GIGABYTE™

# R284-SF0-AAL1

Rack Server - Intel® Xeon® 6 Processors
2U DP 4 x PCIe Gen5 GPUs

## User Manual

Rev. 1.0

## Copyright



## Disclaimer



## 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 of 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 https://esupport.gigabyte.com/ to create a new support ticket

For any general sales or marketing enquiries, you may also message GIGABYTE server directly by email: server.grp@gigabyte.com

## Conventions

The following conventions are used in this user's guide:

| | |
|---|---|
|  | **NOTE!**<br>Pieces of additional<br>information related to the current topic. |
|  | **CAUTION!**<br>Precautionary measures to<br>avoid possible hardware or software problems. |
|  | **WARNING!**<br>Alerts to any damage that might<br>result from doing or not doing specific actions. |

## Server Warnings and Cautions

Before installing a server, be sure that you understand the following warnings and cautions.

**WARNING!**

**To reduce the risk of electric shock or damage to the equipment:**

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.

**WARNING!**

**To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.**

**WARNING!**

**This server is equipped with high speed fans. Keep away from hazardous moving fan blades during servicing.**

**CAUTION!**

- Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
- Danger of explosion if battery is incorrectly replaced.
- Replace battery with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

**CAUTION!**

Risk of explosion if battery is replaced incorrectly or with an incorrect type. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

## Electrostatic Discharge (ESD)

**CAUTION!**

ESD CAN DAMAGE DRIVES, BOARDS, AND OTHER PARTS. WE RECOMMEND THAT YOU PERFORM ALL PROCEDURES AT AN ESD WORKSTATION. IF ONE IS NOT AVAILABLE, PROVIDE SOME ESD PROTECTION BY WEARING AN ANTI-STATIC WRIST STRAP ATTACHED TO CHASSIS GROUND -- ANY UNPAINTED METAL SURFACE -- ON YOUR SERVER WHEN HANDLING PARTS.

Always handle boards carefully, they can be extremely sensitive to ESD. Hold boards only by their edges without touching any components or connectors. After removing a board from its protective ESD bag or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the ESD bag. Do not slide the board over any surface.

**System power on/off:** To service components within the server, please ensure the power has been disconnected.
e.g. Remove the node from the server chassis (to disconnect power) or disconnect the power from the server chassis.
Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

**Hazardous conditions, devices and cables:** Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system chassis and disconnect the cables attached to the system before servicing the chassis. Otherwise, personal injury or equipment damage can result.

**Electrostatic discharge (ESD) and ESD protection:** ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface on the server) when handling parts.

**ESD and handling boards:** Always handle boards carefully. They can be extremely sensi-tive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

**Installing or removing jumpers:** A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fin-gertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can dam-age the contacts inside the jumper, causing intermittent problems with the function con-trolled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

# Table of Contents

# Chapter 1 Hardware Installation

## 1-1 Installation Precautions

The motherboard/system contain numerous delicate electronic circuits and components which can become damaged as a result of electrostatic discharge (ESD). Prior to installation, carefully read the service guide 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

**NOTE:**

**We reserve the right to make any changes to the product specifications and product-related information without prior notice.**

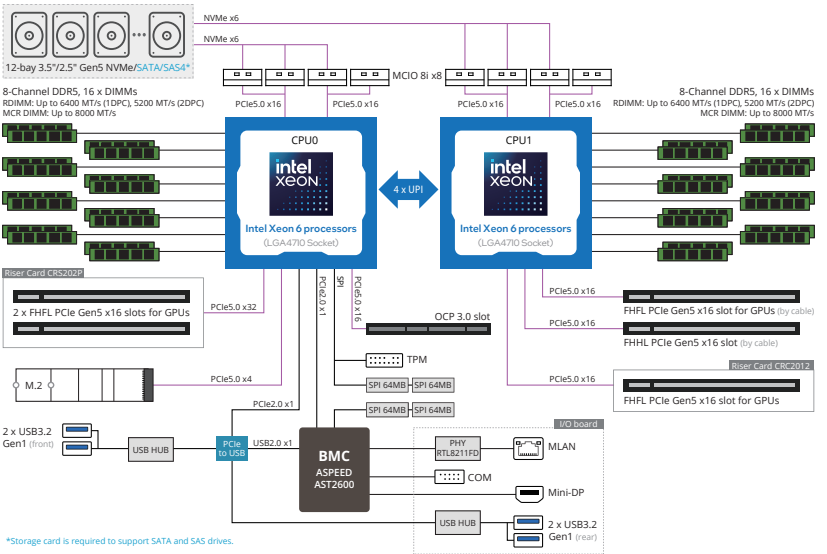
| | |
|---|---|
| System Dimension | ◆ 2U<br>◆ 438 (W) x 87.5 (H) x 815(D) mm |
| CPU | Intel® Xeon® 6 Processors<br>◆ Intel® Xeon® 6700E-Series Processors<br>◆ Intel® Xeon® 6700P-Series Processors (available Q1'25)<br>◆ Intel® Xeon® 6500P-Series Processors (available Q1'25)<br><br>◆ Dual processor, TDP up to 350W<br><br>NOTE: If only 1 CPU is installed, some PCIe or memory functions might be unavailable. |
| Socket | ◆ 2 x LGA 4710<br>◆ Socket E2 |
| Chipset | ◆ System on Chip |
| Security | ◆ UEFI Secure Boot<br>◆ Silicon root of trust<br>◆ SNMP Support: V3 |
| Memory | ◆ 32 x DIMM slots<br>◆ DDR5 memory supported<br>◆ MCR DIMM supported*<br>◆ 8-Channel memory architecture<br>◆ RDIMM: Up to 6400 MT/s (1DPC), 5200 MT/s (2DPC)<br>◆ MCR DIMM: Up to 8000 MT/s<br><br>***MCR DIMMs are only supported with Intel® Xeon® 6 Processors with P-cores and in a 1DPC configuration.** |
| LAN | **Rear side:**<br>◆ 1 x 10/100/1000 Mbps Management LAN |
| Video | ◆ Integrated in Aspeed® AST2600<br>◆ 1 x Mini-DP |
| Storage | **Front side:**<br>◆ 12 x 3.5"/2.5" Gen5 NVMe/SATA/SAS-4* hot-swappable bays<br>◆ (6 x NVMe from CPU_0, 6 x NVMe from CPU_1)<br><br>***Storage card is required to support SATA and SAS drives.** |
| SAS | ◆ Require SAS add-in cards |

| | |
|---|---|
| RAID | ◆ Require RAID add-in cards |
| Expansion Slot | **PCIe Cable x 2:**<br>◆ 1 x PCIe x16 (Gen5 x16) FHFL slot, from CPU_1, for GPUs<br>◆ 1 x PCIe x16 (Gen5 x16) FHHL slot, from CPU_1<br><br>**Riser Card CRC2012:**<br>◆ 1 x PCIe x16 (Gen5 x16) FHFL slot, from CPU_1, for GPUs<br><br>**Riser Card CRS202P:**<br>◆ 2 x PCIe x16 (Gen5 x16) FHFL slots, from CPU_0<br><br>1 x OCP 3.0 slot with PCIe Gen5 x16 bandwidth, from CPU_0<br>Supports NCSI function<br><br>2 x M.2 slots:<br>◆ M-key<br>◆ PCIe Gen5 x4, from CPU_0<br>◆ Supports 2280/22110 cards |
| Internal I/O | ◆ 1 x VROC connector<br>◆ 1 x TPM header<br>◆ 1 x PRoT connector **(only enabled on RoT SKU)** |
| Front I/O | ◆ 2 x USB 3.2 Gen1<br>◆ 1 x Power button with LED<br>◆ 1 x ID button with LED<br>◆ 1 x NMI button<br>◆ 1 x Reset button<br>◆ 2 x LAN activity LEDs (disabled)<br>◆ 1 x Storage activity LED<br>◆ 1 x System status LED |
| Rear I/O | ◆ 2 x USB 3.2 Gen1<br>◆ 1 x Mini-DP<br>◆ 1 x MLAN<br>◆ 1 x ID LED |
| Backplane Board | ◆ Speed and bandwidth:<br>◆ PCIe Gen5 x4 or SATA 6Gb/s or SAS-4 24Gb/s |
| Security Modules | ◆ 1 x TPM header with SPI interface<br>◆ **Optional** TPM2.0 kit: CTM012 |

| | |
|---|---|
| Power Supply | ◆ Dual 2700W 80 PLUS Titanium redundant power supply<br><br>AC Input:<br>◆ 100-127V~/ 12A, 50-60Hz<br>◆ 200-240V~/ 16A, 50-60Hz<br><br>DC Input: (Only for China)<br>◆ 240Vdc/ 16A<br><br>DC Output:<br>◆ Max 1008W/ 100-127V~<br>◆ +12V/ 84A<br>◆ +12Vsb/ 3A<br>◆ - Max 2700W/ 200-240V~ or 240Vdc Input<br>◆ +12V/ 225A<br>◆ +12Vsb/ 3A<br><br>Note: The system power supply requires C19 power cord. |
| System Management | ◆ Aspeed® AST2600 management controller<br>◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface<br><br>◆ Dashboard<br>◆ HTML5 KVM<br>◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status …etc.)<br>◆ Sensor Reading History Data<br>◆ FRU Information<br>◆ SEL Log in Linear Storage / Circular Storage Policy<br>◆ Hardware Inventory<br>◆ Fan Profile<br>◆ System Firewall<br>◆ Power Consumption<br>◆ Power Control<br>◆ Advanced power capping<br>◆ LDAP / AD / RADIUS Support<br>◆ Backup & Restore Configuration<br>◆ Remote BIOS/BMC/CPLD Update<br>◆ Event Log Filter<br>◆ User Management<br>◆ Media Redirection Settings<br>◆ PAM Order Settings<br>◆ SSL Settings<br>◆ SMTP Settings |

| | | |
|---|---|---|
|  Operating Properties | ◆ Operating temperature: 10°C to 30°C<br>◆ Operating humidity: 8%-80% (non-condensing)<br>◆ Non-operating temperature: -40°C to 60°C<br>◆ Non-operating humidity: 20%-95% (non-condensing) | |

# 1-3 System Block Diagram



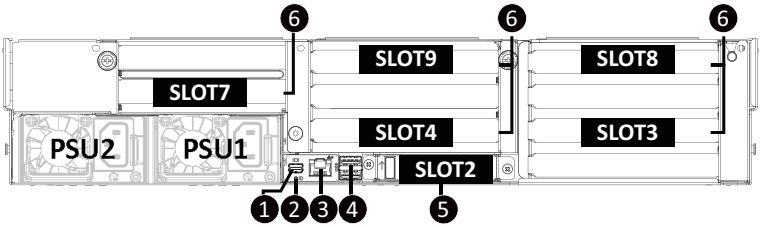
# Chapter 2 System Appearance

## 2-1 Front View


| No. | Description |
|---|---|
| 1. | Front Panel LEDs and Buttons |
| 2. | USB 3.2 Gen1 Port x 2 |

- Refer to section **2-3 Front Panel LEDs and Buttons** for a detailed description of the function of the LEDs.

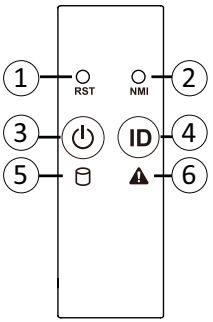
## 2-2 Rear View




| No. | Description | No. | Description |
|---|---|---|---|
| 1. | Mini DisplayPort | 4. | USB 3.2 Gen1 Port x 2 |
| 2. | ID LED | 5. | OCP 3.0 Slot (Option/SFF) |
| 3. | Server Management LAN Port | 6. | PCIe Card Slot |

- Refer to section **2-5 Rear System LAN LEDs** for a detailed description of the function of the LEDs.

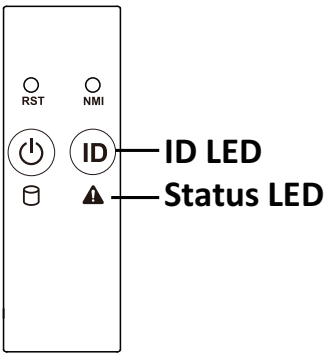
## 2-3 Front Panel LEDs and Buttons




| No. | Name | Color | Status | Description |
|---|---|---|---|---|
| 1. | Reset Button | -- | -- | Press this button to reset the system. |
| 2. | NMI button | -- | -- | Press this button for the server to generate a NMI to the processor. If multiple-bit ECC errors occur, the server will effectively be halted. |
| 3. | Power button with LED | Green | On | Indicates the system is powered on. |
| | | N/A | Off | System is not powered on or in ACPI S5 state (power off) |
| 4. | ID Button with LED(Note) | Blue | On | System identification is active. |
| | | N/A | Off | System identification is disabled. |
| 5. | HDD Status LED | Green | On | Indicates locating the HDD. |
| | | | Blink | Indicates accessing the HDD. |
| | | Amber | On | Indicates HDD error. |
| | | Green/ Amber | Blink | Indicates HDD rebuilding. |
| | | N/A | Off | Indicates no HDD access or no HDD error. |
| 6. | System Status LED(Note) | Green | Solid On | System is operating normally. |
| | | Amber | Solid On | Critical condition, may indicate:<br>System fan failure<br>System temperature |
| | | | Blink | Non-critical condition, may indicate:<br>Redundant power module failure<br>Temperature and voltage issue<br>Chassis intrusion |
| | | N/A | Off | System is not ready, may indicate:<br>POST error<br>NMI error<br>Processor or terminator missing |

(Note) If your server features RoT function, please see the following section for detail LED behavior.

## 2-4 RoT LEDs



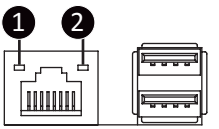

| | LED on Front panel[Note5] | |
|---|---|---|
| | ID LED | Status LED |
| **EC Firmware (FW) Authentication fail or not exit** | | |
| **EC FW is broken or not exit [Note1]** | OFF | OFF |
| **Authenticating/Recovering BMC/BIOS Images** | | |
| **Authenticating Images** | OFF | OFF |
| **Recovering BMC Active Flash** | Blinks Blue 4 times per second | Blinks Green 4 times per second |
| **Recovering BIOS Active Flash** | Blinks Blue 4 times per second | Blinks Green 4 times per second |
| **Authentication (AUTH) Pass** | | |
| **Recovering BIOS Active Flash** | OFF | OFF |
| **BMC : AUTH pass after doing recovery**<br>**BIOS : AUTH pass after doing recovery** | OFF | OFF |
| **BMC : AUTH pass after doing recovery**<br>**BIOS : AUTH pass** | OFF | OFF |
| **BMC : AUTH pass**<br>**BIOS : AUTH pass after doing recovery** | OFF | OFF |

| Active Flash Authentication (AUTH) Fail | | |
|---|---|---|
| **BMC : AUTH Fail**[Note2] | Blinks Blue<br>1 time per second | Blinks Green<br>1 time per second |
| **BIOS : AUTH fail**[Note2] | Blinks Blue<br>1 time per second | Blinks Amber<br>1 time per second |
| **BMC : AUTH fail after doing recovery**[Note3] | Blinks Blue<br>2 times per second<br>[ON OFF OFF] | Blinks Green<br>2 times per second<br>[ON OFF OFF] |
| **BIOS : AUTH fail after doing recovery**[Note3] | Blinks Blue<br>2 times per second<br>[ON OFF OFF] | Blinks Amber<br>2 times per second<br>[ON OFF OFF] |
| **Backup Flash Authentication Fail**[Note4] | | |
| **BMC : AUTH fail** | Blinks Blue<br>2 times per second<br>[ON OFF ON OFF] | Blinks Green<br>2 times per second<br>[ON OFF ON OFF] |
| **BIOS : AUTH fail** | Blinks Blue<br>2 times per second<br>[ON OFF ON OFF] | Blinks Amber<br>2 times per second<br>[ON OFF ON OFF] |

**NOTE!**

1. EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
2 CEC1702's bootloader load EC FW from BMC Flash1 when AC on. It must authenticate this FW firstly before run the FW. If the authenticate fail or not get the FW successfully, CEC1702 is not allowed to execute this FW and ECSTS_LED1 on the MB is OFF state.
3. if active flash is still authentication failed after recovery sequence, Microchip CEC1702 stop the process and showing LED behavior.
4. If backup flash authentication is failed cause by configuration table, public key or protected area is broken. Microchip CEC1702 stop the process and showing LED behavior.
5. Front panel LED is controlled by BMC or Microchip CEC1702. Once Microchip CEC1702 is working(Auth or recovery), the front panel LED is controlled by Microchip CEC1702 and vice versa.

## 2-5 Rear System LAN LEDs

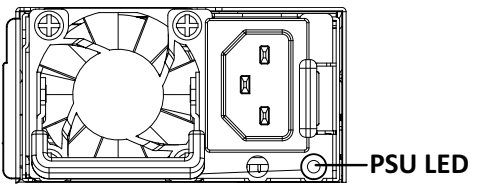



| No. | Name | Color | Status | Description |
|---|---|---|---|---|
| 1. | 1GbE Speed LED | Yellow | On | 1 Gbps data rate |
| | | Green | On | 100 Mbps data rate |
| | | N/A | Off | 10 Mbps data rate |
| 2. | 1GbE Link / Activity LED | Green | On | Link between system and network or no access |
| | | | Blink | Data transmission or reception is occurring. |
| | | N/A | Off | No data transmission or reception is occurring. |

## 2-6 Power Supply Unit LED

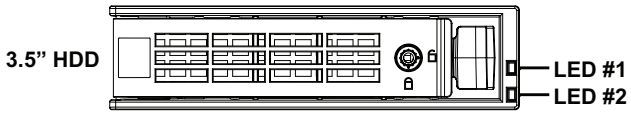
**NOTE!**

The power supply may be vary based on the system configuration.




| State | Description |
|---|---|
| OFF | No AC power to all power supplies |
| 1Hz Green Blinking | AC present / only standby on / Cold redundant mode |
| 2Hz Green Blinking | Power supply firmware updateing mode |
| Amber | AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power |
| | Power supply critical event causing shut down: failure, OCP, OVP, fan failure and UVP |
| 1Hz Amber Blinking | Power supply warning events where the power supply continues to operate: high temp, high power, high current and slow fan |

## 2-7 Hard Disk Drive LEDs




| RAID SKU | | LED #1 | Locate | HDD Fault | Rebuilding | HDD Access | HDD Present (No Access) |
|---|---|---|---|---|---|---|---|
| No RAID configuration (via HBA) | Disk LED (LED on Back Panel) | Green | ON(*1) | OFF | | BLINK (*2) | OFF |
| | | Amber | OFF | OFF | | OFF | OFF |
| | Removed HDD Slot (LED on Back Panel) | Green | ON(*1) | OFF | | -- | -- |
| | | Amber | OFF | OFF | | -- | -- |
| RAID configuration (via HW RAID Card or SW RAID Card) | Disk LED | Green | ON | OFF | | BLINK (*2) | OFF |
| | | Amber | OFF | ON | (Low Speed: 2 Hz) | OFF | OFF |
| | Removed HDD Slot | Green | ON(*1) | OFF | (*3) | -- | -- |
| | | Amber | OFF | ON | (*3) | -- | -- |

| LED #2 | HDD Present | No HDD |
|---|---|---|
| Green | ON | OFF |

**NOTE:**

*1: Depends on HBA/Utility Spec.

*2: Blink cycle depends on HDD's activity signal.

*3: If HDD is pulled out during rebuilding, the disk status of this HDD is regarded as faulty.

# Chapter 3 System Hardware Installation

**Pre-installation Instructions**

Computer components and electronic circuit boards can be damaged by discharges of static electricity. Working on computers that are still connected to a power supply can be extremely dangerous. Follow the simple guidelines below to avoid damage to your computer or injury to yourself.

- Always disconnect the computer from the power outlet whenever you are working inside the computer case.
- If possible, wear a grounded wrist strap when you are working inside the computer case. Alternatively, discharge any static electricity by touching the bare metal system of the computer case, or the bare metal body of any other grounded appliance.
- Hold electronic circuit boards by the edges only. Do not touch the components on the board unless it is necessary to do so. Do not flex or stress the circuit board.
- Leave all components inside the static-proof packaging until you are ready to use the component for the installation.

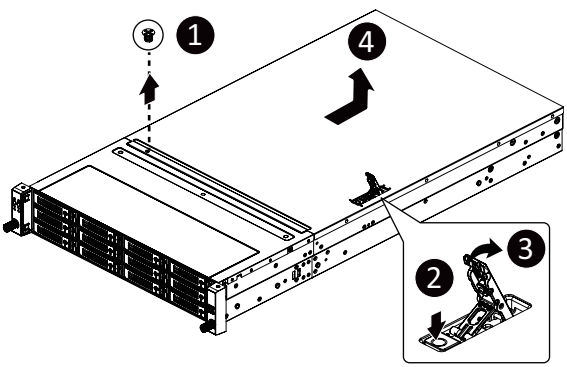
## 3-1 Removing and Installing the Chassis Cover

Before you remove or install the system cover

- Make sure the system is not turned on or connected to AC power.

**Follow these instructions to remove the chassis cover:**

1. Remove the screw securing the chassis cover.
2. Unlock the plastic handle and pull the grip handle to open the panel cover.
3. Slide the cover cover to the rear of the system and then remove the cover in the direction indicated by the arrow.
4. To reinstall the chassis cover follow steps 1-4 in reverse order.



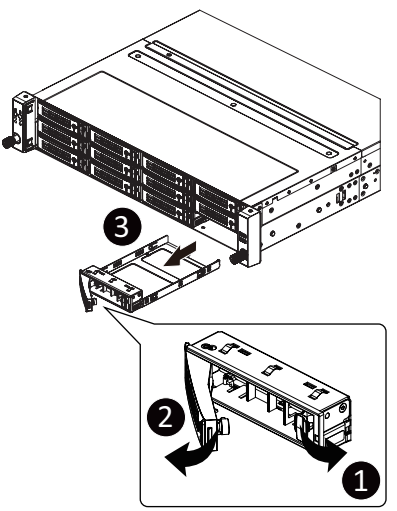
## 3-2 Removing and Installing the Hard Disk Drive

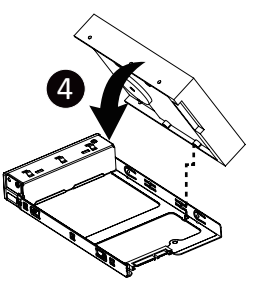
Read the following guidelines before you begin to install the hard disk drive:

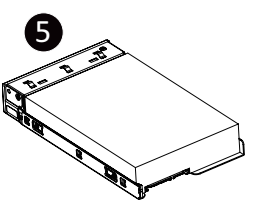
- Take note of the HDD tray orientation before sliding it out.
- The tray will not fit back into the bay if it is inserted incorrectly.
- Make sure that the hard disk drive is connected to the connector on the backplane.

**Follow these instructions to install a 3.5" hard disk drive:**

1. Press the release button.
2. Extend the locking lever.
3. Pull the locking lever in the direction indicated to remove the 3.5" HDD tray.
4. Pull the sides of the HDD tray in the direction indicated.
5. Slide the hard disk drive into the HDD tray.
6. Push the sides of the HDD tray back in the direction indicated to secure the hard disk drive in place.
7. Reinsert the HDD tray into the slot and close the locking lever.

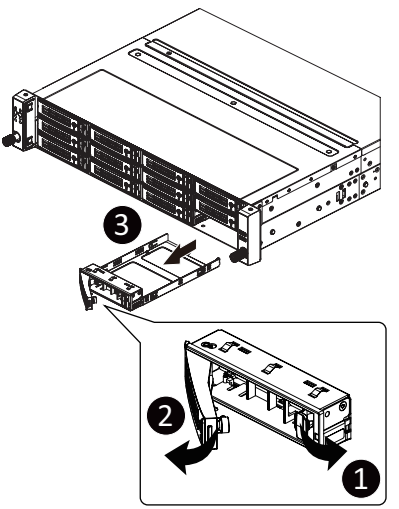


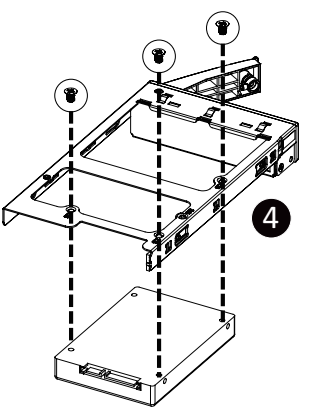



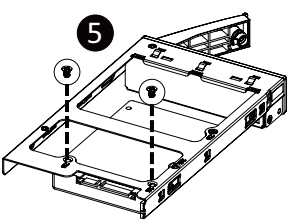



**Follow these instructions to install a 2.5" hard disk drive into 3.5" HDD Tray:**

1. Press the release button.
2. Extend the locking lever.
3. Pull the locking lever in the direction indicated to remove the HDD tray.
4. Align the hard disk drive with the positioning screw on the HDD tray.
5. Secure the hard disk drive with five screws.
6. Reinsert the HDD tray into the slot and close the locking lever



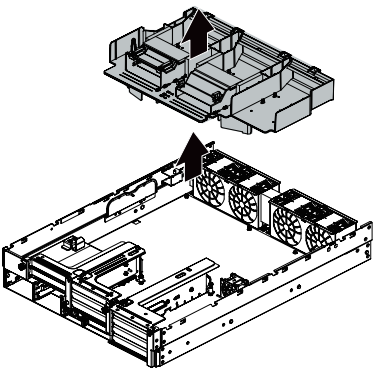



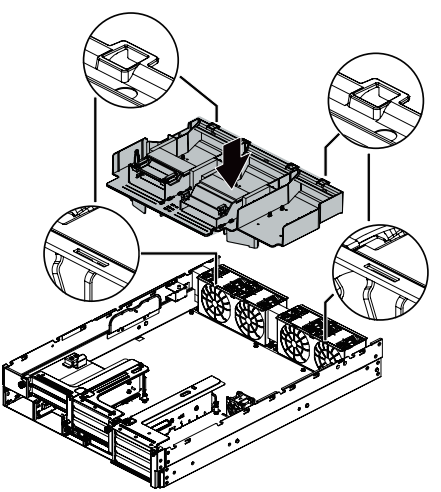



## 3-3 Removing and Installing the Fan Duct

**Follow these instructions to remove the fan duct:**

1. Lift up to remove the fan duct.
2. To reinstall the fan duct, align the fan duct with the guiding groove. Push down the fan duct until it is firmly seated on the system.





## 3-4 Removing and Installing the Heat Sink

Read the following guidelines before you begin to install the heat sink:

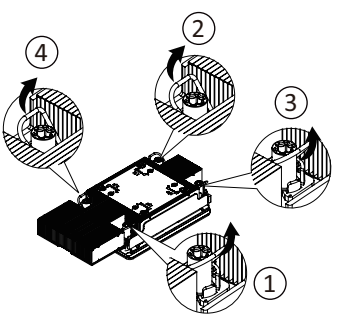
- Always turn off the computer and unplug the power cord from the power outlet before installing the heat sink to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system unit on a flat and stable surface.
- Open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

**WARNING!**

Failure to 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 heat sink:**

1. Loosen the screws securing the heat sink in place in reverse order (4→3→2→1).
2. Lift and remove the heat sink from the system.
3. To install the heat sink, reverse steps 1-2 while ensuring that you tighten the captive screws in sequential order (1→2→3→4) as seen in the image below.



## 3-5 Installing the CPU and Heat Sink

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

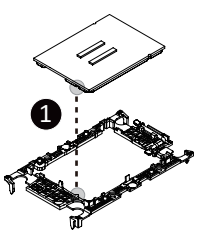
- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system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

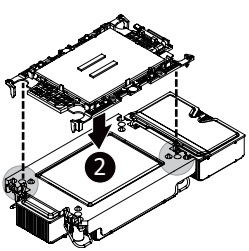
**WARNING!**

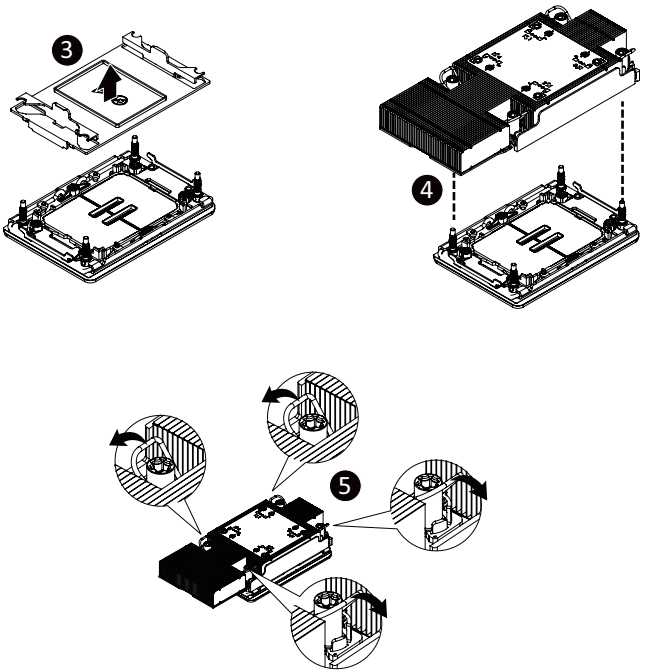
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

**Follow these instructions to install the CPU:**

1. Align the processor to the carrier so that the gold triangle on the processor aligns with the triangle on the carrier, and then install the processor into the carrier.
   NOTE: Apply thermal compound evenly on the top of the CPU.
2. Carefully flip the heatsink over. Align the carrier assembly so that the triangle on the carrier aligns with the triangle on the heatsink, and then install the carrier assembly onto the bottom of the heatsink.
3. Remove the CPU socket cover.
   NOTE: Save and replace the CPU socket cover if the processor is removed from its socket.
4. Align the heatsink to the CPU socket using the guide pins and make sure the gold triangle is in the correct orientation. Then place the heatsink onto the top of the CPU socket.
5. Secure the heatsink by tightening the screws in sequential order (1→2→3→4).
   NOTE: When removing the heatsink, loosen the screws in reverse order (4→3→2→1).






## Carrier Types used for Package Types

| Package Type | Granite Rapids-SP XCC | Granite Rapids-SP HCC<br>Granite Rapids-SP LCC<br>Sierra Forest-SP<br>Clearwater Forest-SP |
|---|---|---|
| **Carrier Code** | E2A | E2B |
| **Shim?** | No | Yes |
| **Integrated TIM Break Lever** | Yes | Yes |

**NOTE!**

- The carrier code is marked on each carrier and matches a code laser marked on to the IHS(Integrated Heat Spreader) to ensure the right parts are used together.
- When installing the heatsink to CPU,use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4.
- The screw tightening torque: 8 ± 0.5 kgf-cm.

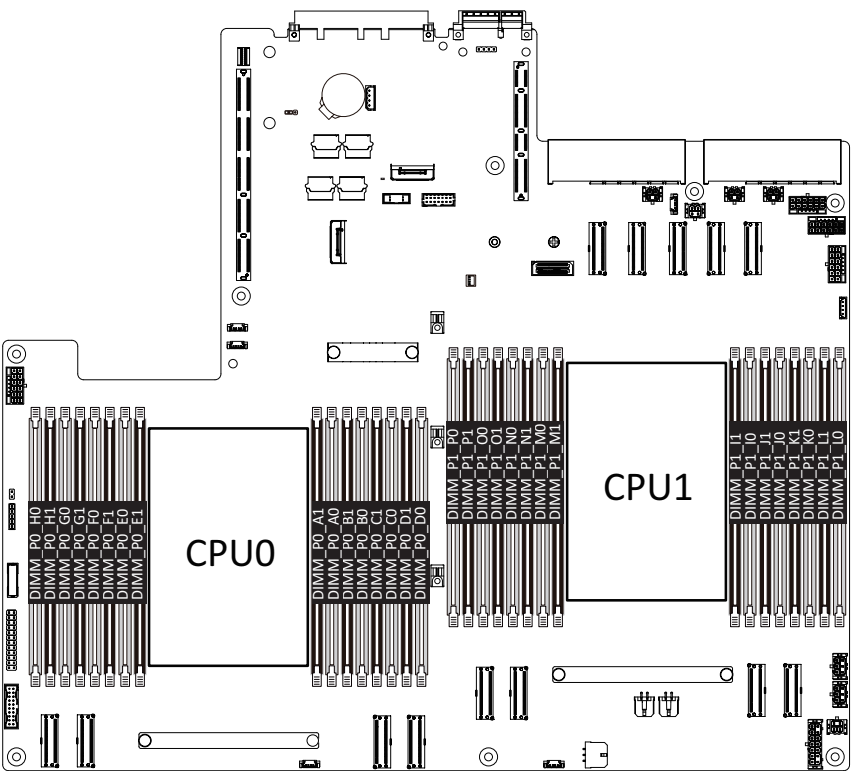
## 3-6 Removing and Installing Memory

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

- Make sure that the motherboard supports the memory. It is recommended that memory of the same capacity, brand, speed, and chips be used.
- 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.

### 3-6-1 Eight Channel Memory Configuration

This motherboard provides 32 DDR5 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.

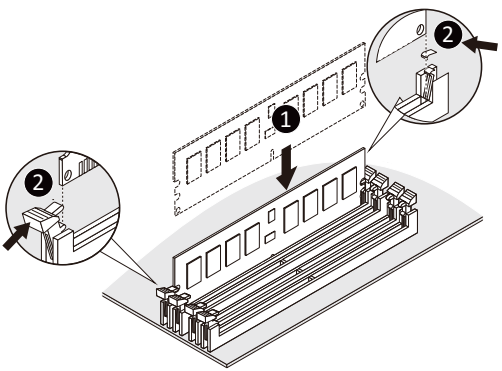


## 3-6-2 Removing and Installing a Memory Module

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 to 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.



## 3-6-3 DIMM Population Table

### Intel Xeon 6700E-Series Memory Support

| Type | Ranks Per DIMM and Data Width | DIMM Capacity (GB) | | | Channel Speed (MT/s); Voltage (V); Slots per Channel (SPC) & DIMMs per Channel (DPC) | |
|---|---|---|---|---|---|---|
| | | DRAM Density | | | | |
| | | 16Gb | | 32Gb | 1DPC/2SPC | 2DPC/2SPC |
| | | 1DPC | 2DPC | 1DPC | 1.1V | |
| RDIMM | 1Rx4 | 32GB | NA | NA | 6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMS only) | NA |
| | 2Rx8 | 32GB | NA | NA | | NA |
| | 2Rx4 | 64GB | 64GB | NA | | 5200, 4800 (DDR5-6400 rated RDIMMS only) |
| | 2Rx4 | NA | NA | 128GB | | NA |

**NOTE:**

- Only DDR5-6400 Rated RDIMMs Supported.

### Intel Xeon 6700E-Series CXL Memory Support

| Native DDR5 Memory Per Socket | | | | CXL Memory Per Socket | | | | |
|---|---|---|---|---|---|---|---|---|
| Slot 0 DIMM Ranks | Slot 0 DIMM Capacity (GB) | DIMM Type | DRAM Density (Gb) | CXL Memory Channels | CXL Memory Type | CXL Capacity Per Device/ Module | CXL Interleave | CXL Mode |
| 2Rx4 | 64 | 10x4 | 16 | 2+2 | DDR5 x8 | 64 GB | 1x4*, 2x2, 4x1 | 1LM+Vol |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR5 x16 | 128 GB | 1x2*, 2x1 | 1LM+Vol |
| 1Rx4 | 32 | 10x4 | 16 | 2 | DDR5 x8 | 128 GB | 1x2* | Intel® Flat Memory Mode |

**NOTE:**

- * Default setting in BIOS
- Intel Xeon 6700E-series (formerly codenamed Sierra Forest-SP) CXL memory configs are 1DPC ('Slot 0') only for native DDR5
- CXL Memory Channel notation: # of devices per root port, with root ports separated by "+". i.e. 2+2+2+2 = four root ports populated with two devices per root port
- CXL Interleave notation: sets x ways. i.e. 2x4 = One set of two modules, interleaved four-way
- CXL Modes:
  - 1LM+Vol = DDR5 ('1LM') and (Volatile) CXL memory visible to SW as separate tiers, separately interleaved
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW

## Intel Xeon 6500P/6700P-Series Memory Support

| Type | Ranks Per DIMM and Data Width | DIMM Capacity (GB) | | | | | Channel Speed (MT/s); Voltage (V); Slots per Channel (SPC) & DIMMs per Channel Density (DPC) | |
|---|---|---|---|---|---|---|---|---|
| | | DRAM Density | | | | | | |
| | | 16Gb | | 24Gb | | 32Gb | 1DPC/2SPC | 2DPC/2SPC |
| | | 1DPC | 2DPC | 1DPC | 2DPC | 2DPC | 1.1V | |
| RDIMM | 1Rx8 | 16GB | NA | 24GB | NA | NA | 6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMS only) | 5200, 4800 (DDR5-6400 rated RDIMMS only) |
| | 1Rx4 | 32GB | NA | 48GB | NA | NA | | |
| | 2Rx8 | 32GB | 32GB | 48GB | NA | NA | | |
| | 2Rx4 | 64GB | 64GB* | 96GB | 96GB* | 128GB* | | |
| RDIMM 3DS | 4Rx4 | NA | 128GB* | NA | NA | NA | | |
| | 8Rx4 | NA | 256GB* | NA | NA | NA | | |
| MCR DIMM | 2Rx8 | 32GB | NA | NA | NA | NA | 8000, 7200 (MCR-8800 only) | N/A (no 2DPC configs for MCR) |
| | 2Rx4 | 64GB | NA | NA | NA | NA | | |

**NOTE:**

- *Supported in 1S/2S/4S/8S systems. All others support 1S/2S only

## Intel Xeon 6500P/6700P-Series CXL Memory Support

| Native DDR5 Memory Per Socket | | | | CXL Memory Per Socket | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Slot0 DIMM Ranks | Slot0 DIMM Capacity (GB) | DIMM Type | DRAM Density (Gb) | CXL Memory Channels | CXL Memory Type | CXL Capacity Per Device/ Module | CXL Interleave | CXL Mode | 4S &8S Support |
| 2Rx4 | 96 | 10x4 | 24 | 2+2 | DDR5 x8 | 96 GB | 1x4*, 2x2, 4x1 | 1LM+Vol | Yes |
| 2H3SD | 64 | 10x4 | 16 | 2+2 | DDR4 x8 DDR5 x8 | 128 GB | 1x4*, 2x2,1 | 1LM+Vol | Yes |
| 2Rx4 | 128 | 10x4 | 16 | 2+2 | DDR5 x8 | 64 GB | hetero x12 | Hetero | Yes |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR5 x16 | 2ch 64 GB | hetero x12 | Hetero | Yes |
| 2Rx4 | 64 | 10x4 | 16 | 2+2+2+2 | DDR5 x8 | 64 GB | 1x8*, 2x4, 4x2 | 1LM+Vol | No |
| 2Rx4 | 64 | 10x4 | 16 | 2 | DDR5 x8 | 256 GB | 1x2* | 1LM+Vol | No |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR4 x16 DDR5 x16 | 2ch 128 GB | 1x2* | Intel® Flat Memory Mode | No |

**NOTE:**

- * Default setting in BIOS
- Xeon 6500P/6700P-series (formerly codenamed Granite Rapids-SP) CXL memory configs are 1DPC ('Slot 0') only for native DDR5
- CXL Memory Channel notation: # of devices per root port, with root ports separated by "+". i.e. 2+2+2+2 = four root ports populated with two devices per root port
- CXL Interleave notation: sets x ways. i.e. 2x4 = Set of two modules, interleaved four-way
- CXL Modes:
  - 1LM+Vol = Native DDR5 ('1LM') and (volatile) CXL memory visible to SW as separate tiers, separately interleaved
  - Hetero x12 = DDR5 and (volatile) CXL memory interleaved together in one 12-way set (See graphic in next slide)
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW.

## 3-6-4 Processor and Memory Module Matrix Table

| Memory Q'ty for each CPU | CPU0 | | | | | | | | | | | | | | | | CPU1 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | H0 | H1 | G0 | G1 | F0 | F1 | E0 | E1 | A1 | A0 | B1 | B0 | C1 | C0 | D1 | D0 | P0 | P1 | O0 | O1 | N0 | N1 | M0 | M1 | I1 | I0 | J1 | J0 | K1 | K0 | L1 | L0 |
| 1 DIMM | | | | | | | | | | v | | | | | | | | | | | | | | | | v | | | | | | |
| 4 DIMM | | | v | | | | v | | | v | | | | v | | | | | v | | | | v | | | v | | | | v | | |
| | v | | | | v | | | | | | | v | | | | v | v | | v | | | | | | | | | v | | | | v |
| 8 DIMM | v | | v | | v | | v | | | v | | v | | v | | v | v | | v | | v | | v | | | v | | v | | v | | v |
| | | | v | v | | | v | v | v | v | | | v | v | | | | | v | v | | | v | v | v | v | | | v | v | | |
| | v | v | | | v | v | | | | | v | v | | | v | v | v | v | | | v | v | | | | | v | v | | | v | v |
| 12 DIMM | v | | v | v | v | | v | v | v | v | | v | v | v | | v | v | | v | v | v | | v | v | v | v | | v | v | v | | v |
| 16 DIMM | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v | v |

**NOTE:**

- Xeon 6700E/6500E-series do not support 12 DIMMs Configuration.

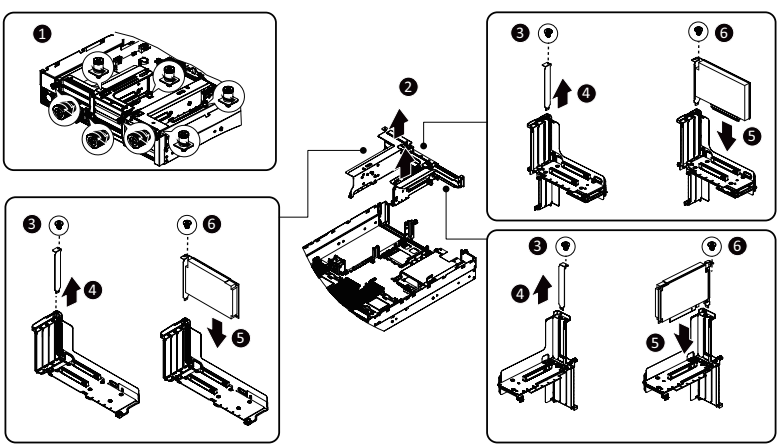
## 3-7 Removing and Installing the PCIe Card

- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered off and all power sources have been disconnected from the server prior to installing a PCIe card.
- Failure to observe these warnings could result in personal injury or damage to equipment.

- The PCIe riser assembly does not include a riser card or any cabling as standard. To install a PCIe card, a riser card must be installed.

**Follow these instructions to install a PCIe card:**

1. Loosen the two thumbnail screws securing the riser bracket inside the system.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the slot cover from riser bracket.
4. Orient the PCIe card with the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCIe card connector.
   **NOTE:** Some riser brackets allow for single or multiple PCIe cards.
   Repeat steps 3-4 as necessary.
5. Secure the PCIe card with the screw.
6. Repeat steps 1-2 to install the PCIe card into the system.



# 3-8 Installing the Mezzanine Card

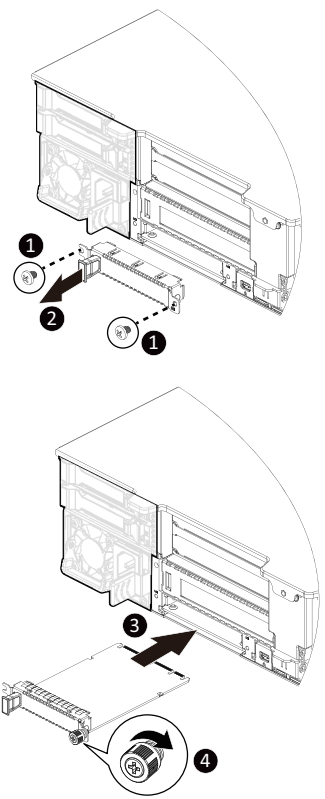
## 3-8-1 Installing the OCP 3.0 Mezzanine Card

Use of the following type of OCP 3.0 NIC is recommended:

- OCP 3.0 SFF with pull tab
- OCP 3.0 SFF with ejector latch

**Follow these instructions to install an OCP 3.0 Mezzanine card:**

1. Remove the two screws securing the OCP 3.0 card slot cover.
2. Remove the slot cover from the system.
3. Insert the OCP 3.0 card into the card slot ensuring that the card is firmly connected to the connector on the motherboard.
4. Tighten the thumbnail screw to secure the OCP 3.0 card in place.
5. Reverse steps 3-4 to replace the OCP 3.0 card.



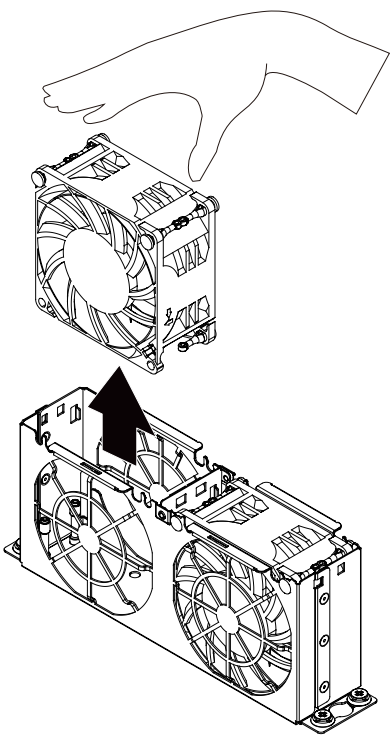
## 3-9 Replacing the Fan Assembly

- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

Failure to observe these warnings could result in personal injury or damage to equipment.

**Follow these instructions to replace a fan assembly:**

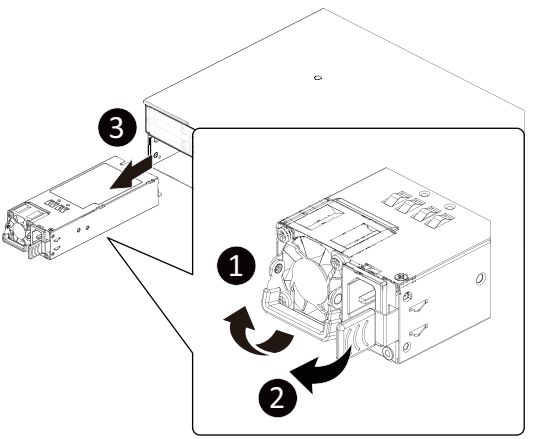
1. Using the latches, lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.

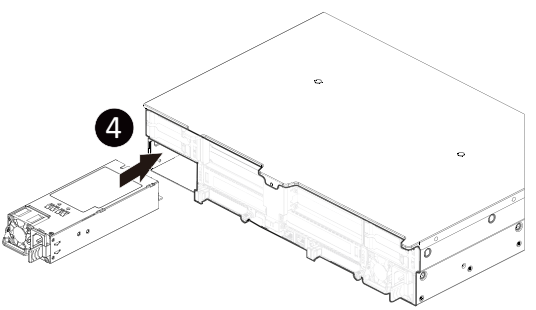


## 3-10 Removing and Installing the Power Supply

**Follow these instructions to replace the power supply:**

1. Flip up and then grasp the power supply handle.
2. Press the retaining clip on the right side of the power supply unit in the direction indicated.
3. Pull out the power supply unit using the handle.
4. Insert the replacement power supply unit firmly into the chassis. Connect the AC power cord to the replacement power supply.
5. Repeat steps 1-4 for replacement of the second power supply.

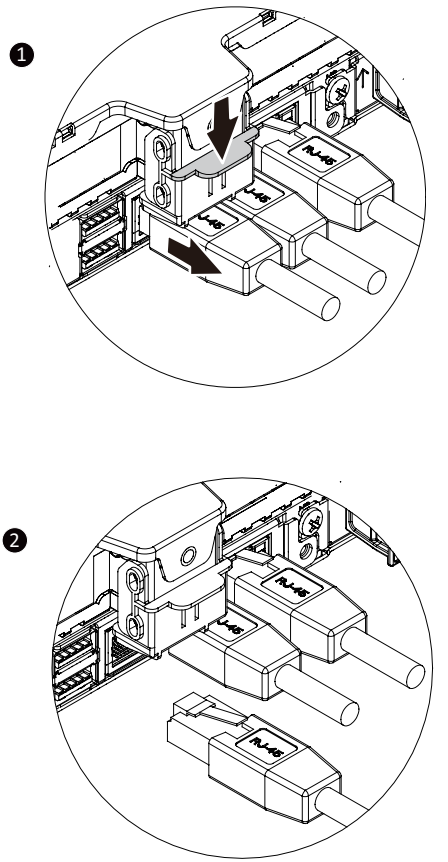


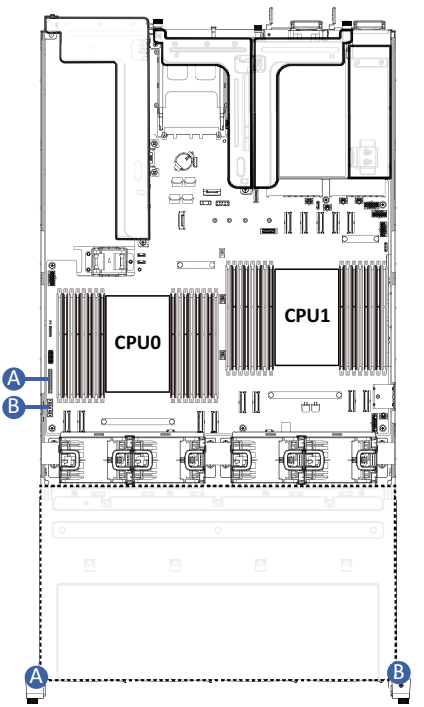
## 3-11 Removing the LAN Cable

**Follow these instructions to remove the LAN cable:**

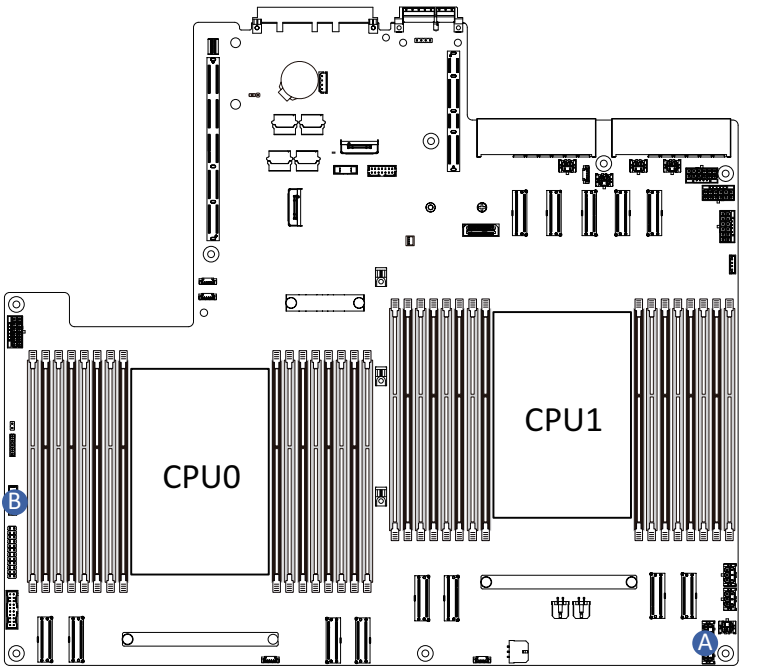
1. Press the release latch while simultaneously pulling out the LAN cable

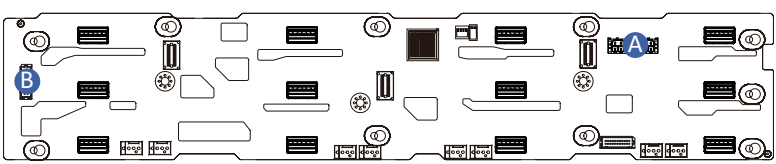


## 3-12 Cable Routing

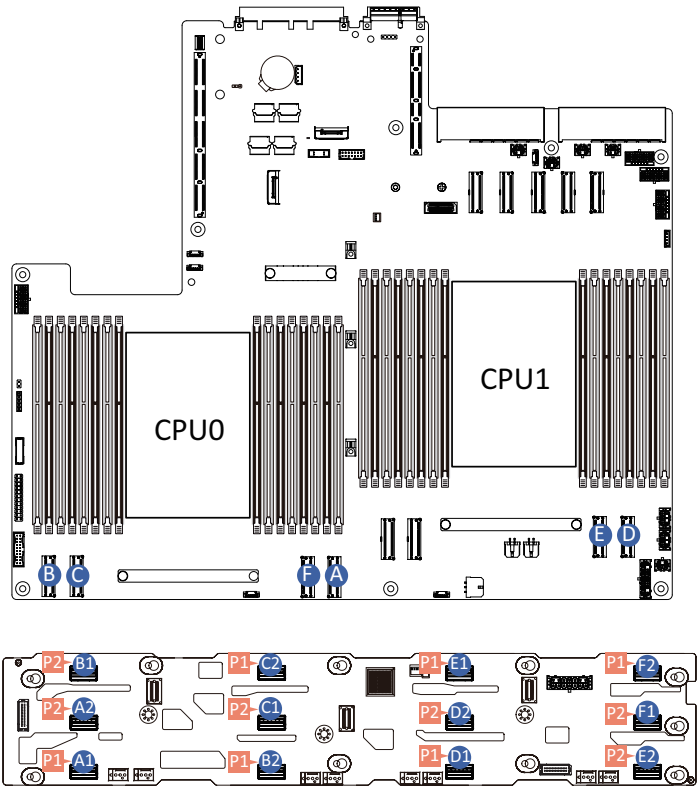



| | | | |
|---|---|---|---|
| A | Front Panel LEDs and Buttons Cable | Motherboard: FP_1<br>Front IO Board: FP_1 |
| | | Front IO Board: FP_1 |
| B | Front Panel USB 3 Ports Cable | Motherboard: FUSB_1 |
| | | -- |

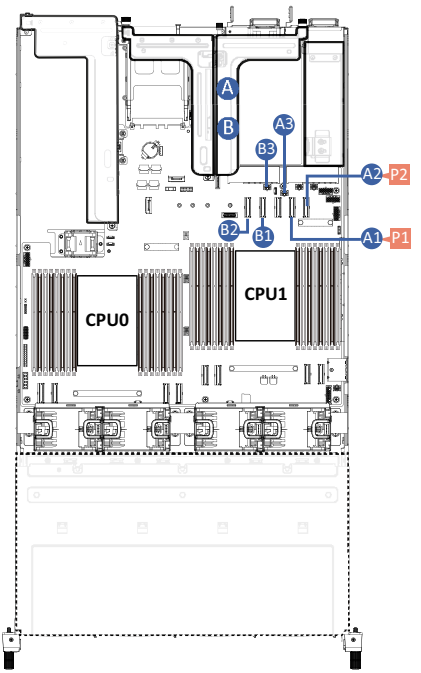


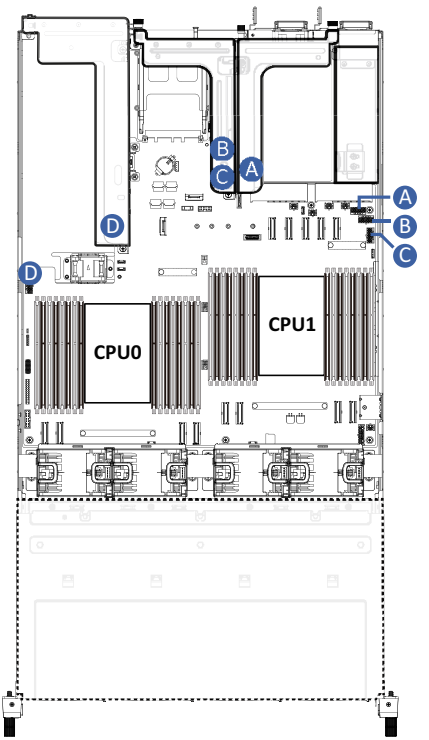

| | | |
|---|---|---|
| **A** | HDD Backplane Board Power Cable | Motherboard: BP_ATX1 |
| | | Front HDD Board: ATX |
| **B** | HDD Backplane Board Signal Cable | Motherboard: BP_1 |
| | | Front HDD Board: BP_1 |




| | | | | | |
|---|---|---|---|---|---|
| A | NVMe 0-1 Cable | Motherboard: U.2_P0_4AC<br>Front HDD Board: A1: U.2_0 A2: U.2_1 | D | NVMe 6-7 Cable | Motherboard: U.2_P1_4AC<br>Front HDD Board: D1: U.2_6 D2: U.2_7 |
| B | NVMe 2-3 Cable | Motherboard: U.2_P0_5CA<br>Front HDD Board: B1: U.2_2 B2: U.2_3 | E | NVMe 8-9 Cable | Motherboard: U.2_P1_4EG<br>Front HDD Board: E1: U.2_8 E2: U.2_9 |
| C | NVMe 4-5 Cable | Motherboard: U.2_P0_5GE<br>Front HDD Board: C1: U.2_4 C2: U.2_5 | F | NVMe 10-11 Cable | Motherboard: U.2_P1_5CA<br>Front HDD Board: F1: U.2_10 F2: U.2_11 |



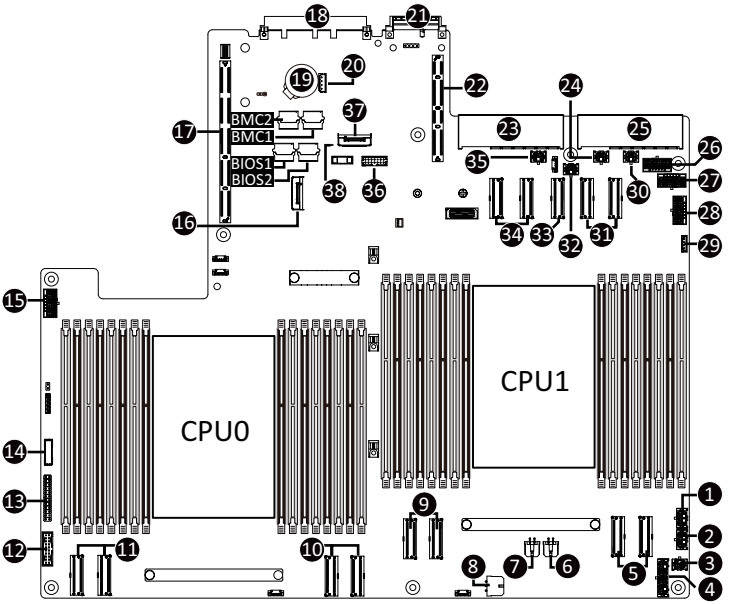

| | | |
|---|---|---|
| **A** | System Rear Side PCIe Signal and Power Cable | PCIe Riser Bracket:<br>Slot 9 |
| | | Motherboard:<br>A1: U2_P1_2AC<br>A2: U2_P1_2EG<br>A3: PCIE_PWR2 |
| **B** | System Rear Side PCIe Signal and Power Cable | PCIe Riser Bracket:<br>Slot 4 |
| | | Motherboard:<br>B1: U2_P1_3AC<br>B2: U2_P1_3EG<br>B3: PCIE_PWR1 |




| | | |
|---|---|---|
| A | GPU Card Power Cable (Reserved) | Motherboard : GPU12V_S9 |
| | | PCIe Riser Bracket |
| B | | Motherboard : GPU12V_S8 |
| | | PCIe Riser Bracket |
| C | | Motherboard : GPU12V_S7 |
| | | PCIe Riser Bracket |
| D | | Motherboard : GPU12V_S3 |
| | | PCIe Riser Bracket |

# Chapter 4 Motherboard Components

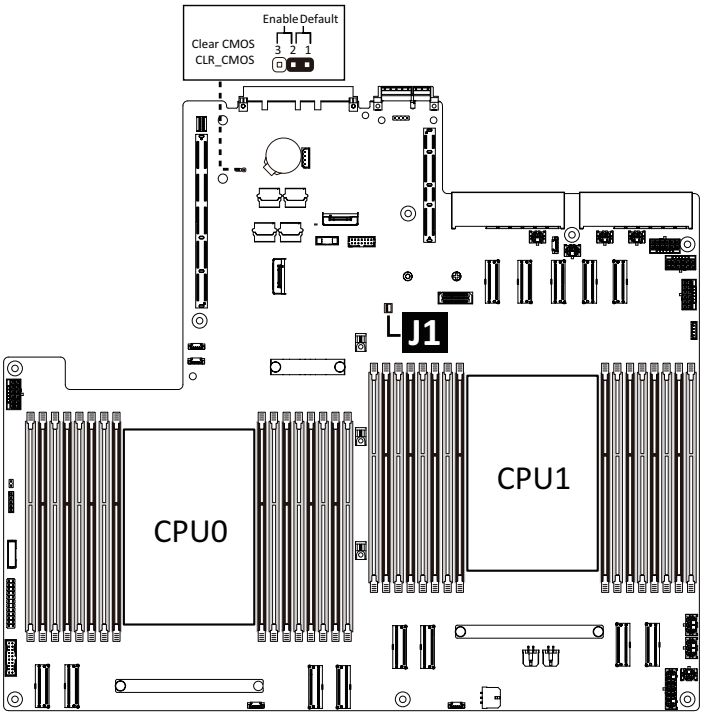
## 4-1 Motherboard Components




| Item | Description |
|---|---|
| 1 | 2 x 3 Pin ATX Power Connector (PWR3) |
| 2 | 2 x 3 Pin ATX Power Connector (PWR2) |
| 3 | 2 x 2 Pin P12V Power Connector (PWR_12V_1) |
| 4 | 2 x 7 Pin ATX Power Connector (PWR1) |
| 5 | MCIO Connector (U2_P1_4EG/4AC/PCIe Gen5) |
| 6 | 2 x 2 Pin 12V Power Connector (PWR_12V_2) |
| 7 | 2 x 2 Pin 12V Power Connector (PWR_12V_3) |
| 8 | 2 x 3 Pin ATX Power Connector (PWR4) |
| 9 | MCIO Connector (U2_P1_5CA/5GE/PCIe Gen5) |
| 10 | MCIO Connector (U2_P0_4EG/4AC/PCIe Gen5) |
| 11 | MCIO Connector (U2_P0_5CA/5GE/PCIe Gen5) |
| 12 | Front Panel USB 3.2 Gen1 Connector |
| 13 | Front Panel Connector |
| 14 | HDD Backplane Board Connector |
| 15 | 12V GPU Power Connector (P12V_S3) |
| 16 | M.2 Slot (PCIe Gen5 x4, NGFF-22110/Supports heatsink) |
| 17 | Riser Connector (GENZ1/PCIe Gen5) |
| 18 | OCP 3.0 Connector (PCIe Gen5 x16) |
| 19 | System Battery Socket |

| Item | Description |
|---|---|
| 20 | IPMB Connector |
| 21 | IO Board Connector |
| 22 | Riser Connector (GENZ2/PCIe Gen5) |
| 23 | Power Supply Connector#1 (Primary) |
| 24 | PCIe Power Connector (PCIE_PWR3) |
| 25 | Power Supply Connector#2 (Secondary) |
| 26 | 12V GPU Power Connector (P12V_S9) |
| 27 | 12V GPU Power Connector (P12V_S8) |
| 28 | 12V GPU Power Connector (P12V_S7) |
| 29 | VROC Upgrade Module Connector |
| 30 | PCIe Power Connector (PCIE_PWR4) |
| 31 | MCIO Connector (U2_P1_2AC/2EG/PCIe Gen5) |
| 32 | PCIe Power Connector (PCIE_PWR2) |
| 33 | MCIO Connector (U2_P1_1AC/PCIe Gen5) |
| 34 | MCIO Connector (U2_P1_3EG/3AC/PCIe Gen5) |
| 35 | PCIe Power Connector (PCIE_PWR1) |
| 36 | TPM Module Connector (SPI Interface) |
| 37 | PRoT Module Connector (M.2 M-Key/only enabled on RoT SKU) |
| 38 | BMC Firmware Readiness LED |

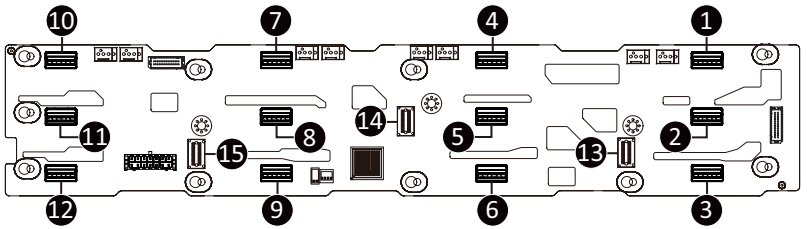
## 4-2 Jumper Settings




| J1 | | ON | OFF |
|---|---|---|---|
| 1 | S3_MASK | Stop initial power on when BMC is not ready | Normal [Default] |
| 2 | BIOS_RCVR | BIOS recovery mode | Normal [Default] |
| 3 | BIOS_PWD | Clear supervisor password | Normal [Default] |
| 4 | RST BMC_EN | ID button to enable BMC reset | Normal [Default] |

## 4-3 Backplane Board Storage Connector

### 4-3-1 CBP20C7




| Item | Description |
|---|---|
| 1. | MCIO Connector (MCIO 4i/U.2_0) |
| 2. | MCIO Connector (MCIO 4i/U.2_1) |
| 3. | MCIO Connector (MCIO 4i/U.2_2) |
| 4. | MCIO Connector (MCIO 4i/U.2_3) |
| 5. | MCIO Connector (MCIO 4i/U.2_4) |
| 6 | MCIO Connector (MCIO 4i/U.2_5) |
| 7. | MCIO Connector (MCIO 4i/U.2_6) |
| 8. | MCIO Connector (MCIO 4i/U.2_7) |
| 9. | MCIO Connector (MCIO 4i/U.2_8) |
| 10. | MCIO Connector (MCIO 4i/U.2_9) |
| 11. | MCIO Connector (MCIO 4i/U.2_10) |
| 12. | MCIO Connector (MCIO 4i/U.2_11) |
| 13. | SlimLine Connector (SFF-8654 4i/SL_SAS0) |
| 14. | SlimLine Connector (SFF-8654 4i/SL_SAS1) |
| 15. | SlimLine Connector (SFF-8654 4i/SL_SAS2) |

# Chapter 5 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 4 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.)

# 5-1 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.

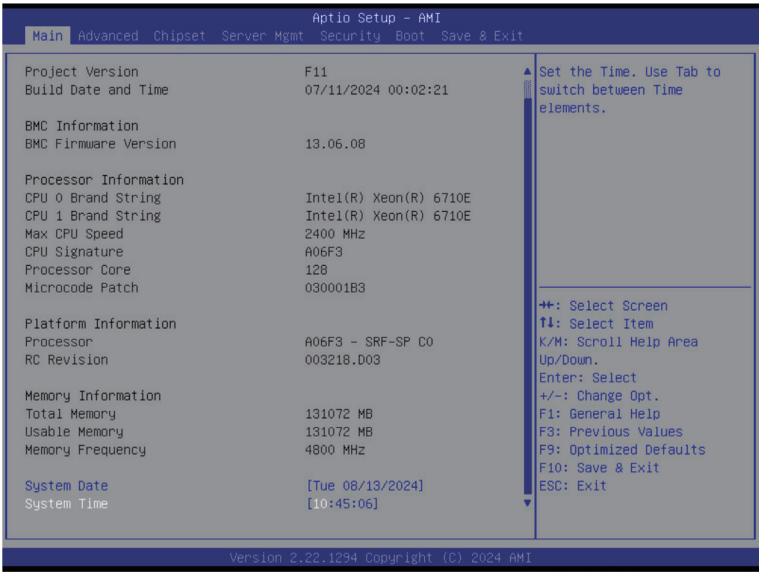
**Main Menu Help**

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.



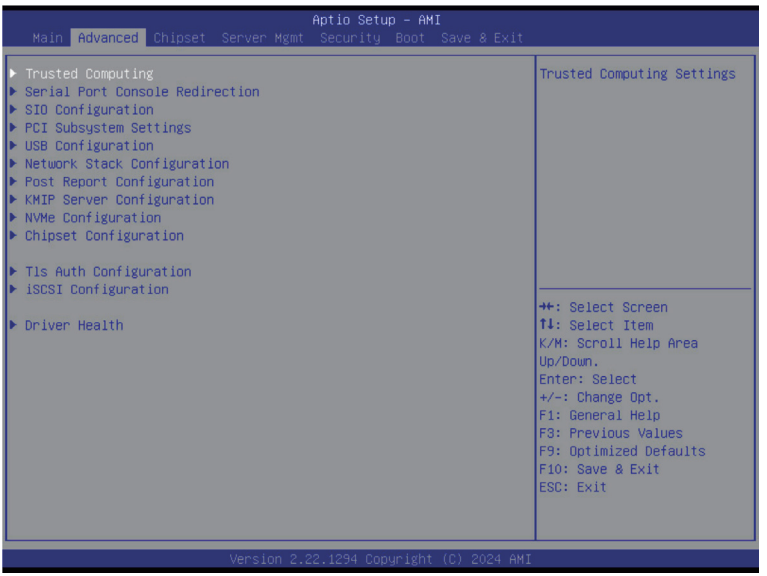

| Parameter | Description |
|---|---|
| Project Name | Displays the project name information. |
| Project Version | Displays version number of the BIOS setup utility. |
| Build Date and Time | Displays the date and time when the BIOS setup utility was created. |
| BMC Information | |
| BMC Firmware Version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

(Note1) This section will display capacity and frequency information of the memory that the customer has installed.

| Parameter | Description |
|---|---|
| System Date | Sets the date following the weekday-month-day-year format. |
| System Time | Sets the system time following the hour-minute-second format. |

## 5-2 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.



## 5-2-1 Trusted Computing


| Parameter | Description |
|---|---|
| Configuration | |
| 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: Disabled, Enabled. Default setting is **Enabled**. |

## 5-2-2 Serial Port Console Redirection


| Parameter | Description |
|---|---|
| COM1 Console Redirection(Note) | Console redirection enables the users to manage the system from a remote location.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| COM1 Console Redirection Settings | Press [Enter] to configure advanced items.<br>**Please note that this item is configurable when COM1 Console Redirection is set to Enabled.**<br>◆ Terminal Type<br>– Selects a terminal type to be used for console redirection.<br>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is **VT100PLUS**.<br>◆ Bits per second<br>– Selects the transfer rate for console redirection.<br>– Options available: 9600, 19200, 38400, 57600, 115200. Default setting is **115200**.<br>◆ Data Bits<br>– Selects the number of data bits used for console redirection.<br>– Options available: 7, 8. Default setting is **8**. |

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

| Parameter | Description |
|---|---|
| COM1 Console Redirection Settings (continued) | ◆ Parity<br>– A parity bit can be sent with the data bits to detect some transmission errors.<br>– Even: parity bit is 0 if the num of 1's in the data bits is even.<br>– Odd: parity bit is 0 if num of 1's in the data bits is odd.<br>– Mark: parity bit is always 1. Space: Parity bit is always 0.<br>– Mark and Space Parity do not allow for error detection.<br>– Options available: None, Even, Odd, Mark, Space. Default setting is **None**.<br>◆ Stop Bits<br>– 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.<br>– Options available: 1, 2. Default setting is **1**.<br>◆ Flow Control<br>– 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.<br>– Options available: None, Hardware RTS/CTS. Default setting is **None**.<br>◆ VT-UTF8 Combo Key Support<br>– Enable/Disable the VT-UTF8 Combo Key Support.<br>– Options available: Enabled, Disabled. Default setting is **Enabled**.<br>◆ Recorder Mode<br>– When this mode enabled, only texts will be send. This is to capture Terminal data.<br>– Options available: Enabled, Disabled. Default setting is **Disabled**.<br>◆ Resolution 100x31<br>– Enable/Disable extended terminal resolution.<br>– Options available: Enabled, Disabled. Default setting is **Enabled**.<br>◆ Putty KeyPad<br>– Selects Function Key and KeyPad on Putty.<br>– Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is **VT100**. |

| Parameter | Description |
|---|---|
| Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection[(Note)] | EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| Serial Port for Out-of-Band EMS Console Redirection Settings | Press [Enter] to configure advanced items.<br>**Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.**<br>◆ Out-of-Band Mgmt Port<br>– Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port.<br>– Default setting is **COM1**.<br>◆ Terminal Type EMS<br>– Selects a terminal type to be used for console redirection.<br>– Options available: VT100, VT100PLUS, VT-UTF8, ANSI. Default setting is **VT100PLUS**.<br>◆ Bits per second EMS<br>– Selects the transfer rate for console redirection.<br>– Options available: 9600, 19200, 57600, 115200. Default setting is **115200**.<br>◆ Flow Control EMS<br>– 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.<br>– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is **None**. |

## 5-2-3 SIO Configuration

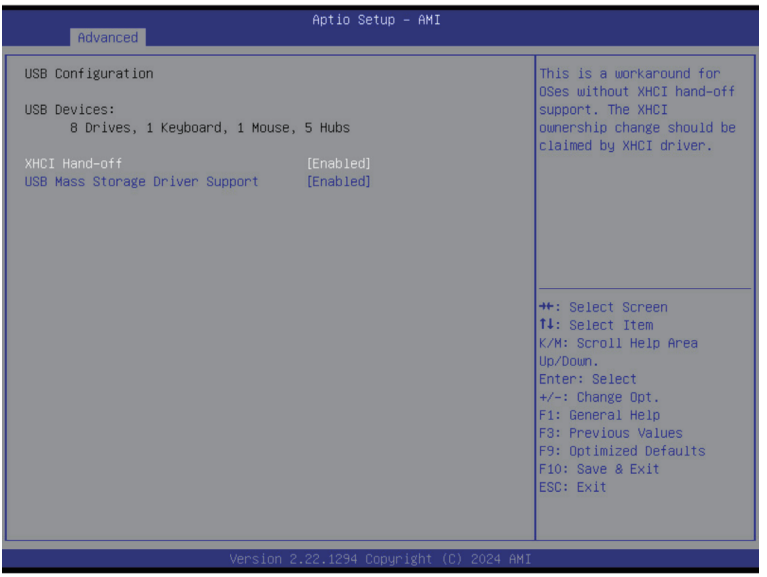

| Parameter | Description |
|---|---|
| AMI SIO Driver Version | Displays the AMI SIO driver version information. |
| Super IO Chip Logical Device(s) Configuration | |
| [*Active*] Serial Port | Press [Enter] to configure advanced items.<br>◆ Use This Device<br>– When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port.<br>– Options available: Enabled, Disabled. Default setting is **Enabled**.<br>◆ Logical Device Settings/Current:<br>– Displays the serial port base I/O address and IRQ.<br>◆ Possible:<br>– Configures the serial port base I/O address and IRQ.<br>Use Automatic Settings<br>IO=3F8h; IRQ=4; DMA;<br>IO=3F8h; IRQ=4; DMA;<br>IO=2F8h; IRQ=4; DMA;<br>IO=3E8h; IRQ=4; DMA;<br>IO=2E8h; IRQ=4; DMA;<br>Default setting is **Use Automatic Settings**. |

## 5-2-4 PCI Subsystem Settings


| Parameter | Description |
|---|---|
| PCI Bus Driver Version | Displays the PCI Bus Driver version information. |
| SLOT_# I/O ROM(Note1) | When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| SLOT_# Lanes(Note1) | Change the PCIe lanes. Default setting is **Auto**. |
| SLOT_#_Max Link Speed(Note1) | Configure PCIe max link speed.<br>Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5.<br>Default setting is **Auto**. |
| M2 I/O ROM(Note2) | Enable/Disable M2 I/O ROM.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| M2 Lanes(Note2) | Change the M2 PCIe lanes. Default setting is **Auto**. |
| M2 Max Link Speed(Note2) | Configure M2 PCIe max link speed.<br>Options available: Auto, Gen1, Gen2, Gen3, Gen4, Gen5.<br>Default setting is **Auto**. |
| PCI Devices Common Settings | |
| Re-Size BAR Support | If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| 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 **Enabled**. |

(Note1) This section is dependent on the available PCIe Slot.
(Note2) This section is dependent on the available M2 Slot.
(Note3) This section is dependent on the available LAN controller.

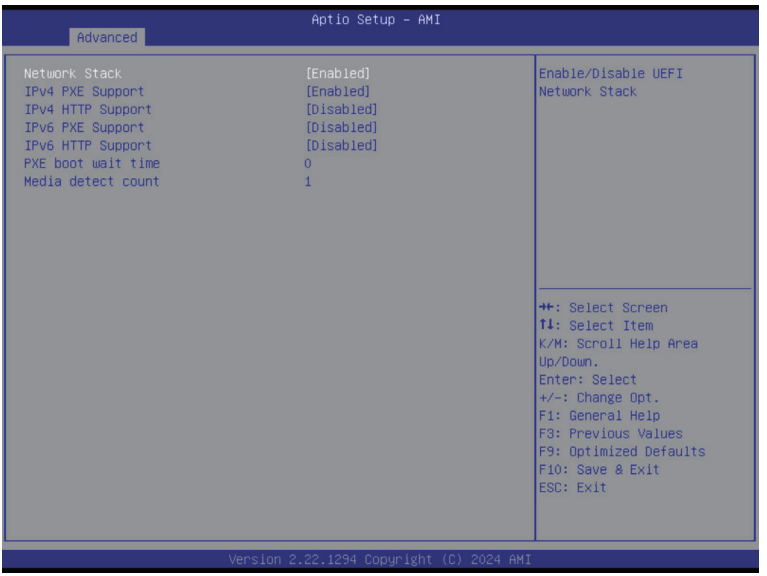
## 5-2-5 USB Configuration




| 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 **Enabled**. |
| USB Mass Storage Driver Support(Note) | Enable/Disable the USB Mass Storage Driver Support.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |

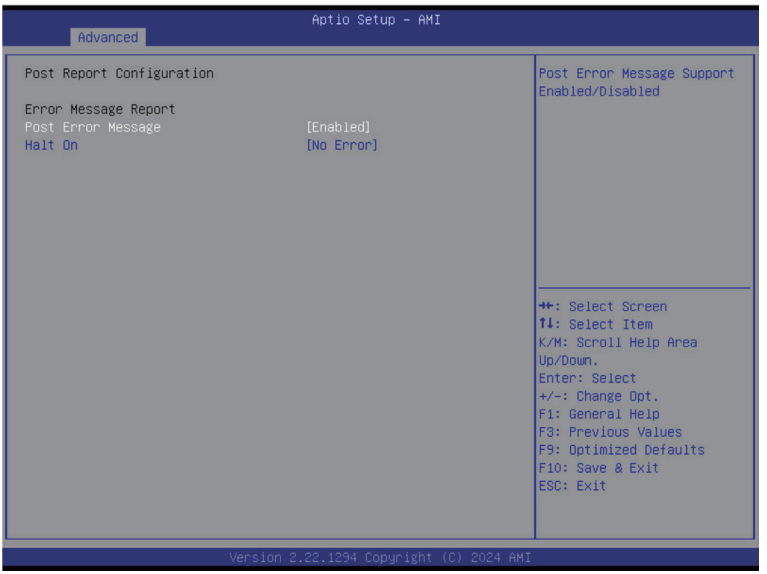
(Note) This item is present only if you attach USB devices.

## 5-2-6 Network Stack Configuration



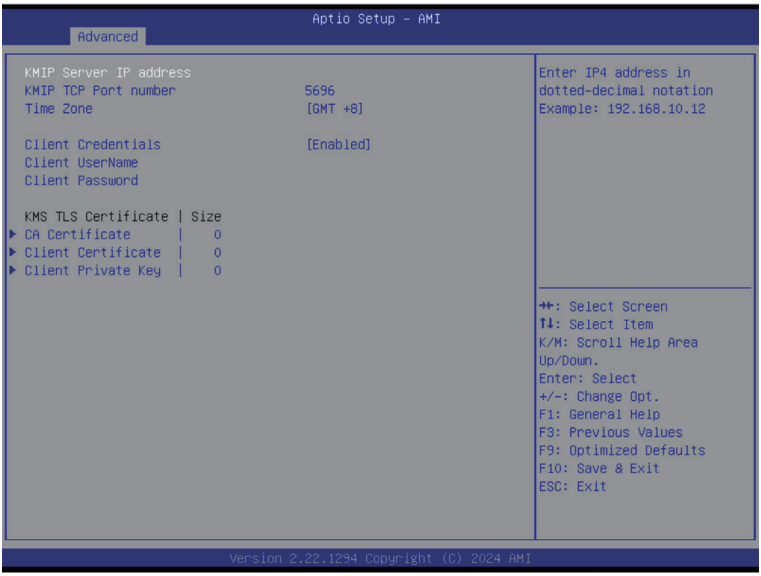

| Parameter | Description |
|---|---|
| Network Stack | Enable/Disable the UEFI network stack.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| Ipv4 PXE Support | Enable/Disable the Ipv4 PXE feature.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| Ipv4 HTTP Support | Enable/Disable the Ipv4 HTTP feature.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| Ipv6 PXE Support | Enable/Disable the Ipv6 PXE feature.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| Ipv6 HTTP Support | Enable/Disable the Ipv6 HTTP feature.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| 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. |

## 5-2-7 Post Report Configuration



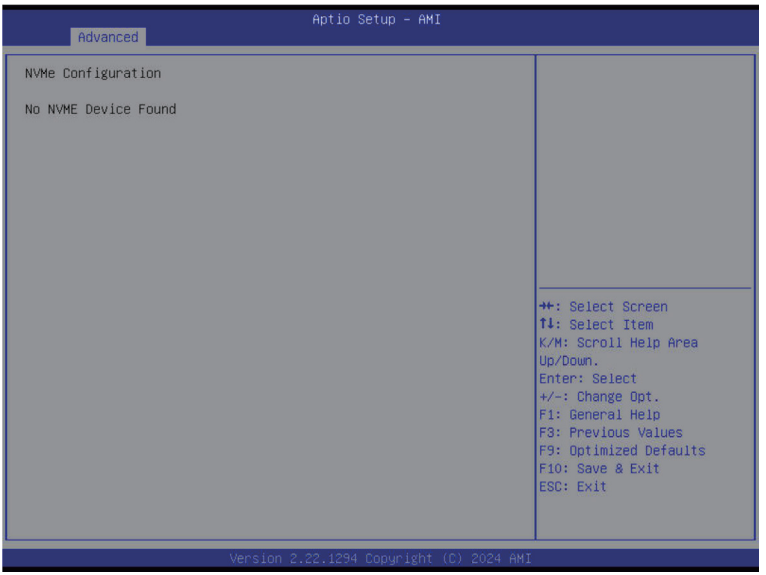

| Parameter | Description |
|---|---|
| Post Report Configuration | |
| Error Message Report | |
| Post Error Message | Enable/Disable the POST Error Message support.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| Halt On | Options available: No Error, All Error. Default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

## 5-2-8 KMIP Server Configuration



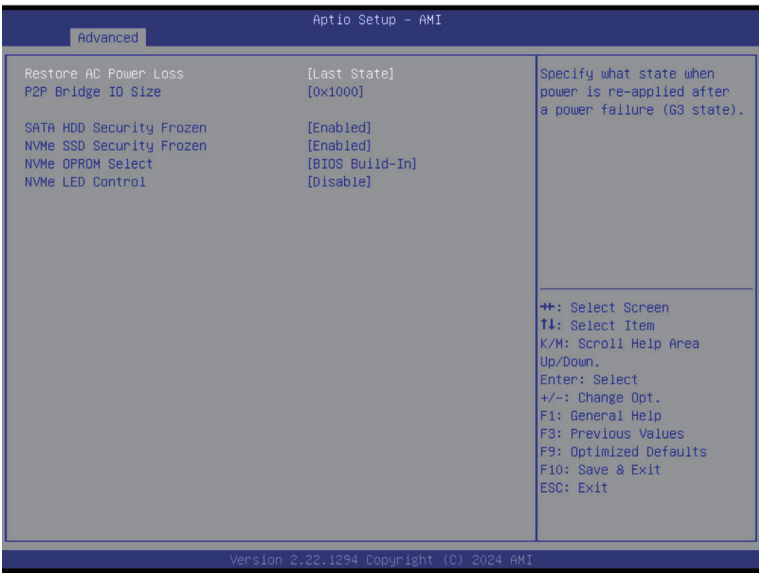

| Parameter | Description |
|---|---|
| KMIP Server IP address | |
| KMIP TCP Port Number | |
| Time Zone | Enter the correct time zone for this server.<br>Default setting is **GMT+8**. |
| Client Credentials | Use User and password credentials to authenticate the Client.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| Client UserName | Enter Client identify: UserName.<br>Name Length: 0-63 characters. |
| Client Password | Enter Client identify: Password.<br>Password Length: 0-31 characters. |
| KMS TLS Certificate / Size | |
| CA Certificate | Enroll factory defaults or load the KMS TLS certificates from the file. |
| Client Certificate | Enroll factory defaults or load the KMS TLS certificates from the file. |
| Client Private Key | Enroll factory defaults or load the KMS TLS certificates from the file. |

## 5-2-9 NVMe Configuration




| Parameter | Description |
|---|---|
| NVMe Configuration | Displays the NVMe devices connected to the system. |

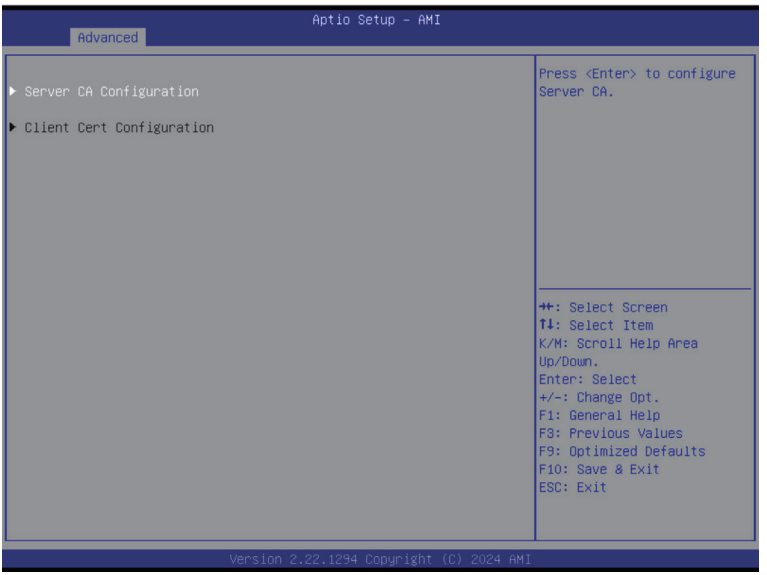
## 5-2-10 Chipset Configuration




| Parameter | Description |
|---|---|
| Restore on AC Power Loss(Note) | 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.<br>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.<br>Options available: 0x100, 0x150, 0x1000. Default setting is **0x1000**. |
| SATA HDD Security Frozen | Enable/Disable this item to send freeze lock command to SATA HDD.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| NVMe SSD Security Frozen | Attempt to send freeze lock command to NVMe SSDs during boot.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| NVMe OPROM Select | BIOS Build-In is default setting. Select Device Itself, then this NVMe page will not display any device. Unless the device doesn't have OPROM.<br>Options available: BIOS Build-In, NVMe Device, Disables.<br>Default setting is **BIOS Build-In**. |
| NVMe LED Control | Enable/Disable allow user control NVMe LED. It only available the NVMe device direct connect to CPU. Default setting is **Disable**. |

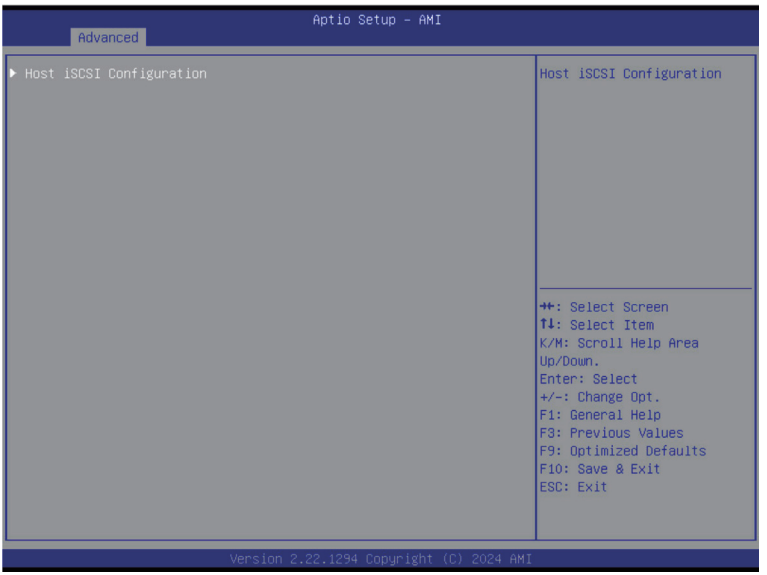
(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

## 5-2-11 Tls Auth Configuration




| Parameter | Description |
|---|---|
| Server CA Configuration | Press [Enter] for configuration of advanced items.<br>◆ Enroll Cert<br>– Press [Enter] to enroll a certificate<br>• Enroll Cert Using File<br>• Cert GUID<br>Input digit character in 1111111-2222-3333-4444-1234567890ab format.<br>– Commit Changes and Exit<br>– Discard Changes and Exit<br>◆ Delete Cert |
| Client Cert Configuration | Press [Enter] for configuration of advanced items. |

## 5-2-12 iSCSI Configuration



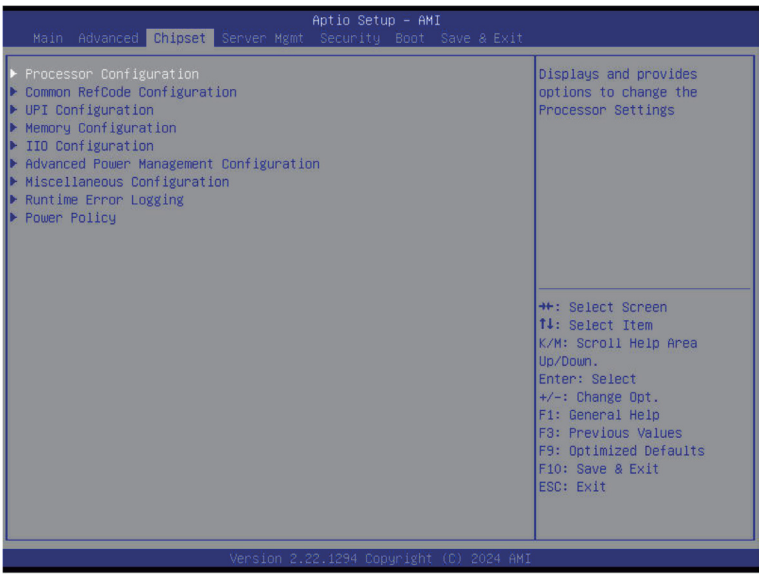

| Parameter | Description |
|---|---|
| Host iSCSI Configuration | Press [Enter] to configure advanced items.<br>◆ iSCSI Initiator Name<br>– Only IQN format is accepted. Range: from 4 to 223<br>◆ Add an Attempt<br>◆ Delete Attempts<br>◆ Change Attempt Order |

## 5-2-13 Driver Health

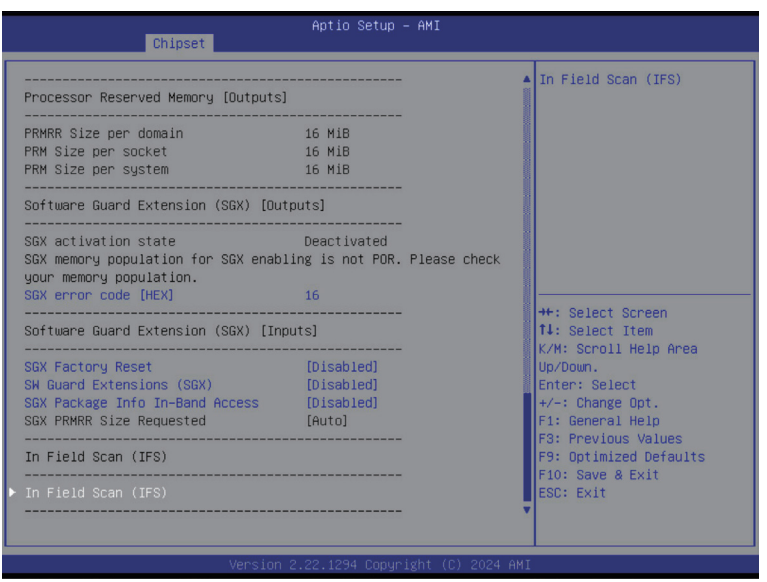

| Parameter | Description |
|---|---|
| Driver Health | Displays driver health status of the devices/controllers if installed |

# 5-3 Chipset Menu

The Chipset Setup menu displays submenu options for configuring the chipset functions. Select a submenu item, then press <Enter> to access the related submenu screen.



## 5-3-1 Processor Configuration

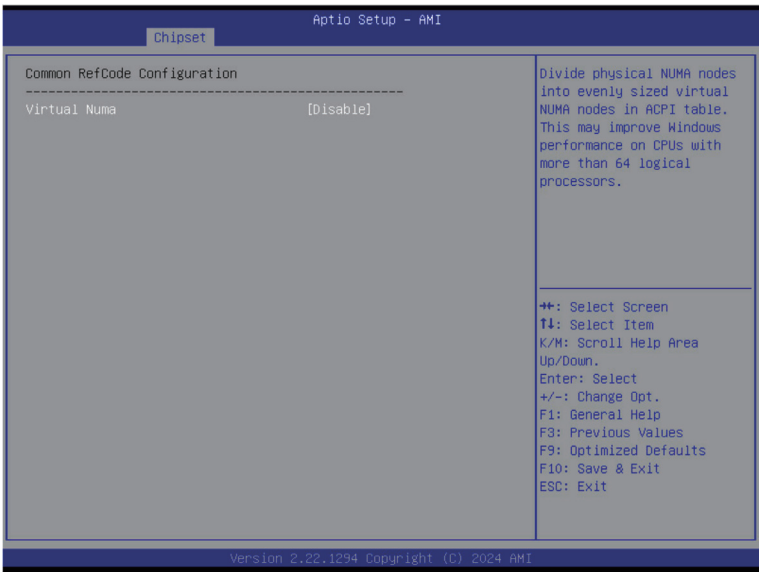



| Parameter | Description |
|---|---|
| Processor Configuration | |
| Pre-Socket Configuration | Press [Enter] to configure advanced items.<br>◆ CPU Socket 0/1 Configuration<br>– Core Disable Bitmap(Hex)<br>• Number of Cores to enable. 0 means all cores. FFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values. |
| Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Package) / L3 Cache RAM(Per Package) / Processor # Version | Displays the technical specifications for the installed processor(s). |
| Hardware Prefetcher | Select whether to enable the speculative prefetch unit of the processor.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| Adjacent Cache Prefetch | When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| DCU Streamer Prefetcher | Enable/Disable DCU streamer prefetcher.<br>Options available: Enable, Disable, Auto. Default setting is **Auto**. |
| DCU IP Prefetcher | Enable/Disable DCU IP Prefetcher.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| L1 Next Page Prefetcher | Next page prefetcher is an L1 data cache page prefetcher (MSR 1A4h [4]). Options available: Enable, Disable. Default setting is **Enable**. |
| Enable Intel(R) TXT | Enable/Disable the Intel Trusted Execution Technology support function.<br>Options available: Enable, Disable. Default setting is **Disable.** |
| VMX | Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| Enable SMX | Enable/Disable the Safer Mode Extensions (SMX) support function.<br>Options available: Enable, Disable. Default setting is **Disable**. |
| AES-NI | Enable/Disable the AES-NI support.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| Debug Consent | Options available: Enable, Disable. Default setting is **Disable**. |
| Memory Encryption (TME) | Enable/Disable memory encryption (TME).<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| Total Memory Encryption Multi-Tenant (TME-MT) | Options available: Enabled, Disabled. Default setting is **Disabled**. |
| Memory integrity | Options available: Enabled, Disabled. Default setting is **Disabled**. |

| Parameter | Description |
|---|---|
| Trust Domain Extension (TDX)(Note) | Options available: Enabled, Disabled. Default setting is **Disabled**. |
| TDX Secure Arbitration Mode Loader (SEAM Loader) | Options available: Enabled, Disabled. Default setting is **Disabled**. |
| TME-MT/TDX Key split | Designate number of bits for TDX usage. The rest will be used by TME-MT. |
| SGX error code [HEX] | Shows hexadecimal SGX internal error code. |
| SGX Factory Reset | Perform SGX Factory Reset, on subsequent boot: delete all registration data, if SGX enabled will force Initial Platform Establishment flow.<br>Options available: Enabled, Disabled. Default setting is **Disabled**. |
| SW Guard Extension (SGX) | Options available: Enabled, Disabled. Default setting is **Disabled**. |
| SGX Package Info In-Band Access | Options available: Enabled, Disabled. Default setting is **Disabled**. |
| SGX PRMRR Size Requested | Default setting is **Auto**. |
| In-Field Scan (IFS) | Press [Enter] to configure advanced items.<br>◆ Enable SAF(Note)<br>– Options available: Disabled, Enabled.<br>– Default setting is **Disabled**.<br>◆ SAF PRMRR Size Requested<br>– Default setting is **8M**. |

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

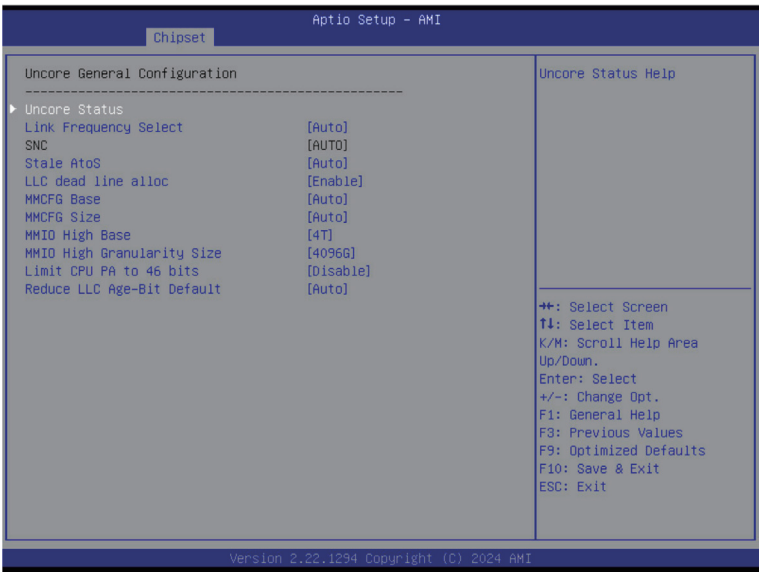
## 5-3-2 Common RefCode Configuration




| Parameter | Description |
|---|---|
| Common RefCode Configuration | |
| Virtual Numa(note) | 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 **Disable**. |
| Number of Virtual Numa Nodes(note) | The number of virtual NUMA nodes per physical NUMA nodes. 0 means automatically set the number of virtual NUMA nodes base on system configuration. 1 equals disabling virtual NUMA. |

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

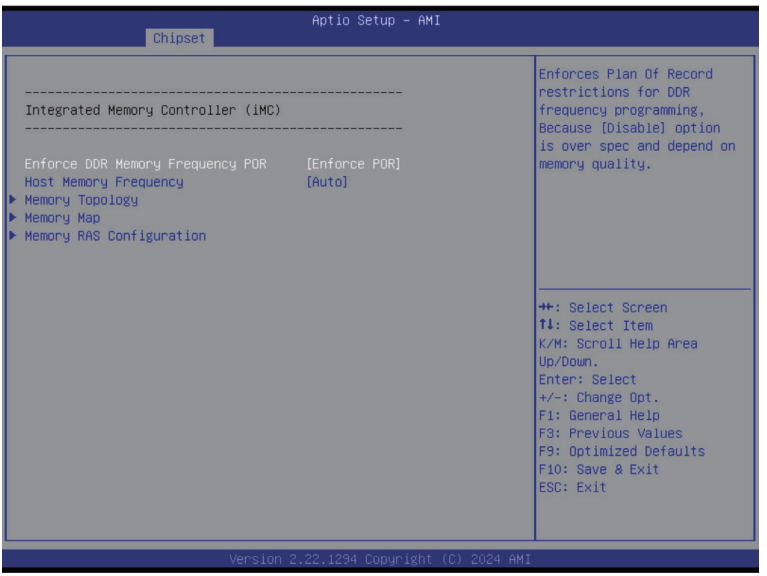
## 5-3-3 UPI Configuration




| Parameter | Description |
|---|---|
| UPI General Configuration | Press [Enter] to configure advanced items.<br>◆ Uncore Status<br>– Press [Enter] to view the Uncore status.<br>◆ Link Frequency Select<br>– Selects the UPI link frequency.<br>– Options available: 16.0GT/s, 20.0GT/s, 24.0GT/s, Auto, Use Per Link Setting. Default setting is **Auto**.<br>◆ SNC<br>– Default setting is **Auto**.<br>◆ Stale AtoS<br>– Enable/Disable Stale A to S directory optimization.<br>– Options available: Disable, Enable, Auto. Default setting is **Auto**.<br>◆ LLC dead line alloc<br>– Enable/Disable fill dead lines in LLC.<br>– Options available: Disable, Enable, Auto. Default setting is **Enable**.<br>◆ MMCFG Base<br>– Options available: 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, Auto.<br>– Default setting is **Auto**.<br>◆ MMCFG Size<br>– Options available: 64M, 128M, 256M, 512M, 1G, 2G, Auto .<br>– Default setting is **Auto**. |

| Parameter | Description |
| --- | --- |
| UPI General Configuration | ◆ MMIO High Base<br>– Options available: 248T, 120T, 88T, 60T, 30T, 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, Auto. Default setting is **4T**.<br>◆ MMIO High Granularity Size<br>– Selects the allocation size used to assign mmioh resources.<br>– Options available: 1G, 4G, 16G, 32G, 64G, 256G, 1024G, 4096G, Auto. Default setting is **4096G**.<br>◆ Limit CPU PA to 46 bits<br>– Options available: Disable, Enable, Auto. Default setting is **Disable**.<br>◆ Reduce LLC Age-Bit Default<br>– Options available: Disable, Enable, Auto. Default setting is **Auto**. |

## 5-3-4 Memory Configuration



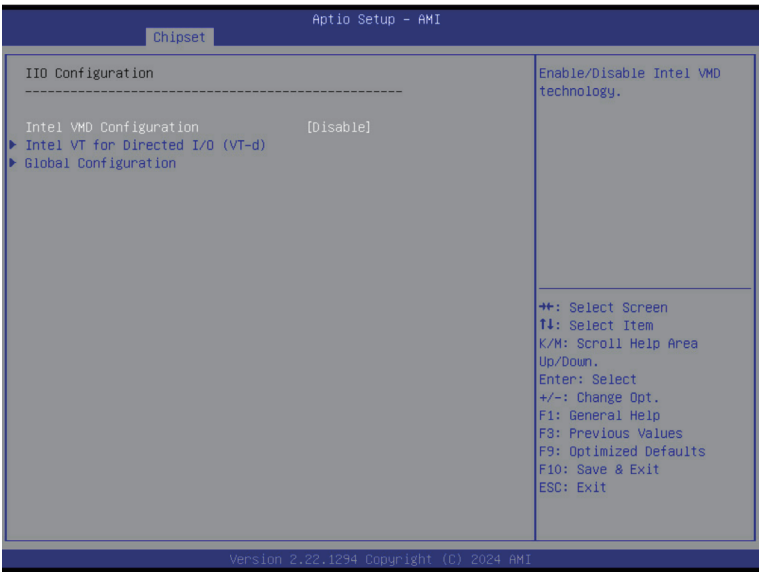

| Parameter | Description |
|---|---|
| Integrated Memory Controller (iMC) | |
| Enforce DDR Memory Frequency POR | When set to Enable, the system enforces Plan Of Record restrictions for DDR frequency programming.<br>Options available: Enforce POR, Enforce Stretch Goals, Disable.<br>Default setting is **Enforce POR**. |
| Host Memory Frequency | Maximum Host DDR Memory Frequency Selections in MT/s.<br>If the AUTO option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD.<br>Options available: Auto, 4800, 5200, 5600, 6000, 6400. Default setting is **Auto**. |
| Memory Topology | Press [Enter] to view memory topology with DIMM population information. |
| Memory Map | Press [Enter] to configure advanced items.<br>◆ Intel(R) Flat Memory Mode Support.<br>– Options available: Enabled, Disabled. Default setting is **Disabled**.<br>◆ DDR CXL Heterogeneous Interleave support.<br>– Options available: Enabled, Disabled. Default setting is **Disabled**. |

| Parameter | Description |
|---|---|
| Memory RAS Configuration | Press [Enter] to configure advanced items.<br>◆ Mirror Mode<br>– 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.<br>– Options available: Disabled, Full Mirror Mode. Default setting is **Disabled**.<br>◆ Correctable Error Threshold<br>– Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket.<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ Leaky bucket time window based interface(Note)<br>– Enable/Disable leaky bucket time window based interface.<br>– Options available: Disabled, Enabled. Default setting is **Disabled**.<br>◆ Leaky bucket time window based interface Hour<br>– Leaky bucket time window based interface hour used for DDR (0-24).<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ Leaky bucket time window based interface Minute<br>– Leaky bucket time window based interface minute used for DDR (0-60).<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ Leaky bucket low bit<br>– Configures leaky bucket low bit (0x1 - 0x29).<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ Leaky bucket high bit<br>– Configures leaky bucket high bit (0x1 - 0x29).<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ ADDDC Sparing(Note)<br>– Enable/Disable ADDDC Sparing.<br>– Options available: Disabled, Enabled. Default setting is **Disabled**.<br>◆ Enable ADDDC Error Injection<br>– Options available: Disabled, Enabled. Default setting is **Enabled**. |

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

| Parameter | Description |
| --- | --- |
| Memory RAS Configuration (continued) | ◆ Patrol Scrub Interval<br>– Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto.<br>◆ DDR5 ECS<br>– Options available: Disabled, Enabled, Enable ECS with Result Collection. Default setting is **Enabled**. |

## 5-3-5 IIO Configuration



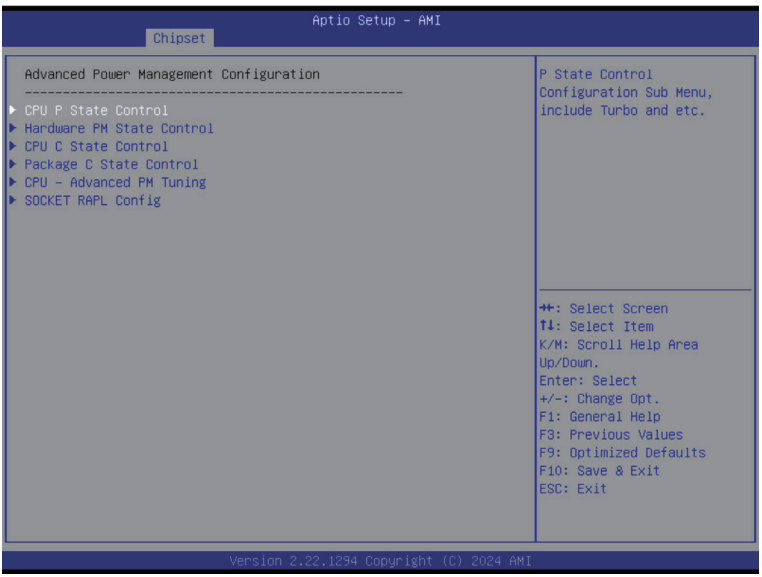

| Parameter | Description |
|---|---|
| IIO Configuration | |
| Intel VMD Configuration | Enable/Disable Intel VMD technology.<br>Options available: Enable, Disable. Default setting is **Disable**. |
| Intel VT for Directed I/O (VT-d) | Press [Enter] to configure advanced items.<br>◆ DMA Control Opt-In Flag<br>– Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).<br>– Options available: Enable, Disable. Default setting is **Enable**.<br>◆ Pre-boot DMA Protection<br>– Options available: Enable, Disable. Default setting is **Eable**.<br>◆ PCIe ACSCTL<br>– Options available: Enable, Disable. Default setting is **Disable**.<br>◆ Source Validation(Note)<br>– Options available: Disabled, Enabled. Default setting is **Disabled**.<br>◆ Translation Blocking(Note)<br>– Options available: Disabled, Enabled. Default setting is **Disabled**.<br>◆ P2P Request Redirect(Note)<br>– Options available: Disabled, Enabled. Default setting is **Enabled**.<br>◆ P2P Completion Redirect(Note)<br>– Options available: Disabled, Enabled. Default setting is **Enabled**. |

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

| Parameter | Description |
|---|---|
| Intel VT for Directed I/O (VT-d) | ◆ Upstream Forwarding Enable(Note)<br>– Options available: Disabled, Enabled. Default setting is **Enabled**.<br>◆ Cache Allocation<br>– Options available: Enable, Disable. Default setting is **Enable**. |
| Global Configuration | Press [Enter] to configure advanced items.<br>◆ Max Read Request Size<br>– Options available: Auto, 128B, 256B, 512B, 1024B, 2048B, 4096B. Default setting is **Auto**.<br>◆ Relaxed Ordering<br>– Options available: Enable, Disable. Default setting is **Enable**. |

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

## 5-3-6 Advanced Power Management Configuration

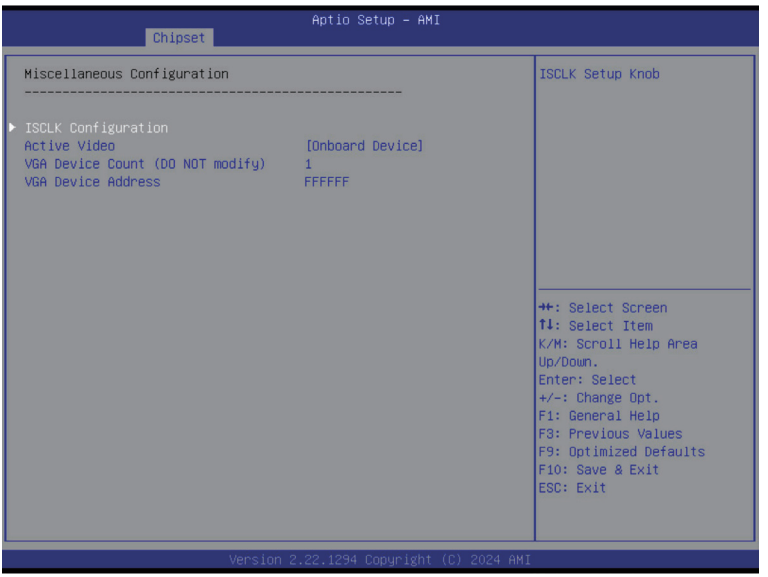



| Parameter | Description |
|---|---|
| CPU P State Control | Press [Enter] to configure advanced items.<br>◆ Intel SST-PP<br>– Intel SST-PP Select allows user to choose level.<br>– Options available: Auto, Level 0, Level 1. Default setting is **Auto**.<br>◆ SpeedStep (Pstates)<br>– Conventional Intel 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 **Enable**.<br>◆ EIST PSD Function<br>– Options available: HW_ALL, SW_ALL. Default setting is **HW_ALL**.<br>◆ Boot performance mode<br>– Select the performance state that the BIOS will set before OS hand off.<br>– Options available: Max Performance, Max Efficiency. Default setting is **Max Performance**.<br>◆ Turbo Mode<br>– 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.<br>– Options available: Enable, Disable. Default setting is **Enable**. |

| Parameter | Description |
|---|---|
| Hardware PM State Control | Press [Enter] to configure advanced items.<br>◆ Hardware P-State<br>– Options available: Disable, Native mode, Out of Band mode, Native Mode with No Legacy Support. Default setting is **Native Mode**.<br>◆ HardwarePM Interrupt<br>– Options available: Disable, Enable. Default setting is **Disable**. |
| CPU C State Control | Press [Enter] to configure advanced items.<br>◆ Monitor MWAIT<br>– Options available: Disable, Enable. Default setting is **Enable**.<br>◆ ACPI C1 Enumeration<br>– Options available: C1, C1e . Default setting is **C1e**.<br>◆ ACPI C6x Enumeration<br>– Options available: Dsiable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto. Default setting is **Auto**. |
| Package C State Control | Press [Enter] to configure advanced items.<br>◆ Package C State<br>– Configures the state for the C-State package limit.<br>– Options available: C0/C1 state, C2 state, C6(non Retention) state, No Limit, Auto. Default setting is **Auto**. |
| CPU - Advanced PM Tuning | Press [Enter] to configure advanced items.<br>◆ Uncore Freq Ratio<br>– Default is **0**.<br>◆ Energy Perf BIAS<br>– Press [Enter] to configure advanced items.<br>» Power Performance Tuning<br>• Options available: OS Controls EPB, BIOS Controls EPB, PECI Controls EPB. Default setting is **OS Controls EPB**.<br>» Energy_PERF_BIAS_CFG mode(Note)<br>• Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is **Balanced Performance**. |
| SOCKET RAPL Config | Press [Enter] to configure advanced items.<br>◆ PL1 Power Limit<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ PL1 Time Window<br>• Default setting is **1**.<br>◆ PL2 Power Limit<br>– Press the <+> / <-> keys to increase or decrease the desired values.<br>◆ PL2 Time Window<br>• Default setting is **1**. |

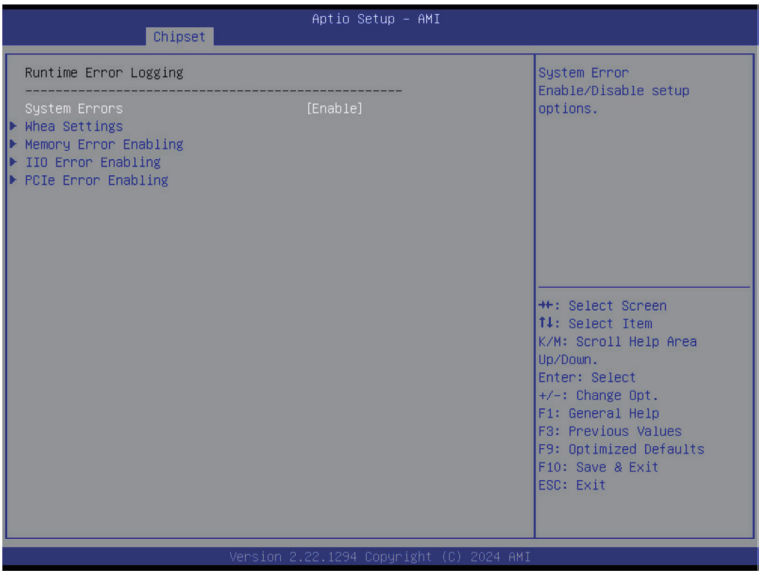
(Note) This item is configurable when **Power Performance Tuning** is set to **BIOS Controls EPB**.

## 5-3-7 Miscellaneous Configuration




| Parameter | Description |
|---|---|
| Miscellaneous Configuration | |
| ISCLK Configuration | Press [Enter] to configure advanced items.<br>◆ SSC1 Enable<br>– Options available: Enable, Disable. Default setting is **Enable**.<br>◆ SSC2 Enable<br>– Options available: Enable, Disable. Default setting is **Enable**. |
| Active Video | Selects the active video type.<br>Options available: Auto, Onboard Device, PCIE Device, Specific PCIE Device. Default setting is **Auto**. |
| VGA Device Count (DO NOT modify) | Default setting is **1**. |
| VGA Device Address | VGA Device Address |

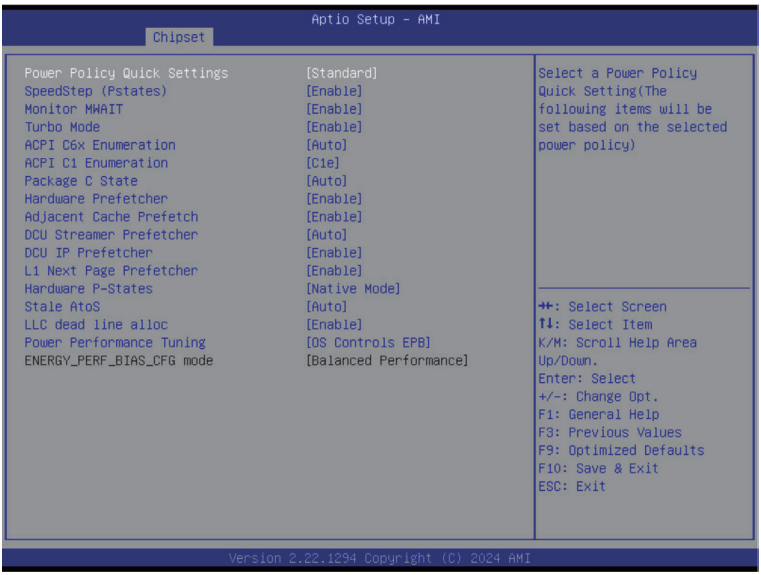
## 5-3-8 Runtime Error Logging Settings




| Parameter | Description |
|---|---|
| Runtime Error Logging | |
| System Errors | Enable/Disable system error logging function.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| Whea Settings | Press [Enter] to configure advanced items.<br>◆ WHEA (Windows Hardware Error Architecture) Support<br>– Enable/Disable WHEA Support.<br>– Options available: Enable, Disable. Default setting is **Enable**. |
| Memory Error Enabling | Press [Enter] to configure advanced items.<br>◆ Memory Corrected Error<br>– Enable/Disable Memory Corrected Error.<br>– Options available: Enable, Disable. Default setting is **Enable**.<br>◆ Uncorrected Error disable Memory<br>– Enable/Disable the Memory that triggers Uncorrected Error.<br>– Options available: Enable, Disable. Default setting is **Disable**. |
| IIO Error Enabling | Press [Enter] to configure advanced items.<br>◆ OS Native AER Support<br>– Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.<br>– Options available: Enable, Disable. Default setting is **Disable**. |

| Parameter | Description |
|---|---|
| PCIe Error Enabling | Press [Enter] to configure advanced items.<br>◆ Corrected Error<br>– Enables and escalates correctable Errors to error pins.<br>– Options available: Enable, Disable. Default setting is **Disable**.<br>◆ Uncorrected Error<br>– Enables and escalates Uncorrectable/Recoverable Errors to error pins.<br>– Options available: Enable, Disable. Default setting is **Enable**.<br>◆ Fatal Error Enable<br>– Enables and escalates Fatal Errors to error pins.<br>– Options available: Enable, Disable. Default setting is **Enable**.<br>◆ Assert NMI on SERR<br>– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs.<br>– Options available: Enabled, Disabled. Default setting is **Enabled**.<br>◆ Assert NMI on PERR<br>– Enable/Disable BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs.<br>– Options available: Enabled, Disabled. Default setting is **Enabled**. |

## 5-3-9 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 **Standard**. |
| 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 **Enable**. |
| Monitor MWAIT | Allows Monitor and MWAIT instructions.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| 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. When this item is disabled, the processor will not overclock any of its core.<br>Options available: Enable, Disable. Default setting is **Enable**. |
| ACPI C6x Enumeration | Options available: Disable,C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, Auto. Default setting is **Auto**. |
| ACPI C1 Enumeration | Options available: C1, C1e. Default setting is **C1e**. |
| Package C State | Configures the C-State package limit.<br>Options available: C0/C1 state, C2 state, C6(non Retention) state, No Limit, Auto. Default setting is **Auto**. |

| Parameter | Description |
|---|---|
| Hardware Prefetcher | Options available: Enable, Disable. Default setting is **Enable**. |
| Adjacent Cache Prefetch | Options available: Enable, Disable. Default setting is **Enable**. |
| DCU Streamer Prefetcher | Options available: Enable, Disable, Auto. Default setting is **Auto**. |
| DCU IP Prefetcher | Options available: Enable, Disable. Default setting is **Enable**. |
| L1 Next page Prefetcher | Options available: Enable, Disable. Default setting is **Enable**. |
| Hardware P-States | Options available: Disable, Native mode, Out of Band mode, Native Mode with No Legacy Support. Default setting is **Native Mode**. |
| Stale AtoS | Options available: Auto, Enable, Disable. Default setting is **Auto**. |
| LLC dead line alloc | Options available: Auto, Enable, Disable. Default setting is **Enable**. |
| Power Performance Tuning | Options available: OS Controls EPB, BIOS Controls EPB, PECI Controls EPB. Default setting is **OS Controls EPB**. |
| ENERGY_PERF_BIAS_CFG mode | Default setting is **Balanced Performance**. |

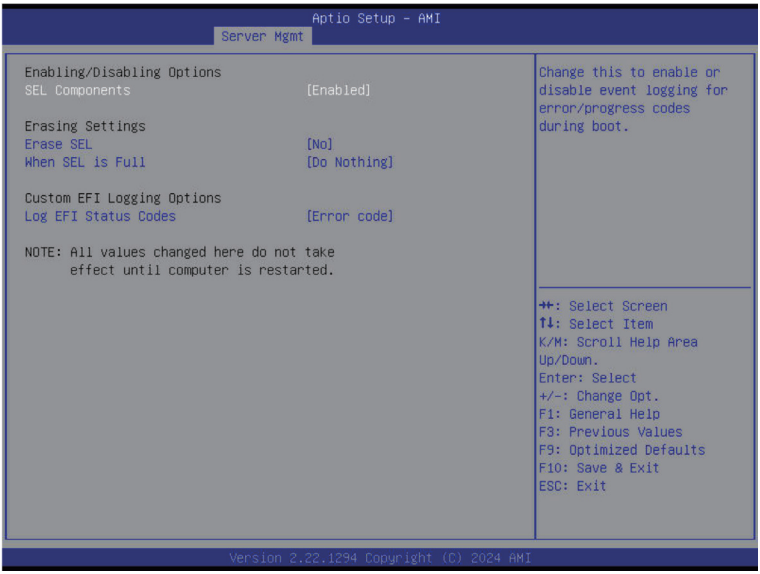
## 5-4 Server Management Menu


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

(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**.

| Parameter | Description |
|---|---|
| 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. |

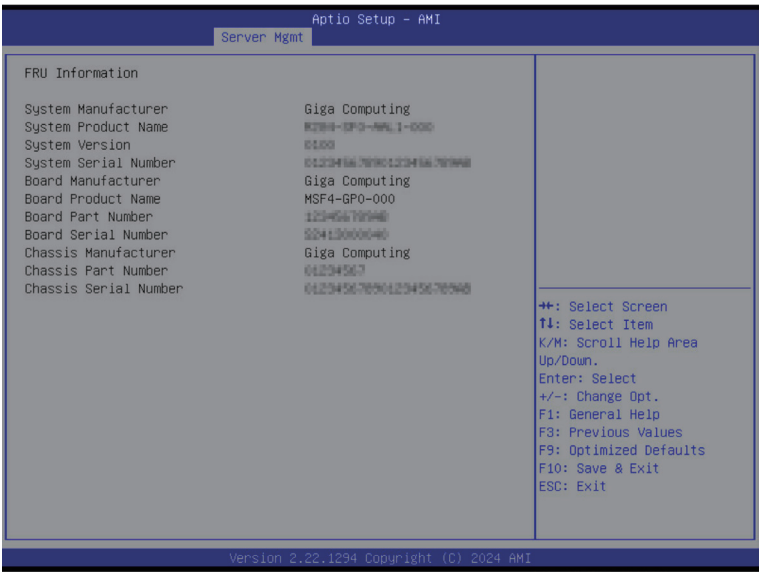
## 5-4-1 System Event Log




| 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 **Enabled**. |
| Erasing Settings | |
| Erase SEL | Choose options for erasing SEL.<br>Options available: No,<br>Yes, On next reset,<br>Yes, On every reset.<br>Default setting is **No**. |
| 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 **Do Nothing**. |
| 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 **Error code**. |

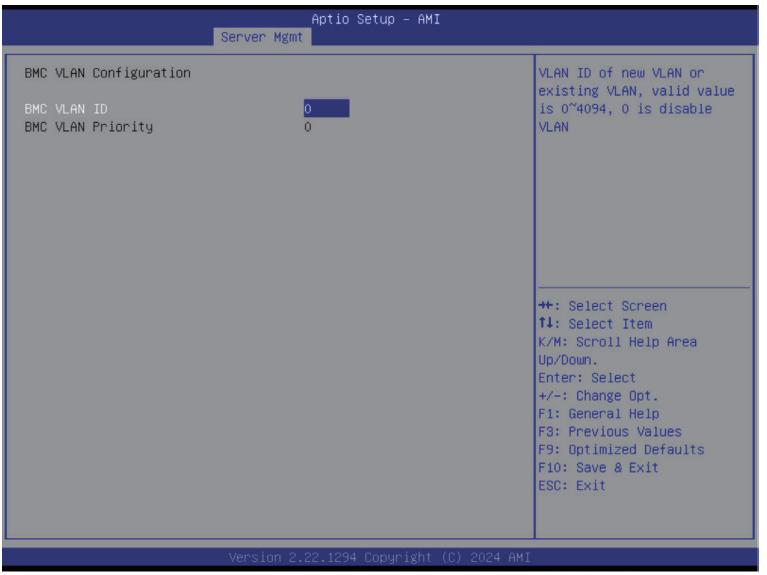
## 5-4-2 View FRU Information

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

## 5-4-3 BMC VLAN Configuration

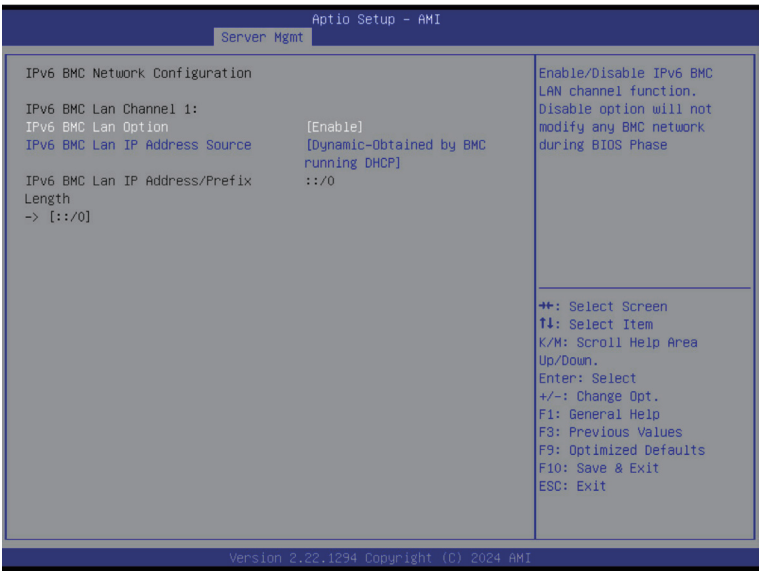



| Parameter | Description |
|---|---|
| BMC VLAN Configuration | |
| BMC VLAN ID | Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled. |
| BMC VLAN Priority | Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN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

## 5-4-4 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 **Do Nothing**. |
| 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 **DynamicBmcDhcp**. |
| 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. |

## 5-4-5 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 **Enable**. |
| 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 **Dynamic-Obtained by BMC running DHCP**. |
| IPv6 BMC Lan IP Address/ Prefix Length | Check if the IPv6 BMC LAN IP address matches those displayed on the screen. |

## 5-5 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

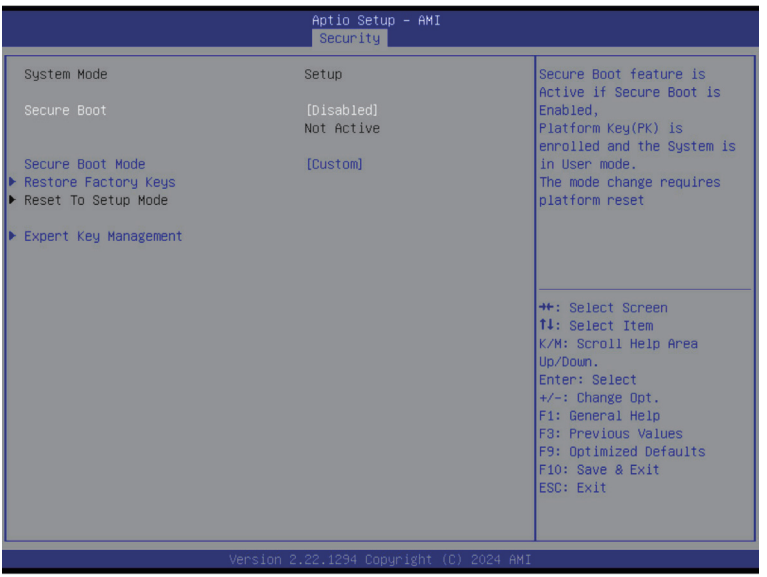
  Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

| 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. |
| Secure Flash Update | Press [Enter] to view the firmware update information. |

## 5-5-1 Secure Boot

The Secure Boot feature is applicable if supported by your Operating System.

If your Operating System is not supporting Secure Boot, the system will hang when starting the 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 **Disabled**. |
| Secure Boot Mode(Note) | 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 the Operating System 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 **Standard**. |
| 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. |

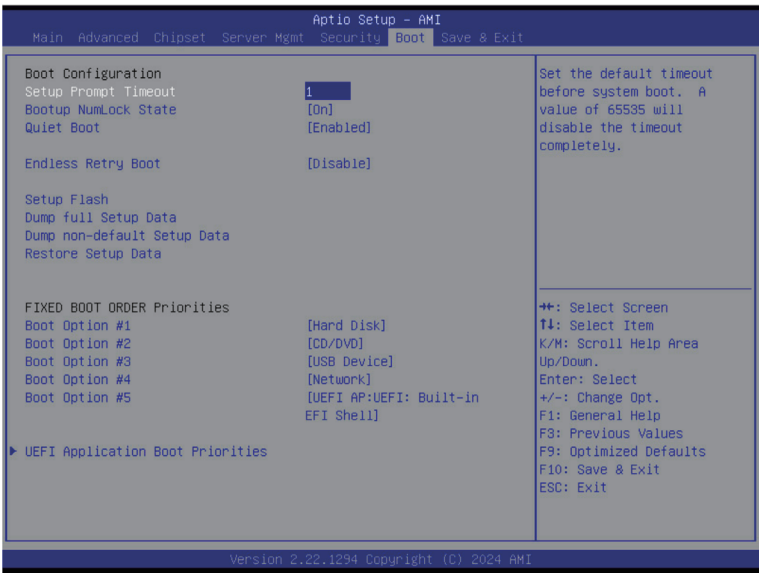
(Note) Advanced items prompt when this item is set to **Custom**.

| Parameter | Description |
|---|---|
| Key Management | Press [Enter] to configure advanced items.<br>**Please note that this item is configurable when Secure Boot Mode is set to Custom.**<br>◆ Factory Key Provision<br>– Allows to provision factory default Secure Boot keys when system is in Setup Mode.<br>– Options available: Enabled, Disabled. Default setting is **Disabled**.<br>◆ Restore Factory Keys<br>– Installs all factory default keys. It will force the system in User Mode.<br>– Options available: Yes, No.<br>◆ Reset To Setup Mode<br>– Reset the system to Setup Mode.<br>– Options available: Yes, No.<br>◆ Enroll Efi Image<br>– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).<br>◆ Export Secure Boot variables<br>– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.<br>◆ Secure Boot variable<br>– Displays the current status of the variables used for secure boot.<br>◆ Platform Key (PK)<br>– Displays the current status of the Platform Key (PK).<br>– Press [Enter] to configure a new PK.<br>– Options available: Update.<br>◆ Key Exchange Keys (KEK)<br>– Displays the current status of the Key Exchange Key Database (KEK).<br>– Press [Enter] to configure a new KEK or load additional KEK from storage devices.<br>– Options available: Update, Append.<br>◆ Authorized Signatures (DB)<br>– Displays the current status of the Authorized Signature Database.<br>– Press [Enter] to configure a new DB or load additional DB from storage devices.<br>– Options available: Update, Append.<br>◆ Forbidden Signatures (DBX)<br>– Displays the current status of the Forbidden Signature Database.<br>– Press [Enter] to configure a new dbx or load additional dbx from storage devices.<br>– Options available: Update, Append. |

| Parameter | Description |
| --- | --- |
| Key Management (continued) | ◆ Authorized TimeStamps (DBT)<br>– Displays the current status of the Authorized TimeStamps Database.<br>– Press [Enter] to configure a new DBT or load additional DBT from storage devices.<br>– Options available: Update, Append.<br>◆ OsRecovery Signatures<br>– Displays the current status of the OsRecovery Signature Database.<br>– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.<br>– Options available: Update, Append. |

## 5-6 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.

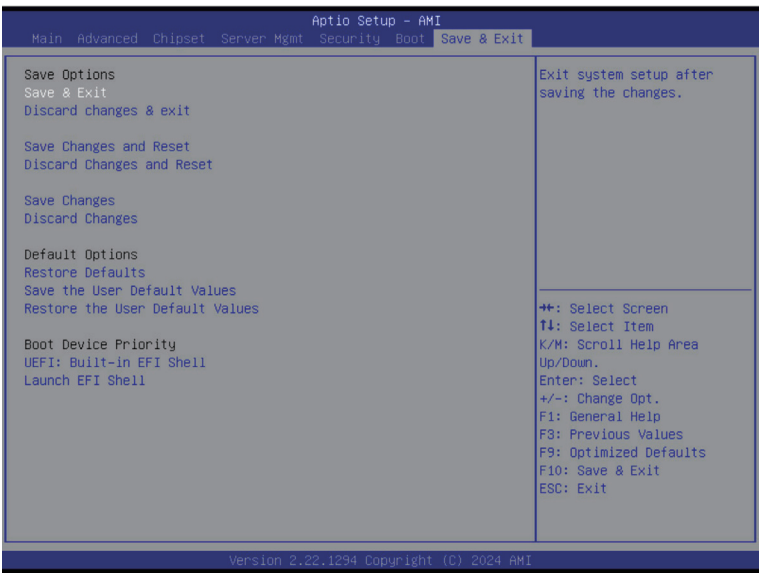



| Parameter | Description |
|---|---|
| Boot Configuration | |
| Setup Prompt Timeout | Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.<br>Press the numeric keys to input the desired values. |
| Bootup NumLock State | Enable/Disable the Bootup NumLock function.<br>Options available: On, Off. Default setting is **On**. |
| Quiet Boot | Enable/Disable showing the logo during POST.<br>Options available: Enabled, Disabled. Default setting is **Enabled**. |
| Endless Retry Boot | Options available: Disable, Enable. Default setting is **Disable**. |
| 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. |

| Parameter | Description |
|---|---|
| FIXED BOOT ORDER Priorities | |
| Boot Option #1 / #2 / #3 / #4 / #5 | Press [Enter] to configure the boot order priority.<br>By default, the server searches for boot devices in the following sequence:<br>1. Hard drive.<br>2. CD-COM/DVD drive.<br>3. USB device.<br>4. Network.<br>5. UEFI. |
| UEFI Application Boot Priorities | Press [Enter] to configure the boot priority. |

## 5-7 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 | |

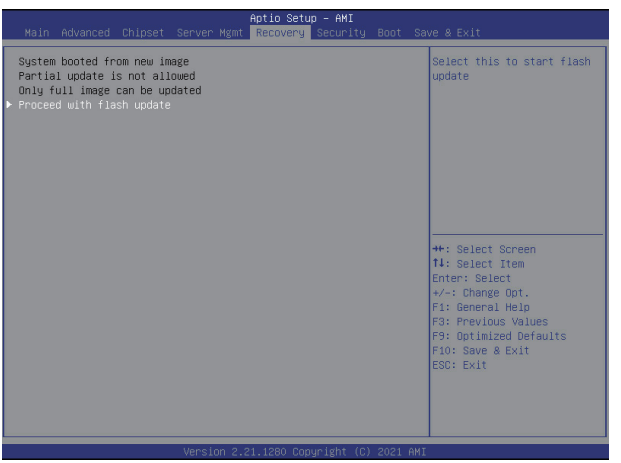
| Parameter | Description |
|---|---|
| Restore Defaults | Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these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

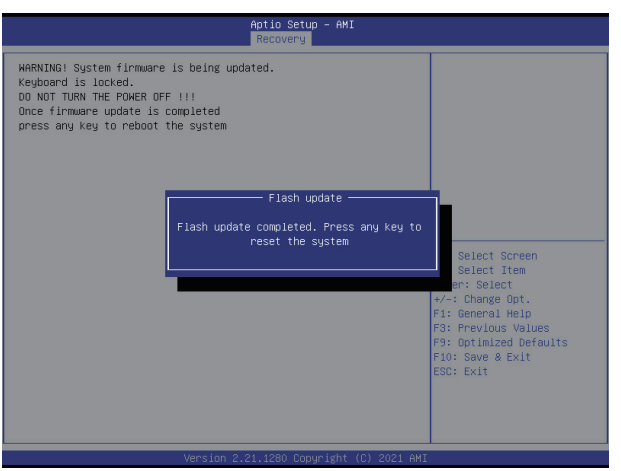
## 5-8 BIOS Recovery

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.



## 5-9 BIOS POST Beep code (AMI standard)

### 5-9-1 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 | DXEIPL was not found |
| 3 | DXE Core Firmware Volume was not found |
| 4 | Recovery failed |
| 4 | S3 Resume failed |
| 7 | Reset PPI is not available |

### 5-9-2 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 |