ASMB6-iKVM

Server Management Board

E6918

First Edition V1
January 2012

Contents

Contents

Contents

Notices

Federal Communications Commission Statement

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

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

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

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

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

Canadian Department of Communications Statement

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

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

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: Installation**

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

- **Chapter 3: ASUS Remote Console**

  This chapter tells you how to use the ASUS Remote Console (ARC) that the server management board supports.

- **Chapter 4: Web-based user interface (ASMB6-iKVM only)**

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

- **Appendix: Reference Information**

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

Where to find more information

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

1. **ASUS websites**

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

2. **Optional documentation**

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

Conventions used in this guide

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

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

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

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

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

Typography

Bold text	Indicates a menu or an item to select.
Italics	Used to emphasize a word or a phrase.
<Key>	Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key.
	Example: <Enter> means that you must press the Enter or Return key.
<Key1+Key2+Key3>	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+).
	Example: <Ctrl+Alt+D>
Command	Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets.
	Example: At the DOS prompt, type the command line: **format a:**

ASMB6-iKVM specifications summary

Chipset	Aspeed 2300
Internal RAM	112 MB for system 16 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
Browsers Support	- HTML5/JS based UI - Multi-language support in Web interface with English as the currently supported language - Internet Explorer 7, 8 (IE6 for SP2) - Firefox 3.0 and above - Google Chrome 2.0 and above - Safari 3.0 and above - Opera 9.64 and above
OS Support	Host Operating System: - Windows Server 2003 32/64-bit - Windows Server 2008 32/64-bit - Red Hat Enterprise Linux 5.x 32/64-bit - SuSE Linux Enterprise Server 10.x 32/64-bit - SuSE Linux Enterprise Server 11.x32/64-bit Client Operating System: - Windows XP - Windows Vista - Windows Server 2003 32/64-bit - Windows 7 32/64-bit - Fedora Core 9 and above 32/64-bit - Red Hat Enterprise Linux 5.x 32/64-bit - Mac OS X
Form factor	22 mm x 17 mm

* Specifications are subject to change without notice.

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

Product introduction

1

1.1 Welcome!

Thank you for buying an ASUS® ASMB6-iKVM server management board!

The ASUS ASMB6-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 ASMB6-iKVM plugging in a server motherboard, you can completely and efficiently monitor your server in real-time. The solution allows you to reduce IT management costs and increase the productivity.

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

1.2 Package contents

Check your server management board package for the following items.

- ASUS ASMB6-iKVM Card
- Support CD
- User guide

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

1.3   Features

1. **IPMI 2.0**
    -   System interface (KCS)
    -   LAN interface (support RMCP+)
    -   System Event Log (SEL)
    -   Sensor Data Record (SDR)
    -   Field Replaceable Unit (FRU)
    -   Remote Power on/off, reboot
    -   Serial Over LAN (SOL)
    -   Authentication Type: RAKP-HMAC-SHA1
    -   Encryption (AES)
    -   Platform Event Filtering (PEF)
    -   Platform Event Trap (PET)
    -   Watchdog Timer

2. **Private I2C Bus**
    -   Auto Monitoring sensors (temperature, voltage, fan speed and logging events

3. **PMBus***
    -   Support Power supply for PMBus device

4. **PSMI***
    -   Support Power supply for PSMI bus device

5. **Web-base GUI**
    -   Monitor Sensor, show SDR, SEL, FRU, configure BMC, LAN
    -   Support SSL (HTTPS)
    -   Multiple user permission level
    -   Upgrade BMC firmware

6. **Update Firmware**
    -   DOS Tool
    -   Web GUI (Windows® XP/Vista/2003/2008, RHEL5.2, SLES10SP2

7. **Notification**
    -   PET
    -   SNMP Trap
    -   e-Mail

---

8. KVM over Internet

   • Web-based remote console

9. Remote Update BIOS

   • Use Remote floppy to update BIOS

10. Remote Storage (Virtual Media)

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

11. Remote Install OS

   • Use remote storage to remote install OS

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

1.4   System requirements

Before you install the ASMB6-iKVM board, check if the remote server system meets the following requirements:

• ASUS server motherboard with Baseboard Management Controller (BMC) connector*

• LAN (RJ-45) port for server management**

• Microsoft® Internet Explorer 5.5 or later; Firefox

> *   Visit the ASUS website (www.asus.com) for an updated list of server motherboards that support the ASMB6-iKVM.
>
> ** See the Appendix for details.

1.5   Network setup

The ASMB6-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

RJ-45 cable

Remote server with ASMB6-iKVM

Remote console with web-based browser
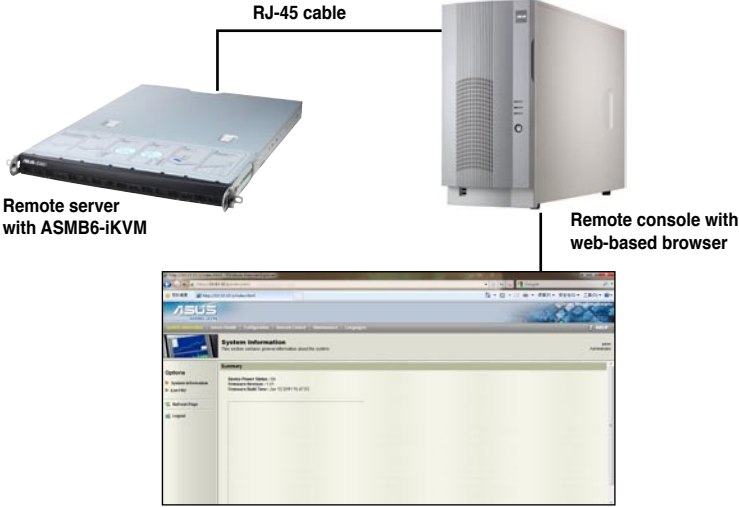
LAN connection through a network hub
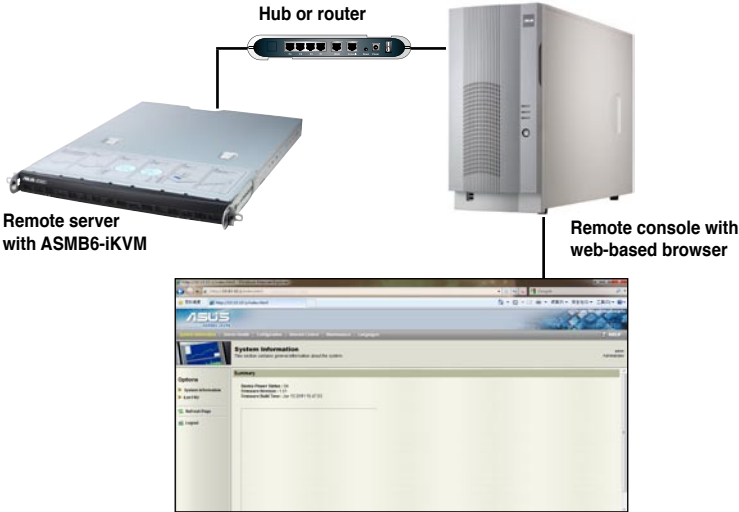
Hub or router

Remote server with ASMB6-iKVM

Remote console with web-based browser

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

Installation2

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 ASMB6 connector on the motherboard.

    📝 Refer to the Appendix section for the location of the ASMB6 connector on supported motherboards.
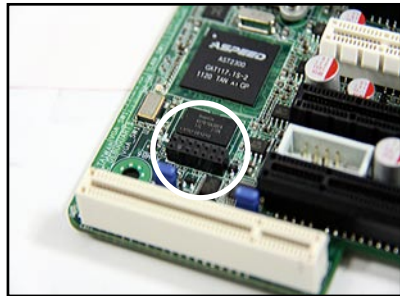
2. Place the card on the ASMB6 connector of the motherboard, aligning with the pin connectors.
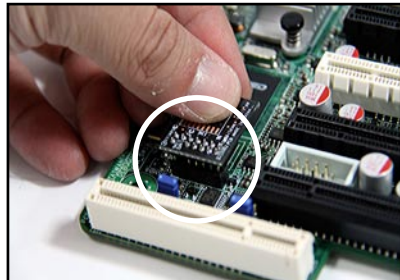
3. Press the board firmly until it is completely seated in place.
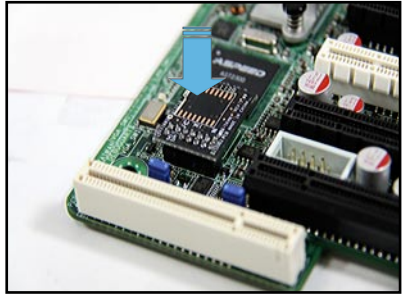
4. When installed, the board appears as shown.
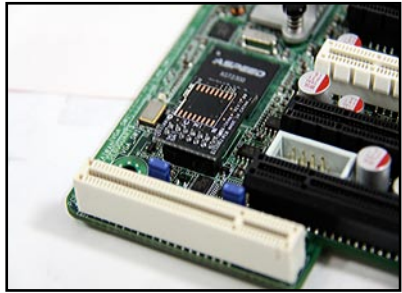
5. Insert the LAN cable plug to the LAN port for server management.

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

6. 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.

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

Everytime after the AC power is re-plugged, you have to wait for about 60 seconds for the system power up.

2.3 Firmware update and IP configuration

You need to update the ASMB6-iKVM firmware and configure IP source before you start using the ASMB6-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, the main menu appears. Select **ASMB6-iKVM Firmware Update for Preserve Configuration**, and press <Enter> to enter the sub-menu.

```
                    ASUS Server Z9PE-D16 MB
FreeDOS command prompt
Configure BMC IP Source Static IP for LAN1
Configure BMC IP Source DHCP for LAN1
Configure BMC IP Source Static IP for DM_LAN1
Configure BMC IP Source DHCP for DM_LAN1
ASMB6 Firmware Update for Preserve Configuration (SDR,LAN,Username)
ASMB6 Firmware Update for Clear Configuration (SDR,LAN,Username)
```
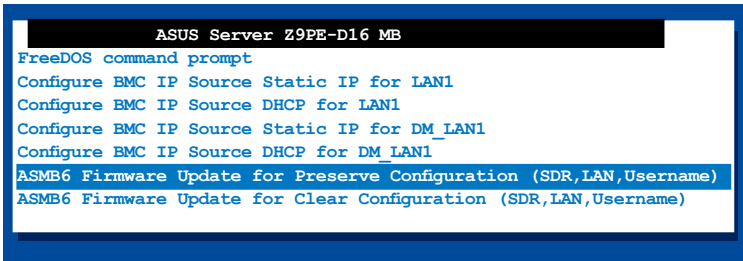
6. A confirmation message appears, asking whether you want to update the firmware or not. Select <Yes> to update.

```
    WARNING !!!
    UPDATE ASMB6 FIRMWARE NOW !
    DO YOU WANT TO CONTINUE ?

                                    No      Yes
```
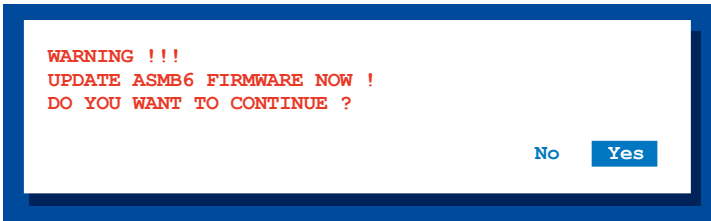
The firmware updating process starts.

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

```
NewImageSize = 32MB, offs = 0

Uploading Firmware Image : Completed


Flash Update Completed


Device Firmware has been upgraded successfully.
The device will be reset within 10 seconds for the new firmware to
take effect. Please wait for 70 seconds to initialize firmware.
Delay     70 seconds
Press any key to continue ...
```
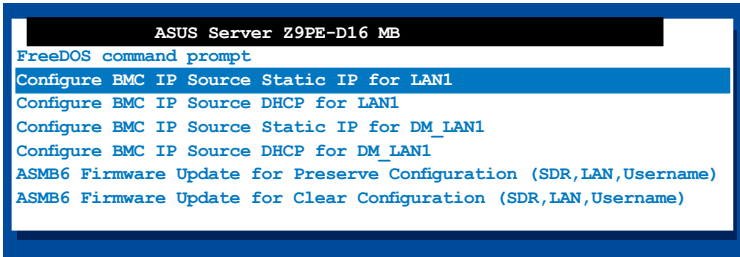
You may update firmware from the web-based user interface. Refer to page 4-13 for details.

8.   Select <Y> twice to confirm.
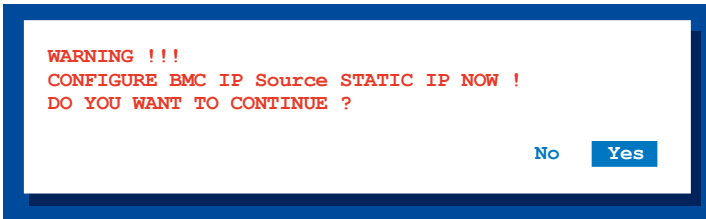
2.3.2   Configure BMC IP source static IP

1.   Repeat the step 1-4 in the previous sub-section.

2.   On reboot, the main menu appears. Select **Configure BMC IP Source Static IP for LAN1 (or DM_LAN1)**, and press <Enter> to enter the sub-menu.

```
                    ASUS Server Z9PE-D16 MB
FreeDOS command prompt
Configure BMC IP Source Static IP for LAN1
Configure BMC IP Source DHCP for LAN1
Configure BMC IP Source Static IP for DM_LAN1
Configure BMC IP Source DHCP for DM_LAN1
ASMB6 Firmware Update for Preserve Configuration (SDR,LAN,Username)
ASMB6 Firmware Update for Clear Configuration (SDR,LAN,Username)
```
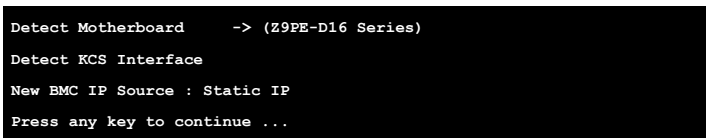
3.   A confirmation message appears, asking if you want to configure the BMC IP source static IP now. Select <Yes> to continue.

```
    WARNING !!!
    CONFIGURE BMC IP Source STATIC IP NOW !
    DO YOU WANT TO CONTINUE ?

                                    No      Yes
```

4.   When the configuration is completed, the below screen appears.
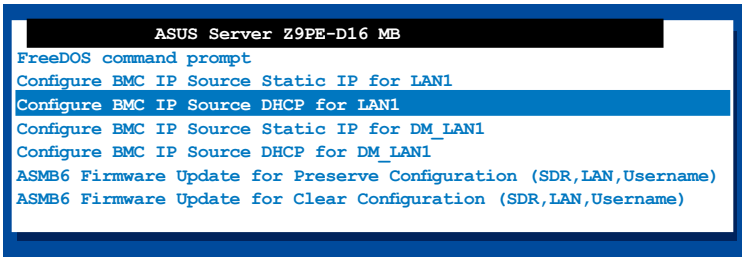
```
Detect Motherboard      -> (Z9PE-D16 Series)

Detect KCS Interface

New BMC IP Source : Static IP

Press any key to continue ...
```

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

2.3.3   Configure BMC IP source DHCP

1.   Repeat the step 1-4 in the previous sub-section.

2.   On reboot, the main menu appears. Select **Configure BMC IP Source DHCP for LAN1 (or DM_LAN1)**, and press <Enter> to enter the sub-menu.

```
                    ASUS Server Z9PE-D16 MB
FreeDOS command prompt
Configure BMC IP Source Static IP for LAN1
Configure BMC IP Source DHCP for LAN1
Configure BMC IP Source Static IP for DM_LAN1
Configure BMC IP Source DHCP for DM_LAN1
ASMB6 Firmware Update for Preserve Configuration (SDR,LAN,Username)
ASMB6 Firmware Update for Clear Configuration (SDR,LAN,Username)
```
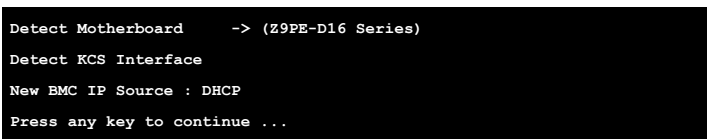
3.   A confirmation message appears, asking if you want to configure the BMC IP source DHCP now. Select <Yes> to continue.

```
    WARNING !!!
    CONFIGURE BMC IP Source DHCP NOW !
    DO YOU WANT TO CONTINUE ?

                                        No     Yes
```

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

```
Detect Motherboard     -> (Z9PE-D16 Series)

Detect KCS Interface

New BMC IP Source : DHCP

Press any key to continue ...
```

5.   Then you can get IP from DHCP server.

2.4 BIOS configuration

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

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

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

2.4.1 Running the BIOS BMC configuration

To configure the BMC in the BIOS:

1. Restart the remote server, then press <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.

```
              Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
       Main   Server Mgmt   Event Logs   Advanced   Monitor   Boot   Tool   Exit

         BMC Firmware Version :          1.02              Enable/Disable interfaces to
                                                           communicate with BMC.
         FRB-2 Timer timeout             [6 minutes]
         FRB-2 Timer Policy              [Reset]
         O/S Watchdog Timer              [Disabled]
         O/S Wtd Timer Timeout           [10 minutes]
         O/S Wtd Timer Policy            [Reset]
       ▶ System Event Log
       ▶ BMC network configuration
                                                           ➡➡: Select Screen
                                                           ↑↓   Select Item
                                                           Enter: Select
                                                           +/—: Change Opt.
                                                           F1:   General Help
                                                           F9:   Optimized Defaults
                                                           F10:  Save   ESC: Exit

              Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.
```

```
              Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
        Server Mgmt

     BMC network configuration                                        Select to configure LAN channel
                                                                      parameters statically or
     DM_LAN1                                                          dynamically(DHCP). Do nothing
                                                                      option will not modify any BMC
     DM_LAN1 IP Address in BMC :              000.000.000.000         network parameters during BIOS
     DM_LAN1 Subnet Mask in BMC :             000.000.000.000         phase.
     DM_LAN1 Gateway Address in BMC :         000.000.000.000
     DM_LAN1 MAC Address in BMC :             90.E6.BA.0A.20.BA

     Configuration source                     [Previous State]        ➡◀:  Select Screen
                                                                      ⬆⬇:   Select Item
     Lan1                                                             Enter: Select
                                                                      +/—:  Change Opt.
     Lan1 IP Address in BMC :                 000.000.000.000         F1:    General Help
     Lan1 Subnet Mask in BMC :                000.000.000.000         F9:    Optimized Defaults
     Lan1 Gateway Address in BMC :            000.000.000.000         F10:  Save   ESC: Exit
     Lan1 MAC Address in BMC :                90.E6.BA.0A.20.BA

     Configuration source                     [Previous State]

              Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.
```

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.

Router MAC Address
Allows you to set the Router MAC address.

2.4.3   System Event Log

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

```
                   Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
      Server Mgmt

 Enabling/Disabling Options                              Select to configure LAN channel
 SEL Components                  [Disabled]              parameters statically or
                                                         dynamically(DHCP). Do nothing
 Erasing Settings                                        option will not modify any BMC
 Erase SEL                       [No]                    network parameters during BIOS
 When SEL is Full                [Do Nothing]            phase.

 NOTE: All values changed here do not take effect
       until computer is restarted.
                                                         →←: Select Screen
                                                         ↑↓: Select Item
                                                         Enter: Select
                                                         +/—: Change Opt.
                                                         F1:   General Help
                                                         F9:   Optimized Defaults
                                                         F10:  Save   ESC: Exit

                   Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.
```

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]

2.5 Running the ASMC6 utility

The ASMC6 utility allows you to update the ASMB6-iKVM firmware, configure the LAN setting for the remote server and change the user name/password in DOS environment. This utility is available from the support CD that came with the package.
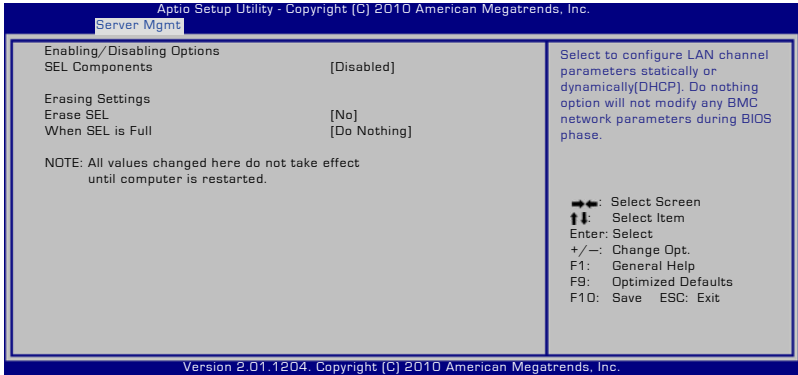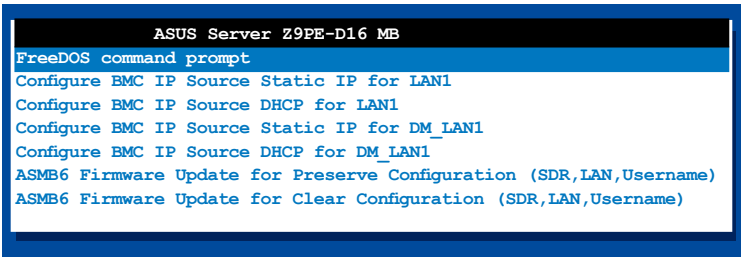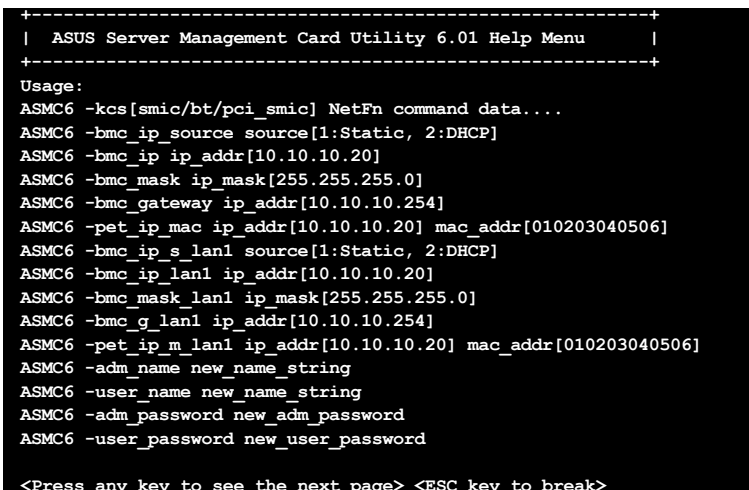
To run the ASMC6 utility:

1. Insert the support CD into the optical drive.

2. Restart the remote server, then press <Del> during POST to enter the BIOS setup.

3. Go to Boot menu and set the Boot Device Priority item to [CD-ROM].

4. When finished, press <F10> to save your changes and exit the BIOS setup.

5. On reboot, the main menu appears. Select **FreeDOS command prompt**, and then press <Enter> .

```
                  ASUS Server Z9PE-D16 MB
FreeDOS command prompt
Configure BMC IP Source Static IP for LAN1
Configure BMC IP Source DHCP for LAN1
Configure BMC IP Source Static IP for DM_LAN1
Configure BMC IP Source DHCP for DM_LAN1
ASMB6 Firmware Update for Preserve Configuration (SDR,LAN,Username)
ASMB6 Firmware Update for Clear Configuration (SDR,LAN,Username)
```

6. When the `C:>` prompt appears, type `ASMC6 -?`, then press <Enter> to display the ASMC6 Utility Help Menu. The screen appears as shown.

```
+---------------------------------------------------------+
|   ASUS Server Management Card Utility 6.01 Help Menu     |
+---------------------------------------------------------+
Usage:
ASMC6 -kcs[smic/bt/pci_smic] NetFn command data....
ASMC6 -bmc_ip_source source[1:Static, 2:DHCP]
ASMC6 -bmc_ip ip_addr[10.10.10.20]
ASMC6 -bmc_mask ip_mask[255.255.255.0]
ASMC6 -bmc_gateway ip_addr[10.10.10.254]
ASMC6 -pet_ip_mac ip_addr[10.10.10.20] mac_addr[010203040506]
ASMC6 -bmc_ip_s_lan1 source[1:Static, 2:DHCP]
ASMC6 -bmc_ip_lan1 ip_addr[10.10.10.20]
ASMC6 -bmc_mask_lan1 ip_mask[255.255.255.0]
ASMC6 -bmc_g_lan1 ip_addr[10.10.10.254]
ASMC6 -pet_ip_m_lan1 ip_addr[10.10.10.20] mac_addr[010203040506]
ASMC6 -adm_name new_name_string
ASMC6 -user_name new_name_string
ASMC6 -adm_password new_adm_password
ASMC6 -user_password new_user_password

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

Press any key to see next page.

```
<Press any key to see the next page> <ESC key to break>
ASMC6 -sol_baud 57600[9600/19200/38400/57600/115200]
ASMC6 -bmc_info
ASMC6 -fru -view fru_id
ASMC6 -fru -load fru_file
ASMC6 -fru -save fru_id ru_file
ASMC6 -sel -clear
C:\>
```

ASMC6 Help Menu options

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

2.5.1   Configuring the LAN controller

Before you can establish connection to the ASMB6-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 ASMC6 utility from the support CD following the instructions in the previous section.

2.   Set IP source:

(a) Type ASMC6 -bmc_ip_source 1 if you want to set a static IP address.

(b) Type ASMC6 -bmc_ip_source 2 if you want to get IP from DHCP server.

3.   Type ASMC6 -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:\>ASMC6 -bmc_ip  10.10.10.243
Detect MotherBoard     -> (Z9PE-D16 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 (a) subnet mask and (b) gateway address if necessary.

(a) Type ASMC6 -bmc_mask xxx.xxx.xxx.xxx (your subnet mask encoded in hexadecimal system)

(b) Type ASMC6 -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 ASMC6 utility.

To change the user name and password:

1. Follow steps 1-5 on page 2-11.
2. When the `C:>` prompt appears, type **ASMC6 -user_name xxxxx**, then press <Enter> to change the user name.

```
C:\>ASMC6 -user_name super
Detect MotherBoard    -> (Z9PE Series)
Detect KCS Interface

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

3. Type **ASMC6 -user_password xxxxxxxx**, then press <Enter> to change the password.
4. Restart the remote server, enter the BIOS setup, then boot from the hard disk drive.

2.6   Software installation

You can monitor, control, or manage the remote server from the local/central server using the ASUS Remote Console (ARC). The ARC is a web-based application available from the support CD that came with theASMB6-iKVM package. You must install the ARC on the local/central server to access the remote server.

Before you install the ARC:

- For SNMP Service: View the Platform Event Trap (PET) information. See page 3-17 for details.

- For Microsoft® ActiveSync: Enable the SMS feature. See page 3-15 for details.

2.6.1   Installing the ARC

To install the ARC to the local/central server:

1.   Place the support CD to the optical drive. The CD automatically displays the Drivers menu if Autorun is enabled in your computer.
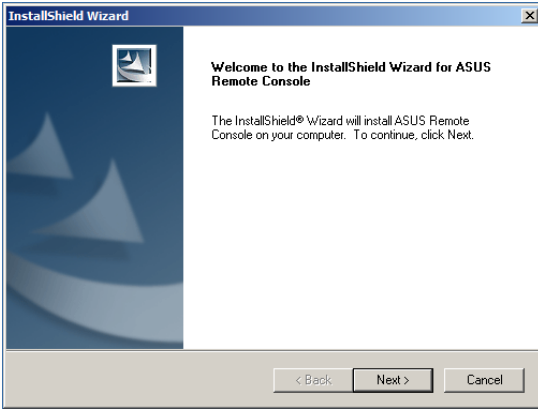
If Autorun is NOT enabled in your computer, browse the contents of the support CD to locate the file ARC.EXE in the ARC folder. Double-click the ARC.EXE to install the application.

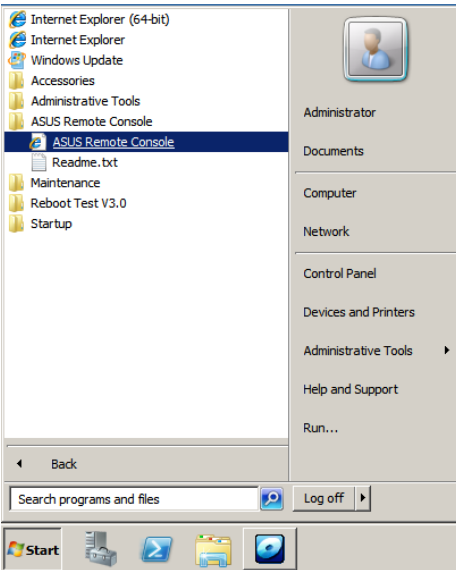2.   Click the **Utilities** tab, then click the item **ASUS Remote Console**.
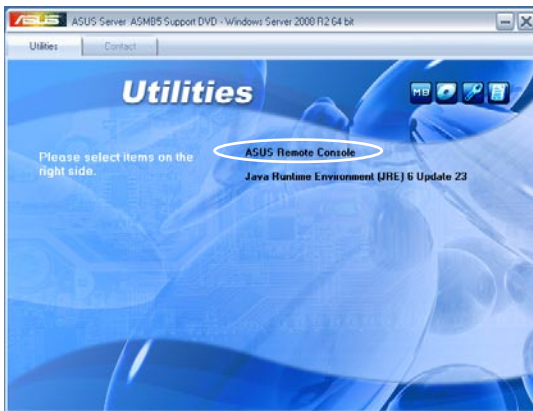
3. Follow the installation wizard instructions to install the utility.

2.6.2 Launching ARC

To launch the ARC utility, click **Start** > **All Programs** > **ASUS Remote Console** > **ASUS Remote Console** from the Windows® desktop.

OR
Double-click the ASUS Remote Console icon on the Windows® desktop.

This chapter tells you how to use the ASUS
Remote Console (ARC) that the server
management board supports.

ASUS
Remote Console

3

3.1   ASUS Remote Console (ARC)

The ASUS Remote Console (ARC) is a web-based utility, designed for
ASMB6-SOL PLUS, that allows you to monitor the remote host's hardware
information including temperatures, fan rotations, voltages, and power. This
application also lets you instantly power on/off or reset the remote server.
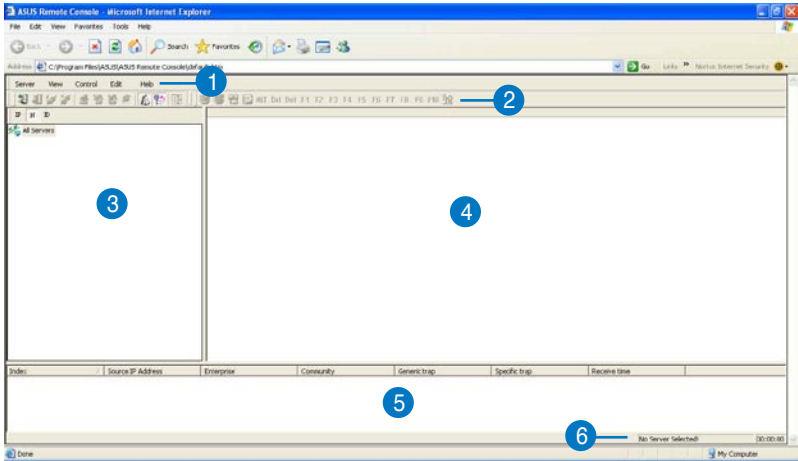
The ARC window is made up of six sections:

1.   Menu bar
2.   Tool bar
3.   Navigation window
4.   Detail/SEL window
5.   Event window
6.   Status bar

Refer to the following sections for details.

3.1.1 ARC sections

Menu bar

The Menu bar contains all the commands for the ARC application. Click on a menu to display a list of available commands.

| | Server | View | Control | Edit | Help |

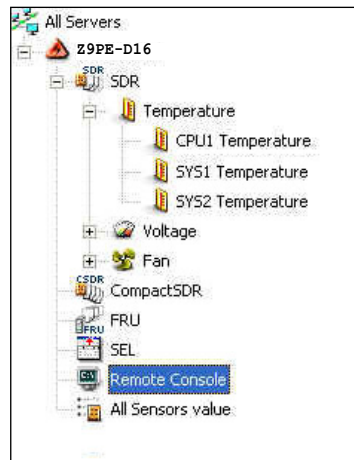| Menu	Available commands
Server	add, delete, connect, disconnect server or change the server settings; load/save server node list; general setting; dump/restore all configuration
View	show or hide the tool bar, status bar, navigation, and PET windows
Control	power down/up, reset, power cycle, power on Lan
Edit	delete the System Event Log (SEL), PET log, Reset PET destination, Reset Baud Rate; Set MAC address
Help	open Help contents or view information about the ARC application

Tool bar

The Tool bar buttons correspond to commonly used commands. The Tool bar offers faster access and execution of these commands. Roll the mouse pointer over a button to display its function.

ALT Ctrl Del F1 F2 F3 F4 F5 F6 F7 F8 F9 F10

Navigation window

The Navigation window displays the directory of connected and disconnected remote server(s). For multiple monitoring, this window allows you to navigate through the remote servers. Click the **All Servers** root directory to display all connected and disconnected servers, then click on the server you want to monitor or control.

Click ⊞ before the server connection to display available remote server information including the **SDR (Sensor Data Record)**, **FRU (Field Replaceable Unit)**, **SEL (System Event Log)**, and **Remote Console**.
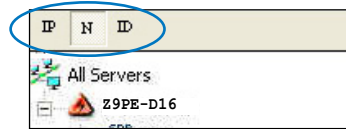
All Servers
- Z9PE-D16
  - SDR
    - Temperature
      - CPU1 Temperature
      - SYS1 Temperature
      - SYS2 Temperature
    - Voltage
    - Fan
  - CompactSDR
  - FRU
  - SEL
  - Remote Console
  - All Sensors value

Some remote server information (such as the SDR) contains several sensor groups such as **Temperature**, **Voltage**, and **Fan**. Click ⊞ before the remote server information to display the sensor groups.

Click ⊞ before a sensor group to display individual sensors. For example, clicking ⊞ before the sensor group Temperature displays the CPU1 and system temperatures.
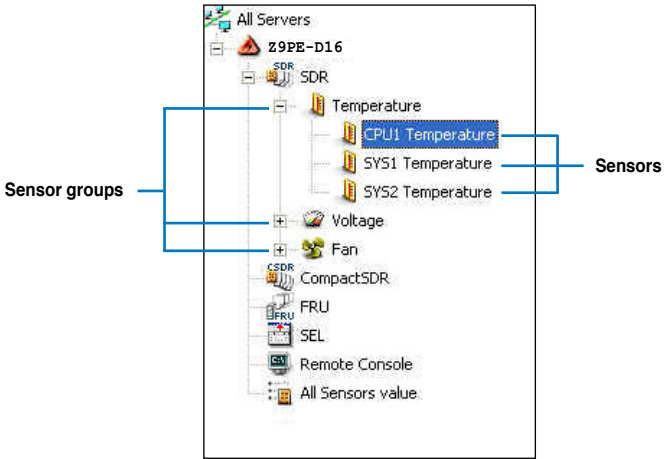

You can also change the server directory display by clicking the buttons on top of the window. For example, clicking the IP button displays the remote server IP address instead of the remote server name (N). Selecting ID displays the remote server ID instead of the server name or IP address.

Detail/SEL window

The **Detail/SEL** window displays the detailed SDR and FRU information, and the SEL (System Event Log). The window provides the link for detailed sensor information or system events and allows you to adjust the sensor threshold values.

Attribute	Value		Meanings
Sensor ID	1	More	
Sensor Name	CPU1 Temperature		
Current Value	0x28		40.0 degrees C
Theory Value	0x28		40.0 degrees C
Upper non-recoverable Threshold	0x60		96.0 degrees C
Upper critical Threshold	0x58		88.0 degrees C
Upper non-critical Threshold	0x50		80.0 degrees C
Lower non-recoverable Threshold	0x08		8.0 degrees C
Lower critical Threshold	0x10		16.0 degrees C
Lower non-critical Threshold	0x18		24.0 degrees C

Event window

The **Event** window displays the Platform Event Trap (PET) received by the ARC. The PET information includes the event index, source IP address, enterprise, community, generic and specific traps, and time ticks. The PET information is a system management alert in SNMP Trap format and is used for IPMI alerting.

Index	Source IP Address	Enterprise	Community	Generic trap	Specific trap	Receive time	

Status bar

The **Status** bar located at the bottom of the ARC window displays the connection status to the remote server, connection duration, IP address of the remote server, and the progress of SDR/SEL/FRU information download.

Get SEL record : 127 ▮▮▮ 10.10.10.10 Connected 00:00:09

3.1.2   Connecting to the remote server

To connect to the remote server:

1. From the menu bar, click **Server**, then select **Add New Server Node**. An **Add new server connection** window appears.
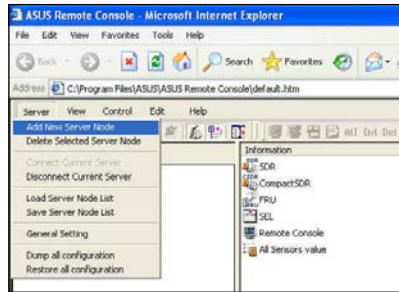

2. Type the remote server name and IP address on the fields. Click **Save Default** to set the remote server connection as the default. Otherwise, click **OK** to continue or **Cancel** to close the window.
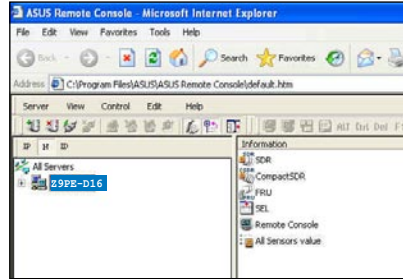

The default server connection name and IP address are automatically displayed everytime you add a new server connection.

3. When prompted, select **IPMI Server**, then click **Continue**.
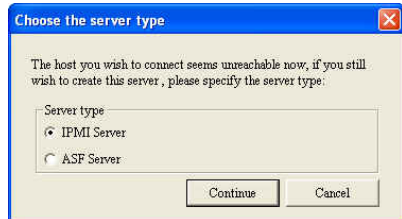
The navigation window displays the remote server. The available remote server information are displayed on the **Detail/SEL** window.

4. Use any of these options to connect to the server:

- Click ⊞ before the remote server to display the remote server information, then select from the list.

- Double-click a remote server information from the **Detail/SEL** window.

- Click **Server**, then select **Connect**.

5. When prompted, enter the default user name (admin) and password (admin).

6. Set the connection request level authentication and privilege, then click **OK**.
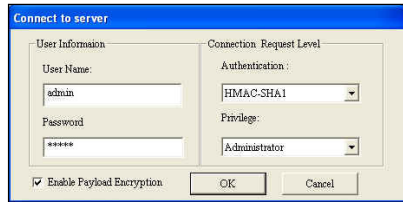
- The default connection request level authentication is HMAC-SHA1 with Administrator privileges. You may change these configuration according to your network settings or preference.

- Check the box before **Enable Payload Encryption** if you want to use Advanced Encryption Standard (AES).

3.1.3 Retrieving sensor information

The Sensor Data Record (SDR) provides remote server system information through available sensors including CPU/system/power temperatures, voltages, fan speeds, chassis intrusion, etc. The SDR also provides information on the sensor location (e.g. CPU1, CPU2, FAN1), event generation, and access information.

To retrieve a sensor information:

1. From the navigation window, click ⊞ before the server name to display the remote server information.
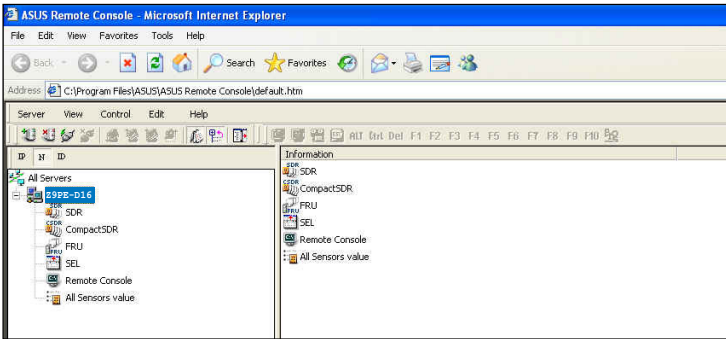
2. Click ⊞ before the **SDR** to display the sensor groups (e.g. Temperature), then click ⊞ before a sensor group to display the individual sensors. Select a sensor (e.g. CPU1 Temperature) to display its values in the **Detail/SEL** window.
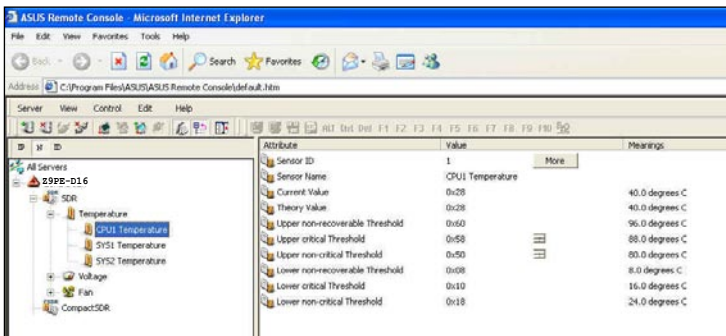

The **Detail/SEL** window displays the sensor data attributes, values, and meanings. From this window, you can adjust the sensor threshold values by clicking the up/down arrow button after each value.

3. Click **More**. A sensor window appears displaying additional information on the sensor.

   The Information tab displays basic sensor information including the sensor name, current status, current value, and sensor type.

   The tab also displays the sensor record ID and SDR version.
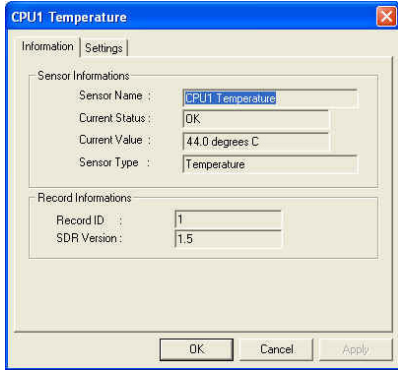
4. Click the **Settings** tab to adjust the sensor threshold values. Click on the up/down arrow button after each threshold value to adjust.

   Click **OK** to close the window.
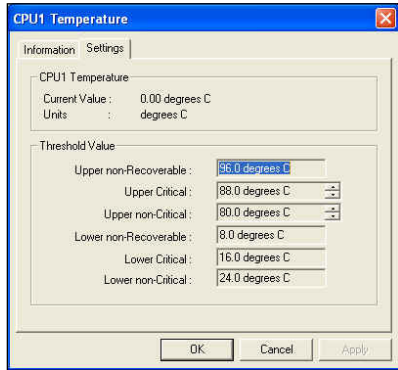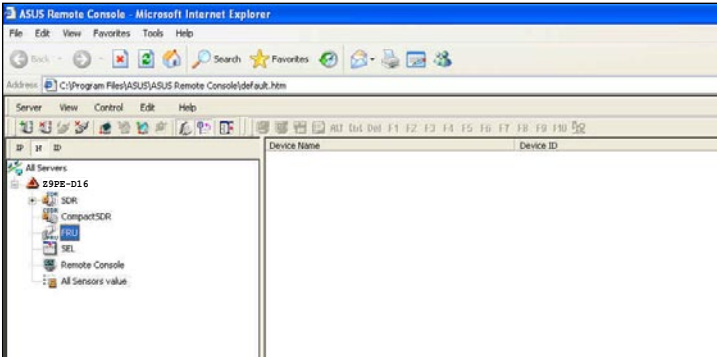
3.1.4 Displaying FRU information

The Field Replaceable Unit (FRU) information provides the manufacturer, product name, and/or serial number of various modules and components installed on the remote server. For example, the FRU feature can display the remote server motherboard name, model, and serial number. You can use this feature when retrieving information on a module or component installed on the remote server.

> • The FRU information feature allows you to obtain component or module information even when the remote server is down or off.
>
> • The motherboard information is not included in the FRU information.

To display the FRU information:

1.   From the navigation window, click ⊞ before the server name to open the remote server information.

2.   Click ⊞ before the **FRU** to display available FRU information, then click ⊞ before the module/component. Select a module or component from the list to display the FRU information in the **Detail/SEL** window.
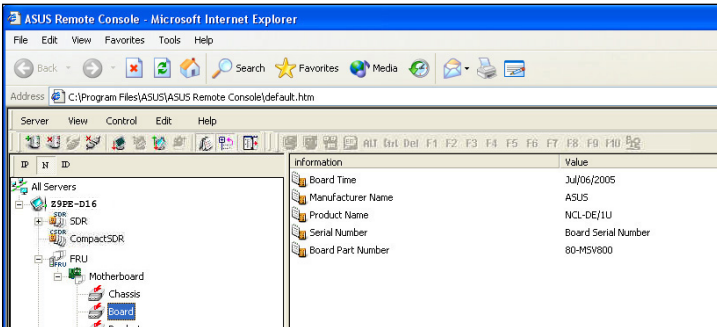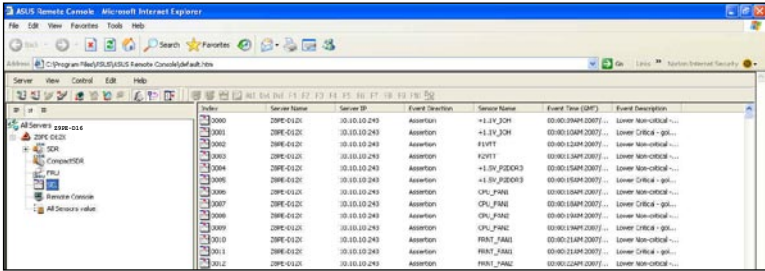
3.1.5   Displaying system event logs

The System Event Log (SEL) is a non-volatile storage area where all remote server system events are stored for real-time tracking or later retrieval. The ARC application can display system events for efficient remote server monitoring and troubleshooting.
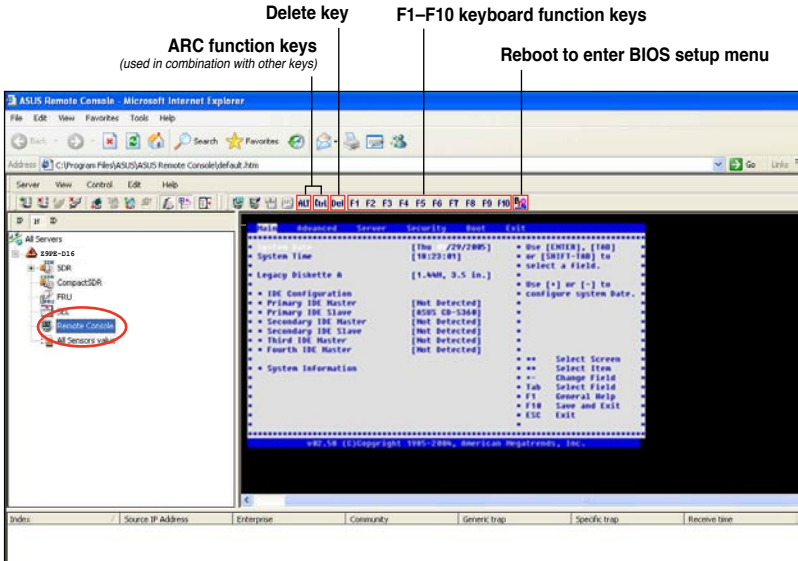
To display the sytem events:

1.   From the navigation window, click ⊞ before the server connection, then click **SEL**. The status bar displays the progress of the SEL download. When finished, the **Detail/SEL** window displays the system events in chronological order.

2.   Double-click an event to display an **Event Information** window.

This window displays the sensor type and record ID, event message, current and threshold values, and other system event information.

3.   Click **OK** to close the window.

3.1.6   Using Remote Console

The Remote Console feature lets you see the remote server screen (text only) and is useful when you adjust the remote server BIOS settings.

To display the remote server console, press the **Remote Console** item from the navigation window. The remote server screen appears in the **Detail/SEL** window.


Delete key

F1–F10 keyboard function keys

ARC function keys
(used in combination with other keys)

Reboot to enter BIOS setup menu

3.1.7   Displaying all remote server sensors

To display all remote server sensors in graphical format:

1.   From the navigation window, click ⊞ before the server name to open the remote server information.

2.   Click **All Sensors value**. All remote server sensors are displayed on the Information window in graphical format.

     The color bar represents the upper/lower threshold values of each sensor. The green pointer indicates the current value of the sensor.
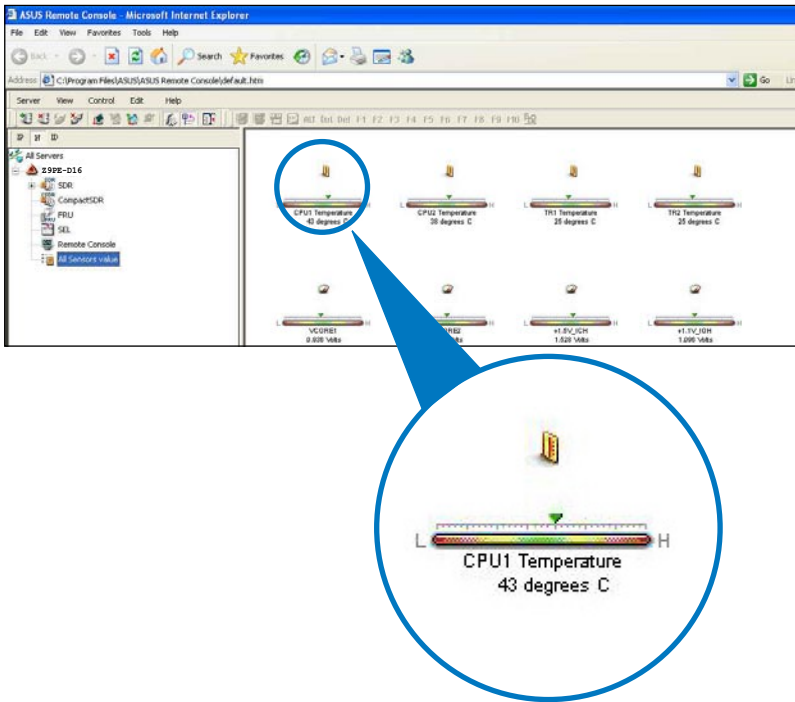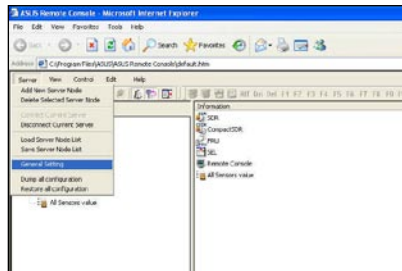
3.1.8 Adjusting the monitoring settings

The ARC application allows you to adjust the remote server monitoring settings including SEL polling, SDR reading, and PET.

To adjust the monitoring settings:

1. Click **Server** on the menu bar, then select **General Setting** from the drop-down menu. A **Server Settings** window appears.

2. Click on the up/down arrow button after each setting to adjust the value.

3. Click **OK** to save your changes and close the window; otherwise, click **Cancel** to ignore your changes.
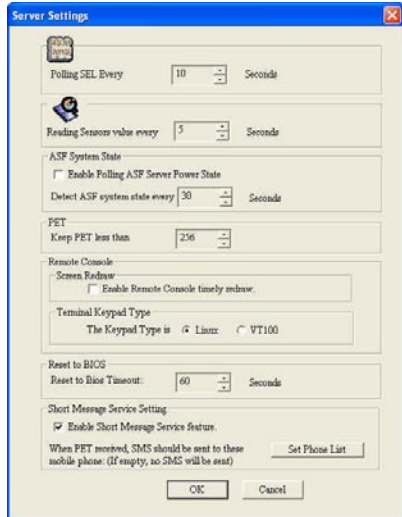
Enabling the Short Message Service (SMS) feature

The Short Message Service or SMS feature allows you to receive Platform Event Trap (PET) information on your smart phone (ASUS P505).

You must install Microsoft® ActiveSync® before you enable the SMS feature. Visit www.microsoft.com to download Microsoft® ActiveSync® .

To enable the SMS feature:

1. Check the box before the **Enable Short Message Service** feature.

2. Click **Set Phone List**.
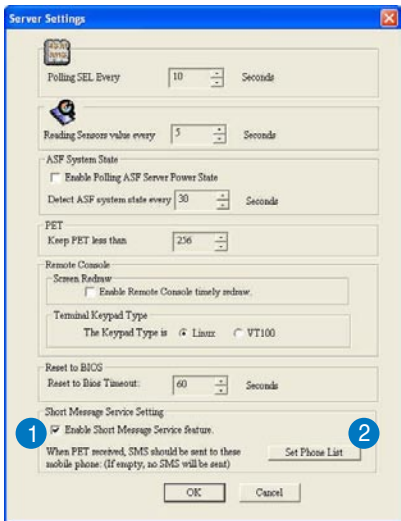
3. When the **SyncSMS mobile phone number setup** window opens, key-in the mobile or PDA phone number in the box.

   You may click the box before each phone number to disable it.

4. Press **OK**.
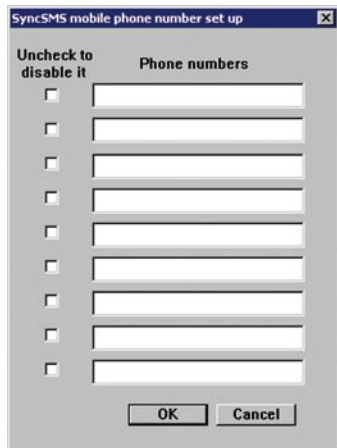
3.1.9   Controlling the remote server power

ARC allows you to power up, power down, or reset the remote server using the power menu.

Before turning off or resetting the remote server, make sure that it is not being used and that no application is currently running on it to avoid data loss.

To power down the remote server:

1. Click **Control** on the menu bar, then select **Power down** from the drop-down menu.

    OR

    Click the power down button on the tool bar.
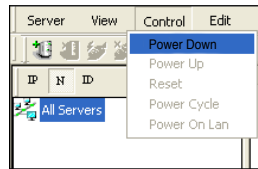
2. Click **Yes** when the Confirm power down window appears.

3. The remote server is turned off. Click **OK** to close the window.

    Use the same instructions as reference when powering up or resetting the remote server.

3.1.10   Viewing PET information

The Platform Event Trap or PET is an SNMP trap used for system management alerts. When the ARC receives a PET, it displays a pop-up window notifying you of the alert and its source (IP address). Right-click the window to close.
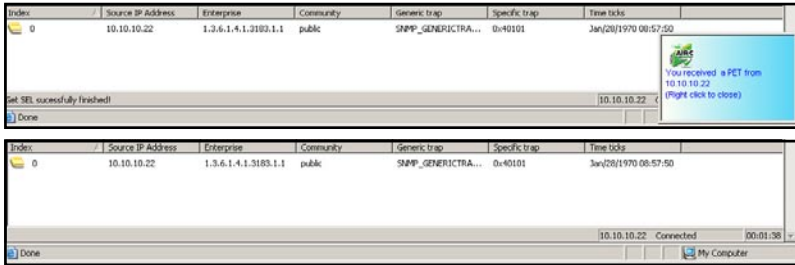
You need to install an SNMP service to the remote server to receive PET information.

To install an SNMP service to the remote service:

1.   On the Windows® taskbar, click **Start > All Programs > Control Panel.**
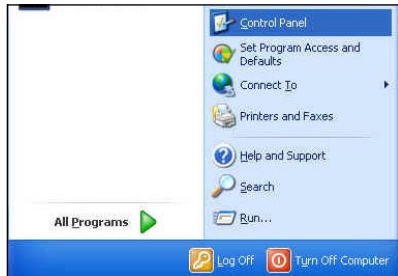
2.   Double-click **Add/Remove Programs.**
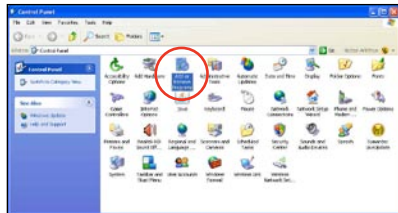
3.   Double-click **Add Windows Components.**

4. Double-click **Management and Monitoring Tools**.

5. Select **Simple Network Management Protocol (SNMP).**

6. Click **OK**.
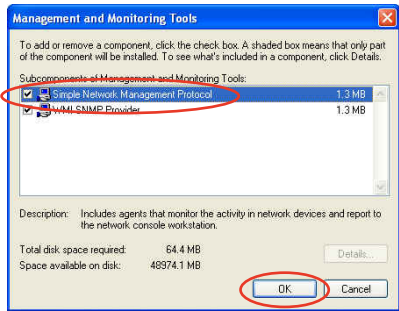
Important notice for Windows® XP (Service Pack 2) users

If the local server system is behind a firewall, you must create a UDP port to receive PET information.

To create a UDP port:

1.   Double-click the **My Computer** icon from the Windows® desktop, then click the **My Network Places** link.
2.   Click the **View network connections** link, then select the LAN connection the remote server system is using.
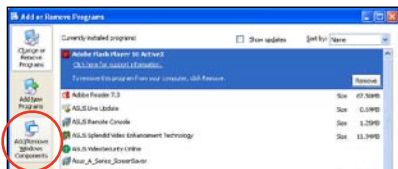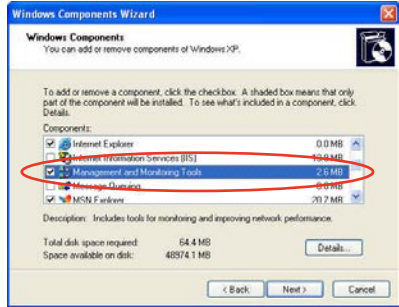3.   Right-click the LAN connection, then select **Properties** from the drop-down menu.
4.   Click the **Advanced** tab, then click the **Settings** button in the **Network Connection Sharing** area.
5.   On the **Services** tab, click the **Add** button to display a **Service Settings** window.
6.   Type a name on the **Description of service field** (i.e. ASUS ARC).
7.   Type the IP address of the local/central server, then set the **External** and **Internal Port number** to **162**.
8.   Select **UDP**, then click **OK**. The created service is displayed in the Services list. Check the box before the service, then click **OK**.

You must also adjust the Internet Explorer settings to allow active contents to run in the local/central server. To do this:

1.   From the **Internet Explorer** menu, click **Tools**, then select **Internet Options** from the drop-down menu.
2.   Click the **Advanced** tab.
3.   Enable the item "**Allow active content to run in files on My Computer**".
4.   Click the **Apply** button, then click **OK** to close the window.

3.2   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.

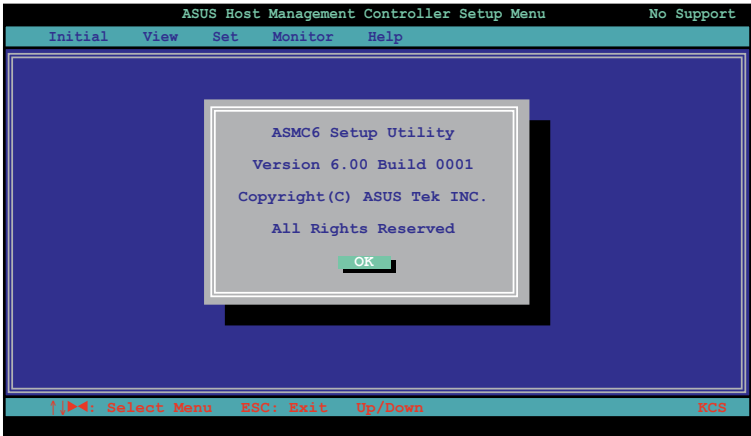### 3.2.1   Installing and launching the ASUS Host Management Controller Setup utility

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 **ASMC6**, then press <Enter> to display the ASMC5 Utility Help Menu. The screen appears as shown.

```
C:\>ASMC6
```

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

3.2.2 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.

```
                    ASUS Host Management Controller Setup Menu        No Support
      ▶  Initial     View      Set     Monitor     Help

          Clear SEL
          Exit
```

Menu options
Menu bar
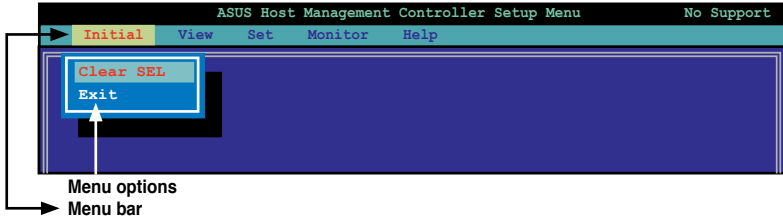
3.2.3 Initial

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.

```
                    ASUS Host Management Controller Setup Menu        No Support
         Initial     View      Set     Monitor     Help

          Clear SEL
          Exit
```
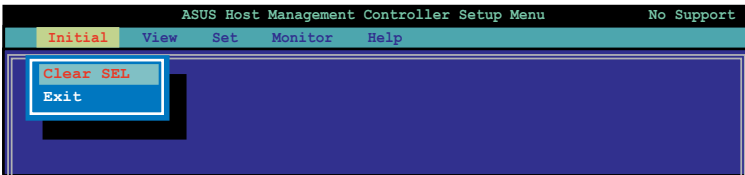
3.2.4 View

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.

```
                    ASUS Host Management Controller Setup Menu        No Support
         Initial     View      Set     Monitor     Help

              BMC SEL
              BMC SDR
              BMC Info
```
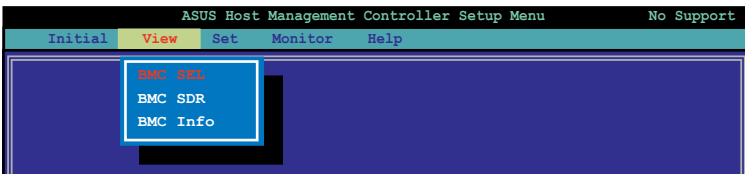
To view the System Event Log (SEL):

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

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

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

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

```
         ASUS Host Management Controller Setup Menu          No Support
    Initial    View    Set    Monitor    Help


   Systen Event Log: (Hex)

   01 00 02 09 4E 98 45 20       Record ID    : 0001h
   00 04 02 3A 01 50 19 09       Record Type  : 02h (System Event Record)
                                 Date & Date  : Fri Jan 21 20:43:00 2011
   1/202                         General ID   : 2008h
                                 EvM Rev      : 04h (IPMI 1.5)
                                 Sensor Type  : 02h (Voltage)
                                 Sensor Number: 3Ah (+1.1V_IOH)
                                 Event Dir    : 01h (Threshold)
                                 Event Datal  : 50h
                                 Event Value  : 19h (0.2 V)
                                 Threshold    : 09h 1.0 V)
                                 Offset: Lower Non-critical - going low




      ↑↓◄►: Select Menu    ESC: Exit    Up/Down                    KCS
```
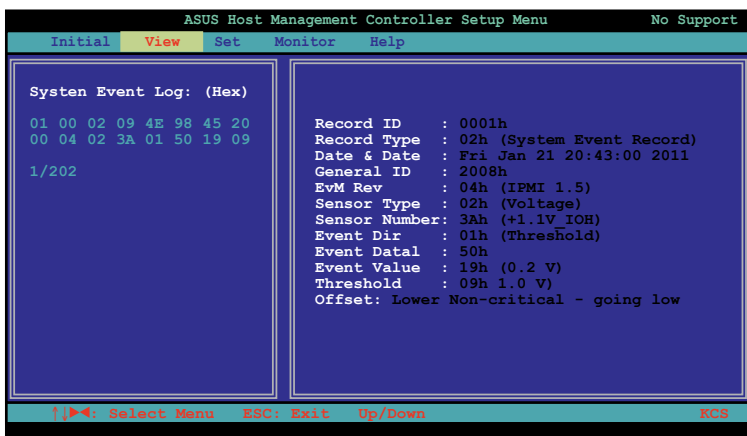
To view the System Data Record (SDR):

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

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

```
             ASUS Host Management Controller Setup Menu          No Support
      Initial    View    Set    Monitor    Help


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


      ↑↓◄►: Select Menu    ESC: Exit    Up/Down                      KCS
```

2. Use the down arrow key to display the next sensor data record.

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

To view the BMC information:

1. Select **BMC Info** from the **View** command option, then press <Enter>. A list of BMC information appears on the left pane.

2. Use the down arrow button to select a BMC information. The BMC information is displayed in the right pane.

```
               ASUS Host Management Controller Setup Menu        No Support
      Initial    View    Set    Monitor    Help

    IPMI Information            Device ID        : 20h
    SEL  Information            Device Revision  : 01h (No SDR)
    SDR  Information            Firmware Revision : 1.04
    BMC  Real Time Clock        IPMI Version     : 2.0
                                Manufacturer ID  : 001043h
                                Product ID       : 0B43h
                                IPMI Device Support:
                                  Chassis Device          -> Support
                                  Bridge                  -> No Support
                                  IPMB Event Generator    -> Support
                                  FRU Inventory Device    -> Support
                                  SEL Device              -> Support
                                  SDR Repository Device   -> Support
                                  Sensor Device           -> Support



      ↑↓►◄: Select Menu    ESC: Exit    Up/Down                        KCS
```

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

3.2.5 Set

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

```
               ASUS Host Management Controller Setup Menu        No Support
      Initial    View    Set    Monitor    Help

                  Host Interface
                  BMC Timer
```

To select the host interface:

1. Select **Host Interface** from the **Set** command option, then press <Enter>. The screen displays the host interfaces supported by the server management board.

2. Use the down arrow button to select a host interface, then press <Enter>.
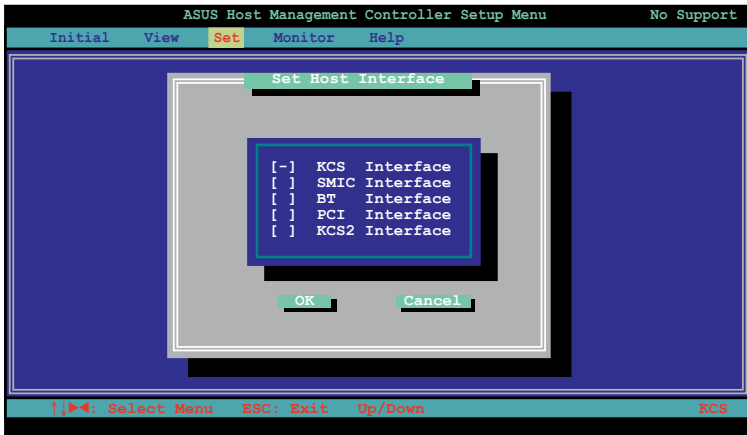
You can select from the following interfaces:

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.

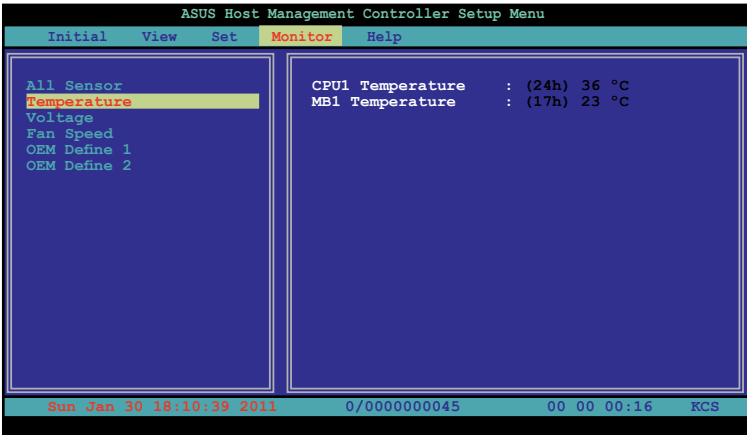3. When finished, press <Esc> to return to the main screen.

3.2.6   Monitor

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

```
        ASUS Host Management Controller Setup Menu        No Support
    Initial    View    Set    Monitor    Help

                          All Sensor
                          Temperature
                          Voltage
                          Fan Speed
                          OEM Define 1
                          OEM Define 2
```
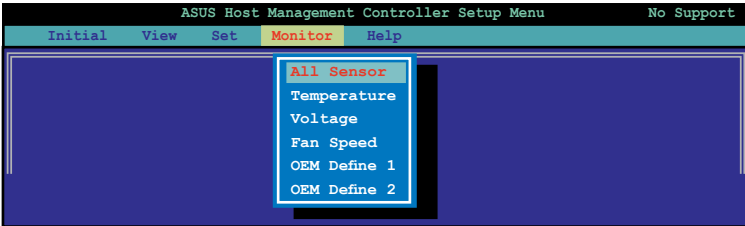
To display a remote server information:

1. Select a sensor from the **Monitor** command options, then press <Enter>. A list of server information appears on the left pane.

2. Use the down arrow button to select a monitor information. The selected monitor information details are displayed in the right pane.

```
        ASUS Host Management Controller Setup Menu
    Initial    View    Set    Monitor    Help

    All Sensor              CPU1 Temperature    : (24h)  36 °C
    Temperature             MB1 Temperature     : (17h)  23 °C
    Voltage
    Fan Speed
    OEM Define 1
    OEM Define 2




       Sun Jan 30 18:10:39 2011      0/0000000045      00 00 00:16    KCS
```

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

3.2.7 Help

The **Help** command displays the available utility options, utility version, and copyright information.
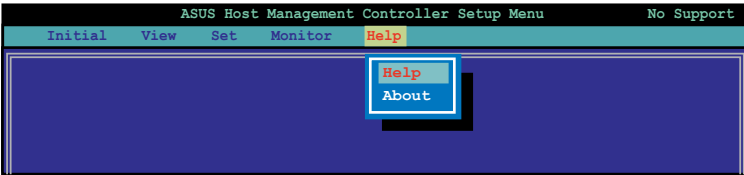
This chapter tells you how to use the
web-based user interface that the server
management board supports.

Web-based
user interface

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 ASMB6-iKVM support CD. You can also download JRE from **http://java.sun.com/javase/downloads**.

4.1.1   Loging in the utility

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

2.   Open the web browser and type in the same IP address as the one in the remote server.

3.   The below screen appears. Enter the default user name (admin) and password (admin). Then click Login.
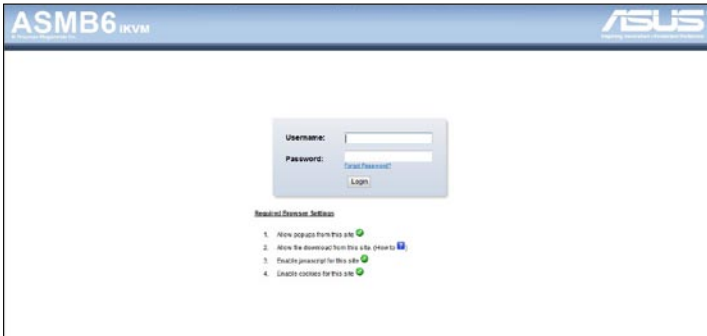
4.1.2 Using the utility

The web-based graphics user interface displays when you login in the utility successfully.
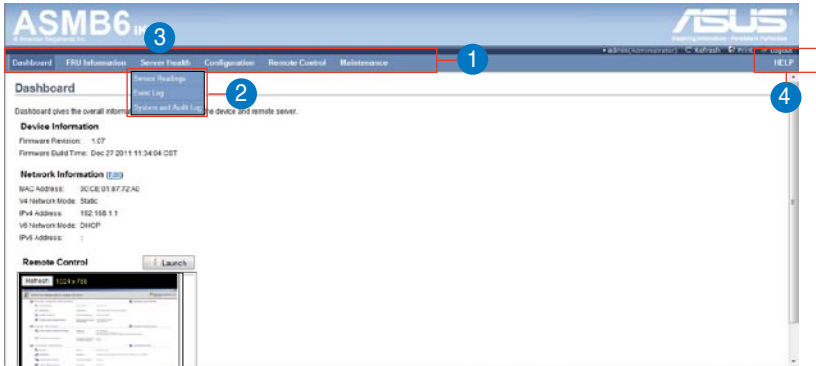
1. **Menu bar:** Click a menu to display available function lists.
2. **Function list:** Click each function key to start using its specific functions.
3. **Function title:** Displays the function title.
4. **Help menu:** Click to display the brief description of the selected function.
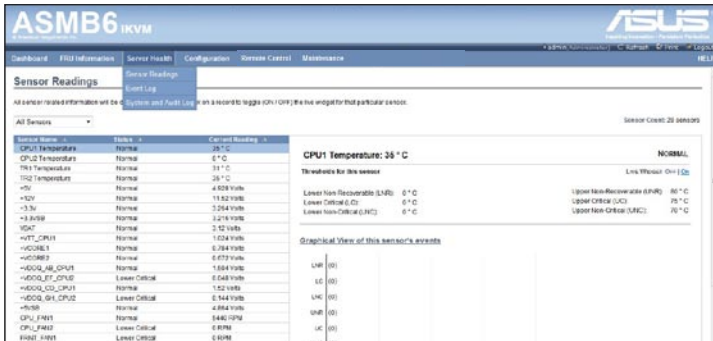
4.2   FRU Information

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

4.3   Server Health

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

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:** Show the type of sensor readings list that you selected in the drop-down list.
3. **Live Widget:** Click to enable or disable the Live Widget function.

4.3.2 Event Log

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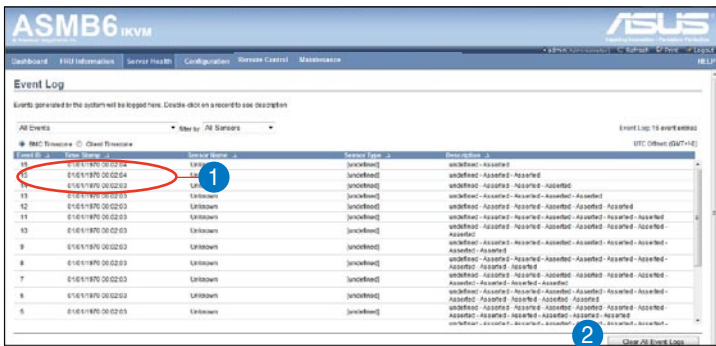
1. **Select an event log category:** Allows you to select the type of events to be displayed in the list.
2. **Clear Event Log:** Click to clear the event log.

4.4 Configuration

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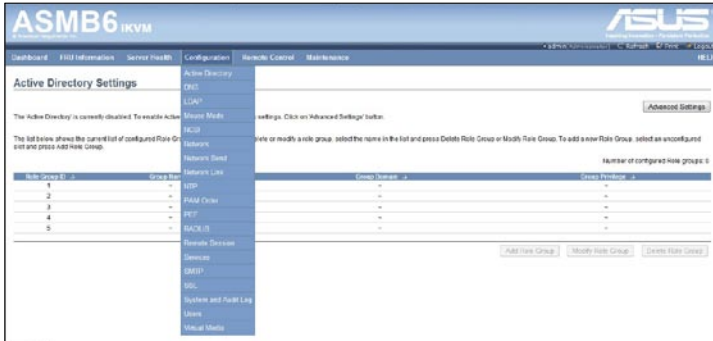
4.4.1 Active Directory

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.

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

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

4.   Specify the Domain Name for the user in the User Domain Name field. e.g. asus.com

5.   Specify the time (in seconds) to wait for Active Directory queries to complete in the Time Out field.
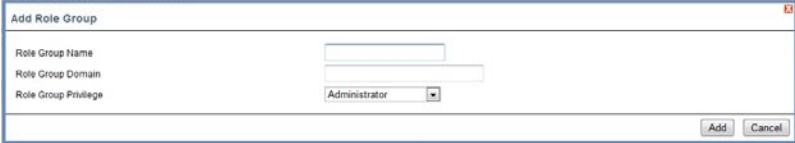
> 1.   Default Time out value: 120 seconds.
>
> 2.   Range from 15 to 300 allowed.

6.   Configure IP addresses in **Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3.**

7.   Click **Save** to save the entered settings and return to Active Directory Settings Page.

8.   Click **Cancel** to cancel the entry and return to Active Directory Settings Page.

To add a new Role Group

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

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

> 1. Role Group Name is a string of 255 alpha-numeric characters.
>
> 2. Special symbols hyphen and underscore are allowed.

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

> 1. Domain Name is a string of 255 alpha-numeric characters.
>
> 2. Special symbols hyphen, underscore and dot are allowed.

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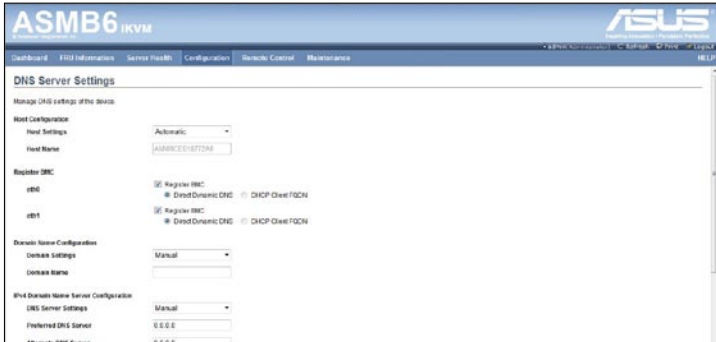
To Modify Role Group

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

To Delete a Role Group

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

4.4.2   DNS

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

4.4.3   LDAP

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

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

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.

1.	IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.

2.	Each Number ranges from 0 to 255.

3.	First Number must not be 0.

4.	Supports IPv4 Address format and IPv6 Address format.

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

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.

> 1. Search Base is a string of 255 alpha-numeric characters.
>
> 2. Special symbols hyphen, underscore and dot are allowed.

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

To Modify Role Group

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

To Delete a Role Group

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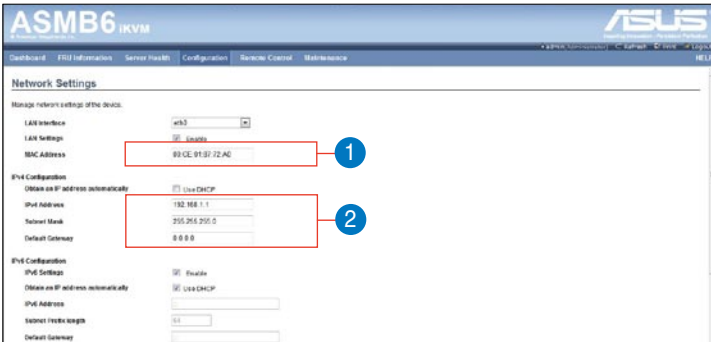
4.4.4 Mouse Mode

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

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

### 4.4.5 Network

The Network page allows you to configure the network settings.

1.   **MAC Address:** Select whether to obtain the IP address automatically or
                    manually configure one.

2.   **IP Address/Subnet Mask/Default Gateway:** If you configure a static IP,
                                    enter the requested address,
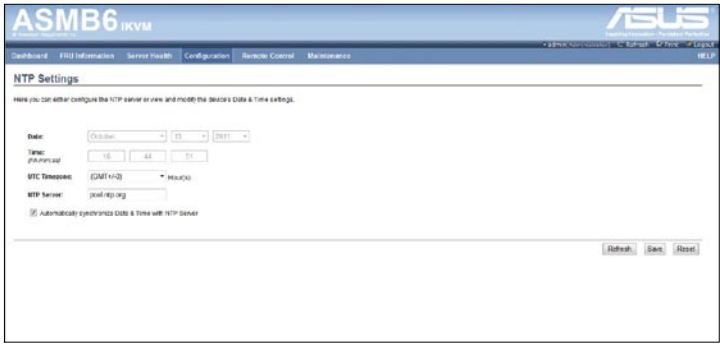   subnet mask and gateway in
                                    the given field.

4.4.6 Network Bond

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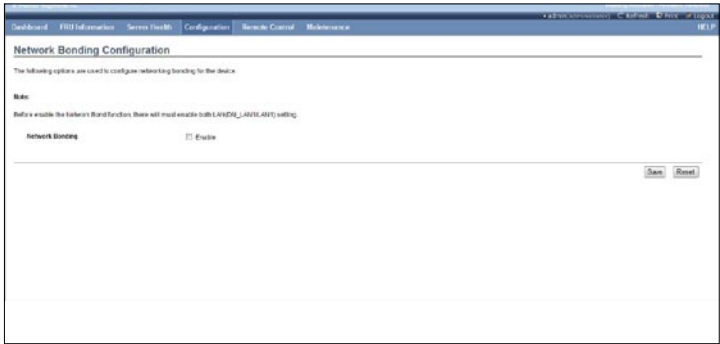

4.4.7 NTP

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

4.4.9 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.
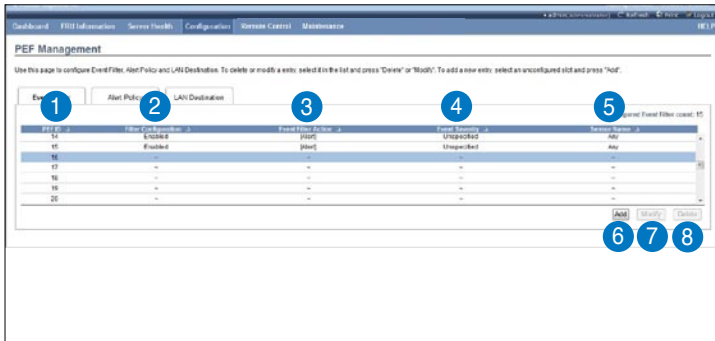
The PEF Management is used to configure the following

• Event Filter

• Alert Policy

• LAN Destination

Event Filter Tab

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.

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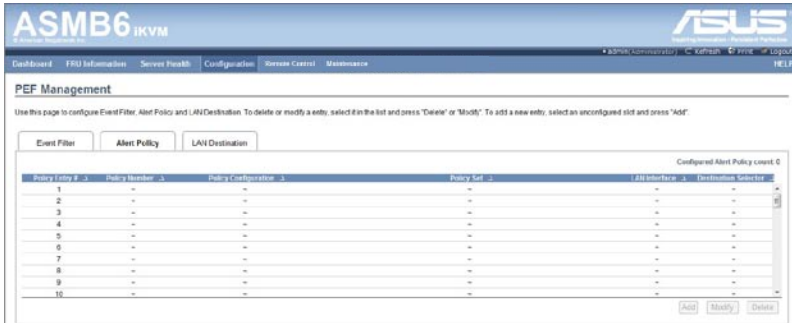
The fields of PEF Management – Alert Policy Tab are explained below.

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. **Channel Number:** To choose a particular channel from the available channel list.

6. **Destination Selector:** To choose a particular destination from the configured destination list.

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

---

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

Procedure:

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** as shown in the screenshot below.

3. **Policy Entry #** is a read only field.

4. Select the **Policy Number** from the list.

5. In the **Policy Configuration** field, check **Enable** if you wish to enable the policy settings.

6. In the **Policy Set** field, choose any of the Policy set from the list.

7. In the **Channel Number field**, choose particular channel from the available channel list.

8. In the **Destination Selector field**, choose particular destination from the configured destination list.

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

9.   In the **Alert String** field, enable the check box if the Alert policy entry is Event Specific.

10. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

11. Click **Add** to save the new alert policy and return to Alert Policy list.

12. Click **Cancel** to cancel the modification and return to Alert Policy list.

13. In the Alert Policy list, to modify a configuration, select the slot to be modified and click **Modify**.

14. In the **Modify Alert Policy Entry Page**, make the necessary changes and click **Modify**.

15. In the Alert Policy list, to delete a configuration, select the slot and click **Delete**.

PEF Management LAN Destination Page

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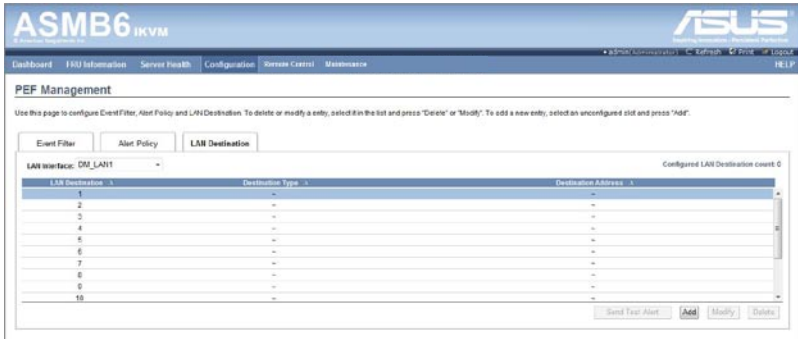
The fields of PEF Management – LAN Destination Tab are explained below.

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.

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

6. Select the **User Name** from the list of users.

7. In the **Subject field**, enter the subject.

8. In the **Message field**, enter the message.

9. Click **Add** to save the new LAN destination and return to LAN destination list.

10. Click **Cancel** to cancel the modification and return to LAN destination list.

11. In the LAN Destination Tab, to modify a configuration, select the row to be modified and click **Modify**.

12. In the **Modify LAN Destination Entry** page, make the necessary changes and click Modify.

13. In the LAN Destination Tab, to delete a configuration, select the slot and click **Delete**.

4.4.10 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. **KVM Encryption:** Enable/Disable encryption on KVM data for the next redirection session.

2. **Media Encryption:** Enable/Disable encryption on Media data for the next redirection session.

3. **Virtual Media Attach Mode:** Two types of VM attach mode are available:

• Attach - Immediately attaches Virtual Media to the server upon bootup. (The option is for local F/W Update using.)

• Auto Attach - Attaches Virtual Media to the server only when a virtual media session is started.

4. **Save:** To save the current changes.

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

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

4.4.12   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.
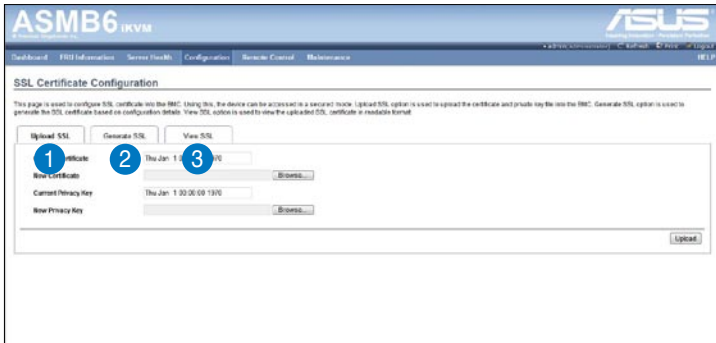
1. **Upload SSL** option is used to upload the certificate and private key file into the BMC.

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.

---

1. Once you Upload/Generate the certificates, only HTTPs service will get restarted.

2. You can now access your Generic MegaRAC® SP securely using the following format in your IP Address field from your Internet browser: https://<your MegaRAC® SP's IP address here>

3. For example, if your MegaRAC® SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30

4. Please note the <s> after <http>. You must accept the certificate before you are able to access your Generic MegaRAC® SP.

4.4.15 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.
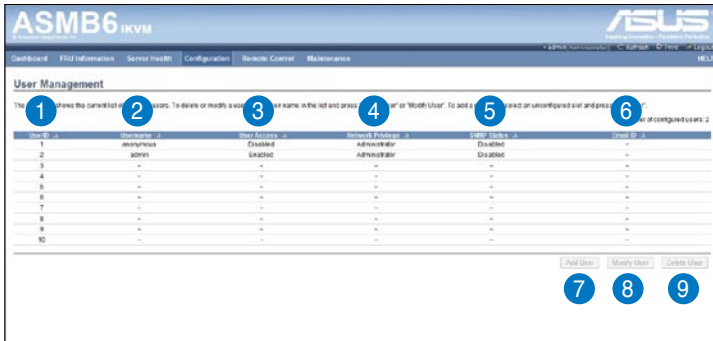
1. **User ID:** Displays the ID number of the user. Note: The list contains a maximum of ten users only.

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.

4.5   Remote Control

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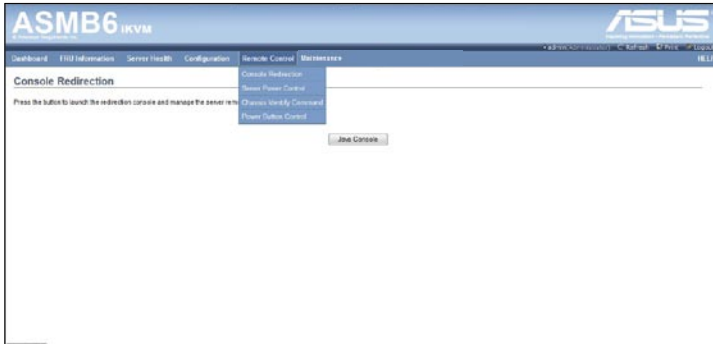
4.5.1   Console Redirection

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**.

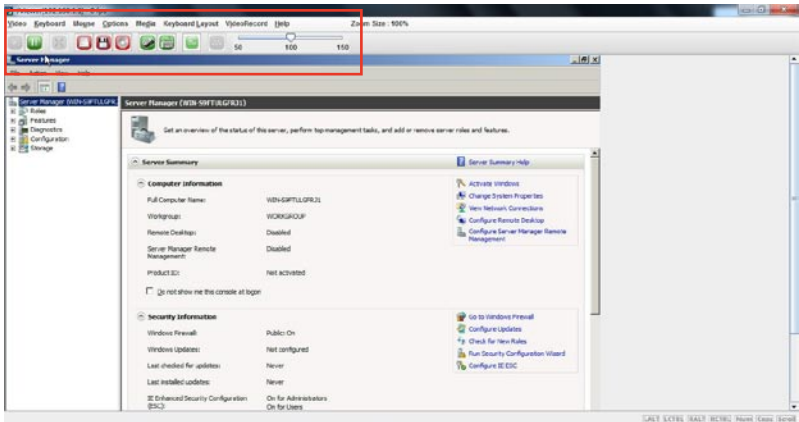This will download the .jnlp file from BMC.

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
•   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. **Compression Mode:** This option is used for setting video compression in Console Redirection. The recommend setting is YUV420.

5. **DCT Quantization Table:** This option is used for setting DCT Quantization in Console Redirection. The recommend setting is "4".

6. **Host Video Output:** If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.

7. **Full Screen:** This option is used to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are same.

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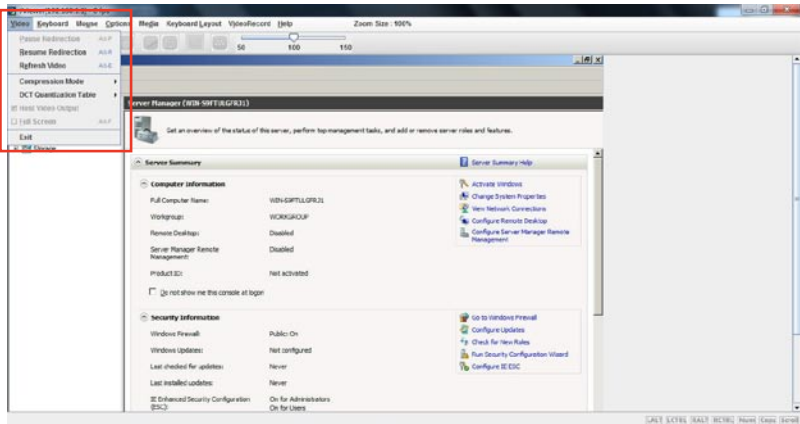
Keyboard

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.
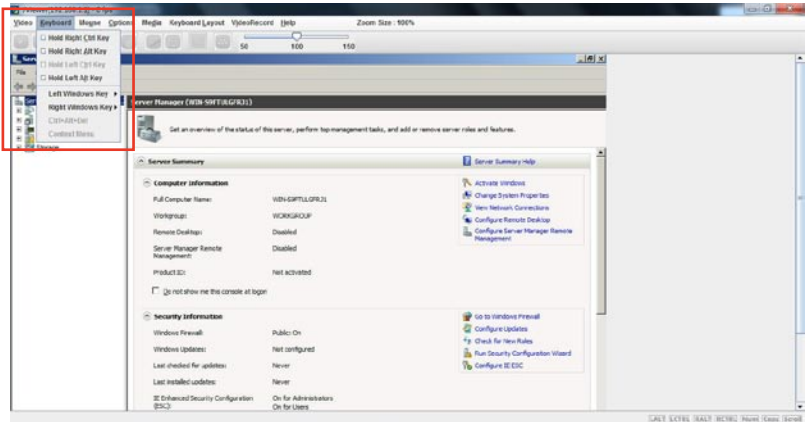
Mouse

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

2. **Mouse Calibration:** This menu item can be used only if the mouse mode is relative.

In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be synchronized in the beginning. Please use '+' or '-' keys to change the threshold settings until both the cursors go out of synch. Please detect the first reading on which cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold value.
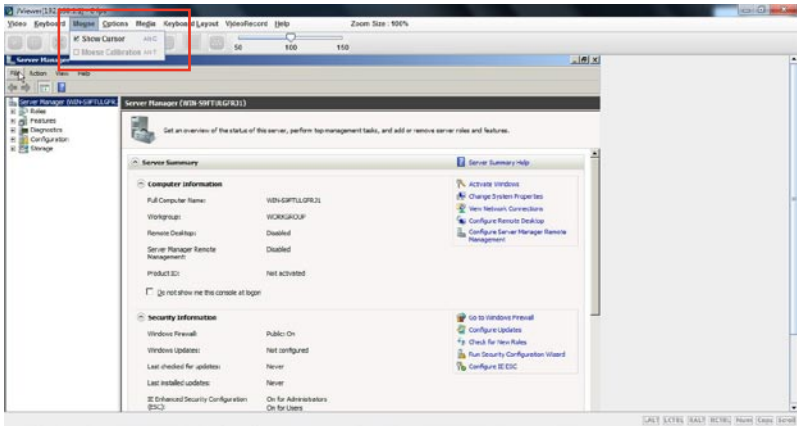
Options

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

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

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

Zoom:

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

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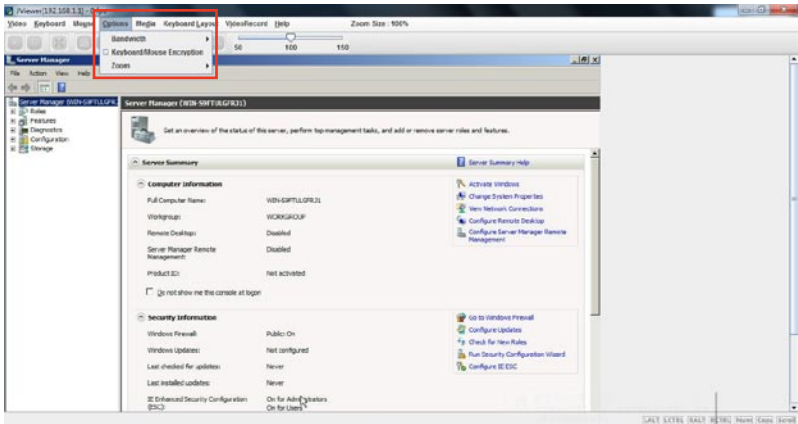
Media

Virtual Media Wizard:

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

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

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

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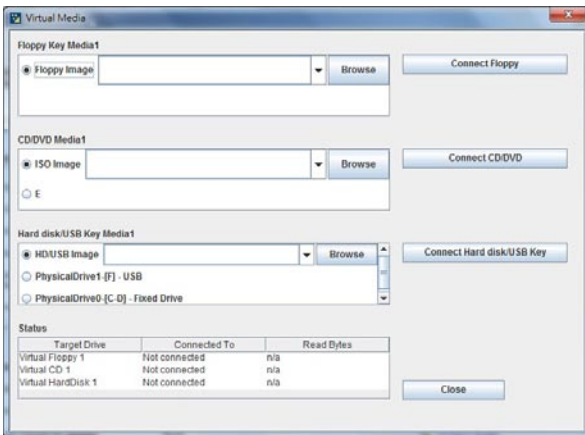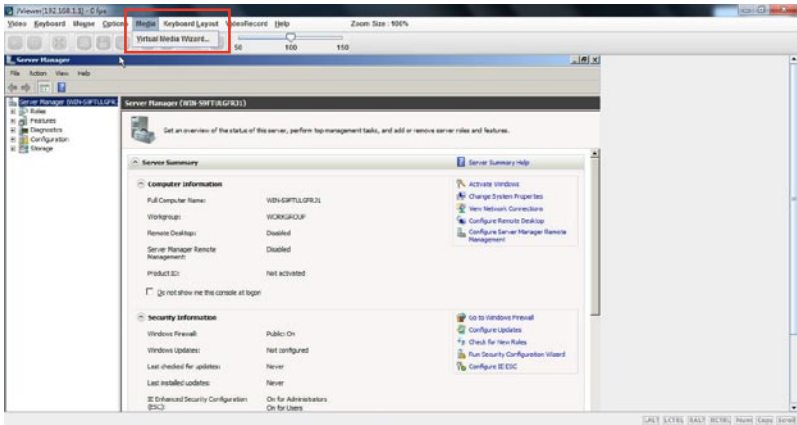
Virtual Media Wizard

Keyboard Layout

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

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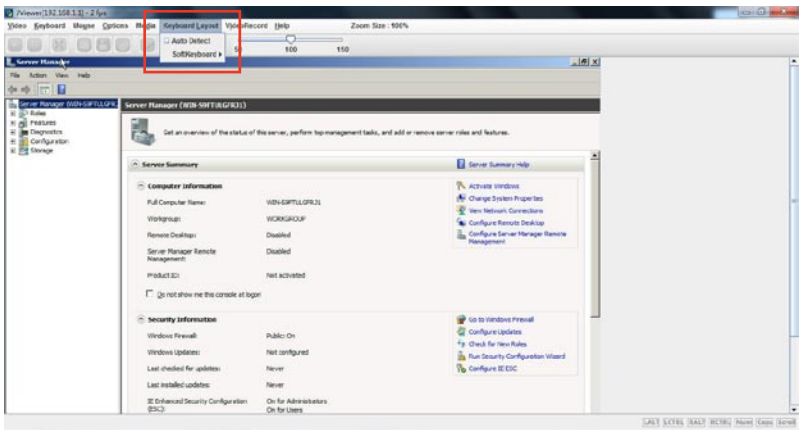
4.5.2 Server Power Control

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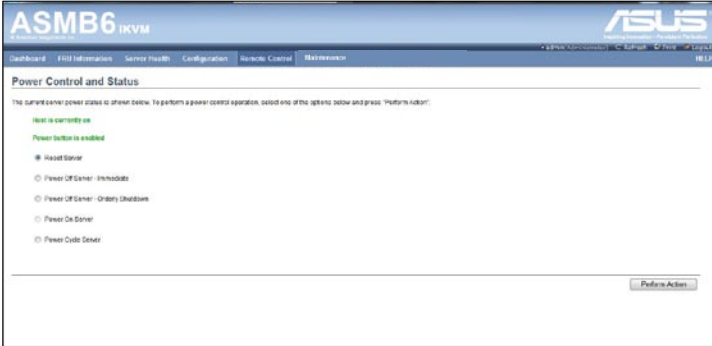
4.5.3 Chassis Identify Command

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

4.5.4 Power Button

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

4.6   Maintenance

This section allows you to perform the firmware update for the remote server. You can also use **Restore Factory Defaults** to reset system settings and use **System Admnistrator** to enable or disable access and change the password for the administrator account.

4.6.1   Firmware Update

This section allows you to enter the update mode, and update the firmware of ASMB6. Please note that after entering update mode widgets, other web pages and services will not work. All oopen widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will reset.
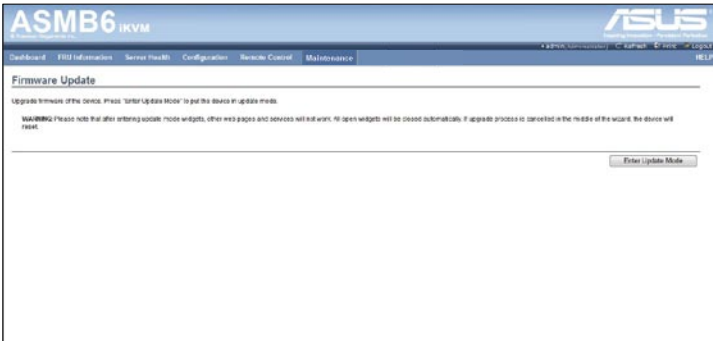
4.6.2 Restore Factory Default

This section allows you to restore all settings to factory default. Please click the **Restore Factory** to reset all settings.
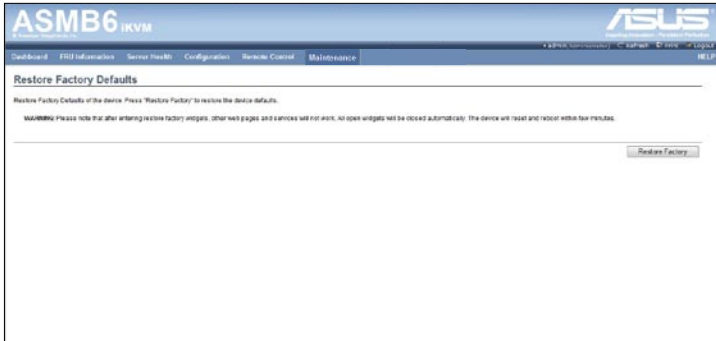
The Appendix shows the location of the
LAN ports for server management and BMC
connector on server motherboards. This
section also presents common problems that
you may encounter when installing or using
the server management board.

Reference
information

A

A.1   BMC connector

The ASUS server motherboards that support the ASMB6-iKVM comes with a Baseboard Management Controller (BMC) connector.

Refer to the illustration below to locate the BMC connector on different server motherboards.
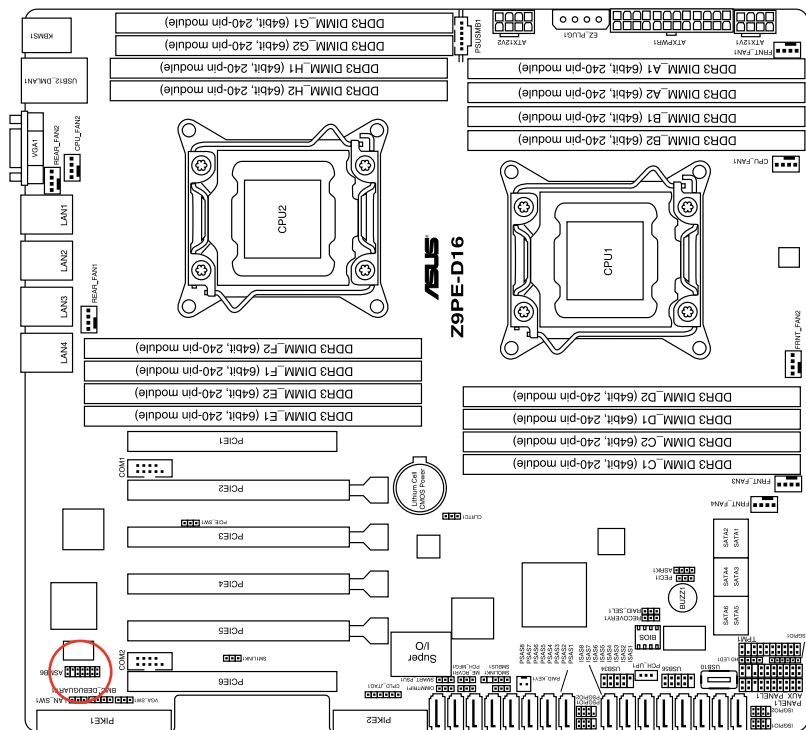
A.2   LAN ports for server management

The ASUS server motherboards that support the ASMB6-iKVM comes with three LAN (RJ-45) ports: one for network connection and the other two for server management. For easy identification, the LAN ports for server management are LAN1 and DM_LAN1 ports. You must use the LAN1 and DM_LAN1 ports for server management to connect the remote server to the local/central host (direct LAN connection) or to the network hub or router.

Refer to the illustration below to identify the LAN1 and DM_LAN1 ports for server management on some server motherboards.
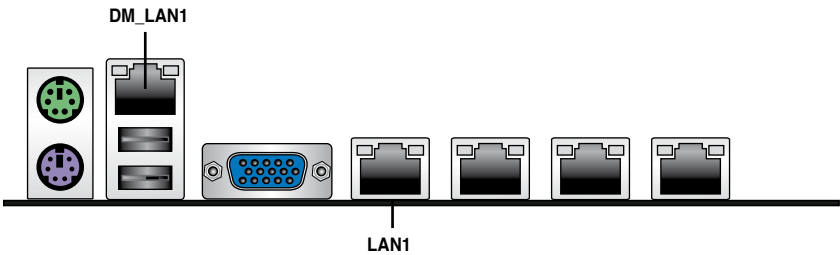
You may refer to motherboard manual for the location of LAN1 and DM_LAN1 ports.

A.3   Troubleshooting

This troubleshooting guide provides answers to some common problems that you may encounter while installing and/or using ASUS ASMB6-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 ASMB6-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.
ASMB6-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.

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
0xD2	CPU1_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_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: DMM_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
0xD4	CPU2_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DMM_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

Backplane HD

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

Power Supply

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

Hardware Monitor

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x31	CPU1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x32	CPU2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCC	TR1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCD	TR2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x34	VCORE1	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x35	VCORE2	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x36	+3.3V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x37	+5V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x38	+12V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
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

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
0x42	P1DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	+1.5V (For Intel UP platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x43	P2DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x44	P1_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x45	P2_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x46	P1_VDDNB (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x47	+1.8V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x48	+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x49	+1.1V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x4A	VTT (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0xA0	CPU_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low

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