Remote Management LAN Card

IPMI expansion card

User Guide

E19387
First Edition
February 2022

Contents

Safety information v
About this guide vi

Chapter 1: Product Introduction

1.1 Welcome! 1-2
1.2 Package contents 1-2
1.3 IPMI Expansion Card specifications summary 1-3
1.4 IPMI Expansion Card Overview 1-4
1.5 Features 1-6
1.6 System requirements 1-9
1.7 Jumper configurations 1-10
1.8 Network setup 1-11

Chapter 2: Installation Information

2.1 Before you proceed 2-2
2.2 Hardware installation 2-2
2.3 BIOS configuration 2-7
2.3.1 Running the BIOS BMC configuration 2-7
2.3.2 Server Mgmt menu 2-7
2.3.3 System Event Log 2-8
2.3.4 BMC network configuration 2-9
2.3.5 View System Event Log 2-11
2.4 BMC management with IPMITool 2-12

Chapter 3: Web-based User Interface

3.1 Web-based user interface 3-2
3.1.1 Logging in the utility 3-2
3.1.2 Using the utility 3-3
3.1.3 BIOS settings 3-4
3.2 Dashboard 3-5
3.3 Sensor 3-6
3.3.1 Sensor detail 3-7
3.4 System Inventory 3-9
3.5 FRU Information 3-10
3.6 Logs & Reports 3-11
3.6.1 IPMI Event Log 3-12
3.6.2 System Log 3-14
3.6.3 Audit Log 3-15
3.6.4 Video Log 3-16

Contents

3.7 Settings 3-17

3.7.1 Date & Time 3-17
3.7.2 External User Services 3-19
3.7.3 KVM Mouse Setting 3-24
3.7.4 Log Settings 3-24
3.7.5 Manage Licenses 3-26
3.7.6 Media Redirection Settings 3-26
3.7.7 Network Settings 3-29
3.7.8 PAM Order Settings 3-33
3.7.9 Platform Event Filters 3-34
3.7.10 Services 3-40
3.7.11 SMTP Settings 3-42
3.7.12 SSL Settings 3-46
3.7.13 System Firewall 3-49
3.7.14 User Management 3-53
3.7.15 Video Recording 3-56
3.7.16 Fan Control 3-59
3.7.17 PSU Redundancy 3-60

3.8 Remote Control 3-61
3.9 Image Redirection 3-65
3.10 Power Control 3-66
3.11 Locator LED 3-67
3.12 Maintenance 3-68

Appendix

A.1 IPMITool help commands A-2
A.2 Common IPMITool commands A-3
A.3 Troubleshooting A-6
Notices A-9
Warranty A-13
ASUS contact information A-15
Service and Support A-15

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 IPMI expansion card features, system requirements, and network settings.

- **Chapter 2: Installation Information**

  This chapter provides instructions on how to install the IPMI expansion card to the client device motherboard and BIOS BMC settings.

- **Chapter 3: Web-based User Interface**

  This chapter tells you how to use the web-based user interface to manage and configure the client device with an IPMI expansion card installed.

- **Appendix**

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

Where to find more information

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

1. **ASUS websites**

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

2. **Optional documentation**

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

Conventions used in this guide

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

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

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

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

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

Typography

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

1 Product Introduction

This chapter describes the IPMI expansion card features, system requirements, and network settings.

1.1 Welcome!

Thank you for buying an ASUS IPMI Expansion Card!

The ASUS IPMI Expansion Card can be installed to a non-server ASUS motherboard, and allows you to monitor your remote device in real-time when installed to the ASUS motherboard of your remote device. The solution allows you to reduce IT management costs and increase the productivity. Compatibility with IPMI (Intelligent Platform Management Interface) 2.0 will allow you to monitor, control, and manage a remote client device from the local or central server in your local area network (LAN).

Before you start installing the IPMI Expansion Card, check the items in your package with the list below.

1.2 Package contents

Check your server management board package for the following items.

- 1 x IPMI Expansion Card
- 1 x BMC cable
- 1 x SPI cable
- 1 x Power On/Off cable
- 1 x Reset cable
- 1 x USB 2.0 cable
- 1 x IPMI TPM adapter
- 1 x Quick start guide

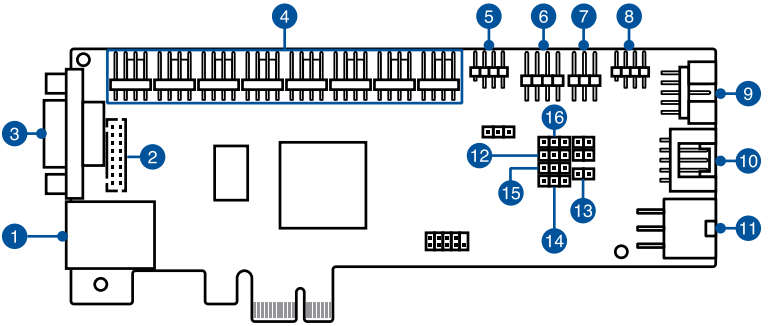
If any of the above items is damaged or missing, contact your retailer.

1.3 IPMI Expansion Card specifications summary

Chipset	ASPEED VIDEO PROCESSOR AST2600A3-GP
Onboard RAM	System: 384MB Video: 64MB
Onboard ROM	64MB
Interface	PCIe 3.0 x1 interface
VGA	1 x D-sub supports max. resolution 1920 x 1200 @ 60Hz
External connectors	1 x D-Sub 1 x LAN (RJ45) port
Internal connectors	8 x fan headers 1 x 6-pin PSU connector 1 x BMC header 1 x LAN IP mode switch jumper 1 x SMART_PSU switch jumper 1 x SPI header 1 x PM_BUS header 1 x USB 2.0 connector 1 x VGA header 1 x Panel header(links to PWR/RST header of motherboard and chassis) 3 x T-sensor headers 1 x BMC switch jumper 1 x VGA switch jumper 1 x LOC switch jumper 1 x BMC Indicator LED
Watchdog	32-bit Watchdog Timer
Main Features	- Compatible and supports IPMI 2.0 and supports KVM over LAN - Supports Web UI (Remote management) - Supports Virtual media - Supports Network Bonding
Operating System	Windows® 10 - 64 bit, Linux OS including Cent OS, Redhat, and Ubuntu
Dimensions	6.4 inch x 2.7 inch (162mm x 68.95mm)

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

1.4 IPMI Expansion Card Overview



1. **RTL8211F-CG 1G LAN connector:** Connects directly to the central server or to a router/hub using a LAN cable.
2. **Onboard VGA header:** Connects to front VGA using an adapter cable.
3. **VGA connector:** Connects to a display using a VGA cable.
4. **Fan headers 1-8:** Connects to fans to view fan information and management.

To use the CHA FAN sensor and control function, ensure the fans are connected to the **Fan headers 1-8**, and the **6-pin PSU connector** is connected to a power supply.

5. **SPI header:** Connects to IPMI TPM adapter with cable for burning BIOS.

- Client device motherboard model needs to support this function.
- To use the BIOS burning function, ensure the **SPI header** is connected to the IPMI TPM header on the motherboard.

6. **PANEL header:** Connects to motherboard and chassis PANEL to control power/reset functions.

To use the power on/off and reset function, ensure the **PANEL header** is connected to the motherboard and the chassis panel.

7. **T_SENSOR headers 1-3:** Used for temperature measuring.

To use the TR temperature sensor function, ensure the **T_SENSOR headers 1-3** are connected to the motherboard.

8. **BMC header:** Connects to motherboard BMC header for real-time sensor monitoring.

To use the real-time sensor monitoring function (if supported), ensure the **BMC header** is connected to the BMC header on the motherboard.

9 **USB header:** Connects to motherboard USB 2.0 front header for data transfer and KVM keyboard/mouse remote control.

To use the keyboard and mouse function for KVM remote control, ensure the **USB header** is connected to the USB 2.0 connector on the motherboard.

10 **PSU PM_BUS header:** Connects to power supply for PSU detection.

- Power supply needs to support PSU function.
- To use the PSU sensor and power redundancy settings function, ensure the power supply is connected to the **PSU PM_BUS header**, and the **SMART_PSU switch jumper** is set to **Enable**.

11 **6-pin PSU connector:** Connects to PCIE power +12V for fan power.

To use the CHA FAN sensor and control function, ensure the fans are connected to the **Fan headers 1-8**, and the **6-pin PSU connector** is connected to a power supply.

12 **VGA switch jumper:** Used to turn on/off the display; default set to On.

13 **LOC switch jumper:** Used to toggle heartbeat LED lit up/breathing.

14 **BMC switch jumper:** Used to turn on/off the BMC card.

15 **SMART_PSU switch jumper:** Used for controlling alert.

- Power supply needs to support PSU function.
- To use the PSU sensor and power redundancy settings function, ensure the power supply is connected to the **PSU PM_BUS header**, and the **SMART_PSU switch jumper** is set to **Enable**.

16 **LAN IP mode switch jumper:** Used to control LAN IP - Dynamic/Fixed(10.10.10.10).

1.5 Features

1. IPMI 2.0

- LAN interface (supports RMCP+)
- Serial Over LAN (SOL)
- Universal Series Bus (USB)
- IPMI Serial Interface
- Field Replaceable Unit (FRU)
- IPMI Sensor
- IPMI Event Log
- Platform Event Trap (PET)
- Email Alert
- Internet Protocol version 6 (IPv6)
- Data Center Manageability Interface (DCMI)
- IPMI command to read BIOS Post Code
- Platform Environment Control Interface (PECI) over IPMI
- Power Control
- FW Maintenance
- BMC Syslog & Audit
- Remote syslog
- SOLSSH
- Backup-Restore BMC Configuration
- BIOS Configuration
- BIOS Update
- ASUS Thermal Radar
- BMC Secured Boot

2. KVM Support

- JViewer support
- HML5Viewer Support
- Jviewer Standalone Application
- Physical KeyBoard Language Selection support
- Keyboard LED sync with Client Keyboard LED status
- Keyboard LED sync with Host Keyboard LED status

3. Remote Media Support

- Remote CD/DVD Device support
- Remote Hard disk server support
- Remote Media multiple image redirection
- Multiple Remote Media CD redirection
- Multiple Remote Media Hard disk redirection

4. **Web support**
   - HTML5 based WebUI Support
   - Dashboard
   - Sensor
   - Sensor Detail
   - Sensor Threshold Setting
   - System Inventory
   - FRU Information
   - Log & Report
   - IPMI Log
   - System Log
   - Audit Log
   - Video Log
   - Setting
   - Date & Time
   - Active Directory
   - Lightweight Directory Access Protocol (LDAP)
   - Radius
   - KVM Mouse
   - Log
   - Media Redirection
   - Network
   - Network Bond
   - Domain Name Server (DNS)
   - Platform Event Filter (PEF)
   - Services
   - Simple Mail Transfer Protocol (SMTP)
   - Secure Sockets Layer (SSL) protocol provides secure encryption schemes, and supports security mechanisms such as SSL (Secure Sockets Layer) and SSH (Secure Shell)
   - Provides the user with support of 2 or more simultaneous and synchronized remote control graphic user interface control panels, allowing different administrators to work on the same issues from different places
   - Allows remote control and monitoring through the Internet
   - System Firewall
   - User Management
   - Video Recording
   - Web Server Instances
   - FAN Control (ASUS Thermal Radar)
   - Remote Control
   - iKVM

- HTML5 based SOL
- Image Redirection
- Power Control
- Maintenance
- Configuration Backup & Restore
- Firmware Update
- Restore Factory Defaults
- Sign Out
- RedFish API Support

5. Network Support

- IPv4 support
- IPv6 support
- Bonding Support
- Fully Qualified Domain Name (FQDN) Support
- Network Time Protocol (NTP) Server support
- Advanced IP Routing
- Set default Network to DHCP
- Dynamic DNS Support
- Ethernet Over USB Support
- System Firewall Support
- Timezone Configuration Support
- Active Directory Authentication support
- LDAP authentication support
- PAM Reorder support
- Radius Authentication support
- SNMP Support
- SNMP trap v2c/v3 alerting at run time
  - CPU, Memory warning
  - Temperature, Fan and PSU

6. Device Support

- I2C Device Support
- ADC Device Support
- eSPI Device Support
- GPIO Device Support
- Host SPI Flash Device Support
- Netmon Device Support
- PECI Device Support
- PWMTACH Device Support

- BMC Reset Driver Support
- UART Route Support
- USB Device Support
- Video Device Support
- Watchdog Device Support

7. Firmware Update

- Supports firmware update for onboard management processor
- Supports firmware update for motherboard BIOS firmware

8. Notification

- Self diagnosing LED indicators to display hardware status
- Supports Web based or GUI remote management interfaces for damage monitoring of CPU, RAM, storage device, etc. (*requires support from client device BIOS)

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

1.6 System requirements

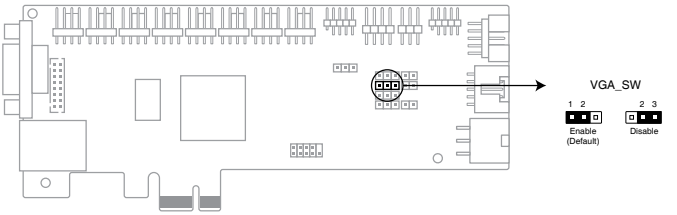
Before you install the IPMI expansion card, check if the client device meets the following requirements:

- ASUS motherboard that supports IPMI expansion card*
- LAN (RJ-45) port for server management
- Firefox (Windows and Linux), Chrome (Windows and Linux), Edge-Chromium Version (Windows)

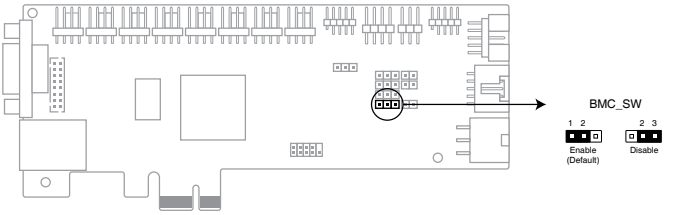
* Visit www.asus.com for an updated list of motherboards that support the IPMI expansion card.

1.7 Jumper configurations

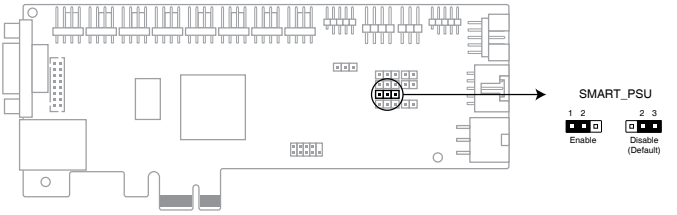
VGA switch jumper



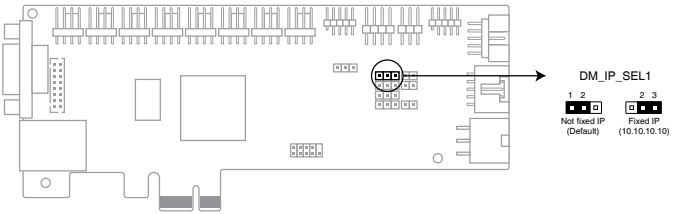
BMC switch jumper



SMART_PSU switch jumper



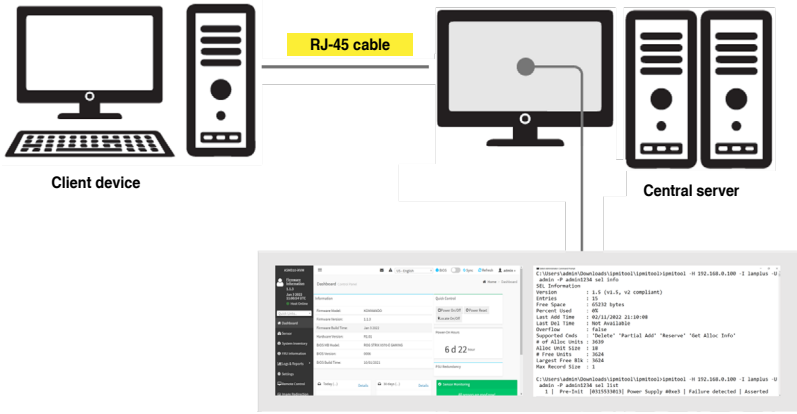
LAN IP mode switch jumper



1.8 Network setup

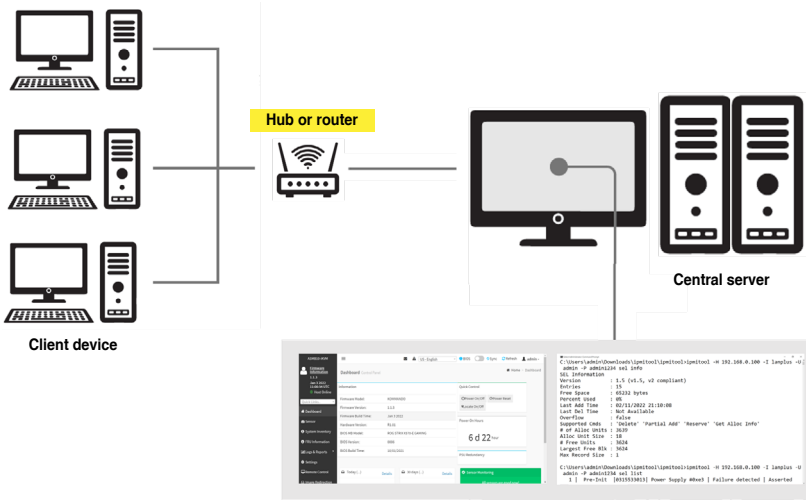
The IPMI expansion card installed on the client device motherboard connects to a local/central server via direct LAN connection or through a network hub. Below are the supported network management configurations.

Direct LAN connection



Remote console with web-based browser or IPMITool

LAN connection through a network hub



Remote console with web-based browser or IPMITool

2 Installation Information

This chapter provides instructions on how to install the IPMI expansion card to the client device motherboard and BIOS BMC settings.

2.1 Before you proceed

Take note of the following precautions before you install the IPMI expansion card to the client device's motherboard.

- 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.

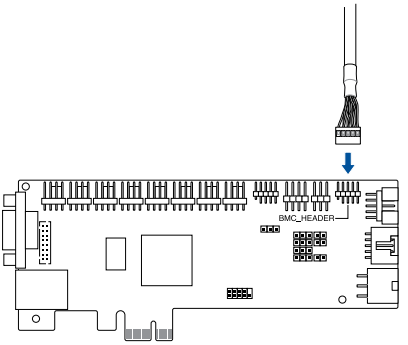
2.2 Hardware installation

To install the IPMI expansion card to the client device's motherboard:

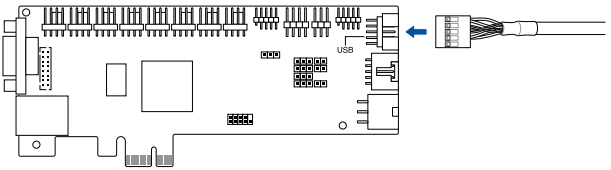
The cables connectors are notched to fit in only one orientation. Do not force the cable connectors onto the board headers/connectors in the incorrect orientation.

1. (on selected models) Connect the BMC cable to the BMC header (**BMC_HEADER**) on the IPMI expansion card and the BMC header on your motherboard.

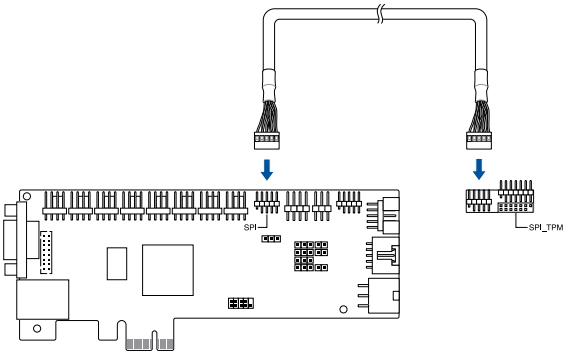
Only connect this header if your motherboard features a **BMC_HEADER**, please refer to the user manual that came with your motherboard package for more details.



2. To supply the IPMI expansion card with power, connect the USB 2.0 cable to the USB connector (**USB**) on the IPMI expansion card and the USB 2.0 connector on your motherboard.



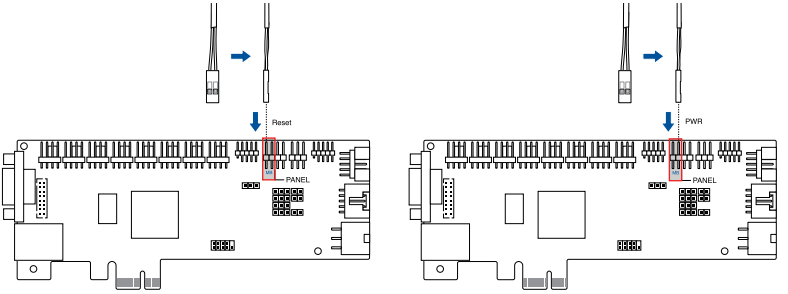
3. For SPI functions, connect the SPI cable to the SPI TPM header (**SPI**) on the IPMI expansion card and the header on the IPMI TPM adapter. Connect the IPMI TPM adapter to the SPI TPM header on your motherboard.



4. Connect the Power On/Off cable and Reset cables to the MB pins on the Panel header (**PANEL**) on the IPMI expansion card then connect them to the Panel header on the motherboard. Ensure the cables are connected such that the red cable is closest to the PCB.

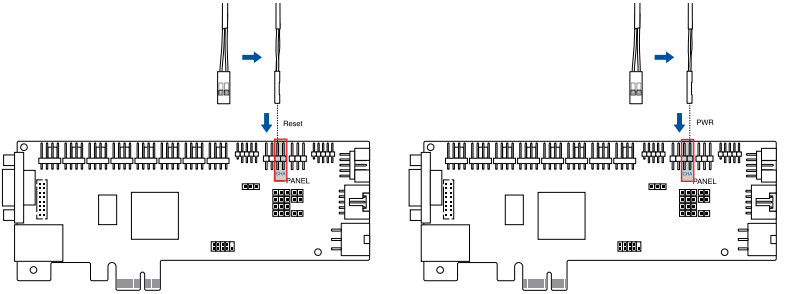
The Power On/Off cable and Reset cable are connected in opposite orientations when connecting them to the Panel header on your motherboard. For more information on the pin definitions of the Panel header on your motherboard, please refer to your motherboard's user guide.

MB pins

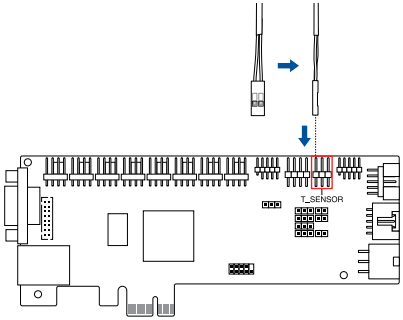


5. Connect the Power On/Off cable and Reset cables from the chassis to the CHA pins on the Panel header. Ensure the cables are connected such that the red cable is closest to the PCB.

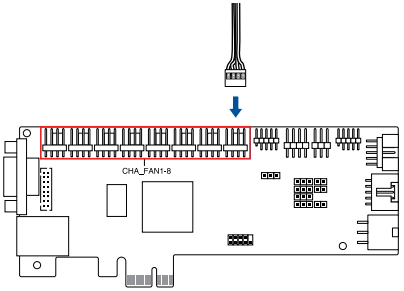
CHA pins



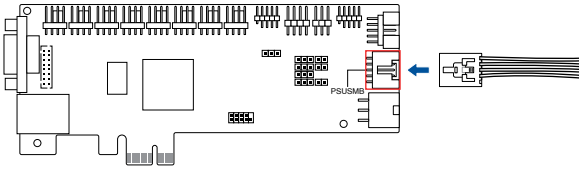
6. This board features three (3) T-Sensor headers (**T_SENSOR**) which allow you to connect T-sensor cables for temperature monitoring functions.



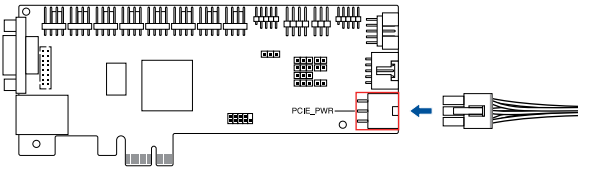
7. Connect the fans to the fan headers (**CHA_FAN1-8**) to monitor the fans.



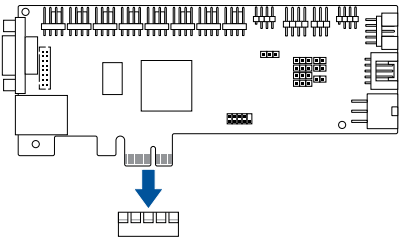
8. Connect the PMBus connector from the PSU to the PSU PM_BUS header (**PSUSMB**) for monitoring information on the PSU such as voltage, current, and temperature.



9. Connect the 6-pin PCIE power connector from the PSU to the 6-pin PSU connector (**PCIE_PWR**).

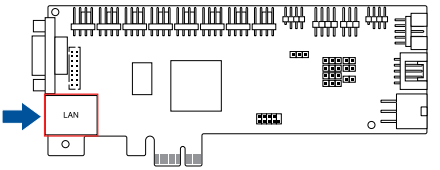


10. Insert the IPMI expansion card to a PCIe slot on your motherboard.



11. Connect a LAN cable to the LAN port for remote management.

- 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.



12. Check that everything is properly connected, then plug the power cable of the power supply to a grounded wall socket.

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

2.3 BIOS configuration

Before using the BMC remote management controller, ensure to download the BIOS version which supports the IPMI expansion card for the client device motherboard. Follow the steps below to configure the BIOS settings of the client device after updating the BIOS.

- Update the motherboard BIOS file following the instructions in the motherboard 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.

2.3.1 Running the BIOS BMC configuration

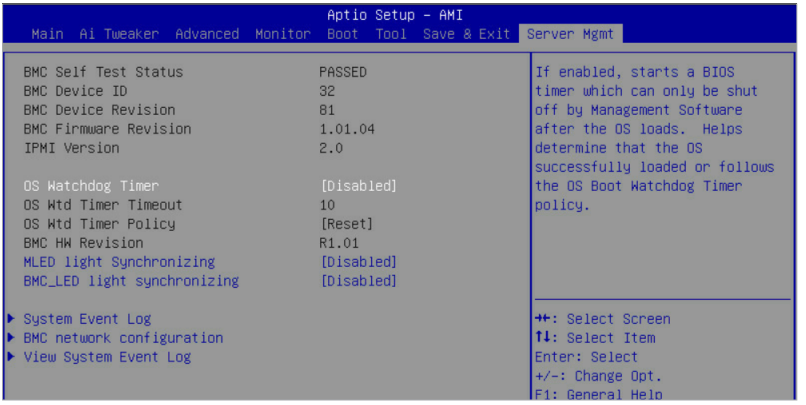
To configure the BMC in the BIOS:

1. Restart the client device, 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.

2.3.2 Server Mgmt menu

The Server Management menu displays the server management status and allows you to change the settings.

Not all BIOS items are mentioned in this section as they may vary between system models. Only the BMC related items are mentioned.



OS Watchdog Timer

This item allows you to start a BIOS timer which can only be shut off by Intel Management Software after the OS loads.
Configuration options: [Disabled] [Enabled]

The following items is configurable only when the **OS Watchdog Timer** is set to **[Enabled]**.

OS Wtd Timer Timeout

Allows you to configure the length fo the OS Boot Watchdog Timer.
Configuration options: [5 minutes] [10 minutes] [15 minutes] [20 minutes]

OS Wtd Timer Policy

This item allows you to configure the how the system should respond if the OS Boot Watch Timer expires.
Configuration options: [Do Nothing] [Reset] [Power Down]

MLED light Synchronizing

Allows you to synchronize the left LAN port LED of the IPMI Expansion card with the Message LED.
Configuration options: [Disabled] [Enabled]

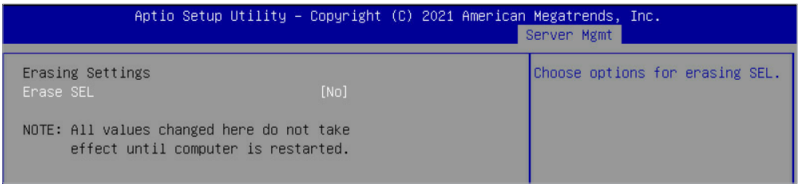
BMC_LED light synchronizing

Allows you to synchronize the right LAN port LED of the IPMI Expansion card with the BMC_ LED.
Configuration options: [Disabled] [Enabled]

2.3.3 System Event Log

Allows you to change the SEL event log configuration.

All values changed here do not take effect until computer is restarted.

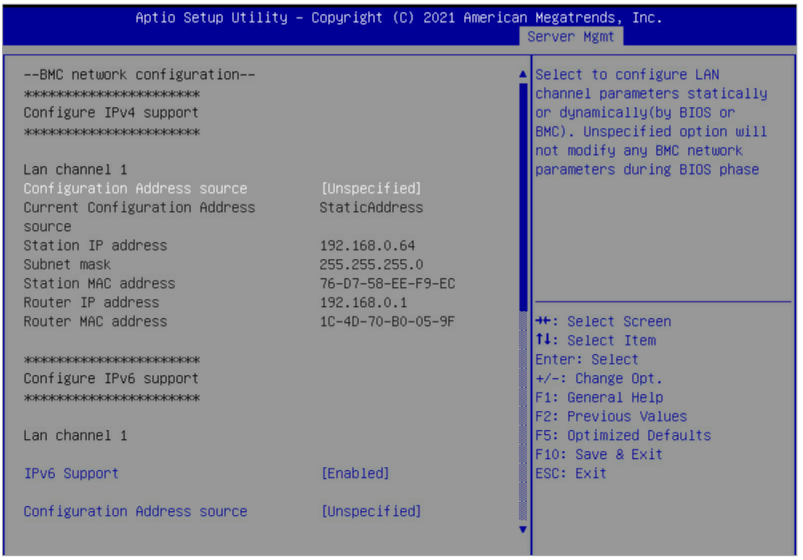


Erase SEL

Allows you to choose options for erasing SEL.
Configuration options: [No] [Yes, On next reset] [Yes, On every reset]

2.3.4 BMC network configuration

Allows you to set the BMC LAN parameter settings.



Configure IPV4 support

Lan channel 1

Configuration Address source

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Unspecified]** option will not modify any BMC network parameters during BIOS phase.
Configuration options: [Unspecified] [Static] [DynamicBmcDhcp]

The following items are available only when **Configuration Address source** is set to **[Static]**.

Station IP address

Allows you to set the station IP address.

Subnet mask

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

Router IP Address

Allows you to set the router IP address.

Router MAC Address

Allows you to set the router MAC address.

Configure IPV6 support

Lan channel 1

IPV6 support

Allows you to enable or disable IPV6 support.
Configuration options: [Enabled] [Disabled]

The following items appear only when **IPV6 support** is set to **[Enabled]**.

Configuration Address source

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Unspecified]** option will not modify any BMC network parameters during BIOS phase.
Configuration options: [Unspecified] [Static] [DynamicBmcDhcp]

The following items are available only when **Configuration Address source** is set to **[Static]**.

Station IPV6 address

Allows you to set the station IPV6 address.

Prefix Length

Allows you to set the prefix length (maximum of Prefix Length is 128).

Configuration Router Lan1 Address source

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Unspecified]** option will not modify any BMC network parameters during BIOS phase.
Configuration options: [Unspecified] [Static] [DynamicBmcDhcp]

The following items are available only when **Configuration Router Lan1 Address source** is set to **[Static]**.

IPV6 Router1 IP Address

Allows you to set the IPV6 Router1 IP address.

IPV6 Router1 Prefix Length

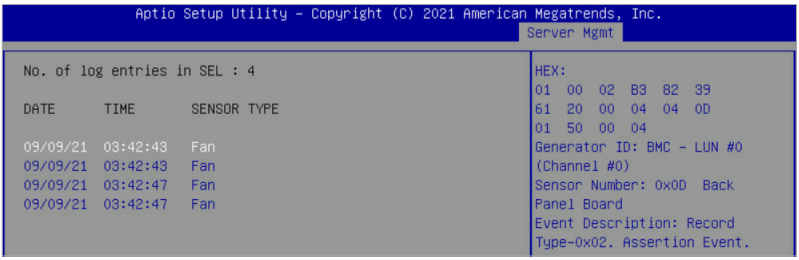
Allows you to set the IPV6 router prefix length (maximum of IPV6 Router Prefix Length is 128).

IPV6 Router1 Prefix Value

Allows you to change the IPV6 router prefix value.

2.3.5 View System Event Log

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



2.4 BMC management with IPMITool

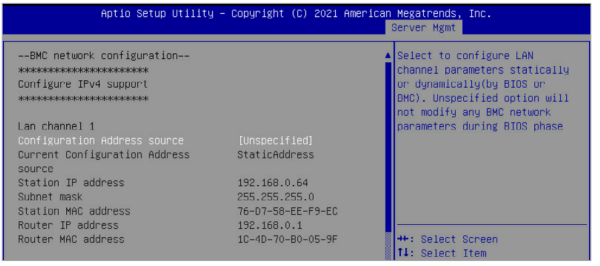
You can download and use IPMITool to use a console to configure the BMC settings, manage, and use functions of the remote device, such as IP address configuration, view details on the sensors, manage users, view the power status of the remote device, or manage the power controls.

```
C:\ipmitool>ipmitool -I lanplus -H 192.168.0.64 -U admin -P admin1234 sensor
CPU Temperature  | 31.000     | degrees C  | ok  | 0.000    | 0.000    | 0.000    | 84.000   | 89.000   | 95.000
MB Temperature   | 34.000     | degrees C  | ok  | 0.000    | 0.000    | 0.000    | 60.000   | 70.000   | 95.000
TR1 Temperature  | na         | degrees C  | na  | 0.000    | 0.000    | 0.000    | 37.000   | 40.000   | 60.000
TR2 Temperature  | na         | degrees C  | na  | 0.000    | 0.000    | 0.000    | 90.000   | 95.000   | 100.000
TR3 Temperature  | na         | degrees C  | na  | 0.000    | 0.000    | 0.000    | 90.000   | 95.000   | 100.000
+12V             | 12.000     | Volts      | ok  | 9.600    | 10.200   | 10.800   | 13.200   | 13.800   | 14.400
+3.3V            | 3.312      | Volts      | ok  | 2.640    | 2.800    | 2.976    | 3.632    | 3.792    | 3.968
+3.3VSB          | 3.360      | Volts      | ok  | 2.640    | 2.800    | 2.976    | 3.632    | 3.792    | 3.968
+5VSB_USBKB      | 4.944      | Volts      | ok  | 4.008    | 4.248    | 4.512    | 5.496    | 5.760    | 6.000
CPU_FAN          | 1400.000   | RPM        | ok  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
OPT_FAN          | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN1         | 3100.000   | RPM        | ok  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN2         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN3         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN4         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN5         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN6         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN7         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
CHA_FAN8         | na         |            | na  | 0.000    | 400.000  | 400.000  | 22500.000| 23700.000| 25000.000
PSU1 Power In    | na         | Watts      | na  | 0.000    | 0.000    | 0.000    | 1360.000 | 1600.000 | 1840.000
PSU2 Power In    | na         | Watts      | na  | 0.000    | 0.000    | 0.000    | 1360.000 | 1600.000 | 1840.000
PSU1 Power Out   | na         | Watts      | na  | 0.000    | 0.000    | 0.000    | 1360.000 | 1600.000 | 1840.000
PSU2 Power Out   | na         | Watts      | na  | 0.000    | 0.000    | 0.000    | 1360.000 | 1600.000 | 1840.000
PSU1 Over Temp   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU2 Over Temp   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU1 AC Lost     | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU2 AC Lost     | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU1 Slow FAN1   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU2 Slow FAN1   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU1 PWR Detect  | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU2 PWR Detect  | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU1 Over Curr   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
PSU2 Over Curr   | na         | discrete   | na  | na       | na       | na       | na       | na       | na
VERSION_ERR      | 0x0        | discrete   | 0x0080| na     | na       | na       | na       | na       | na
Watchdog2        | 0x0        | discrete   | 0x0080| na     | na       | na       | na       | na       | na
```

- For a list of IPMITool commands, please refer to the **Appendix**.
- When using IPMITool to execute a command, the command must include the client device's BMC IP address. To view the BMC IP address:

  a. Restart the client device, then enter the BIOS setup.

  b. Go to the **Server Mgmt** menu, then select the **BMC network configuration** sub-menu. The BMC IP address can be found in the BMC network configuration sub-menu.



3

Web-based User Interface

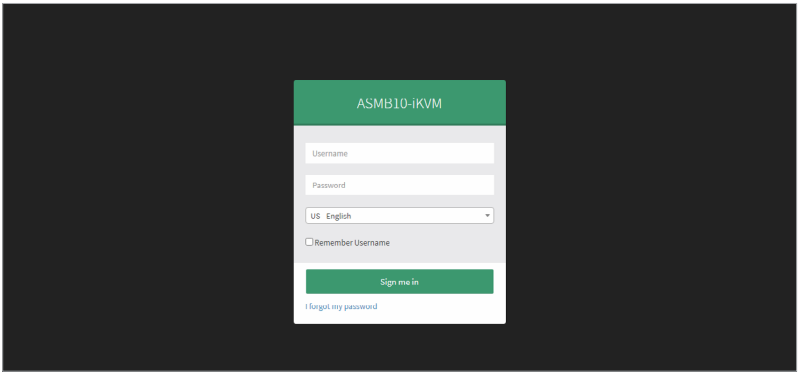
This chapter tells you how to use the web-based user interface to manage and configure the client device with an IPMI expansion card installed.

3.1 Web-based user interface

The web-based user interface allows you to easily monitor the client device's hardware information including temperatures, fan rotations, voltages, and power. By opening the GUI in a browser you can manage the client device remotely, even when there is no OS installed on the client device. This application also lets you instantly power on/off or reset the remote device.

3.1.1 Logging in the utility

1. Open the web browser and type in the same IP address as the one in the remote device.
2. The below screen appears. If you are logging in for the first time, enter the default user name (admin) and password (admin). Then click **Sign me in**.

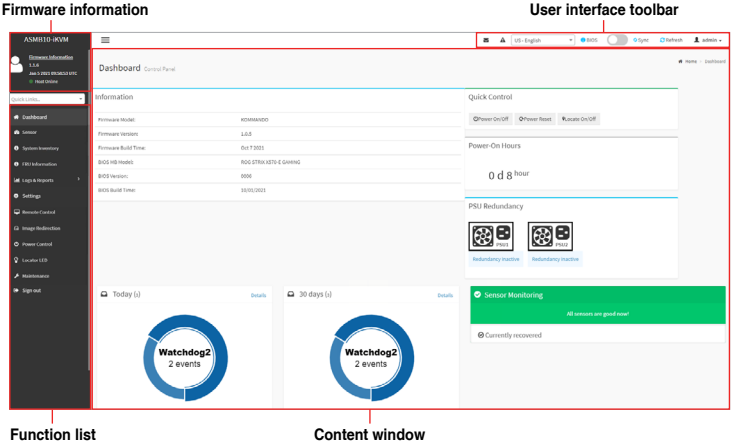


3. You will be prompted to change your password after logging in for the first time. Please ensure that you change the password to a new password.
4. After updating the password, please log in again using the new password.

- Ensure the administrator's device and the remote client device are in the same subnetwork and have a stable connection before using the web-based user interface.
- You can select the language (**English**, **Traditional Chinese**, **Simplified Chinese**) for the web-based user interface in the language drop down menu.
- Checking the **Remember Username** item will auto fill the username entered the next time you wish to log in to the web--based user interface..

3.1.2 Using the utility

The web-based graphics user interface displays when you login in the utility successfully. Click on a function from the list on the left hand side to start using its specific functions.



Firmware information		Displays the firmware version, time created, and connection information of the remote device.
Quick links		Quick access to a function entered or select from previously searched results.
User interface toolbar	**Messages**	Displays all received messages.
	Notifications	Displays all received notifications.
	Change Languages	Allows you to switch between languages (**English**, **Traditional Chinese**, **Simplified Chinese**).
	BIOS Settings	Opens a new window or a popup window to configure BIOS settings.
	Sync	Enable or disable synchronization with the latest hardware sensor and event log updates.
	Refresh	Reloads the current page.
	Profile	Log out the currently logged in profile, or view or manage the profile.
Function list		View the device information or use remote device function.
Content window		Displays all information related to the function selected.

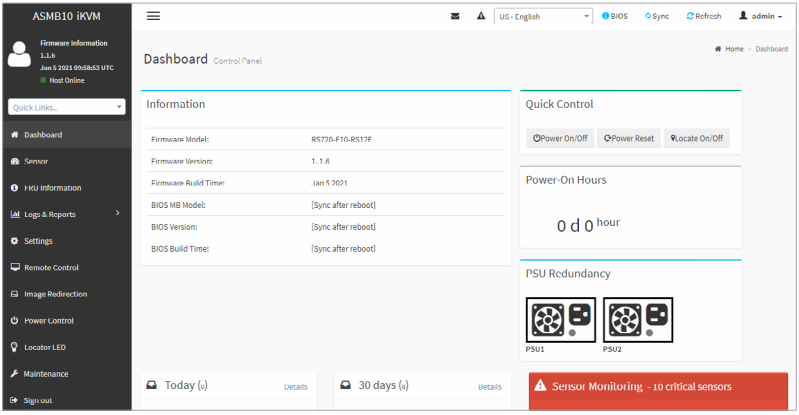
3.1.3 BIOS settings

Set the BIOS settings for the remote device.

1. Click on **BIOS** from the user interface toolbar located in the top right of the main page.
2. Enter the user account name and password.
3. You can begin configuring or viewing the BIOS settings of the remote device once you have successfully logged in.

3.2 Dashboard

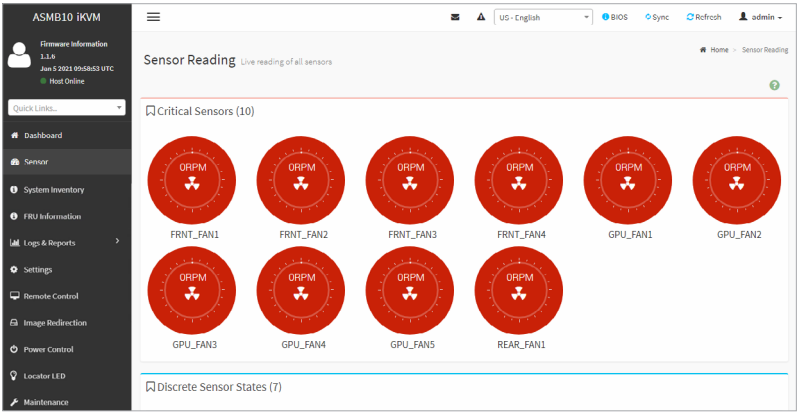
The dashboard gives you a quick overview of the system status, quick control options, power-on hours, power redundancy, sensors, messages, and logs. Click or hover your mouse over an item to see more details. Scroll down to view more items.



Information	• Firmware Model • Firmware Version • Firmware Build Time • Hardware Version • BIOS MB Model • BIOS Version • BIOS Build Time
Quick Control	• Power On / Off • Power Reset • Locate On / Off
Power-On Hours	Displays the amount of hours the remote device has been powered on for.
PSU Redundancy	Displays the PSU redundancy status.
Sensor Monitoring	Displays the sensor monitoring status.
Event Log	• Displays the event log records for today. • Displays the event log records for the past 30 days.

3.3 Sensor

The Sensor Readings page displays live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior. This page will automatically refresh itself with data from the database. Please note that there may be some delay when retrieving live data. Scroll down to view more items.



The Sensor Readings page consists of different types of sensors and sensor states:

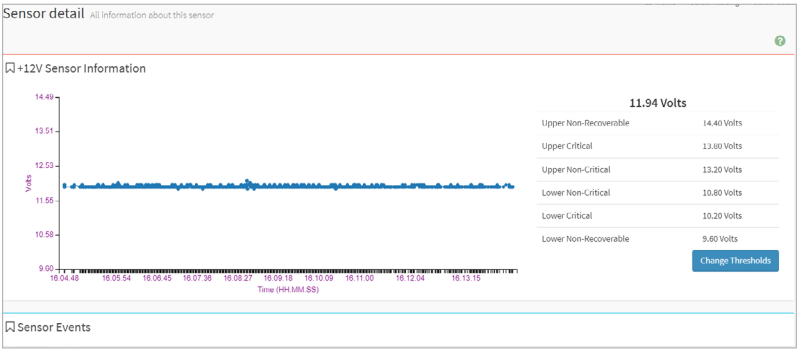
Critical Sensors	Displays all sensors which are in critical state, including the name, status and current reading.
Discrete Sensors States	Displays all discrete sensors, including the names and states.
Normal Sensors	Displays all normal sensors, including the names, current readings, and behavior.
Disabled Sensors	Displays all disabled sensors.

- Click on a sensor to view the sensor information such as threshold value and graphical representations of all associated events.
- Selecting a sensor from the Normal Sensors section will display a Live Widget which will display its behavior over time.
- Under certain platforms, some sensors can only support one-time updates and will not update over time.
- The fan's UNC / UC / UNR will not create an event log when the rotation speed exceeds the upper threshold.
- The temperature's LNR / LC / LNC will not create an event log when the temperature drops below the lower threshold.
- You can view the UNR / LNR values of the sensors, but no event log will be created if the sensor's UNR exceeds the upper threshold or if the sensor's LNR drops below the lower threshold.
- To use the CHA FAN sensor and control function, ensure the fans are connected to the **Fan headers 1-8**, and the **6-pin PSU connector** is connected to a power supply.

- To use the PSU sensor and power redundancy settings function, ensure the power supply is connected to the **PSU PM_BUS header**, and the **SMART_PSU switch jumper** is set to **Enable**.
- To use the TR temperature sensor function, ensure the **T_SENSOR headers 1-3** are connected to the motherboard.
- To use the real-time sensor monitoring function (if supported), ensure the **BMC header** is connected to the BMC header on the motherboard.

3.3.1 Sensor detail

The Sensor detail page provides information on a selected sensor, and also displays the readings on a dynamic graph. You can configure the sensor threshold value or display all the events of the sensor in chronological order.



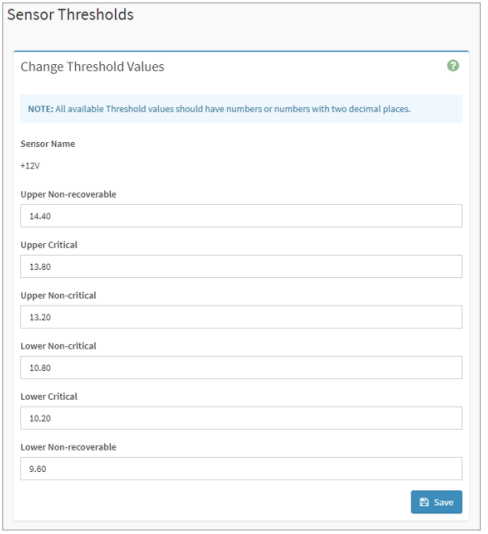
Changing the Threshold value

You can change the threshold value according to your needs. To change the threshold value:

1. Click **Change Thresholds** on the Sensor Details page.

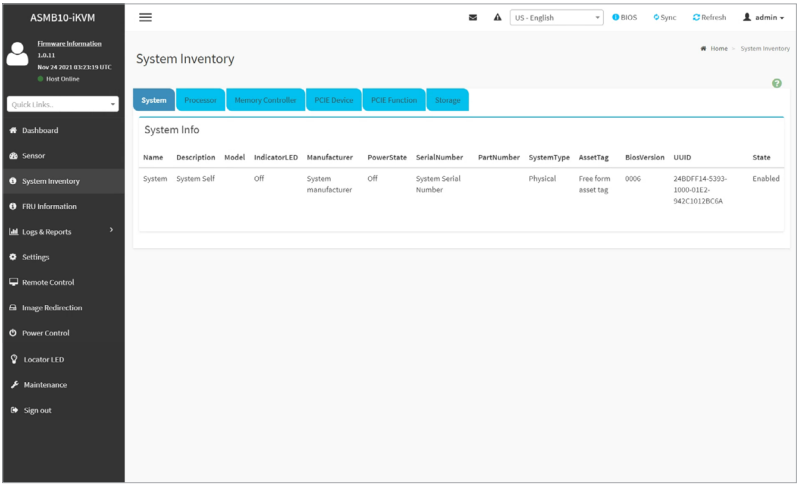
The **Change Thresholds** button will only be enabled and available for administrator or operator privilege users. For other users, this button will be disabled.

2. Adjust the threshold values, then click on **Save**.



3.4 System Inventory

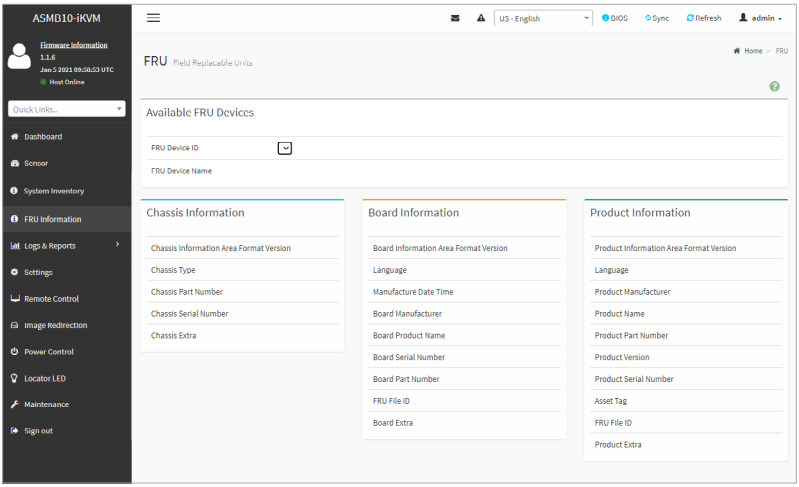
This page displays Inventory Information of the remote device.



System	Displays information on the remote device: system name, description, model, indicator LED, manufacturer, power state, serial number, part number, system type, asset tag, BIOS version, UUID, and state.
Processor	Displays the processor information of the remote device: ID, name, manufacturer, brand name, state, Max speed (MHz), model, processor architecture, processor type, socket, total cores, and TDP Watts.
Memory Controller	Displays the memory controller information of the remote device: ID, name, state, operating speed (MHz), capacity (MiB), memory type, manufacturer, part number, serial number, description, allowed spped (MHz), and device locator.
PCIE Device	Displays the PCIe device information of the remote device: name, description, manufacturer, asset tag, device type, firmware version, and state.
PCIE Function	Displays the PCIe function information of the remote device: ID, name, device linked, device class, class code, device ID, vendor ID, function ID, revision ID, sub system ID, sub system vendor ID, and state.
Storage	Displays the storage device controller information of the remote device: name, serial number, manufacturer, protocol, model, revision, enryption status, media type, state, size (GB), and speed (Gbps).

3.5 FRU Information

This Page displays the BMC's FRU (Field Replaceable Units) device information. The FRU page shows Basic Information, Chassis Information, Board Information and Product Information of the FRU device. Scroll down to view more items.



To view the information on an FRU device:

1. Select an FRU Device ID from the **FRU Device ID** drop down menu.
2. The FRU device name and information on the FRU device selected will be displayed once your selection has been made.

Writing FRU information using IPMITool

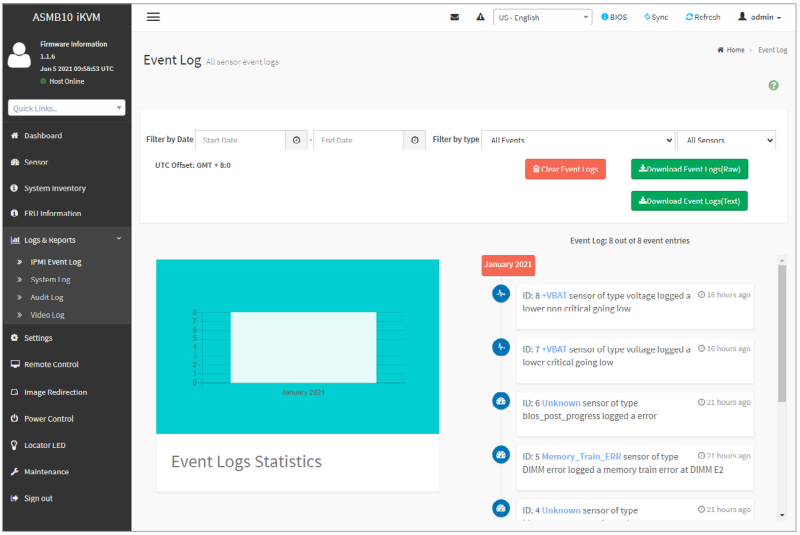
You can write the FRU information by entering commands through the IPMITool. To write the FRU information using IPMITool:

1. Unlock the FRU by entering the command in IPMITool.
2. After unlocking the FRU, write the information from the modified .bin file to the FRU using the command in IPMITool.
3. Entering the print command will display the newly written FRU information.

For a list of IPMITool commands, please refer to the **Appendix**.

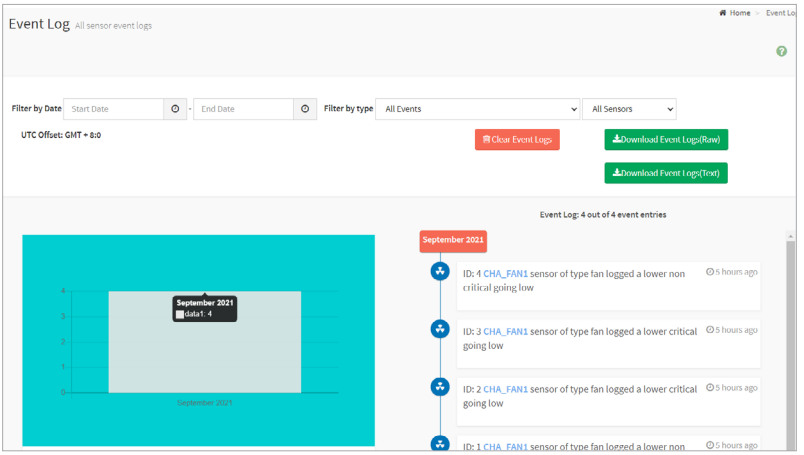
3.6 Logs & Reports

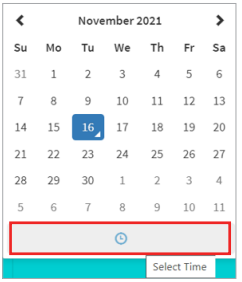
This menu contains the IPMI Event Log, System Log, Audit Log, and Video Log.



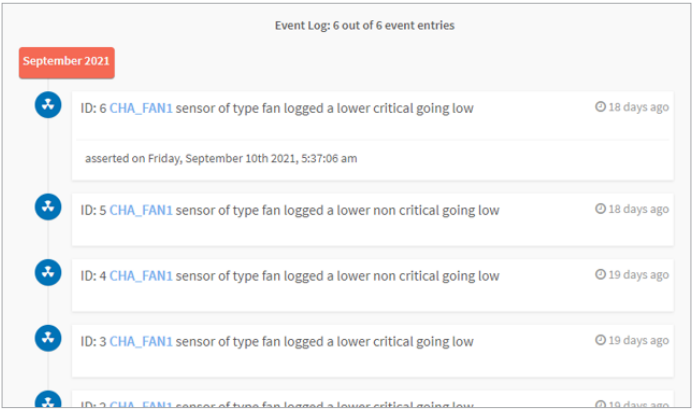
3.6.1 IPMI Event Log

This page displays the list of events incurred by different sensors on this device. Click on a record to see the details of that entry. Hovering over the graph will allow you to view the number of events by date.



Filter by Date	Select the time period to filter by selecting the **Start Date** and the **End Date** from the calender. You can also click on the clock icon at the bottom of the calendar to add a time filter.  
Filter by Type	Select the type of event and sensor name to view the events of the selected event type for that sensor.
Clear Event Logs	Clears all events of all sensors.
Download Event Logs (Raw)	Download all logs as raw data.
Download Event Logs (Text)	Download all logs as text format.

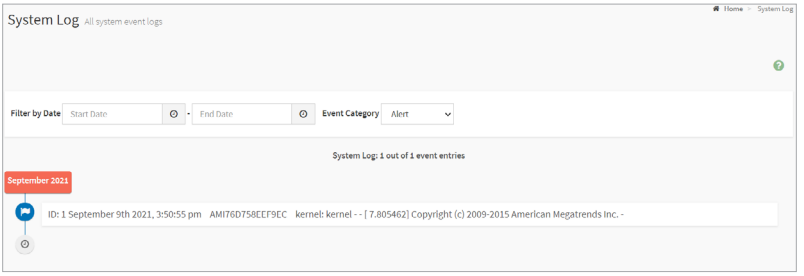
You can click on an event to view the date and time of the event.

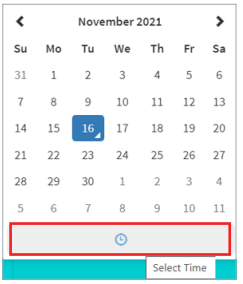


3.6.2 System Log

This page displays logs of system events for this device (if the options have been configured).

- Logs have to be configured under **Settings** > **Log Settings** > **Advanced Log Settings** in order to display any entries. Filtering options are also available for all log entries.
- The System Log will be displayed with the default time if the BMC remote device was not connected to the network when it was powered on.

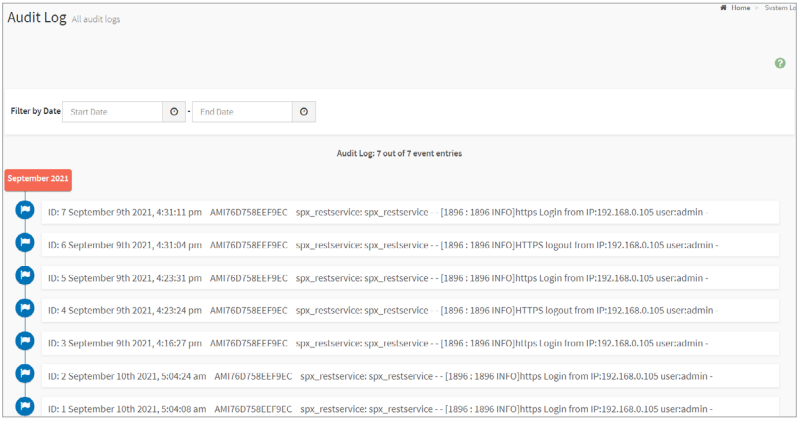


Filter by Date	Select the time period to filter by selecting the **Start Date** and the **End Date** from the calender. You can also click on the clock icon at the bottom of the calendar to add a time filter.  
Filter by Type	Select the type of event and sensor name to view the events of the selected event type for that sensor.

3.6.3 Audit Log

This page displays logs of audit events for this device (if the options have been configured).

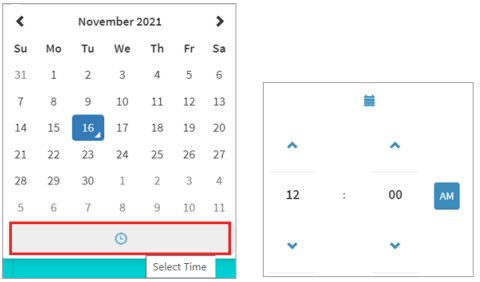
Logs have to be configured under **Settings** > **Log Settings** > **Advanced Log Settings** in order to display any entries.



Filter by Date

Select the time period to filter by selecting the **Start Date** and the **End Date** from the calender.

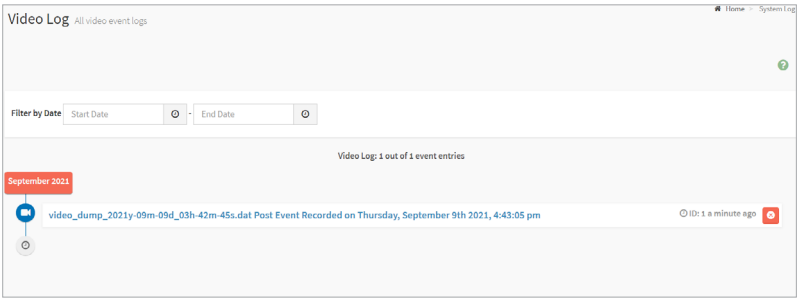
You can also click on the clock icon at the bottom of the calendar to add a time filter.



3.6.4 Video Log

This page displays logs of available recorded video files (if the options have been configured). You can click on a video recording to play/pause the video recording, or download the video file to the remote device in .avi format. Clicking on the **X** icon will close the video recording file.

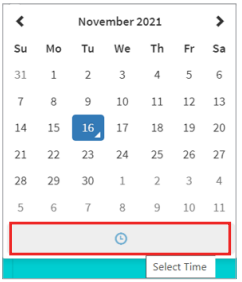
Configurations have to be set under **Settings** > **Video Recording** > **Auto Video Settings** > **Video Trigger Settings** in order to display any entries.



Filter by Date

Select the time period to filter by selecting the **Start Date** and the **End Date** from the calender.

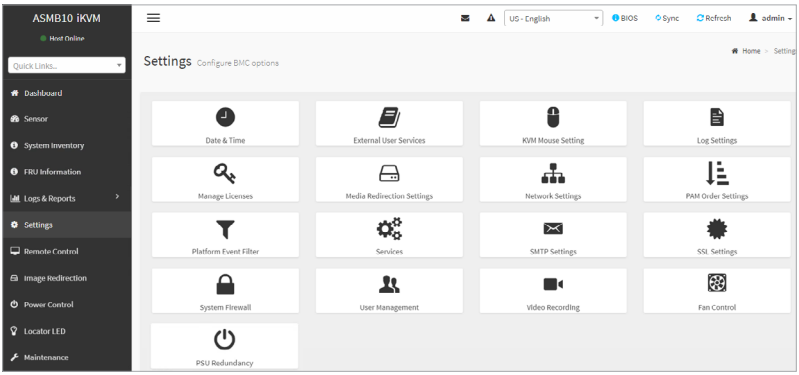
You can also click on the clock icon at the bottom of the calendar to add a time filter.



- If remote video support is enabled, a maximum of 3 pre-event videos may be recorded. If remote video support is disabled, only 1 pre-event and 2 post-event videos may be recorded.
- Browsers will not be able to store and playback data which exceed 40MB, only video files less than 40MB can be downloaded or played. If the video recording exceeds 40MB, a message will prompt the user to use a Java Player Application instead.

3.7 Settings

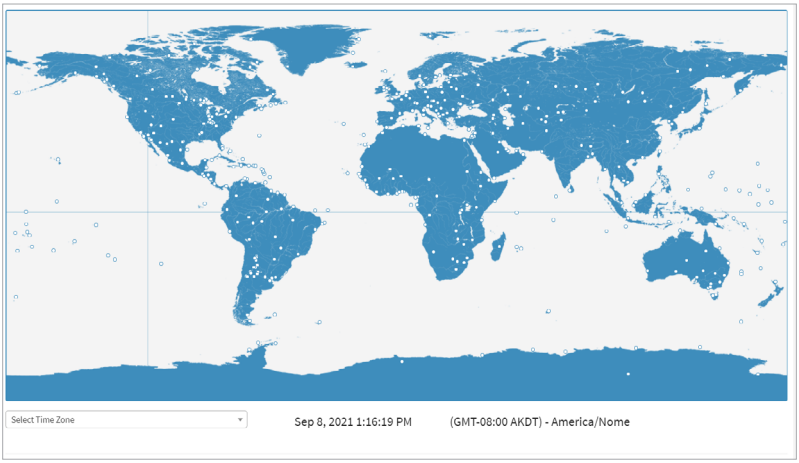
This page allows you to configure the BMC settings. Click on an item for more options.



3.7.1 Date & Time

This page allows you to set the date and time on the BMC. You can either select a time zone from the interactive map, or manually set the date and time.

- If the time zone is selected from the group of manual offset (GMT/ETC time zones), the interactive map selection feature will be disabled.
- Ensure to click on **Save** to save the changes made. The new settings will only be applied after the changes have been saved.
- If the BIOS time and BMC time differs by over 30 minutes when the remote device is powered on, the web-based user interface will be logged out. Ensure to manually or automatically set the BMC time after the BMC is connected.



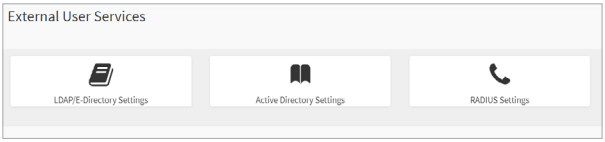
Select Time Zone	Select the time zone from the **Select Time Zone** drop down menu, or double click on a time zone on the interactive map.
Date & Time	Displays the date and time of the selected time zone.
Automatic NTP Date & Time	Enable or disable automatic time and date synchronization with the NTP server.
Primary NTP Server	Allocate the primary NTP server to automatically update date and time.
Secondary NTP Server	Allocate the secondary NTP server to automatically update date and time.
Automatic PTP Date & Time	Enable or disable the PTP server from automatically setting the date and time.
PTP Interface	Configure a PTP server interface to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Preset	Configure a PTP preset type to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Transport	Configure a PTP transport type to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Ipmode	Configure a PTP Ipmode type to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Unicast IP	Configure a Unicast IP when Ipmode is unicast and server to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Delay Mechanism	Configure a PTP delay mechanism to use when automatically settings the date and time.  This item is only configurable if **Automatic PTP Date & Time** is set to enabled.

(continued on the next page)

PTP Inbound Latency	Configure an inbound latency of the server to use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Outbound Latency	Configure a PTP outbound latency of the server to use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Priority1	Configure a priority of PTP clock to use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Max Master capacity	Configure a max master capacity of the PTP clock to use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
PTP Log request delay	Configure a PTP log request delay, use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.
Panic Mode	Configure PTP clock to not reset if jump is more than 1 second, use when automatically settings the date and time. This item is only configurable if **Automatic PTP Date & Time** is set to enabled.

3.7.2 External User Services

This page allows you to set the LDAP/E-directory Settings, Active directory Settings, and RADIUS Settings.



LDAP/E-directory Settings

This page allows you to set the LDAP/E-directory Settings. 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.

- **General Settings**

Enable LDAP/E-Directory Authentication	Enable or disable LDAP/E-Directory Authentication.
Encryption Type	Select the LDAP/E-Directory encryption type (**No encryption**, **SSL**, **StartTLS**). If **SSL** is enabled a port number should be configured.
Common Name Type	Check to set **IP Address** or **FQDN** as common name type. **FQDN** option only appears when **Encryption Type** is set to **StartTLS**.
Server Address	Enter LDAP/E-Directory server address. • IPV4 and IPV6 address formats are supported by LDAP/E-Directory Server Address. • When using **StartTLS** with **FQDN** please enter the FQDN address.
Port	Set LDAP/E-Directory port. • Default port is 389. • The default port for SSL connections is 636. • Port value ranges from 1 - 65535. • Port 80 is blocked for TCP/UDP protocols.

(continued on the next page)

Bind DN	Used in bind operations, which authenticates the client to the server. • Must be a combination of 4-63 alpha-numeric characters. • It must start with an alphabetical character. • Special characters such as dot (.), comma (,), hyphen (-), underscore (_), equal to (=) is allowed. For example: cn-manager, ou-login, dc-domain, dc-com.
Password	Also used in the bind authentication operations between client and server.
Search Base	Allows the LDAP/E-Directory server to find which part of the external directory tree is to be searched.
Attribute of User Login	Set the attribute to indicate to the LDAP/E-Directory which attribute to identify the user by. Only supports cn or uid.
CA certificate file	Browse for the file that contains the certificate of the trusted CA certs. • CA certificate file should be of the type pem. • This file is required when **Encryption Type** is set to **SSL** or **StartTLS**. • This item is only configurable if **Encryption Type** is set to **SSL**.
Certificate file	Browse for the client certificate file. • Certificate file should be of the type pem. • This file is required when **Encryption Type** is set to **SSL** or **StartTLS**. • This item is only configurable if **Encryption Type** is set to **SSL**.
Private Key	Browse for the client private key. • Private key should be of the type pem. • This file is required when **Encryption Type** is set to **SSL** or **StartTLS**. • This item is only configurable if **Encryption Type** is set to **SSL**.

- **Role Groups**
  Allows you to set LDAP/E-Directory user role groups.
  - Clicking on an unassigned empty box will allow you to add a new role group.
  - Clicking on a cell with an existing role group will allow you to modify the role group.
  - Clicking on the **x** to the top right corner of a role group will delete the role group.

Active directory Settings

This page allows you to set the Active directory Settings. 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.

- **General Settings**

Enable Active Directory Authentication	Enable or disable Active Directory Authentication.
SSL	Enable or disable SSL encryption.
Secret Username	Set the active directory server administrator username. • Must be a combination of 1-64 alpha-numeric characters. • It must start with an alphabetical character. • Special characters and spaces are not allowed. • If the **Secret Username** and **Secret Password** are not necessary, please leave both fields blank.
Secret Password	Set the active directory server administrator password. • Must be at least 6 characters long. • White space is not allowed. • Must not exceed 127 characters. • If the **Secret Username** and **Secret Password** are not necessary, please leave both fields blank.
User Domain Name	Set a domain name for the user.
Domain Controller Server Address 1-3	Enter the IP address of the active directory server. • At least 1 Domain Controller Server Address must be configured • Supports IPV4 and IPV6 Address format.

- **Role Groups**
  Allows you to set Active Directory user role groups.
  - Clicking on an unassigned empty box will allow you to add a new role group.
  - Clicking on a cell with an existing role group will allow you to modify the role group.
  - Clicking on the **x** to the top right corner of a role group will delete the role group.

RADIUS Settings

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

- **General RADIUS Settings**

Enable RADIUS Authentication	Enable or disable RADIUS Authentication.
Server Address	Enter RADIUS server address. IPV4 and IPV6 address formats, and FQDN (Fully Qualified Domain Name) format is supported.
Port	Set RADIUS port. • Default port is 1812. • Port value ranges from 1 - 65535. • Port 80 is blocked for TCP/UDP protocols.
Secret	Set RADIUS server password. • Must be at least 4 characters long. • White space is not allowed. • Must not exceed 32 characters.

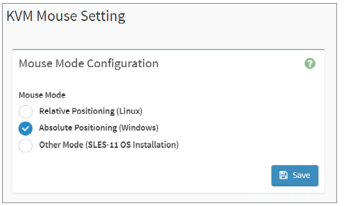
- **Advanced RADIUS Settings**
  For authorization purposes, when setting the items in the Advanced RADIUS Settings page, you should use Vendor Specific Attributes for the radius users on the server.

- Do not exceed 127 characters for each field.
- The '**#**' character is not allowed.

3.7.3 KVM Mouse Setting

This page allows you to set the mouse mode. The Redirection Console handles mouse emulation from local window to remote screen using either of the three methods. Only the Administrator has the permissions to configure this option.

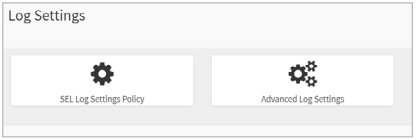
To use the keyboard and mouse function for KVM remote control, ensure the **USB header** is connected to the USB 2.0 connector on the motherboard.



Relative Positioning (Linux)	Calculated relative mouse position displacement is sent to the server.
Absolute Positioning (Windows)	Absolute position of the local mouse is sent to the server. This option is recommended for Windows or later versions on Linux.
Other Mode (SLES-11 OS Installation)	Calculated displacement from the local mouse in the center position is sent to the server.

3.7.4 Log Settings

This page allows you to set the log policy for the event log and also configure advanced log settings.



SEL Log Settings Policy

This page is used to configure the log policy for the event log.

Linear Storage Policy	Set the SEL Log Setting Policy as a Linear Storage Policy.
Circular Storage Policy	Set the SEL Log Setting Policy as a Circular Storage Policy.

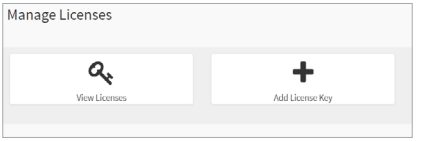
Advanced Log Settings

This page allows you to set advanced settings for the event logs.

System Log	Enable **System Log** to view all system events. Entries can be filtered based on their classification levels.
Local Log	Check this item to save the logs locally (BMC)
Remote Log	Check this item to save the logs in a remote machine.
Port Type	The port type for the remote log. Users can select between UDP or TCP.  Setting the port type will only be supported when **Remote Log** is enabled.
File Size	Specify the size of the local log file in bytes.  • Only applies when **Local Log** is enabled. • Size ranges from 3 to 65535. • Log files are rotated when the size is larger than the mentioned bytes, with regards for the last rotation time interval (1 minute).
Rotate Count	When logged information exceeds the specified file size, the old log information automatically gets moved to back up files based on the rotate count value.  • Rotate count value must be 0 or 1. • If the rotate count is 0, the old log information will be permanently cleared each time.
Remote Log Server	Set the remote server address to log system events.  IPV4 and IPV6 address formats, and FQDN (Fully Qualified Domain Name) format is supported.
Remote Server Port	Set the port number to log system events.  If 0 is entered as the port number, the default port number will be set. The default port number is 514.
Enable Audit Log	Enable this item to view all audit events for this remote device.

3.7.5 Manage Licenses

This page allows you to manage and view KVM, LMEDIA, MEDIA, and RMEDIA license information.



View Licenses

This page allows you to view Licenses already added as well as the number of days the license is still valid for.

KVM	Displays the number of days KVM is still valid for.
LMEDIA	Displays the number of days LMEDIA is still valid for.
MEDIA	Displays the number of days MEDIA is still valid for.
RMEDIA	Displays the number of days RMEDIA is still valid for.

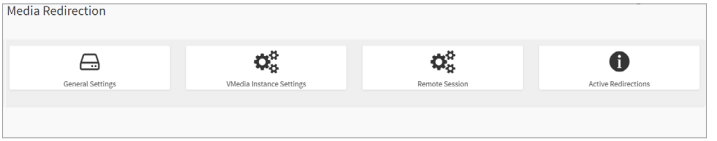
Add License Key

This page allows you to add a license key to activate or extend the associated feature(s).

- License Key must be a minimum of 8 characters long.
- Dashes are allowed but not counted.

3.7.6 Media Redirection Settings

This page allows you to set the media redirection settings.



General Settings

This page allows you to enable or disable Local Media support, check or uncheck the checkbox respectively.

Remote Media Support	Enable or disable remote media support. When enabled, CD/DVD and Hard disk remote media types will appear. Users can configure different settings for the different remote media types. Configuration options will be displayed for each media type, or the same options can be applied to both.

(continued on the next page)

Mount CD/ DVD	**Server Address for CD/DVD Images**	Enter the address of the server where remote videos are to be stored  IPV4 and IPV6 address formats, and FQDN (Fully Qualified Domain Name) format is supported.
	Path in server	Enter the path of the remote media on the server.  Path must be alpha-numeric and only the following special characters are allowed: '**/**' (backward slash), '****' (forward slash), '**_**' (underscore), and '**.**' (dot).
	Share Type for CD/DVD	The shared type of the remote media; either NFS or Samba (CIFS).
	Domain Name	Enter the domain name of the remote media.  • **Domain Name** is optional • If Samba (CIFS) is selected as the **Share Type for CD/DVD**, then enter user credentials to authenticate the server.
	Username	Enter the username.
	Password	Enter the password.  Password must be alpha-numeric and the following special characters are not allowed: **{ } < > & * ` | = ? ; [ ] $ - # ~ ! " % / : + , '**
Same settings for Harddisk Images		Check this item to apply the server information entered for CD/DVD media type to hard disk remote media type.
Mount Harddisk	**Server Address for Harddisk Images**	Enter the address of the server where remote videos are to be stored  IPV4 and IPV6 address formats, and FQDN (Fully Qualified Domain Name) format is supported.
	Path in server	Enter the path of the remote media on the server.  Path must be alpha-numeric and only the following special characters are allowed: '**/**' (backward slash), '****' (forward slash), '**_**' (underscore), and '**.**' (dot).
	Share Type for Harddisk	The shared type of the remote media; either NFS or Samba (CIFS).

(continued on the next page)

Mount Harddisk	**Domain Name**	Enter the domain name of the remote media. • **Domain Name** is optional • If Samba (CIFS) is selected as the **Share Type for CD/DVD**, then enter user credentials to authenticate the server.
	Username	Enter the username.
	Password	Enter the password. Password must be alpha-numeric and the following special characters are not allowed: **{ } < > & * ` | = ? ; [ ] $ - # ~ ! " % / : + , '**

VMedia Instance Settings

This page allows you to configure settings for the redirection of virtual media to the number of supported CD/DVD devices.

CD/DVD device instances	Select the number of CD/DVD devices to be supported for Virtual Media redirection.
Hard disk instances	Select the number of Hard disk devices to be supported for Virtual Media redirection.
Remote KVM CD/DVD device instances	Select the number of Remote KVM CD/DVD devices to be supported for Virtual Media redirection.
Remote KVM hard disk instances	Select the number of Remote KVM hard disk devices to be supported for Virtual Media redirection.

Remote Session

This page allows you to change the settings for the remote session.

KVM Single Port Application	Allows Single Port Application support in BMC.
Enable KVM Encryption	Allows KVM encryption support in BMC.
Keyboard Language	Select the keyboard language.
Virtual Media Attach Mode	Select the Virtual Media Attach Mode.
Retry Count	Set the number of times to retry when a KVM failure occurs. Retry count ranges from 1 to 20.
Retry Time Interval (Seconds)	Set the number of seconds to wait for subsequent retries. Time interval ranges from 5 to 30 seconds.
Server Monitor OFF Features Status	Enable or disable the Server Monitor OFF feature.

Active Redirections

This page displays the list of media currently being redirected, and also displays the status and other basic information of each media item.

Media Type	Displays the media type of the active redirection.
Media Instance	Displays the media instance of the active redirection.
Client Type	Displays the remote machine type of the active redirection.
Image Name	Displays the media name of the active redirection.
Redirection Status	Displays the redirection status of the active redirection.
Client IP	Displays the remote machine's IP of the active redirection.

3.7.7 Network Settings

The Network Settings page allows you to configure the network settings.

Network IP Settings

This page allows you to manage LAN support for the interface.

Enable LAN	Enable or disable LAN support for the interface shown.
LAN Interface	Select the LAN interface to be configured.
MAC Address	Displays the MAC address of the selected interface and is read only.
Enable IPv4	Enable or disable IPv4 support for the selected interface.
Enable IPv4 DHCP	Enable this option to dynamically configure IPv4 address using Dynamic Host Configuration Protocol (DHCP).
IPv4 Address	Specify a static IPv4 address for the selected interface. • This item is only configurable if **Enable IPv4 DHCP** is disabled. • Consists of 4 sets of numbers separated by dots as in '**xxx.xxx.xxx.xxx**'. • Each set ranges from 0 to 255. • First number cannot be 0.

(continued on the next page)

IPv4 Subnet	Specify a static Subnet Mask. • This item is only configurable if **Enable IPv4 DHCP** is disabled. • Consists of 4 sets of numbers separated by dots as in '**xxx.xxx.xxx.xxx**'. • Each set ranges from 0 to 255. • First number cannot be 0.
IPv4 Gateway	Specify a static Default Gateway. • This item is only configurable if **Enable IPv4 DHCP** is disabled. • Consists of 4 sets of numbers separated by dots as in '**xxx.xxx.xxx.xxx**'. • Each set ranges from 0 to 255. • First number cannot be 0.
Enable IPv6	Enable or disable IPv6 support for the selected interface.
Enable IPv6 DHCP	Enable this option to dynamically configure IPv6 address using Dynamic Host Configuration v6 Protocol (DHCPv6).
IPv6 Index	Select an IPv6 Index. This item is only configurable if **Enable IPv6 DHCP** is disabled.
IPv6 Address	Specify a static IPv6 for the selected interface. • This item is only configurable if **Enable IPv6 DHCP** is disabled. • Consists of 4 sets of numbers separated by dots as in '**xxx.xxx.xxx.xxx**'. • Each set ranges from 0 to 255. • First number cannot be 0.
Subnet Prefix Length	Specify the subnet prefix length for the IPv6 settings. • This item is only configurable if **Enable IPv6 DHCP** is disabled. • Values range from 0 to 28.

(continued on the next page)

IPv6 Gateway	Specify an IPv6 gateway. • This item is only configurable if **Enable IPv6 DHCP** is disabled. • Consists of 4 sets of numbers separated by dots as in '**xxx.xxx.xxx.xxx**'. • Each set ranges from 0 to 255. • First number cannot be 0.
Enable VLAN	Enable or disable VLAN support for the selected interface.
VLAN ID	Specify an ID for this VLAN configuration. • This item is only configurable if **Enable VLAN** is enabled. • Values range from 2 to 4094. • VLAN ID cannot be changed without resetting the VLAN configuration. • VLAN ID 0, 1, and 4095 are reserved VLAN IDs.
VLAN Priority	Specify the priority for VLAN configuration. • This item is only configurable if **Enable VLAN** is enabled. • Values range from 0 to 7, with 7 being the highest priority.

DNS Configuration

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

DNS Enabled	Enable or disable all DNS services.
mDNS Enabled	Enable or disable Multicast DNS.
Host Name Setting	Select whether the host name will be configured manually or automatically.
Host Name	Enter the hostname for the device. • This item will automatically display a hostname and cannot be configured if **Host Name Setting** is set to **Automatic**. • This item is only configurable if **Host Name Setting** is set to **Manual**.

(continued on the next page)

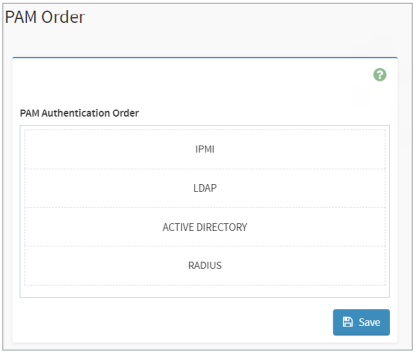
BMC Registration Settings: BMC Interface	**Register BMC**	Enable or disable BMC registration.
	Registration method	Select from the following registration methods: - **Nsupdate**: Register with the DNS server using the nsupdate application. - **DHCP Client FQDN**: Register with the DNS server using DHCP option 81. - **Hostname**: Register with the DNS server using DHCP option 12. • This item is only configurable if **Register BMC** is enabled. • The **Hostname** option should be selected if the DHCP server does not support option 81, and Hostname method registration does not support IPv6 Domain Interface.
	TSIG Authentication Enabled	Enable or disable TSIG authentication (if registering DNS via nsupdate only).
	Current TSIG Private File Info	Display the date and time of the current TSIG private file (Read-Only)
	New TSIG Private File	Browse for a new TSIG private file to upload to the BMC.
	Domain Setting	Select whether the domain interface will be configured manually or automatically.
	Domain Interface	Specify the domain interface This item is only configurable if **Domain Setting** is set to **Automatic**.
	Domain Name	Enter the domain name of the device. This item is only configurable if **Domain Setting** is set to **Manual**.
	Domain Name Server Setting	Select whether the DNS interface will be configured manually or automatically.
	DNS Interface	Specify the interface to use. This item is only configurable if **Domain Setting** is set to **Automatic**.

(continued on the next page)

BMC Registration Settings: BMC Interface	**IP Priority**	Select the IP Priority. • If IP priority is IPv4, then 2 IPv4 and 1 IPv6 DNS servers can be used. • If IP priority is IPv6, then 1 IPv4 and 2 IPv6 DNS servers can be used. • This item is only configurable if **Domain Setting** is set to **Automatic**.
	DNS Server 1-3	Specify the DNS (Domain Name System) server address to be configured for the BMC. • IPv4 Addresses should be given dotted decimal representation. • IPv6 Addresses are supported and must be global unicast addresses. • These items are only configurable if **Domain Setting** is set to **Manual**.

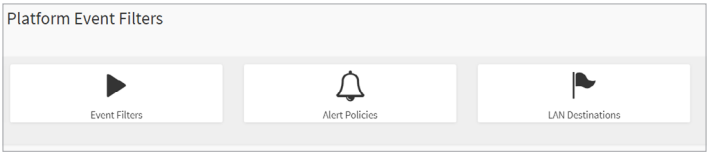
3.7.8 PAM Order Settings

This page allows you to configure the PAM order for user authentication into the BMC. The list of PAM modules supported in the BMC is displayed, and you can drag and drop the PAM modules to reorganize their positions in the sequence.



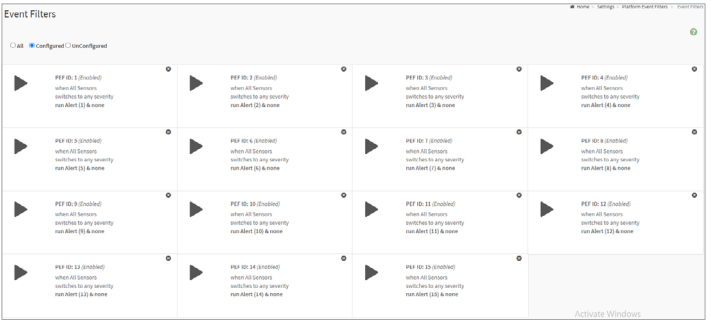
3.7.9 Platform Event Filters

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.



Event Filters

This page shows all configured Event filters and available slots. You can modify or add new event filter entry on this page. By default,15 event filter entries are configured among the 40 available slots.



- **All:** View both available Configured and UnConfigured slots.
- **Configured** or **UnConfigured:** View either available Configured or available UnConfigured slots.

Click on the **x** icon to the top right of the event filter slot to delete the event filter slot from the list.

- **Event Filter Configuration**

  Clicking on a Configured or UnConfigured slot will allow you to edit an event filter, or add a new event filter.

Enable this filter	Enable or disable PEF settings.
Event severity to trigger	Select an Event Severity from the dropdown list.
Event Filter Action Alert	Enable or disable PEF Alert action.
Power Action	Select a power action (**None**, **Power Down**, **Power Cycle**, **Reset**) from the dropdown list.

(continued on the next page)

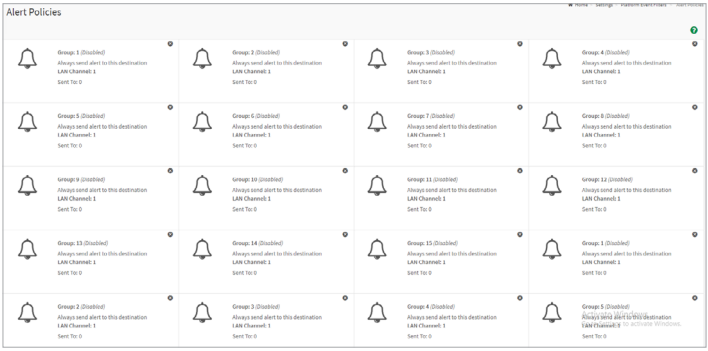
Alert Policy Group Number	Select a configured alert policy number from the dropdown list.  Alert Policy can be configured under **Configuration** > **PEF** > **Alert Policy**.
Raw Data	Enable this option to enter the Generator ID with raw data.
Generator ID 1	Enter the raw generator ID1 data value.  This item is only configurable if **Raw Data** is enabled.
Generator ID 2	Enter the raw generator ID2 data value.  • In the RAW data field, prefix the value with '0x' to specify hexidecimal value. • This item is only configurable if **Raw Data** is enabled.
Generator Type	Select the event generator as Slave Address - if event is generated from IPMB, or software.  This item is only configurable if **Raw Data** is disabled.
Slave Address/Software ID	Select the System Software ID - if event is generated from system software.  This item is only configurable if **Raw Data** is disabled.
Channel Number	Select the particular channel number through which the event message is received over. Select '0' if the event message is received via the system interface, primary IPMB, or internally generated by the BMC.  This item is only configurable if **Raw Data** is disabled.
IPMB Device LUN	Select the corresponding IPMB Device if event is generated by IPMB.  This item is only configurable if **Raw Data** is disabled.
Sensor type	Select the type of sensor that will trigger the event filter action.
Sensor name	Select the particular sensor from the sensor list.

(continued on the next page)

Event Options	Select an event option from either All events or Sensor specific events.
Event trigger	This field is used to give Event/Reading type value. Value ranges from 0 to 255.
Event Data 1 AND Mask	This field is used to indicate wildcarded or compared bits. Value ranges from 0 to 255.
Event Data 1 Compare 1	This field is used to indicate whether each bit position's comparison is an exact comparison or not. Value ranges from 0 to 255.
Event Data 1 Compare 2	This field is used to indicate whether each bit position's comparison is an exact comparison or not. Value ranges from 0 to 255.
Event Data 2 AND Mask	This field is similar to Event Data 1 AND Mask.
Event Data 2 Compare 1	These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
Event Data 2 Compare 2	
Event Data 3 AND Mask	This field is similar to Event Data 1 AND Mask.
Event Data 3 Compare 1	These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
Event Data 3 Compare 2	

Alert Policies

This page shows all configured Alert policies and available slots. You can modify or add new alert policy entry from on this page. A maximum of 60 slots are available.



Click on the **x** icon to the top right of the alert policy slot to delete an alert policy from the list.

- **Alert Policy Configuration**

  Clicking on a Configured or UnConfigured slot will allow you to edit an alert policy, or add a new alert policy.

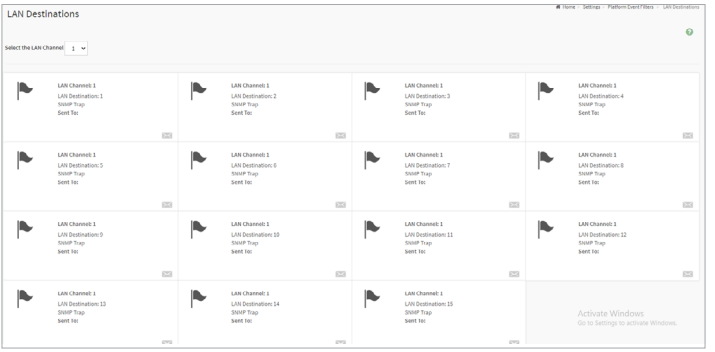
Policy Group Number	Select a policy number that was configured in the Event filter table.
Enable this alert	Enable or disable policy settings.
Policy Action	Select a policy action from the list: - 0: Always send alert to this destination - 1: If alert to previous destination was successful, do not send 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.
LAN Channel	Select a LAN channel for the policy.
Destination Selector	Select a destination from the configured destination list. LAN destinations have to be configured under **Configuration** > **PEF** > **LAN Destination.**

(continued on the next page)

Event Specific Alert String	Check this item to specify an event-specific Alert String.
Alert String Key	Select from a set of values (all linked to strings that are kept in the PEF configuration parameters), to specify which is to be sent for this Alert Policy entry.

LAN Destinations

This page shows all configured LAN destinations and available slots. You can modify or add new LAN destination entry from on this page. A maximum of 15 slots are available.



- **Send Test Alert:** Select a configured slot and click **Send Test Alert** to generate a sample alert message to the configured destination.

- Test alert for emails can only be sent when SMTP configuration is enabled. To set SMTP configuration, go to **Settings** > **SMTP**. Make sure that SMTP server address and port numbers are configured properly.
- After a LAN destination has been configured, an **x** icon will appear to the top right of the LAN Channel slot. Click on the **x** icon to delete the LAN Channel slot from the list.

- **LAN Destination Configuration**

  Clicking on a Configured or UnConfigured slot will allow you to edit a LAN destination, or add a new LAN destination.

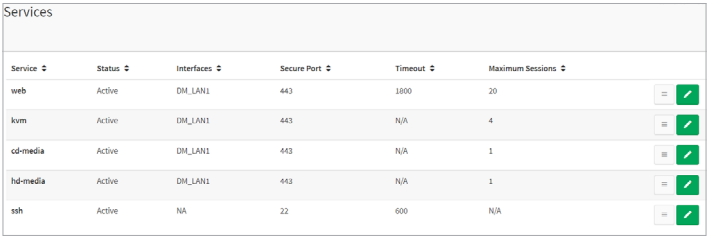
LAN Channel	Displays the LAN Channel Number of the selected slot (read only).
LAN Destination	Displays the Destination number of the selected slot (read only).
Destination Type	Select between **SMNP Trap** or **E-Mail** as the destination type.
SMNP Trap Versions	Select an SMNP Trap Version This item is only configurable if **Destination Type** is set to **SNMP Trap**.

(continued on the next page)

SMNP Destination Address	Enter the IP address of the system that will receive the alert.  • IPV4 and IPV6 address formats are supported. • This item is only configurable if **Destination Type** is set to **SNMP Trap**.
BMC Username	If Destination type is **E-Mail** Alert, then select the user to whom the email alert has to be sent.  • Email address for the user has to be configured under **Settings** > **User Management.** • BMC Username should be configured for SMNP Trap Version - 3.
Email Subject	An email is sent to the configured email address of the user 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.  • These fields are not applicable for 'AMI-Format' email body. • This item must be configured if **E-Mail** is selected as the **Destination Type**. • This item is only configurable if **Destination Type** is set to **E-Mail**.
Email Message	

3.7.10 Services

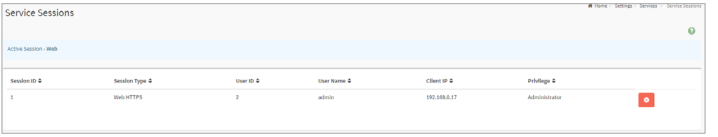
This page lists services running on the BMC. It shows current status and other basic information about the services.



- Click on the to modify the services configuration.
- Click on the icon view or terminate the connected session for this device.
- Only the Administrator can modify a service.

View Services

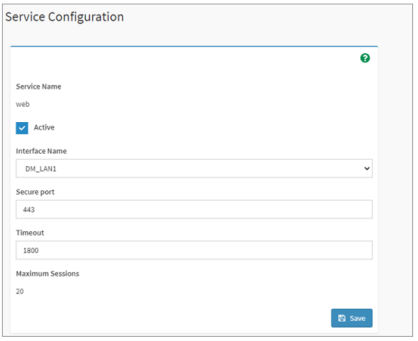
This page displays basic information about the Active sessions on this BMC. You may also terminate the session as the Administrator.



- Click on the icon to terminate the particular session of the service.
- Click on the icon view or terminate the connected session for this device.
- The default user ID ranges for the supported PAM Modules are:
  - Active Directory User: from 3000 - 3999
  - LDAP/E-Directory User: from 2000 - 2999
  - RADIUS User: from 4000 - 4999

Service Configuration

This page allows you to configure the selected service.



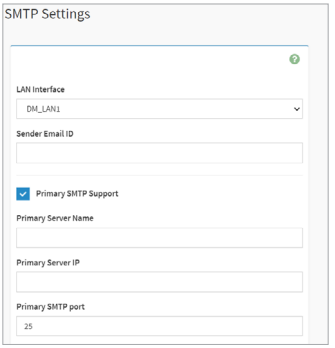
Service Name	Displays the service name of the selected slot (read only).
Active	Displays the current status of the service, either active or inactive. Check to activate the service.
Interface Name	This indicates the interface on which the service is running. The user can choose any one of the available interfaces. • Service mapping to disabled interfaces will not work. Status of interface can be checked/enabled, under **Configuration** > **Network** > **LAN Settings**. • Media and KVM interfaces are read only when single port is enabled. • This item is only configurable if **Active** is enabled.
Secure Port	Used to configure secure port numbers for the services. • Web default port is 443. • KVM default port is 443. • CD Media default port is 443. • HD Media default port is 443. • SSH default port is 22. • Port value ranges from 1 to 65535. • Port 80 is blocked for TCP/UDP protocols. • This item is only configurable if **Active** is enabled.

(continued on the next page)

Timeout	Where supported, user can configure the session timeout value. • Web and KVM timeout value ranges from 300 to 1800 seconds. • Web timeout will be ignored if there is any ongoing KVM session. • SSH timeout value ranges from 60 to 1800 seconds. • Timeout value should be in multiples of 60 seconds. • This item is only configurable if **Active** is enabled.
Maximum Sessions	Displays the maximum number of allowed sessions for the service.

3.7.11 SMTP Settings

The SMTP page allows you to configure SMTP mail server.



LAN Interface	Select the LAN interface to be configured.
Sender Email ID	Enter a valid **Sender Email ID** on the SMTP Server. Maximum allowed size for Email ID is 64 bytes, which includes username and domain name.
Primary SMTP Support	Enable or disable SMTP support for the BMC.

(continued on the next page)

Primary Server Name	Enter the Machine Name of the SMTP Server. This field is only for Information Purpose Only. • Machine Name is a string of 25 alpha-numeric characters maximum. • Spaces and special characters are not allowed. • This item is only configurable if **Primary SMTP Support** is enabled.
Primary Server IP	Enter the Server Address for the SMTP Server. • Consists of 4 sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'. • Each set ranges from 0 to 255. • First number cannot be 0. • IPV4 and IPV6 address formats, and Host Name format is supported. • This item is only configurable if **Primary SMTP Support** is enabled.
Primary SMTP port	Specify the SMTP Port. • Default port is 25. • Port value ranges from 1 to 65535. • This item is only configurable if **Primary SMTP Support** is enabled.
Primary Secure SMTP port	Specify the SMTP Secure Port. • Default port is 465. • Port value ranges from 1 to 65535.
Primary SMTP Authentication	Enable or disable SMTP Authentication. Supported SMTP Server Authentication Types are: - CRAM-MD5 - LOGIN - PLAIN If the SMTP server does not support any of the above authentication types, the user will get an error message stating, '*Authentication type is not supported by SMTP server*'.

(continued on the next page)

Primary Username	Enter the username required to access SMTP Accounts.  • User Name can be a length of 4 to 64 alpha-numeric characters, dot (.), at sign (@), hyphen (-), and underscore (_). • It must start with an alphabetical character. • Other special characters are not allowed. • This item is only configurable if **Primary SMTP Authentication** is enabled.
Primary Password	Enter the password for the SMTP User Account.  • Must be at least 4 characters long, and the field has a maximum limit of 64 characters. • White space is not allowed. • This item is only configurable if **Primary SMTP Authentication** is enabled.
Primary SMTP SSLTLS Enable	Enable or disable the SMTP SSLTLS protocol.  This item is only configurable if **Primary SMTP Support** is enabled.
Primary SMTP STARTTLS Enable	Enable or disable the SMTP STARTTLS protocol.  This item is only configurable if **Primary SMTP Support** is enabled.
Secondary SMTP Support	Enable or disable Secondary SMTP support for the BMC.
Secondary Server Name	Enter the Machine Name of the Secondary SMTP Server. This field is only for Information Purpose Only.  • Machine Name is a string of 25 alpha-numeric characters maximum. • Spaces and special characters are not allowed. • This item is only configurable if **Secondary SMTP Support** is enabled.

(continued on the next page)

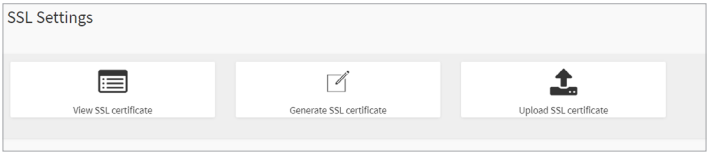
Secondary Server IP	Enter the Server Address for the Secondary SMTP Server. • Consists of 4 sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'. • Each set ranges from 0 to 255. • First number cannot be 0. • IPV4 and IPV6 address formats, and Host Name format is supported. • This item is only configurable if **Secondary SMTP Support** is enabled.
Secondary SMTP port	Specify the Secondary SMTP Port. • Default port is 25. • Port value ranges from 1 to 65535. • This item is only configurable if **Secondary SMTP Support** is enabled.
Secondary Secure SMTP port	Specify the Secondary SMTP Secure Port. • Default port is 465. • Port value ranges from 1 to 65535.
Secondary SMTP Authentication	Enable or disable Secondary SMTP Authentication. Supported SMTP Server Authentication Types are: - CRAM-MD5 - LOGIN - PLAIN If the SMTP server does not support any of the above authentication types, the user will get an error message stating, '*Authentication type is not supported by SMTP server*'.
Secondary Username	Enter the username required to access SMTP Accounts. • User Name can be a length of 4 to 64 alpha-numeric characters, dot (.), at sign (@), hyphen (-), and underscore (_). • It must start with an alphabetical character. • Other special characters are not allowed. • This item is only configurable if **Secondary SMTP Authentication** is enabled.

(continued on the next page)

Secondary Password	Enter the password for the SMTP User Account. • Must be at least 4 characters long, and the field has a maximum limit of 64 characters. • White space is not allowed. • This item is only configurable if **Primary SMTP Authentication** is enabled.
Secondary SMTP SSLTLS Enable	Enable or disable the SMTP SSLTLS protocol. This item is only configurable if **Primary SMTP Support** is enabled.
Secondary SMTP STARTTLS Enable	Enable or disable the SMTP STARTTLS protocol. This item is only configurable if **Primary SMTP Support** is enabled.

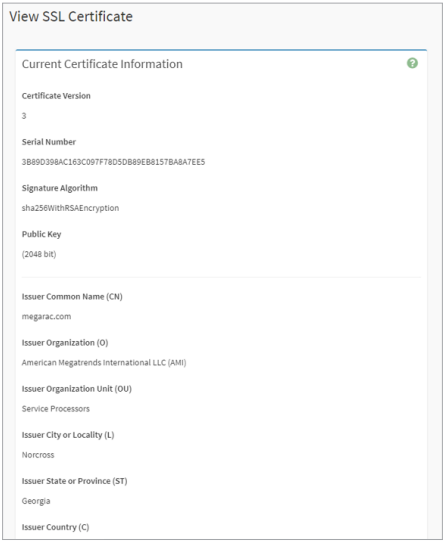
3.7.12 SSL Settings

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.



View SSL Certificate

This page displays the basic information about the uploaded SSL certificate.



Certificate Version	The **Basic Information** section displays basic information about the uploaded SSL certificate.
Serial Number	
Signature Algorithm	
Public Key	
Issuer Common Name (CN)	The **Issued From** section contains information about the Certificate Issuer.
Issuer Organization (O)	
Issuer Organization Unit (OU)	
Issuer City or Locality (L)	
Issuer State or Province (ST)	
Issuer Country (C)	
Issuer Email Address	
Valid From	The **Validity Information** displays the validity period of the uploaded certificate.
Valid Till	
Issued to Common Name (CN)	The **Issued To** section contains information for the certificate holder.
Issued to Organization (O)	
Issued to Organization Unit (OU)	
Issued to City or Locality (L)	
Issued to State or Province (ST)	
Issued to Country (C)	
Issued to Email Address	

Generate SSL Certificate

This page allows you to create an SSL certificate.

Common Name (CN)	Enter the common name for which the certificate is to be generated. • Maximum of 64 alpha-numeric characters. • Special characters '**#**' and '**$**' are not allowed.
Organization (O)	Enter the name of the organization for which the certificate is to be generated. • Maximum of 64 alpha-numeric characters. • Special characters '**#**' and '**$**' are not allowed.
Organization Unit (OU)	Enter the section or unit of the organization for which the certificate is to be generated. • Maximum of 64 alpha-numeric characters. • Special characters '**#**' and '**$**' are not allowed.
City or Locality (L)	Enter the City or Locality. • Maximum of 128 alpha-numeric characters. • Special characters '**#**' and '**$**' are not allowed.
State or Province (ST)	Enter the State or Province. • Maximum of 128 alpha-numeric characters. • Special characters '**#**' and '**$**' are not allowed.
Country (C)	Enter the Country code. • Only two characters can be entered. • Special characters are not allowed.
Email Address	Enter the Email Address of the organization.
Valid For	Enter the requested validity days for the certificate. Value ranges from 1 to 3650 days.
Key Length	Select the key length bit value of the certificate.

Upload SSL Certificate

This page allows you to upload a certificates and private keys.

Current Certificate	Contains information of the Current Certificate. The date and time it was uploaded will also be displayed (read only).
New Certificate	Click the Browse button and navigate to the new certificate file. Certificate file should be of pem type.
Current Private Key	Contains information for the current private key. The date and time it was uploaded will also be displayed (read only).
New Private Key	Click the Browse button and navigate to the private key file. Private Key file should be of pem type.

3.7.13 System Firewall

This page allows you to create and manage firewalls on the BMC, IP address, and port firewall rule management.

General Firewall Settings

This page allows you to create and manage existing general firewall settings.

- **Existing Firewall Settings**
  This page displays the list of general firewall rules on this BMC.

- To view the page, the user must at least have Operator privileges.
- To add or delete a firewall, the user must have Administrator privileges.
- To ensure the date and time of the firewall rule works properly, make sure to set the BMC system time before setting the firewall.
- Click on the **x** icon to delete a firewall rule from the list.

- **Add Firewall Settings**
  This page allows you to add firewall settings.

Block All	Blocks all incoming IPv4, IPv6, and Ports.
Flush All	Clear all existing system firewall rules.
Timeout	Enable or disable firewall rules with timeout.

(continued on the next page)

Start Date	The firewall rule will become effective from this date. This item is only configurable if **Timeout** is enabled.
Start Time	The firewall rule will become effective from this time. This item is only configurable if **Timeout** is enabled.
End Date	The firewall rule will expire on this date. This item is only configurable if **Timeout** is enabled.
End Time	The firewall rule will expire at this time. This item is only configurable if **Timeout** is enabled.

IP Address Firewall Rules

This page allows you to create and manage existing firewall settings based on IP.

- **Existing IP Rules**
  This page displays the list of existing IP firewall rules.

- To view the page, the user must at least have Operator privileges.
- To add or delete a firewall, the user must have Administrator privileges.
- To ensure the date and time of the firewall rule works properly, make sure to set the BMC system time before setting the firewall.
- Click on the **x** icon to delete a IP firewall rule from the list.

- **Add New IP Rule**
  This page allows you to add IP firewall settings for the BMC.

IP Single (or) Range Start	Enter the start IP Address or start of a Range of IP Addresses. IP Address must follow the IPv4 Address format. • Consists of 4 sets of numbers separated by dots as in 'xxx.xxx.xxx.xxx'. • Each set ranges from 0 to 255. • First number cannot be 0.
IP Range End	Used to indicate the IP Address or end of an IP address range.

(continued on the next page)

Enable Timeout	Enable or disable Timeout.
Start Date	The firewall rule will become effective from this date. This item is only configurable if **Enable Timeout** is enabled.
Start Time	The firewall rule will become effective from this time. This item is only configurable if **Enable Timeout** is enabled.
End Date	The firewall rule will expire on this date. This item is only configurable if **Enable Timeout** is enabled.
End Time	The firewall rule will expire at this time. This item is only configurable if **Enable Timeout** is enabled.
Rule	Allow or block this firewall rule.

Port Firewall Rules

This page allows you to create and manage existing firewall settings based on ports.

- **Existing Port Rules**
  This page displays the list of existing firewall port rules.

- To view the page, the user must at least have Operator privileges.
- To add or delete a firewall, the user must have Administrator privileges.
- To ensure the date and time of the firewall rule works properly, make sure to set the BMC system time before setting the firewall.
- Port 80 is blocked for TCP/UDP protocols.
- Click on the **x** icon to delete a port rule from the list.

- **Add New Port Rule**
  This page allows you to add IP firewall port settings for the BMC.

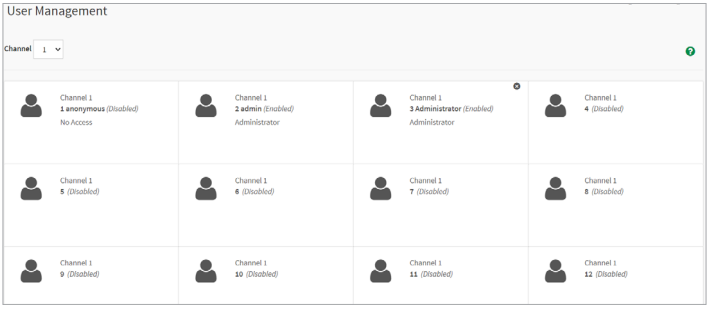
Port Single (or) Range Start	Specify the port or start of a range of Port Addresses. • Port value ranges from 1 to 65535. • Port 80 is blocked for TCP/UDP protocols.
Port Range End	Used to configure the Port or end of a range of Port Addresses.

(continued on the next page)

Protocol	Select the protocol (**TCP**, **UDP**, or **Both**).
Network Type	Select the network type (**IPv4**, **IPv6**, or **Both**).
Enable Timeout	Enable or disable Timeout support for the new rule.
Start Date	The firewall rule will become effective from this date. This item is only configurable if **Enable Timeout** is enabled.
Start Time	The firewall rule will become effective from this time. This item is only configurable if **Enable Timeout** is enabled.
End Date	The firewall rule will expire on this date. This item is only configurable if **Enable Timeout** is enabled.
End Time	The firewall rule will expire at this time. This item is only configurable if **Enable Timeout** is enabled.
Rule	Allow or block this firewall rule.

3.7.14 User Management

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.



- **Channel:** Displays the amount of available users for the current LAN channel.

- Click on any available slot to add or edit a user.
- A maximum of 10 slots are available. This number includes the default admin and anonymous users.
- To view the page, the user must at least have Operator privileges.
- To modify or add a user, the user must have Administrator privileges.
- Click on the **x** icon to delete a user from the list.

It is advised that the anonymous user's privilege and password should be modified immediately as a security measure.

User Management Configuration

This page allows you to manage configurations of the selected user.

Username	Enter the name of the new user or edit the name of existing user. • Must be a string of 1 to 16 alpha-numeric characters. • Special characters hyphen (-), underscore (_), and at sign (@) are allowed. • It must start with an alphabetical character. • Case-sensitive.
Change password	Check this option to change the password. This item is only available when editing an existing user.

(continued on the next page)

Password Size		Select the preferred size for the password. This item is only configurable if **Change password** is enabled or when adding a new user.
Password		The password field is mandatory and should have a minimum of 8 characters. This item is only configurable if **Change password** is enabled or when adding a new user.
Confirm Password		Confirm the password by entering it again in this field. This item is only configurable if **Change password** is enabled or when adding a new user.
Enable User Access		Enable or disable User Access.
Enable Channel Access	**Channel 1**	Check the boxes to enable network access for the user. Upon enabling, the corresponding IPMI messaging privilege will be assigned to the user. It is recommended that the IPMI messaging option should be enabled as well if user is created through IPMI.
	Channel 2	
Privilege (Channel 1)		Select the privilege level for each channel to be assigned to this user for access to the BMC through the network interface. There are 5 levels of Network Privileges (Administrator, Operator, User, OEM, and None). These items are only configurable if **Channel 1** or **Channel 2** under **Enable Channel Access** is enabled.
Privilege (Channel 2)		
SNMP Access		Enable or disable SNMP access for the user.
SMNP Access Level		Select the SNMP Access level option for this new user. This item is only configurable if **SNMP Access** is enabled.
SMNP Authentication Protocol		Select an SNMP Authentication Protocol for this user. This item is only configurable if **SNMP Access** is enabled.

(continued on the next page)

SMNP Privacy Protocol	Select the Encryption algorithm to be used for the SNMP settings.  This item is only configurable if **SNMP Access** is enabled.
Email Format	Select the format for the email. This format will be used when sending emails. The two type or formats available are: • AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content includes sensor information, such as Sensor type and Description. • FixedSubject-Format: This format displays the specific subject and message configured for email alerts for the specific user.
Email ID	Enter the email ID for the user. If the user forgets the password, a new password will be mailed to this email ID.  The SMTP Server must also be configured for this option. The Maximum allowed size for the Email ID is 64 bytes (including username and domain name).
Existing SSH Key	If available, the uploaded SSH key information will be displayed (read only).
Upload SSH Key	Click the Browse button and navigate to the new public SSH key file.  SSH Key file should be of pub type.

3.7.15 Video Recording

This page allows you to customize the video recording settings.

Auto Video Settings

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

- **Video Trigger Settings**
  This page allows you to configure the video recording triggers.

Critical Events (Temperature/Voltage)	You can check/uncheck a box on the Event List to add/remove that trigger for your system. KVM service should be enabled to perform auto-video recording. The date and time event should be in advance of the current system date and time.
Non Critical Events (Temperature/Voltage)	
Non Recoverable Events (Temperature/Voltage)	
Fan state changed Events	
Watchdog Timer Events	
Chassis Power On Events	
Chassis Power Off Events	
Chassis Reset Events	
LPC Reset Events	
Date and Time Event	
Pre-Event Video Recording	Pre-Event Video Recording information.

- **Video Remote Storage**
  This page allows you to configure video remote storage settings.

Record Video to Remote Server	Enable or disable Remote Video support. By default, video files will be stored in the local path of the BMC. If remote video support is enabled, then the video files will be stored only to the remote path, and not within the BMC.
Maximum Dumps	The maximum dumps value should range from 1 to 100. This item is only configurable if **Record Video to Remote Server** is enabled.

(continued on the next page)

Maximum Duration (Sec)	The maximum duration should range from 1 to 3600 seconds. This item is only configurable if **Record Video to Remote Server** is enabled.
Maximum Size (MB)	The maximum size should range from 1 to 500 MB. This item is only configurable if **Record Video to Remote Server** is enabled.
Server Address	Enter the IP address of the server where the remote videos are to be stored. • IPV4 and IPV6 address formats, and FQDN (Fully Qualified Domain Name) format is supported. • This item is only configurable if **Record Video to Remote Server** is enabled.
Path in server	Enter the path of the remote media on the server. • Path must be alpha-numeric and only the following special characters are allowed: '**/**' (backward slash), '\' (forward slash), '**-**' (hyphen), '_' (underscore), '**.**' (dot), and '**:**' (colon). • This item is only configurable if **Record Video to Remote Server** is enabled.
Share Type	Select the share type of the remote server. **NFS** or Samba (**CIFS**) are supported.

- **Pre-Event Video Recordings**
  This page is used to configure the Pre-Event video recording options.

- **Pre-Event Video Recordings** is disabled by default, to enable **Pre-Event Video Recordings**, please go to the **Video Trigger Settings** page.
- Disable/Enable the **Pre-Event Video Recording** on the **Video Trigger Settings** page for the newly modified configurations to take effect.

Video Quality	Select the video quality.
Compression Mode	Select the compression mode.
Frames Per Second	Select the frames per second (FPS).
Video Duration	Select the duration of the video recording (seconds)

SOL Settings

The Java SOL page allows you to configure trigger settings for SOL video recording events.

- **SOL Trigger Settings**
  This page allows you to configure which events will trigger the SOL video.

Critical Events (Temperature/Voltage)	You can check/uncheck a box on the Event List to add/remove that trigger for your system.
Non Critical Events (Temperature/Voltage)	
Non Recoverable Events (Temperature/Voltage)	
Fan state changed Events	
Watchdog Timer Events	
Chassis Power On Events	
Chassis Power Off Events	
Chassis Reset Events	
LPC Reset Events	
Date and Time Event	

The date and time event should be in advance of the current system date and time.

- **SOL Video Settings**
  This page allows you to configure SOL video settings.

Log Size (KB)	Enter the preferred size of the log file. Maximum log file size is 128 KB.
Log File Count	Enter whether you want to have log files. Maximum log file count is 1.
Record Video to Remote Server	Enable or disable Remote Video support.

By default, video files will be stored in the local path of the BMC. If remote video support is enabled, then the video files will be stored only to the remote path, and not within the BMC.

- **SOL Recorded Video**
  This page displays the list of SOL recorded video(s).

- By default, the video files will be stored in the local path of the BMC. If remote video support is enabled, then the video files will be stored only to the remote path, and not within the BMC.
- Click on the icon to download and save the file.
- Click on the **x** icon to delete the selected video from the list.

3.7.16 Fan Control

This page allows you to set the fan control configurations.

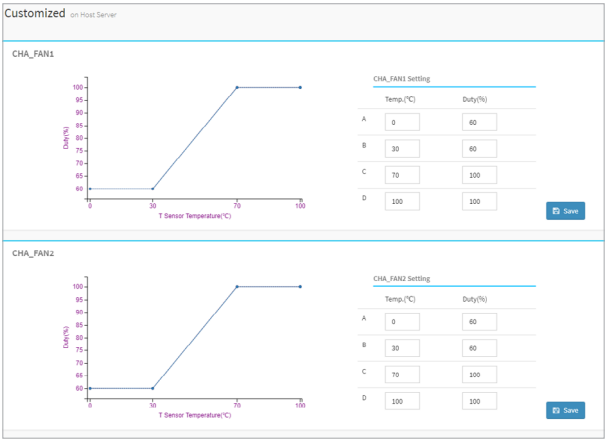
Auto Mode

This page allows you to view the current fan mode, and also configure the fan mode.

Generic mode	Select this option to set the fan mode to generic mode.
Full speed mode	Select this option to set the fan mode to full speed mode.

Customizedf

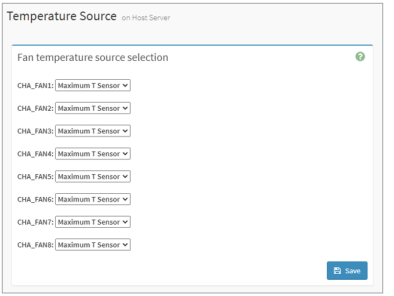
This page allows you to configure fan duty corresponding to different temperatures.



Temperature Source

This page allows you to select a desired temperature source to control your fan. If no temperature is obtained, the CPU temperature will be used. If CPU temperature is not obtained, fan control will be set to 60%. These settings will also be applied to every fan in control mode.

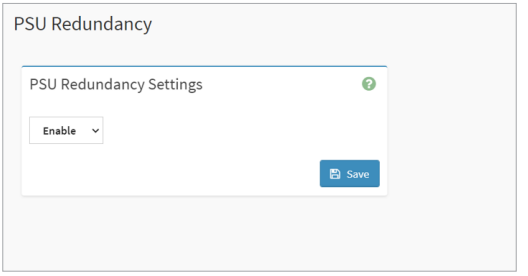
To use the CHA FAN sensor and control function, ensure the fans are connected to the **Fan headers 1-8**, and the **6-pin PSU connector** is connected to a power supply.



3.7.17 PSU Redundancy

This page allows you to configure PSU redundancy settings, allowing you to focus system power consumption on one PSU device for improved power efficiency.

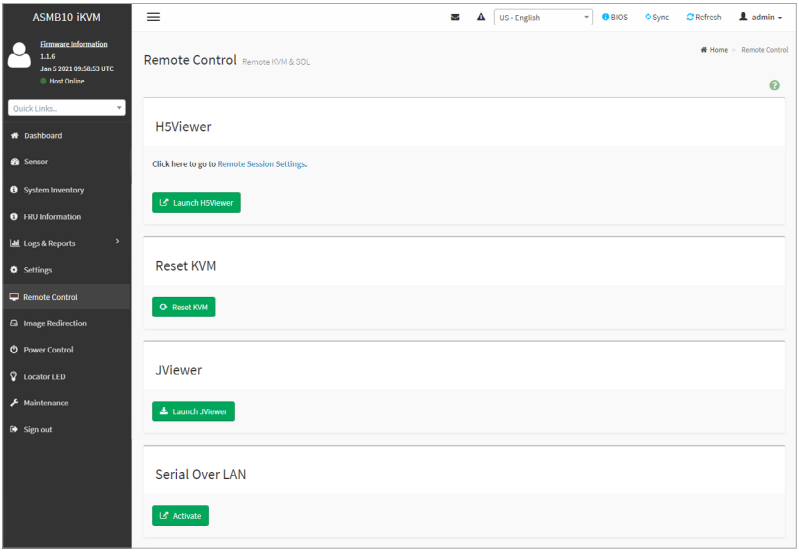
PSU will start balancing power when system is in heavy loading.



Enable	Enable PSU redundancy.
Disable	Disable PSU redundancy.

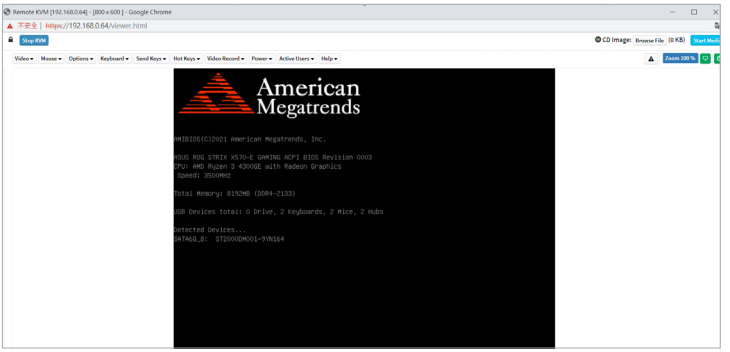
3.8 Remote Control

This menu allows you to perform remote operations on the server. Click **Launch H5Viewer** to start the remote KVM.



H5Viewer	Click to launch the H5Viewer window for the KVM function.
Reset KVM	Click to reset the KVM function.
JViewer	Click to download the jviewer (.jnlp) file. • Download and install IcedTea Windows x64 if you wish to open the jviewer (.jnlp) file. • Launch the Command Prompt (CMD) as administrator, then use the command line to execute the Java Web Start exe file and the corresponding .jnlp file to use the JViewer function.
Serial Over LAN	Click to launch the HTML Serial Over LAN window.

Remote KVM interface



Video	**Pause Video**	This option is used for pausing Console Redirection.
	Resume Video	This option is used to resume the Console Redirection when the session is paused.
	Refresh Video	This option can be used to update the display shown in the Console Redirection window.
	Host display	If you turn this option ON, the client device's screen will be unlocked. If you turn this option OFF, the client device's screen will be locked.
	Capture Screen	This option allows you to screen capture the console redirection screen.
Mouse	**Show Client Cursor**	This option can be used to show or hide the local mouse cursor on the remote client system.
	Mouse Mode	This option allows you to select the mode or type of mouse support: - Absolute Mouse Mode - Relative Mouse Mode - Other Mouse Mode
Options	**Zoom**	This option allows you to adjust the zoom on the KVM screen: - Normal - Zoom In - Zoom Out
	Block Privilege Request	This option allows you to block privilege requests: - Partial Permission - No Permission

(continued on the next page)

Options	**Bandwidth**	This option allows you to select the console redirection bandwidth: - Auto Detect - 256 kbps - 512 kbps - 1 Mbps - 10 Mbps - 100 Mbps
	Compression Mode	This option allows you to select the YUV: - YUV 420 - YUV 444 - YUV 444 + 2 color VQ - YUV 444 + 4 color VQ
	DCT Quantization table	This option allows you to set the quality that ranges from 0 (Best Quality) to 7 (Worst Quality).
Keyboard		This option allows you to select the keyboard layout: - English U.S - German - Japanese
Send Keys	**Hold Down**	This option can be used to act as holding down the corresponding key when in Console Redirection: - Right Ctrl Key - Right Alt Key - Right Windows Key - Left Ctrl Key - Left Alt Key - Left Windows Key
	Press and Release	This option can be used to act as a press and release on the corresponding key when in Console Redirection: - Ctrl + Alt + Del - Left Windows Key - Right Windows Key - Context Menu Key - Print Screen Key
Hot Keys	**Add Hot Keys**	This option allows you to add a new hotkey. Click on **Add Hot Keys** > **Add**, then place the cursor in the text box and press then release the key event combination to define a macro. 

(continued on the next page)

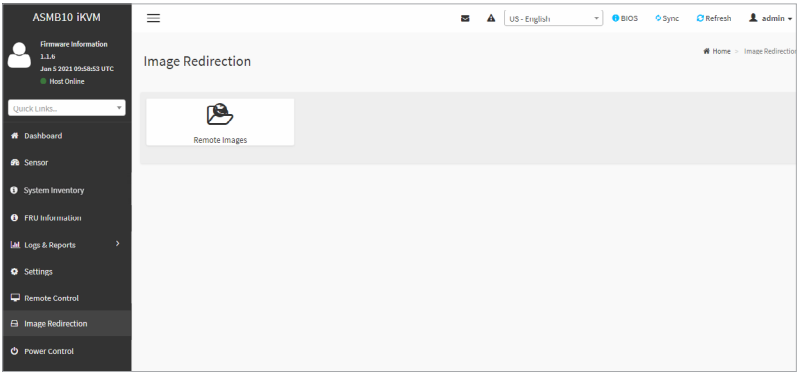
Video Record	**Record Video**	This option allows you to start recording the console redirection screen.
	Stop Recording	This option allows you to stop recording the console redirection screen.
	Record Settings	This menu item allows you to configure the video recording settings.
Power		This option allows you to change the power settings. Click the desired option to execute the selected action: - Reset Server - Immediate shutdown - Orderly shutdown - Power On Server - Power Cycle Server
Active Users		This option will display the currently active users on the server.
Help		This option will provide more information on H5Viewer.
Browse File		Click this button to add or modify a CD media, then click **Start Media** to start or stop the redirection of a physical DVD/CD-ROM drive and CD image types such as iso.
Start Media		Click this button to start or stop the newly added or modified redirection media file.

Remote Control functions

	Display all received notifications.
	Display the KVM display's current zoom.
	Display whether the client device's screen is locked or unlocked.
	Perform a power control action on the client device.

3.9 Image Redirection

This menu allows you to emulate CD/DVD/HDD Images as media drives to host.



Remote Images

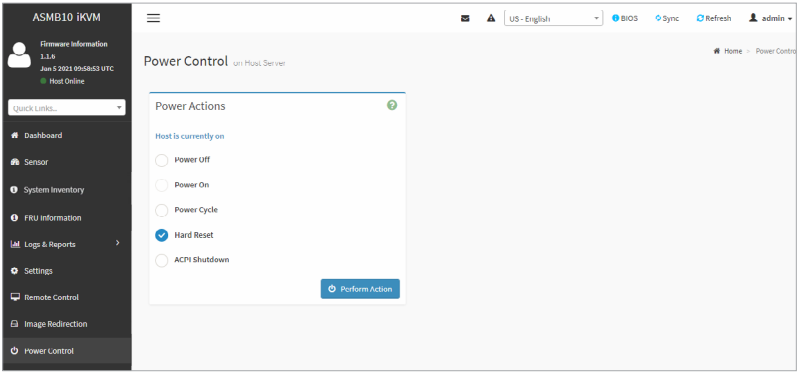
This page allows you to select a remote media to emulate to host as media through BMC. The displayed table shows remote images available to the BMC. You can start redirection, or clear images from here.

Start/Stop Redirection	Click on the Play button to redirect the selected image.
	Click on the Stop button to stop the remote image redirection.
Clear	Click the Clear button to clear the selected image from the BMC.
Refresh Image List	Click the Refresh Image List button to get the latest list of images from the remote storage server.
Sync Image Status	Click the Sync Image Status button to turn on/off the redirection status of images from the BMC.

- Up to 4 images can be added for each image type, depending on the configuration.
- To configure the image, you need to enable **Remote Media Support** in **Settings** > **Media Redirection** > **General Settings**.
- To start redirection or clear an image, you must have Administrator privileges.
- Supported CD/DVD format: ISO9660, UDF(v1.02~v2.60)
- Supported CD/DVD media file type: (*.iso), (*.nrg)
- Supported HDD media file type: (*.img), (*.ima)

3.10 Power Control

The Power Control 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.

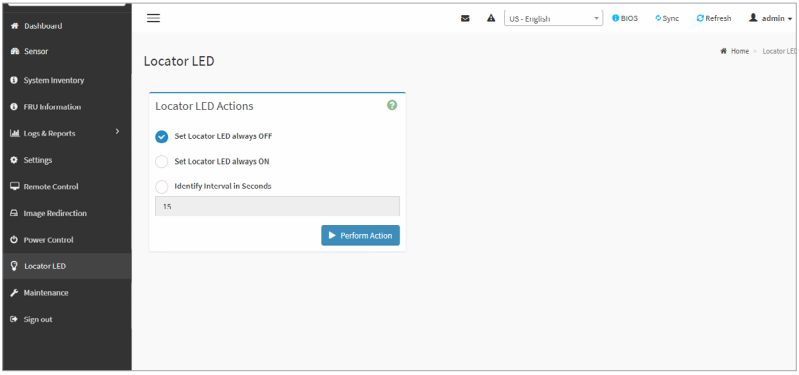


Power Off	Immediately power off the remote device.
Power On	Power on the remote device.
Power Cycle	Turn off the power then reboot the remote device (cold boot).
Hard Reset	Reboot the system without powering off (warm boot).
ACPI Shutdown	Initiate operating system shutdown prior to the shutdown.

To use the power on/off and reset function, ensure the **PANEL header** is connected to the motherboard and the chassis panel.

3.11 Locator LED

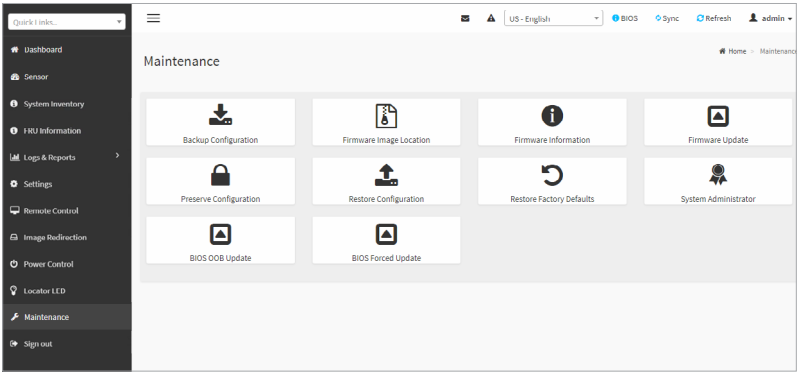
The Locator LED allows you to perform a chassis identify command control operation. Select the desired LED locator LED behavior, or select the **Identify Interval in Seconds** option and enter the amount of seconds, then click **Perform Action** to execute the selected action.



Set Locator LED always OFF	Turn off the Locator LED. Once it is off, the LED will blink.
Set Locator LED always ON	Turn on the Locator LED. Once it is on, the LED will stay lit up.
Identify Interval in Seconds	Enter the identify interval in seconds then press **Perform Action** to perform a chassis identify command control operation.

3.12 Maintenance

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



Backup Configuration

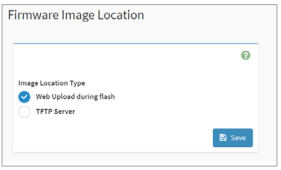
This page allows you to select specific configuration items to backup. Check the desired items and click **Download Config** to download the .bak file.

Check All	Check all items.
SNMP	Check the item that needs to be backed up.
KVM	
Network & Services	
IPMI	
NTP	
Authentication	
SYSLOG	

- You will be able to save the backup config file to a location of your choice. That saved file can be used to restore the configuration when needed.
- Network configurations are inter-related to IPMI, hence, by default, **IPMI** configurations will be selected automatically when you check the **Network & Services** box and vice versa.

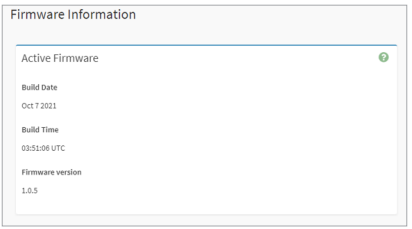
Firmware Image Location

This page allows you to select the protocol (**Web Upload during flash**, **TFTP Server**) to be used to transfer the firmware image onto the BMC.



Firmware Information

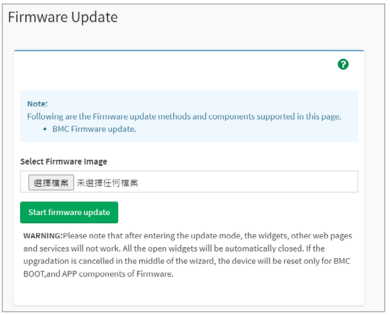
This page displays the Build Date, Build Time, and Firmware Version of the active BMC image.



Build Date	Displays the build date of the active BMC image.
Build Time	Displays the build time of the active BMC image.
Firmware version	Displays the firmware version of the active BMC image.

Firmware Update

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

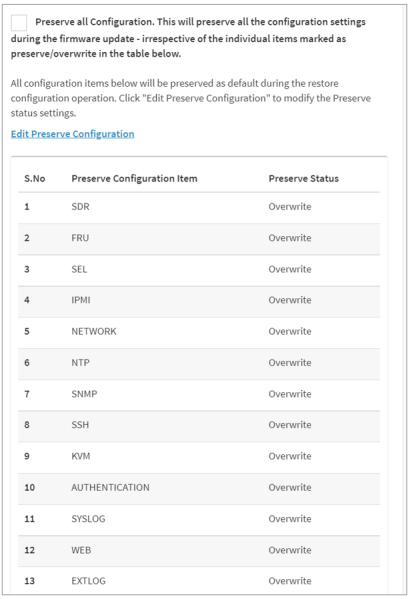


To update the firmware, please follow the steps below:

1. Browse and select the firmware image file (.ima) you wish to use to update the firmware.
2. Click on **Start firmware update**.

3. Uncheck (default option) or check the **Preserve all Configuration** option. If left unchecked all configurations will be overwritten when updating the firmware, else checking this option will preserve all configurations when updating the firmware. You can also click on **Edit Preserve Configuration** to select configurations to preserve if you wish to only preserve selected configurations.

Some functions may be affected after updating the firmware if you chose to preserve all configurations or some configurations, due to the preserved items not being updated.



4. Click on **Proceed to Flash**, then click **OK** on the pop-up window.
5. The Section Firmware Update will display and compare the existing version and uploaded version. You can on check **Version Compare Flash** then select which sections to update by checking that section, or check **Full Flash** to update all sections.
6. Click on **Flash selected sections** to begin flashing the selected sections.

- After entering the update mode, the widgets, other web pages and services will not work. All open widgets will be automatically closed. If the upgrade is cancelled in the middle of the update, the device will be reset only for BMC, BOOT, and APP components of the firmware. A system reset is required for the device to work normally.
- Please refresh the Web GUI and set the client device's BMC administrator password again after the BMC firmware has finished updating.

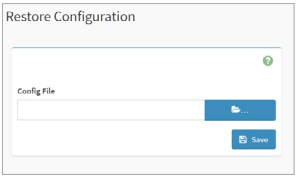
Preserve Configuration

This page allows you to select specific configuration items to be preserved in while performing **Restore Factory Defaults** or **Firmware Update** functions.

Check All	Check this option to check all configuration items on the list.
SDR	Check configuration items to preserve the item when restoring factory defaults or updating firmware. Uncheck configuration items to overwrite the item when restoring factory defaults or updating firmware. Network configurations are inter-related to IPMI, hence, by default, **IPMI** configurations will be selected automatically when you check the **Network** box and vice versa.
FRU	
SEL	
IPMI	
Network	
NTP	
SNMP	
SSH	
KVM	
Authentication	
Syslog	
Web	
Extlog	
Redfish	
Fan	

Restore Configuration

This page allows you to select and upload a .bak file to restore the configuration settings.



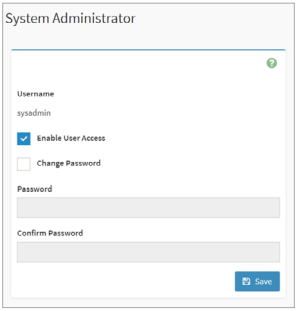
Restore Factory Defaults

This page allows you to view configuration items that will be preserved while all the other configuration items will be restored to their default values. If none are selected, all the configuration items will be restored to their default values, essentially restoring the device configuration to its factory defaults.

- You can modify the checked/unchecked configuration items on the **Preserve Configuration** page.
- After restoring the factory defaults, the Web-based user interface screen will become white and you will be automatically logged out of the Web-based user interface.

System Administrator

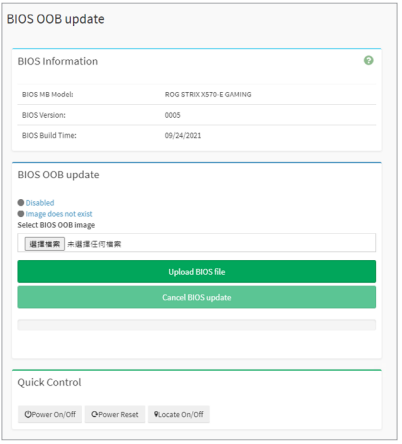
This page allows you to change the System Administrator settings.



Username	Displays the username of the system administrator (read-only).
Enable User Access	Enable or disable user access for the system administrator.
Change Password	Check this option to change the existing password.
Password	Enter the new password. • Must be at least 8 characters long and may not exceed 64 characters. • White space is not allowed. • This item is only configurable if **Change password** is enabled.
Confirm Password	Confirm the password by entering it again in this field. This item is only configurable if **Change password** is enabled.

BIOS OOB Update

This page allows you to view the BIOS information and perform a BIOS OOB update.



BIOS Information		Displays the current BIOS information (**BIOS MB Model**, **BIOS Version**, **BIOS Build Time**) for the remote device.
BIOS OOB Update		Select the BIOS image file you wish to use for the update, then click **Upload BIOS file** and perform the BIOS OOB update.
Quick Control	**Power On/Off**	Perform the quick control command selected.
	Power Reset	
	Locate On/Off	

To update the BIOS OOB, please follow the steps below:

1. Click on Browse, then select the BIOS image file (.cap) you wish to use for the update.

BIOS firmware only supports .cap files.

2. Click on **Upload BIOS file** to activate local media and mount the BIOS file into the virtual storage after a reset.
3. After the file has been successfully uploaded, click on **Power Reset** in the **Quick Control** block.
4. After resetting, the host will detect that a BIOS update is available and search the virtual storage for the BIOS file and perform the BIOS update.

BIOS Forced Update

This page allows you to select a BIOS image file and force the BIOS update of the current device through BMC when the client device cannot.

Only use the force BIOS update function when there is an error with the client device's BIOS and the BIOS information cannot be retrieved.

To force update the BIOS, please follow the steps below:

1. Click on Browse, then select the BIOS image file (.rom) you wish to use for the update.

BIOS force update only supports .rom files.

2. Click on **Start BIOS update**, then click **OK** on the confirmation window to begin the force update.

To use the force BIOS update function, ensure the **SPI header** is connected to the IPMI TPM header on the motherboard.

Clear MB CMOS

This page allows you to restore the client device's BIOS to factory settings.

- The Clear MB CMOS function is only available if the client device's motherboard supports this function.
- The Clear MB CMOS function can only be used when the client device is powered off.

To clear the motherboard's CMOS, please follow the steps below:

1. Click on **Perform Action**.
2. Click **OK** on the confirmation window.

Appendix

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

A.1 IPMITool help commands

Command	Description
raw	Send a RAW IPMI request and print response.
i2c	Send an I2C Master Write-Read command and print response.
spd	Print SPD info from remote I2C device.
lan	Configure LAN Channels.
chassis	Get chassis status and set power state.
power	Shortcut to chassis power commands.
event	Send pre-defined events to MC.
mc	Management Controller status and global enables.
sdr	Print Sensor Data Repository entries and readings.
sensor	Print detailed sensor information.
fru	Print built-in FRU and scan SDR for FRU locators.
gendev	Read/Write Device associated with Generic Device locators sdr.
sel	Print System Event Log (SEL).
pef	Configure Platform Event Filtering (PEF).
sol	Configure and connect IPMIv2.0 Serial-over-LAN.
tsol	Configure and connect with Tyan IPMIv1.5 Serial-over-LAN.
isol	Configure IPMIv1.5 Serial-over-LAN.
user	Configure Management Controller users.
channel	Configure Management Controller channels.
session	Print session information.
sunoem	OEM Commands for Sun servers.
kontronoem	OEM Commands for Kontron devices.
picmg	Run a PICMG/ATCA extended cmd.
fwum	Update IPMC using Kontron OEM Firmware Update Manager.
firewall	Configure Firmware Firewall.
exec	Run list of commands from file.
set	Set runtime variable for shell and exec.
hpm	Update HPM components using PICMG HPM.1 file.
ekanalyzer	Run FRU-Ekeying analyzer using FRU files.
ime	Update Intel Manageability Engine Firmware.
vita	Run a VITA 46.11 extended cmd.
lan6	Configure IPv6 LAN Channels.

A.2 Common IPMITool commands

Operation commands should include the client device's BMC IP address. To view the client device's BMC IP address, please enter the client device's BIOS setting > **Server Mgmt** > **BMC network configuration**, the BMC IP address can be found in this sub-menu.

Command option	Description
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) mc info`	View BMC information.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) lan print (ChannelNo)`	View network configuration.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) lan set (ChannelNo) ipsrc <static/dhcp>`	Set the IP as Static/DHCP mode.
`ipmitool -H (BMC IPaddress) -I lanplus -U (username) -P (password) lan set (ChannelNo) ipaddr <IPAddress>`	Configure IP address.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) lan set (ChannelNo) netmask <NetMask>`	Configure Subnet mask.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) lan set (ChannelNo) defgw ipaddr <DefaultGateway>`	Configure default gateway.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) chassis status`	View status of chassis power supply and fan(s).
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) power status`	View power status.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) power on`	Power on.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) power off`	Power off.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) power reset`	Hard reset.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) power cycle`	View power cycle.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) user list (ChannelNo)`	View user information.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) user set name <user id> <username>`	Add user. Set `<user id>` to `1` for anonymous user, and `2` for administrator.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) user set password <user id> <password>`	Set user password.

(continued on the next page)

Command option	Description
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) user priv <user id> <privilege level>	Set user privileges. Set <privilege level> to 2 for user level permissions, 3 for operator level permissions, and 4 for administrator level permissions.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) user enable/disable <user id>	Enable/Disable user.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sol activate	Activate SOL function.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sol deactivate	Deactivate SOL function.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sel info	View SEL information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sel list	View SEL records.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sel elist	View detailed SEL records.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sel clear	Clear SEL records.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) fru list	View FRU information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) raw 0x30 0x17 0x01	Unlock FRU.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) fru write (FRU channel to write)(FRU bin file to write to)	Write FRU information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) fru print	Print FRU information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sdr list	View SDR Sensor information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) sensor list	View Sensor information.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) mc reset <warm/cold>	Reset BMC.
ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) raw 0x30 0x96 [PSU1 address] [PSU2 address] [PSU3 address] [PSU4 address]	Set PSU address.

(continued on the next page)

Command option	Description
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) raw 0x30 0x96`	Get PSU address.
`ipmitool -H (BMC IP address) -I lanplus -U (username) -P (password) raw 0x30 0x98`	Get BMC hardware version.

A.3 Troubleshooting

This troubleshooting guide provides answers to some common problems that you may encounter while installing and/or using the IPMI Expansion Card. 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 IPMI Expansion Card.	1. Make sure the IPMI Expansion Card is installed correctly onto the client device's motherboard, and the LED indicators on the IPMI Expansion Card light up when the client device is powered on. 2. Check if the LAN cable is properly connected to the LAN port on the IPMI Expansion Card and the local/central server's LAN port. 3. Check the network and parameter settings of the client device's BMC remote management controller card. Please refer to **2.3.4 BMC network configuration** for more details. 4. Make sure that the IP address of both the remote and local/central servers are on the same subnet.
The Web-based user interface shows a VERSION_ERR message, and the LED indicator on the IPMI Expansion card lights up orange.	1. Check if the BIOS of the client device's motherboard supports the version of the IPMI Expansion Card. 2. If you are updating the firmware of the IPMI Expansion Card, make sure to restart the client device's system after the update has been completed.
The date/time shown on the SEL (System Event Log) screen is incorrect.	1. The system event logs will display the default date/time if there was no network connection when the BMC remote device was turned on. 2. Go to **Settings** > **Date & Time**, and make sure the time zone, date, and time are correct.
Certain sensor readings on the Sensors page are not updating for specific platforms.	Temperature, processor, hard disks, and memory only update when turning on the remote device and will not update over time.

(continued on the next page)

Problem	Solution
Some sensors are not creating event logs, even after the Sensors have been configured.	1. The UNC/UC/UNR of the fan will not create an event log when the rotation speed exceeds the upper threshold 2. The temperature's LNR / LC / LNC will not create an event log when the temperature drops below the lower threshold. 3. You can view the UNR / LNR values of the sensors, but no event log will be created if the sensor's UNR exceeds the upper threshold or if the sensor's LNR drops below the lower threshold.
Some items do not display any information when viewing the FRU information.	FRU information can be written using IPMITool commands, for more information on IPMITool commands, please refer to **3.5 FRU Information** or the **Appendix**.
The firewall is not functioning according to the settings configured.	Make sure to set the BMC system time before configuring the firewall. This will ensure the date and time of the configured firewall rule is working properly.
Any precautions before using the firmware update function?	1. You may choose between overriding all configurations, preserving all configurations, or selecting and editing specific options as preserved configurations when using the firmware update function: - (default) Uncheck **Preserve all Configurations** to override all configurations when updating the firmware. - Check **Preserve all Configurations** to preserve all configurations when updating the firmware. The configurations will not be updated. - Edit and select specific items to be preserved when updating the firmware. 2. Some functions may have incomplete functionality due to it not being updated if **Preserve all Configurations** is checked, or if the item was selected to be preserved when updating the firmware, 3. You can compare the current version and the uploaded version then select which sections to update or check update all on the section firmware update page.

(continued on the next page)

Problem	Solution
How do you perform an update after selecting and uploading the BIOS when executing BIOS OOB update.	Click on power restart from the shortcut menu after uploading the BIOS file, the BIOS OOB will automatically update after the client device has restarted.

Notices

FCC Compliance Information

Responsible Party: Asus Computer International

Address: 48720 Kato Rd., Fremont, CA 94538, USA

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

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

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 the 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 into 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.

HDMI Trademark Notice

The terms HDMI, HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.

Compliance Statement of Innovation, Science and Economic Development Canada (ISED)

This device complies with Innovation, Science and Economic Development Canada licence exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-003(B)/NMB-003(B)

Déclaration de conformité de Innovation, Sciences et Développement économique Canada (ISED)

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-003(B)/NMB-003(B)

VCCI: Japan Compliance Statement

Class B ITE

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

ＶＣＣＩ－Ｂ

Japan JATE

本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線LANを含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルーター等を経由し接続してください。

KC: Korea Warning Statement

B급 기기 (가정용 방송통신기자재)
이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Google™ License Terms

Declaration of compliance for product environmental regulation

ASUS follows the green design concept to design and manufacture our products, and makes sure that each stage of the product life cycle of ASUS product is in line with global environmental regulations. In addition, ASUS disclose the relevant information based on regulation requirements.

Please refer to http://csr.asus.com/Compliance.htm for information disclosure based on regulation requirements ASUS is complied with:

EU REACH and Article 33

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

EU RoHS

This product complies with the EU RoHS Directive. For more details, see http://csr.asus.com/english/article.aspx?id=35

India RoHS

This product complies with the “India E-Waste (Management) Rules, 2016” and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls (PBBs) and polybrominated diphenyl ethers (PBDEs) in concentrations exceeding 0.1% by weight in homogenous materials and 0.01% by weight in homogenous materials for cadmium, except for the exemptions listed in Schedule II of the Rule.

Vietnam RoHS

ASUS products sold in Vietnam, on or after September 23, 2011,meet the requirements of the Vietnam Circular 30/2011/TT-BCT.

Các sản phẩm ASUS bán tại Việt Nam, vào ngày 23 tháng 9 năm2011 trở về sau, đều phải đáp ứng các yêu cầu của Thông tư 30/2011/TT-BCT của Việt Nam.

Turkey RoHS

AEEE Yönetmeliğine Uygundur

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.

Australia statement notice

From 1 January 2012 updated warranties apply to all ASUS products, consistent with the Australian Consumer Law. For the latest product warranty details please visit https://www.asus.com/support/. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

If you require assistance please call ASUS Customer Service 1300 2787 88 or visit us at https://www.asus.com/support/.

Simplified EU Declaration of Conformity

English ASUSTeK Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related Directives. Full text of EU declaration of conformity is available at: www.asus.com/support

Français AsusTek Computer Inc. déclare par la présente que cet appareil est conforme aux critères essentiels et autres clauses pertinentes des directives concernées. La déclaration de conformité de l'UE peut être téléchargée à partir du site Internet suivant : www.asus.com/support.

Deutsch ASUSTeK Computer Inc. erklärt hiermit, dass dieses Gerät mit den wesentlichen Anforderungen und anderen relevanten Bestimmungen der zugehörigen Richtlinien übereinstimmt. Der gesamte Text der EU-Konformitätserklärung ist verfügbar unter: www.asus.com/support

Italiano ASUSTeK Computer Inc. con la presente dichiara che questo dispositivo è conforme ai requisiti essenziali e alle altre disposizioni pertinenti con le direttive correlate. Il testo completo della dichiarazione di conformità UE è disponibile all'indirizzo: www.asus.com/support

Русский Компания ASUS заявляет, что это устройство соответствует основным требованиям и другим соответствующим условиям соответствующих директив. Подробную информацию, пожалуйста, смотрите на www.asus.com/support

Български С настоящото ASUSTeK Computer Inc. декларира, че това устройство е в съответствие със съществените изисквания и другите приложими постановления на свързаните директиви. Пълният текст на декларацията за съответствие на ЕС е достъпна на адрес: www.asus.com/support

Hrvatski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj sukladan s bitnim zahtjevima i ostalim odgovarajućim odredbama vezanih direktiva. Cijeli tekst EU izjave o sukladnosti dostupan je na: www.asus.com/support

Čeština Společnost ASUSTeK Computer Inc. tímto prohlašuje, že toto zařízení splňuje základní požadavky a další příslušná ustanovení souvisejících směrnic. Plné znění prohlášení o shodě EU je k dispozici na adrese: www.asus.com/support

Dansk ASUSTeK Computer Inc. erklærer hermed, at denne enhed er i overensstemmelse med hovedkravene og andre relevante bestemmelser i de relaterede direktiver. Hele EU-overensstemmelseserklæringen kan findes på: www.asus.com/support

Nederlands ASUSTeK Computer Inc. verklaart hierbij dat dit apparaat voldoet aan de essentiële vereisten en andere relevante bepalingen van de verwante richtlijnen. De volledige tekst van de EU-verklaring van conformiteit is beschikbaar op: www.asus.com/support

Eesti Käesolevaga kinnitab ASUSTeK Computer Inc, et see seade vastab asjakohaste direktiivide oluliste nõuetele ja teistele asjassepuutuvatele sätetele. EL vastavusdeklaratsiooni täielik tekst on saadaval järgmisel aadressil: www.asus.com/support

Suomi ASUSTeK Computer Inc. ilmoittaa täten, että tämä laite on asiaankuuluvien direktiivien olennaisten vaatimusten ja muiden tätä koskevien säädösten mukainen. EU-yhdenmukaisuusilmoituksen koko teksti on luettavissa osoitteessa: www.asus.com/support

Ελληνικά Με το παρόν, η AsusTek Computer Inc. δηλώνει ότι αυτή η συσκευή συμμορφώνεται με τις θεμελιώδεις απαιτήσεις και άλλες σχετικές διατάξεις των Οδηγιών της ΕΕ. Το πλήρες κείμενο της δήλωσης συμβατότητας είναι διαθέσιμο στη διεύθυνση: www.asus.com/support

Magyar Az ASUSTeK Computer Inc. ezennel kijelenti, hogy ez az eszköz megfelel a kapcsolódó Irányelvek lényeges követelményeinek és egyéb vonatkozó rendelkezéseinek. Az EU megfelelőségi nyilatkozat teljes szövege innen letölthető: www.asus.com/support

Latviski ASUSTeK Computer Inc. ar šo paziņo, ka šī ierīce atbilst saistīto Direktīvu būtiskajām prasībām un citiem citiem saistošajiem nosacījumiem. Pilns ES atbilstības paziņojuma teksts pieejams šeit: www.asus.com/support

Lietuvių „ASUSTeK Computer Inc." šiuo tvirtina, kad šis įrenginys atitinka pagrindinius reikalavimus ir kitas svarbias susijusių direktyvų nuostatas. Visą ES atitikties deklaracijos tekstą galima rasti: www.asus.com/support

Norsk ASUSTeK Computer Inc. erklærer herved at denne enheten er i samsvar med hovedsaklige krav og andre relevante forskrifter i relaterte direktiver. Fullstendig tekst for EU-samsvarserklæringen finnes på: www.asus.com/support

Polski Firma ASUSTeK Computer Inc. niniejszym oświadcza, że urządzenie to jest zgodne z zasadniczymi wymogami i innymi właściwymi postanowieniami powiązanych dyrektyw. Pełny tekst deklaracji zgodności UE jest dostępny pod adresem: www.asus.com/support

Português A ASUSTeK Computer Inc. declara que este dispositivo está em conformidade com os requisitos essenciais e outras disposições relevantes das Diretivas relacionadas. Texto integral da declaração da UE disponível em: www.asus.com/support

Română ASUSTeK Computer Inc. declară că acest dispozitiv se conformează cerinţelor esenţiale şi altor prevederi relevante ale directivelor conexe. Textul complet al declaraţiei de conformitate a Uniunii Europene se găseşte la: www.asus.com/support

Srpski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj u saglasnosti sa osnovnim zahtevima i drugim relevantnim odredbama povezanih Direktiva. Pun tekst EU deklaracije o usaglašenosti je dostupan da adresi: www.asus.com/support

Slovensky Spoločnosť ASUSTeK Computer Inc. týmto vyhlasuje, že toto zariadenie vyhovuje základným požiadavkám a ostatým príslušným ustanoveniam príslušných smerníc. Celý text vyhlásenia o zhode pre štáty EÚ je dostupný na adrese: www.asus.com/support

Slovenščina ASUSTeK Computer Inc. izjavlja, da je ta naprava skladna z bistvenimi zahtevami in drugimi ustreznimi določbami povezanih direktiv. Celotno besedilo EU-izjave o skladnosti je na voljo na spletnem mestu: www.asus.com/support

Español Por la presente, ASUSTeK Computer Inc. declara que este dispositivo cumple los requisitos básicos y otras disposiciones pertinentes de las directivas relacionadas. El texto completo de la declaración de la UE de conformidad está disponible en: www.asus.com/support

Svenska ASUSTeK Computer Inc. förklarar härmed att denna enhet överensstämmer med de grundläggande kraven och andra relevanta föreskrifter i relaterade direktiv. Fulltext av EU-försäkran om överensstämmelse finns på: www.asus.com/support

Українська ASUSTeK Computer Inc. заявляє, що цей пристрій відповідає основним вимогам та іншим відповідним положенням відповідних Директив. Повний текст декларації відповідності стандартам ЄС доступний на: www.asus.com/support

Türkçe AsusTek Computer Inc., bu aygıtın temel gereksinimlerle ve ilişkili Yönergelerin diğer ilgili koşullarıyla uyumlu olduğunu beyan eder. AB uygunluk bildiriminin tam metni şu adreste bulunabilir: www.asus.com/support

Bosanski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj usklađen sa bitnim zahtjevima i ostalim odgovarajućim odredbama vezanih direktiva. Cijeli tekst EU izjave o usklađenosti dostupan je na: www.asus.com/support

Simplified UKCA Declaration of Conformity

ASUSTek Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of The Radio Equipment Regulations 2017 (S.I. 2017/1206). Full text of UKCA declaration of conformity is available at https://www.asus.com/support/.

Warranty

EN: ASUS Guarantee Information

- ASUS offers a voluntary manufacturer's Commercial Guarantee.
- ASUS reserves the right to interpret the provisions of the ASUS Commercial Guarantee.
- This ASUS Commercial Guarantee is provided independently and in addition to the statutory Legal Guarantee and in no way affects or limits the rights under the Legal Guarantee.

For all the guarantee information, please visit https://www.asus.com/support.

F: Garantie ASUS

- ASUS fournit une garantie commerciale en tant que garantie volontaire du fabricant.
- ASUS se réserve le droit d'interpréter et de clarifier les informations relatives à la garantie commerciale ASUS.
- Cette garantie commerciale ASUS est fournie indépendamment et parallèlement à la garantie légale, elle n'affecte ou ne limite d'aucune façon les droits acquis par la garantie légale.

Pour plus d'informations sur la garantie, consultez le site https://www.asus.com/fr/support/.

G: ASUS Garantieinformationen

- ASUS bietet eine freiwillige Warengarantie des Herstellers an.
- ASUS behält sich das Recht zur Auslegung der Bestimmungen in der ASUS Warengarantie vor.
- Diese ASUS Warengarantie wird unabhängig und zusätzlich zur rechtmäßigen gesetzlichen Garantie gewährt und beeinträchtigt oder beschränkt in keiner Weise die Rechte aus der gesetzlichen Garantie.

Die vollständigen Garantieinformationen finden Sie unter https://www.asus.com/de/support/.

I: Informativa sulla Garanzia ASUS

- ASUS offre una Garanzia Commerciale volontaria del produttore.
- ASUS si riserva il diritto di interpretare le disposizioni della Garanzia Commerciale ASUS.
- La presente Garanzia Commerciale ASUS viene fornita in modo indipendente e in aggiunta alla Garanzia Legale prevista per legge e non pregiudica o limita in alcun modo i diritti previsti dalla Garanzia Legale.

Per tutte le informazioni sulla garanzia, visitare https://www.asus.com/it/support.

R: Информация о гарантии ASUS

- ASUS предлагает добровольную гарантию от производителя.
- ASUS оставляет за собой право интерпретирование положений гарантии ASUS.
- Настоящая гарантия ASUS никоим образом не ограничивает Ваши права, предусмотренные локальным законодательством.

Для получения полной информации о гарантии посетите https://www.asus.com/ru/support/.

DA: ASUS garantioplysninger

- ASUS tilbyder en valgfri handelsmæssig garanti.
- ASUS forbeholder sig retten til at fortolke bestemmelserne i ASUS' handelsmæssige garanti.
- Denne handelsmæssige garanti fra ASUS tilbydes uafhængigt, som en tilføjelse til den lovbestemte juridiske garanti og den påvirker eller begrænser på ingen måde rettighederne i den juridiske garanti.

Alle garantioplysningerne kan findes på https://www.asus.com/dk/support/.

BG: Информация за гаранцията от ASUS

- ASUS предлага доброволна търговска гаранция от производителя.
- ASUS си запазва правото да тълкува условията на търговската гаранция на ASUS.
- Тази търговска гаранция на ASUS се предлага независимо от и в допълнение на законовата гаранция. Тя по никакъв начин не оказва влияние върху правата на потребителя в законовата гаранция и по никакъв начин не ги ограничава.

За цялостна информация относно гаранцията, моля, посетете https://www.asus.com/support.

CZ: Informace o záruce společnosti ASUS

- Společnost ASUS nabízí dobrovolnou komerční záruku výrobce.
- Společnost ASUS si vyhrazuje právo vykládat ustanovení komerční záruky společnosti ASUS.
- Tato komerční záruka společnosti ASUS je poskytována nezávisle a jako doplněk zákonné záruky a žádným způsobem neovlivňuje ani neomezuje práva vyplývající ze zákonné záruky.

Všechny informace o záruce najdete na adrese https://www.asus.com/cz/support/.

DU: ASUS-garantie-informatie

- SUS biedt een vrijwillige commerciële garantie van de fabrikant.
- ASUS behoudt zich het recht voor om de bepalingen van de commerciële garantie van ASUS uit te leggen.
- Deze commerciële garantie van ASUS wordt onafhankelijk en als aanvulling op de statutaire Wettelijke garantie geboden en beïnvloedt of beperkt in geen geval de rechten onder de wettelijke garantie.

Voor alle informatie over de garantie, gaat u naar https://www.asus.com/nl/support/.

CR: Informacije o ASUS jamstvu

- ASUS dragovoljno nudi komercijalno proizvođačko jamstvo.
- ASUS zadržava prava na tumačenje odredbi ASUS komercijalnog jamstva.
- Ovo ASUS komercijalno jamstvo daje se neovisno i kao dodatak zakonskom jamstvu i ni na koji način ne ograničuje prava iz okvira zakonskog jamstva.

Sve informacije o jamstvu potražite na https://www.asus.com/support.

EE: Teave ASUS-e garantii kohta

- ASUS pakub vabatahtlikku tasulist tootjagarantiid.
- ASUS jätab endale õiguse tõlgendada ASUS-e tasulise garantii tingimusi.
- See ASUS-e tasuline garantii on sõltumatu lisagarantii seadusega kehtestatud garantiile ega mõjuta mingil määral seadusega kehtestatud garantiid ning seadusega kehtestatud garantii piiranguid.

Vaadake garantiiga seotud teavet veebisaidilt https://www.asus.com/ee/.

GK: Πληροφορίες εγγύησης ASUS

- Η ASUS προσφέρει μια εθελοντική Εμπορική εγγύηση κατασκευαστή.
- Η ASUS διατηρεί το δικαίωμα ερμηνείας των διατάξεων της Εμπορικής εγγύησης ASUS.
- Αυτή η Εμπορική εγγύηση ASUS παρέχεται ανεξάρτητα και επιπροσθέτως της θεσμικής Νομικής εγγύησης και σε καμία περίπτωση δεν επηρεάζει ή περιορίζει τα δικαιώματα βάσει της Νομικής εγγύησης.

Για όλες τις πληροφορίες εγγύησης, επισκεφθείτε τη διεύθυνση https://www.asus.com/gr-el/.

HUG: ASUS garanciális információk

- Az ASUS önkéntes gyártói kereskedelmi garanciát kínál.
- Az ASUS fenntartja magának a jogot, hogy értelmezze az ASUS kereskedelmi garanciára vonatkozó rendelkezéseket.
- Ezt a kereskedelmi garanciát az ASUS függetlenül és a törvényes garancia mellett nyújtja és semmilyen módon nem befolyásolja, vagy korlátozza a jogi garancia nyújtotta jogokat.

A garanciára vonatkozó teljes körű információkért látogasson el a https://www.asus.com/hu/support/ oldalra.

LV: ASUS garantijas informācija

- ASUS piedāvā brīvprātīgu ražotāja komerciālo garantiju.
- ASUS patur tiesības interpretēt ASUS komerciālās garantijas noteikumus.
- Šī ASUS komerciālā garantija tiek piedāvāta neatkarīgi un papildus likumā noteiktajai juridiskajai garantijai, un tā nekādi neietekmē vai neierobežo juridiskajā garantijā noteiktās tiesības.

Lai iegūtu informāciju par garantiju, apmeklējiet vietni https://www.asus.com/lv/.

LT: Informacija apie ASUS garantiją

- ASUS siūlo savanorišką komercinę gamintojo garantiją.
- ASUS pasilieka teisę savo nuožiūra aiškinti šios komercinės ASUS garantijos nuostatas.
- Ši komercinė ASUS garantija suteikiama nepriklausoma, be įstatyminės teisinės garantijos, ir jokiu būdu nepaveikia ar neapriboja teisinės garantijos suteikiamų teisių.

Norėdami gauti visą informaciją apie garantiją, apsilankykite https://www.asus.com/lt/.

PL: Informacje o gwarancji firmy ASUS

- Firma ASUS oferuje dobrowolną gwarancję handlową producenta.
- Firma ASUS zastrzega sobie prawo do interpretacji warunków gwarancji handlowej firmy ASUS.
- Niniejsza gwarancja handlowa firmy ASUS jest udzielana niezależnie, jako dodatek do wymaganej ustawowo gwarancji prawnej i w żaden sposób nie wpływa na prawa przysługujące na mocy gwarancji prawnej ani ich nie ogranicza.

Wszelkie informacje na temat gwarancji można znaleźć na stronie https://www.asus.com/pl/support.

PG: Informações de Garantia ASUS

- A ASUS oferece uma Garantia Comercial voluntária do fabricante.
- A ASUS reserva o direito de interpretar as disposições da Garantia Comercial da ASUS.
- Esta Garantia Comercial da ASUS é fornecida de forma independente além da Garantia Legal estatutária e não afeta nem limita de qualquer forma os direitos estabelecidos na Garantia Legal.

Para consultar todas as informações sobre a garantia, visite https://www.asus.com/pt/support/.

RO: Informații despre garanția ASUS

- ASUS oferă o garanție comercială voluntară a producătorului.
- ASUS își rezervă dreptul de a interpreta prevederile garanției comerciale ASUS.
- Această garanție comercială ASUS este oferită independent și în plus față de garanția obligatorie legal și nu afectează sau limitează în niciun fel drepturile acordate conform garanției legale.

Pentru toate informațiile legate de garanție, vizitați https://www.asus.com/ro/support.

SL: Informacije o garanciji ASUS

- ASUS ponuja prostovoljno tržno garancijo proizvajalca.
- ASUS si pridržuje pravico do razlage določb tržne garancije družbe ASUS.
- Ta tržna garancija družbe ASUS je na voljo neodvisno in kot dodatek zakonsko predpisani pravni garanciji ter na noben način ne vpliva na pravice, ki jih zagotavlja pravna garancija, oziroma jih omejuje.

Vse informacije o garanciji najdete na spletnem mestu https://www.asus.com/support.

SK: Informácie o záruke ASUS

- ASUS ponúka dobrovoľnú obchodnú záruku výrobcu.
- ASUS si vyhradzuje právo interpretovať ustanovenia obchodnej záruky ASUS.
- Táto obchodná záruka ASUS je poskytnutá nezávisle a navyše k zákonnej záruke a v žiadnom prípade neovplyvňuje ani neobmedzuje tieto práva podľa tejto zákonnej záruky.

Všetky ďalšie informácie o záruke nájdete na https://www.asus.com/sk/support.

ES: Información de garantía de ASUS

- ASUS ofrece una garantía comercial voluntaria del fabricante.
- ASUS se reserva el derecho de interpretar las disposiciones de esta garantía comercial de ASUS.
- Esta garantía comercial de ASUS se proporciona de forma independiente y adicional a la garantía estatutaria y de ninguna manera afecta a los derechos bajo la garantía legal ni los limita.

Para obtener toda la información sobre la garantía, visite https://www.asus.com/ES/support/.

TR: ASUS Garanti Bilgileri

- ASUS, gönüllü olarak üretici Ticari Garantisi sunar.
- ASUS, ASUS Ticari Garantisinin hükümlerini yorumlama hakkını saklı tutar.
- Bu ASUS Ticari Garantisi, bağımsız olarak ve hukuki Yasal Garanti'ye ek olarak sağlanır ve hiçbir şekilde Yasal Garanti kapsamındaki hakları etkilemez veya sınırlandırmaz.

Tüm garanti bilgileri için lütfen https://www.asus.com/tr/support adresini ziyaret edin.

FI: ASUS-takuutiedot

- ASUS tarjoaa vapaaehtoisen valmistajan kaupallisen takuun.
- ASUS pidättää oikeuden tulkita ASUS-kaupallisen takuun ehdot.
- Tämä ASUS-kaupallinen takuu tarjotaan itsenäisesti lakisääteisen oikeudellisen takuun lisäksi eikä se vaikuta millään tavoin laillisen takuun oikeuksiin tai rajoita niitä.

Saadaksesi kaikki takuutiedot, siirry osoitteeseen https://www.asus.com/fi/support.

NW: Informasjon om ASUS-garanti

- ASUS tilbyr som produsent en frivillig kommersiell garanti.
- ASUS forbeholder seg retten til å tolke bestemmelsene i ASUS sin kommersielle garanti.
- ASUS sin kommersielle garanti gis uavhengig og i tillegg til den lovbestemte juridiske garantien, og verken påvirker eller begrenser rettighetene under den juridiske garantien på noen måte.

Du finner fullstendig informasjon om garanti på https://www.asus.com/no/support/.

SB: Informacije o ASUS garanciji

- ASUS nudi dobrovoljnu proizvođačku komercijalnu garanciju.
- ASUS zadržava pravo da tumači odredbe svoje ASUS komercijalne garancije.
- Ova ASUS komercijalna garancija daje se nezavisno, kao dodatak zakonskoj pravnoj garanciji, i ni ka koji način ne utiče na i ne ograničava prava data pravnom garancijom.

Za sve informacije o garanciji, posetite https://www.asus.com/support/.

SW: ASUS garantiinformation

- ASUS erbjuder en frivillig kommersiell tillverkningsgaranti.
- ASUS förbehåller sig rätten att tolka bestämmelserna i ASUS kommersiella garanti.
- Denna kommersiella garanti från ASUS tillhandahålles separat och som tillägg till den lagstadgade garantin, och påverkar eller begränsar på intet sätts rättigheterna under den lagstadgade garantin.

För all garantiinformation, besök https://www.asus.com/se/support/.

UA: Інформація про Гарантію ASUS

- ASUS пропонує добровільну Комерційну Гарантію виробника.
- ASUS застерігає за собою право тлумачити положення Комерційної Гарантії ASUS
- Цю Комерційну Гарантію надано незалежно і на додаток до обов'язкової Законної Гарантії; вона жодним чином не впливає на права за Законною Гарантією і не обмежує їх.

Всю інформацію про гарантію подано тут: https://www.asus.com/ua/support.

BP: Informações de garantia ASUS

Esta garantia aplica-se ao período definido pela garantia legal (90 dias) mais o período de garantia comercial oferecido pela ASUS. Por exemplo: 12M significa 12 meses de garantia no total (3 meses de garantia legal mais 9 meses de garantia contratual), 24 meses significa 24 meses de garantia no total (3 meses de garantia legal mais 21 meses de garantia contratual) e 36 meses significa 36 meses de garantia no total (3 meses de garantia legal e 33 de garantia contratual) a contar da data da garantia declarada (Data de Início da Garantia).

Para todas as informações de garantia, visite https://www.asus.com/br/support/.

MX: Garantía y Soporte

Esta Garantía aplica en el país de compra. Usted acepta que en esta garantía:

- Los procedimientos de servicio pueden variar en función del país.
- Algunos servicios y/o piezas de reemplazo pudieran no estar disponibles en todos los países.
- Algunos países pueden tener tarifas y restricciones que se apliquen en el momento de realizar el servicio, visite el sitio de soporte de ASUS en https://www.asus.com/mx/support/ para ver más detalles.
- Si tiene alguna queja o necesidad de un centro de reparación local o el periodo de garantía del producto ASUS, por favor visite el sitio de Soporte de ASUS en https://www.asus.com/mx/support/ para mayores detalles.

Información de contacto ASUS

Esta garantía está respaldada por:
ASUSTeK Computer Inc.
Centro de Atención ASUS +52 (55) 1946-3663

ID: Informasi Garansi ASUS

Garansi ini berlaku di negara tempat pembelian.

Periode Garansi tertera pada kemasan/kotak dari Produk dan Masa Garansi dimulai sejak tanggal pembelian Produk ASUS dengan kondisi baru.

Silahkan pindai Kode QR di bagian bawah halaman terakhir untuk Kartu Garansi versi Web dalam format PDF untuk lebih informasi jelas mengenai jaminan garansi Produk ASUS.

- Informasi Dukungan ASUS, silakan kunjungi https://www.asus.com/id/support.
- Informasi Lokasi Layanan, silakan kunjungi https://www.asus.com/id/support/Service-Center/Indonesia.
- Layanan Call Center: 1500128

VI: Thông tin đảm bảo của ASUS

- ASUS cung cấp Bảo hành thương mại tự nguyện của nhà sản xuất.
- ASUS bảo lưu quyền giải thích các điều khoản của Bảo hành thương mại của ASUS.
- Bảo hành thương mại này của ASUS được cung cấp độc lập và ngoài Bảo đảm pháp lý theo luật định và không có cách nào ảnh hưởng đến hoặc giới hạn các quyền theo Bảo lãnh pháp lý. Để biết tất cả các thông tin bảo hành, vui lòng truy cập

https://www.asus.com/vn/support

ASUS contact information

ASUSTeK COMPUTER INC.

Address: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan

ASUS COMPUTER INTERNATIONAL (America)

Address: 48720 Kato Rd., Fremont, CA 94538, USA

ASUS COMPUTER GmbH (Germany and Austria)

Address: Harkortstrasse 21-23, 40880 Ratingen, Germany

ASUSTeK (UK) LIMITED

Address: 1st Floor, Sackville House, 143-149 Fenchurch Street, London, EC3M 6BL, England, United Kingdom

Service and Support

Visit our multi-language website at https://www.asus.com/support.