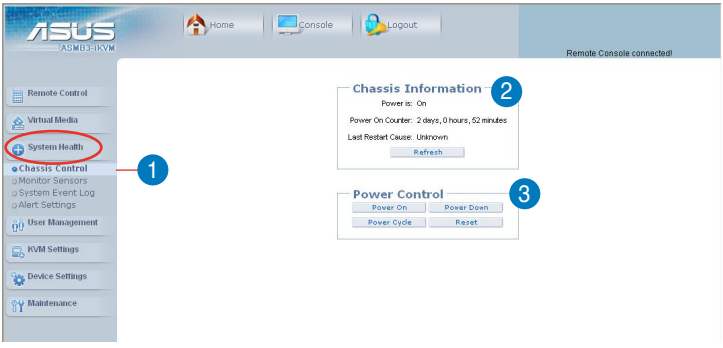


1. **Options:** Click this function key to open the Virtual Media options.
2. **Virtual Media Options:** Check this box to disable the funciton of Virtual Media options to prevent data stored in a local drive from being accessed by the user in the remote server.
3. **Apply:** Click to apply the setting 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.

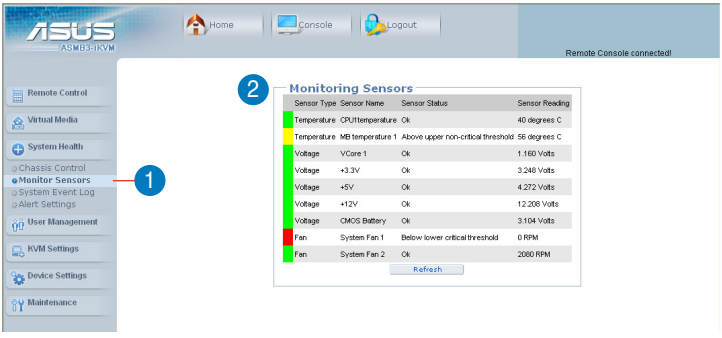
Chassis Control



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.

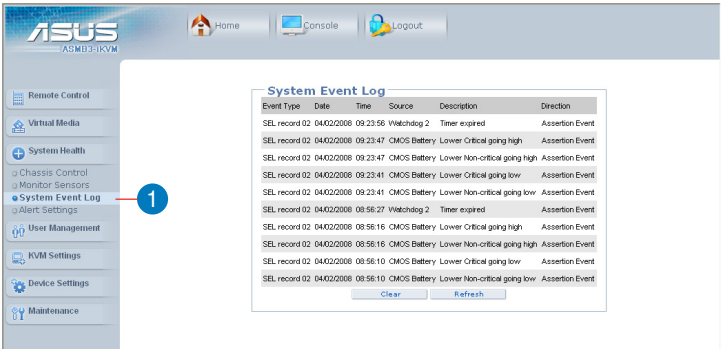
Click **Power Cycle** to turn off the remote server, and allow the remote server to be powered on automatically after about 3 minutes.

Monitor Sensors



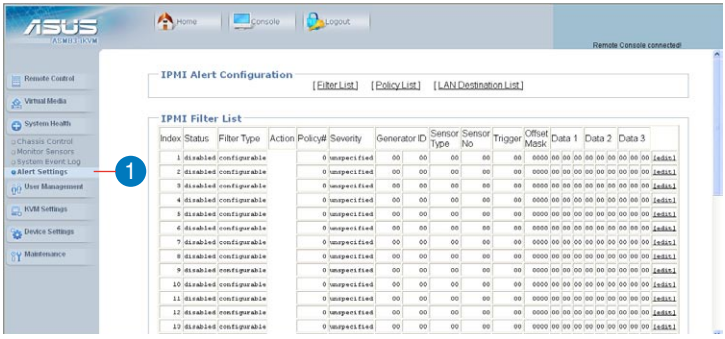
1. **Monitor Sensors:** Click this function key to display the health monitoring information for the remote server.
2. **Monitoring Sensors:** Allows you to see the related health monitoring information for the remote server. Click **Refresh** to update the information on this window.

System Event Log



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

Alert Settings

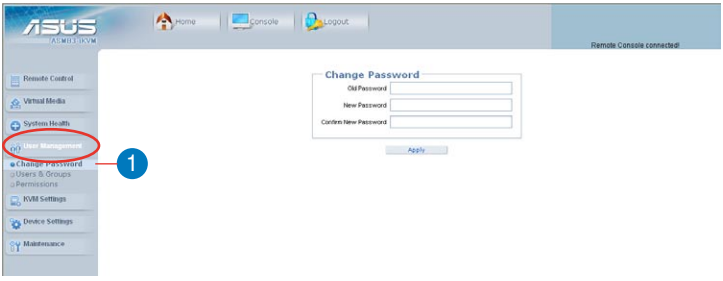


1. **Alert Settings:** Click this function key to enter the alert settings submenu for the remote server.

3.1.6 User Management

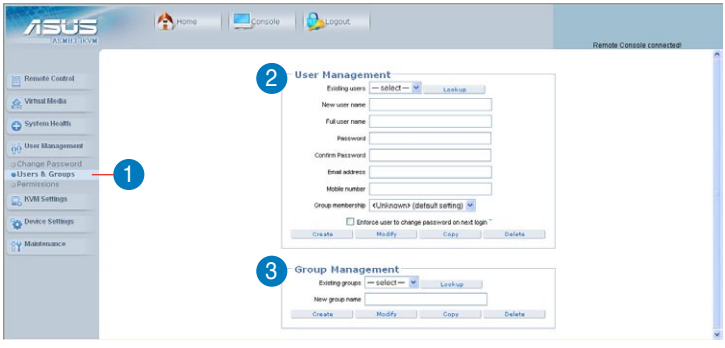
Click **User Management** to open its submenu.

Change Password



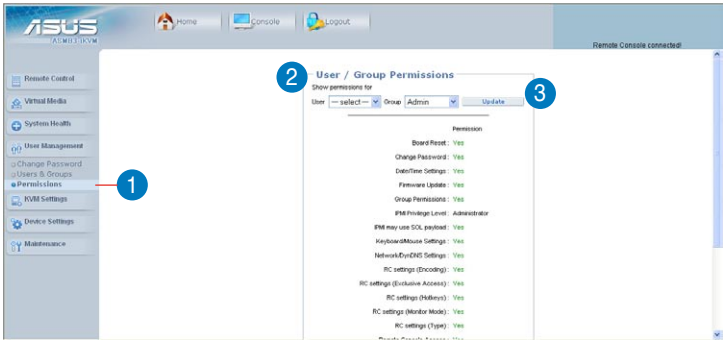
1. **Change Password:** Click this function key to enter the **Change Password** window. After entering all the necessary information, click **Apply** to apply the new settings.

Users & Groups



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



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.

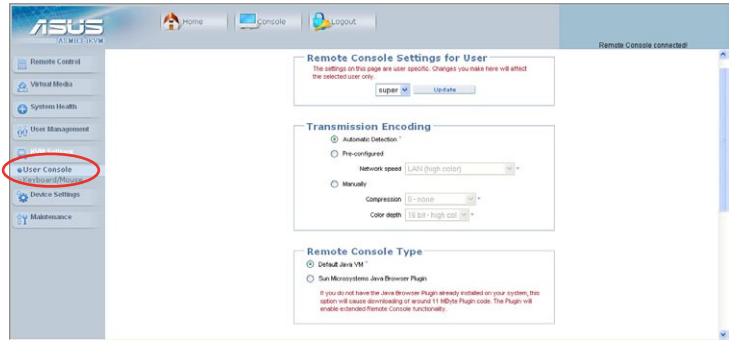
You can only set the user permission by setting group only.

3.1.7 KVM Settings

Click **KVM Settings** to open its submenu.

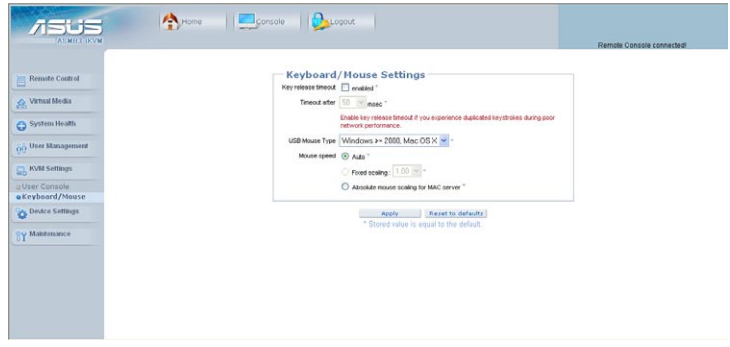
User Console

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



Keyboard/Mouse

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

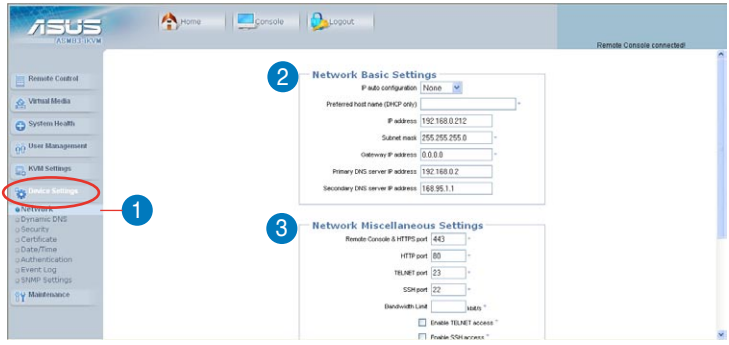


Set **USB Mouse Type** to [Windows > = 2000, Mac OS X] if your operating system is Windows®; set **USB Mouse Type** to [Other Operating Systems] if your operating system is Linux.

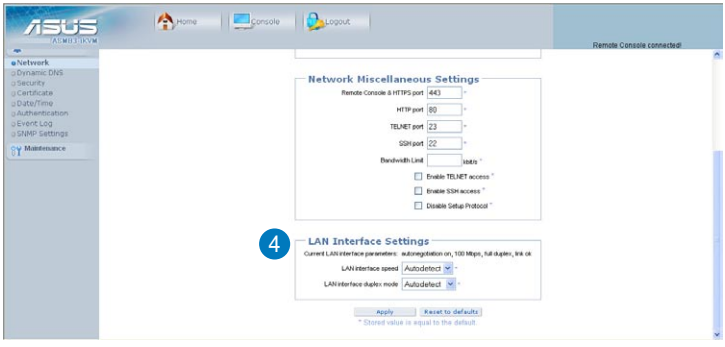
3.1.8 Device Settings

Click **Device Settings** to open its submenu.

Network

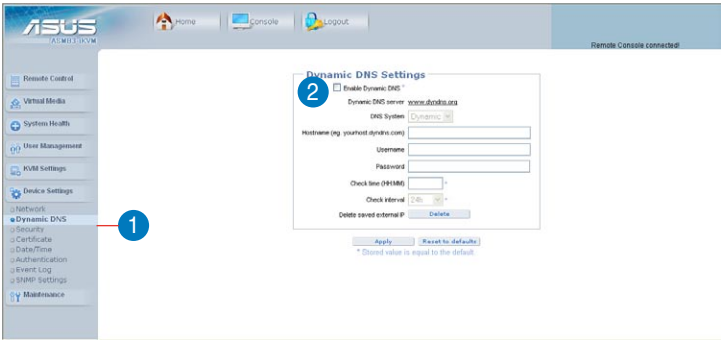


Scroll down to display more items.



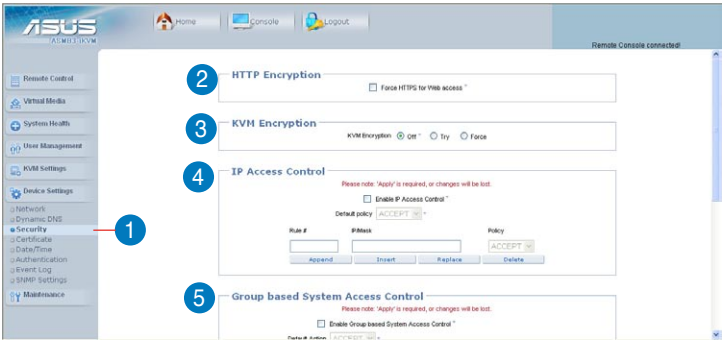
1. **Network:** Click this function key to enter the network submenus.
2. **Network Basic Settings:** Allows you to configure basic settings for the network.
3. **Network Miscellaneous Settings:** Allows you to configure other settings for the network.
4. **LAN Interface Settings:** Allows you to configure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

Dynamic DNS

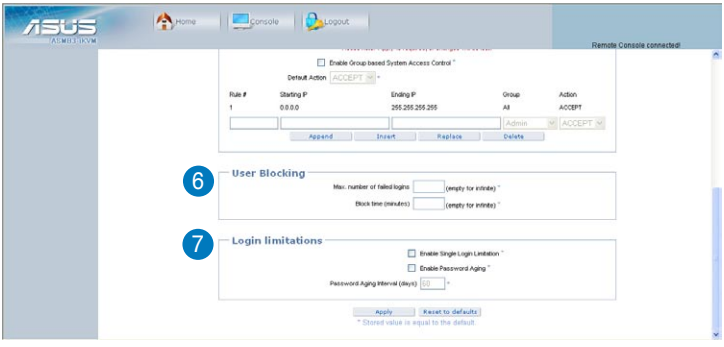


1. **Dynamic DNS:** Click this function key to enter the dynamic DNS submenus and configure its related settings.
2. **Enable Dynamic DNS:** Check this box to enable the dynamic DNS service.

Security

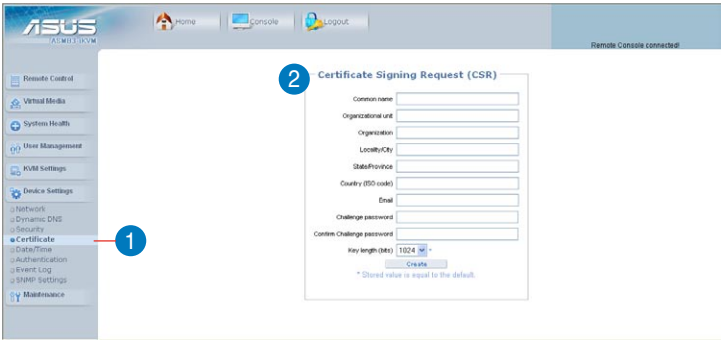


Scroll down to display more items.



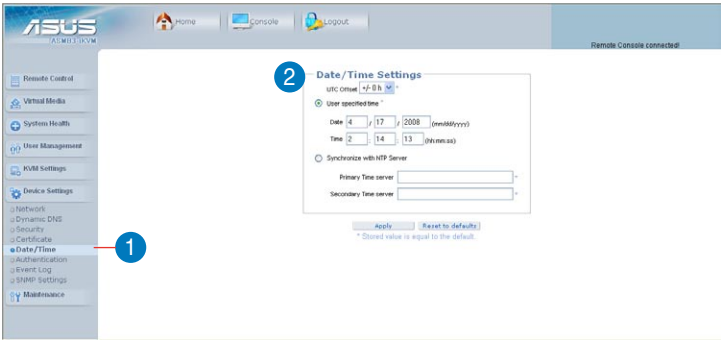
1. **Security:** Click this function key to enter the security submenus.
2. **HTTP Encryption:** Allows you to set to use the the HTTPS connection to access the web.
3. **KVM Encryption:** Allows you to set to use the encrypted connection.
4. **IP Access Control:** Allows you to configure the detailed IP access control settings.
5. **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



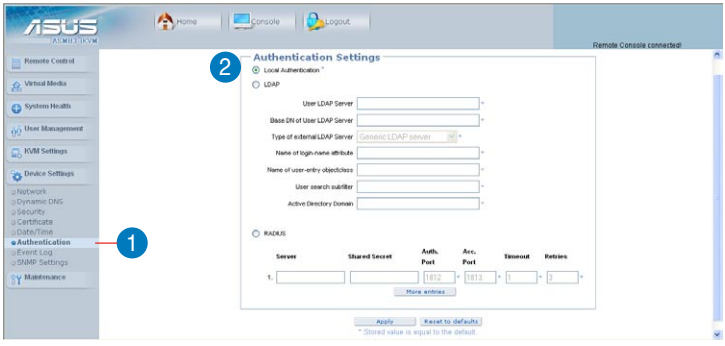
1. **Certificate:** Click this function key to enter the **Certificate** submenus and configure its related settings.
2. **Certificate Signing Request (CSR):** Allows you to define the Certificate Signing Request (CSR) form. Click **Create** to apply the settings.

Date/Time



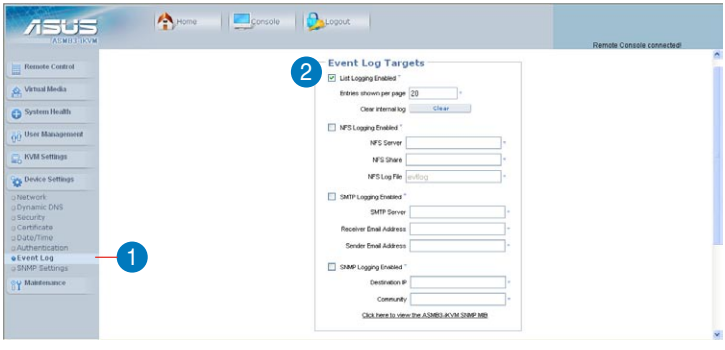
1. **Date/Time:** Click this function key to enter the **Date/Time** submenus.
2. **Date/Time Settings:** Allows you to configure the internal realtime clock for the remote server.

Authentication

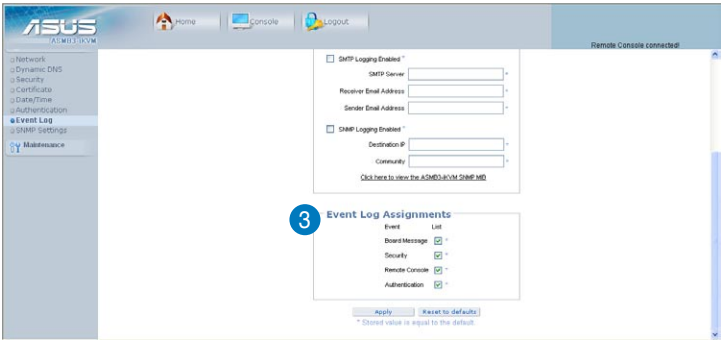


1. **Authentication:** Click this function key to enter the **Authentication** submenus.
2. **Authentication Settings:** Allows you to configure the authentication settings. Click **Apply** to apply the settings.

Event Log

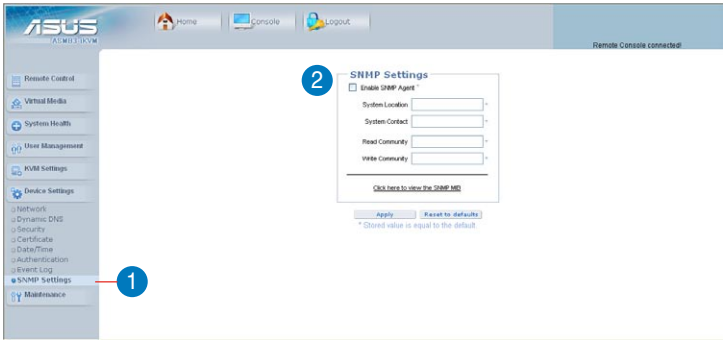


Scroll down to display more items.



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

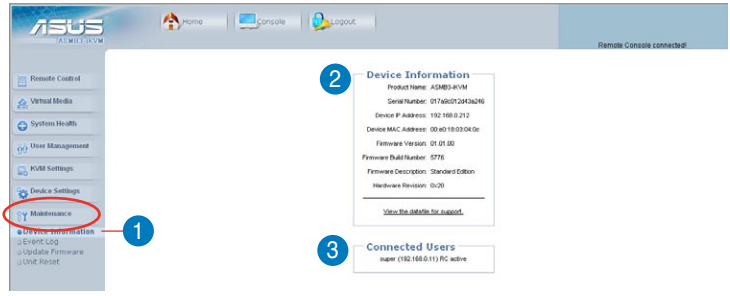


1. **SNMP Settings:** Click this function key to enter the **SNMP** submenus.
2. **SNMP Settings:** Allows you to configure the S**imple Network Management Protocol (SNMP)** settings.

3.1.9 Maintenance

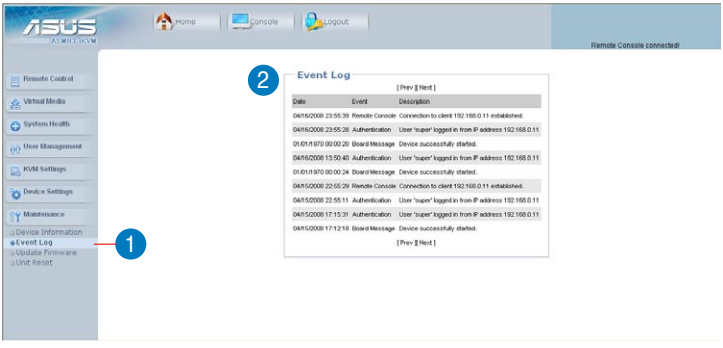
Click **Maintenance** to open its submenu.

Device Information



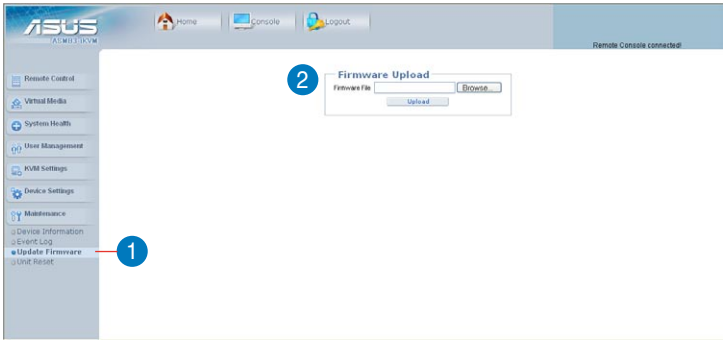
1. **Device Information:** Click this function key to enter the **Device Information** submenus.
2. **Device Information:** Displays the detailed information of the ASMB3-IKVM board.
3. **Connected Users:** Displays the user name, IP address and status of the users connected to the remote system.

Event Log



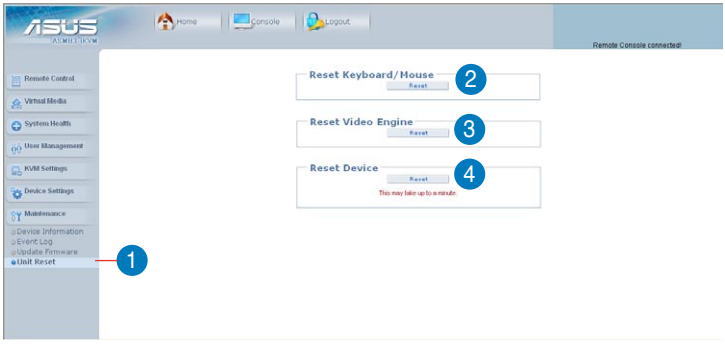
1. **Event Log:** Click this function key to enter the **Event Log** submenus.
2. **Event Log:** Displays the event log list.

Update Firmware



1. **Update Firmware:** Click this function key to enter the **Firmware Update** submenus.
2. **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



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.

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.

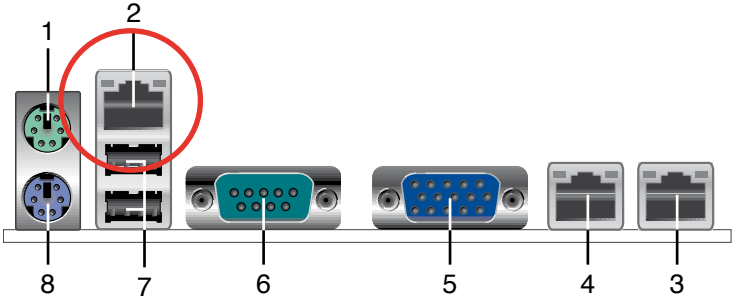
A Reference information

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



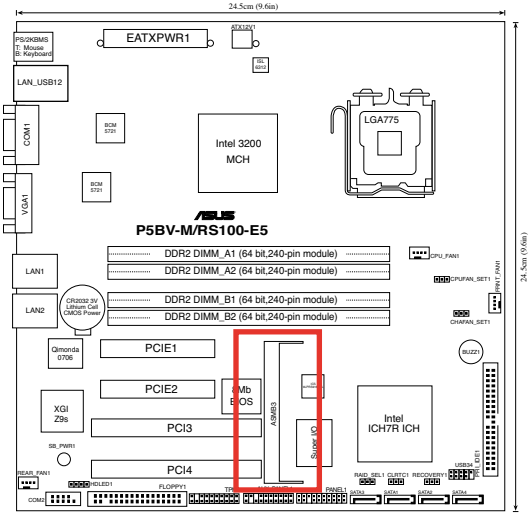
You can refer to motherboard manual for the location of IKVM LAN port.

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

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	1. Check if the LAN cable is connected to the IKVM LAN port. See section **A.1 LAN port for server management** for details. 2. 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. 3. 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	1. 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. 2. Click **Options** in the remote server console screen. From the pop-up menu, click **Local Cursor**, and then select **Transparent** or **default**. 3. 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. 1. Right-click the **Network Connections** icon on the Windows® taskbar, and then select **Open Network Connections**. 2. Right-click **Local Area Connection**, and then select **Properties**. 3. Click **Install** button, the **Select Network Connection Type** screen appears. 4. Select **Protocol**, and then click **Add...**. 5. Select **NWLink IPX/SPX/NetBIOS compatible Transport Protocol**, and then click **OK** to install.