ASMB8-iKVM

Server Management Board

User Guide

E10970
Revised Edition V2
October 2015

Contents

Contents

Chapter 4: Web-based User Interface

Contents

Appendix

Notices

Federal Communications Commission Statement

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

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

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

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

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

Canadian Department of Communications Statement

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

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

REACH

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

ASUS Recycling/Takeback Services

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

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

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

Safety information

Electrical safety

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

Operation safety

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

About this guide

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

How this guide is organized

This guide contains the following parts:

- **Chapter 1: Product Introduction**

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

- **Chapter 2: Hardware Information**

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

- **Chapter 3: ASUS Host Management Controller Set-up**

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

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

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

- **Appendix**

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

Where to find more information

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

1. **ASUS websites**

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

2. **Optional documentation**

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

Conventions used in this guide

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

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

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

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

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

Typography

Bold text	Indicates a menu or an item to select.
Italics	Used to emphasize a word or a phrase.
<Key>	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> + <Del>
`Command`	Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets. Example: At DOS prompt, type the command line: `format A:/S`

ASMB8-iKVM specifications summary

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

*** Specifications are subject to change without notice.**

1 Product Introduction

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

1.1 Welcome!

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

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

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

1.2 Package contents

Check your server management board package for the following items.

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

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

1.3 Features

1. IPMI 2.0

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

2. Private I2C Bus

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

3. PMBus*

- Support Power supply for PMBus device

4. PSMI*

- Support Power supply for PSMI bus device

5. Web-base GUI

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

6. Update Firmware

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

7. Notification

- PET
- SNMP Trap
- e-Mail

8. KVM over Internet

- Web-based remote console

9. Remote Update BIOS

- Use Remote floppy to update BIOS

10. Remote Storage (Virtual Media)

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

11. Remote Install OS

- Use remote storage to remote install OS

12. Support MIB file

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

*** A power supply supported PMBus and PSMI is necessary.**
**** Specifications are subject to change without notice.**

1.4 System requirements

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

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

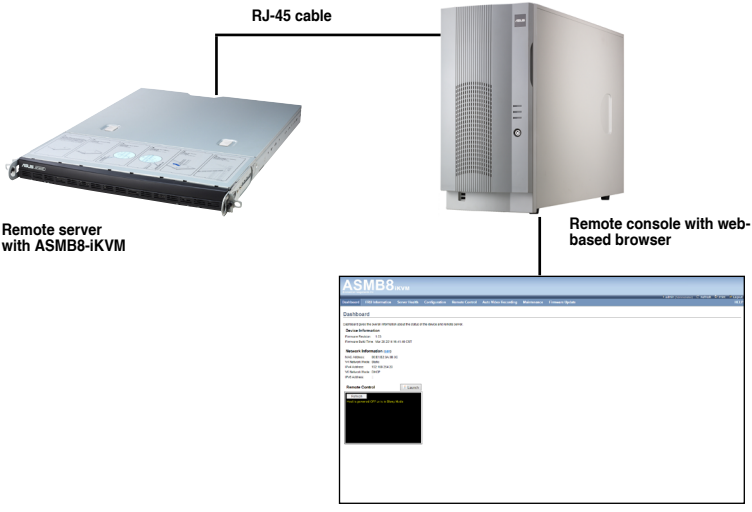
* Visit www.asus.com for an updated list of server motherboards that support the ASMB8-iKVM.

** See the Appendix for details.

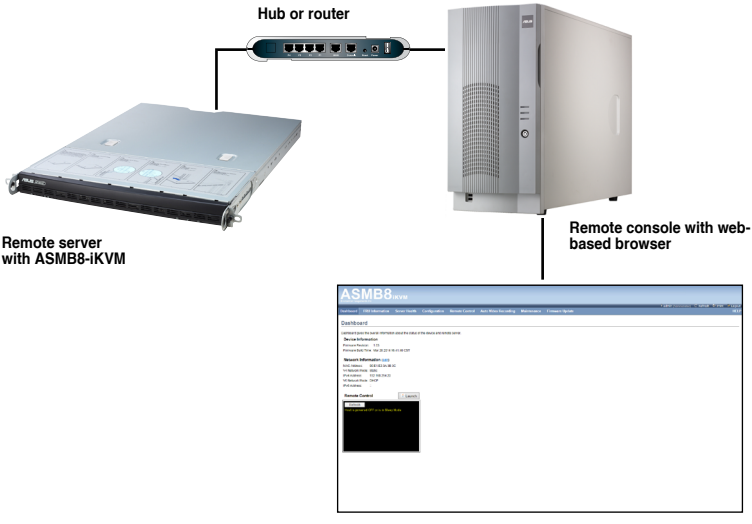
1.5 Network setup

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

Direct LAN connection



LAN connection through a network hub



2 Hardware Information

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

2.1 Before you proceed

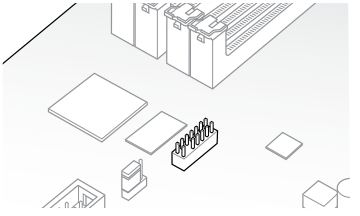
Take note of the following precautions before you install the server management board to the remote server system.

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

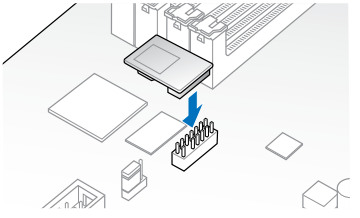
2.2 Hardware installation

To install the server management board:

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



2. Orient and press the Management Card in place.



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

3. Press the board firmly until it is completely seated in place.

4. Insert the LAN cable plug to the LAN port for server management.

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

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

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

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

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

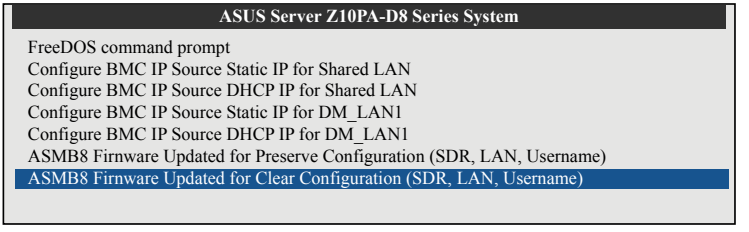
2.3 Firmware update and IP configuration

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

2.3.1 Firmware update

To update the firmware:

1. Insert the support CD into the optical drive.
2. Restart the remote server then press <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, select **ASMB8-iKVM Firmware Update for Clear Configuration** from the main menu and press <Enter> to enter the sub-menu.



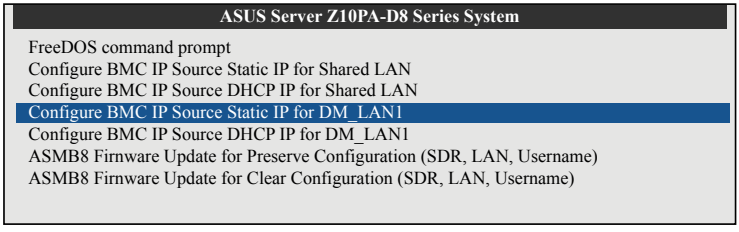
6. From the confirmation message, select <Yes> to update the firmware.

7. Wait for the firmware updating process to finish.

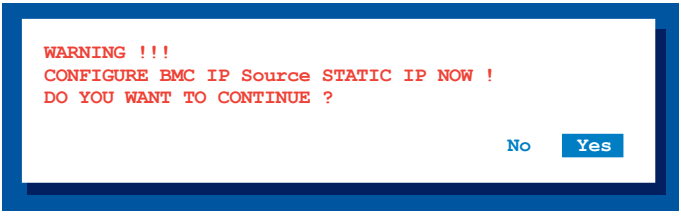
You may update the firmware from the web-based user interface. Refer to the **Firmware Update** section for more information.

2.3.2 Configure BMC IP source static IP

1. Insert the support CD into the optical drive.
2. Restart the remote server then press <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, select **Configure BMC IP Source Static IP for Shared LAN (or DM_LAN1) from the main menu** and press <Enter> to enter the sub-menu.



6. Select <Yes> from the confirmation window.

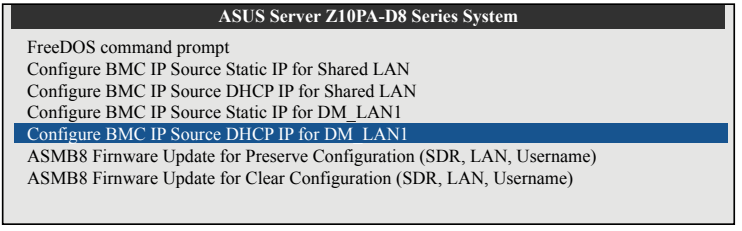


7. Wait for the configuration to finish. When done, press any key to continue.

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

2.3.3 Configure BMC IP source DHCP

1. Insert the support CD into the optical drive.
2. Restart the remote server then press <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, select **Configure BMC IP Source DHCP for Shared LAN (or DM_LAN1)** from the main menu and press <Enter> to enter the sub-menu.



6. Select <Yes> from the confirmation window.

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

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

2.4 BIOS configuration

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

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

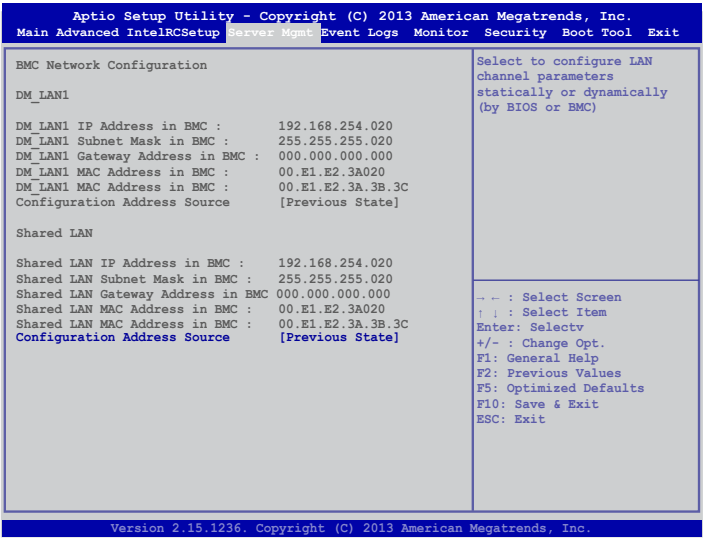
2.4.1 Running the BIOS BMC configuration

To configure the BMC in the BIOS:

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

2.4.2 BMC network configuration

Allows you to set the BMC LAN Parameter settings.



Configuration Source [Previous State]

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

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

Station IP Address

Allows you to set the BMC IP address.

Subnet Mask

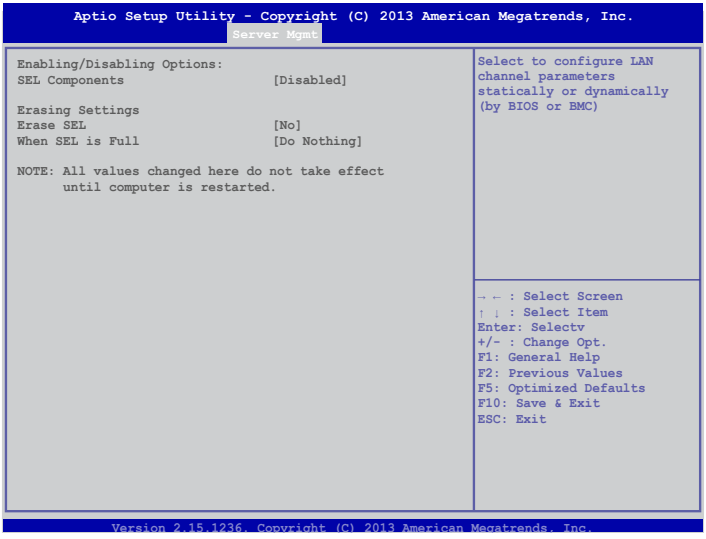
Allows you to set the BMC subnet mask. We recommend that you use the same Subnet Mask you have specified on the operating system network for the used network card.

Gateway IP Address

Allows you to set the Gateway IP address.

2.4.3 System Event Log

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



SEL Components [Disabled]

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

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

Erase SEL [No]

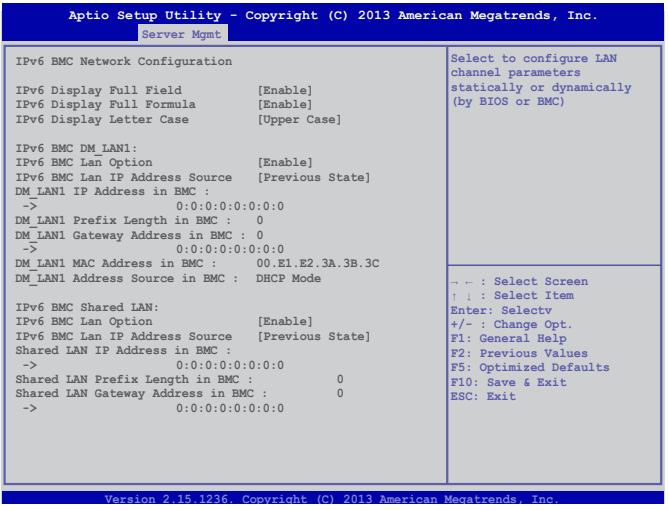
Allows you to select how to erase SEL.
Configuration options: [No] [Yes, On next reset] [Yes, On every reset]

When SEL is Full [Do Nothing]

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

2.4.4 IPv6 BMC Network Configuration

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



IPv6 BMC DM_LAN1 IP Address Source [Previous State]

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

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

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

IPv6 BMC DM_LAN1 IP Address
Allows you to set the IPv6 BMC DM_LAN1 IP address.

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

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

IPv6 BMC Shared LAN IP Address Source [Previous State]

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

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

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

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

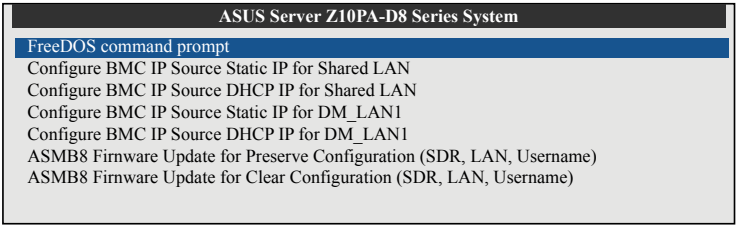
IPv6 BMC Shared LAN Default Gateway
Allows you to set the IPv6 BMC Shared LAN Gateway IP address.

2.5 Running the ASMC8 utility

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

To run the ASMC8 utility:

1. Insert the support CD into the optical drive.
2. Restart the remote server then press <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, select **FreeDOS command prompt** from the main menu then press <Enter>.



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

```
+-----------------------------------------------+
|  ASUS Server Management card Utility 8.00 Help Menu          |
+-----------------------------------------------+
Usage:
ASMC8  -kcs[smic/bt/pci_smic] NetFn command data . . . .
ASMC8  -bmc_ip_source source[1:Static, 2:DHCP]
ASMC8  -bmc_ip ip_addr[10.10.10.20]
ASMC8  -bmc_mask ip_mask[255.255.255.0]
ASMC8  -bmc_gateway ip_addr[10.10.10.254]
ASMC8  -ipv6_source source[1:Static, 2:DHCP]
ASMC8  -ipv6 ipv6_addr[2001: 0db8 : 1234 : 5678 : 8769 : e1cb : aabb : ccdd]
ASMC8  -ipv6_prefix prefix_length[64]
ASMC8  -pet_ip_mac ip_addr[10.10.10.20] mac_addr[010203040506]
ASMC8  -bmc_ip_s_lan1 source[1:Static, 2:DHCP]
ASMC8  -bmc_ip_lan1 ip_addr[10.10.10.20]
ASMC8  -bmc_mask_lan1 ip_mask[255.255.255.0]
ASMC8  -bmc_g_lan1 ip_addr[10.10.10.254]
ASMC8  -ipv6_s_lan1 source[1:Static, 2:DHCP]
ASMC8  -ipv6_lan1 ip_addr[2001: 0db8 : 1234 : 5678 : 8769 : e1cb : aabb : ccdd]
ASMC8  -ipv6_prefix_lan1 prefix_length[64]
ASMC8  -pet_ip_m_lan1 ip_addr[10.10.10.20] mac_addr[010203040506]

<Press any key to see the next page> <ESC key to break>
```

Press any key to see next page.

ASMC8 Help Menu options

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

2.5.1 Configuring the LAN controller

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

To configure the LAN port of the remote server:

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

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

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

When finished, the utility returns to the DOS prompt.

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

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

2.5.2 Configuring the user name and password

You may change your user name and password from the ASMC8 utility.

To change the user name and password:

1. Insert the support CD into the optical drive.
2. Restart the remote server then press <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, select **FreeDOS command prompt** from the main menu then press <Enter>.
6. From the **C:>** prompt, type **ASMC8 -user_name xxxxx** then press <Enter> to change the user name.

```
c:\>ASMC8 -user_name super
Detect MotherBoard     -> (Z10PA-D8 Series)
Detect KCS Interface

Change User Name to super
c:\>
```

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

3

ASUS Host Management Controller Set-up

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

3.1 ASUS Host Management Controller Setup

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

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

3.1.1 Installing and launching the ASUS Host Management Controller Setup utility

To install the ASUS Host Management Controller Setup utility:

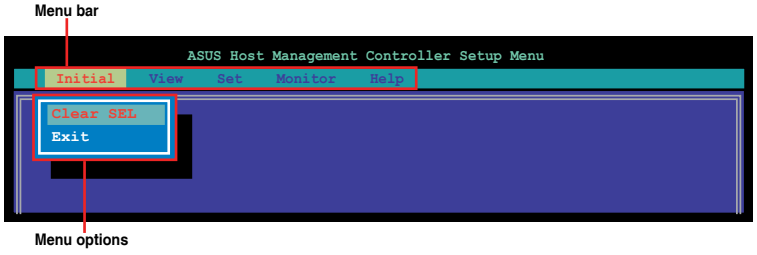
1. Boot the server in DOS mode using the support CD.
2. At the prompt, type **ASMC8**, then press <Enter> to display the ASMC8 Utility Help Menu. The screen appears as shown.

```
C:\>ASMC8
```

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

3.1.2 Command fields

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

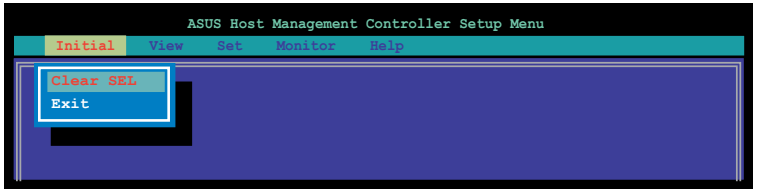


3.1.3 Initial

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

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

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



3.1.4 View

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

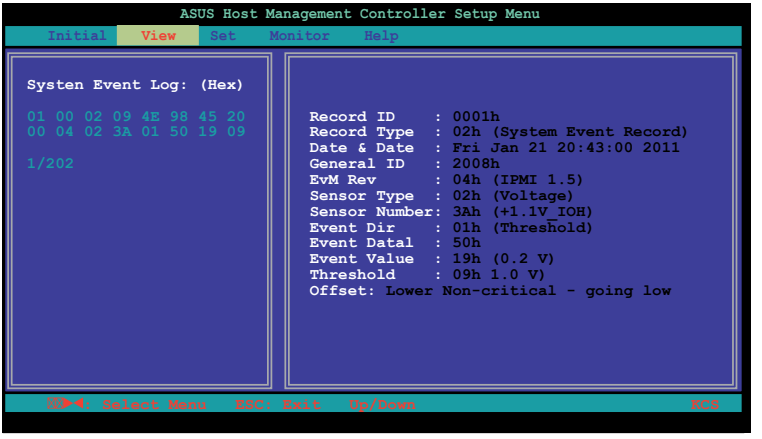
To view the System Event Log (SEL):

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

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

2. Use the down arrow key to display the next sensor event.

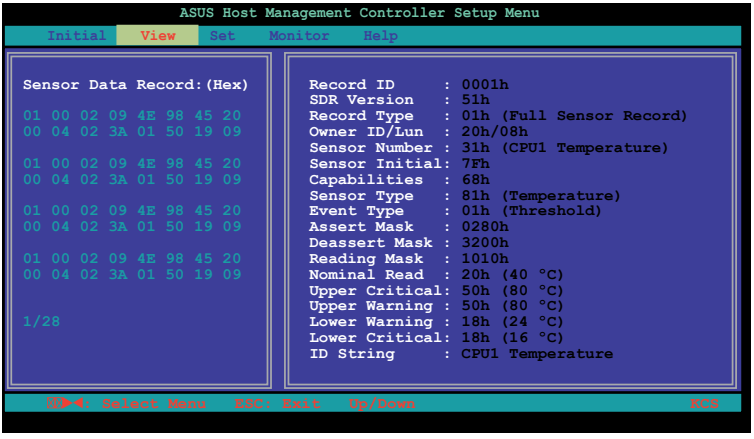
3. Press <Esc> to return to the main screen.



To view the System Data Record (SDR):

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

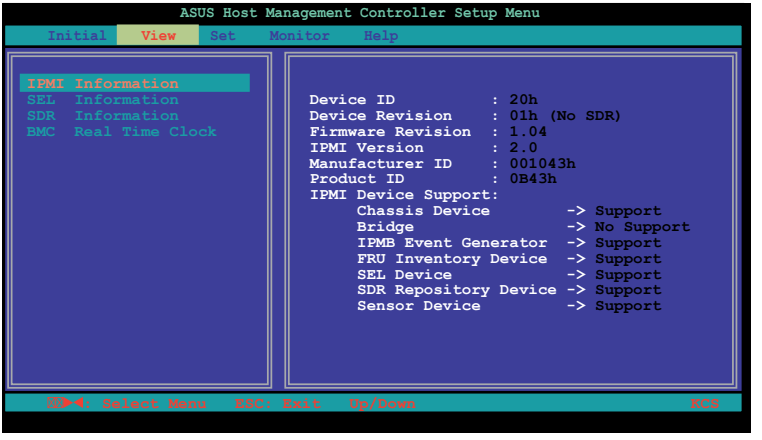
   The number on the bottom left of the screen indicates the data record displayed in the right window pane over the total number of sensor data records in the remote host.



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

To view the BMC information:

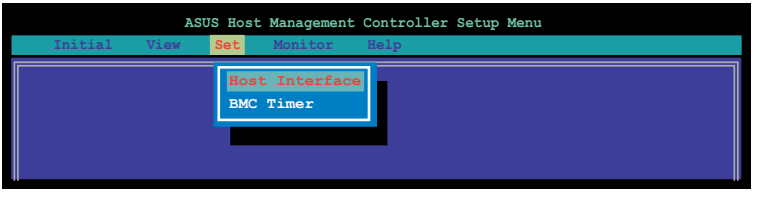
1. Select **BMC Info** from the **View** command option, then press <Enter>. A list of BMC information appears on the left pane.
2. Use the down arrow button to select a BMC information. The BMC information is displayed in the right pane.



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

3.1.5 Set

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



To select the host interface:

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

You can select from the following interfaces:

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

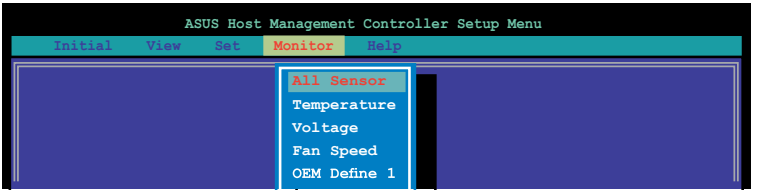
3. When finished, press <Esc> to return to the main screen.

To set the BMC Timer:

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

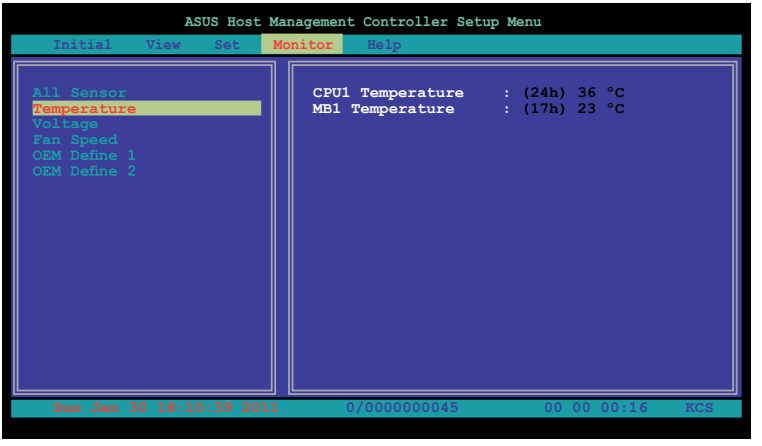
3.1.6 Monitor

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



To display a remote server information:

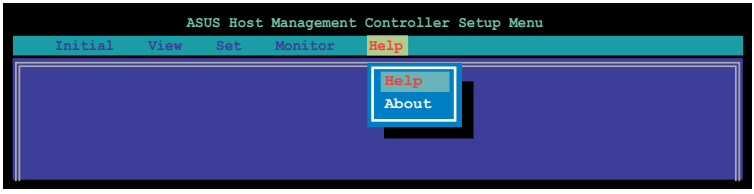
1. Select a sensor from the **Monitor** command options, then press <Enter>. A list of server information appears on the left pane.
2. Use the down arrow button to select a monitor information. The selected monitor information details are displayed in the right pane.



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

3.1.7 Help

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



4

Web-based User Interface

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

4.1 Web-based user interface

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

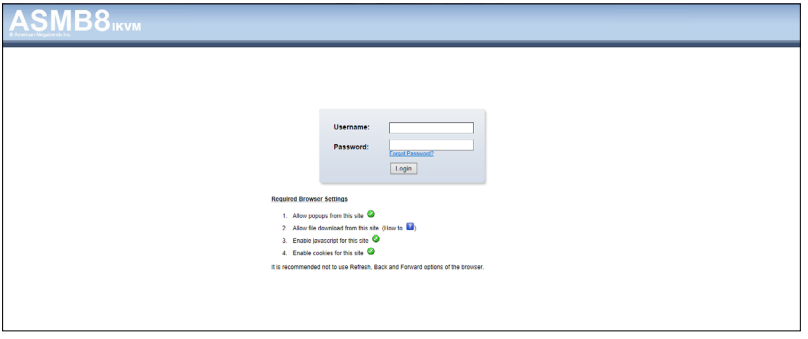
To enter the Web-based user interface:

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

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

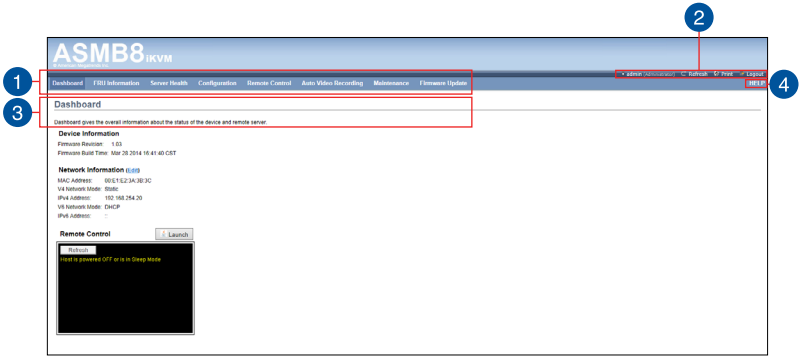
4.1.1 Logging in the utility

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



4.1.2 Using the utility

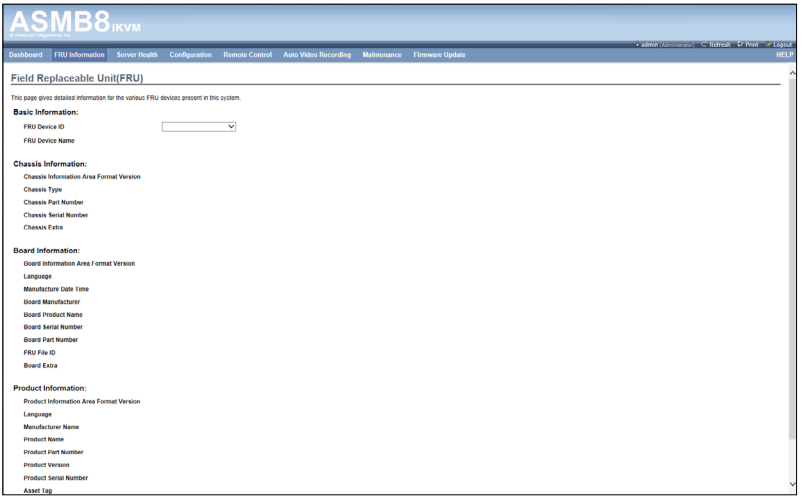
The web-based graphics user interface displays when you login in the utility successfully.



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

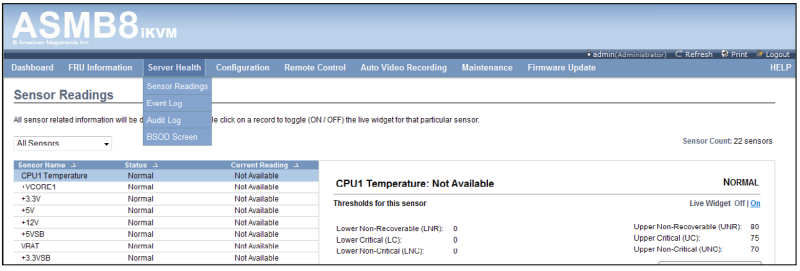
4.2 FRU Information

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



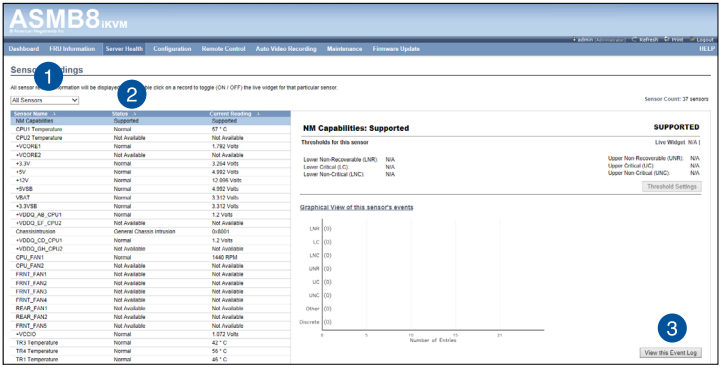
4.3 Server Health

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



4.3.1 Sensor Readings (with Thresholds)

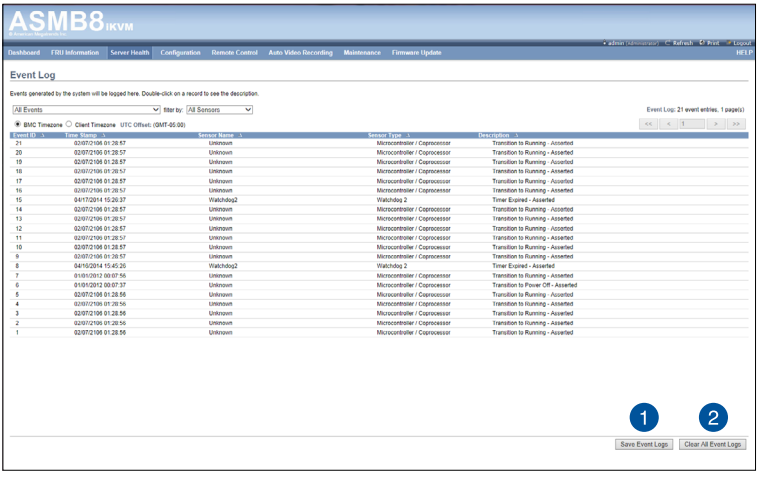
The Sensor Readings page displays the system sensor information, including readings and status.



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

4.3.2 Event Log

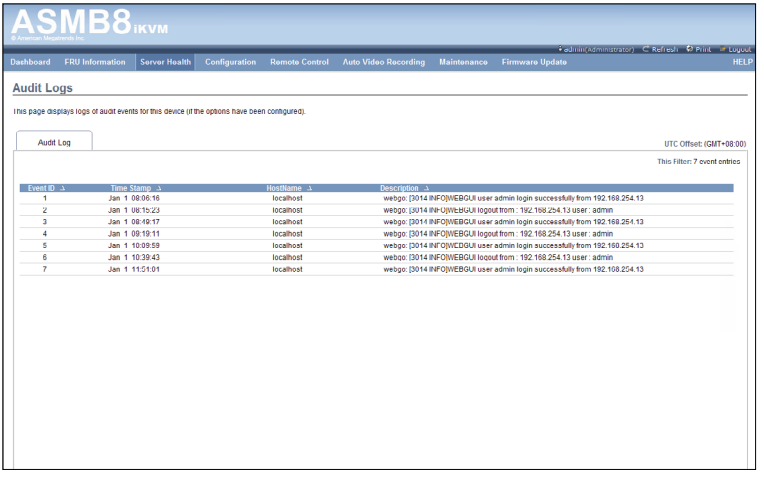
The Event Log page displays a table of system event log.



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

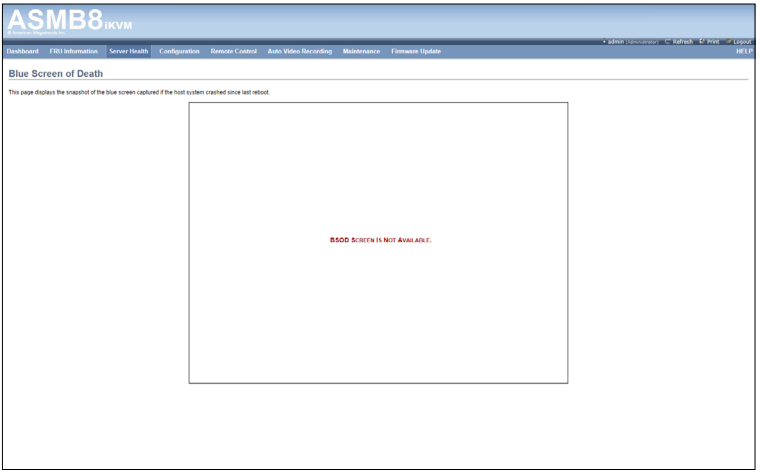
4.3.3 Audit Log

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



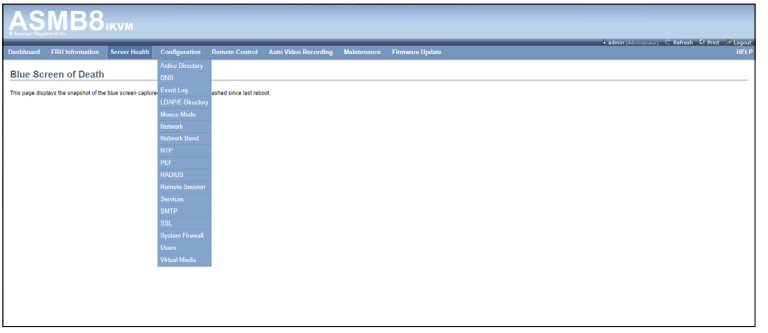
4.3.4 BSOD Screen

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



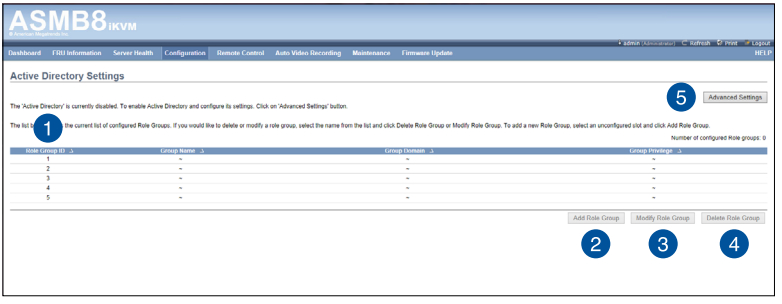
4.4 Configuration

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



4.4.1 Active Directory

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

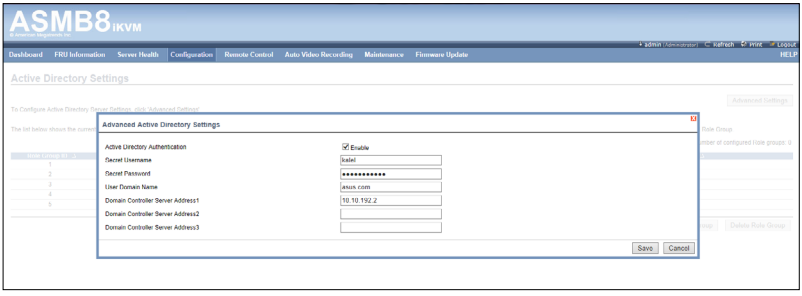


1. **Role Group ID**: The name that identifies the role group in the Active Directory. Role Group Name is a string of 255 alpha-numeric characters. Special symbols hyphen and underscore are allowed.
2. **Add Role Group:** To add a new role group to the device.
3. **Modify Role Group:** To modify that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

Procedure:

Entering the details in Advanced Active Directory Settings Page

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



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

   - **Active Directory Authentication:** To enable/disable Active Directory, check or uncheck the **Enable** checkbox respectively.

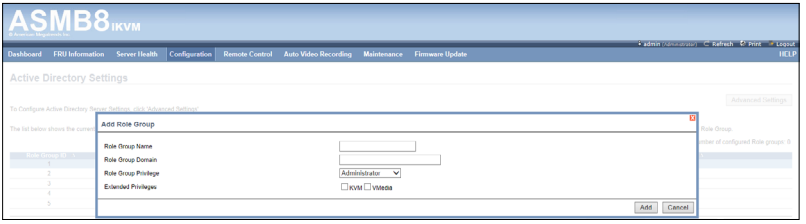
If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

   - **Secret Username:** Key in a username.
   - **Secret Password:** Key in a password.
   - **User Domain Name:** For the user in the User Domain Name field. e.g. asus.com
   - **IP addresses:** Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address 3.

3. Click **Save** to save the settings and return to Active Directory Settings Page or click **Cancel** to cancel the entry and return to Active Directory Settings Page.

To add a new Role Group

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



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

- Role Group Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen and underscore are allowed.

3. In the **Role Group Domain** field, enter the domain where the role group is located.

- Domain Name is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.

4. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.
5. Click **Add** to save the new role group and return to the Role Group List.
6. Click **Cancel** to cancel the settings and return to the Role Group List.

To Modify Role Group

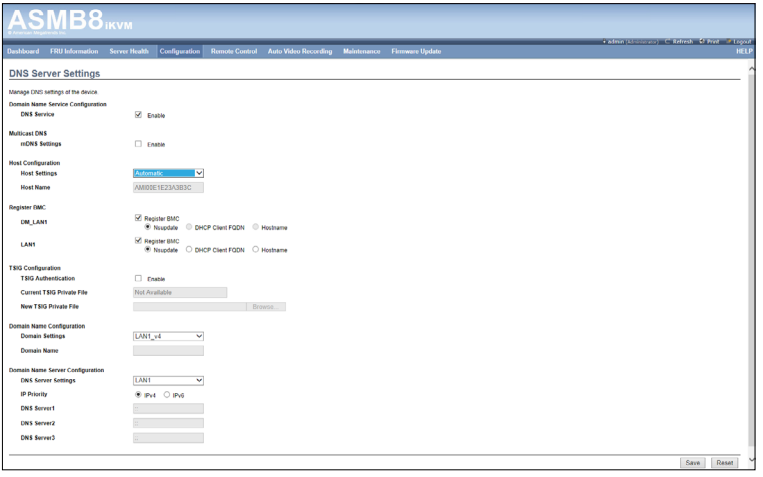
1. In the Advanced Directory Settings Page, select the row that you wish to modify and click **Modify Role Group**.
2. Make the necessary changes and click **Save**.

To Delete a Role Group

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

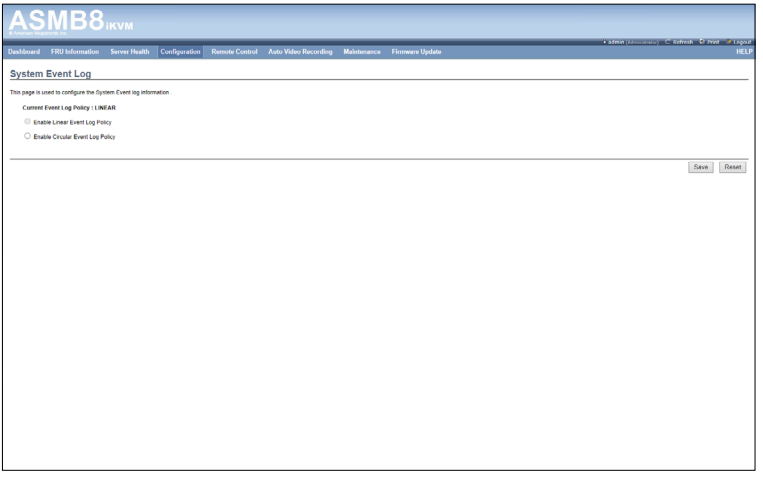
4.4.2 DNS

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



4.4.3 Event Log

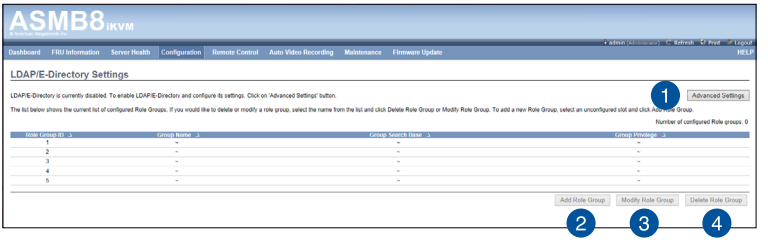
This page is used to configure the System Event log information .



4.4.4 LDAP/E-Directory

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

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

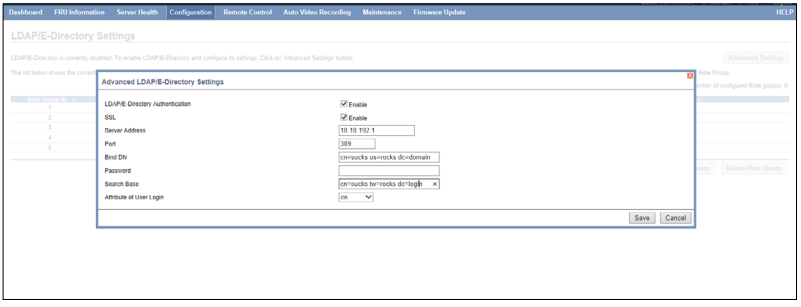


1. **Advanced Settings**: To configure LDAP Advanced Settings. Options are Enable LDAP Authentication, IP Address, Port and Search base.
2. **Add Role Group**: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.
3. **Modify Role Group**: To modify the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

Procedure

Entering the details in Advanced LDAP Settings Page

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



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

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

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

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

4. Specify the LDAP Port in the **Port** field.

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

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

To add a new Role Group

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

- Search Base is a string of 255 alpha-numeric characters.
- Special symbols hyphen, underscore and dot are allowed.

4. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.
5. Click **Add** to save the new role group and return to the Role Group List.
6. Click Cancel to cancel the settings and return to the Role Group List.

To Modify Role Group

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

To Delete a Role Group

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

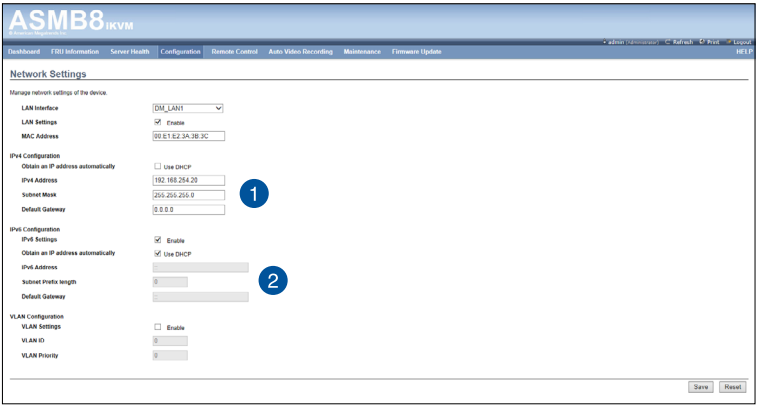
4.4.5 Mouse Mode

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

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

4.4.6 Network

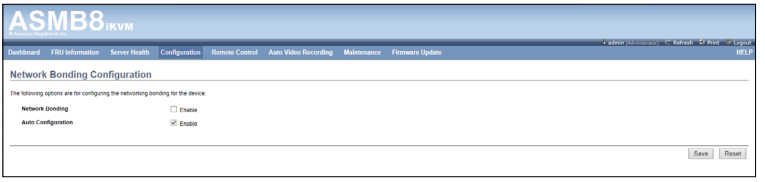
The Network page allows you to configure the network settings.



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

4.4.7 Network Bond

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



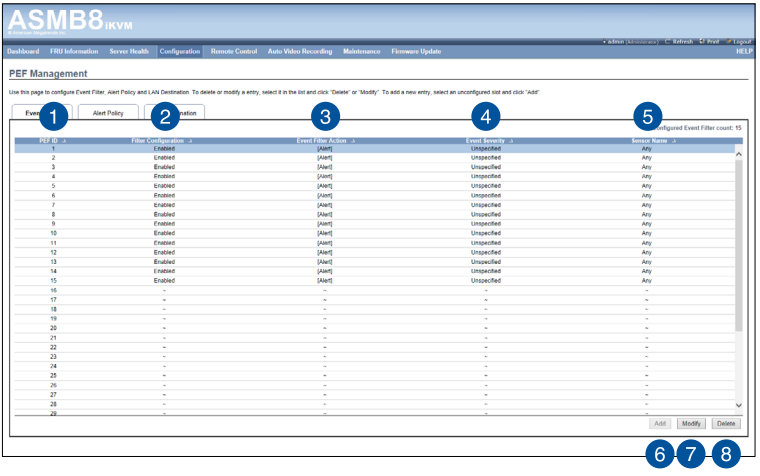
4.4.8 NTP

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

4.4.9 PEF

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

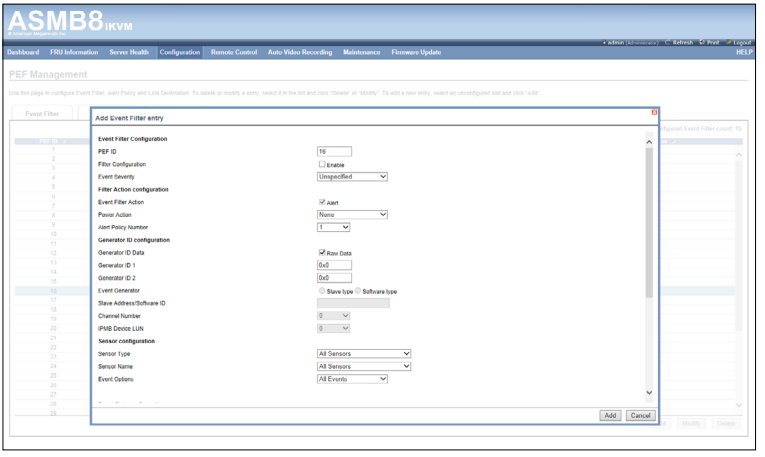
To open PEF Management Settings page, click **Configurations > PEF** from the main menu. A sample screenshot of PEF Management Settings Page is shown in the screen shot below.



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

Procedure:

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



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

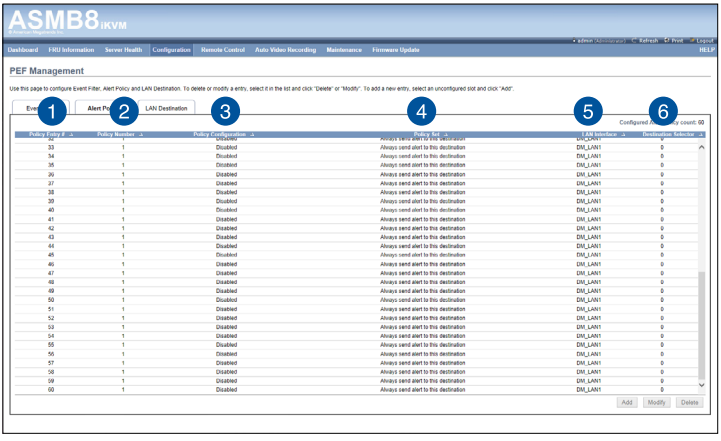
Alert Policy has to be configured - under Configuration->PEF->Alert Policy.

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

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

Alert Policy Tab

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



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

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

   0 - Always send alert to this destination.

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

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

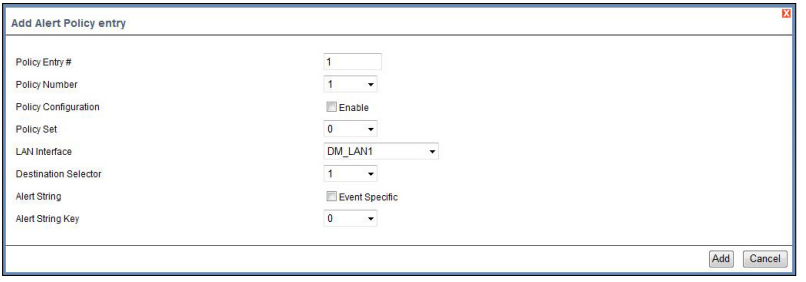
   3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

   4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
5. **LAN Interface:** To choose a particular channel from the available channel list.
6. **Destination Selector:** To choose a particular destination from the configured destination list.

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

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

Procedure:



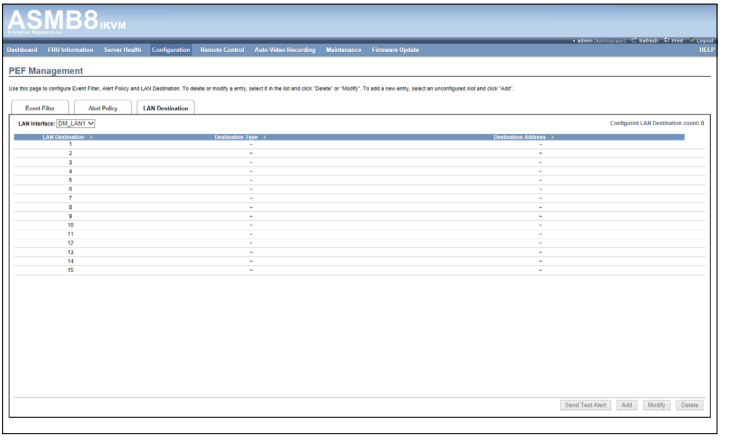
1. In the Alert Policy Tab, select the slot for which you have to configure the Alert policy. That is, In the **Event Filter Entry Page**, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click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

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

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

PEF Management LAN Destination Page

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



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

1. **LAN Destination:** Displays Destination number for the newly configured entry (read-only).

2. **Destination Type:** Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields - destination Email address, subject and body of the message needs to be filled. The SMTP server information also has to be added - under Configuration->SMTP. For SNMP Trap, only the destination IP address has to be filled.

3. **Destination Address:** If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.

- IPv6 address format.

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

4. **Subject & Message:** These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body.

5. **Add:** To save the new LAN destination and return to LAN destination list.

6. **Cancel:** To cancel the modification and return to LAN destination list.

Procedure:

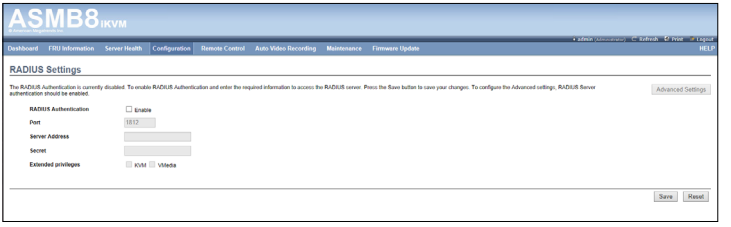
1. In the **LAN Destination Tab**, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to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

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

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

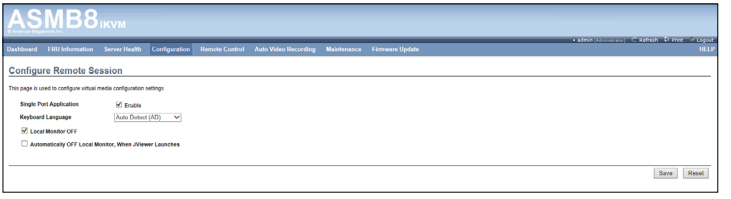
4.4.10 RADIUS

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



4.4.11 Remote Session

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



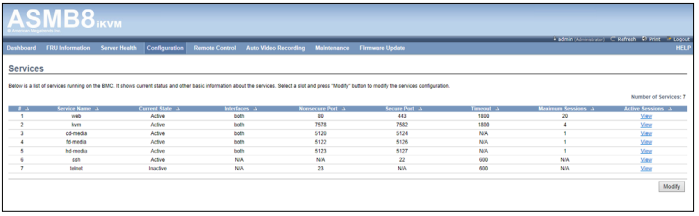
1. **Single Port Application:** Tick to enable.
2. **Keyboard Language:** Select the keyboard language from the drop down list box.
3. **Local Monitor OFF:** Tick to enable or disable.
4. **Automatically OFF Local Monitor, When JViewer Launches:** Tick to enable or disable.
5. **Save:** Click to save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

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

6. **Reset:** Click to reset the modified changes.

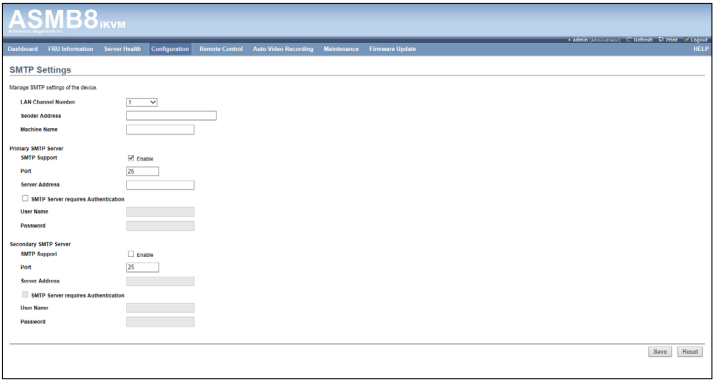
4.4.12 Services

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



4.4.13 SMTP

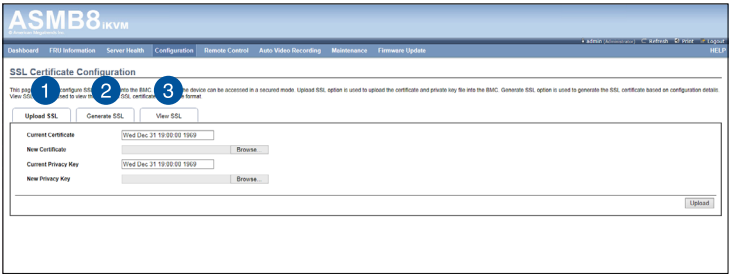
The SMTP page allows you to configure SMTP mail server. Enter the IP address of the mail server, and then click **Save** to apply the settings.



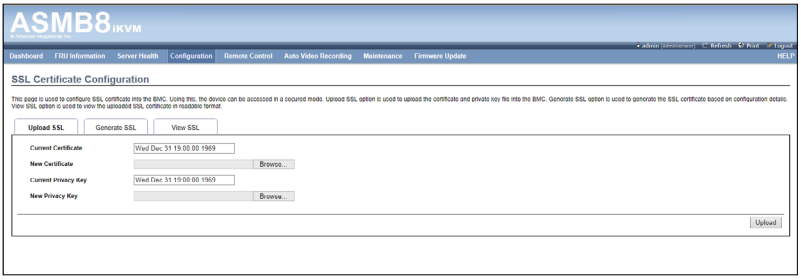
4.4.14 SSL

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

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



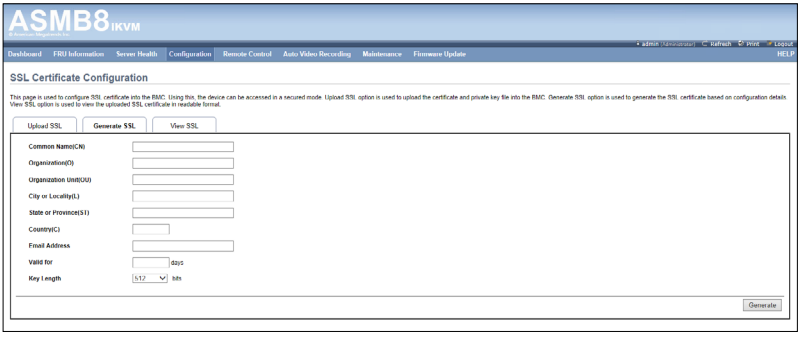
1. **Upload SSL** option is used to upload the certificate and private key file into the BMC.
2. **Generate SSL** option is used to generate the SSL certificate based on configuration details.
3. **View SSL** option is used to view the uploaded SSL certificate in readable format.



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

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

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



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

1. **Common Name(CN):** Common name for which certificate is to be generated.

   - Maximum length of 64 characters.

   - Special characters '#' and '$' are not allowed.

2. **Organization(O):** Organization name for which the certificate is to be generated.

   - Maximum length of 64 characters.

   - Special characters '#' and '$' are not allowed.

3. **Organization Unit(OU):** Over all organization section unit name for which certificate is to be generated.

   - Maximum length of 64 characters.

   - Special characters '#' and '$' are not allowed.

4. **City or Locality(L):** City or Locality of the organization (mandatory).

   - Maximum length of 64 characters.

   - Special characters '#' and '$' are not allowed.

5. **State or Province(ST):** State or Province of the organization (mandatory).

   - Maximum length of 64 characters.

   - Special characters '#' and '$' are not allowed.

6. **Country(C):** Country code of the organization (mandatory).

   - Only two characters are allowed.

   - Special characters are not allowed.

7. **Email Address:** Email Address of the organization (mandatory).

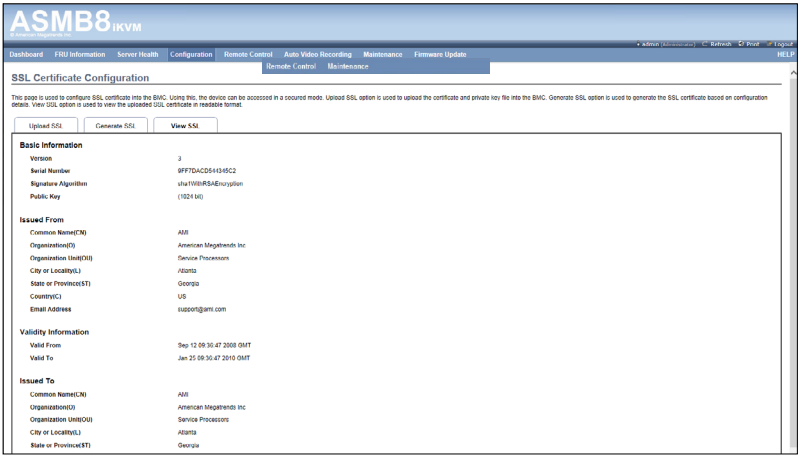
8. **Valid for:** Validity of the certificate.

   - Value ranges from 1 to 3650 days.

9. **Key Length:** The key length bit value of the certificate.

10. **Generate:** To generate the new SSL certificate.

HTTPs service will get restarted, to use the newly generated SSL certificate.



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

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

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

Procedure

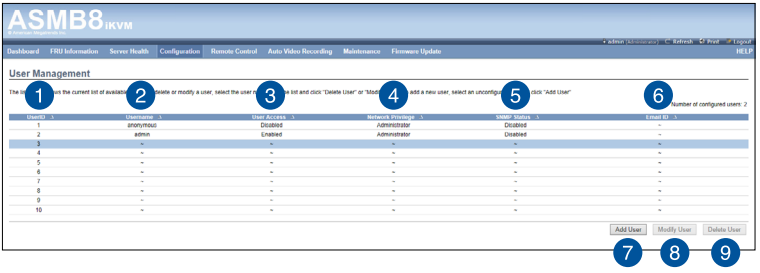
1. Click the Upload SSL Tab, **Browse** the **New Certificate** and **New Privacy key**.
2. Click **Upload** to upload the new certificate and privacy key.
3. In **Generate SSL** tab, enter the following details in the respective fields
    - The **Common Name** for which the certificate is to be generated.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

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

4.4.15 Users

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

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



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

Add a new user:

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

5 Enable or Disable the User Access Privilege.

6. In the Network Privilege field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.

7. Check the SNMP Status check box to enable SNMP access for the user. NOTE: Password field is mandatory, if SNMP Status is enabled.

8. Choose the SNMP Access level option for user from the SNMP Access dropdown list. Either it can be Read Only or Read Write.

9. Choose the Authentication Protocol to use for SNMP settings from the drop down list. NOTE: Password field is mandatory, if Authentication protocol is changed.

10. Choose the Encryption algorithm to use for SNMP settings from the Privacy protocol dropdown list.

11. In the Email ID field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

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

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

12. In the **New SSK Key** field, click Browse and select the SSH key file. Note: SSH key file should be of pub type.

13. Click **Add** to save the new user and return to the users list.

14. Click **Cancel** to cancel the modification and return to the users list.

Modify an existing User

1. Select an existing user from the list and click Modify User. This opens the Add User screen as shown in the screenshot below.

2. Edit the required fields.

3. To change the password, enable the Change Password option.

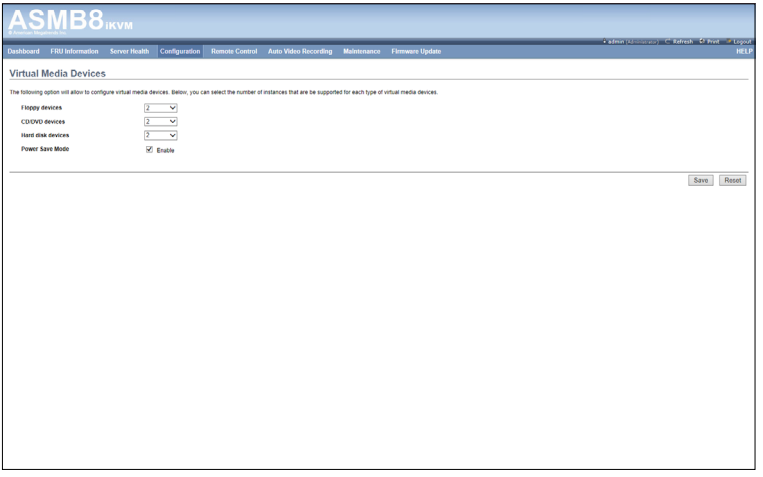
4. After editing the changes, click Modify to return to the users list page.

Delete an existing User

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

4.4.16 Virtual Media

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

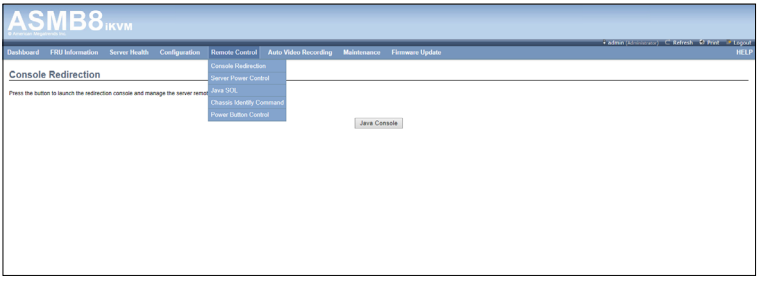


4.5 Remote Control

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

4.5.1 Console Redirection

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



Browser Settings

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

Java Console:

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

The Java Console can be launched in two ways

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

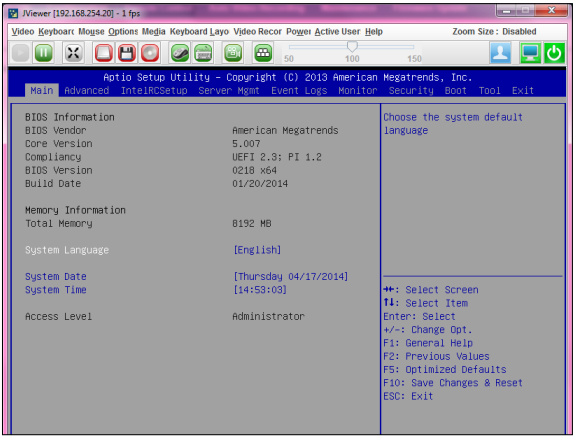
This will download the .jnlp file from BMC.

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

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

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

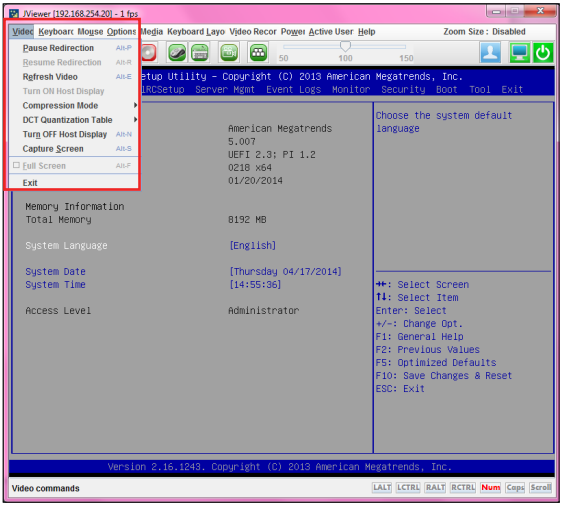
A detailed explanation of these menu items are given below.



Video

This menu contains the following sub menu items.

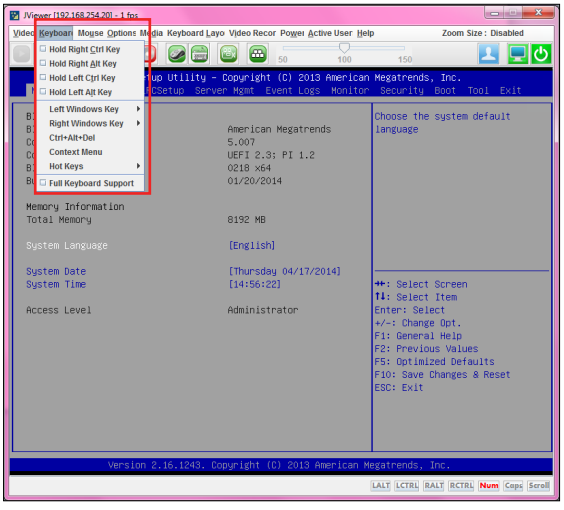
1. **Pause redirection:** This option is used for pausing Console Redirection.
2. **Resume Redirection:** This option is used to resume the Console Redirection when the session is paused.
3. **Refresh Video:** This option can be used to update the display shown in the Console Redirection window.
4. **Turn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



Keyboard

This menu contains the following sub menu items.

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

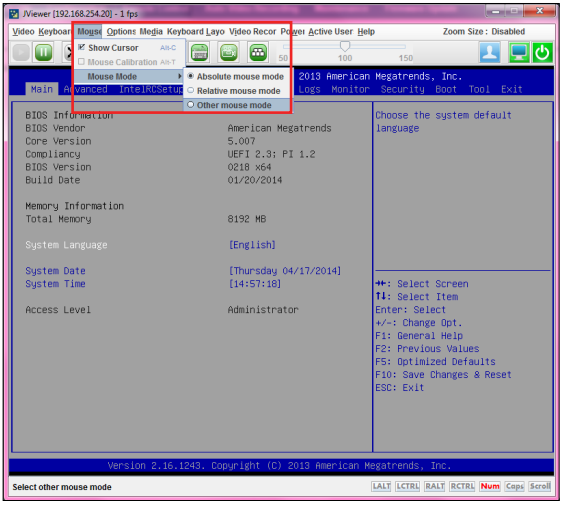


Mouse

1. **Show Cursor:** This menu item can be used to show or hide the local mouse cursor on the remote client system.

2. **Mouse Calibration:** This menu item can be used only if the mouse mode is relative. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be synchronized in the beginning. Please use '+' or '-' keys to change the threshold settings until both the cursors go out of sync. Please detect the first reading on which cursors go out of sync. Once this is detected, use 'ALT-T' to save the threshold value.

3. **Mouse Mode:** This menu item allows you to select the mode or type of mouse support.



Options

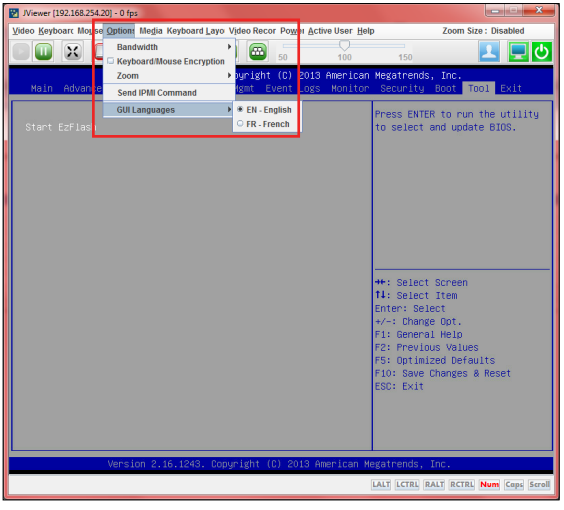
Band width: The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following:

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

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

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

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



Media

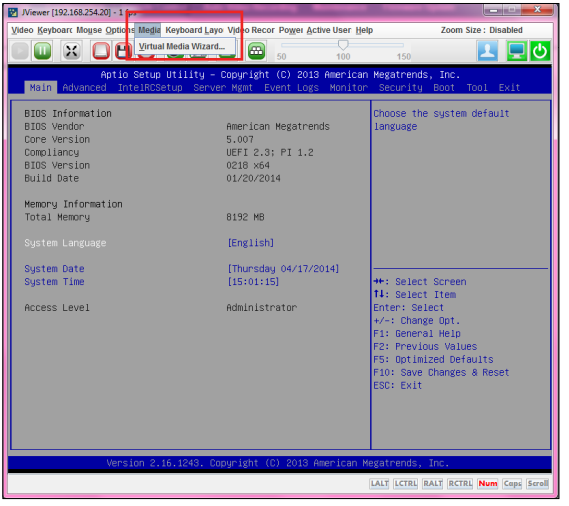
Virtual Media Wizard:

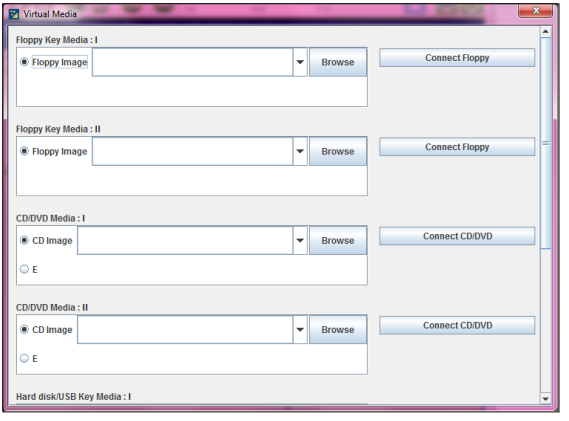
To add or modify a media, select and click 'Virtual Media Wizard' button, which pops out a box named “Virtual Media” where you can configure the media. A sample screenshot of Virtual media screen is given below. Virtual Media.

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

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

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

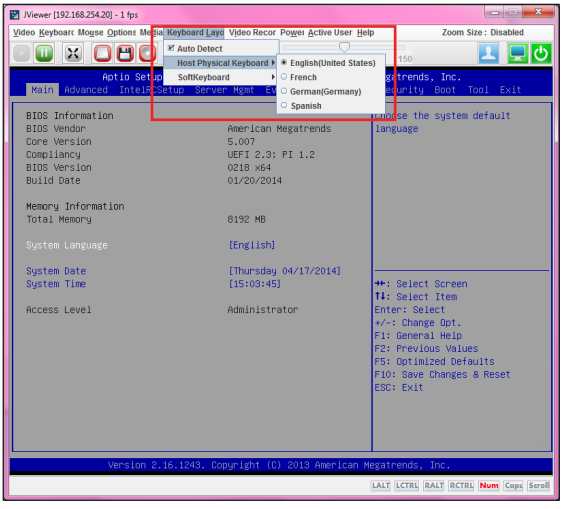




Keyboard Layout

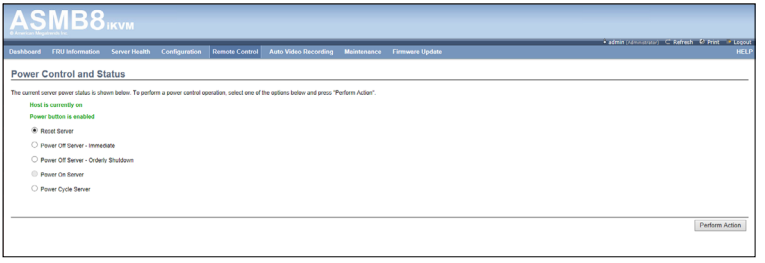
Auto Detect: This option is used to detect keyboard layout automatically. The languages supported automatically are English – US, French – France, Spanish – Spain, German-Germany, Japanese- Japan. If the client and host languages are same, then for all the languages other than English mentioned above,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

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



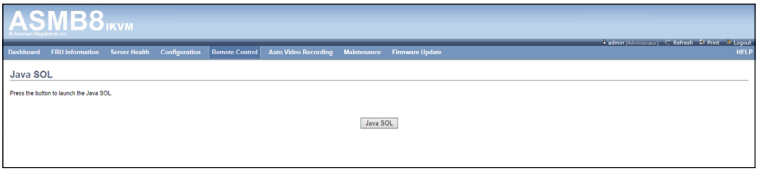
4.5.2 Server Power Control

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



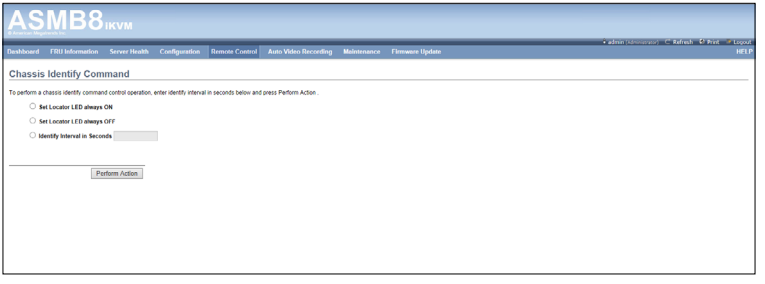
4.5.3 Java SOL

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



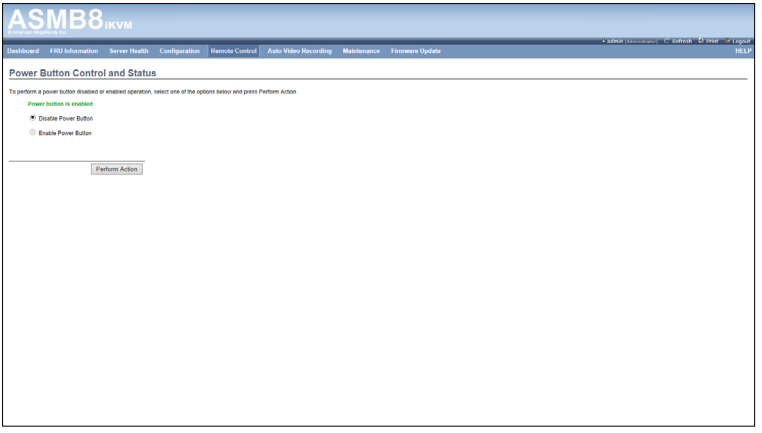
4.5.4 Chassis Identify Command

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



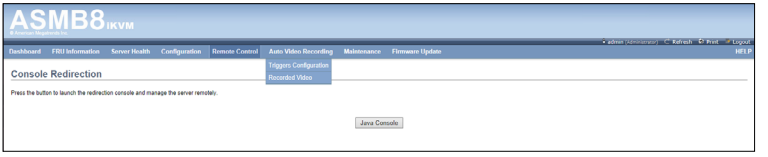
4.5.5 Power Button Control

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



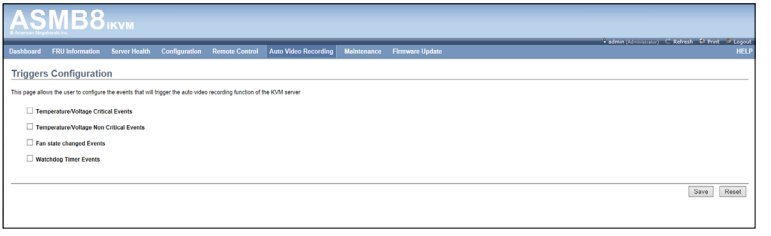
4.6 Auto Video Recording

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



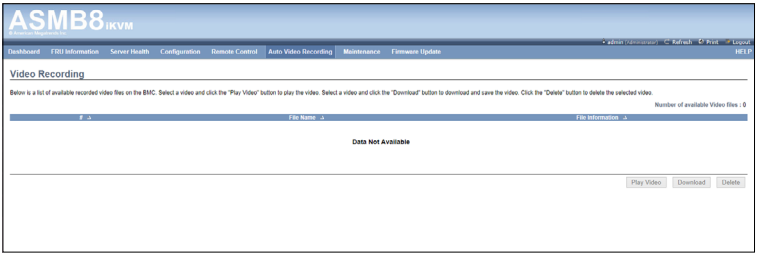
4.6.1 Triggers Configuration

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



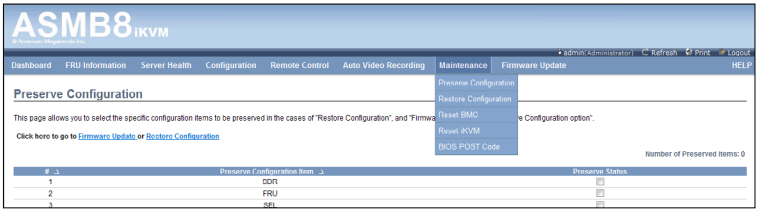
4.6.2 Recorded Video

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



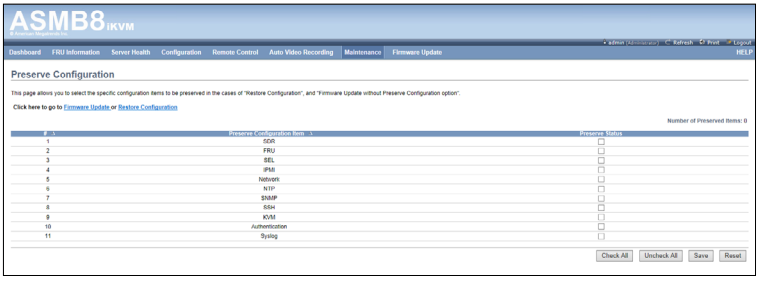
4.7 Maintenance

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



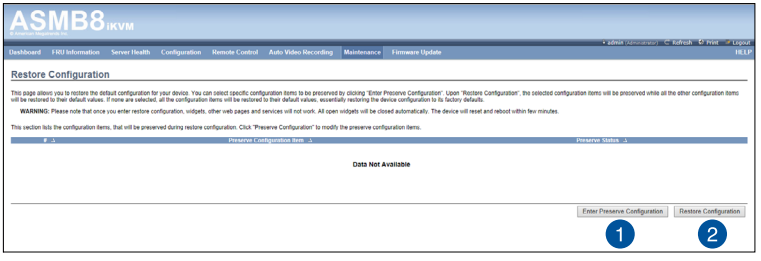
4.7.1 Preserve Configuration

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



4.7.2 Restore Configuration

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



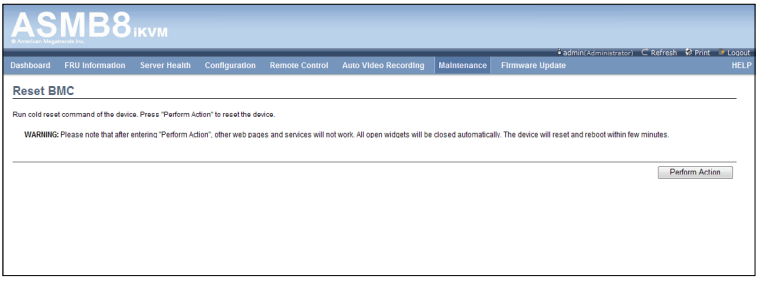
1. **Enter Preserve Configuration.** Click to select specific configuration items to be preserved

2. **Restore Configuration.** Selected configuration items will be preserved while all the other configuration items will be restored to their default values. If none are selected, all the configuration items will be restored to their default values, essentially restoring the device configuration to its factory defaults.

4.7.3 Reset BMC

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

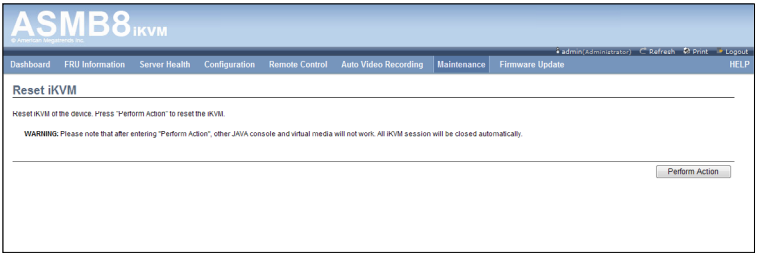
Please note that after entering **Perform Action**, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.



4.7.4 Reset iKVM

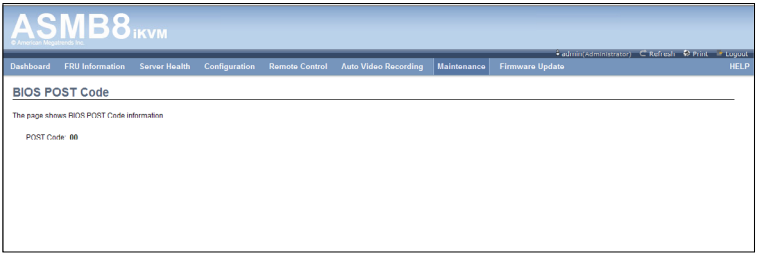
This page allows you reset the iKVM of the device.

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



4.7.5 BIOS POST Code

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



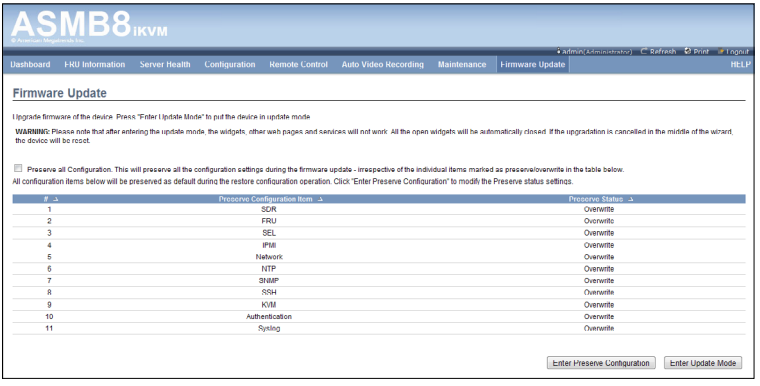
4.8 Firmware Update

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

4.8.1 Firmware Update

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

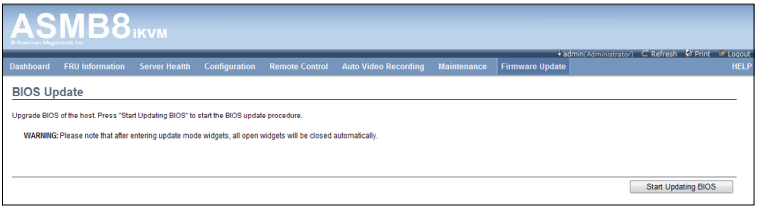
Please note that after entering **Enter Update Mode**, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.



4.8.2 BIOS Update

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

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



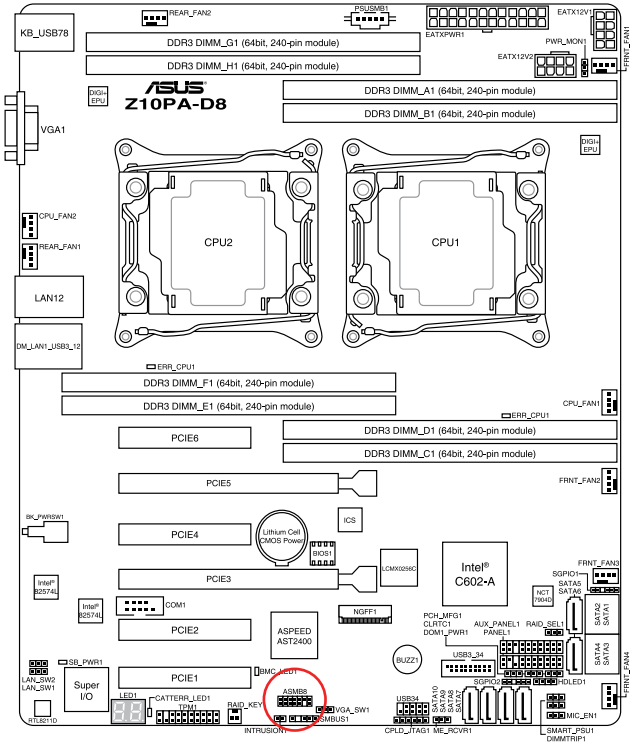
Appendix

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

A.1 BMC connector

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

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



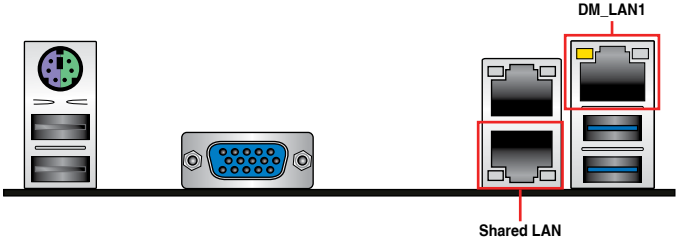
The motherboard illustration is for reference only. The motherboard layout and appearance may vary depending on the model..

A.2 LAN ports for server management

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

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

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



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

A.3 Troubleshooting

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

Problem	Solution
The local/central server cannot connect to the ASMB8-iKVM board	1. Check if the LAN cable is connected to the LAN port. 2. Make sure that the IP address of both the remote and local/central servers are on the same subnet. (Refer to chapter 2 for details.) Try “ping xx.xx.xx.xx” (remote server ip) on local/central server and make sure remote server could reply the ping request. 3. Check if the IP source is set to [DHCP]. When set to [DHCP], you’ll not be able to configure the IP address.
All the SEL (System Event Log) cannot be displayed	The maximum SEL number is 900 events.
The date/time shown in SEL (System Event Log) screen is incorrect	Refer to section 4.4.9 to check if the time zone is set up correctly.
ASMB8-iKVM has network connection problems in Firewall environment	Ask MIS to add the following port numbers in Firewall: 5123 (virtual floppy) (TCP) 5120 (virtual CDROM) (TCP) 623 (IPMI) (TCP & UDP) 80 (HTTP) (TCP) 7578 (iKVM) (TCP) 443 (HTTPs) (TCP) 161 (SNMP) (UDP)
The Java redirection screen cannot be displayed normally	Click **Refresh Page** button to refresh the redirection screen.

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

A.4 Sensor Table

Memory ECC

Sensor No.	Sensor Name	Sensor Type	Sensor Type code	Sensor Value or Event Type	Event Data 3
0xD1	CPU1_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03:DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD3	CPU2_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DIMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4

CPU CATERR

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

Memory Error

Sensor No.	Sensor Name	Sensor Type	Sensor Type code	Sensor Value or Event Type	Event Data 3
0xDB	Memory_Train_ERR	OEM Type	0xC5	Discrete (6Fh) 0x01: Memory Train Error	[7:0] - Memory module/device 0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0a: DIMM_C3, 0x0c: DIMM_D1, 0x0d: DIMM_D2, 0x0e: DIMM_D3, 0x10: DIMM_E1, 0x11: DIMM_E2, 0x12: DIMM_E3, 0x14: DIMM_F1, 0x15: DIMM_F2, 0x16: DIMM_F3, 0x18: DIMM_G1, 0x19: DIMM_G2, 0x1a: DIMM_G3, 0x1c: DIMM_H1, 0x1d: DIMM_H2, 0x1e: DIMM_H3

Backplane HD

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

Power Supply

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

Hardware Monitor

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

(continued on the next page)

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

(continued on the next page)

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

ASUS contact information

ASUSTeK COMPUTER INC.

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

Technical Support

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

ASUSTeK COMPUTER INC. (Taiwan)

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

Technical Support

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

ASUSTeK COMPUTER INC. (China)

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

Technical Support

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

ASUS contact information

ASUS COMPUTER INTERNATIONAL (America)

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

Technical Support

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

ASUS COMPUTER GmbH (Germany and Austria)

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

Technical Support

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

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

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

Technical Support

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

ASUS contact information

ASUS Holland BV (The Netherlands)

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

Technical Support

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

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

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

Technical Support

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

ASK-Service (Russia and CIS)

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

Technical Support

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

DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)

Responsible Party Name: **Asus Computer International**

Address: **800 Corporate Way, Fremont, CA 94539.**

Phone/Fax No: **(510)739-3777/(510)608-4555**

hereby declares that the product

Product Name : Management card

Model Number : ASMB8-IKVM

Conforms to the following specifications:

☒ FCC Part 15, Subpart B, Unintentional Radiators

Supplementary Information:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Representative Person's Name : **Steve Chang / President**

Signature :

Date : **May. 09, 2014**

Ver. 140331

EC Declaration of Conformity

ASUS IN SEARCH OF INCREDIBLE

We, the undersigned,

Manufacturer:	ASUSTeK COMPUTER INC.
Address:	4F, No. 150, LI-TE Rd., PEITOU, TAIPEI 112, TAIWAN
Authorized representative in Europe:	ASUS COMPUTER GmbH
Address, City:	HARKORT STR. 21-23, 40880 RATINGEN
Country:	GERMANY

declare the following apparatus:

Product name :	**Management card**
Model name :	**ASMB8-iKVM**

conform with the essential requirements of the following directives:

☒2004/108/EC-EMC Directive

☒ EN 55022:2010+AC:2011	☒ EN 55024:2010
☒ EN 61000-3-2:2006+A2:2009	☒ EN 61000-3-3:2008
☐ EN 55013:2001+A1:2003+A2:2006	☐ EN 55020:2007+A11:2011

☐1999/5/EC-R&TTE Directive

☐ EN 300 328 V1.7.1(2006-10)	☐ EN 301 489-1 V1.9.2(2011-09)
☐ EN 300 440-1 V1.6.1(2010-08)	☐ EN 301 489-3 V1.4.1(2002-08)
☐ EN 300 440-2 V1.4.1(2010-08)	☐ EN 301 489-4 V1.4.1(2009-05)
☐ EN 301 511 V9.0.2(2003-03)	☐ EN 301 489-7 V1.3.1(2005-11)
☐ EN 301 908-1 V5.2.1(2011-05)	☐ EN 301 489-9 V1.4.1(2007-11)
☐ EN 301 908-2 V5.2.1(2011-07)	☐ EN 301 489-17 V2.2.1(2012-09)
☐ EN 301 893 V1.6.1(2011-11)	☐ EN 301 489-24 V1.5.1(2010-09)
☐ EN 302 544-2 V1.1.1(2009-01)	☐ EN 302 326-2 V1.2.2(2007-06)
☐ EN 302 623 V1.1.1(2009-01)	☐ EN 302 326-3 V1.3.1(2007-09)
☐ EN 50360:2001	☐ EN 301 357-2 V1.4.1(2008-11)
☐ EN 62479:2010	☐ EN 302 291-1 V1.1.1(2005-07)
☐ EN 50385:2002	☐ EN 302 291-2 V1.1.1(2005-07)
☐ EN 62311:2008	

☐2006/95/EC-LVD Directive

☐ EN 60950-1 / A12:2011	☐ EN 60065:2002 / A12:2011

☐2009/125/EC-ErP Directive

☐ Regulation (EC) No. 1275/2008	☐ Regulation (EC) No. 278/2009
☐ Regulation (EC) No. 642/2009	☐ Regulation (EC) No. 617/2013

☒2011/65/EU-RoHS Directive Ver. 140331

☒CE marking

CE (EC conformity marking)

Position : **CEO**

Name : **Jerry Shen**

Signature : _____

Declaration Date: 09/05/2014

Year to begin affixing CE marking: 2014