

# **GIGABYTE™**

## **MW53-HP0**

Intel® Socket LGA4677 processor motherboard

### User Manual

Rev. 1.0

## **Copyright**

© 2023 Giga Computing TECHNOLOGY CO., LTD. All rights reserved.

The trademarks mentioned in this manual are legally registered to their respective owners.

## **Disclaimer**

Information in this manual is protected by copyright laws and is the property of GIGABYTE.

Changes to the specifications and features in this manual may be made by Giga Computing without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without Giga Computing's prior written permission.

## **Documentation Classifications**

In order to assist in the use of this product, Giga Computing provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents

## **For More Information**

For related product specifications, the latest firmware and software, and other information, please visit our website at: <http://www.gigabyte.com/enterprise>.

For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: <http://reseller.b2b.gigabyte.com>

For further technical assistance, please contact your GIGABYTE representative or visit <http://esupport.gigabyte.com/> to create a new support ticket.

For any general sales or marketing enquires, you may message GIGABYTE server directly by email: [server.grp@gigabyte.com](mailto:server.grp@gigabyte.com).

**⚠ WARNING**

- **INGESTION HAZARD:** This product contains a button cell or coin battery.
- **DEATH** or serious injury can occur if ingested.
- A swallowed button cell or coin battery can cause **Internal Chemical Burns** in as little as **2 hours**.
- **KEEP** new and used batteries **OUT OF REACH OF CHILDREN**
- **Seek immediate medical attention** if a battery is suspected to be swallowed or inserted inside any part of the body.



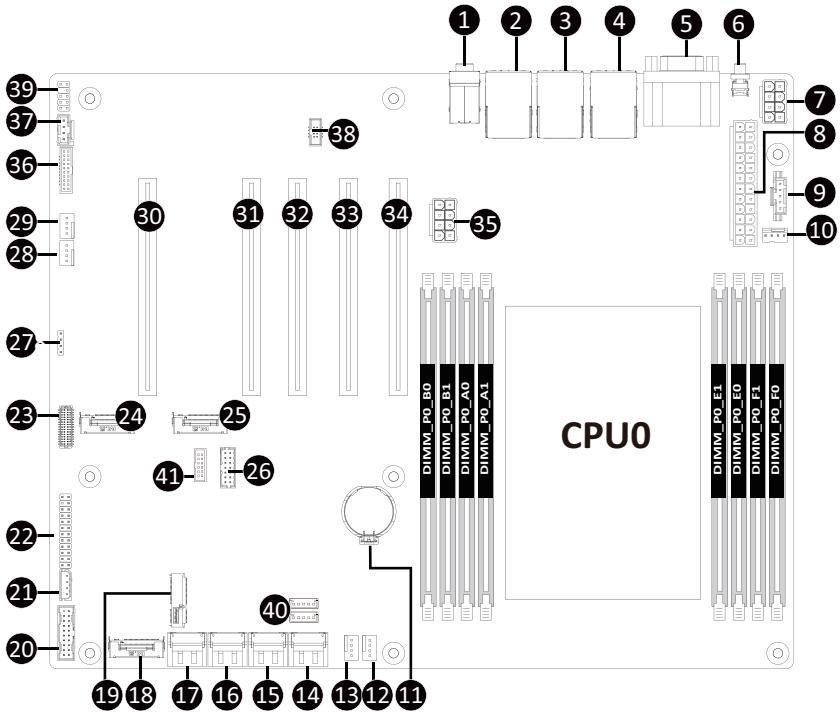
- Battery type: CR2032, voltage rating: +3VDC.
- Non-rechargeable batteries are not to be recharged.
- Remove and immediately recycle or dispose of used batteries, batteries from equipment not used for an extended period of time according to local regulations and keep away from children. Do NOT dispose of batteries in household trash or incinerate.
- Even used batteries may cause severe injury or death.
- Do not force discharge, recharge, disassemble, heat above (manufacturer's specified temperature rating) or incinerate. Doing so may result in injury due to venting, leakage or explosion resulting in chemical burns.
- For treatment information, call a local poison control center.
- The product contains non-replaceable batteries.

# Table of Contents

|  |    |
|--|----|
| MW53-HP0 Motherboard Layout.....                             | 6  |
| Block Diagram .....  | 8  |
| Chapter 1 Hardware Installation .....                        | 8  |
| 1-1 Installation Precautions .....                           | 8  |
| 1-2 Product Specifications.....                              | 9  |
| 1-3 Installing and Removing the CPU .....                    | 11 |
| 1-4 Installing and Removing Memory.....                      | 13 |
| 1-4-1 4-Channel Memory Configuration .....                   | 13 |
| 1-4-2 Installing and Removing a Memory Module .....          | 14 |
| 1-4-3 DIMM Population Table .....                            | 14 |
| 1-5 Installing the M.2 SSD Module.....                       | 15 |
| 1-6 Back Panel Connectors.....                               | 16 |
| 1-7 Internal Connectors.....                                 | 18 |
| 1-8 Jumper Settings .....                                    | 29 |
| Chapter 2 BIOS Setup .....                                   | 30 |
| 2-1 The Main Menu .....                                      | 32 |
| 2-2 Advanced Menu .....                                      | 35 |
| 2-2-1 Trusted Computing .....                                | 36 |
| 2-2-2 Serial Port Console Redirection .....                  | 38 |
| 2-2-3 SIO Configuration .....                                | 41 |
| 2-2-4 PCI Subsystem Settings.....                            | 42 |
| 2-2-5 USB Configuration.....                                 | 44 |
| 2-2-6 Network Stack Configuration .....                      | 45 |
| 2-2-7 Post Report Configuration .....                        | 46 |
| 2-2-8 NVMe Configuration .....                               | 47 |
| 2-2-9 Chipset Configuration.....                             | 48 |
| 2-2-10 Tls Auth Configuration .....                          | 49 |
| 2-2-11 iSCSI Configuration .....                             | 50 |
| 2-2-12 Intel(R) Ethernet Controller X710 for 10GBASE-T ..... | 51 |
| 2-2-13 VLAN Configuration.....                               | 53 |
| 2-2-14 Driver Health.....                                    | 54 |
| 2-3 Chipset Menu.....  | 55 |
| 2-3-1 Processor Configuration .....                          | 56 |
| 2-3-2 Common RefCode Configuration .....                     | 59 |
| 2-3-3 UPI Configuration .....                                | 60 |
| 2-3-4 Memory Configuration .....                             | 61 |

|        |   |    |
|--------|---|----|
| 2-3-5  | I/O Configuration .....                       | 64 |
| 2-3-6  | Advanced Power Management Configuration ..... | 66 |
| 2-3-7  | PCH Configuration.....                        | 68 |
| 2-3-8  | Miscellaneous Configuration .....             | 70 |
| 2-3-9  | Server ME Configuration .....                 | 71 |
| 2-3-10 | Runtime Error Logging Settings .....          | 72 |
| 2-3-11 | Power Policy.....                             | 74 |
| 2-4    | Server Management Menu.....                   | 76 |
| 2-4-1  | System Event Log .....                        | 78 |
| 2-4-2  | View FRU Information .....                    | 79 |
| 2-4-3  | BMC VLAN Configuration.....                   | 80 |
| 2-4-4  | BMC Network Configuration.....                | 81 |
| 2-4-5  | IPv6 BMC Network Configuration.....           | 82 |
| 2-5    | Security Menu .....                           | 83 |
| 2-5-1  | Secure Boot .....                             | 84 |
| 2-6    | Boot Menu.....                                | 87 |
| 2-7    | Save & Exit Menu.....                         | 89 |
| 2-8    | BIOS Recovery .....                           | 91 |
| 2-9    | BIOS POST Beep code (AMI standard).....       | 92 |
| 2-9-1  | PEI Beep Codes .....                          | 92 |
| 2-9-2  | DXE Beep Codes .....                          | 92 |

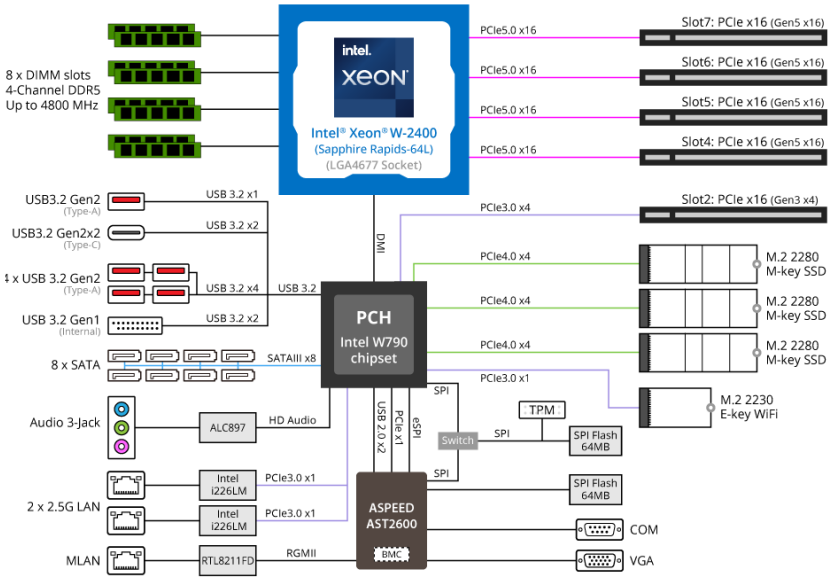
# MW53-HP0 Motherboard Layout



| Item | Code      | Description  |
|------|-----------|--|
| 1    | AUDIO     | Audio Connectors   |
| 2    | USB3_MLAN | Sever Management LAN Port (Top)/USB 3.2 Gen2 Type A Ports (Bottom) |
| 3    | LAN1      | 2.5GbE LAN Port #1 / USB 3.2 Gen2 Type-A Ports                     |
| 4    | LAN2      | 2.5GbE LAN Port #2 / USB 3.2 Gen2 Type-A Ports + Type-C Port       |
| 5    | COM1_VGA  | Serial Port (Top)/VGA Port (Bottom)                                |
| 6    | SW_ID     | ID Button with LED   |
| 7    | P12V_AUX2 | 2x4 Pin 12V Power Connector  |
| 8    | ATX1      | 2x12 Pin Main Power Connector                                      |
| 9    | PMBUS     | PMBus Connector  |
| 10   | CPU_FAN   | CPU Fan Connector  |
| 11   | BAT       | Battery Socket   |
| 12   | SYS_FAN4  | System Fan Connector #4  |
| 13   | SYS_FAN2  | System Fan Connector #2  |
| 14   | SATA_6_7  | Slimline Connector #2 (SATA 6Gb/s Signal)                          |
| 15   | SATA_4_5  | Slimline Connector #2 (SATA 6Gb/s Signal)                          |

| Item | Code      | Description                                   |
|------|-----------|---|
| 16   | SATA_2_3  | Slimline Connector #2 (SATA 6Gb/s Signal)     |
| 17   | SATA_0_1  | Slimline Connector #1 (SATA 6Gb/s Signal)     |
| 18   | M2_2      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280)    |
| 19   | M2E       | M.2 E-Key Slot (Support PCIe WIFI, Bluetooth) |
| 20   | F_USB3_V  | Front Panel USB 3.2 Gen1 Connector            |
| 21   | IPMB      | IPMB Connector                                |
| 22   | FP_1      | Front Panel Header                            |
| 23   | BP_1      | HDD Backplane Board Connector                 |
| 24   | M2_0      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280)    |
| 25   | M2_1      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280)    |
| 26   | SPI_TPM   | TPM Connector                                 |
| 27   | JTAG_BMC  | SATA RAID Upgrade Key                         |
| 28   | SYS_FAN1  | System Fan Connector #1                       |
| 29   | SYS_FAN3  | System Fan Connector #3                       |
| 30   | PCIE_2    | PCIe x16 Slot (Gen3 x4)                       |
| 31   | PCIE_4    | PCIe x16 Slot (Gen5 x16)                      |
| 32   | PCIE_5    | PCIe x16 Slot (Gen5 x16)                      |
| 33   | PCIE_6    | PCIe x16 Slot (Gen5 x16)                      |
| 34   | PCIE_7    | PCIe x16 Slot (Gen5 x16)                      |
| 35   | P12V_AUX1 | 2x4 Pin 12V Power Connector                   |
| 36   | CN_NCSI   | NCSI Connector                                |
| 37   | BMC_USB2B | BMC USB Connector                             |
| 38   | CN_I2C    | I2C Connector                                 |
| 39   | F_AUDIO   | Front Audio Header                            |
| 40   | SPGIO_1_2 | Connect to BPB for SATA LED                   |
| 41   | DB_ESPI   | ESPI Connector                                |

# Block Diagram













# Chapter 1 Hardware Installation









## 1-1 Installation Precautions

The motherboard contains numerous delicate electronic circuits and components which can become damaged as a result of electrostatic discharge (ESD). Prior to installation, carefully read the user's manual and follow these procedures:

- Prior to installation, do not remove or break motherboard S/N (Serial Number) sticker or warranty sticker provided by your dealer. These stickers are required for warranty validation.
- Always remove the AC power by unplugging the power cord from the power outlet before installing or removing the motherboard or other hardware components.
- When connecting hardware components to the internal connectors on the motherboard, make sure they are connected tightly and securely.
- When handling the motherboard, avoid touching any metal leads or connectors.
- It is best to wear an electrostatic discharge (ESD) wrist strap when handling electronic components such as a motherboard, CPU or memory. If you do not have an ESD wrist strap, keep your hands dry and first touch a metal object to eliminate static electricity.
- Prior to installing the motherboard, please have it on top of an antistatic pad or within an electrostatic shielding container.
- Before unplugging the power supply cable from the motherboard, make sure the power supply has been turned off.
- Before turning on the power, make sure the power supply voltage has been set according to the local voltage standard.
- Before using the product, please verify that all cables and power connectors of your hardware components are connected.
- To prevent damage to the motherboard, do not allow screws to come in contact with the motherboard circuit or its components.
- Make sure there are no leftover screws or metal components placed on the motherboard or within the computer casing.
- Do not place the computer system on an uneven surface.
- Do not place the computer system in a high-temperature environment.
- Turning on the computer power during the installation process can lead to damage to system components as well as physical harm to the user.
- If you are uncertain about any installation steps or have a problem related to the use of the product, please consult a certified computer technician.

## 1-2 Product Specifications

|   |  |
|---|--|
|  CPU                         | <ul style="list-style-type: none"> <li>◆ Intel® Xeon® W-2400 Processor Family</li> <li>◆ Single Processor, TDP up to 225W</li> <li>◆ 1 x LGA 4677</li> </ul>   |
|  Chipset                     | <ul style="list-style-type: none"> <li>◆ Intel® W790 Chipset</li> </ul>  |
|  Memory Type                 | <ul style="list-style-type: none"> <li>◆ 8 x DIMM slots</li> <li>◆ DDR5 memory module supported only</li> <li>◆ 4-channel memory architecture</li> <li>◆ RDIMM modules up to 64GB supported</li> <li>◆ RDIMM-3DS modules up to 256GB supported</li> <li>◆ Memory speed: up to 4800 MHz (1DPC), 4400 MHz (2DPC)</li> </ul> <p>NOTE: When installing memory modules, make sure to begin with the first socket of each channel, such as DIMM_P0_A0, DIMM_P0_B0, DIMM_P0_C0, DIMM_P0_D0</p>  |
|  Integrated Audio Controller | <ul style="list-style-type: none"> <li>◆ Realtek® ALC897 HD audio codec</li> <li>◆ Supports 2/4/5.1/7.1 channel configurations</li> <li>◆ 3 ports Audio Jack (Audio in/Audio out/Mic)</li> </ul>   |
|  Integrated Network          | <ul style="list-style-type: none"> <li>◆ 2 x 2.5 GbE LAN ports (Intel® i226LM)</li> <li>◆ 1 x 10/100/1000 Management LAN (Realtek® RTL8211FD)</li> </ul>   |
|  Expansion Slots             | <ul style="list-style-type: none"> <li>◆ Slot_7: 1 x PCIe x16 (Gen5 x16 bus) slot, from CPU</li> <li>◆ Slot_6: 1 x PCIe x16 (Gen5 x16 bus) slot, from CPU</li> <li>◆ Slot_5: 1 x PCIe x16 (Gen5 x16 bus) slot, from CPU</li> <li>◆ Slot_4: 1 x PCIe x16 (Gen5 x16 bus) slot, from CPU</li> <li>◆ Slot_2: 1 x PCIe x16 (Gen3 x4 bus) slot, from PCH</li> </ul><br><ul style="list-style-type: none"> <li>◆ 3 x M.2 slots for Storage:             <ul style="list-style-type: none"> <li>◆ - M-key</li> <li>◆ - PCIe Gen4 x4, from PCH</li> <li>◆ - Supports NGFF-2280 card</li> </ul> </li> <br/> <li>◆ 1 x M.2 slot for Wi-Fi:             <ul style="list-style-type: none"> <li>◆ - E-key</li> <li>◆ - PCIe Gen3 x1, from PCH</li> <li>◆ - Supports NGFF-2230 card</li> </ul> </li> </ul> |
|  Storage Interface         | <ul style="list-style-type: none"> <li>◆ 8 x SATA III 6Gb/s ports</li> </ul>   |
|  Support RAID Function     | <ul style="list-style-type: none"> <li>◆ Intel® SATA RAID 0/1/10/5</li> </ul>  |

|  |   |
|--|---|
|  <b>On-Board Connectors</b>                               | <ul style="list-style-type: none"> <li>◆ 1 x 24-pin ATX main power connector</li> <li>◆ 2 x 8-pin ATX 12V power connectors for CPU and DDR 12V input</li> <li>◆ 1 x CPU fan header</li> <li>◆ 4 x System fan headers</li> <li>◆ 2 x USB 3.2 Gen1 headers</li> <li>◆ 1 x Front audio header</li> <li>◆ 1 x PMBus connector</li> <li>◆ 1 x Clear CMOS jumper</li> <li>◆ 8 x SATA connectors</li> <li>◆ 3 x M.2 slots</li> <li>◆ 1 x Front panel header</li> <li>◆ 1 x Backplane board header</li> <li>◆ 1 x TPM header</li> <li>◆ 1 x VROC connector</li> </ul> |
|  <b>Rear I/O Connectors</b>                               | <ul style="list-style-type: none"> <li>◆ 1 x VGA</li> <li>◆ 1 x COM</li> <li>◆ 2 x RJ45</li> <li>◆ 1 x MLAN</li> <li>◆ 5 x USB 3.2 Gen2 Type-A</li> <li>◆ 1 x USB3.2 Gen2x2 Type-C</li> <li>◆ 1 x ID button with LED</li> <li>◆ 3 x Audio jacks</li> </ul>  |
|  <b>TPM</b>   | <ul style="list-style-type: none"> <li>◆ 1 x TPM header with SPI interface</li> <li>◆ Optional TPM2.0 kit: CTM010</li> </ul>  |
|  <b>Form Factor</b>                                       | <ul style="list-style-type: none"> <li>◆ ATX</li> <li>◆ 304.8W x 244D (mm)</li> </ul>   |
|  <b>Server Management</b>                                 | <ul style="list-style-type: none"> <li>◆ Aspeed® AST2600</li> </ul>   |
|  <b>Operating Properties</b>                              | <ul style="list-style-type: none"> <li>◆ Operating temperature: 10°C to 40°C</li> <li>◆ Operating humidity: 8-80% (non-condensing)</li> <li>◆ Non-operating temperature: -40°C to 60°C</li> <li>◆ Non-operating humidity: 20%-95% (non-condensing)</li> </ul>   |
|  <b>PSU Connectors</b>                                  | <ul style="list-style-type: none"> <li>◆ 1 x 24-pin ATX main power connector</li> <li>◆ 2 x 8-pin ATX 12V power connectors</li> </ul>   |
|  <b>OS Driver Supported</b>                             | <ul style="list-style-type: none"> <li>◆ Windows 11 Enterprise (x64)</li> <li>◆ Red Hat Enterprise Linux 9.0 (x64)</li> <li>◆ Ubuntu 22.04 LTS (x64)</li> <li>◆ CentOS Stream 9 (x64)</li> <li>◆ Debian 11.5.0</li> </ul>   |
| <p>GIGABYTE reserves the right to make any changes to the product specifications and product-related information without prior notice.</p> |   |

## 1-3 Installing and Removing the CPU



Read the following guidelines before you begin to install the CPU:

- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open the system according to the instructions.

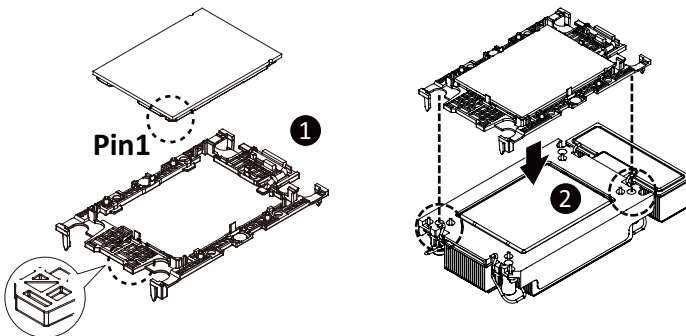
### **WARNING!**

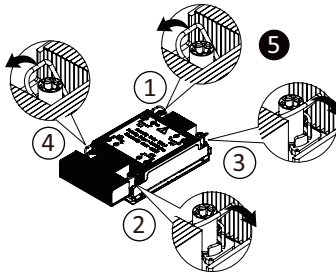
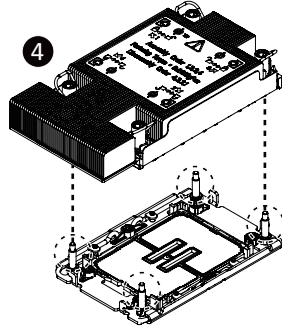
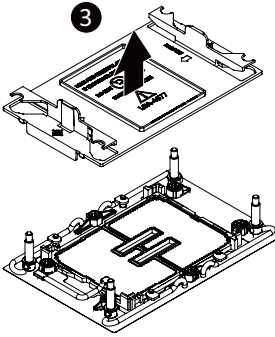
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

### **Follow these instructions to Install the CPU:**

1. Align and install the processor on the carrier.  
**NOTE:** Apply thermal compound evenly on the top of the CPU. Remove the protective cover from the underside of the heat sink.
2. Carefully flip the heat sink cover. Then install the carrier assembly on the bottom of the heat sink and make sure the gold arrow is located in the correct direction.
3. Remove the CPU cover.  
**NOTE:** Save the CPU cover in the event that you need to remove the CPU from the socket.
4. Align the heat sink with the CPU socket by the guide pins and make sure the gold arrow is located in the correct direction. Then place the heat sink onto the top of the CPU socket.
5. Position the rotating wires into the latch position. Tighten the screws in a sequential order (1→2→3→4).

**NOTE:** When disassembling the heat sink, loosen the screws in reverse order (4→3→2→1) and then move the rotating wires into the unlatch position.





**Note!**

- The illustrations of the heat-sink installation shown are for reference only..

## 1-4 Installing and Removing Memory

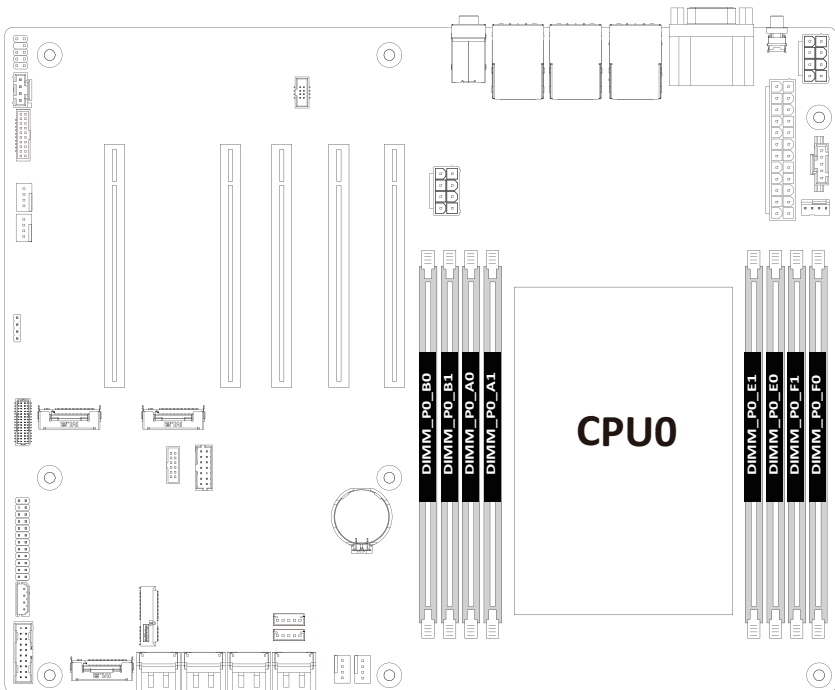


Read the following guidelines before you begin to install the memory:

- Make sure that the motherboard supports the memory. It is recommended to use memory of the same capacity, brand, speed, and and chips.
- Always turn off the computer and unplug the power cord from the power outlet before installing the memory to prevent hardware damage.
- Memory modules have a foolproof design. A memory module can be installed in only one direction. If you are unable to insert the memory, switch the direction.

### 1-4-1 4-Channel Memory Configuration

This motherboard provides 8 DDR5 memory slots and supports 4-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



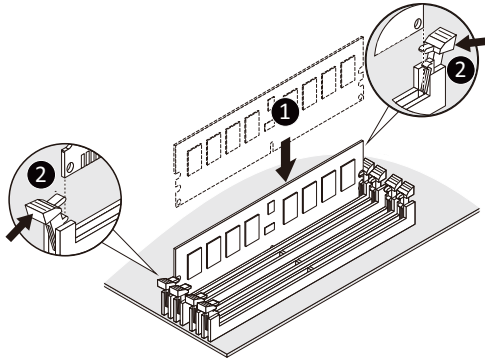
### 1-4-2 Installing and Removing a Memory Module



Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module. Be sure to install DDR5 DIMMs on this motherboard.

Follow these instructions to install a DIMM module:

1. Insert the DIMM memory module vertically into the DIMM slot and push it down.
2. Close the plastic clip at both edges of the DIMM slots to lock the DIMM module.
3. Reverse the installation steps when you want to remove the DIMM module.



### 1-4-3 DIMM Population Table

| Type      | Ranks Per DIMM and Data Width | DIMM Capacity (GB) | Speed (MT/s); Voltage (V); DIMM per Channel (DPC) |       |
|-----------|-------------------------------|--------------------|---|-------|
|           |                               |                    | 1DPC*   | 2DPC* |
|           |                               | 16Gb               | 1.1V  |       |
| RDIMM     | SRx8 (RC D)                   | 16GB               | 4800  | 4400  |
|           | SRx4 (RC C)                   | 32GB               |   |       |
|           | DRx8 (RC E)                   | 32GB               |   |       |
|           | DRx4 (RC A)                   | 64GB               |   |       |
| RDIMM 3DS | (4R/8R)x4                     | 2H-128GB           |   |       |
|           | (RC A)                        | 4H-256GB           |   |       |

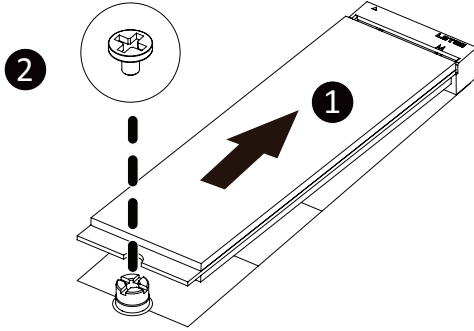
\*1DPC applies to 1SPC or 2SPC implementations (SPC - Sockets Per Channel)

## 1-5 Installing the M.2 SSD Module

Follow the steps below to install a M.2 SSD module on your motherboard.

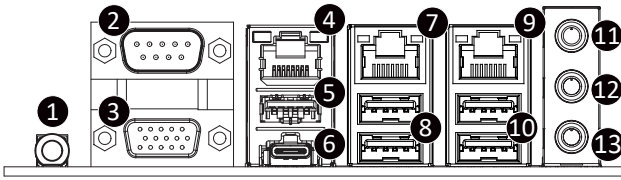
Step1. Insert the M.2 SSD module into the slot.

Step2. Secure it with the screw, tightening as necessary to fasten the M.2 SSD module in place.





## 1-6 Back Panel Connectors



### 1 ID Button with LED

When the system identification is active, the ID LED on the front/ back panel glows blue.

### 2 Serial Port

Connect to serial-based mouse or data processing devices.

### 3 VGA Port

Connect to a monitor device.

### 4 2.5GbE LAN Port #2

The Gigabit Ethernet LAN port provides Internet connection at up to 2.5 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

### 5 USB 3.2 Type-A Port

The USB port supports the USB 3.2 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

### 6 USB 3.2 Type-C Port

The USB port supports the USB 3.2 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

### 7 2.5GbE LAN Port #1

The Gigabit Ethernet LAN port provides Internet connection at up to 2.5 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

### 8 USB 3.2 Gen2 Ports

The USB port supports the USB 3.2 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

### 9 Server Management 10/100/1000 LAN Port

The LAN port provides Internet connection with data transfer speeds of 10/100/1000Mbps. This port is the dedicated LAN port for Server Management.

### 10 USB 3.2 Gen2 Ports

The USB port supports the USB 3.2 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

### 11 Line In Jack (Blue)

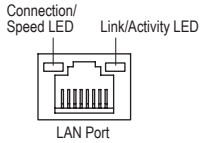
The default Line in jack. Use this audio jack for line in devices such as an optical drive, walkman, etc

### 12 Line Out Jack (Green)

The default Line Out jack. Use this audio jack for a headphone or 2-channel speaker. This jack can be used to connect front speakers in a 4/5.1/7.1-channel audio configuration.

### 13 Mic In (Pink)

The default MIC In jack. A microphone can be connected to the MIC In jack.



2.5GbE LAN LED:

| State     | Description               |
|-----------|---------------------------|
| Yellow On | 1 Gbps, 100Mbps data rate |
| Green On  | 2.5 Gbps data rate        |
| Off       | 10 Mbps data rate         |

10/100/1000 LAN LED:

| State     | Description        |
|-----------|--------------------|
| Yellow On | 1 Gbps data rate   |
| Green On  | 100 Mbps data rate |
| Off       | 10 Mbps data rate  |

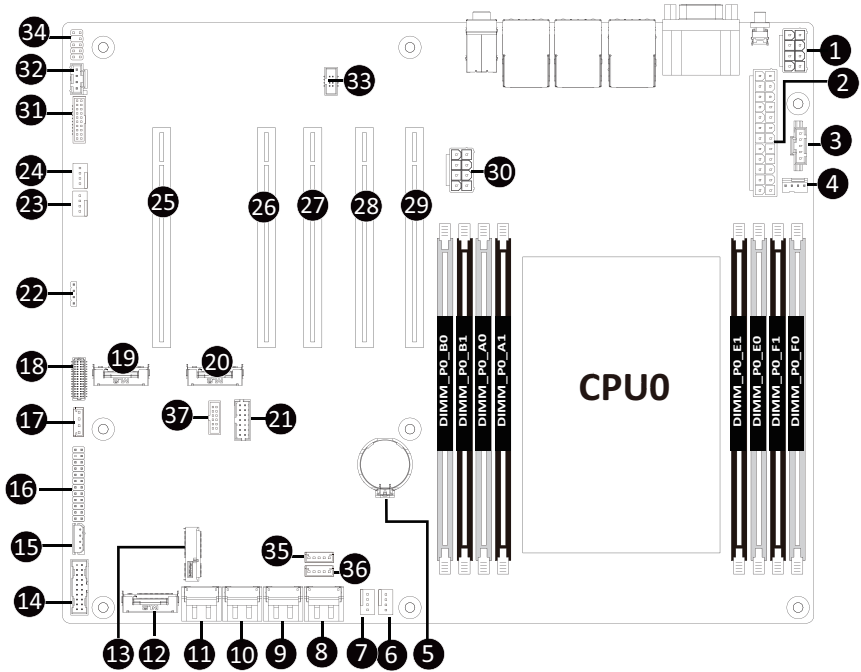
ID Button / LED:

| State   | Description                      |
|---------|----------------------------------|
| Blue on | System identification is active  |
| Off     | System identification is disable |



- When removing the cable connected to a back panel connector, first remove the cable from your device and then remove it from the motherboard.
- When removing the cable, pull it straight out from the connector. Do not rock it side to side to prevent an electrical short inside the cable connector.

# 1-7 Internal Connectors



| No. | Code      | Description                                   | No. | Code      | Description                                |
|-----|-----------|---|-----|-----------|--|
| 1   | P12V_AUX2 | 2x4 Pin 12V Power Connector                   | 20  | M2_1      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280) |
| 2   | ATX1      | 2x12 Pin Main Power Connector                 | 21  | SPI_TPM   | TPM Connector                              |
| 3   | PMBUS     | PMBus Connector                               | 22  | JTAG_BMC  | SATA RAID Upgrade Key                      |
| 4   | CPU_FAN   | CPU Fan Connector                             | 23  | SYS_FAN3  | System Fan Connector #3                    |
| 5   | BAT       | Battery Socket                                | 24  | SYS_FAN1  | System Fan Connector #1                    |
| 6   | SYS_FAN4  | System Fan Connector #4                       | 25  | PCIE_2    | PCIe x16 Slot (Gen3 x4)                    |
| 7   | SYS_FAN2  | System Fan Connector #2                       | 26  | PCIE_4    | PCIe x16 Slot (Gen5 x16)                   |
| 8   | SATA_6_7  | Slimline Connector #4 (SATA 6Gb/s Signal)     | 27  | PCIE_5    | PCIe x16 Slot (Gen5 x16)                   |
| 9   | SATA_4_5  | Slimline Connector #3 (SATA 6Gb/s Signal)     | 28  | PCIE_6    | PCIe x16 Slot (Gen5 x16)                   |
| 10  | SATA_2_3  | Slimline Connector #2 (SATA 6Gb/s Signal)     | 29  | PCIE_7    | PCIe x16 Slot (Gen5 x16)                   |
| 11  | SATA_0_1  | Slimline Connector #1 (SATA 6Gb/s Signal)     | 30  | P12V_AUX1 | 2x4 Pin 12V Power Connector                |
| 12  | M2_2      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280)    | 31  | CN_NCSI   | NCSI Connector                             |
| 13  | M2E       | M.2 E-Key Slot (Support PCIe WIFI, Bluetooth) | 32  | BMC_USB2B | BMC USB Connector                          |
| 14  | F_USB3_V  | Front Panel USB 3.2 Gen1 Connector            | 33  | CN_I2C    | I2C Connector                              |
| 15  | IPMB      | IPMB Connector                                | 34  | F_AUDIO1  | Front Audio Header                         |
| 16  | FP_1      | Front Panel Header                            | 35  | SATA_SGP1 | Connect to BPB for SATA LED                |
| 17  | SW_RAID   | VRROC Module Connector                        | 36  | SATA_SGP2 | Connect to BPB for SATA LED                |
| 18  | BP_1      | HDD Backplane Board Connector                 | 37  | DB_ESPI   | ESPI Connector                             |
| 19  | M2_0      | M.2 Slot (PCIe Gen4 x4, Support NGFF-2280)    |     |           |  |



Read the following guidelines before connecting external devices:

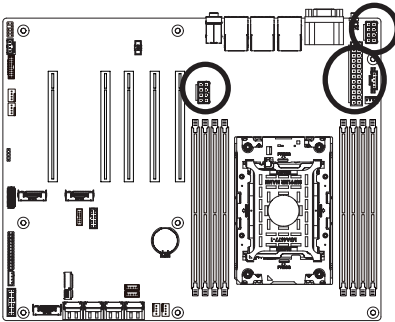
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the computer, make sure the device cable has been securely attached to the connector on the motherboard.

## 1/18/2) P12V\_AUX2/P12V\_AUX1/ATX1 (2x4 12V Power Connector and 2x12 Main Power Connector)

With the use of the power connector, the power supply can supply enough stable power to all the components on the motherboard. Before connecting the power connector, first make sure the power supply is turned off and all devices are properly installed. The power connector possesses a foolproof design. Connect the power supply cable to the power connector in the correct orientation. The 12V power connector mainly supplies power to the CPU. If the 12V power connector is not connected, the computer will not start.



To meet expansion requirements, it is recommended that a power supply that can withstand high power consumption be used (500W or greater). If a power supply is used that does not provide the required power, the result can lead to an unstable or unbootable system.



**P12V\_AUX1/ P12V\_AUX2**

| Pin No. | Definition |
|---------|------------|
| 1       | GND        |
| 2       | GND        |
| 3       | GND        |
| 4       | GND        |
| 5       | +12V       |
| 6       | +12V       |
| 7       | +12V       |
| 8       | +12V       |

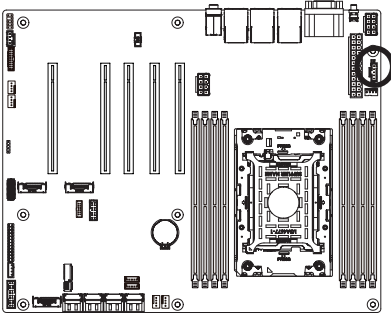


**ATX**

| Pin No. | Definition | Pin No. | Definition |
|---------|------------|---------|------------|
| 1       | 3.3V       | 13      | 3.3V       |
| 2       | 3.3V       | 14      | -12V       |
| 3       | GND        | 15      | GND        |
| 4       | +5V        | 16      | PS_ON      |
| 5       | GND        | 17      | GND        |
| 6       | +5V        | 18      | GND        |
| 7       | GND        | 19      | GND        |
| 8       | Power Good | 20      | NC         |
| 9       | 5VSB       | 21      | +5V        |
| 10      | +12V       | 22      | +5V        |
| 11      | +12V       | 23      | +5V        |
| 12      | 3.3V       | 24      | GND        |

### 3) PMBus Connector

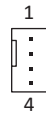
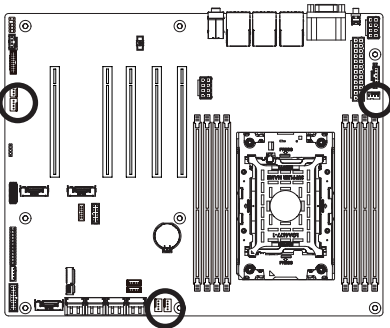
The Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



| Pin No. | Definition  |
|---------|-------------|
| 1       | PMBus Clock |
| 2       | PMBus Data  |
| 3       | PMBus Alert |
| 4       | GND         |
| 5       | 3.3V Sense  |

### 4/6/7/13/14) CPU\_FAN/SYS\_FAN4/SYS\_FAN2/SYS\_FAN1/SYS\_FAN3/SYS\_FAN5 (CPU Fan/System Fan Headers)

The motherboard has one 4-pin CPU fan header (CPU\_FAN), and two 4-pin (SYS\_FAN) system fan headers. Most fan headers possess a foolproof insertion design. When connecting a fan cable, be sure to connect it in the correct orientation (the black connector wire is the ground wire). The motherboard supports CPU fan speed control, which requires the use of a CPU fan with fan speed control design. For optimum heat dissipation, it is recommended that a system fan be installed inside the chassis.



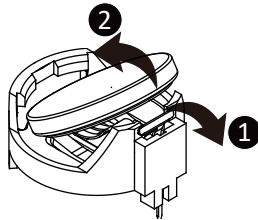
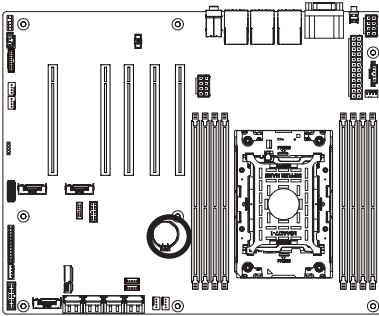
| Pin No. | Definition    |
|---------|---------------|
| 1       | GND           |
| 2       | +12V          |
| 3       | Sense         |
| 4       | Speed Control |



- Be sure to connect fan cables to the fan headers to prevent your CPU and system from overheating. Overheating may result in damage to the CPU or the system may hang.
- These fan headers are not configuration jumper blocks. Do not place a jumper cap on the headers.

## 5) BAT (Battery Socket)

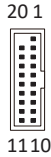
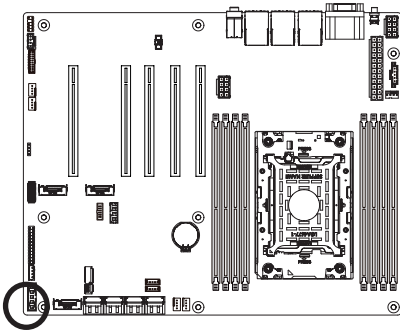
The battery provides power to keep the values (such as BIOS configurations, date, and time information) in the CMOS when the computer is turned off. Replace the battery when the battery voltage drops to a low level, or the CMOS values may not be accurate or may be lost.



- Always turn off your computer and unplug the power cord before replacing the battery.
- Replace the battery with an equivalent one. Danger of explosion if the battery is replaced with an incorrect model.
- Contact the place of purchase or local dealer if you are not able to replace the battery by yourself or uncertain about the battery model.
- Used batteries must be handled in accordance with local environmental regulations.

### 8) F\_USB3\_V (Front Panel USB 3.2 Gen1 Connector)

The connectors conform to USB 3.2 specification. Each USB header can provide two USB ports via an optional USB bracket. For purchasing the optional USB bracket, please contact the local dealer.

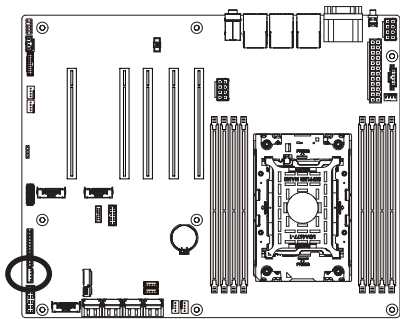


USB 3.2 Connector

| Pin No. | Definition    | Pin No. | Definition    |
|---------|---------------|---------|---------------|
| 1       | Power         | 11      | IntA_P2_D+    |
| 2       | IntA_P1_SSRX- | 12      | IntA_P2_D-    |
| 3       | IntA_P1_SSRX+ | 13      | GND           |
| 4       | GND           | 14      | IntA_P2_SSTX+ |
| 5       | IntA_P1_SSTX- | 15      | IntA_P2_SSTX- |
| 6       | IntA_P1_SSTX+ | 16      | GND           |
| 7       | GND           | 17      | IntA_P2_SSRX+ |
| 8       | IntA_P1_D-    | 18      | IntA_P2_SSRX- |
| 9       | IntA_P1_D+    | 19      | Power         |
| 10      | NC            | 20      | No Pin        |

### 9) IPMB (IPMB Connector)

The IPMB connector is used to connect Intelligent Platform Management Bus (IPMB) devices in a computer system for remote monitoring and management capabilities..

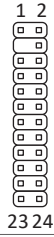
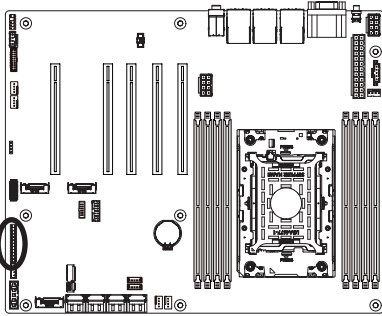


| Pin No. | Definition |
|---------|------------|
| 1       | Clock      |
| 2       | GND        |
| 3       | Data       |
| 4       | VCC        |



### 10) FP\_1 (Front Panel Header)

Connect the power switch, reset switch, speaker, chassis intrusion switch/sensor and system status indicator on the chassis to this header according to the pin assignments below. Note the positive and negative pins before connecting the cables.

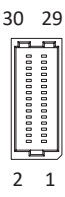
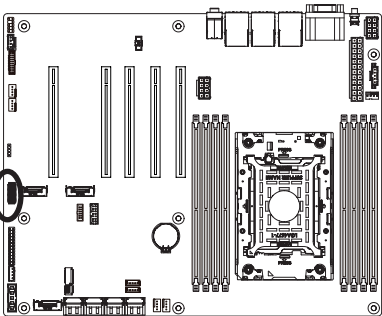


| Pin No. | Definition   | Pin No. | Definition         |
|---------|--------------|---------|--------------------|
| 1       | Power LED+   | 2       | 5V Standby         |
| 3       | No Pin       | 4       | ID LED+            |
| 5       | Power LED-   | 6       | ID LED-            |
| 7       | HDD LED+     | 8       | System Status LED+ |
| 9       | HDD LED-     | 10      | System Status LED- |
| 11      | Power Button | 12      | LAN1 Active LED+   |
| 13      | GND          | 14      | LAN1 Link LED-     |
| 15      | Reset Button | 16      | SMBus Data         |
| 17      | GND          | 18      | SMBus Clock        |
| 19      | ID Button    | 20      | Case Open          |
| 21      | GND          | 22      | LAN2 Active LED+   |
| 23      | NMI Switch   | 24      | LAN2 Link LED-     |



The front panel design may differ by chassis. A front panel module mainly consists of power switch, reset switch, power LED, hard drive activity LED, speaker etc. When connecting your chassis front panel module to this header, make sure the wire assignments and the pin assignments are matched correctly.

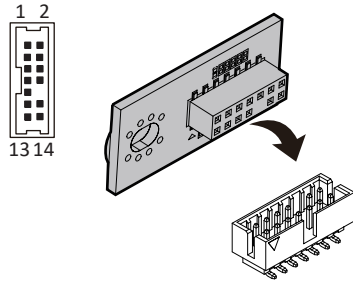
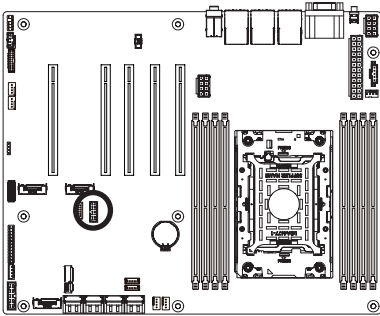
### 11) BP\_1 (HDD Backplane Board Connector)



| Pin No. | Definition     | Pin No. | Definition     |
|---------|----------------|---------|----------------|
| 1       | HP_ALERT_L     | 2       | BPMI DIN/OUT   |
| 3       | GND            | 4       | BPMI DOUT/IN   |
| 5       | BPMI_LOAD      | 6       | GND            |
| 7       | BPMI_CLK       | 8       | PLD_Program_EN |
| 9       | GLED_AMB_N     | 10      | GLED_GRN_N     |
| 11      | FAN_IRQ_N      | 12      | Reserved       |
| 13      | BP_SCL         | 14      | GND            |
| 15      | BP_SDA         | 16      | BP_RST_N       |
| 17      | SMB_U2_TMP_SCL | 18      | GND            |
| 19      | SMB_U2_TMP_SDA | 20      | I2C_DEV_RST    |
| 21      | PH_HP_SCL0     | 22      | GND            |
| 23      | PH_HP_SDA0     | 24      | GND            |
| 25      | PH_HP_SCL1     | 26      | GND            |
| 27      | PH_HP_SDA1     | 28      | GND            |
| 29      | P3V3_AUX       | 30      | P3V3_AUX       |

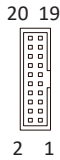
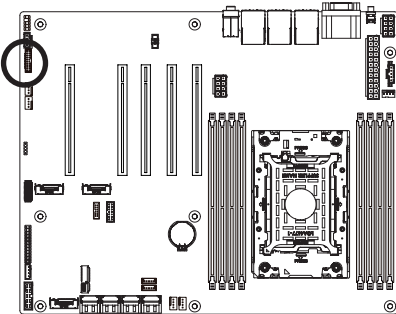
## 12) TPM (Trusted Platform Module Connector)

Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.



| Pin No. | Definition | Pin No. | Definition |
|---------|------------|---------|------------|
| 1       | Clock      | 8       | No Connect |
| 2       | P_3V3_AUX  | 9       | No Connect |
| 3       | LPC_RST    | 10      | No Pin     |
| 4       | No Connect | 11      | No Connect |
| 5       | SPI_MISO   | 12      | GND        |
| 6       | IRQ_SPI    | 13      | SPI_CS_N   |
| 7       | SPI_MOSI   | 14      | GND        |

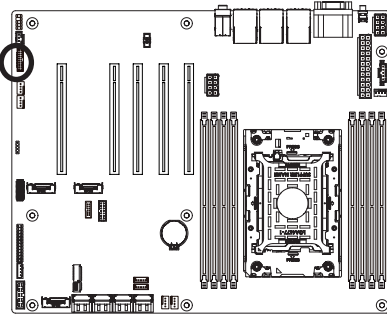
## 16) CN\_NCSI (NCSI Connector)



| Pin No. | Definition   | Pin No. | Definition |
|---------|--------------|---------|------------|
| 1       | NCSI_CLK     | 2       | GND        |
| 3       | NCSI_RX_D0   | 4       | GND        |
| 5       | NCSI_RX_D1   | 6       | GND        |
| 7       | NCSI_CRD_V   | 8       | GND        |
| 9       | NCSI_RX_ER   | 10      | GND        |
| 11      | P3V3_AUX     | 12      | GND        |
| 13      | NCSI_TX_D1   | 14      | GND        |
| 15      | NCSI_TX_D0   | 16      | GND        |
| 17      | NCSI_TX_EN   | 18      | GND        |
| 19      | NCSI_PRESENT | 20      | P3V3_AUX   |

### 17) F\_AUDIO (Front Panel Audio Header)

The front panel audio header supports High Definition audio (HD). You may connect your chassis front panel audio module to this header. Make sure the wire assignments of the module connector match the pin assignments of the motherboard header. Incorrect connection between the module connector and the motherboard header will make the device unable to work or even damage it.



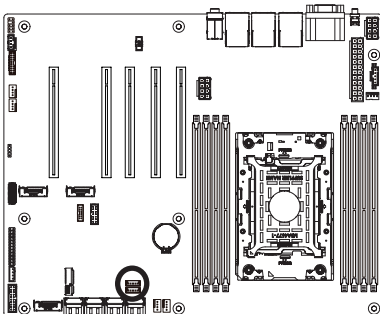
| Pin No. | Definition  |
|---------|-------------|
| 1       | MIC-L       |
| 2       | GND         |
| 3       | MIC-R       |
| 4       | Power(3.3V) |
| 5       | LINE-R-     |
| 6       | GND         |
| 7       | AUDIO_JD    |
| 8       | NA          |
| 9       | LINE-L      |
| 10      | GND         |



Some chassis provide a front panel audio module that has separated connectors on each wire instead of a single plug. For information about connecting the front panel audio module that has different wire assignments, please contact the chassis manufacturer

### 18) SGPIO\_1\_2 (SATA SGPIO) Connector

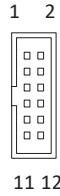
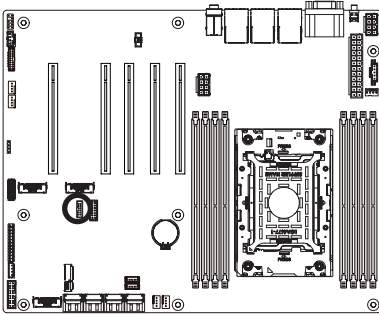
Serial General Purpose Input/Output (SGPIO) is a communication method used between a host bus adapter (HBA) and a main board.



| Pin No. | Definition     |
|---------|----------------|
| 1       | SGPIO DATA OUT |
| 2       | GND            |
| 3       | No Pin         |
| 4       | SGPIO LOAD     |
| 5       | SGPIO CLOCK    |

## 19) DP ESPI

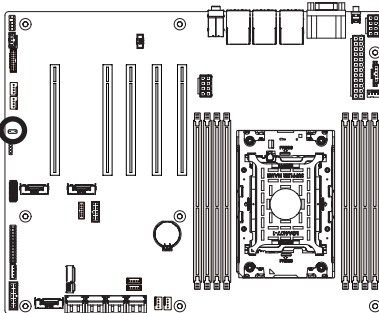
Connect the DisplayPort and Enhanced Serial Peripheral Interface (ESPI) interfaces for communication between a computer's chipset and a monitor's embedded controller.



| Pin No. | Definition    |
|---------|---------------|
| 1       | Clock 24M_66M |
| 2       | GND           |
| 3       | ESPI_CS0_N    |
| 4       | ESPI_IO0_LAD0 |
| 5       | ESPI_RST_N    |
| 6       | ESPI_IO1_LAD1 |
| 7       | ESPI_IO3      |
| 8       | ESPI_IO2_LAD2 |
| 9       | ESPI_ALERT0_N |
| 10      | ESPI_ALERT1_N |
| 11      | VCC           |
| 12      | ESPI_CS1_N    |

## 20) CASE\_OPEN (Case Open Intrusion Alert Header)

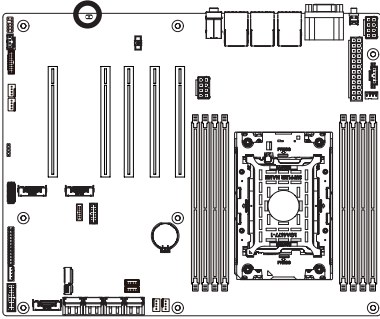
This motherboard provides a chassis detection feature that detects if the chassis cover has been removed. This function requires a chassis with chassis intrusion detection design.



- Open: Normal Operation (Default)
- Closed: Active Chassis Intrusion Alert

## 21) LED\_BMC (BMC Firmware Readiness LED)

This motherboard provides a chassis detection feature that detects if the chassis cover has been removed. This function requires a chassis with chassis intrusion detection design.



| State | Description             |
|-------|-------------------------|
| On    | BMC firmware is initial |
| Blink | BMC firmware is ready   |
| Off   | AC loss                 |



## Chapter 2 BIOS Setup

BIOS (Basic Input and Output System) records hardware parameters of the system in the EFI on the motherboard. Its major functions include conducting the Power-On Self-Test (POST) during system startup, saving system parameters, loading the operating system etc. The BIOS includes a BIOS Setup program that allows the user to modify basic system configuration settings or to activate certain system features. When the power is turned off, the battery on the motherboard supplies the necessary power to the CMOS to keep the configuration values in the CMOS.

To access the BIOS Setup program, press the <DEL> key during the POST when the power is turned on.



- BIOS flashing is potentially risky, if you do not encounter any problems when using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 1 for how to clear the CMOS values.)

### BIOS Setup Program Function Keys

|          |  |
|----------|--|
| <<-><->> | Move the selection bar to select the screen                              |
| <↑><↓>   | Move the selection bar to select an item                                 |
| <+>      | Increase the numeric value or make changes                               |
| <->      | Decrease the numeric value or make changes                               |
| <Enter>  | Execute command or enter the submenu                                     |
| <Esc>    | Main Menu: Exit the BIOS Setup program<br>Submenus: Exit current submenu |
| <F1>     | Show descriptions of general help  |
| <F3>     | Restore the previous BIOS settings for the current submenus              |
| <F9>     | Load the Optimized BIOS default settings for the current submenus        |
| <F10>    | Save all the changes and exit the BIOS Setup program                     |

■ **Main**

This setup page includes all the items of the standard compatible BIOS.

■ **Advanced**

This setup page includes all the items of AMI BIOS special enhanced features.

(ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)

■ **Chipset**

This setup page includes all the submenu options for configuring the functions of the Platform Controller Hub.

■ **Server Management**

Server additional features enabled/disabled setup menus.

■ **Security**

Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.

A supervisor password allows you to make changes in BIOS Setup.

A user password only allows you to view the BIOS settings but not to make changes.

■ **Boot**

This setup page provides items for configuration of the boot sequence.

■ **Save & Exit**

Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)

Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)



## 2-1 The Main Menu

Once you enter the BIOS Setup program, the Main Menu (as shown below) appears on the screen. Use arrow keys to move among the items and press <Enter> to accept or enter other sub-menu.

### Main Menu Help

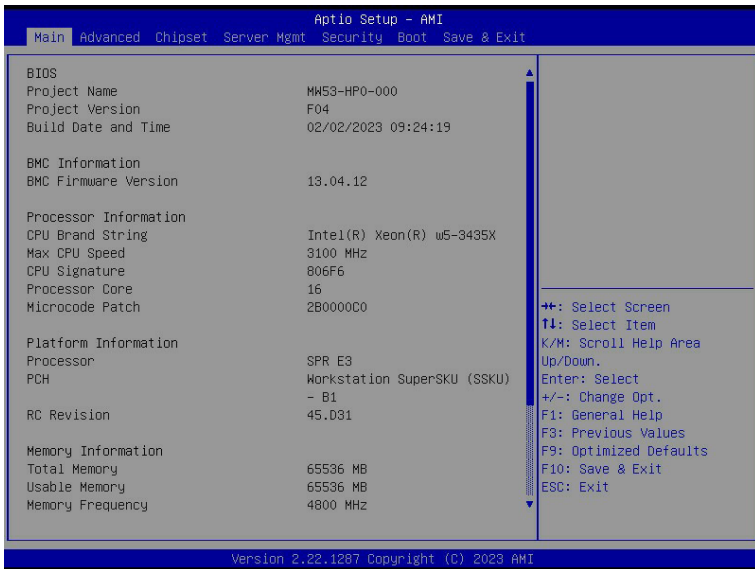
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

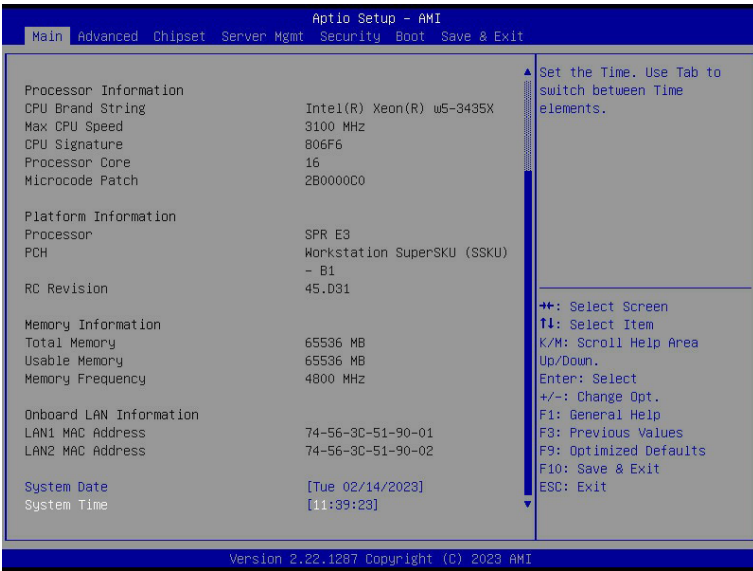
### Submenu Help

While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.



- When the system is not stable as usual, select the **Restore Defaults** item to set your system to its defaults.
- The BIOS Setup menus described in this chapter are for reference only and may differ by BIOS version.





| Parameter  | Description   |
|--|---|
| <b>BIOS Information</b>  |   |
| Project Name   | Displays the project name information.                              |
| Project Version  | Displays version number of the BIOS setup utility.                  |
| Build Date and Time  | Displays the date and time when the BIOS setup utility was created. |
| <b>BMC Information<sup>(Note1)</sup></b>   |   |
| BMC Firmware Version <sup>(Note1)</sup>  | Displays BMC firmware version information.                          |
| <b>Processor Information</b>   |   |
| CPU Brand String/ Max CPU Speed / CPU Signature / Processor Core / Microcode Patch | Displays the technical information for the installed processor(s).  |
| <b>Platform Information</b>  |   |
| Processor/ PCH/ RC Revision  | Displays the information of the installed processor(s) and PCH.     |
| <b>Memory Information<sup>(Note2)</sup></b>  |   |
| Total Memory   | Displays the total memory size of the installed memory.             |
| Usable Memory  | Displays the usable memory size of the installed memory.            |

(Note1) Functions available on selected models.

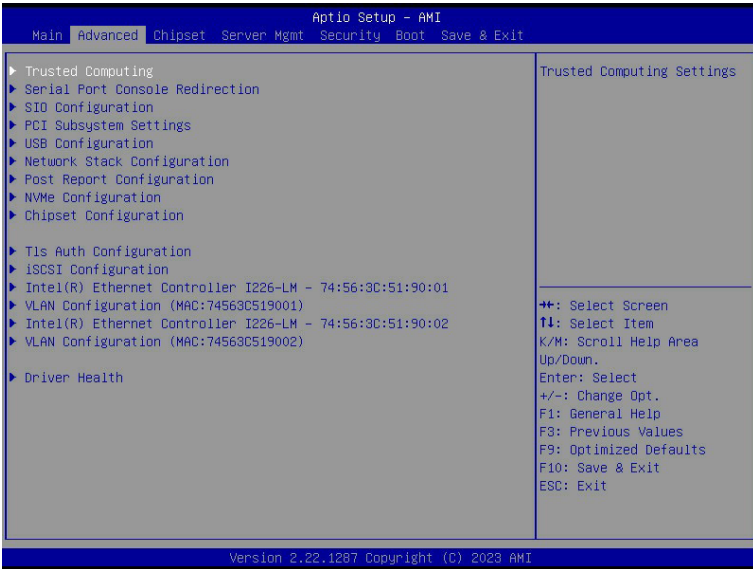
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

| <b>Parameter</b>                           | <b>Description</b>  |
|--|---|
| Memory Frequency                           | Displays the frequency information of the installed memory.   |
| Onboard LAN Information <sup>(Note3)</sup> |   |
| LAN# MAC Address                           | Displays LAN MAC address information.                         |
| System Date                                | Sets the date following the weekday-month-day-year format.    |
| System Time                                | Sets the system time following the hour-minute-second format. |

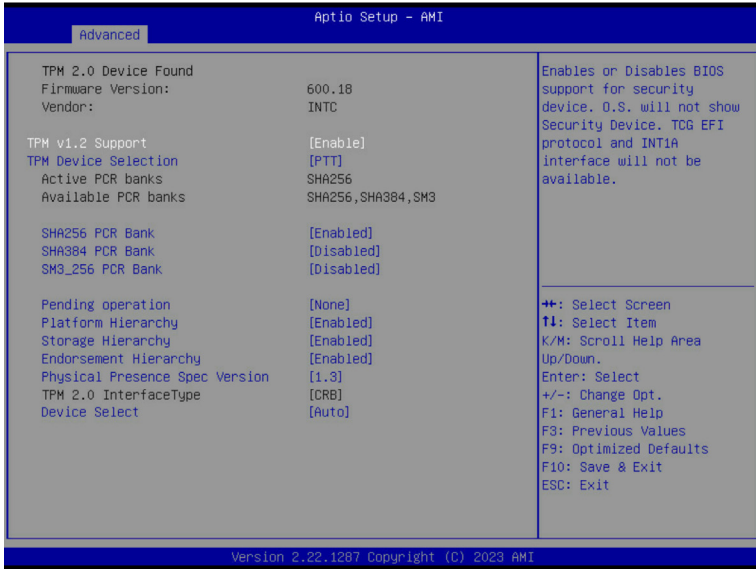
(Note3) The number of LAN ports listed will depend on the motherboard / system model.

## 2-2 Advanced Menu

The Advanced Menu displays submenu options for configuring the function of various hardware components. Select a submenu item, then press <Enter> to access the related submenu screen.



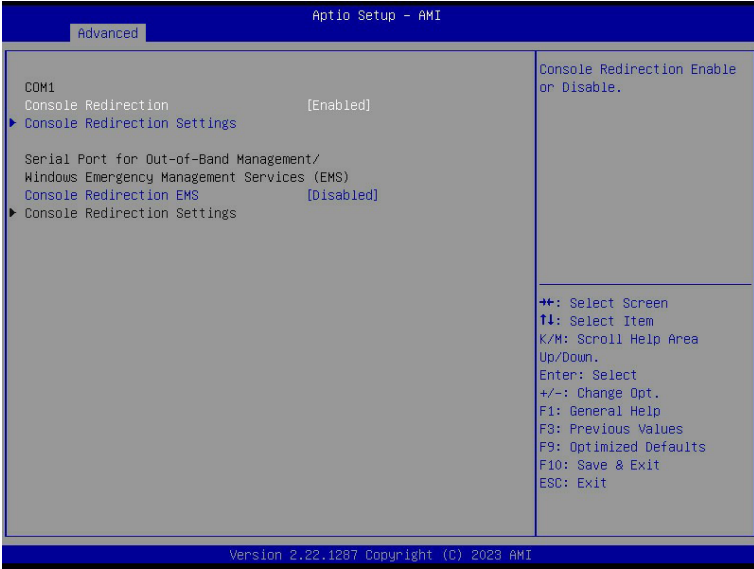
## 2-2-1 Trusted Computing



| Parameter                             | Description  |
|---------------------------------------|--|
| TPM 2.0 Device Found                  |  |
| Firmware Version/ Vendor              | Displays the firmware version and Vendor information.  |
| TPM v1.2 Support                      | Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.<br>Options available: Disable, Enable. Default setting is <b>Enable</b> . |
| TPM Device Selection                  | Selects TPM device.<br>Options available: dTPM, PTT. Default setting is <b>PTT</b> .   |
| Active PCR banks/ Available PCR banks | Displays active/available Platform Configuration Register (PCR) banks.   |
| SHA256 PCR Bank                       | Enable/Disable SHA256 PCR bank.<br>Options available: Disabled, Enabled. Default setting is <b>Enabled</b> .   |
| SHA384 PCR Bank                       | Enable/Disable SHA384 PCR bank.<br>Options available: Disabled, Enabled. Default setting is <b>Disabled</b> .  |
| SM3_256 PCR Bank                      | Enable/Disable SM3_256 PCR bank.<br>Options available: Disabled, Enabled. Default setting is <b>Disabled</b> .   |

| Parameter                      | Description   |
|--------------------------------|---|
| Pending operation              | Schedule an operation for the security device.<br>NOTE: Your computer will reboot during restart in order to change the state of a security device.<br>Options available: None, TPM Clear. Default setting is <b>None</b> . |
| Platform Hierarchy             | Enable/Disable platform hierarchy.<br>Options available: Disabled, Enabled. Default setting is <b>Enabled</b> .   |
| Storage Hierarchy              | Enable/Disable storage hierarchy.<br>Options available: Disabled, Enabled. Default setting is <b>Enabled</b> .  |
| Endorsement Hierarchy          | Enable/Disable endorsement hierarchy.<br>Options available: Disabled, Enabled. Default setting is <b>Enabled</b> .  |
| Physical Presence Spec Version | Selects the physical presence spec version.<br>Options available: 1.2, 1.3. Default setting is <b>1.3</b> .   |
| TPM 20 InterfaceType           | Displays the TPM 2.0 interface type.  |
| Device Select                  | Selects the TPM device.<br>Options available: TPM 1.2, TPM 2.0, Auto. Default setting is <b>Auto</b> .  |

## 2-2-2 Serial Port Console Redirection



| Parameter                                  | Description   |
|--|---|
| COM1 Console Redirection <sup>(Note)</sup> | <p>Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</p>  |
| COM1 Console Redirection Settings          | <p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when COM1 Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Terminal Type <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is <b>VT100PLUS</b>.</li> </ul> </li> <li>◆ Bits per second <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 38400, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> <li>◆ Data Bits <ul style="list-style-type: none"> <li>– Selects the number of data bits used for console redirection.</li> <li>– Options available: 7, 8. Default setting is <b>8</b>.</li> </ul> </li> </ul> |

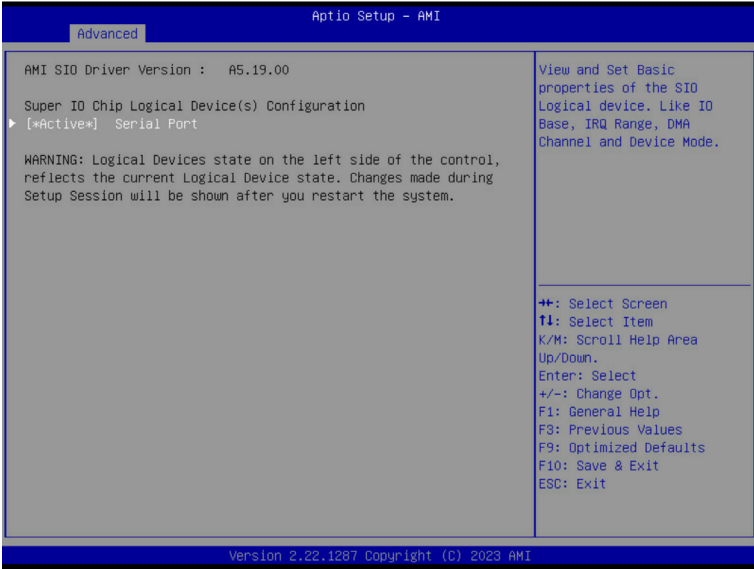
(Note) Advanced items prompt when this item is defined.

| Parameter                                     | Description   |
|---|---|
| COM1 Console Redirection Settings (continued) | <ul style="list-style-type: none"> <li>◆ Parity <ul style="list-style-type: none"> <li>– A parity bit can be sent with the data bits to detect some transmission errors.</li> <li>– Even: parity bit is 0 if the num of 1's in the data bits is even.</li> <li>– Odd: parity bit is 0 if num of 1's in the data bits is odd.</li> <li>– Mark: parity bit is always 1. Space: Parity bit is always 0.</li> <li>– Mark and Space Parity do not allow for error detection.</li> <li>– Options available: None, Even, Odd, Mark, Space. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ Stop Bits <ul style="list-style-type: none"> <li>– Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.</li> <li>– Options available: 1, 2. Default setting is <b>1</b>.</li> </ul> </li> <li>◆ Flow Control <ul style="list-style-type: none"> <li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li> <li>– Options available: None, Hardware RTS/CTS. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ VT-UTF8 Combo Key Support <ul style="list-style-type: none"> <li>– Enable/Disable the VT-UTF8 Combo Key Support.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Recorder Mode <ul style="list-style-type: none"> <li>– When this mode enabled, only texts will be send. This is to capture Terminal data.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Resolution 100x31 <ul style="list-style-type: none"> <li>– Enable/Disable extended terminal resolution.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Putty Keypad <ul style="list-style-type: none"> <li>– Selects Function Key and Keypad on Putty.</li> <li>– Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is <b>VT100</b>.</li> </ul> </li> </ul> |



| Parameter  | Description  |
|--|--|
| Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection <sup>(Note)</sup> | <p>EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.</p> <p>Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</p>   |
| Serial Port for Out-of-Band EMS Console Redirection Settings   | <p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Out-of-Band Mgmt Port <ul style="list-style-type: none"> <li>– Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port.</li> <li>– Default setting is <b>COM1</b>.</li> </ul> </li> <li>◆ Terminal Type EMS <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is <b>VT100PLUS</b>.</li> </ul> </li> <li>◆ Bits per second EMS <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> <li>◆ Flow Control EMS <ul style="list-style-type: none"> <li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li> <li>– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is <b>None</b>.</li> </ul> </li> </ul> |

## 2-2-3 SIO Configuration



| Parameter                                     | Description   |
|---|---|
| AMI SIO Driver Version                        | Displays the AMI SIO driver version information.  |
| Super IO Chip Logical Device(s) Configuration | Press [Enter] to configure advanced items.  |
| [*Active*] Serial Port                        | <ul style="list-style-type: none"> <li>◆ Use This Device               <ul style="list-style-type: none"> <li>– When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Logical Device Settings/Current:               <ul style="list-style-type: none"> <li>– Displays the serial port base I/O address and IRQ.</li> </ul> </li> <li>◆ Possible:               <ul style="list-style-type: none"> <li>– Configures the serial port base I/O address and IRQ.                   <ul style="list-style-type: none"> <li>Use Automatic Settings</li> <li>IO=3F8h; IRQ=4; DMA;</li> <li>IO=3F8h; IRQ=4; DMA;</li> <li>IO=2F8h; IRQ=4; DMA;</li> <li>IO=3E8h; IRQ=4; DMA;</li> <li>IO=2E8h; IRQ=4; DMA;</li> </ul> </li> <li>Default setting is <b>Use Automatic Settings</b>.</li> </ul> </li> </ul> |

## 2-2-4 PCI Subsystem Settings

Aptio Setup - AMI

| Advanced               |           |  |
|------------------------|-----------|--|
| PCI Bus Driver Version | A5.01.29  | Enable/Disable PCIe_2 I/O ROM<br><br>++: Select Screen<br>T1: Select Item<br>K/M: Scroll Help Area Up/Down.<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F8: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |
| PCIE_2 I/O ROM         | [Enabled] |  |
| PCIE_2 Lanes           | [Auto]    |  |
| PCIE_2 Max Link Speed  | [Auto]    |  |
| PCIE_4 I/O ROM         | [Enabled] |  |
| PCIE_4 Lanes           | [Auto]    |  |
| PCIE_4 Max Link Speed  | [Auto]    |  |
| PCIE_5 I/O ROM         | [Enabled] |  |
| PCIE_5 Lanes           | [Auto]    |  |
| PCIE_5 Max Link Speed  | [Auto]    |  |
| PCIE_6 I/O ROM         | [Enabled] |  |
| PCIE_6 Lanes           | [Auto]    |  |
| PCIE_6 Max Link Speed  | [Auto]    |  |
| PCIE_7 I/O ROM         | [Enabled] |  |
| PCIE_7 Lanes           | [Auto]    |  |
| PCIE_7 Max Link Speed  | [Auto]    |  |
| M2_0 I/O ROM           | [Enabled] |  |
| M2_0 Lanes             | [Auto]    |  |
| M2_0 Max Link Speed    | [Auto]    |  |

Version 2.22.1287 Copyright (C) 2023 AMI

Aptio Setup - AMI

| Advanced                     |           |  |
|------------------------------|-----------|--|
| PCIE_7 Lanes                 | [Auto]    | If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root ID Virtualization Support.<br><br>++: Select Screen<br>T1: Select Item<br>K/M: Scroll Help Area Up/Down.<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F8: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |
| PCIE_7 Max Link Speed        | [Auto]    |  |
| M2_0 I/O ROM                 | [Enabled] |  |
| M2_0 Lanes                   | [Auto]    |  |
| M2_0 Max Link Speed          | [Auto]    |  |
| M2_1 I/O ROM                 | [Enabled] |  |
| M2_1 Lanes                   | [Auto]    |  |
| M2_1 Max Link Speed          | [Auto]    |  |
| M2_2 I/O ROM                 | [Enabled] |  |
| M2_2 Lanes                   | [Auto]    |  |
| M2_2 Max Link Speed          | [Auto]    |  |
| M2_E I/O ROM                 | [Enabled] |  |
| Onboard LAN1 Controller      | [Enabled] |  |
| Onboard LAN2 Controller      | [Enabled] |  |
| Onboard LAN1 I/O ROM         | [Enabled] |  |
| Onboard LAN2 I/O ROM         | [Enabled] |  |
| PCI Devices Common Settings: |           |  |
| Above 4G Decoding            | [Enabled] |  |
| SR-IOV Support               | [Enabled] |  |

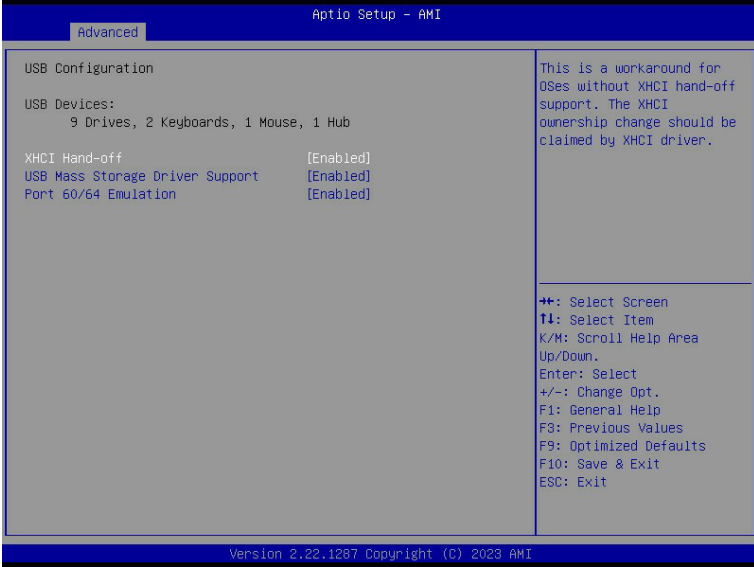
Version 2.22.1287 Copyright (C) 2023 AMI

| Parameter   | Description   |
|---|---|
| PCI Bus Driver Version                            | Displays the PCI Bus Driver version information.  |
| PCIE_# I/O ROM <sup>(Note1)</sup>                 | When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                |
| PCIE_# Lanes <sup>(Note1)</sup>                   | Change the PCIe lanes. Default setting is <b>Auto</b> .   |
| PCIE_#_Max Link Speed <sup>(Note1)</sup>          | Configure PCIe max link speed.<br>Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5.<br>Default setting is <b>Auto</b> .  |
| Onboard LAN1 & LAN2 Controller <sup>(Note3)</sup> | Enable/Disable the onboard LAN devices.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .  |
| Onboard LAN1/ LAN2 I/O ROM <sup>(Note2)</sup>     | Enable/Disable the onboard LAN devices, and initializes device expansion ROM.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                                  |
| PCI Devices Common Settings                       |   |
| Above 4G Decoding                                 | Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding).<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                          |
| SR-IOV Support                                    | If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> . |

(Note1) This section is dependent on the available PCIe Slot.

(Note2) This section is dependent on the available LAN controller.

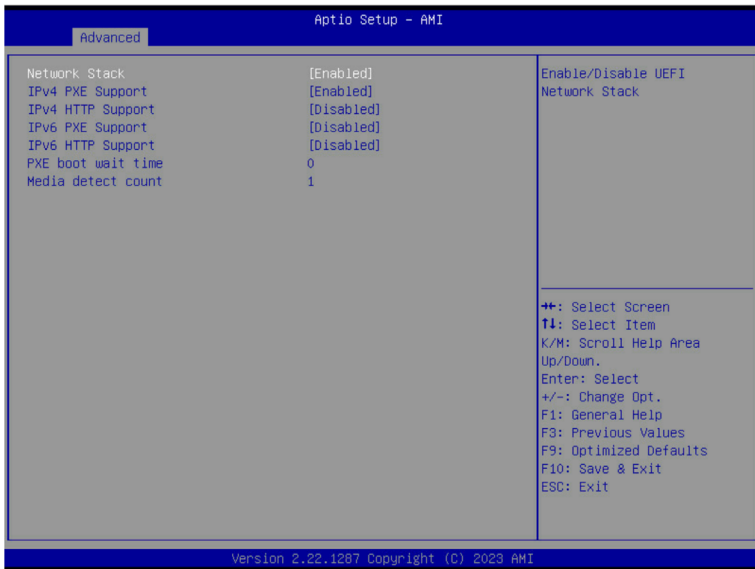
## 2-2-5 USB Configuration



| Parameter   | Description  |
|---|--|
| USB Configuration                                 |  |
| USB Devices:                                      | Displays the USB devices connected to the system.  |
| XHCI Hand-off                                     | Enable/Disable the XHCI (USB 3.0) Hand-off support.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .   |
| USB Mass Storage Driver Support <sup>(Note)</sup> | Enable/Disable the USB Mass Storage Driver Support.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .   |
| Port 60/64 Emulation                              | Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OSes.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> . |

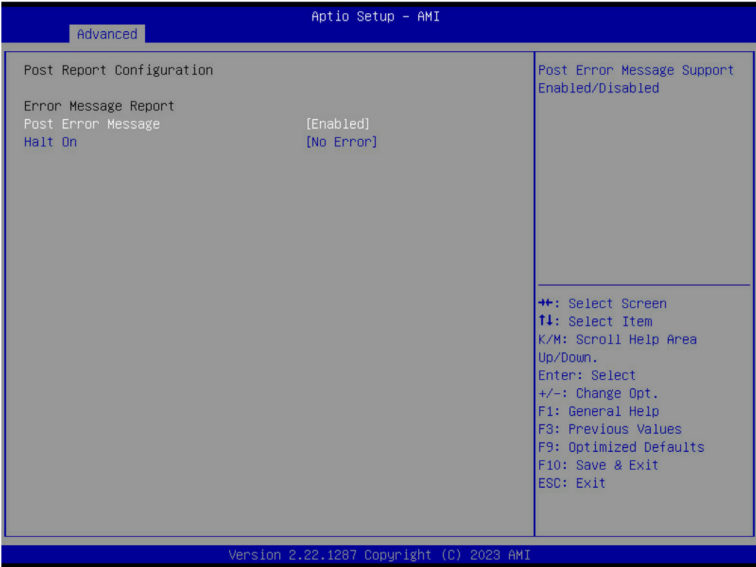
(Note) This item is present only if you attach USB devices.

## 2-2-6 Network Stack Configuration



| Parameter          | Description  |
|--------------------|--|
| Network Stack      | Enable/Disable the UEFI network stack.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                  |
| Ipv4 PXE Support   | Enable/Disable the Ipv4 PXE feature.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                    |
| Ipv4 HTTP Support  | Enable/Disable the Ipv4 HTTP feature.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .                  |
| Ipv6 PXE Support   | Enable/Disable the Ipv6 PXE feature.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .                   |
| Ipv6 HTTP Support  | Enable/Disable the Ipv6 HTTP feature.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .                  |
| PXE boot wait time | Wait time in seconds to press ESC key to abort the PXE boot.<br>Press the <+> / <-> keys to increase or decrease the desired values. |
| Media detect count | Number of times the presence of media will be checked.<br>Press the <+> / <-> keys to increase or decrease the desired values.       |

## 2-2-7 Post Report Configuration



| Parameter                 | Description   |
|---------------------------|---|
| Post Report Configuration |   |
| Error Message Report      |   |
| Post Error Message        | Enable/Disable the POST Error Message support.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> . |
| Halt On                   | Options available: No Error, All Error. Default setting is <b>No Error</b> .  |

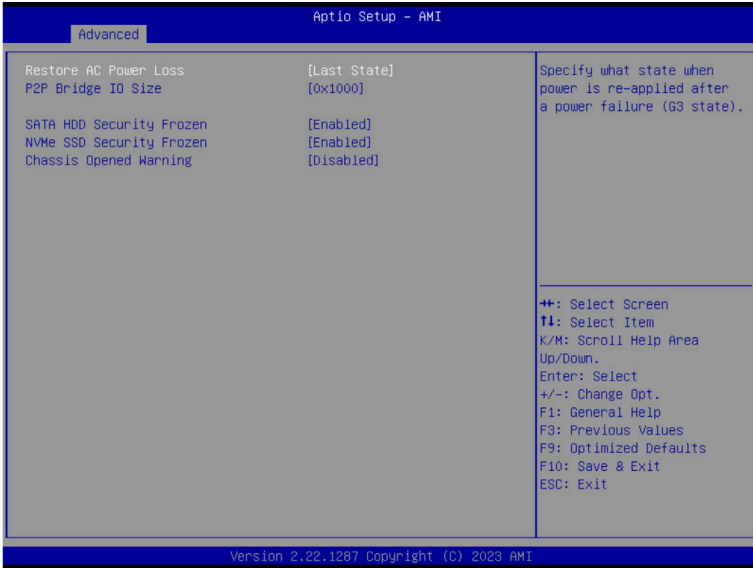
## 2-2-8 NVMe Configuration



| Parameter          | Description  |
|--------------------|--|
| NVMe Configuration | Displays the NVMe devices connected to the system.                                       |
| NVMe OPROM Select  | Options available: BIOS Build-In, NVMe Device. Default setting is <b>BIOS Build-In</b> . |



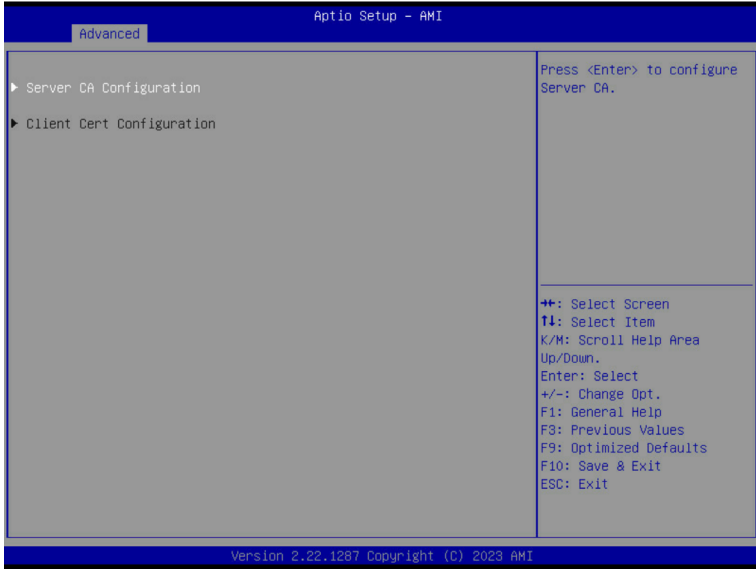
## 2-2-9 Chipset Configuration



| Parameter                                  | Description   |
|--|---|
| Restore on AC Power Loss <sup>(Note)</sup> | Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting. |
| P2P Bridge IO Size                         | Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is <b>0x1000</b> .  |
| SATA HDD Security Frozen                   | Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .   |
| NVMe SSD Security Frozen                   | Attempt to send freeze lock command to NVMe SSDs during boot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .   |
| Chassis Opened Warning                     | Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is <b>Disabled</b> .  |

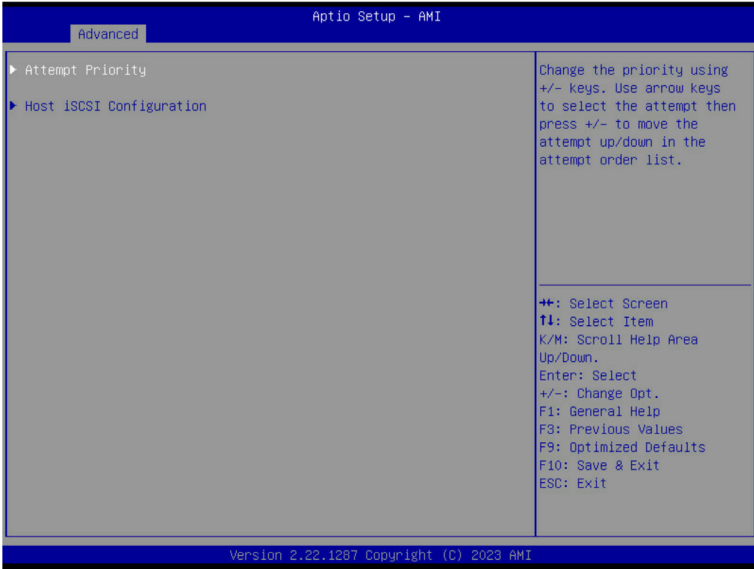
(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

## 2-2-10 Tls Auth Configuration



| Parameter                 | Description   |
|---------------------------|---|
| Server CA Configuration   | <p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ Enroll Cert <ul style="list-style-type: none"> <li>– Press [Enter] to enroll a certificate <ul style="list-style-type: none"> <li>• Enroll Cert Using File</li> <li>• Cert GUID</li> </ul> </li> <li>Input digit character in 1111111-2222-3333-4444-1234567890ab format.</li> <li>– Commit Changes and Exit</li> <li>– Discard Changes and Exit</li> </ul> </li> <li>◆ Delete Cert</li> </ul> |
| Client Cert Configuration | Press [Enter] for configuration of advanced items.  |

## 2-2-11 iSCSI Configuration



| Parameter                | Description  |
|--------------------------|--|
| Attempt Priority         | <p>Press [Enter] configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Attempt Priority                             <ul style="list-style-type: none"> <li>– Use arrow keys to select the attempt, then press +/- keys to move the attempt up/down in the attempt order list.</li> </ul> </li> <li>◆ Commit Changes and Exit</li> </ul> |
| Host iSCSI Configuration | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ iSCSI Initiator Name                             <ul style="list-style-type: none"> <li>– Only IQN format is accepted. Range: from 4 to 223</li> </ul> </li> <li>◆ Add an Attempt</li> <li>◆ Delete Attempts</li> <li>◆ Change Attempt Order</li> </ul>       |

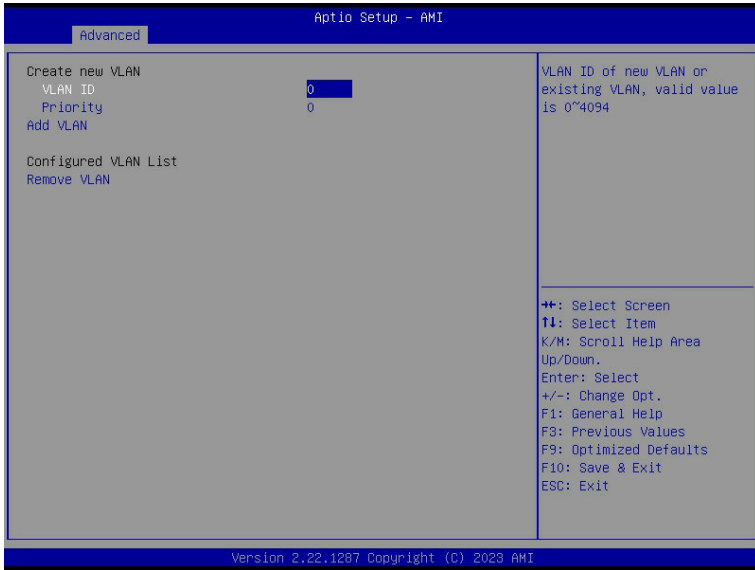
## 2-2-12 Intel(R) Ethernet Controller X710 for 10GBASE-T

| Advanced  |  | Aptio Setup - AMI  |  |
|---|--|--|--|
| <p>▶ NIC Configuration</p> <p>Blink LEDs 0</p> <p>UEFI Driver Intel(R) 40GbE 3.5.23<br/>           Adapter PBA H64862-000<br/>           Device Name Intel(R) Ethernet Controller X710 for 10GBASE-T</p> <p>Chip Type Intel X710<br/>           PCI Device ID 15FF<br/>           PCI Address 01:00:00</p> <p>Link Status [Connected]</p> <p>MAC Address 00:00:00:00:01:00<br/>           Virtual MAC Address 00:00:00:00:00:00</p> |  | <p>Click to configure the network device port.</p>   |  |
|   |  | <p>++: Select Screen<br/>           T1: Select Item<br/>           K/M: Scroll Help Area Up/Down.<br/>           Enter: Select<br/>           +/-: Change Opt.<br/>           F1: General Help<br/>           F8: Previous Values<br/>           F9: Optimized Defaults<br/>           F10: Save &amp; Exit<br/>           ESC: Exit</p> |  |
| Version 2.22.1287 Copyright (C) 2023 AMI  |  |  |  |

| Advanced   |  | Aptio Setup - AMI  |  |
|--|--|--|--|
| <p>Link Speed [Auto Negotiated]</p> <p>Wake On LAN [Enabled]</p> <p>LLDP Agent [Enabled]</p> |  | <p>Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.</p>   |  |
|  |  | <p>++: Select Screen<br/>           T1: Select Item<br/>           K/M: Scroll Help Area Up/Down.<br/>           Enter: Select<br/>           +/-: Change Opt.<br/>           F1: General Help<br/>           F8: Previous Values<br/>           F9: Optimized Defaults<br/>           F10: Save &amp; Exit<br/>           ESC: Exit</p> |  |
| Version 2.22.1287 Copyright (C) 2023 AMI   |  |  |  |

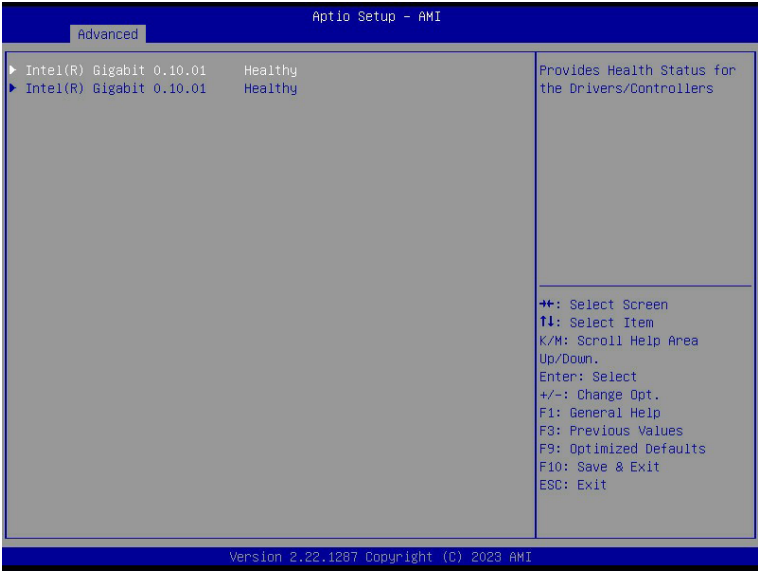
| Parameter           | Description  |
|---------------------|--|
| NIC Configuration   | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Link Speed <ul style="list-style-type: none"> <li>– Default setting is <b>Auto Negotiated</b>.</li> </ul> </li> <li>◆ Wake On LAN <ul style="list-style-type: none"> <li>– Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ LLDP Agent <ul style="list-style-type: none"> <li>– Enable/Disable firmware's LLDP Agent.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b></li> </ul> </li> </ul> |
| Blink LEDs          | <p>Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).</p>  |
| UEFI Driver         | Displays the technical specifications for the Network Interface Controller.  |
| Adapter PBA         | Displays the technical specifications for the Network Interface Controller.  |
| Device Name         | Displays the technical specifications for the Network Interface Controller.  |
| Chip Type           | Displays the technical specifications for the Network Interface Controller.  |
| PCI Device ID       | Displays the technical specifications for the Network Interface Controller.  |
| PCI Address         | Displays the technical specifications for the Network Interface Controller.  |
| Link Status         | Displays the technical specifications for the Network Interface Controller.  |
| MAC Address         | Displays the technical specifications for the Network Interface Controller.  |
| Virtual MAC Address | Displays the technical specifications for the Network Interface Controller.  |

## 2-2-13 VLAN Configuration



| Parameter                | Description   |
|--------------------------|---|
| Enter Configuration Menu | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Create new VLAN</li> <li>◆ VLAN ID                             <ul style="list-style-type: none"> <li>– Sets VLAN ID for a new VLAN or an existing VLAN.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li>– The valid range is from 0 to 4094.</li> </ul> </li> <li>◆ Priority                             <ul style="list-style-type: none"> <li>– Sets 802.1Q Priority for a new VLAN or an existing VLAN.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li>– The valid range is from 0 to 7.</li> </ul> </li> <li>◆ Add VLAN                             <ul style="list-style-type: none"> <li>– Press [Enter] to create a new VLAN or update an existing VLAN.</li> </ul> </li> <li>◆ Configured VLAN List</li> <li>◆ Remove VLAN                             <ul style="list-style-type: none"> <li>– Press [Enter] to remove an existing VLAN.</li> </ul> </li> </ul> |

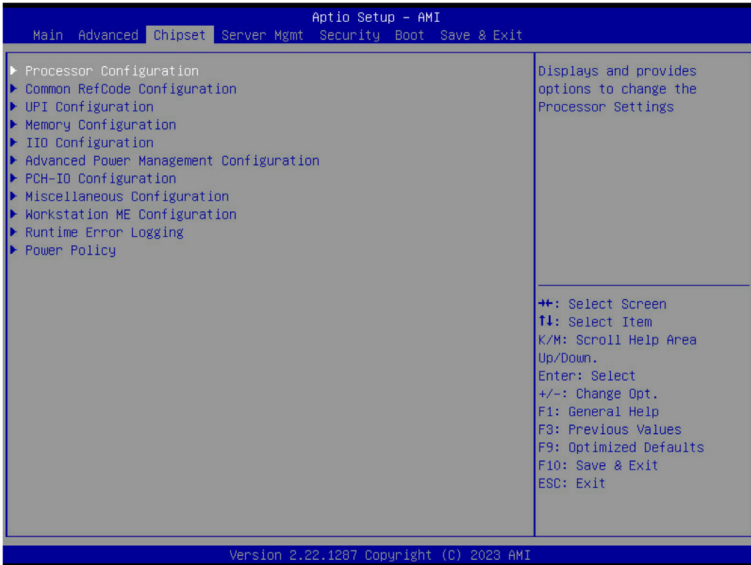
## 2-2-14 Driver Health



| Parameter     | Description  |
|---------------|--|
| Driver Health | Displays driver health status of the devices/controllers if installed. |

## 2-3 Chipset Menu

Chipset Setup menu displays submenu options for configuring the function of Platform Controller Hub(PCH). Select a submenu item, then press <Enter> to access the related submenu screen.





## 2-3-1 Processor Configuration

Aptio Setup - AMI

Chipset

| Processor Configuration    |                               | Change Per-Socket Settings   |
|----------------------------|-------------------------------|--|
| -----                      |                               |  |
| ▶ Per-Socket Configuration |                               |  |
| Processor Socket           | Socket 0                      | ++: Select Screen<br>↑↓: Select Item<br>K/M: Scroll Help Area<br>Up/Down.<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |
| Processor ID               | 000806F6*                     |  |
| Processor Die Type         | XCC                           |  |
| Processor Frequency        | 3.100GHz                      |  |
| Processor Max Ratio        | 1FH                           |  |
| Processor Min Ratio        | 06H                           |  |
| Microcode Revision         | 2B0000C0                      |  |
| L1 Cache RAM(Per Core)     | 80KB                          |  |
| L2 Cache RAM(Per Core)     | 2048KB                        |  |
| L3 Cache RAM(Per Package)  | 46080KB                       |  |
| Processor 0 Version        | Intel(R) Xeon(R) w5-343<br>5X |  |
| Enable LP [Global]         | [ALL LPs]                     |  |
| Hardware Prefetcher        | [Enable]                      |  |
| L2 RFO Prefetch Disable    | [Disable]                     |  |
| Adjacent Cache Prefetch    | [Enable]                      |  |
| DCU Streamer Prefetcher    | [Enable]                      |  |
| DCU IP Prefetcher          | [Enable]                      |  |
| Extended APIC              | [Enable]                      |  |
| Enable Intel(R) TXT        | [Disable]                     |  |
| VMX                        | [Enable]                      |  |

Version 2.22.1287 Copyright (C) 2023 AMI

Aptio Setup - AMI

Chipset

|  |                               |   |
|--|-------------------------------|---|
| L3 Cache RAM(Per Package)  | 46080KB                       | ▲ Displays and provides option to change the Processor CFR Settings |
| Processor 0 Version  | Intel(R) Xeon(R) w5-343<br>5X |   |
| Enable LP [Global]   | [ALL LPs]                     |   |
| Hardware Prefetcher  | [Enable]                      |   |
| L2 RFO Prefetch Disable  | [Disable]                     |   |
| Adjacent Cache Prefetch  | [Enable]                      |   |
| DCU Streamer Prefetcher  | [Enable]                      |   |
| DCU IP Prefetcher  | [Enable]                      |   |
| Extended APIC  | [Enable]                      |   |
| Enable Intel(R) TXT  | [Disable]                     |   |
| VMX  | [Enable]                      |   |
| Enable SMX   | [Disable]                     |   |
| AES-NI   | [Enable]                      |   |
| -----  |                               |   |
| TME, TME-MT, TDX   |                               |   |
| Memory Encryption (TME)  | [Disabled]                    |   |
| SGX hardware configuration preconditions for enabling were NOT met. SGX is NOT supported by the hardware.                |                               |   |
| SGX setup configuration preconditions for enabling were NOT met. Please check TME, MirrorMode or Extended APIC settings. |                               |   |
| -----  |                               |   |
| ▶ Processor CFR Configuration  |                               |   |

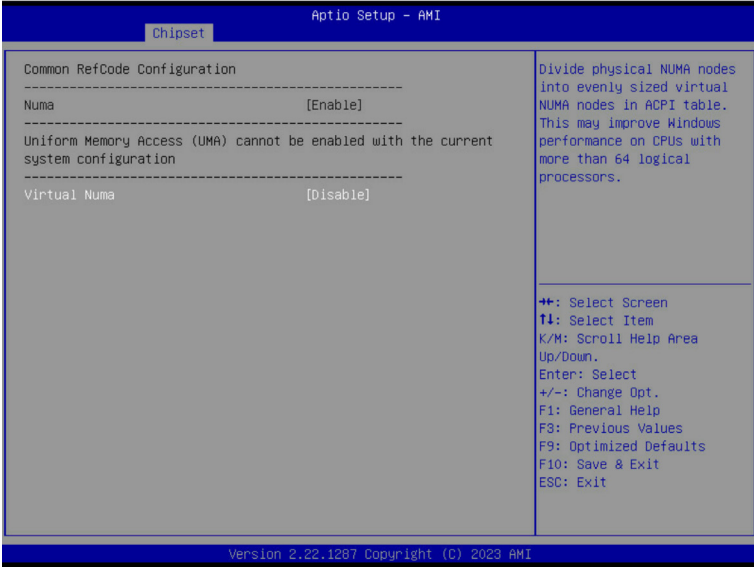
Version 2.22.1287 Copyright (C) 2023 AMI

| Parameter   | Description  |
|---|--|
| Processor Configuration   |  |
| Pre-Socket Configuration  | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ CPU Socket 0 Configuration <ul style="list-style-type: none"> <li>– Core Disable Bitmap(Hex) <ul style="list-style-type: none"> <li>• Number of Cores to enable. 0 means all cores. FFFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.</li> </ul> </li> </ul> </li> </ul> |
| Processor Socket / Processor ID / Processor Die Type / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Per Core) / L3 Cache RAM(Per Package) / Processor # Version | Displays the technical specifications for the installed processor(s).  |
| Enable LP [Global]  | <p>Enables Logical processor (Software Method to Enable/Disable Logical Processor threads).</p> <p>Options available: ALL LPs, Single LP. Default setting is <b>ALL LPs</b>.</p>   |
| Hardware Prefetcher   | <p>Select whether to enable the speculative prefetch unit of the processor.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>   |
| L2 RF0 Prefetch Disable   | Options available: Enable, Disable. Default setting is <b>Disable</b> .  |
| Adjacent Cache Prefetch   | <p>When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>  |
| DCU Streamer Prefetcher   | <p>Enable/Disable DCU streamer prefetcher.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>  |
| DCU IP Prefetcher   | <p>Enable/Disable DCU IP Prefetcher.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>  |
| Extended APIC   | <p>Enable/Disable extended APIC support. Note: The VT-d will be enabled automatically when x2APIC is enabled.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>   |
| Enable Intel(R) TXT   | <p>Enable/Disable the Intel Trusted Execution Technology support function.</p> <p>Options available: Enable, Disable. Default setting is <b>Disable</b>.</p>   |
| VMX   | <p>Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>  |
| Enable SMX  | <p>Enable/Disable the Safer Mode Extensions (SMX) support function.</p> <p>Options available: Enable, Disable. Default setting is <b>Disable</b>.</p>  |
| AES-NI  | <p>Enable/Disable the AES-NI support.</p> <p>Options available: Enable, Disable. Default setting is <b>Enable</b>.</p>   |

| Parameter                                     | Description  |
|---|--|
| Memory Encryption (TME) <sup>(Note)</sup>     | Enable/Disable memory encryption (TME).<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .  |
| Total Memory Encryption Multi-Tenant (TME-MT) | Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .   |
| Processor CFR Configuration                   | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Provision S3M CFR <ul style="list-style-type: none"> <li>– Options available: Disable, Enable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Manual Commit S3M FW CFR <ul style="list-style-type: none"> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Provision PUcode CFR <ul style="list-style-type: none"> <li>– Options available: Disable, Enable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Manual Commit PUcode CFR <ul style="list-style-type: none"> <li>– Options available: Enable, Disable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Socket0 CFR Revision Info <ul style="list-style-type: none"> <li>– Displays CFR Revision information of the socket.</li> </ul> </li> </ul> |

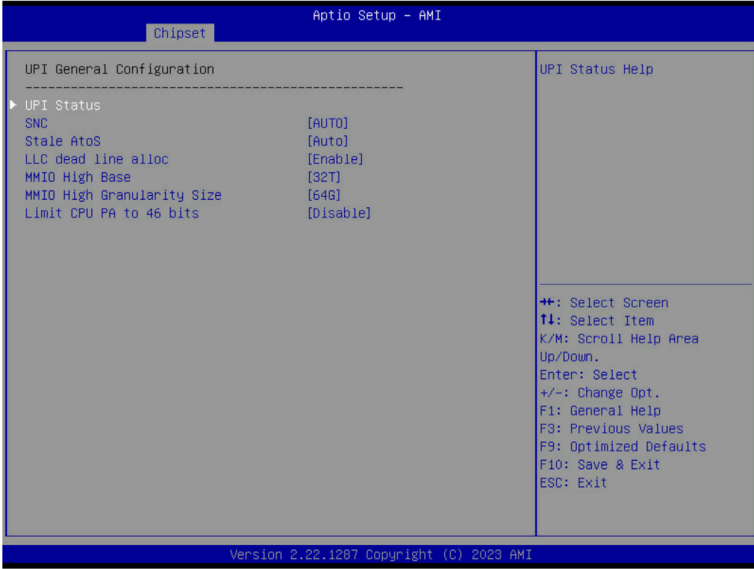
(Note) Advanced items prompt when this item is defined.

## 2-3-2 Common RefCode Configuration



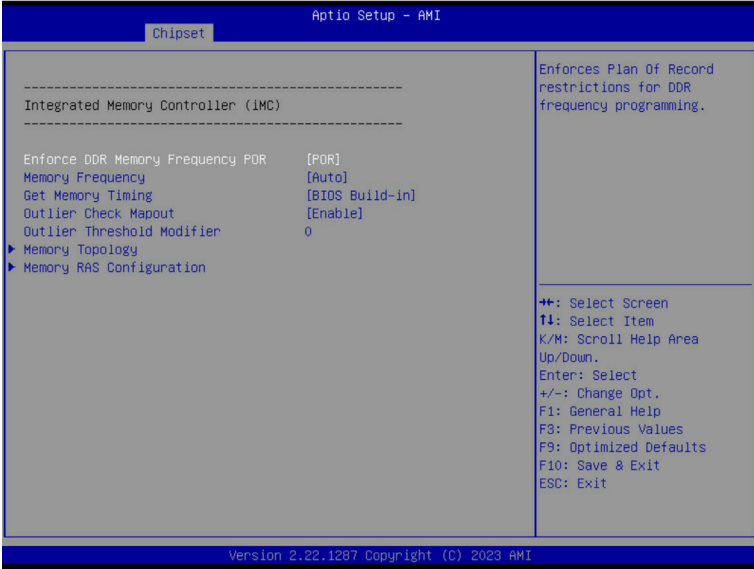
| Parameter                    | Description  |
|------------------------------|--|
| Common RefCode Configuration |  |
| Numa                         | Default setting is <b>Enable</b> .   |
| Virtual Numa                 | Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors.<br>Options available: Enable, Disable. Default setting is <b>Disable</b> . |

### 2-3-3 UPI Configuration



| Parameter                 | Description  |
|---------------------------|--|
| UPI General Configuration | Press [Enter] to configure advanced items.   |
|                           | <ul style="list-style-type: none"> <li>◆ UPI Status <ul style="list-style-type: none"> <li>– Press [Enter] to view the Uncore status.</li> </ul> </li> <li>◆ SNC <ul style="list-style-type: none"> <li>– Enable/Disable Sub NUMA Cluster function.</li> <li>– Options available: Auto, Disable, Enable SNC2 (2-clusters), Enable SNC4 (4-clusters). Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Stale AtoS <ul style="list-style-type: none"> <li>– Enable/Disable Stale A to S directory optimization.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ LLC dead line alloc <ul style="list-style-type: none"> <li>– Enable/Disable fill dead lines in LLC.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ MMIO High Base <ul style="list-style-type: none"> <li>– Options available: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T. Default setting is <b>32T</b>.</li> </ul> </li> <li>◆ MMIO High Granularity Size <ul style="list-style-type: none"> <li>– Selects the allocation size used to assign mmioh resources.</li> <li>– Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is <b>64G</b>.</li> </ul> </li> <li>◆ Limit CPU PA to 46 bits <ul style="list-style-type: none"> <li>– Options available: Disable, Enable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul> |

## 2-3-4 Memory Configuration



| Parameter                          | Description   |
|------------------------------------|---|
| Integrated Memory Controller (iMC) |   |
| Enforce DDR Memory Frequency POR   | When set to Enable, the system enforces Plan Of Record restrictions for DDR frequency programming.<br>Options available: POR, Disable. Default setting is <b>POR</b> .  |
| Memory Frequency                   | Configures the maximum memory frequency. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support).<br>Default setting is <b>Auto</b> . |
| Get Memory Timing                  | Auto is the detected SPD value and use it, otherwise use BIOS Build-in.<br>Options available: Auto, BIOS Build-in. Default setting is <b>BIOS Build-in</b> .  |
| Outlier Check Mapout               | Enable/Disable Vendor Specific DIMM Outlier check and mapout.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> .   |
| Outlier Threshold Modifier         | Specifies how much to modify the base outlier threshold.<br>Default setting is <b>0</b> .   |
| Memory Topology                    | Press [Enter] to view memory topology with DIMM population information.   |

| Parameter                | Description   |
|--------------------------|---|
| Memory RAS Configuration | <p data-bbox="391 142 724 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="391 169 953 341">◆ Mirror Mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li data-bbox="426 200 953 279">– Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch.</li> <li data-bbox="426 286 953 341">– Options available: Disabled, Full Mirror Mode, Partial Mirror Mode. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="391 349 953 396">◆ Partial Mirror 1 Size (GB) <ul style="list-style-type: none"> <li data-bbox="426 381 953 396">– Selects multiplier of 1GB for the size of the SAD to be created.</li> </ul> </li> <li data-bbox="391 404 953 482">◆ Memory Correctable Error Flood Policy <ul style="list-style-type: none"> <li data-bbox="426 435 953 482">– Options available: Disable, Once, Frequency. Default setting is <b>Frequency</b>.</li> </ul> </li> <li data-bbox="391 490 953 631">◆ Correctable Error Threshold <ul style="list-style-type: none"> <li data-bbox="426 522 953 569">– Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket.</li> <li data-bbox="426 577 953 631">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li data-bbox="391 639 953 749">◆ Trigger SW Error Threshold<sup>(Note)</sup> <ul style="list-style-type: none"> <li data-bbox="426 671 953 686">– Enable/Disable Sparing trigger SW Error Match Threshold.</li> <li data-bbox="426 694 953 749">– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="391 757 953 898">◆ SW Per Bank Threshold <ul style="list-style-type: none"> <li data-bbox="426 788 953 835">– SW Per Bank Threshold (1-0x7FFF) used for DDR bank level error.</li> <li data-bbox="426 843 953 898">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li data-bbox="391 906 953 1016">◆ SW Correctable Error Time Window <ul style="list-style-type: none"> <li data-bbox="426 937 953 953">– SW Correctable Error time window based interface in hour (0-24).</li> <li data-bbox="426 961 953 1016">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li data-bbox="391 1023 953 1133">◆ Leaky bucket time window based interface <ul style="list-style-type: none"> <li data-bbox="426 1055 953 1070">– Enable/Disable leaky bucket time window based interface.</li> <li data-bbox="426 1078 953 1133">– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="391 1141 953 1274">◆ Leaky bucket time window based interface Hour <ul style="list-style-type: none"> <li data-bbox="426 1172 953 1219">– Leaky bucket time window based interface hour used for DDR (0-24).</li> <li data-bbox="426 1227 953 1274">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> </ul> |

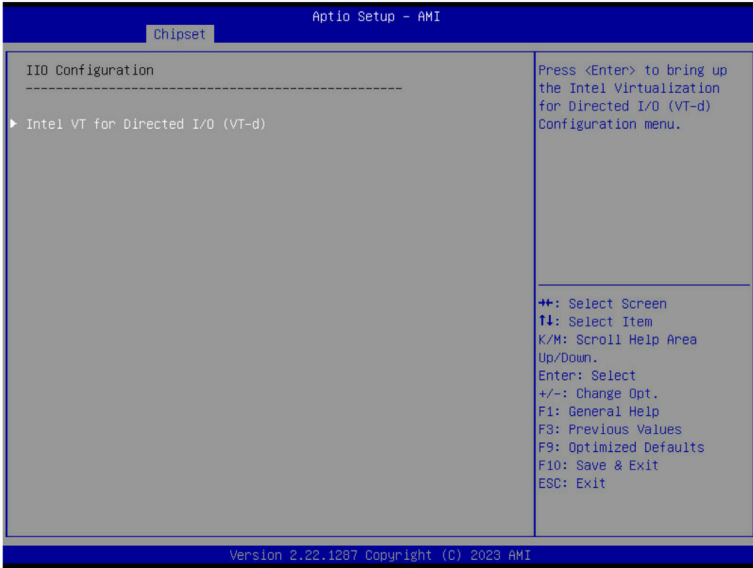
(Note) Advanced items prompt when this item is defined.

| Parameter                               | Description  |
|---|--|
| Memory RAS Configuration<br>(continued) | <ul style="list-style-type: none"> <li>◆ Leaky bucket time window based interface Minute <ul style="list-style-type: none"> <li>– Leaky bucket time window based interface minute used for DDR (0-60).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket low bit <ul style="list-style-type: none"> <li>– Configures leaky bucket low bit (0x1 - 0x29).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket high bit <ul style="list-style-type: none"> <li>– Configures leaky bucket high bit (0x1 - 0x29).</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ ADDDC Sparing<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable ADDDC Sparing.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Enable ADDDC Error Injection <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Patrol Scrub <ul style="list-style-type: none"> <li>– Options available: Disabled, Enable at End of POST. Default setting is <b>Enable at End of POST</b>.</li> </ul> </li> <li>◆ Patrol Scrub Interval <ul style="list-style-type: none"> <li>– Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto.</li> </ul> </li> <li>◆ DDR5 ECS <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled, Enable ECS with Result Collection. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul> |

(Note) Advanced items prompt when this item is defined.



## 2-3-5 I/O Configuration

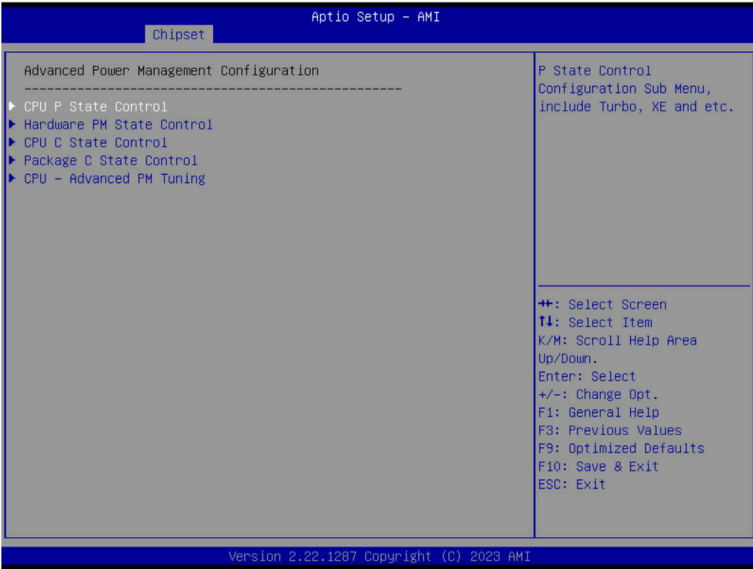


| Parameter                         | Description  |
|-----------------------------------|--|
| I/O Configuration                 | Press [Enter] to configure advanced items.   |
| Intel® VT for Directed I/O (VT-d) | <ul style="list-style-type: none"> <li>◆ Intel® VT for Directed I/O               <ul style="list-style-type: none"> <li>– Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ ACS Control               <ul style="list-style-type: none"> <li>– Enable: Programs ACS only to Chipset PCIe Root Ports Bridges.</li> <li>– Disable: Programs ACS to all PCIe bridges.</li> <li>– Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Cache Allocation               <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ DevTLB Invalidation Timeout Configuration               <ul style="list-style-type: none"> <li>– Options available: Auto, 68s to 103s, 8s to 12s, 268ms to 402ms, 8ms to 12ms, 131us to 196us. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Opt-Out Illegal MSI Mitigation               <ul style="list-style-type: none"> <li>– Enable/Disable Opt-Out Illegal 0xFEE Platform Mitigation.</li> <li>– Options available: Disable, Enable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul> |

| Parameter | Description  |
|-----------|--|
|           | <ul style="list-style-type: none"> <li>◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> <li>– Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Interrupt Remapping <ul style="list-style-type: none"> <li>– Enable/Disable the interrupt remapping support function.</li> <li>– Options available: Auto, Enable, Disable. Default setting is <b>Auto</b></li> </ul> </li> <li>◆ x2APIC Opt Out <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Pre-boot DMA Protection <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ SATC Support <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ RHSA Support <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ PCIe ACSCTL <ul style="list-style-type: none"> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Source Validation<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Translation Blocking<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ P2P Request Redirect<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ P2P Completion Redirect<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Upstream Forwarding Enable<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul> |

(Note) This item is configurable when **PCIe ACSCTL** is set to **Enable**.

## 2-3-6 Advanced Power Management Configuration

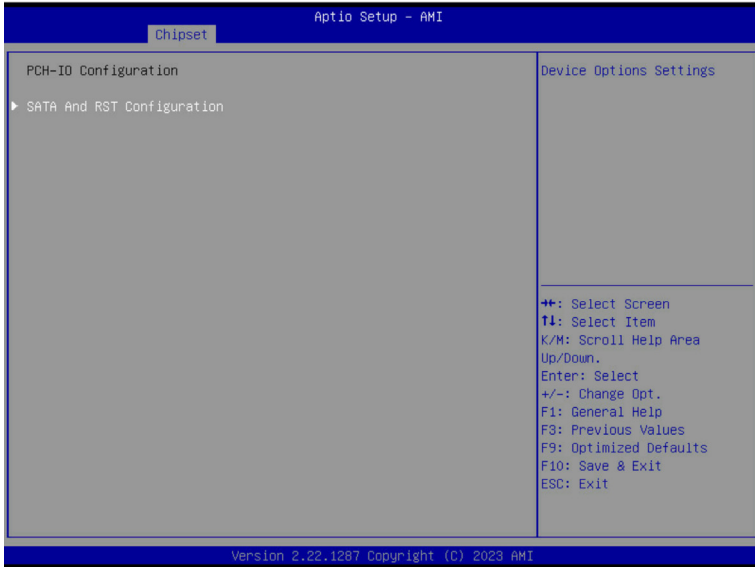


| Parameter                 | Description   |
|---------------------------|---|
| CPU P State Control       | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ SpeedStep (Pstates)               <ul style="list-style-type: none"> <li>– Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Turbo Mode               <ul style="list-style-type: none"> <li>– When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul> |
| Hardware PM State Control | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Hardware P-States               <ul style="list-style-type: none"> <li>– When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States).</li> <li>– In Native mode, the processor hardware chooses a P-state based on OS guidance.</li> <li>– In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance).</li> <li>– Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is <b>Native Mode</b>.</li> </ul> </li> </ul>  |

| Parameter                | Description  |
|--------------------------|--|
| CPU C State Control      | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Enable Monitor MWAIT <ul style="list-style-type: none"> <li>– Allows Monitor and MWAIT instructions.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ CPU C6 Report <ul style="list-style-type: none"> <li>– Enable/Disable CPU C6(ACPI C3) report to OS.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> <li>– Core C1E auto promotion control. Takes effect after reboot.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul> |
| Package C State Control  | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Package C State <ul style="list-style-type: none"> <li>– Configures the state for the C-State package limit.</li> <li>– Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>  |
| CPU - Advanced PM Tuning | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Energy Perf BIAS <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>• Power Performance Tuning <ul style="list-style-type: none"> <li>» Options available: OS Controls EPB, BIOS Controls EPB, PECI Controls EPB. Default setting is <b>OS Controls EPB</b>.</li> </ul> </li> <li>• Energy_PERF_BIAS_CFG mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>» Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is <b>Balanced Performance</b>.</li> </ul> </li> </ul> </li> </ul> </li> </ul>   |

(Note) This item is configurable when **Power Performance Tuning** is set to **BIOS Controls EPB**.

## 2-3-7 PCH Configuration



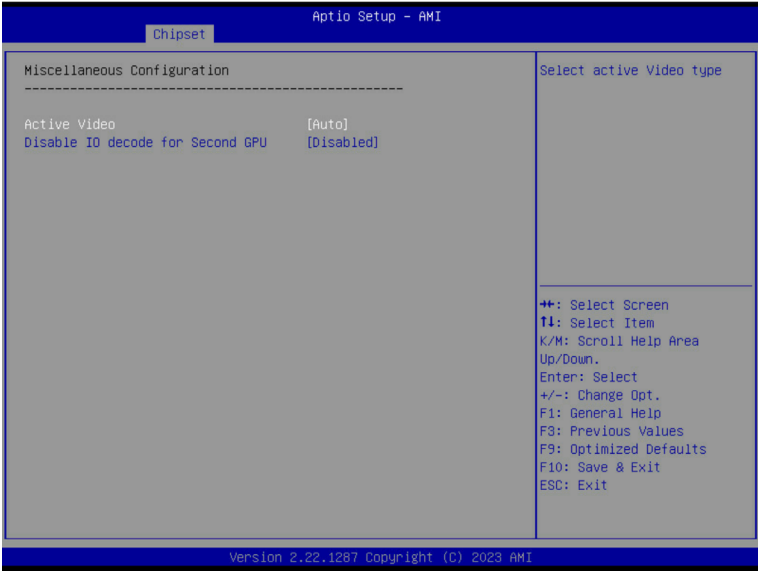
| Parameter                  | Description  |
|----------------------------|--|
| PCH-IO Configuration       |  |
| SATA And RST Configuration | <ul style="list-style-type: none"> <li>◆ SATA Controller And RST Configuration           <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items.</li> <li>• SATA Configuration               <ul style="list-style-type: none"> <li>» Enable/Disable SATA controller.</li> <li>» Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>• SATA Mode Selection               <ul style="list-style-type: none"> <li>» Configures on chip SATA type.</li> <li>» AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time.</li> <li>» RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time.</li> <li>» Options available: AHCI, RAID. Default setting is <b>AHCI</b>.</li> </ul> </li> <li>• RAID Device ID<sup>(Note)</sup> <ul style="list-style-type: none"> <li>» Choose RAID Device ID.</li> <li>» Options available: Client, Alternate, Server. Default setting is <b>Server</b>.</li> </ul> </li> </ul> </li> </ul> |

(Note) Only appears when HDD sets to **RAID Mode**.

| Parameter                             | Description   |
|---------------------------------------|---|
| SATA And RST Configuration(continued) | <ul style="list-style-type: none"> <li>• SATA Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> <li>» The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.</li> </ul> </li> <li>• Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> <li>» Enable/Disable Port 0/1/2/3/4/5/6/7 device.</li> <li>» Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>• Hot Plug (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> <li>» Enable/Disable HDD Hot-Plug function.</li> <li>» Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>• Spin Up Device (for Port 0/1/2/3/4/5/6/7) <ul style="list-style-type: none"> <li>» If enabled for any of ports staggered spin up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.</li> <li>» Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Low Power S0 Idle Capability <ul style="list-style-type: none"> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ PUIS Enable<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul> |

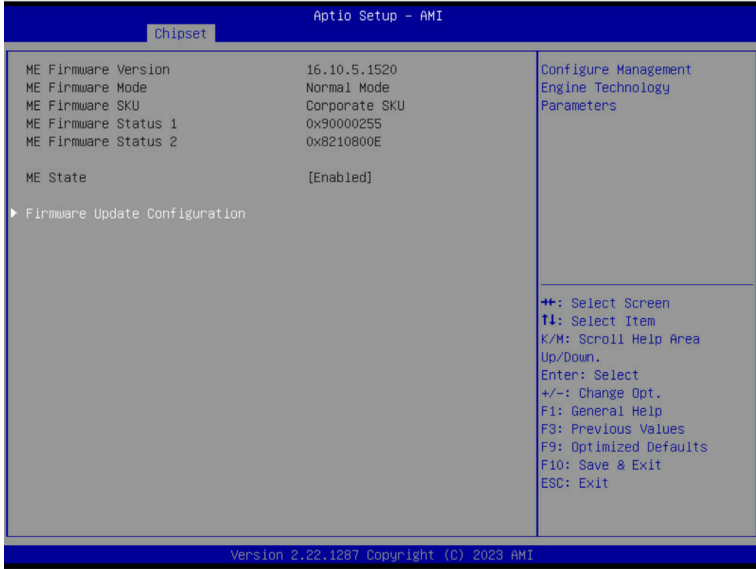
(Note) This item is configurable when **Low Power S0 Idle Capability** is set to **Enabled**.

### 2-3-8 Miscellaneous Configuration



| Parameter                        | Description   |
|----------------------------------|---|
| Miscellaneous Configuration      |   |
| Active Video                     | Selects the active video type.<br>Options available: Auto, Onboard Device, PCIE Device, Specific PCIE Device. Default setting is <b>Auto</b> .              |
| Disable IO decode for Second GPU | Enables this knob to disable IO decode on second GPU in a Dual GPU ML Config.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> . |

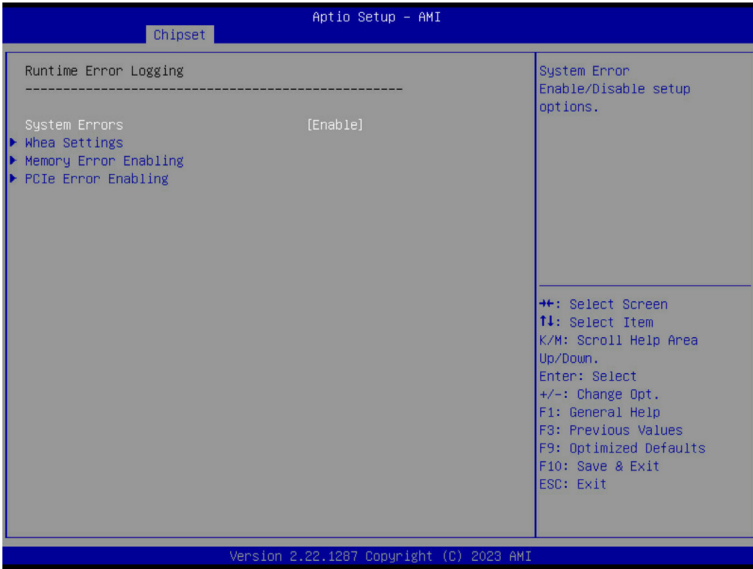
## 2-3-9 Server ME Configuration



| Parameter                     | Description  |
|-------------------------------|--|
| ME Firmware Version           | Displays the operational firmware version.   |
| ME Firmware Mode              | Displays the operational firmware mode.  |
| ME Firmware SKU               | Displays ME firmware sku information.  |
| ME Firmware Status #1/#2      | Displays ME firmware status information.   |
| ME State                      | Default setting is <b>Enabled</b> .  |
| Firmware Update Configuration | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Me FW Image Re-Flash <ul style="list-style-type: none"> <li>– Enable/Disable ME firmware image re-flash function.</li> <li>– Options available: Disabled, Enabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul> |



## 2-3-10 Runtime Error Logging Settings



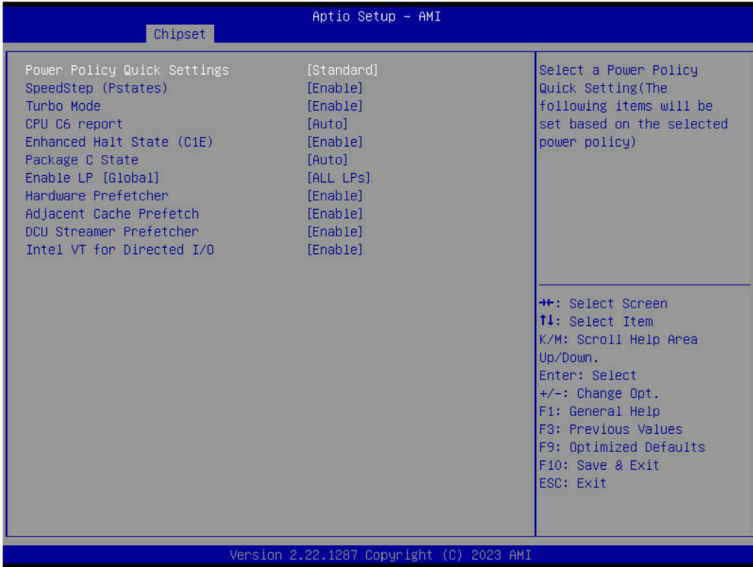
| Parameter             | Description  |
|-----------------------|--|
| Runtime Error Logging |  |
| System Errors         | Enable/Disable system error logging function.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> .  |
| Whea Settings         | Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ WHEA (Windows Hardware Error Architecture) Support <ul style="list-style-type: none"> <li>– Enable/Disable WHEA Support.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>   |
| Memory Error Enabling | Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Memory Corrected Error <ul style="list-style-type: none"> <li>– Enable/Disable Memory Corrected Error.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Uncorrected Error disable Memory <ul style="list-style-type: none"> <li>– Enable/Disable the Memory that triggers Uncorrected Error.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul> |
| PCIe Error Enabling   | Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ PCIe Error <ul style="list-style-type: none"> <li>– Enable/Disable PCIe error.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Corrected Error<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enables and escalates Correctable Errors to error pins.</li> <li>– Options available: Enable, Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>                           |

(Note) This item appears when **PCIe Error** is set to **Enable**.

| Parameter           | Description   |
|---------------------|---|
| PCIe Error Enabling | <ul style="list-style-type: none"> <li>◆ Uncorrected Error<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enables and escalates Uncorrectable/Recoverable Errors to error pins.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Fatal Error Enable<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enables and escalates Fatal Errors to error pins.</li> <li>– Options available: Enable, Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Assert NMI on SERR<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Assert NMI on PERR<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul> |

(Note) This item appears when **PCIE Error** is set to **Enable**.

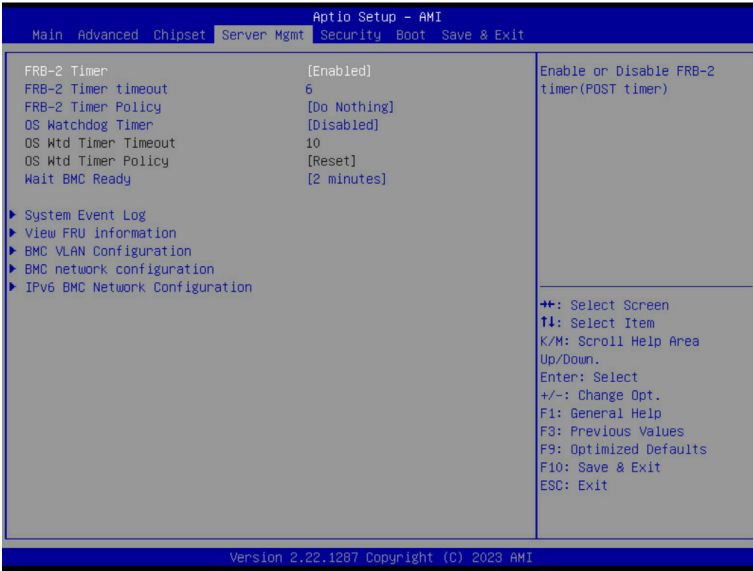
## 2-3-11 Power Policy



| Parameter                   | Description   |
|-----------------------------|---|
| Power Policy Quick Settings | Selects a Power Policy Quick Setting.<br>Options available: Standard, Best Performance, Energy Efficient. Default setting is <b>Standard</b> .  |
| SpeedStep (Pstates)         | Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> .  |
| Turbo Mode                  | When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance.<br>When this item is disabled, the processor will not overclock any of its core.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> . |
| CPU C6 report               | Enable/Disable the BIOS to enable the report from the CPU C6 state (ACPI C3) to the OS.<br>Options available: Disable, Enable, Auto. Default setting is <b>Auto</b> .   |
| Enhanced Halt State (C1E)   | Enable/Disable the C1E support for lower power consumption. Takes effect after reboot.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> .  |
| Package C State             | Configures the C-State package limit.<br>Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>Auto</b> .   |

| Parameter                  | Description  |
|----------------------------|--|
| Enable LP [Global]         | Enables Logical processor (Software Method to Enable/Disable Logical Processor threads).<br>Options available: ALL LPs, Single LP. Default setting is <b>ALL LPs</b> .   |
| Hardware Prefetcher        | Options available: Enable, Disable. Default setting is <b>Enable</b> .   |
| Adjacent Cache Prefetch    | Options available: Enable, Disable. Default setting is <b>Enable</b> .   |
| DCU Streamer Prefetcher    | Options available: Enable, Disable. Default setting is <b>Enable</b> .   |
| Intel® VT for Directed I/O | Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables.<br>Options available: Enable, Disable. Default setting is <b>Enable</b> . |

## 2-4 Server Management Menu



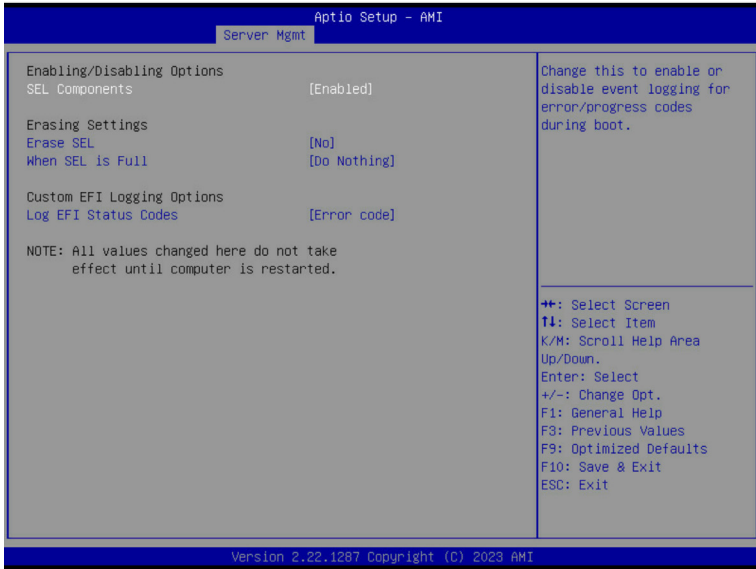
| Parameter                               | Description  |
|---|--|
| FRB-2 Timer                             | Enable/Disable FRB-2 timer (POST timer).<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                            |
| FRB-2 Timer <sup>(Note1)</sup> timeout  | Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes.<br>Default setting is <b>6 minutes</b> .                                |
| FRB-2 Timer Policy <sup>(Note1)</sup>   | Configures the FRB2 Timer policy.<br>Options available: Do Nothing, Reset, Power Down, Power Cycle.<br>Default setting is <b>Do Nothing</b> .    |
| OS Watchdog Timer                       | Enable/Disable OS Watchdog Timer function.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .                         |
| OS Wtd Timer Timeout <sup>(Note2)</sup> | Configures OS Watchdog Timer. The value is between 1 to 30 minutes.<br>Default setting is <b>10 minutes</b> .                                    |
| OS Wtd Timer Policy <sup>(Note2)</sup>  | Configure OS Watchdog Timer Policy.<br>Options available: Reset, Do Nothing, Power Down, Power Cycle.<br>Default setting is <b>Reset</b> .       |
| Wait BMC Ready                          | POST wait BMC ready and reboot system.<br>Options available: Disabled, 2 minutes, 4 minutes, 6 minutes.<br>Default setting is <b>2 minutes</b> . |

(Note1) This item is configurable when **FRB-2 Timer** is set to **Enabled**.

(Note2) This item is configurable when **OS Watchdog Timer** is set to **Enabled**.

| <b>Parameter</b>               | <b>Description</b>                         |
|--------------------------------|--|
| System Event Log               | Press [Enter] to configure advanced items. |
| View FRU Information           | Press [Enter] to view the FRU information. |
| BMC VLAN Configuration         | Press [Enter] to configure advanced items. |
| BMC network Configuration      | Press [Enter] to configure advanced items. |
| IPv6 BMC Network Configuration | Press [Enter] to configure advanced items. |

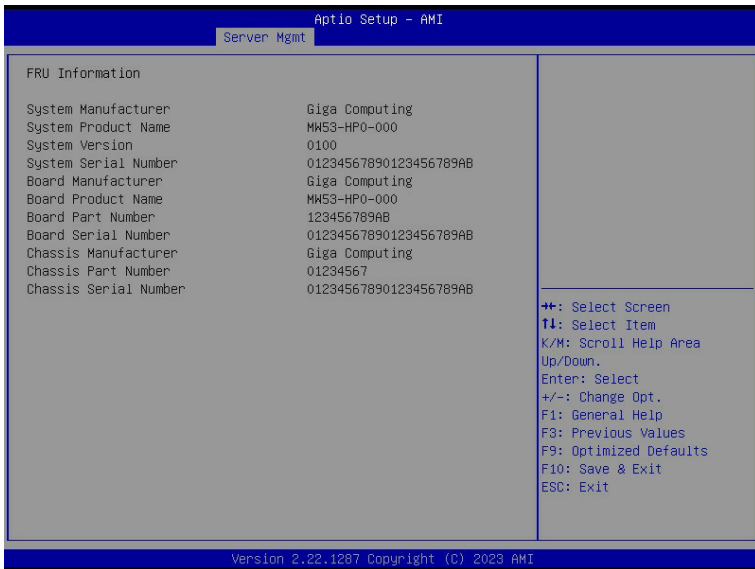
## 2-4-1 System Event Log



| Parameter                    | Description  |
|------------------------------|--|
| Enabling / Disabling Options |  |
| SEL Components               | Change this item to enable or disable all features of System Event Logging during boot.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                         |
| Erasing Settings             |  |
| Erase SEL                    | Choose options for erasing SEL.<br>Options available: No, Yes, On next reset, Yes, On every reset.<br>Default setting is <b>No</b> .   |
| When SEL is Full             | Choose options for reactions to a full SEL.<br>Options available: Do Nothing, Erase Immediately, Delete Oldest Record.<br>Default setting is <b>Do Nothing</b> .                             |
| Custom EFI Logging Options   |  |
| Log EFI Status Codes         | Enable/Disable the logging of EFI Status Codes (if not already converted to legacy).<br>Options available: Disabled, Both, Error code, Progress code. Default setting is <b>Error code</b> . |

## 2-4-2 View FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information. Items on this window are non-configurable.



(Note) The model name will vary depends on the product you purchased

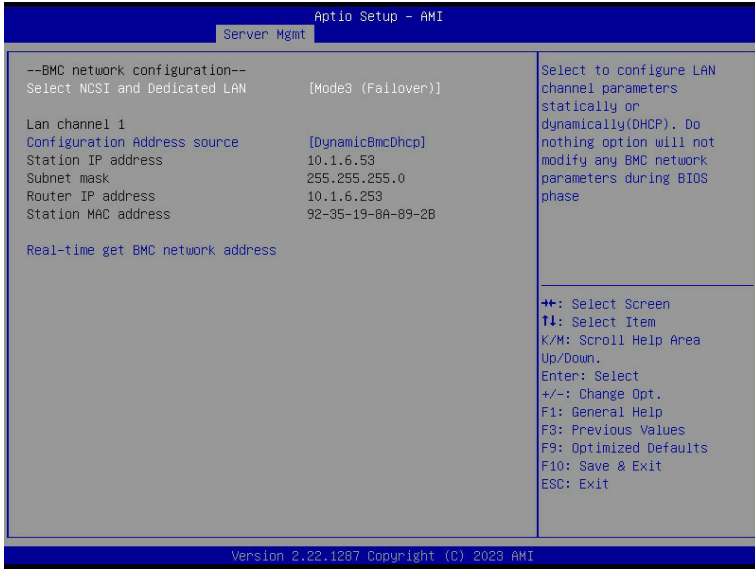


## 2-4-3 BMC VLAN Configuration



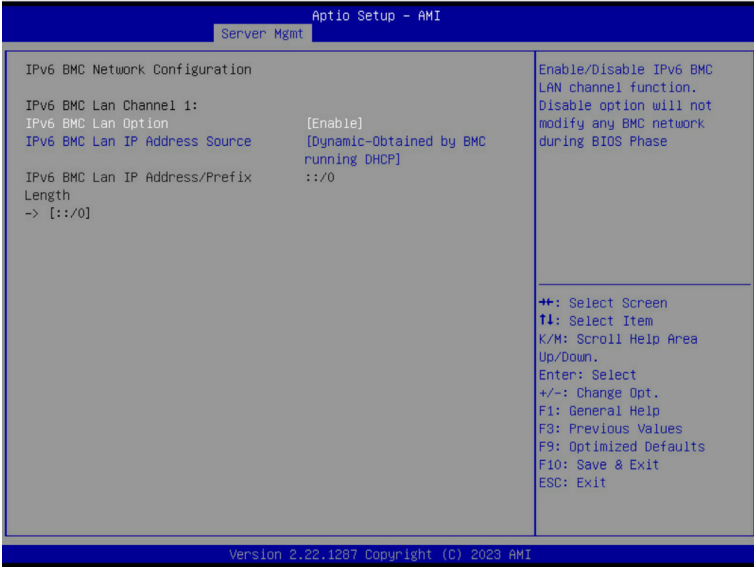
| Parameter              | Description  |
|------------------------|--|
| BMC VLAN Configuration |  |
| BMC VLAN ID            | Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.                             |
| BMC VLAN Priority      | Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority will not be selected. |

## 2-4-4 BMC Network Configuration



| Parameter                         | Description   |
|-----------------------------------|---|
| BMC network configuration         |   |
| Select NCSI and Dedicated LAN     | Options available: Do Nothing, Model1(Dedicated), Model2(NCSI), Mode3(Failover). Default setting is <b>Do Nothing</b> .   |
| Lan Channel 1                     |   |
| Configuration Address source      | Selects to configure LAN channel parameters statically or dynamically (DHCP).<br>Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is <b>DynamicBmcDhcp</b> . |
| Station IP address                | Displays IP Address information.  |
| Subnet mask                       | Displays Subnet Mask information.<br>Please note that the IP address must be in three digitals, for example, 192.168.000.001.   |
| Router IP address                 | Displays the Router IP Address information.   |
| Station MAC address               | Displays the MAC Address information.   |
| Real-time get BMC network address | Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.  |

## 2-4-5 IPv6 BMC Network Configuration



| Parameter                             | Description   |
|---------------------------------------|---|
| IPv6 BMC network configuration        |   |
| IPv6 BMC Lan Channel 1                |   |
| IPv6 BMC Lan Option                   | Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase.<br>Options available: Unspecified, Disable, Enable. Default setting is <b>Enable</b> .            |
| IPv6 BMC Lan IP Address Source        | Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC).<br>Options available: Unspecified, Static, Dynamic-Obtained by BMC running DHCP. Default setting is <b>Dynamic-Obtained by BMC running DHCP</b> . |
| IPv6 BMC Lan IP Address/Prefix Length | Check if the IPv6 BMC LAN IP address matches those displayed on the screen.   |

## 2-5 Security Menu

The Security menu allows you to safeguard and protect the system from unauthorized use by setting up access passwords.



There are two types of passwords that you can set:

- **Administrator Password**  
Entering this password will allow the user to access and change all settings in the Setup Utility.
- **User Password**  
Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

| Parameter              | Description  |
|------------------------|--|
| Administrator Password | Press [Enter] to configure the administrator password. |
| User Password          | Press [Enter] to configure the user password.          |
| Secure Boot            | Press [Enter] to configure advanced items.             |

## 2-5-1 Secure Boot

The Secure Boot submenu is applicable when your device is installed the Windows® 8 (or above) operating system.



| Parameter                          | Description   |
|------------------------------------|---|
| System Mode                        | Displays if the system is in User mode or Setup mode.   |
| Secure Boot                        | Enable/ Disable the Secure Boot function.<br>Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .   |
| Secure Boot Mode <sup>(Note)</sup> | Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before Windows loads to the login screen have not been tampered with.<br>When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases.<br>When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database.<br>Options available: Standard, Custom. Default setting is <b>Custom</b> . |
| Restore Factory Keys               | Forces the system to user mode and installs factory default Secure Boot key database.   |
| Reset To Setup Mode                | Reset the system to Setup Mode.   |

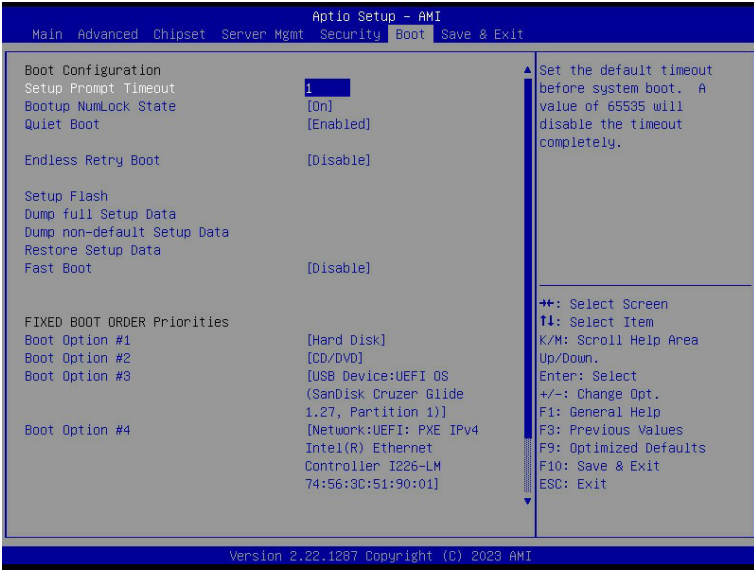
(Note) Advanced items prompt when this item is set to **Custom**.

| Parameter      | Description  |
|----------------|--|
| Key Management | <p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 941 235"><b>Please note that this item is configurable when Secure Boot Mode is set to Custom.</b></p> <ul style="list-style-type: none"> <li data-bbox="335 243 946 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 946 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li data-bbox="367 326 909 352">– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="335 357 931 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 931 404">– Installs all factory default keys. It will force the system in User Mode.</li> <li data-bbox="367 409 611 431">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 435 654 509">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode.</li> <li data-bbox="367 487 611 509">– Options available: Yes, No.</li> </ul> </li> <li data-bbox="335 514 904 595">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 537 904 595">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li data-bbox="335 600 941 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 624 941 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.</li> </ul> </li> <li data-bbox="335 686 899 744">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 899 744">– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li data-bbox="335 749 803 854">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 773 803 796">– Displays the current status of the Platform Key (PK).</li> <li data-bbox="367 801 680 823">– Press [Enter] to configure a new PK.</li> <li data-bbox="367 827 601 854">– Options available: Update.</li> </ul> </li> <li data-bbox="335 859 941 995">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 882 941 906">– Displays the current status of the Key Exchange Key Database (KEK).</li> <li data-bbox="367 911 909 964">– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li data-bbox="367 969 675 995">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 1000 941 1136">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1023 909 1047">– Displays the current status of the Authorized Signature Database.</li> <li data-bbox="367 1052 941 1105">– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li data-bbox="367 1110 675 1136">– Options available: Update, Append.</li> </ul> </li> <li data-bbox="335 1141 904 1277">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1165 904 1188">– Displays the current status of the Forbidden Signature Database.</li> <li data-bbox="367 1193 893 1246">– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li data-bbox="367 1251 675 1277">– Options available: Update, Append.</li> </ul> </li> </ul> |

| Parameter                     | Description   |
|-------------------------------|---|
| Key Management<br>(continued) | <ul style="list-style-type: none"> <li>◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li>– Displays the current status of the Authorized TimeStamps Database.</li> <li>– Press [Enter] to configure a new DBT or load additional DBT from storage devices.</li> <li>– Options available: Update, Append.</li> </ul> </li> <li>◆ OsRecovery Signatures <ul style="list-style-type: none"> <li>– Displays the current status of the OsRecovery Signature Database.</li> <li>– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.</li> <li>– Options available: Update, Append.</li> </ul> </li> </ul> |

## 2-6 Boot Menu

The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



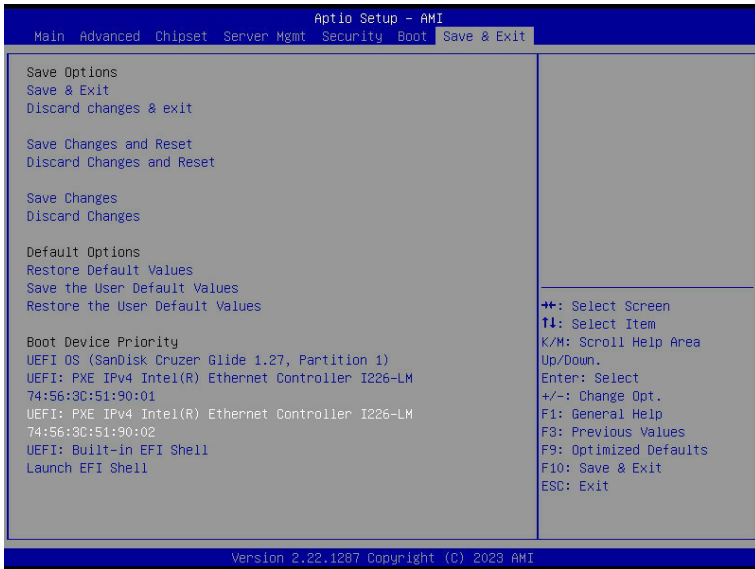
| Parameter                   | Description   |
|-----------------------------|---|
| Boot Configuration          |   |
| Setup Prompt Timeout        | Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.<br>Press the numeric keys to input the desired values. |
| Bootup NumLock State        | Enable/Disable the Bootup NumLock function.<br>Options available: On, Off. Default setting is <b>On</b> .   |
| Quiet Boot                  | Enable/Disable showing the logo during POST.<br>Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .                           |
| Endless Retry Boot          | Options available: Disable, Enable. Default setting is <b>Disable</b> .   |
| Setup Flash                 | Press [Enter] to run setup flash.   |
| Dump full Setup Data        | Press [Enter] to dump full setup data to file.  |
| Dump non-default Setup Data | Press [Enter] to dump non-default setup data to file.   |
| Restore Setup Data          | Press [Enter] to restore setup data from file.  |
| Fast Boot                   | Enable/Disable the fast boot by skipping some drivers.<br>Options available: Disable, Enable. Default setting is <b>Disable</b> .                   |



| Parameter                          | Description  |
|------------------------------------|--|
| FIXED BOOT ORDER Priorities        |  |
| Boot Option #1 / #2 / #3 / #4 / #5 | <p>Press [Enter] to configure the boot order priority.<br/>By default, the server searches for boot devices in the following sequence:</p> <ol style="list-style-type: none"> <li>1. Hard drive.</li> <li>2. CD-COM/DVD drive.</li> <li>3. USB device.</li> <li>4. Network.</li> <li>5. UEFI.</li> </ol> |
| UEFI Network Drive BBS Priorities  | Press [Enter] to configure the boot priority.  |
| UEFI Application Boot Priorities   | Press [Enter] to configure the boot priority.  |

## 2-7 Save & Exit Menu

The Save & Exit menu displays the various options to quit from the BIOS setup. Highlight any of the exit options then press <Enter>.



| Parameter                 | Description   |
|---------------------------|---|
| Save Options              |   |
| Save and Exit             | Saves changes made and closes the BIOS setup.<br>Options available: Yes, No.          |
| Discard changes and exit  | Discards changes made and exits the BIOS setup.<br>Options available: Yes, No.        |
| Save Changes and Reset    | Restarts the system after saving the changes made.<br>Options available: Yes, No.     |
| Discard Changes and Reset | Restarts the system without saving any changes.<br>Options available: Yes, No.        |
| Save Changes              | Saves changes done so far to any of the setup options.<br>Options available: Yes, No. |
| Discard Changes           | Discards changes made and closes the BIOS setup.<br>Options available: Yes, No.       |
| Default Options           |   |

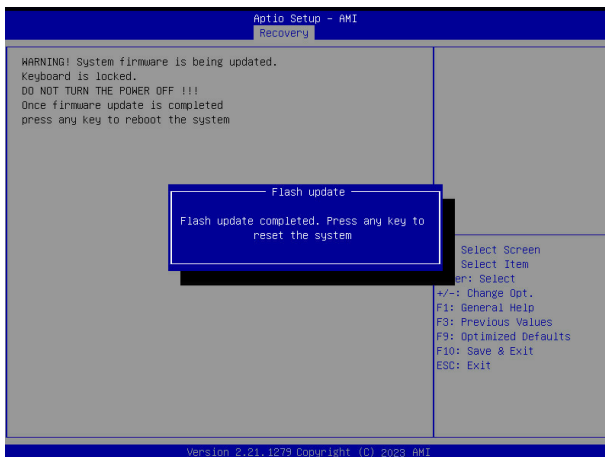
| Parameter                       | Description   |
|---------------------------------|---|
| Restore Default Values          | <p>Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly.</p> <p>Options available: Yes, No.</p> |
| Save the User Default Values    | <p>Saves the changes made as the user default settings.</p> <p>Options available: Yes, No.</p>  |
| Restore the User Default Values | <p>Loads the user default settings for all BIOS setup parameters.</p> <p>Options available: Yes, No.</p>  |
| Boot Device Priority            | <p>Press [Enter] to configure the device as the boot-up drive.</p>  |
| Launch EFI Shell                | <p>Attempts to Launch EFI Shell application (Shell.efi) from one of the available file system devices.</p>  |

## 2-8 BIOS Recovery

The system has an embedded recovery technique. In the event that the BIOS becomes corrupt the boot block can be used to restore the BIOS to a working state. To restore your BIOS, please follow the instructions listed below:

Recovery Instruction:

1. Copy the XXX.rom to USB diskette.
2. Setting BIOS Recovery jump to enabled status.
3. Boot into BIOS recovery.
4. Run Proceed with flash update.
5. BIOS updated.



## 2-9 BIOS POST Beep code (AMI standard)

### 2-9-1 PEI Beep Codes

| # of Beeps | Description  |
|------------|--|
| 1          | Memory not Installed.  |
| 1          | Memory was installed twice (InstallPeiMemory routine in PEI Core called twice) |
| 2          | Recovery started   |
| 3          | DXE IPL was not found  |
| 3          | DXE Core Firmware Volume was not found   |
| 4          | Recovery failed  |
| 4          | S3 Resume failed   |
| 7          | Reset PPI is not available   |

### 2-9-2 DXE Beep Codes

| # of Beeps | Description   |
|------------|---|
| 1          | Invalid password                                      |
| 4          | Some of the Architectural Protocols are not available |
| 5          | No Console Output Devices are found                   |
| 5          | No Console Input Devices are found                    |
| 6          | Flash update is failed                                |
| 7          | Reset protocol is not available                       |
| 8          | Platform PCI resource requirements cannot be met      |