

# **GIGABYTE™**

# **R162-ZA0**

AMD EPYC™ 7002 Server System - 1U 4-Bay

## **User Manual**

Rev. 1.0

## **Copyright**

© 2020 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.

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

## **Disclaimer**

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

## **Documentation Classifications**

In order to assist in the use of this product, GIGABYTE 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>




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](mailto:server.grp@gigabyte.com)

## Conventions

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

|   |   |
|---|---|
|  | <b>NOTE!</b><br>Gives bits and pieces of additional information related to the current topic.           |
|  | <b>CAUTION!</b><br>Gives precautionary measures to avoid possible hardware or software problems.        |
|  | <b>WARNING!</b><br>Alerts you to any damage that might 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.**



### **WARNING!**

**This equipment is not suitable for use in locations where children are likely to be present.**



### **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 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 any component and pin touching. 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.

**System power on/off:** To remove power from system, you must remove the system from rack. 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 and disconnect the cables attached to the system before servicing it. 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 sensitive 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 fingertips 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 damage the contacts inside the jumper, causing intermittent problems with the function controlled 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.

**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.

# Table of Contents

|  |    |
|--|----|
| Chapter 1 Hardware Installation .....          | 11 |
| 1-1 Installation Precautions .....             | 11 |
| 1-2 Product Specifications .....               | 12 |
| 1-3 System Block Diagram .....                 | 16 |
| Chapter 2 System Appearance .....              | 17 |
| 2-1 Front View .....                           | 17 |
| 2-2 Rear View .....                            | 18 |
| 2-3 Front Panel LEDs and Buttons .....         | 19 |
| 2-4 RoT LEDs .....                             | 20 |
| 2-5 Rear System LAN LEDs .....                 | 22 |
| 2-6 Power Supply Unit LED .....                | 23 |
| 2-7 Hard Disk Drive LEDs .....                 | 24 |
| Chapter 3 System Hardware Installation .....   | 25 |
| 3-1 Removing Chassis Cover .....               | 26 |
| 3-2 Removing and Installing the Fan Duct ..... | 27 |
| 3-3 Removing the Heat Sink .....               | 28 |
| 3-4 Installing the CPU .....                   | 29 |
| 3-5 Installing the Memory .....                | 31 |
| 3-5-1 Eight Channel Memory Configuration ..... | 31 |
| 3-5-2 Installing a Memory .....                | 32 |
| 3-5-3 DIMM Population Table .....              | 32 |
| 3-6 Installing the PCI Expansion Card .....    | 34 |
| 3-7 Installing the Mezzanine Card .....        | 35 |
| 3-7-1 OCP 3.0 .....                            | 35 |
| 3-7-2 OCP 2.0 .....                            | 36 |
| 3-8 Installing the Hard Disk Drive .....       | 37 |
| 3-9 Replacing the Fan Assembly .....           | 38 |
| 3-10 Replacing the Power Supply .....          | 39 |
| 3-11 Cable Routing .....                       | 40 |
| Chapter 4 Motherboard Components .....         | 45 |
| 4-1 Motherboard Components .....               | 45 |
| 4-2 Jumper Settings .....                      | 47 |
| Chapter 5 BIOS Setup .....                     | 49 |
| 5-1 The Main Menu .....                        | 51 |

|        |  |     |
|--------|--|-----|
| 5-2    | Advanced Menu .....                            | 53  |
| 5-2-1  | Trusted Computing .....                        | 55  |
| 5-2-2  | PSP Firmware Versions.....                     | 56  |
| 5-2-3  | Legacy Video Select.....                       | 57  |
| 5-2-4  | AST2500 Super IO Configuration.....            | 58  |
| 5-2-5  | S5 RTC Wake Settings.....                      | 61  |
| 5-2-6  | Serial Port Console Redirection .....          | 62  |
| 5-2-7  | CPU Configuration.....                         | 66  |
| 5-2-8  | AMI Graphic Output Protocol Policy.....        | 67  |
| 5-2-9  | PCI Subsystem Settings.....                    | 68  |
| 5-2-10 | USB Configuration.....                         | 70  |
| 5-2-11 | NVMe Configuration .....                       | 72  |
| 5-2-12 | SATA Configuration.....                        | 73  |
| 5-2-13 | UEFI Configuration.....                        | 74  |
| 5-2-14 | Network Stack Configuration .....              | 75  |
| 5-2-15 | AMD Mem Configuration Status .....             | 76  |
| 5-2-16 | iSCSI Configuration .....                      | 77  |
| 5-2-17 | Tls Auth Configuration .....                   | 78  |
| 5-2-18 | Intel(R) I350 Gigabit Network Connection ..... | 79  |
| 5-2-19 | VLAN Configuration.....                        | 81  |
| 5-2-20 | MAC IPv4 Network Configuration.....            | 83  |
| 5-2-21 | MAC IPv6 Network Configuration.....            | 84  |
| 5-3    | AMD CBS Menu.....                              | 86  |
| 5-3-1  | CPU Common Options .....                       | 87  |
| 5-3-2  | DF Common Options.....                         | 92  |
| 5-3-3  | UMC Common Options .....                       | 97  |
| 5-3-4  | NBIO Common Options.....                       | 110 |
| 5-3-5  | FCH Common Options .....                       | 116 |
| 5-3-6  | NTB Common Options .....                       | 119 |
| 5-3-7  | SOC Miscellaneous Control .....                | 120 |
| 5-4    | AMD PBS Menu .....                             | 121 |
| 5-4-1  | RAS .....                                      | 122 |
| 5-5    | Chipset Setup Menu.....                        | 124 |
| 5-5-1  | North Bridge .....                             | 125 |
| 5-6    | Server Management Menu.....                    | 126 |
| 5-6-1  | System Event Log .....                         | 128 |
| 5-6-2  | View FRU Information .....                     | 129 |
| 5-6-3  | BMC Network Configuration .....                | 130 |
| 5-6-4  | IPv6 BMC Network Configuration .....           | 131 |
| 5-7    | Security Menu .....                            | 132 |
| 5-7-1  | Secure Boot .....                              | 133 |



|         |  |     |
|---------|--|-----|
| 5-8     | Boot Menu.....                                       | 135 |
| 5-8-1   | UEFI NETWORK Drive BBS Priorities .....              | 137 |
| 5-8-2   | UEFI Application Boot Priorities .....               | 138 |
| 5-9     | Save & Exit Menu.....                                | 139 |
| 5-10    | ABL POST Codes .....                                 | 140 |
| 5-10-1  | StartProcessorTestPoints .....                       | 140 |
| 5-10-2  | Memory test points .....                             | 140 |
| 5-10-3  | PMU Test Points .....                                | 140 |
| 5-10-4  | Original Post Code .....                             | 141 |
| 5-10-5  | CPU test points.....                                 | 142 |
| 5-10-6  | Topology test points.....                            | 142 |
| 5-10-7  | Extended memory test point.....                      | 142 |
| 5-10-8  | Gnb Earlier init.....                                | 143 |
| 5-10-9  | PMU test points .....                                | 146 |
| 5-10-10 | ABL0 test points .....                               | 146 |
| 5-10-11 | ABL5 test points .....                               | 146 |
| 5-11    | Agesa POST Codes.....                                | 150 |
| 5-11-1  | Universal Post Code.....                             | 150 |
| 5-11-2  | [0xA1XX] For CZ only memory Postcodes.....           | 150 |
| 5-11-3  | S3 Interface Post Code .....                         | 153 |
| 5-11-4  | PMU Post Code.....                                   | 153 |
| 5-11-5  | [0xA5XX] assigned for AGESA PSP Module.....          | 153 |
| 5-11-6  | [0xA9XX, 0xAAXX] assigned for AGESA NBIO Module..... | 156 |
| 5-11-7  | [0xACXX] assigned for AGESA CCX Module .....         | 158 |
| 5-11-8  | [0xADXX] assigned for AGESA DF Module.....           | 159 |
| 5-11-9  | [0xAFXX] assigned for AGESA FCH Module.....          | 159 |
| 5-12    | BIOS POST Beep code (AMI standard).....              | 161 |
| 5-12-1  | PEI Beep Codes .....                                 | 161 |
| 5-12-2  | DXE Beep Codes .....                                 | 161 |

This page intentionally left blank








# 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

|   |                                      |  |
|---|--------------------------------------|--|
|  | System Dimension                     | <ul style="list-style-type: none"> <li>◆ 1U</li> <li>◆ 438 (W) x 43.5 (H) x 730 (D) mm</li> </ul>  |
|  | CPU                                  | <ul style="list-style-type: none"> <li>◆ AMD EPYC™ 7002 series processor family</li> <li>◆ Single processor, 7nm technology</li> <li>◆ Up to 64-core, 128 threads per processor</li> <li>◆ TDP up to 225W, cTDP up to 240W</li> <br/> <li>◆ Compatible with AMD EPYC™ 7001 series processor family</li> </ul>  |
|  | Chipset                              | <ul style="list-style-type: none"> <li>◆ System on Chip</li> </ul>   |
|  | Hardware-Level Root of Trust Support | <ul style="list-style-type: none"> <li>◆ Supported</li> </ul> <p><b>NOTE! The system will take extra time to boot as it goes through RoT authentication.</b></p>   |
|  | Memory                               | <ul style="list-style-type: none"> <li>◆ 16 x DIMM slots</li> <li>◆ DDR4 memory supported only</li> <li>◆ 8-Channel memory architecture</li> <li>◆ RDIMM modules up to 128GB supported</li> <li>◆ LRDIMM modules up to 128GB supported</li> <li>◆ Memory speed: Up to 3200*/ 2933 MHz</li> <br/> <li>Note: <ul style="list-style-type: none"> <li>◆ * Follow BIOS setting and memory QVL list if running 3200 Mhz with 2DPC</li> </ul> </li> </ul> |
|  | LAN                                  | <ul style="list-style-type: none"> <li>◆ 2 x 1GbE LAN ports (1 x Intel® I350-AM2)</li> <li>◆ 1 x 10/100/1000 management LAN</li> </ul>   |
|  | Video                                | <ul style="list-style-type: none"> <li>◆ Integrated in Aspeed® AST2500</li> <li>◆ 2D Video Graphic Adapter with PCIe bus interface</li> <li>◆ 1920x1200@60Hz 32bpp</li> </ul>  |



#### Expansion Slot

##### **Riser Card CRS101E:**

- ◆ 1 x PCIe x16 slot (Gen4 x16), Full height half-length

##### **Riser Card CRS101E:**

- ◆ 1 x PCIe x16 slot (Gen4 x8 or x16), shared with OCP 2.0, Full height half-length  
( Please see NOTE below)

##### **Internal Riser Card CRS101H:**

- ◆ 1 x PCIe x16 slot (Gen4 x16), Full height half-length
- ◆ 1 x OCP 3.0 mezzanine slot with PCIe Gen4 x16 bandwidth
- ◆ 1 x OCP 2.0 mezzanine slot with PCIe Gen3 x0 or x8 bandwidth, shared with CRS101E ( Please see NOTE below)

##### NOTE:

1. GIGABYTE offers an optional riser card to support full bandwidth PCIe Gen4 x16 and OCP 2.0 Gen3 x8
2. Contact GIGABYTE sales rep or technical support for more details about supporting full bandwidth



#### Storage

- ◆ 4 x 3.5/ 2.5" SATA/ SAS hot-swappable SSD bays

- ◆ 1 x M.2 slot:
  - M-key
  - PCIe Gen4 x4
  - Supports NGFF-2280/22110 cards






##### NOTE:

SAS card is required for SAS devices support



#### Internal I/O

- ◆ 1 x M.2 slot
- ◆ 1 x USB 3.0 header
- ◆ 1 x COM header
- ◆ 1 x TPM header
- ◆ 1 x OCP 3.0 mezzanine slot
- ◆ 1 x OCP 2.0 mezzanine slot
- ◆ 1 x Front panel header
- ◆ 1 x HDD back plane board header
- ◆ 1 x PMBus connector
- ◆ 1 x IPMB connector
- ◆ 1 x Clear CMOS jumper
- ◆ 1 x BIOS recovery jumper

|   |                   |   |
|---|-------------------|---|
|  | Front I/O         | <ul style="list-style-type: none"> <li>◆ 2 x USB 3.0</li> <li>◆ 1 x Power button with LED</li> <li>◆ 1 x ID button with LED</li> <li>◆ 1 x NMI button</li> <li>◆ 1 x Reset button</li> <li>◆ 2 x LAN activity LEDs</li> <li>◆ 1 x HDD activity LED</li> <li>◆ 1 x System status LED</li> </ul>  |
|  | Rear I/O          | <ul style="list-style-type: none"> <li>◆ 2 x USB 3.0</li> <li>◆ 1 x VGA</li> <li>◆ 2 x RJ45</li> <li>◆ 1 x MLAN</li> <li>◆ 1 x ID button with LED</li> </ul>  |
|  | Backplane I/O     | <ul style="list-style-type: none"> <li>◆ Backplane P/N: 9CBP1042NR-00</li> <li>◆ Speed and bandwidth:</li> <li>◆ SAS 12Gb/s, SATA 6Gb/s</li> </ul>  |
|  | TPM               | <ul style="list-style-type: none"> <li>◆ 1 x TPM header with SPI interface</li> <li>◆ Optional TPM2.0 kit: CTM010</li> </ul>  |
|  | System Management | <ul style="list-style-type: none"> <li>◆ Aspeed® AST2500 management controller</li> <li>◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface</li> <li>◆ Dashboard</li> <li>◆ JAVA Based Serial Over LAN</li> <li>◆ HTML5 KVM</li> <li>◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)</li> <li>◆ Sensor Reading History Data</li> <li>◆ FRU Information</li> <li>◆ SEL Log in Linear Storage / Circular Storage Policy</li> <li>◆ Hardware Inventory</li> <li>◆ Fan Profile</li> <li>◆ System Firewall</li> <li>◆ Power Consumption</li> <li>◆ Power Control</li> <li>◆ LDAP / AD / RADIUS Support</li> <li>◆ Backup &amp; Restore Configuration</li> <li>◆ Remote BIOS/BMC/CPLD Update</li> <li>◆ Event Log Filter</li> <li>◆ User Management</li> <li>◆ Media Redirection Settings</li> <li>◆ PAM Order Settings</li> <li>◆ SSL Settings</li> <li>◆ SMTP Settings</li> </ul> |



#### Power Supply

- ◆ Dual 800W 80 PLUS Platinum redundant power supply

##### AC Input:

- 100-240V~/ 10-4A, 50-60Hz

- ◆ DC Input:

- 240Vdc/ 4.5A

- ◆ DC Output:

- 800W

+12V/ 66A

+12Vsb/ 2.5A

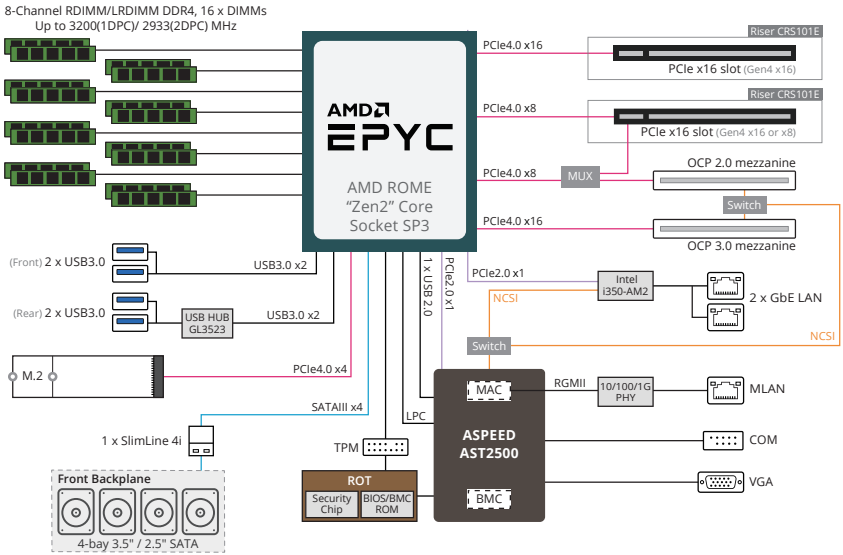


#### Operating Properties

- ◆ Operating temperature: 10°C to 35°C
- ◆ Operating humidity: 8% to 80% (non-condensing)
- ◆ Non-operating temperature: -40°C to 60°C
- ◆ Non-operating humidity: 20% to 95% (non-condensing)

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

# 1-3 System Block Diagram





# Chapter 2 System Appearance

## 2-1 Front View

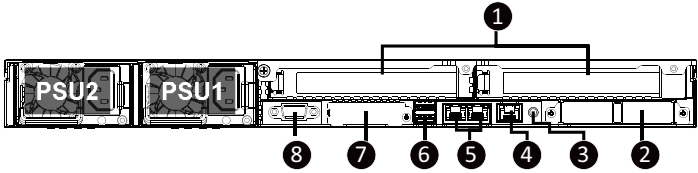


| No.                             | Description                  |
|---------------------------------|------------------------------|
| 1.                              | USB 3.0 Port x 2             |
| 2.                              | Front Panel LEDs and Buttons |
| Orange HDD Latches Support NVMe |                              |



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

## 2-2 Rear View

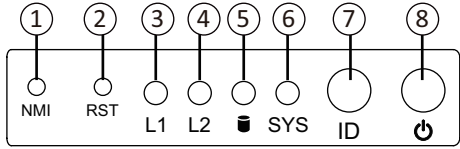


| No. | Description                              |
|-----|--|
| 1.  | PCIe Card Slot x 2                       |
| 2.  | Mezzanine Card Slot (Option/OCP 3.0/SFF) |
| 3.  | ID Button with LED                       |
| 4.  | Server Management LAN Port               |
| 5.  | GbE LAN Port x 2                         |
| 6.  | USB 3.0 Port x 2                         |
| 7.  | Mezzanine Card Slot (Option/OCP 2.0)     |
| 8.  | VGA Port                                 |



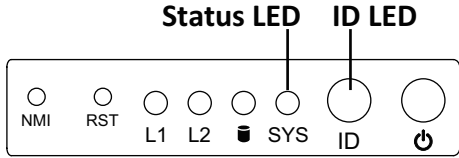
- Refer to section **2-5 Rear System LAN LEDs** for a detailed description of the function of the LEDs.

## 2-3 Front Panel LEDs and Buttons



| No.   | Name                     | Color       | Status | Description   |
|-------|--------------------------|-------------|--------|---|
| 1.    | 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.                   |
| 2.    | Reset button             | --          | --     | Press this button to reset the system.  |
| 3./4. | LAN 1/2 Active/Link LEDs | Green       | On     | Indicates a link between the system and the network or no access.   |
|       |                          | Green       | Blink  | Indicates data transmission or receiving is occurring.  |
|       |                          | N/A         | Off    | Indicates no data transmission or receiving is occurring.   |
| 5.    | HDD Status LED           | Green       | On     | Indicates locating the HDD.   |
|       |                          | Green       | 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        |             |        | This LED represents the RoT function LED behavior. Please see the following section for detail LED behavior.  |
| 7.    | ID Button with LED       |             |        | This LED represents the RoT function LED behavior. Please see the following section for detail LED behavior.  |
| 8.    | Power button with LED    | Green       | On     | Indicates the system is powered on.   |
|       |                          | Green       | Blink  | System is in ACPI S1 state (sleep mode).  |
|       |                          | N/A         | Off    | <ul style="list-style-type: none"> <li>System is not powered on or in ACPI S5 state (power off)</li> <li>System is in ACPI S4 state (hibernate mode)</li> </ul> |

## 2-4 RoT LEDs



| LED on Front pane <sup>(Note5)</sup>  |                                      |                                       |
|---|--------------------------------------|---------------------------------------|
|   | ID LED                               | Status LED                            |
| <b>EC Firmware (FW) Authentication fail or not exit</b>                       |                                      |                                       |
| EC FW is broken or not exit <sup>(Note1)</sup>                                | OFF                                  | OFF                                   |
| <b>Authenticating/Recovering BMC/BIOS Images</b>                              |                                      |                                       |
| Authenticating Images   | OFF                                  | OFF                                   |
| Recovering BMC Active Flash   | Blinks Blue<br>4 times per<br>second | Blinks Green<br>4 times per<br>second |
| Recovering BIOS Active Flash  | Blinks Blue<br>4 times per<br>second | Blinks Green<br>4 times per<br>second |
| <b>Authentication (AUTH) Pass</b>   |                                      |                                       |
| 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                                   |
| <b>Active Flash Authentication (AUTH) Fail</b>                                |                                      |                                       |
| BMC : AUTH Fail <sup>(Note2)</sup>  | Blinks Blue<br>1 time per<br>second  | Blinks Green<br>1 time per second     |

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

**NOTE!**

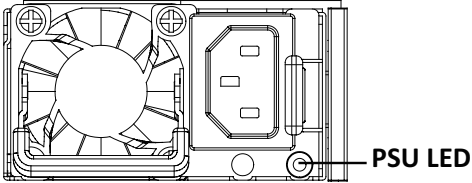
1. EC FW is broken or not exited result in Microchip CEC1702 cannot load EC FW for authentication.
2. (1) Authentication fail include below scenarios  
Configuration table is missing or modified  
Public key is missing or modified  
Protected area or signature is modified  
Flash empty
3. if active flash 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



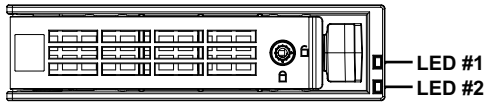
| No. | Name                    | Color  | Status | Description                                    |
|-----|-------------------------|--------|--------|--|
| 1.  | 1GbE Speed LED          | Yellow | On     | 1 Gbps data rate                               |
|     |                         | Green  | On     | 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 receiving is occurring    |
|     |                         | N/A    | Off    | No data transmission or receiving is occurring |

## 2-6 Power Supply Unit LED



| 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 Chassis Cover

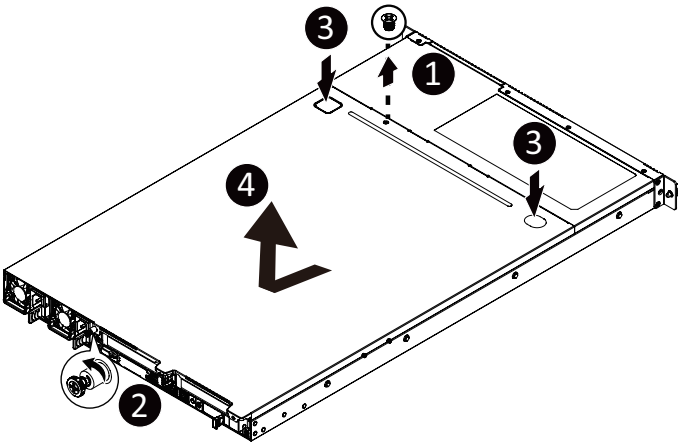


Before you remove or install the system cover

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

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

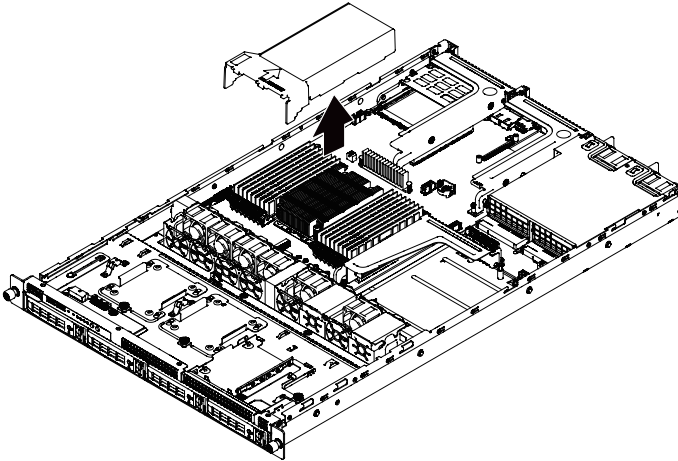
1. Remove the screw securing the chassis cover.
2. Loosen the thumbscrew securing the chassis cover.
3. Push down the indentations located on the sides of the chassis cover.
4. Slide the cover cover to the rear of the system and then remove the cover in the direction indicated by the arrow.
5. To reinstall the chassis cover reverse steps 1-4.



## 3-2 Removing and Installing the Fan Duct

Follow these instructions to remove/install the fan duct:

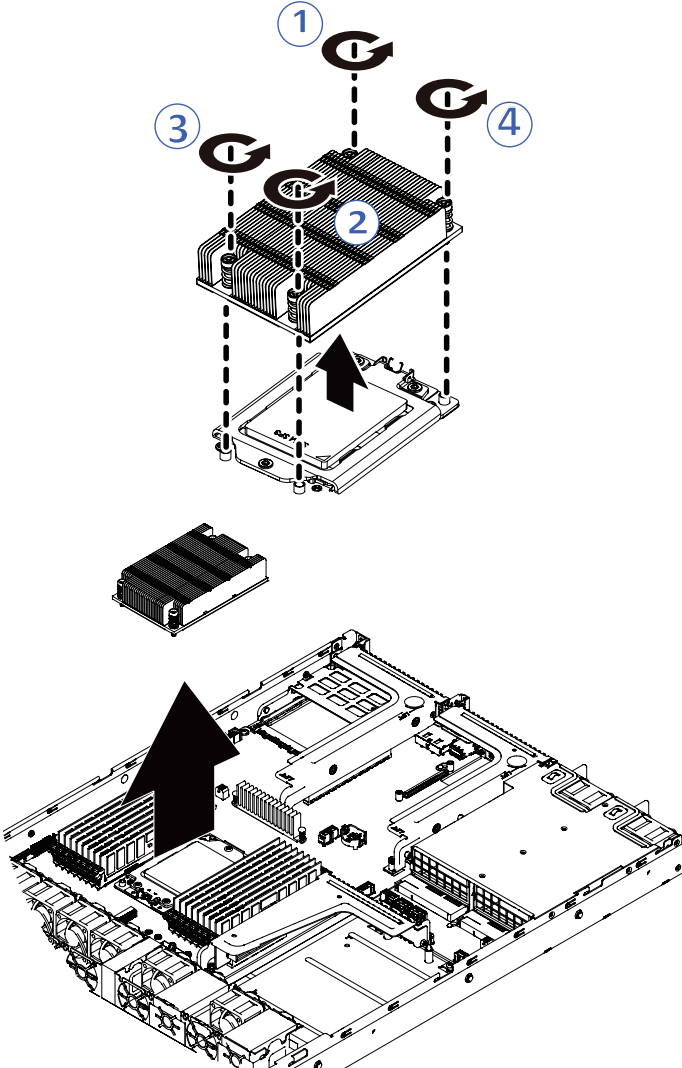
1. Lift up to remove the two fan ducts
2. To install the fan duct, align the fan duct with the guiding groove. Push down the fan duct into chassis until its firmly seats



### 3-3 Removing the Heat Sink

Follow these instructions to remove/install the fan duct:

1. Loosen the captive screws securing the heatsink in place in reverse order (4→3→2→1).
2. Lift and remove the heat sink from the system.
3. To reinstall 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.



### 3-4 Installing the CPU



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

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



#### **WARNING!**

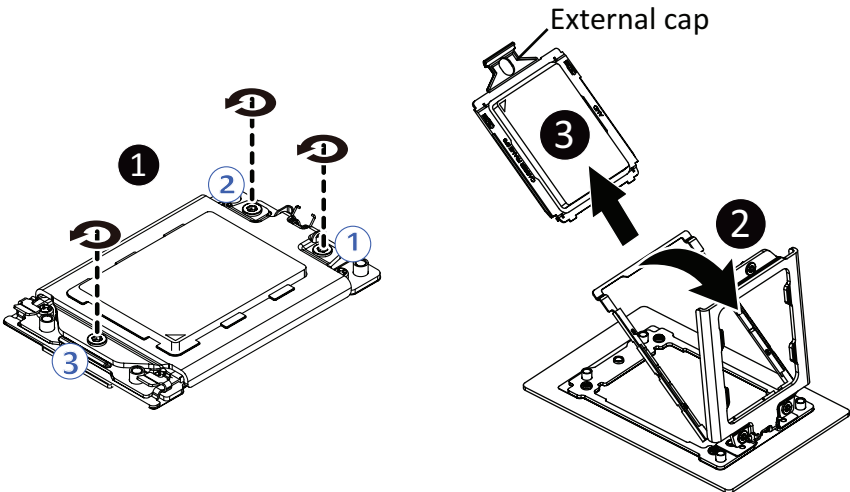
Failure to properly turn off the server before you start installing components may cause serious damage. Do not attempt the procedures described in the following sections unless you are a qualified service technician.

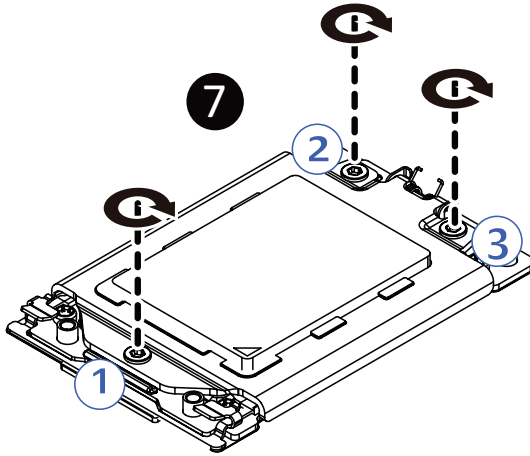
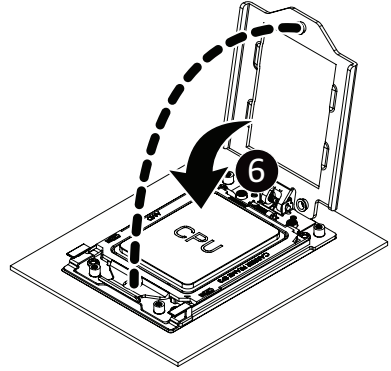
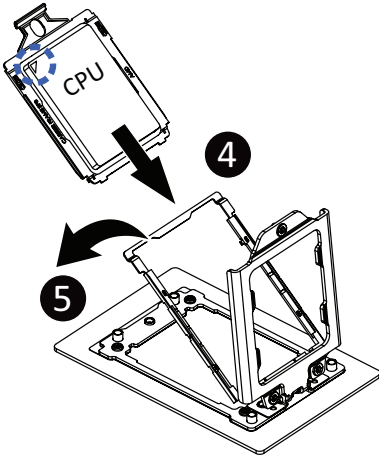
#### **Follow these instructions to install the CPU:**

1. Loosen the three captive screws securing the CPU cover in sequential order (1 → 2 → 3).
2. Flip open the CPU cover.
3. Remove the CPU carrier from the CPU frame using the handle on the CPU carrier.
4. Using the handle on the CPU carrier insert the new CPU carrier with CPU installed into the CPU frame.

**NOTE:** Ensure the CPU is installed in the CPU carrier in the correct orientation, with the triangle on the CPU aligned to the top left corner of the CPU carrier.

5. Flip the CPU frame with CPU installed into place in the CPU socket.
6. Flip the CPU cover into place over the CPU socket.
7. Tighten the CPU cover screws in sequential order (1 → 2 → 3) to secure the CPU cover in place.





### 3-5 Installing the Memory

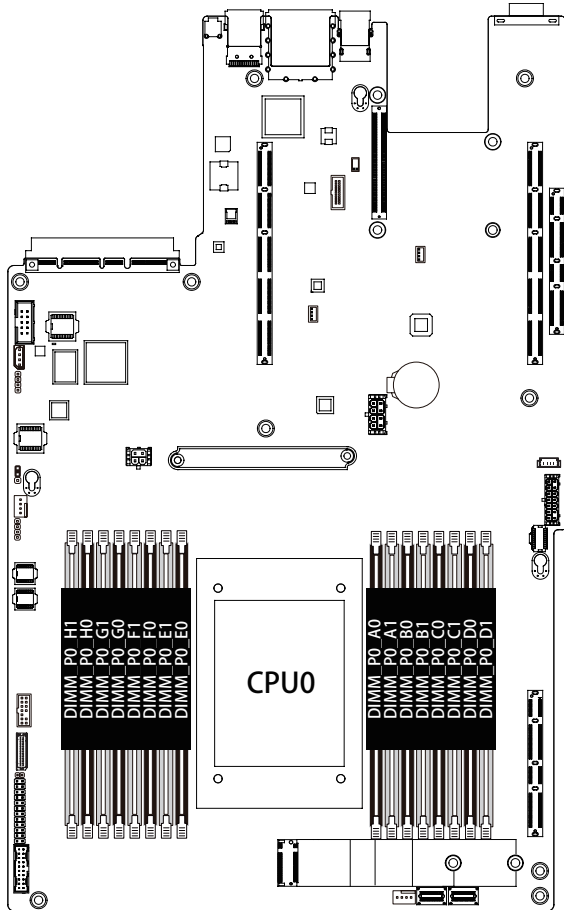


Read the following guidelines before you begin to install the memory:

- 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.

#### 3-5-1 Eight Channel Memory Configuration

This motherboard provides 16 DDR4 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



### 3-5-2 Installing a Memory

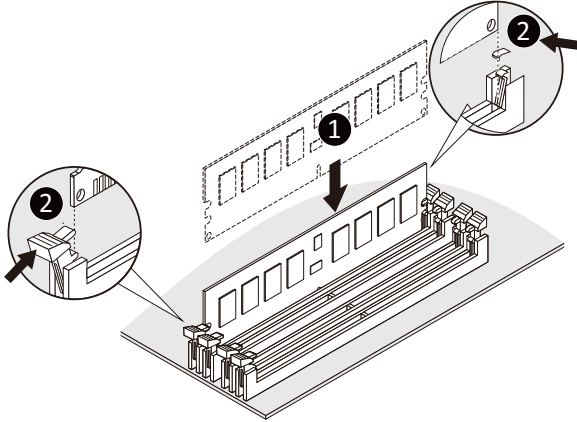


Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on this motherboard.

Follow these instructions to install the Memory:

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.



### 3-5-3 DIMM Population Table

#### RDIMM Maximum Frequency Supported Table

| DIMMs Populated | DIMM |           | Frequency (MT/s) |
|-----------------|------|-----------|------------------|
|                 | 1R   | 2R<br>2DR | 1.2V             |
| 1               | 1    | --        | 3200             |
|                 | --   | 1         | 3200             |
| 2               | 2    | --        | 2933             |
|                 | 1    | 1         | 2933             |
|                 | --   | 2         | 2933             |



## LRDIMM Maximum Frequency Supported Table

| DIMMs Populated | DIMM         |     | Frequency (MT/s) |
|-----------------|--------------|-----|------------------|
|                 | 2S2R<br>2S4R | 4DR | 1.2V             |
| 1               | 1            | --  | 3200             |
|                 | --           | 1   | 3200             |
| 2               | 2            | --  | 2933             |
|                 | 1            | 1   | Not Supported    |
|                 | --           | 2   | 2933             |

## 3DS RDIMM Maximum Frequency Supported Table

| DIMMs Populated | DIMM         | Frequency (MT/s) |
|-----------------|--------------|------------------|
|                 | 2S2R<br>2S4R | 1.2V             |
| 1               | 1            | 2933             |
| 2               | 2            | 2666             |

### NOTE!

- 1R: 1 package rank of SDP DRAMs
- 2R: 2 package rank of SDP DRAMs
- 2DR: 2 package rank of DDP DRAMs
- 4DR: 4 package rank of DDP DRAMs
- 2S2R/2S4R/2S8R: 2 package rank of 2/4/8 high 3DS DRAMs
- DIMM must be populated in sequential alphabetic order, starting with bank A.
- When only one DIMM is used, it must be populated in memory slot A1.

### 3-6 Installing the PCI Expansion 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-down and all power sources have been disconnected from the server prior to installing a PCI card.

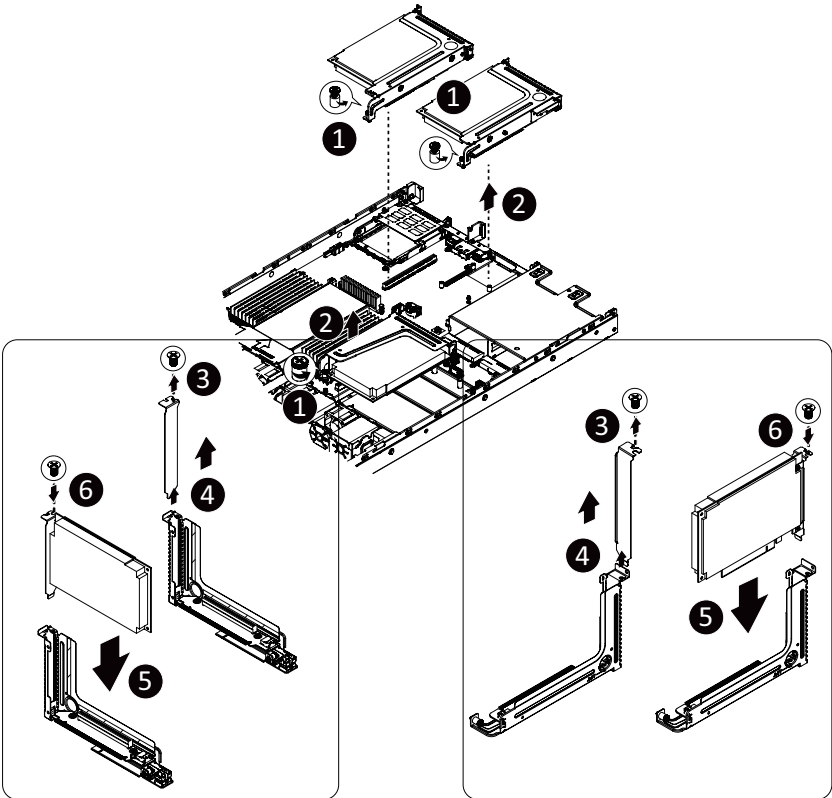
Failure to observe these warnings could result in personal injury or damage to equipment.



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

#### Follow these instructions to PCI Expansion card:

1. Loosen the thumbscrew securing the riser bracket to the system.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the slot cover to the riser bracket.
4. Remove the slot covers from the riser bracket.
5. Orient the PCI-E card with the riser guide slot and push in the direction of the arrow until the PCI-E card sits in the PCI card connector.
6. Secure the PCI-E card with the screw.
7. Reverse the steps 3 - 1 to install the riser bracket.



## 3-7 Installing the Mezzanine Card

### 3-7-1 OCP 3.0

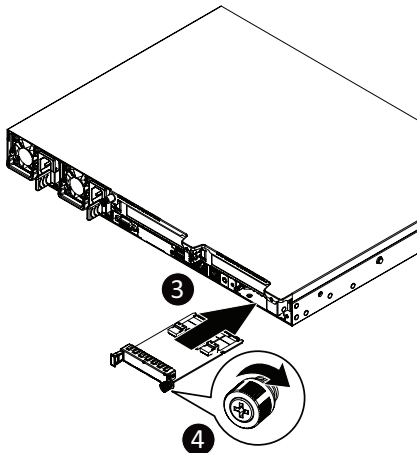
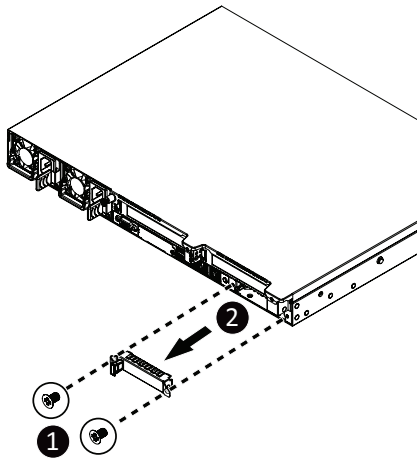


Use of the following type of OCP 3.0 NIC is recommended:

- 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:**

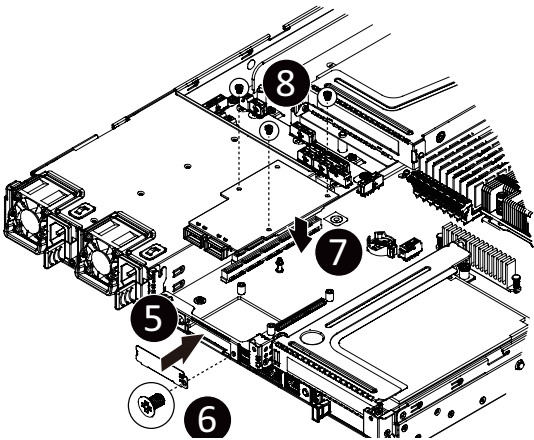
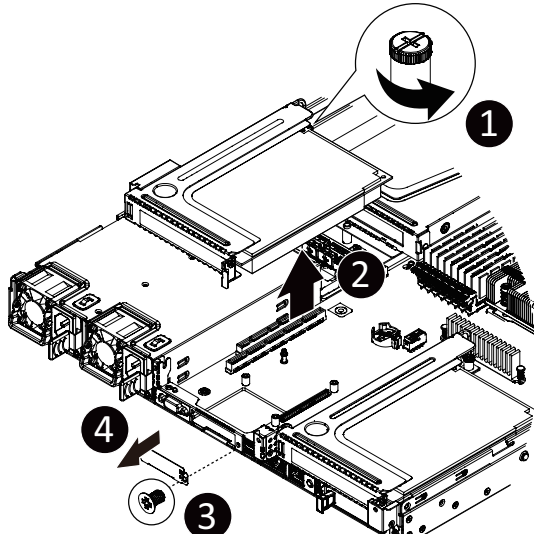
1. Remove the two screws securing the mezzanine card slot cover.
2. Remove the slot cover from the system.
3. Insert the OCP 3.0 mezzanine card into the card slot ensuring that the card is firmly connected to the connector on the motherboard.
4. Tighten the thumbnail screw to secure the OCP 3.0 mezzanine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



### 3-7-2 OCP 2.0

Follow these instructions to install an OCP 2.0 mezzanine card:

1. Loosen the thumbscrew on the riser bracket
2. Lift up the riser bracket out of system.
3. Remove the screw securing the mezzanine card slot cover.
4. Remove the slot cover from the system..
5. Insert the OCP 2.0 mezzanine card into the compartment ensuring that the card is firmly connected to the connector on the motherboard.
6. Secure the OCP 2.0 mezzanine card into the system with three screws.
7. Reverse steps 5-6 to replace the OCP 2.0 mezzanine card.



### 3-8 Installing the Hard Disk Drive

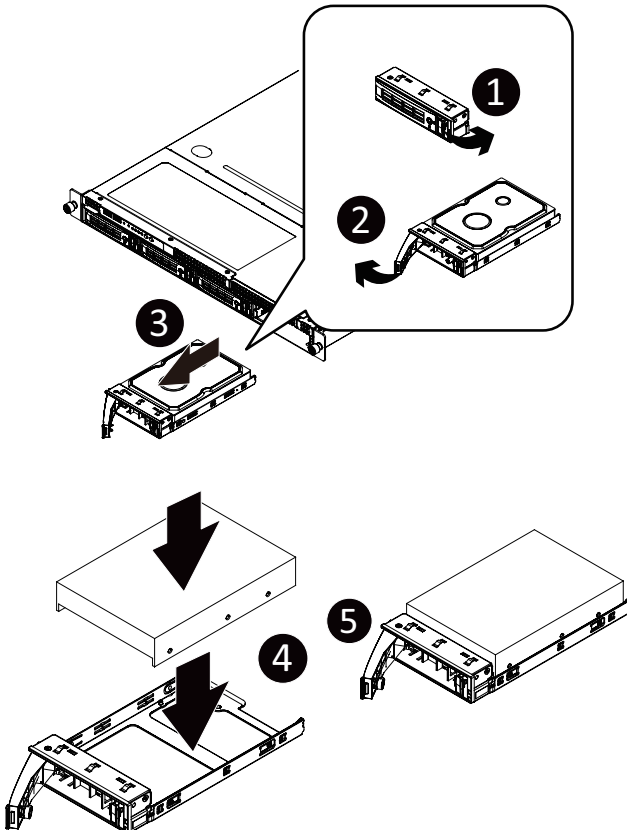


Read the following guidelines before you begin to install the Hard disk drive:

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

**Follow these instructions to install a 2.5" 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 2.5" HDD tray.
4. Orient the hard disk drive so the opening on the rear of the hard disk drive is aligned to the positioning stud on the HDD tray.
5. Slide the hard disk drive into the HDD tray.
6. Reinsert the HDD tray into the slot and close the locking lever.



### 3-9 Replacing the Fan Assembly

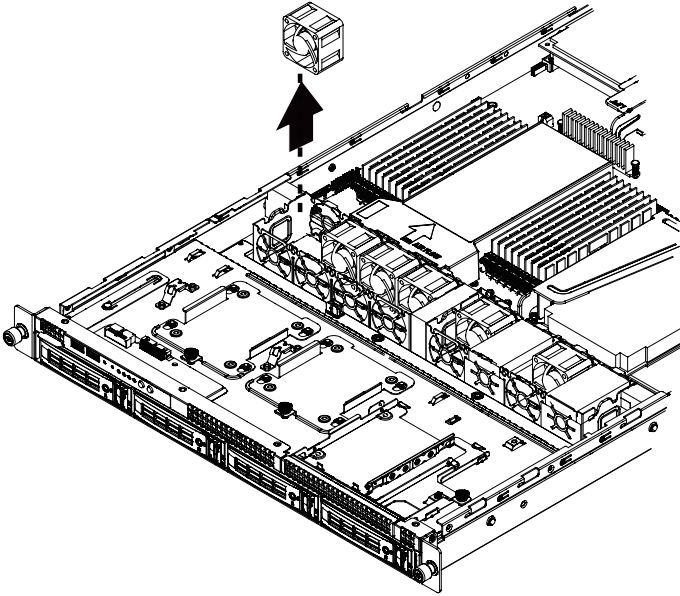


- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to replacing a system fan.

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

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

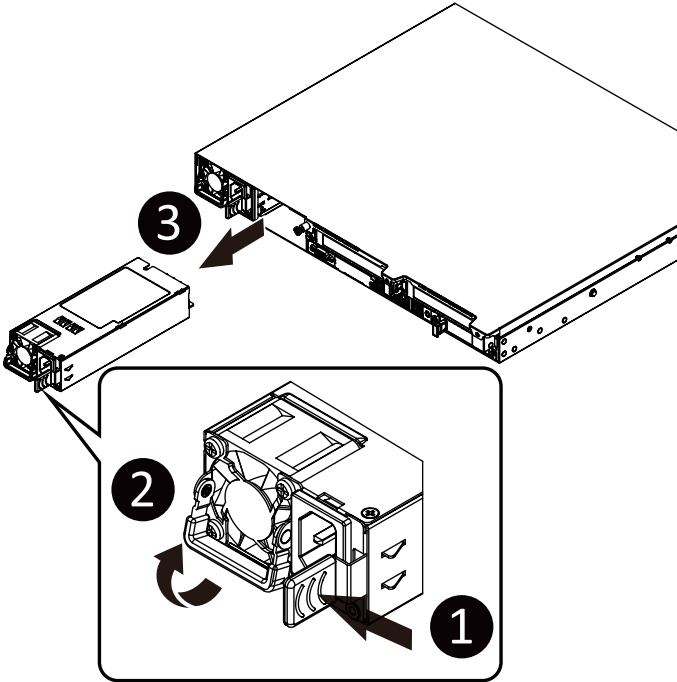
1. Lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



## 3-10 Replacing the Power Supply

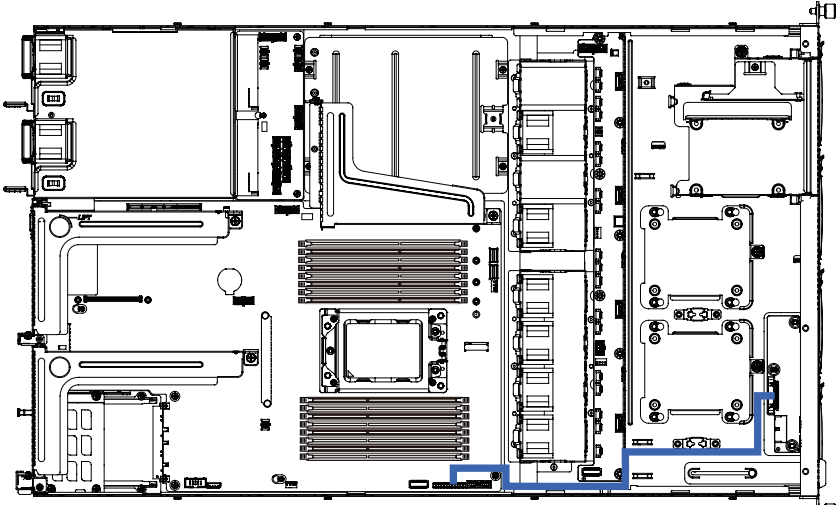
Follow these instructions to replace the power supply:

1. Press the retaining clip on the right side of the power supply along the direction of the arrow.
2. Pull up the power supply handle at the same time and pull out the power supply.
3. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.

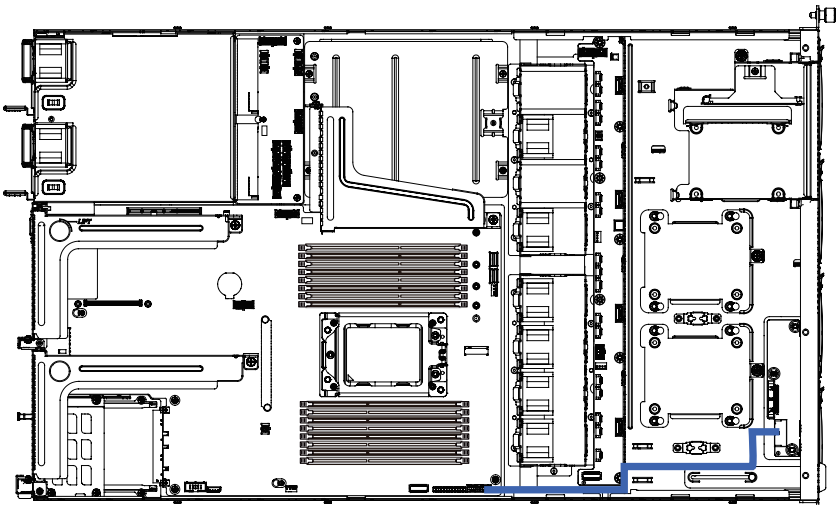


# 3-11 Cable Routing

## Front Switch Cable/Front LED Cable

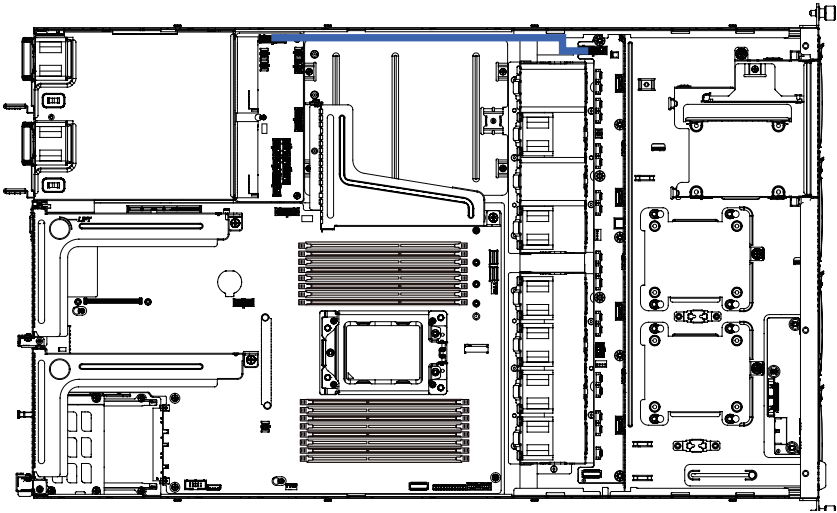


## Front Panel USB 3.0 Cable

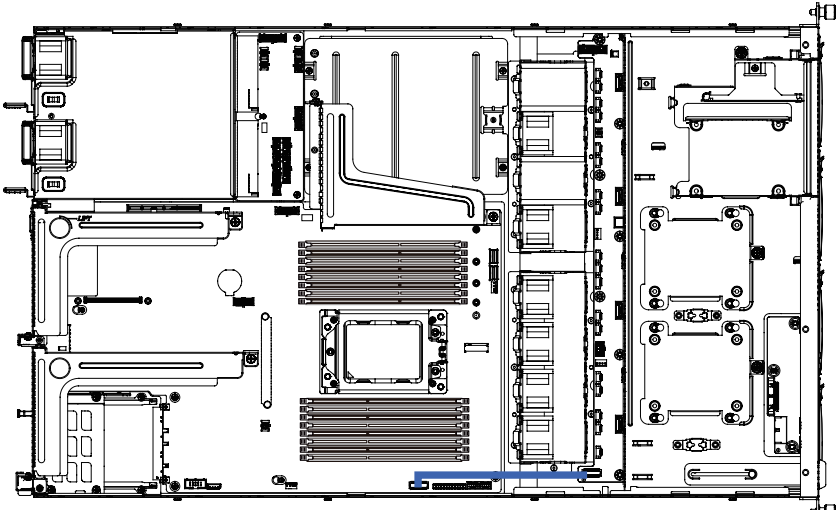




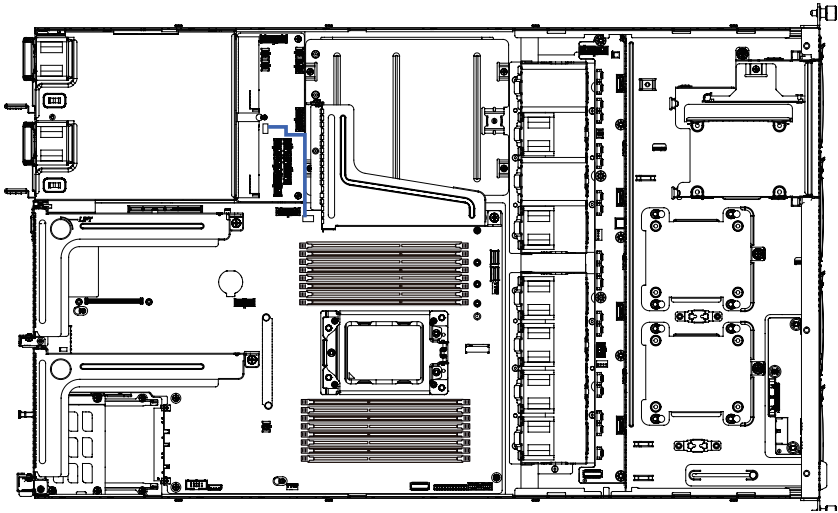
HDD Backplane Board Power Cable



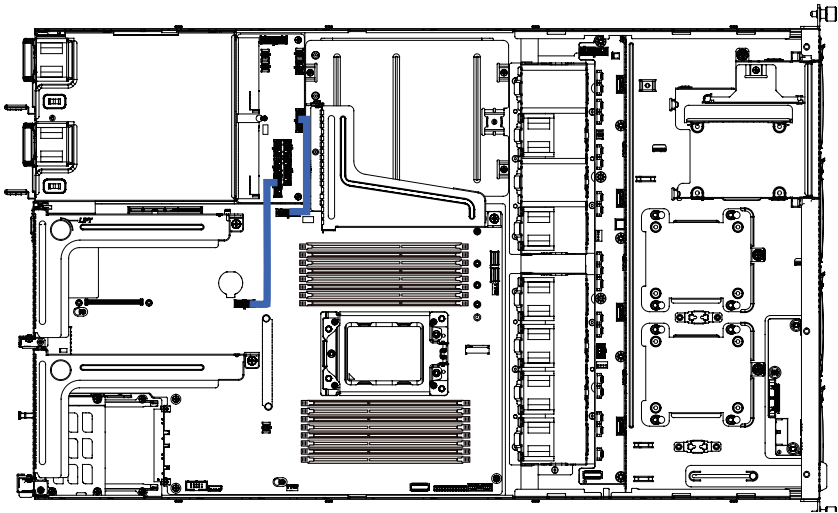
HDD Backplane Board Signal Cable



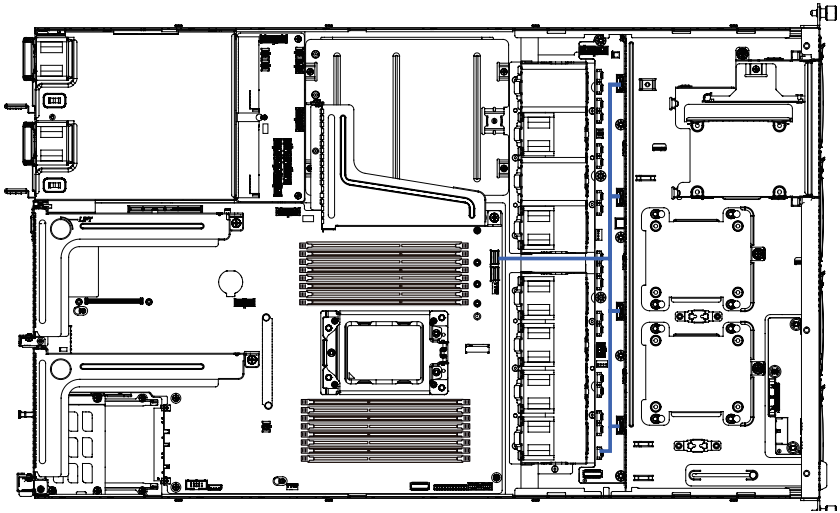
Power Distribution Board Signal Cable



System Power Cable



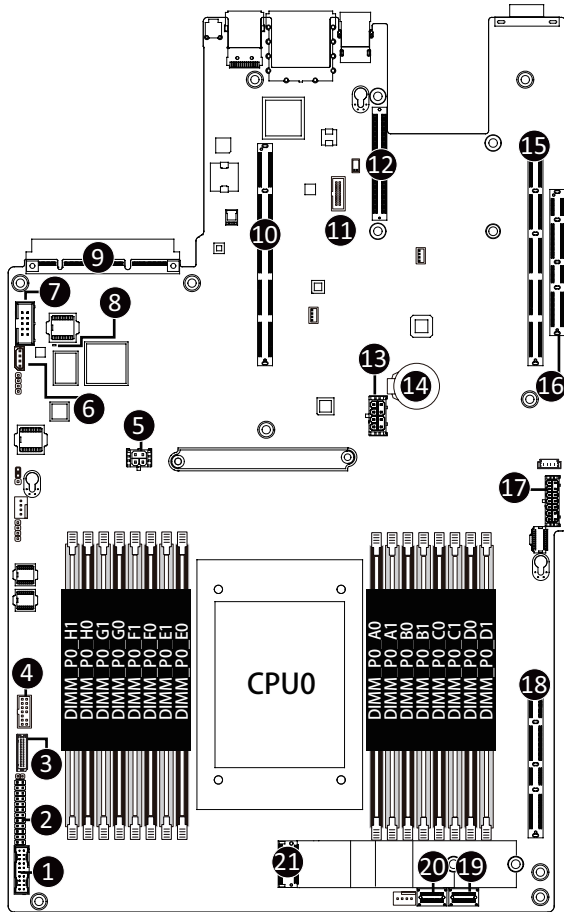
SlimLine to SATA Cable



This page intentionally left blank

# Chapter 4 Motherboard Components

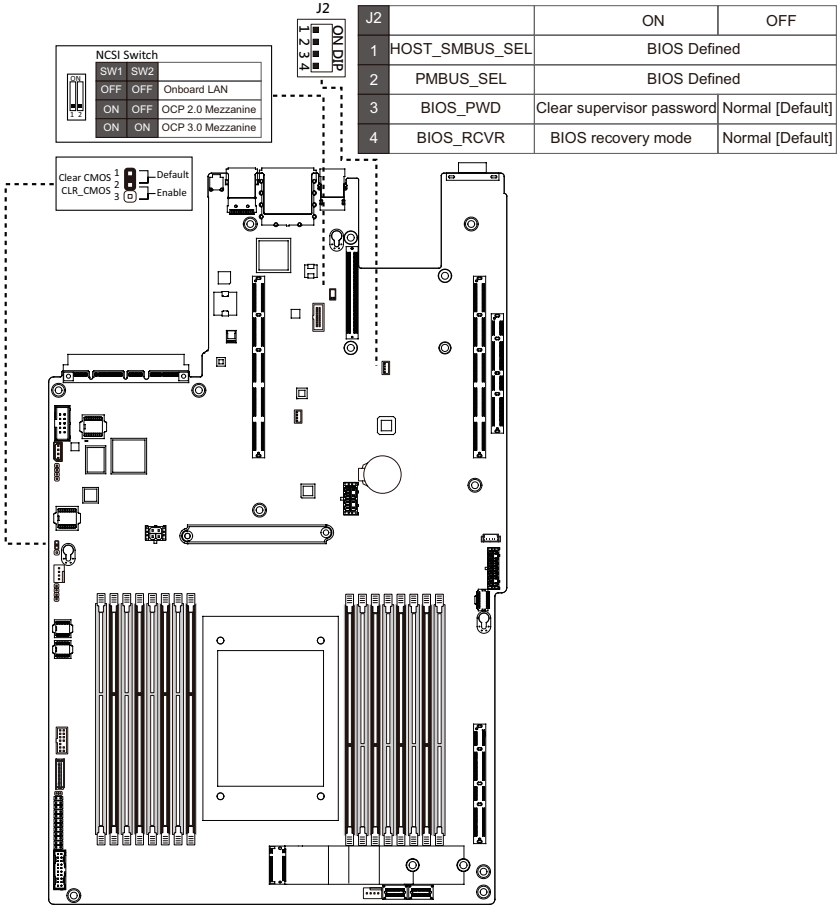
## 4-1 Motherboard Components



| Item | Description                          |
|------|--------------------------------------|
| 1    | Front Panel USB 3.0 Connector        |
| 2    | Front Panel Connector                |
| 3    | HDD Back Plane Board Connector       |
| 4    | TPM Module Connector (SPI Interface) |
| 5    | 2 x 2 Pin P12V Power Connector       |
| 6    | IPMB Connector                       |
| 7    | Serial Port Cable Connector          |

|    |  |
|----|--|
| 8  | BMC Firmware Readiness LED                                 |
| 9  | OCN Mezzanine Connector (OCN 3.0/SFF Type/Gen4 x16)        |
| 10 | Riser Connector #1 (PCIe Gen4/x32 Slot)                    |
| 11 | GbE LAN Cable Connector                                    |
| 12 | OCN Mezzanine Connector (OCN 2.0/Gen3 x8)                  |
| 13 | 2 x 5 Pin P12V Power Connector                             |
| 14 | System Battery   |
| 15 | Riser Connector #2 (PCIe Gen4/x32 Slot)                    |
| 16 | Riser Connector #3 (PCIe Gen4/x16 Slot)                    |
| 17 | 2 x 6 Pin Power Connector                                  |
| 18 | Riser Connector #4 (PCIe Gen4/x16 Slot)                    |
| 19 | SlimLine SAS Connector (SLSAS_0/PCIe/SATA/Defined by SKUs) |
| 20 | SlimLine SAS Connector (SLSAS_1/PCIe/SATA/Defined by SKUs) |
| 21 | M.2 Connector (PCIe4 x4, Supports NGFF-22110)              |

# 4-2 Jumper Settings



This page intentionally left blank



## 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 1 for how to clear the CMOS values.)

### BIOS Setup Program Function Keys

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

■ **Main**

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

■ **Advanced**

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

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

■ **AMD CBS**

This setup page includes the common items for configuration of AMD motherboard-related information.

■ **AMD PBS Option**

This setup page includes the common items for configuration of AMD CPM RAS related settings.

■ **Chipset**

This setup page includes all the submenu options for configuring the functions of the North Bridge.

■ **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

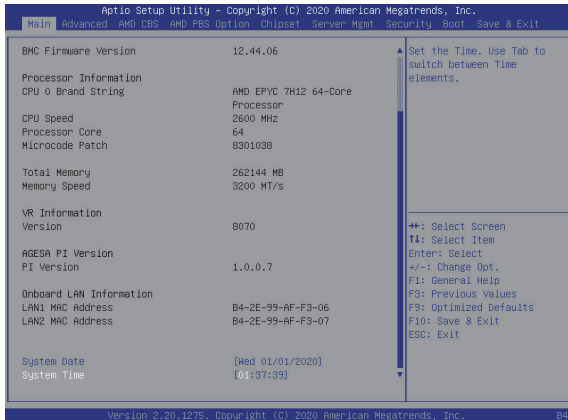
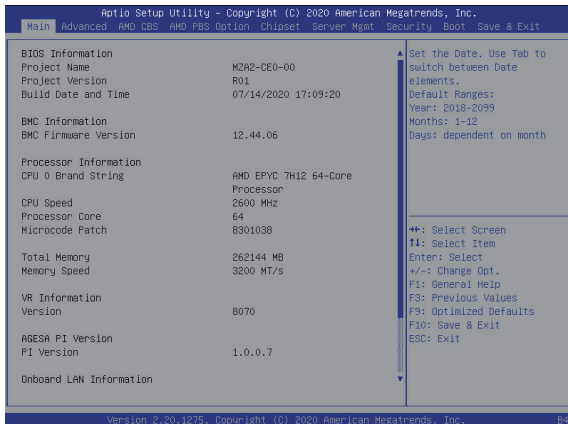
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

## 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   |
|---|---|
| BIOS Information  |   |
| 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.                          |
| CPU Brand String / CPU Speed / Processor Core / Microcode Patch | Displays the technical information for the installed processor(s).  |
| Total Memory <sup>(Note3)</sup>                                 | Displays the total memory size of the installed memory.             |
| Memory Frequency <sup>(Note3)</sup>                             | Displays the frequency information of the installed memory.         |
| VR Information Version  | Displays VR version information.                                    |
| AGESA PI Version PI Version                                     | Displays AGESA PI version information.                              |
| Onboard LAN Information   |   |
| LAN1 MAC Address <sup>(Note1)</sup>                             | Displays LAN MAC address information.                               |
| LAN2 MAC Address <sup>(Note2)</sup>                             | Displays LAN MAC address information.                               |
| System Date   | Sets the date following the weekday-month-day-year format.          |
| System Time   | Sets the system time following the hour-minute-second format.       |

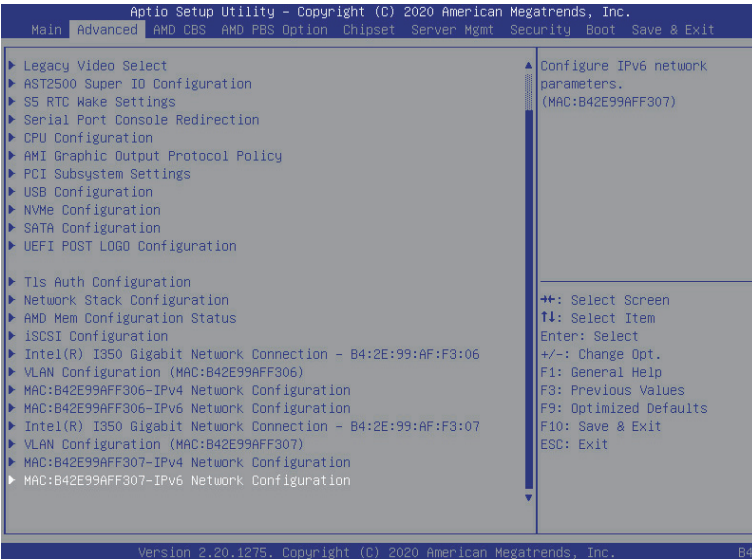
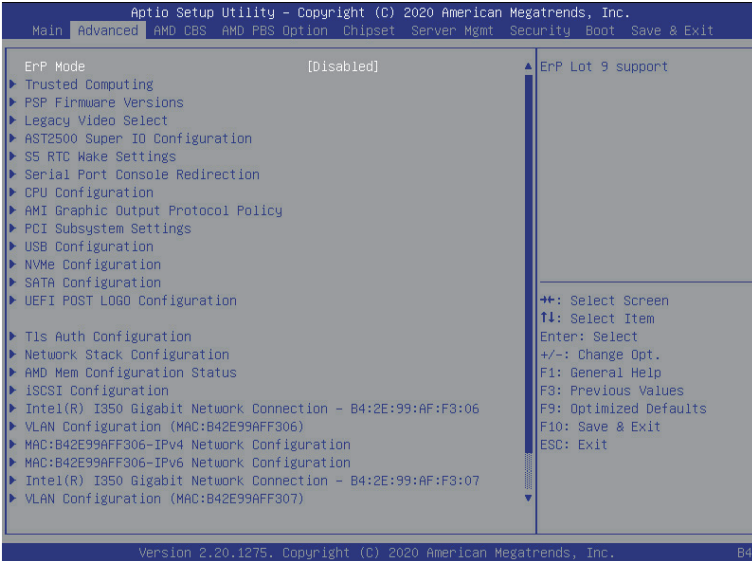
(Note1) The number of LAN ports listed will depend on the motherboard / system model.

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

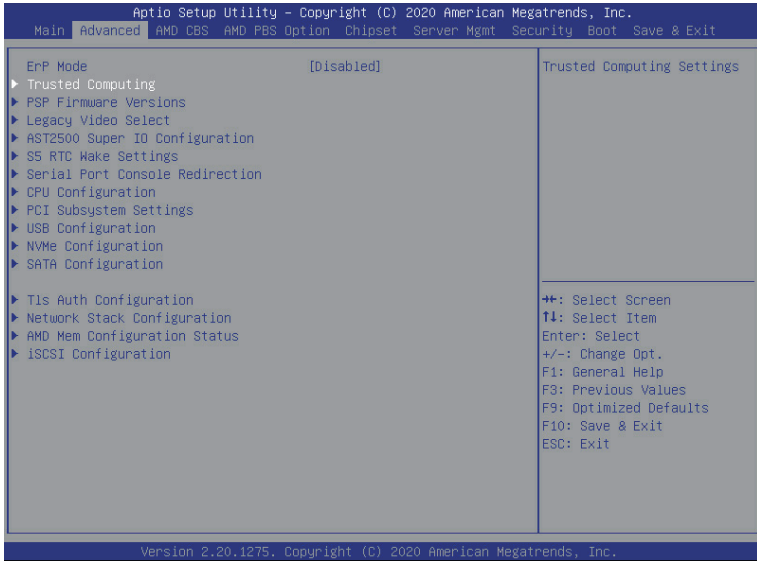
## 5-2 Advanced Menu

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.

### When Boot Mode Select is set to UEFI (Default)



**When "Boot Mode Select" is set to Legacy in the Boot > Boot Mode Select section**



| Parameter | Description   |
|-----------|---|
| ErP Mode  | Enable/Disable ErP Lot 9 support.<br>Options available: Enable/Disable. Default setting is <b>Disable</b> . |

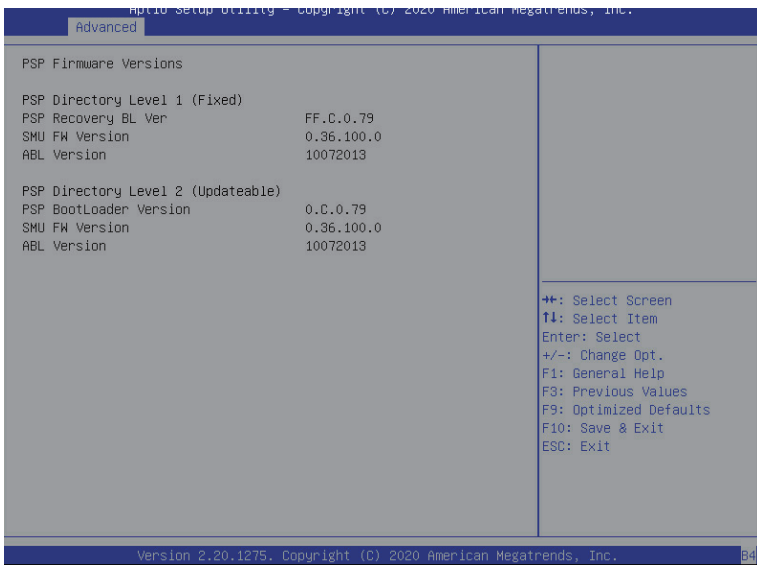
## 5-2-1 Trusted Computing



| Parameter               | Description   |
|-------------------------|---|
| Configuration           |   |
| Security Device Support | <p>Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.</p> <p>Options available: Enable/Disable. Default setting is <b>Enable</b>.</p> |
| SPI TPM Support         | <p>Select Enable to activate TPM support feature.</p> <p>Options available: Enabled/Disabled. Default setting is <b>Disabled</b></p>  |

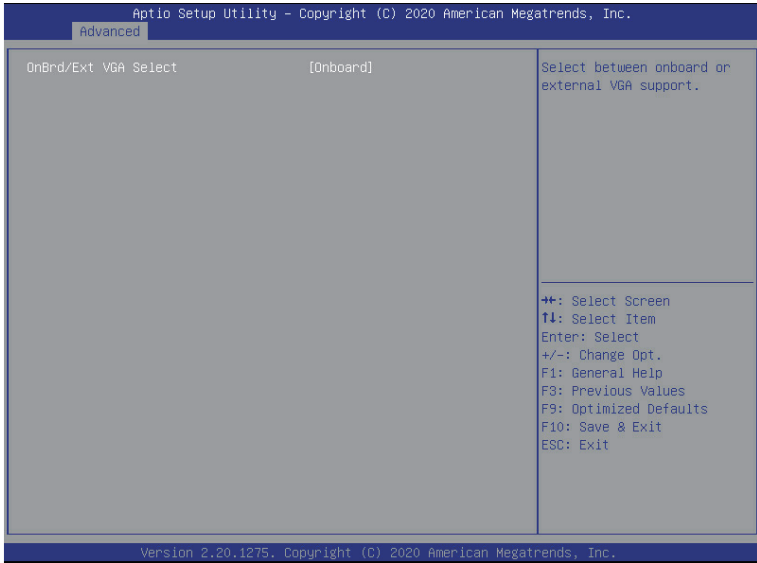
## 5-2-2 PSP Firmware Versions

The PSP Firmware Versions page displays the basic PSP firmware version information. Items on this window are non-configurable.





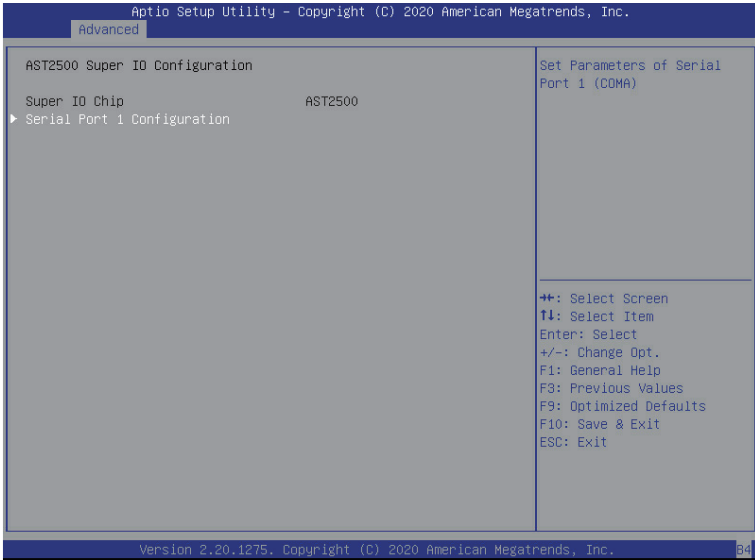
### 5-2-3 Legacy Video Select



| Parameter                              | Description   |
|--|---|
| OnBrd/Ext VGA Select <sup>(Note)</sup> | Selects between onboard or external VGA support.<br>Options available: Auto, Onboard, External. Default setting is <b>Onboard</b> . |

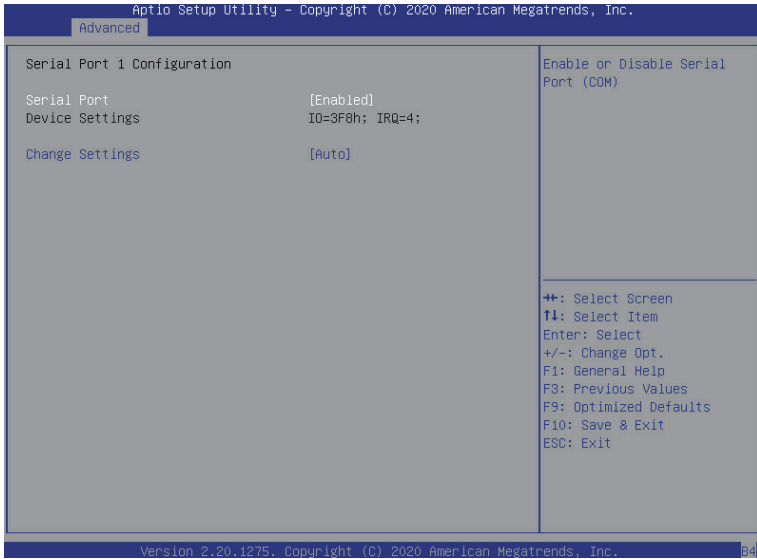
(Note) This configurable option will be displayed when "Boot Mode Select" is set to **Legacy** in the Boot > Boot Mode Select section.

## 5-2-4 AST2500 Super IO Configuration



| Parameter                      | Description  |
|--------------------------------|--|
| AST2500 Super IO Configuration |  |
| Super IO Chip                  | Displays the super IO chip information             |
| Serial Port 1/2 Configuration  | Press [Enter] for configuration of advanced items. |

## 5-2-4-1 Serial Port 1 Configuration



| Parameter                           | Description  |
|-------------------------------------|--|
| Serial Port 1/2 Configuration       |  |
| Serial Port <sup>(Note1)</sup>      | Enable/Disable the Serial Port (COM). When set to Enabled allows you to configure the Serial port 1/2 settings. When set to Disabled, displays no configuration for the serial port.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> . |
| Devices Settings <sup>(Note2)</sup> | Displays the Serial Port 1/2 device settings.  |

(Note1) Advanced items prompt when this item is defined.

Select an optimal settings for Super IO Device.

Options available for Serial Port 1:

Auto

IO=3F8h; IRQ=4;

IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

Default setting is **Auto**.

Change Settings<sup>(Note2)</sup>

Options available for Serial Port 2:

Auto

IO=2F8h; IRQ=3;

IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

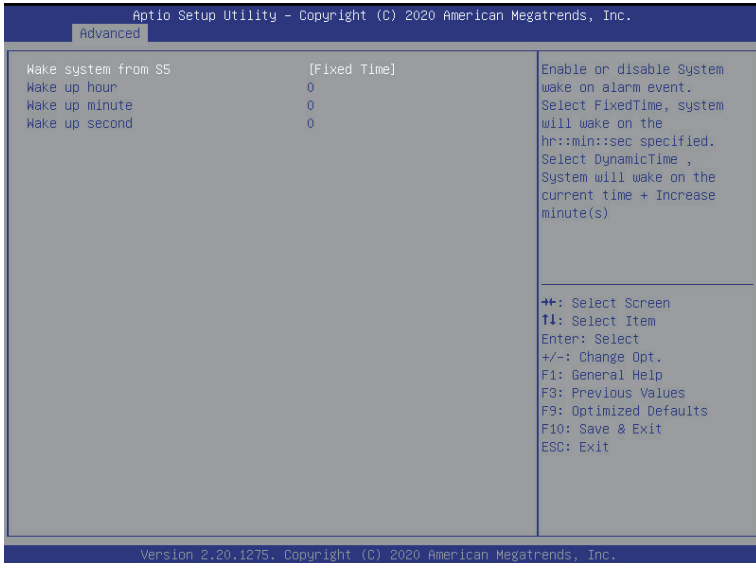
IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

Default setting is **Auto**.

**Please note that this item is configurable when Serial Port is set to Enabled.**

(Note2) This item appears when **Serial Port** is set to **Enabled**.

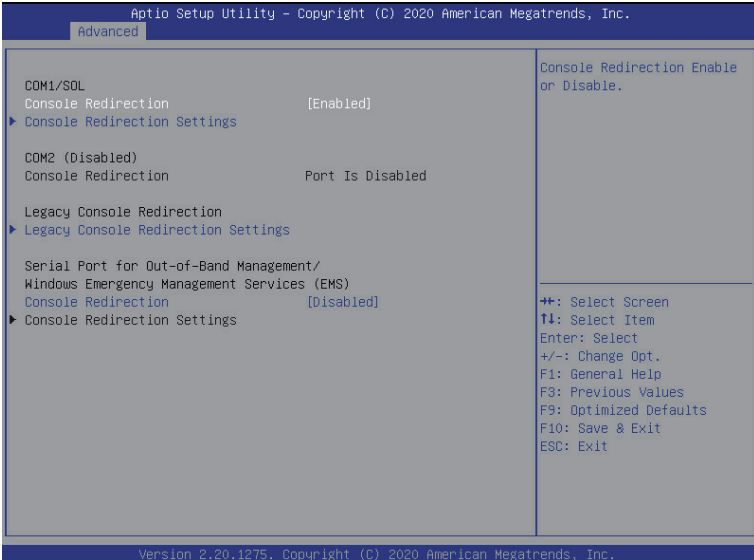
## 5-2-5 S5 RTC Wake Settings



| Parameter                              | Description  |
|--|--|
| Wake System from S5 <sup>(Note1)</sup> | Enable/Disable system wake on alarm event.<br>Options available: Disabled/Fixed Time. When Fixed Time enabled, system will wake on the hr::min::sec specified.<br>Default setting is <b>Disabled</b> . |

(Note1) Advanced items prompt when this item is defined.

## 5-2-6 Serial Port Console Redirection



| Parameter  | Description   |
|--|---|
| COM1/Serial Over LAN <sup>(Note)</sup>               | <p>Select whether to enable console redirection for specified device. Console redirection enables the users to manage the system from a remote location.</p> <p>Options available: Enabled/Disabled. Default setting is <b>Disabled</b>.</p>  |
| COM1/Serial Over LAN<br>Console Redirection Settings | <p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when COM1/Serial Over LAN &amp; COM2 Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Terminal Type                             <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is <b>ANSI</b>.</li> </ul> </li> <li>◆ Bits per second                             <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 38400, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> <li>◆ Data Bits                             <ul style="list-style-type: none"> <li>– Selects the number of data bits used for console redirection.</li> <li>– Options available: 7/8. Default setting is <b>8</b>.</li> </ul> </li> </ul> |

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

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

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

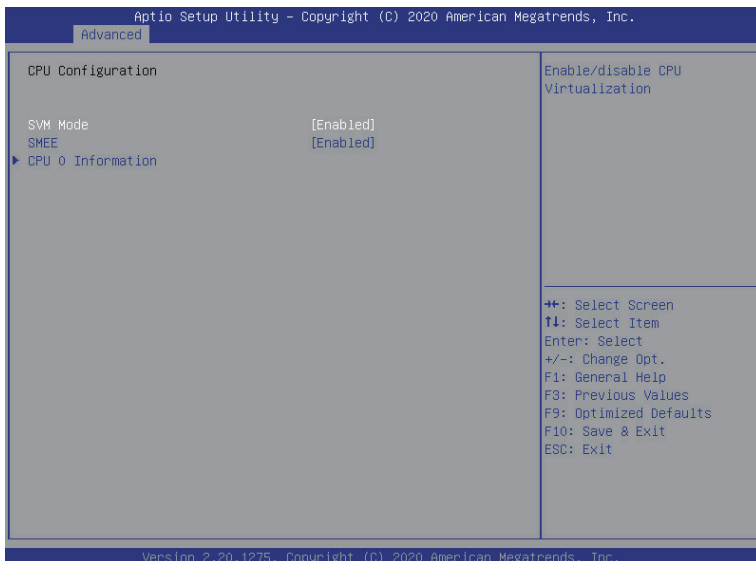
| Parameter  | Description  |
|--|--|
| Legacy Console Redirection   |  |
| Legacy Console Redirection Settings  | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Redirection COM Port <ul style="list-style-type: none"> <li>– Selects a COM port for Legacy serial redirection.</li> <li>– Options available: COM1/Serial Over LAN, COM2. Default setting is <b>COM1/Serial Over LAN</b>.</li> </ul> </li> <li>◆ Resolution <ul style="list-style-type: none"> <li>– Selects the number of rows and columns used in Console Redirection for legacy OS support.</li> <li>– Options available: 80x24, 80x25. Default setting is <b>80x24</b>.</li> </ul> </li> <li>◆ Redirect After POST <ul style="list-style-type: none"> <li>– When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS.</li> <li>– Options available: Always Enable, BootLoader. Default setting is <b>Always Enable</b>.</li> </ul> </li> </ul>  |
| Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection <sup>(Note)</sup> | <p>EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management.</p> <p>Options available: Enabled/Disabled. Default setting is <b>Disabled</b>.</p>  |
| Serial Port for Out-of-Band EMS Console Redirection Settings   | <p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.</b></p> <ul style="list-style-type: none"> <li>◆ Out-of-Band Mgmt Port <ul style="list-style-type: none"> <li>– Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port.</li> <li>– Options available: COM1/Serial Over LAN, COM2. Default setting is <b>COM1/Serial Over LAN</b>.</li> </ul> </li> <li>◆ Terminal Type <ul style="list-style-type: none"> <li>– Selects a terminal type to be used for console redirection.</li> <li>– Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is <b>ANSI</b>.</li> </ul> </li> <li>◆ Bits per second <ul style="list-style-type: none"> <li>– Selects the transfer rate for console redirection.</li> <li>– Options available: 9600, 19200, 38400, 57600, 115200. Default setting is <b>115200</b>.</li> </ul> </li> </ul> |

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



| Parameter   | Description   |
|---|---|
| Serial Port for Out-of-Band<br>EMS Console Redirection<br>Settings(continued) | <ul style="list-style-type: none"><li>◆ Flow Control<ul style="list-style-type: none"><li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li><li>– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is <b>None</b>.</li></ul></li></ul> |

## 5-2-7 CPU Configuration



| Parameter         | Description   |
|-------------------|---|
| SVM Mode          | Enable/Disable the CPU Virtualization.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                        |
| SMEE              | Controls the Secure Memory Encryption Enable (SMEE) function.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> . |
| CPU 0 Information | Press [Enter] to view more information related to CPU.  |

## 5-2-8 AMI Graphic Output Protocol Policy



| Parameter                   | Description                               |
|-----------------------------|---|
| ASPEED Graphics PCI Adapter |   |
| ASPEED Graphics Driver      |   |
| Output Select               | Press [Enter] to select output interface. |

## 5-2-9 PCI Subsystem Settings

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                            |           |   |
|----------------------------|-----------|---|
| PCI Bus Driver Version     | A5.01.19  | ▲ Change SLOT1_FRONT 1 PCIe lanes.<br><br>++: Select Screen<br>T1: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |
| SLOT1_FRONT Lanes          | [Auto]    |   |
| SLOT1_FRONT I/O ROM        | [Enabled] |   |
| SLOT1_FRONT Max Link Speed | [Auto]    |   |
| SLOT1_REAR Lanes           | [Auto]    |   |
| SLOT1_REAR ROM             | [Enabled] |   |
| SLOT1_REAR Max Link Speed  | [Auto]    |   |
| SLOT2_FRONT Lanes          | [Auto]    |   |
| SLOT2_FRONT I/O ROM        | [Enabled] |   |
| SLOT2_FRONT Max Link Speed | [Auto]    |   |
| SLOT2_REAR Lanes           | [Auto]    |   |
| SLOT2_REAR I/O ROM         | [Enabled] |   |
| SLOT2_REAR Max Link Speed  | [Auto]    |   |
| SLOT3 Lanes                | [Auto]    | ++: Select Screen<br>T1: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit   |
| SLOT3 I/O ROM              | [Enabled] |   |
| SLOT3 Max Link Speed       | [Auto]    |   |
| DCP1 Lanes                 | [Auto]    |   |
| DCP1 I/O ROM               | [Enabled] |   |
| DCP1 Max Link Speed        | [Auto]    |   |

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                              |           |  |
|------------------------------|-----------|--|
| SLOT2_REAR Max Link Speed    | [Auto]    | ▲ If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.<br><br>++: Select Screen<br>T1: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |
| SLOT3 Lanes                  | [Auto]    |  |
| SLOT3 I/O ROM                | [Enabled] |  |
| SLOT3 Max Link Speed         | [Auto]    |  |
| DCP1 Lanes                   | [Auto]    |  |
| DCP1 I/O ROM                 | [Enabled] |  |
| DCP1 Max Link Speed          | [Auto]    |  |
| DCP2 Lanes                   | [Auto]    |  |
| DCP2 I/O ROM                 | [Enabled] |  |
| DCP2 Max Link Speed          | [Auto]    |  |
| SLOT4 Lanes                  | [Auto]    |  |
| SLOT4 I/O ROM                | [Enabled] |  |
| SLOT4 Max Link Speed         | [Auto]    |  |
| Onboard LAN Controller       | [Enabled] | ++: Select Screen<br>T1: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit  |
| Onboard LAN1 I/O ROM         | [Enabled] |  |
| Onboard LAN2 I/O ROM         | [Enabled] |  |
| PCI Devices Common Settings: |           |  |
| Above 4G Decoding            | [Enabled] |  |
| SR-IOV Support               | [Enabled] |  |

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

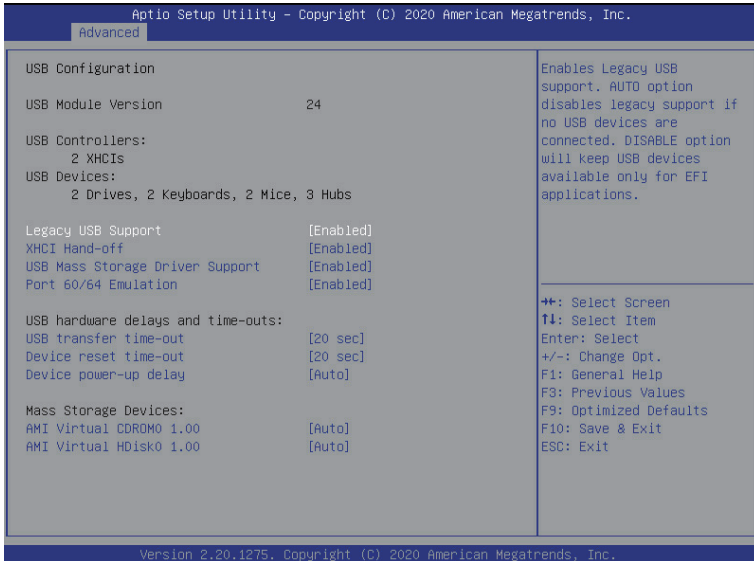
| Parameter                                      | Description  |
|--|--|
| PCI Bus Driver Version                         | Displays the PCI Bus Driver version information.   |
| SLOT_# <sup>(Note1)</sup> Lanes Configuration  | Change the PCIe lanes.<br>Options available: Disabled, Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is <b>Auto</b> .   |
| SLOT Express Slot # I/O ROM <sup>(Note1)</sup> | When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                |
| OCP# <sup>(Note2)</sup> Lanes                  | Change mezzanine PCIe lanes.<br>Options available: Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4, Disabled. Default setting is <b>Auto</b> .   |
| OCP# <sup>(Note2)</sup> I/O ROM                | When enabled, this setting will initialize the device expansion ROM for the related U.2 device.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                |
| OCP# <sup>(Note2)</sup> Max Link Speed         | Configure mezzanine PCIe max link speed.<br>Options available: Auto/Maximum/Gen1/Gen2/Gen3.<br>Default setting is <b>Auto</b> .  |
| Onboard LAN Controller <sup>(Note3)</sup>      | Enable/Disable the onboard LAN devices.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .  |
| Onboard LAN I/O ROM <sup>(Note3)</sup>         | Enable/Disable the onboard LAN devices, and initializes device expansion ROM.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                                  |
| PCI Devices Common Settings                    |  |
| Above 4G Decoding                              | Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding).<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                          |
| SR-IOV Support                                 | If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> . |

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

(Note2) This section is dependent on the available OCP connector.

(Note3) This section is dependent on the available LAN controller.

## 5-2-10 USB Configuration

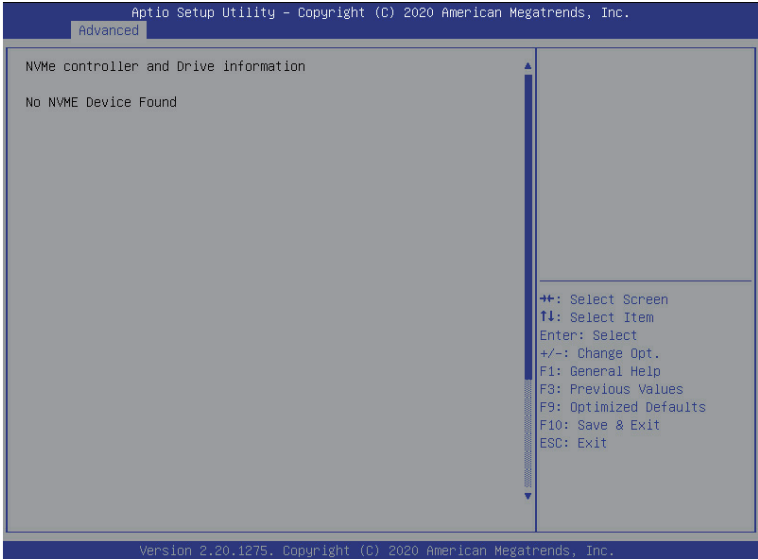


| Parameter   | Description   |
|---|---|
| USB Configuration                                 |   |
| USB Module Version                                | Displays the USB version.   |
| USB Controllers                                   | Displays the supported USB controllers.   |
| USB Devices                                       | Displays the USB devices connected to the system.   |
| Legacy USB Support                                | Enable/disable the Legacy USB support function. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.<br>Options available: Auto/Enabled/Disabled. Default setting is <b>Enabled</b> . |
| XHCI Hand-off                                     | Enable/Disable the XHCI (USB 3.0) Hand-off support.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .   |
| USB Mass Storage Driver Support <sup>(Note)</sup> | Enable/Disable the USB Mass Storage Driver Support.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .   |
| Port 60/64 Emulation                              | Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OS.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .   |
| USB hardware delays and time-outs                 |   |
| USB transfer time-out                             | The time-out value for Control, Bulk, and Interrupt transfers.<br>Options available: 1 sec/5 sec/10 sec/20 sec. Default setting is <b>20 sec</b> .  |

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

| Parameter  | Description  |
|--|--|
| Device reset time-out  | USB mass storage device Start Unit command time-out.<br>Options available: 10 sec/20 sec/30 sec/40 sec. Default setting is <b>20 sec.</b>  |
| Device power-up delay  | Maximum time the device will take before it properly reports itself to the Host Controller. "Auto" uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.<br>Options available: Auto/Manual. Default setting is <b>Auto.</b>                     |
| Mass Storage Devices   |  |
| AMI Virtual CDROM 1.00 /<br>AMI HDisk0 1.00 / Generic<br>Flash Disk 8.07 / ADATA USB<br>Flash Drive 1100 | Mass storage device emulation type. AUTO enumerates devices according to their media format. Optical drives are emulated as CDROM, drives with no media will be emulated according to a drive type.<br>Options available: Auto/Floppy/Forced FDD/Hard Disk/CD-ROM. Default setting is <b>Auto.</b> |

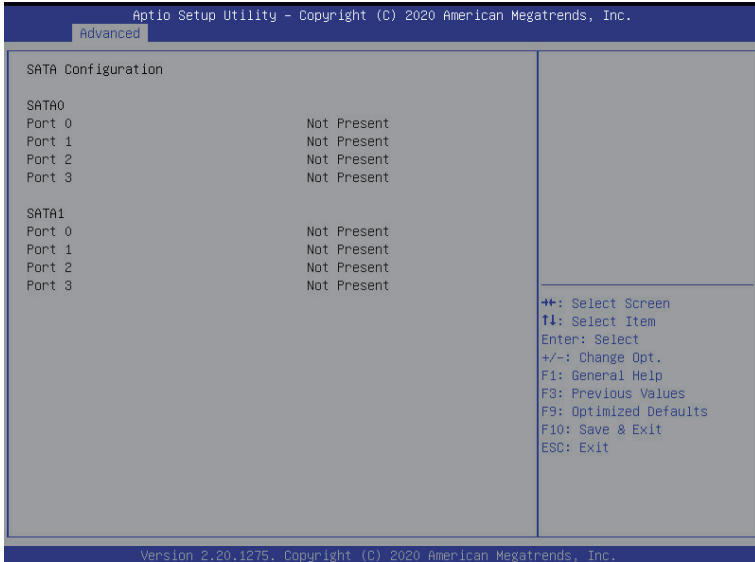
## 5-2-11 NVMe Configuration



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

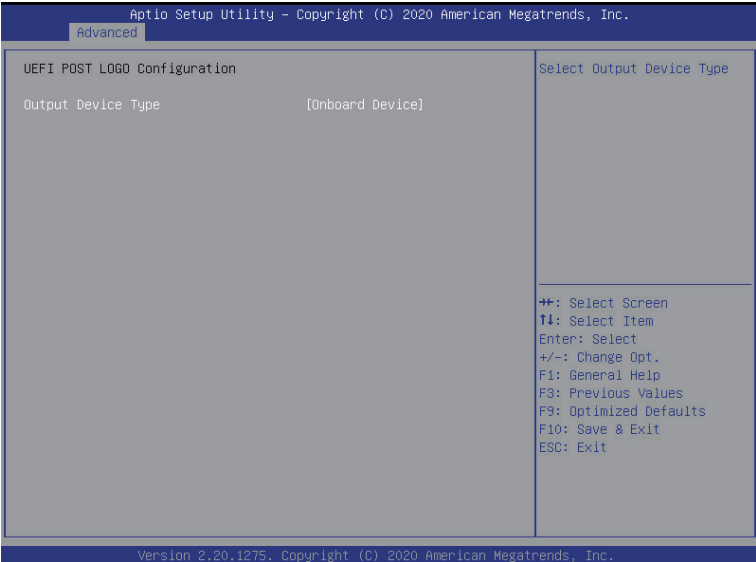


## 5-2-12 SATA Configuration



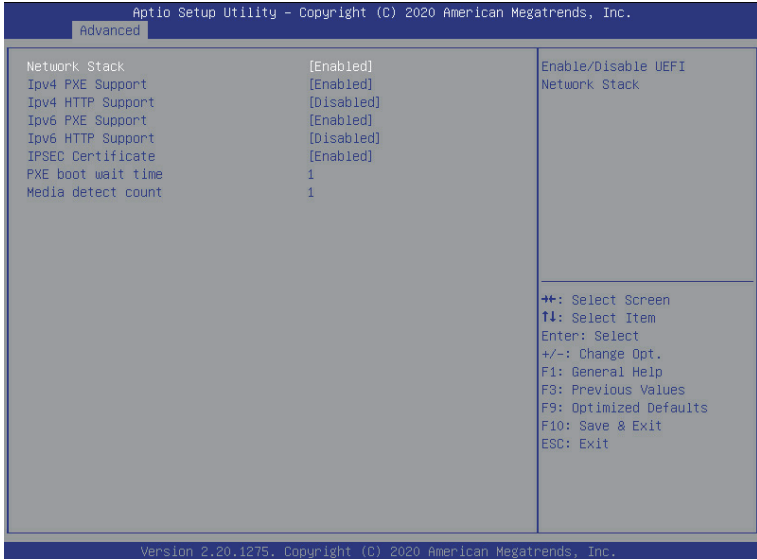
| Parameter          | Description  |
|--------------------|--|
| SATA Configuration | Displays the installed HDD devices information. System will automatically detect HDD type. |

## 5-2-13 UEFI Configuration



| Parameter          | Description                |
|--------------------|----------------------------|
| UEFI Configuration | Select output device type. |

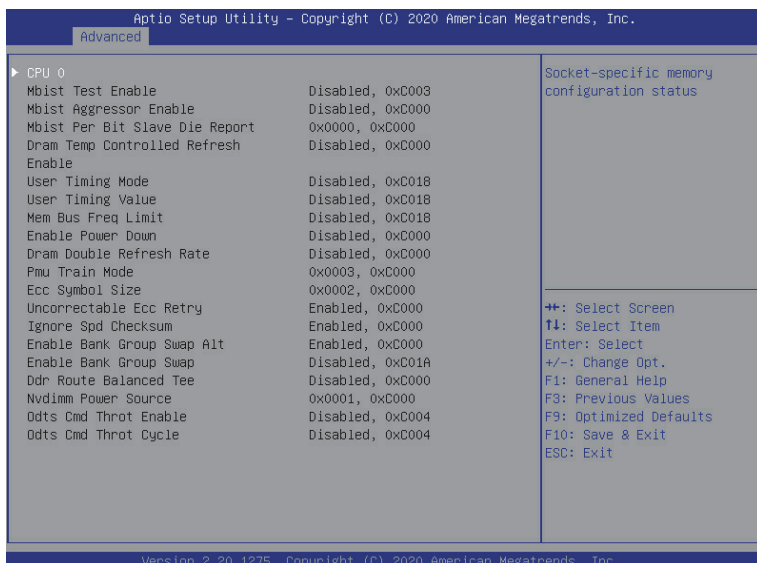
## 5-2-14 Network Stack Configuration



| Parameter                            | Description  |
|--------------------------------------|--|
| Network Stack                        | Enable/Disable the UEFI network stack.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                   |
| IPv4 PXE Support <sup>(Note)</sup>   | Enable/Disable the IPv4 PXE feature.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                     |
| IPv4 HTTP Support <sup>(Note)</sup>  | Enable/Disable the IPv4 HTTP feature.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .                   |
| IPv6 PXE Support <sup>(Note)</sup>   | Enable/Disable the IPv6 PXE feature.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .                     |
| IPv6 HTTP Support <sup>(Note)</sup>  | Enable/Disable the IPv6 HTTP feature.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .                   |
| IPSEC Certificate <sup>(Note)</sup>  | Enable/Disable the IPSEC Certificate feature.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .            |
| PXE boot wait time <sup>(Note)</sup> | 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 <sup>(Note)</sup> | Number of times the presence of media will be checked.<br>Press the <+> / <-> keys to increase or decrease the desired values.       |

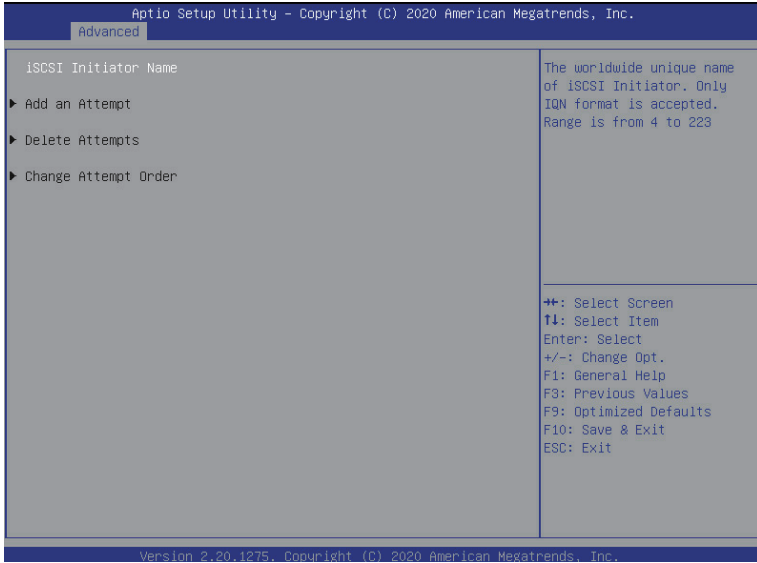
(Note) This item appears when **Network Stack** is set to **Enabled**.

## 5-2-15 AMD Mem Configuration Status



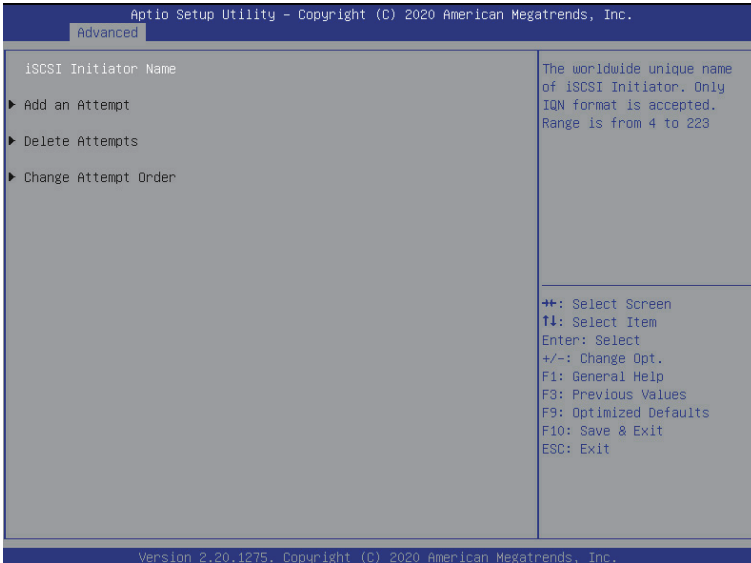
| Parameter | Description   |
|-----------|---|
| CPU0/1    | Press [Enter] to view the memory configuration status related to CPU 0. |

## 5-2-16 iSCSI Configuration



| Parameter            | Description   |
|----------------------|---|
| iSCSI Initiator Name | Press [Enter] and name iSCSI Initiator. Only IQN format is accepted. Range: from 4 to 223 |
| Add an Attempt       | Press [Enter] to configure advanced items.  |
| Delete Attempts      | Press [Enter] to configure advanced items.  |
| Change Attempt Order | Press [Enter] to configure advanced items.  |

## 5-2-17 Tls Auth Configuration



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

## 5-2-18 Intel(R) I350 Gigabit Network Connection

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                            |   |  |
|----------------------------|---|--|
| <p>▶ NIC Configuration</p> |   | <p>Click to configure the network device port.</p>   |
| <p>Blink LEDs</p>          | <p>0</p>  |  |
| <p>UEFI Driver</p>         | <p>Intel(R) PRO/1000 8.5.21<br/>PCI-E</p>           | <p>++: Select Screen<br/>↑↓: Select Item<br/>Enter: Select<br/>+/-: Change Opt.<br/>F1: General Help<br/>F9: Previous Values<br/>F9: Optimized Defaults<br/>F10: Save &amp; Exit<br/>ESC: Exit</p> |
| <p>Adapter PBA</p>         | <p>140422-008</p>                                   |  |
| <p>Device Name</p>         | <p>Intel(R) I350 Gigabit<br/>Network Connection</p> |  |
| <p>Chip Type</p>           | <p>Intel i350</p>                                   |  |
| <p>PCI Device ID</p>       | <p>1521</p>   |  |
| <p>PCI Address</p>         | <p>C3:00:00</p>                                     |  |
| <p>Link Status</p>         | <p>[Disconnected]</p>                               |  |
| <p>MAC Address</p>         | <p>B4:2E:99:AF:F3:06</p>                            |  |
| <p>Virtual MAC Address</p> | <p>00:00:00:00:00:00</p>                            |  |

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                    |                          |  |
|--------------------|--------------------------|--|
| <p>Link Speed</p>  | <p>[Auto Negotiated]</p> | <p>Specifies the port speed used for the selected boot protocol.</p> |
| <p>Wake On LAN</p> | <p>[Enabled]</p>         |  |

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

| Parameter           | Description  |
|---------------------|--|
| NIC Configuration   | <p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Link Speed <ul style="list-style-type: none"> <li>– Allows for automatic link speed adjustment.</li> <li>– Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. Default setting is <b>Auto Negotiated</b>.</li> </ul> </li> <li>◆ Wake On LAN <ul style="list-style-type: none"> <li>– Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states.</li> <li>– Options available: Enabled/Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> </ul> |
| Blink LEDs          | <p>Identifies the physical network port by blinking the associated LED.<br/>Press the numeric keys to adjust desired values.</p>   |
| UEFI Driver         | Displays the technical specifications for the Network Interface Controller.  |
| Adapter PBA         | Displays the technical specifications for the Network Interface Controller.  |
| Device Name         | Displays the technical specifications for the Network Interface Controller.  |
| Chip Type           | Displays the technical specifications for the Network Interface Controller.  |
| PCI Device ID       | Displays the technical specifications for the Network Interface Controller.  |
| PCI Address         | Displays the technical specifications for the Network Interface Controller.  |
| Link Status         | Displays the technical specifications for the Network Interface Controller.  |
| MAC Address         | Displays the technical specifications for the Network Interface Controller.  |
| Virtual MAC Address | Displays the technical specifications for the Network Interface Controller.  |



## 5-2-19 VLAN Configuration

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                   |            |  |
|-------------------|------------|--|
| Configured        | [Enabled]  | Indicate whether network address configured successfully or not. |
| Enable DHCP       | [Disabled] |  |
| Local IP Address  |            |  |
| Local NetMask     |            |  |
| Local Gateway     |            |  |
| Local DNS Servers |            |  |

Save Changes and Exit

++: Select Screen  
↑↓: Select Item  
Enter: Select  
+/-: Change Opt.  
F1: General Help  
F3: Previous Values  
F9: Optimized Defaults  
F10: Save & Exit  
ESC: Exit

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.

Advanced

|                 |   |   |
|-----------------|---|---|
| Create new VLAN |   | VLAN ID of new VLAN or existing VLAN, valid value is 0~4094 |
| VLAN ID         | 0 |   |
| Priority        | 0 |   |
| Add VLAN        |   |   |

Configured VLAN List

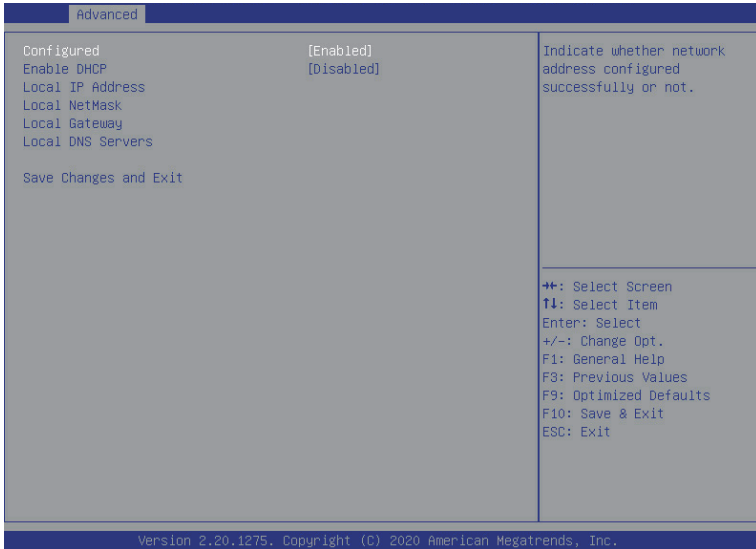
Remove VLAN

++: Select Screen  
↑↓: Select Item  
Enter: Select  
+/-: Change Opt.  
F1: General Help  
F3: Previous Values  
F9: Optimized Defaults  
F10: Save & Exit  
ESC: Exit

Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.

| Parameter                | Description   |
|--------------------------|---|
| Enter Configuration Menu | <p data-bbox="341 161 671 181">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="341 189 519 210">◆ Create new VLAN</li> <li data-bbox="341 217 447 238">◆ VLAN ID <ul style="list-style-type: none"> <li data-bbox="376 246 802 266">– Sets VLAN ID for a new VLAN or an existing VLAN.</li> <li data-bbox="376 274 934 294">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li data-bbox="376 302 663 323">– The valid range is from 0 to 4094.</li> </ul> </li> <li data-bbox="341 330 434 351">◆ Priority <ul style="list-style-type: none"> <li data-bbox="376 359 849 379">– Sets 802.1Q Priority for a new VLAN or an existing VLAN.</li> <li data-bbox="376 387 934 407">– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> <li data-bbox="376 415 636 435">– The valid range is from 0 to 7.</li> </ul> </li> <li data-bbox="341 443 461 464">◆ Add VLAN <ul style="list-style-type: none"> <li data-bbox="376 471 902 492">– Press [Enter] to create a new VLAN or update an existing VLAN.</li> </ul> </li> <li data-bbox="341 500 551 520">◆ Configured VLAN List</li> <li data-bbox="341 528 493 548">◆ Remove VLAN <ul style="list-style-type: none"> <li data-bbox="376 556 732 577">– Press [Enter] to remove an existing VLAN.</li> </ul> </li> </ul> |

## 5-2-20 MAC IPv4 Network Configuration



| Parameter                           | Description  |
|-------------------------------------|--|
| Configured                          | Indicates whether network address is configured successfully or not. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> . |
| Enable DHCP <sup>(Note)</sup>       | Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .   |
| Local IP Address <sup>(Note)</sup>  | Press [Enter] to configure local IP address.   |
| Local NetMask <sup>(Note)</sup>     | Press [Enter] to configure local NetMask.  |
| Local Gateway <sup>(Note)</sup>     | Press [Enter] to configure local Gateway   |
| Local DNS Servers <sup>(Note)</sup> | Press [Enter] to configure local DNS servers   |
| Save Changes and Exit               | Press [Enter] to save all configurations.  |

(Note) This item appears when **Configured** is set to **Enabled**.

## 5-2-21 MAC IPv6 Network Configuration

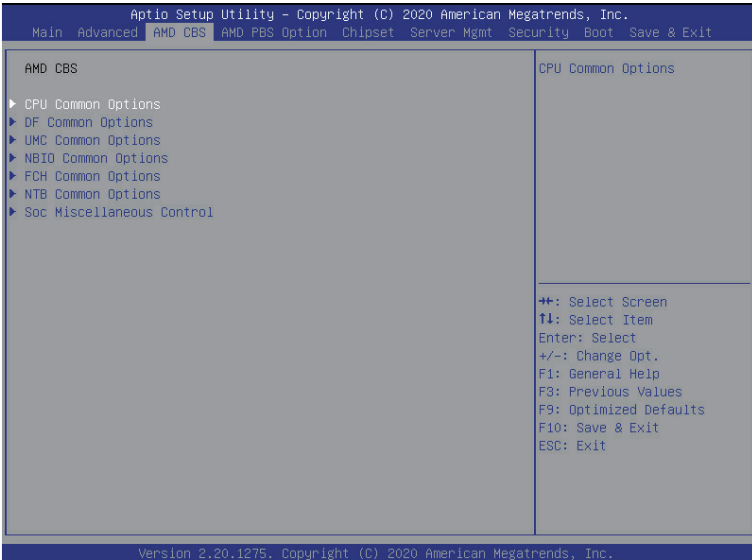
| Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.  |            |  |
|---|------------|--|
| Advanced  |            |  |
| Configured  | [Enabled]  | Indicate whether network address configured successfully or not. |
| Enable DHCP   | [Disabled] |  |
| Local IP Address  |            |  |
| Local NetMask   |            |  |
| Local Gateway   |            |  |
| Local DNS Servers   |            |  |
| Save Changes and Exit   |            |  |
| ++: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |            |  |
| Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.   |            |  |

| Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.  |                                |  |
|---|--------------------------------|--|
| Advanced  |                                |  |
| Interface Name  | : eth0                         | The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3 |
| Interface Type  | : Ethernet                     |  |
| MAC address   | : B4-2E-99-AF-F3-06            |  |
| Host addresses  | : FE80::B62E:99FF:FEAF:F306/64 |  |
| Route Table   | : FE80::/64 >>::               |  |
| Gateway addresses   | : FE80::/64 >>::               |  |
| DNS addresses   | : FE80::/64 >>::               |  |
| Interface ID  | : B6:2E:99:FF:FE:AF:F3:6       |  |
| DAD Transmit Count  | : 1                            |  |
| Policy  | : [automatic]                  |  |
| Save Changes and Exit   |                                |  |
| ++: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/-: Change Opt.<br>F1: General Help<br>F3: Previous Values<br>F9: Optimized Defaults<br>F10: Save & Exit<br>ESC: Exit |                                |  |
| Version 2.20.1275. Copyright (C) 2020 American Megatrends, Inc.   |                                |  |

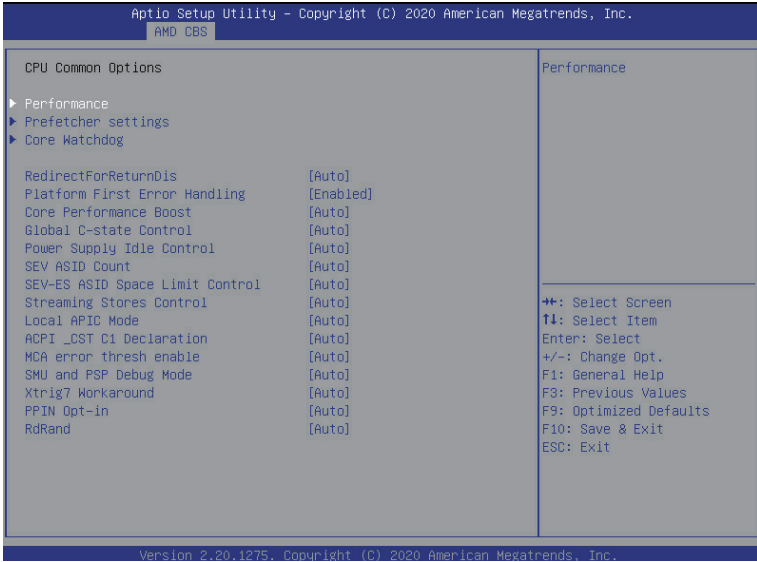
| Parameter                | Description  |
|--------------------------|--|
| Enter Configuration Menu | <p data-bbox="338 174 671 197">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="338 202 682 225">◆ Displays the MAC Address information.</li> <li data-bbox="338 230 937 315">◆ Interface ID <ul style="list-style-type: none"> <li data-bbox="376 260 937 315">– The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3.</li> </ul> </li> <li data-bbox="338 319 937 459">◆ DAD Transmit Count <ul style="list-style-type: none"> <li data-bbox="376 349 937 459">– The number of consecutive Neighbor solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.</li> </ul> </li> <li data-bbox="338 464 916 519">◆ Policy <ul style="list-style-type: none"> <li data-bbox="376 493 916 519">– Options available: automatic/manual. Default setting is <b>automatic</b>.</li> </ul> </li> <li data-bbox="338 523 703 578">◆ Save Changes and Exit <ul style="list-style-type: none"> <li data-bbox="376 553 703 578">– Press [Enter] to save all configurations.</li> </ul> </li> </ul> |

## 5-3 AMD CBS Menu

AMD CBS menu displays submenu options for configuring the CPU-related information that the BIOS automatically sets. Select a submenu item, then press [Enter] to access the related submenu screen.



### 5-3-1 CPU Common Options

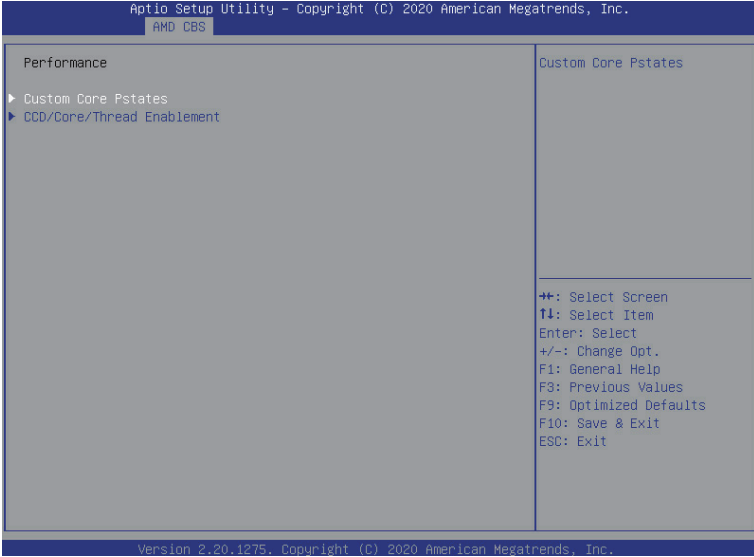


| Parameter                     | Description  |
|-------------------------------|--|
| CPU Common Options            |  |
| Performance                   | Press [Enter] for configuration of advanced items.   |
| Prefetcher settings           | Press [Enter] for configuration of advanced items.   |
| Core Watchdog                 | Press [Enter] for configuration of advanced items.   |
| RedirectForReturnDis          | From a workaround for GCC/C000005 issue for XV Core on CZ A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrcForReturns] to 1.<br>Options available: Auto, 1, 0. Default setting is <b>Auto</b> . |
| Platform First Error Handling | Enable/Disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Core Performance Boost        | Enable/Disable the Core Performance Boost function.<br>Options available: Auto/Disabled. Default setting is <b>Auto</b> .  |
| Global C-State Control        | Controls the IO based C-state generation and DF C-states.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Power Supply Idle Control     | Configures the Power Supply Idle Control.<br>Options available: Auto, Low Current Idle, Typical Current Idle. Default setting is <b>Auto</b> .   |
| SEV ASID Count                | Specifies the maximum valid ASID, which affects the maximum system physical address space.<br>Options available: Auto, 253 ASIDs, 509 ASIDs. Default setting is <b>Auto</b> .  |

| <b>Parameter</b>                | <b>Description</b>  |
|---------------------------------|---|
| SEV-ES ASID Space Limit Control | Space limit control for SEV-ES ASIDs.<br>Options available: Auto/Manual. Default setting is <b>Auto</b> .   |
| Streaming Stores Control        | Enable/Disable the Streaming Stores functionality.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Local APIC Mode                 | Sets the Local APIC Mode.<br>Options available: Auto, xAPIC, x2APIC. Default setting is <b>Auto</b> .   |
| ACPI_CST C1 Decaration          | Determines whether or not to declare the C1 state to the OS..<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| MCA error thresh enable         | Enable MCA error thresholding.<br>Options available: Auto, False, True. Default setting is <b>Auto</b> .  |
| SMU and PSP Debug Mode          | When this option is enabled, specific uncorrected errors detected by the PSP FW or SMU FW will hand and not reset the system.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| Xtrig7 Workaround               | Options available: Auto, No Workaround, Bronze Workaround, Sliver Workaround. Default setting is <b>Auto</b> .  |
| PPIN Opt-in                     | Enable/Disable the PPIN feature.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| RdRand                          | Enable/Disable RdRand instruction.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |



### 5-3-1-1 Performance



| Parameter                  | Description  |
|----------------------------|--|
| Performance                |  |
| Custom Core Pstates        | Allows you to accept or decline enabling Custom Core Pstates. When accepted, you can disable or customize core pstates.  |
| CCD/Core/Thread Enablement | Allows you to accept or decline enabling CCDs, processor cores and threads. When accepted, you can control the number of CCDs to be used, the number of cores to be used, and whether to enable or disable Simultaneous Multithreading Technology (SMT) support. |

## 5-3-1-2 Prefetcher Settings



| Parameter               | Description   |
|-------------------------|---|
| Prefetcher settings     |   |
| L1 Stream HW Prefetcher | Enable/Disable L1 Stream HW Prefetcher.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| L2 Stream HW Prefetcher | Enable/Disable L2 Stream HW Prefetcher.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |

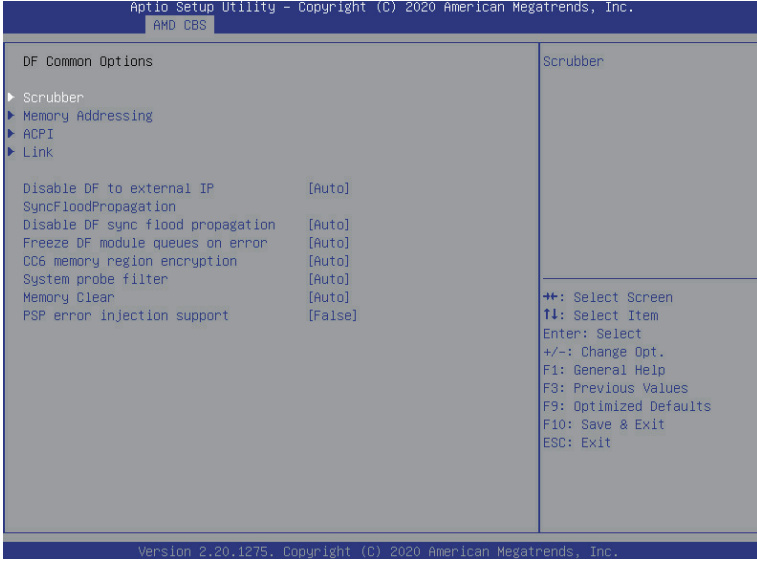
### 5-3-1-3 Core Watchdog



| Parameter   | Description   |
|---|---|
| <b>Core Watchdog</b>                                  |   |
| Core Watchdog Timer Enable                            | Enable/Disable CPU Watchdog Timer.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .          |
| Core Watchdog Timer Interval <sup>(Note)</sup>        | Enable/Disable CPU Watchdog Timer Interval.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| Core Watchdog Timer Enable Severity <sup>(Note)</sup> | Enable/Disable CPU Watchdog Timer Severity.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |

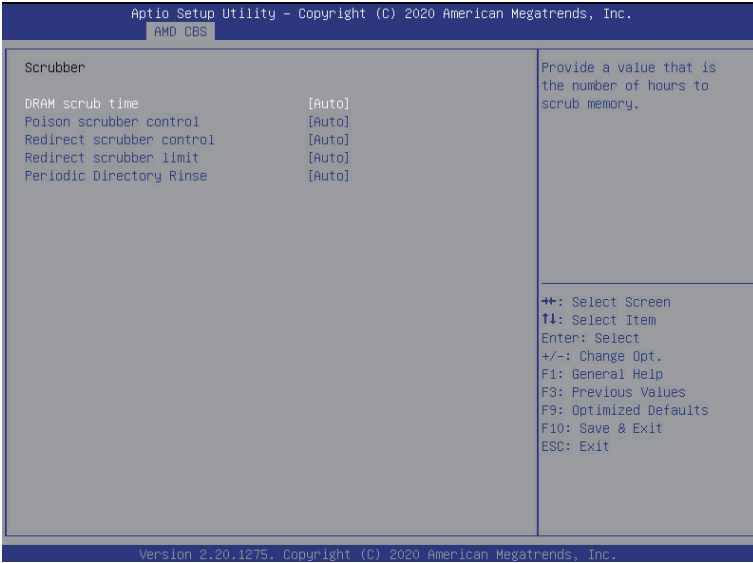
(Note) This item appears when **Core Watchdog Timer Enable** is set to **Enabled**.

## 5-3-2 DF Common Options



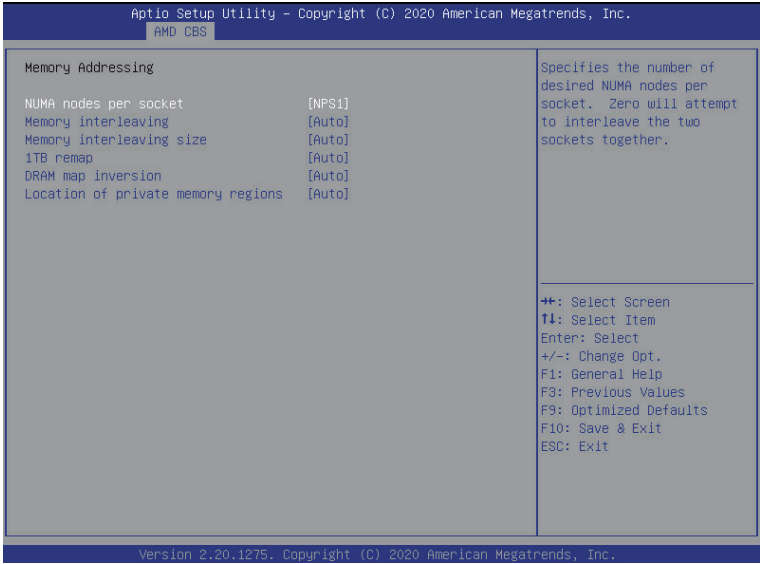
| Parameter   | Description   |
|---|---|
| DF Common Options                                   |   |
| Scrubber  | Press [Enter] for configuration of advanced items.  |
| Memory Addressing                                   | Press [Enter] for configuration of advanced items.  |
| ACPI  | Press [Enter] for configuration of advanced items.  |
| Link  | Press [Enter] for configuration of advanced items.  |
| Disable DF to external IP<br>sync flood propagation | Enable/Disable SyncFlood to UMC & downstream slaves.<br>Options available: Auto, Sync flood disabled, Sync flood enabled.<br>Default setting is <b>Auto</b> . |
| Disable DF sync flood<br>propagation                | Enable/Disable DF Sync Flood propagation.<br>Options available: Auto, Sync flood disabled, Sync flood enabled.<br>Default setting is <b>Auto</b> .            |
| Freeze DF module queues on<br>error                 | Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| CC6 memory region encryption                        | Controls whether or not the CC6 save/restor memory is encrypted.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .              |
| System probe filter                                 | Enable/Disable System probe filter.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| Memory Clear  | Enable/Disable the Memory Clear feature.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                                      |
| PSP error injection support                         | Enable/Disable PSP error injection support.<br>Options available: False/True. Default setting is <b>False</b> .   |

### 5-3-2-1 Scrubber



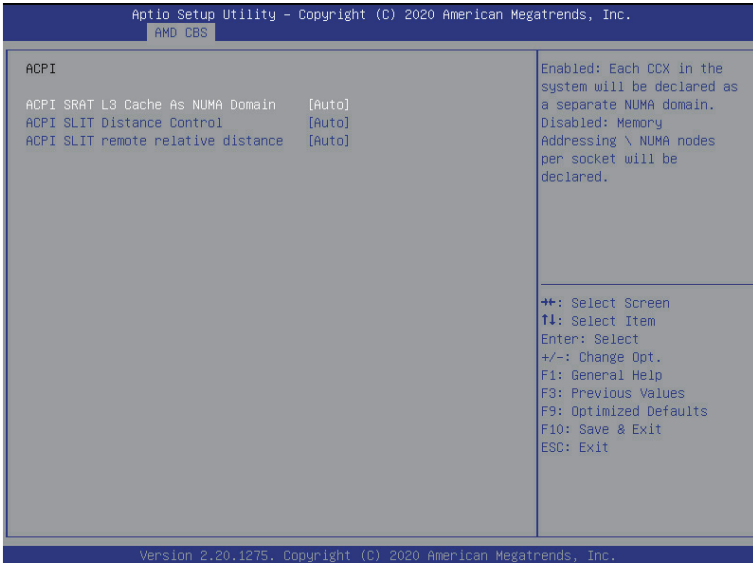
| Parameter                 | Description   |
|---------------------------|---|
| Scrubber                  |   |
| DRAM scrub time           | Provide a value that is the number of hours to scrub memory.<br>Options available: Auto, Disabled, 1 hour, 4 hours, 8 hours, 16 hours, 24 hours, 48 hours. Default setting is <b>Auto</b> . |
| Poison scrubber control   | Enable/Disable the Poison scrubber control feature.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| Redirect scrubber control | Enable/Disable the Redirect scrubber control feature.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| Redirect scrubber limit   | Sets the redirect scrubber limit.<br>Options available: Auto, 2, 4, 8, Infinite. Default setting is <b>Auto</b> .   |
| Periodic Directory Rinse  | Control Periodic Directory Rinse Mode<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |

### 5-3-2-2 Memory Addressing



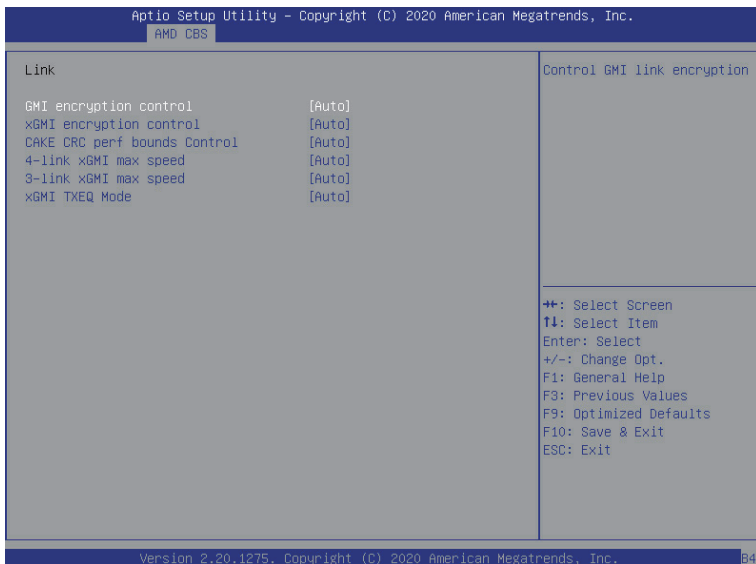
| Parameter                          | Description  |
|------------------------------------|--|
| Memory Addressing                  |  |
| NUMA nodes per socket              | Specifies the number of desired NUMA nodes per socket.<br>Options available: Auto, NPS0, NPS1, NPS2, NPS4. Default setting is <b>Auto</b> .  |
| Memory inerleaving                 | Enable/Disable the Memory interleaving feature.<br>Options available: Auto/Disabled. Default setting is <b>Auto</b> .  |
| Memory interleaving size           | Controls the memory interleaving size. This determines the starting address of the interleave (bit 8, 9, 10 or 11).<br>Options available: Auto, 256Bytes, 512Bytes, 1KB, 2KB. Default setting is <b>Auto</b> .   |
| 1TB remap                          | Enable/Disable to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection, and may not always be possible.<br>Options available: Auto, Do not remap, Attempt to remap.<br>Default setting is <b>Auto</b> .  |
| DRAM map inversion                 | Enable/Disable the DRAM map inversion function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Location of private memory regions | Control whether or not the rprivate memory regions (PSP, SMU, and CC6) are at the top of DRAM or distributed. Note that distributed requires memory on all dies. Note that it will always be at the top of DRAM if some dies don't have memory regardless of this.<br>Options available: Auto, Distributed, Consolidated. Default setting is <b>Auto</b> . |

### 5-3-2-3 ACPI



| Parameter                          | Description  |
|------------------------------------|--|
| ACPI                               |  |
| ACPI SRAT L3 Cache As NUMA Domain  | Enable/Disable the ACPI SRAT L3 Cache As NUMA Domain function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .     |
| ACPI SLIT Distance Control         | Determines how the SLIT distances are declared.<br>Options available: Auto/Manual. Default setting is <b>Auto</b> .                                |
| ACPI SLIT remote relative distance | Sets the remote socket distance for 2P systems as near (2.8) or far (3.2).<br>Options available: Auto, Near, Far. Default setting is <b>Auto</b> . |

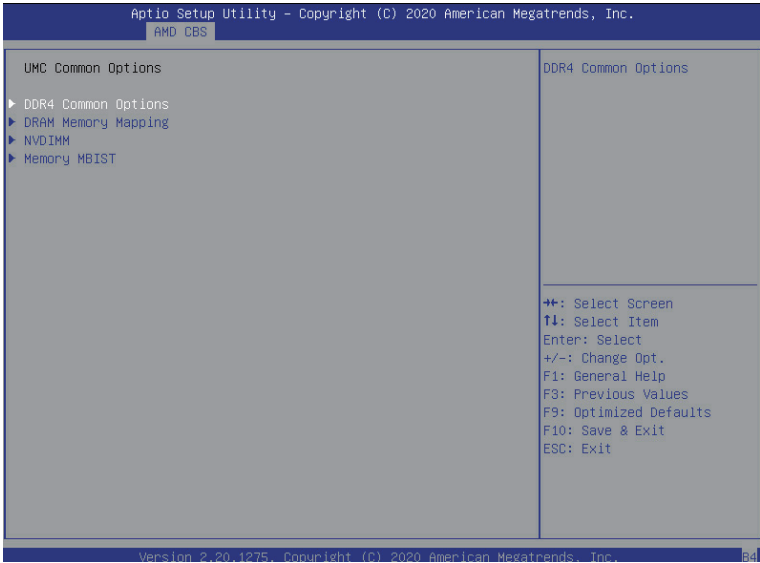
## 5-3-2-4 Link



| Parameter                    | Description  |
|------------------------------|--|
| Link                         |  |
| GMI encryption control       | Enable/Disable GMI link encryption.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| xGMI encryption control      | Enable/Disable xGMI link encryption.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                                       |
| CAKE CRC perf bounds Control | Options available: Auto/Manual. Default setting is <b>Auto</b> .   |
| 4-link xGMI max speed        | Specifies the max speed of 4-link xGMI.<br>Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps.<br>Default setting is <b>10.667Gbps</b> .          |
| 3-link xGMI max speed        | Specifies the max speed of 3-link xGMI.<br>Options available: Auto, 10.667Gbps, 13Gbps, 16Gbps, 18Gbps.<br>Default setting is <b>10.667Gbps</b> .          |
| xGMI TXEQ Mode               | Configures xGMI TXEQ/RX vetting Mode.<br>Options available: Auto, TXEQ_Disabled, TXEQ_Lane, TXEQ_Link, TXEQ_RX_Vet. Default setting is <b>10.667Gbps</b> . |

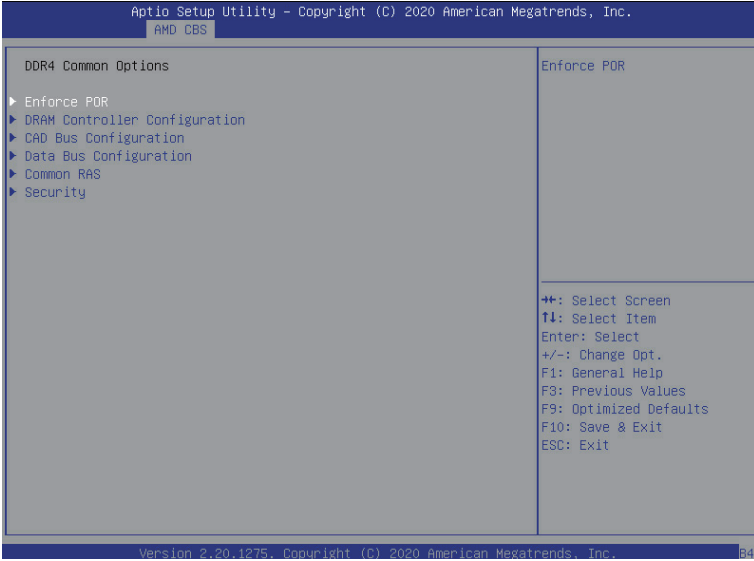


### 5-3-3 UMC Common Options



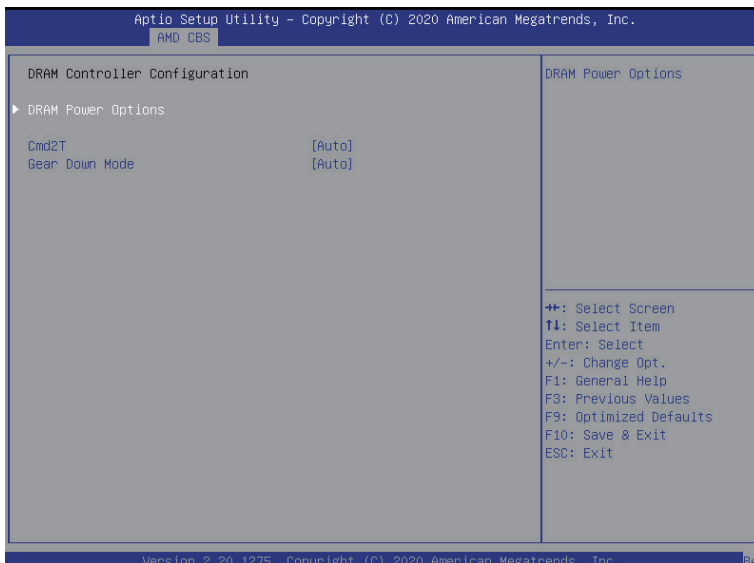
| Parameter           | Description  |
|---------------------|--|
| UMC Common Options  |  |
| DDR4 Common Options | Press [Enter] for configuration of advanced items. |
| DRAM Memory Mapping | Press [Enter] for configuration of advanced items. |
| NVDIMM              | Press [Enter] for configuration of advanced items. |
| Memory MBIST        | Press [Enter] for configuration of advanced items. |

### 5-3-3-1 DDR4 Common Options



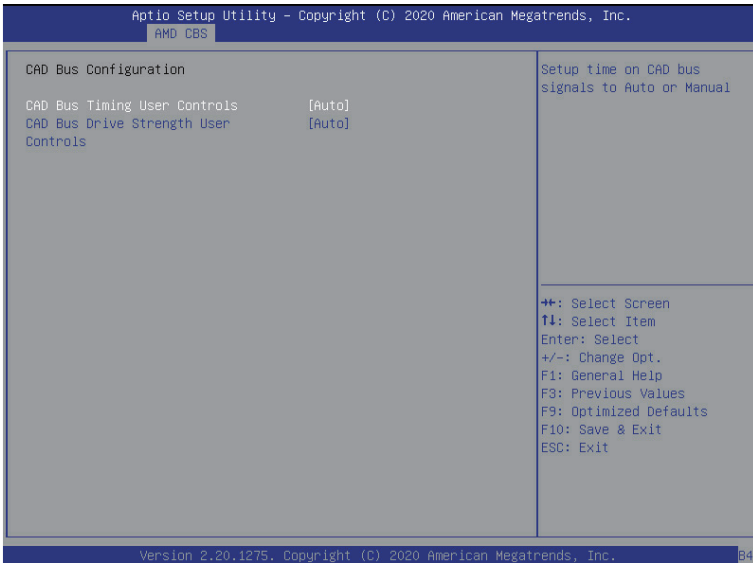
| Parameter                     | Description  |
|-------------------------------|--|
| DDR4 Common Options           |  |
| Enforce POR                   | Press [Enter] to configure the Plan of Record (POR) to enable / disable restrictions for DDR4 frequency and voltage programming. Memory speeds will be capped at AMD guidelines.<br><b>Note: To enable 2 DIMMs per Channel at 3200MHz function, select [Accept] at warning message, change Overclock from [Auto] to [Enabled], and then set memory speed to 3200MHz.</b> |
| DRAM Controller Configuration | Press [Enter] to configure DRAM Controller Configuration.  |
| CAD Bus Configuration         | Press [Enter] to configure CAD Bus Configuration.  |
| Data Bus Configuration        | Press [Enter] to configure Data Bus Configuration.   |
| Common RAS                    | Press [Enter] to configure Common RAS.   |
| Security                      | Press [Enter] to configure Security.   |

## 5-3-3-1-1 DRAM Controller Configuration



| Parameter                     | Description   |
|-------------------------------|---|
| DRAM Controller Configuration |   |
| DRAM Power Options            | <p>Press [Enter] to configure DRAM Power OptionsMa.</p> <ul style="list-style-type: none"> <li>◆ Power Down Enable               <ul style="list-style-type: none"> <li>– Enable/Disable DDR power down mode.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul> |
| Cmd2T                         | <p>Selects the Cmd2T mode on ADDR/CMD.</p> <p>Options available: Auto, 1T, 2T. Default setting is <b>Auto</b>.</p>  |
| Gear Down Mode                | <p>Enable/Disable the Gear Down Mode function.</p> <p>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</p>   |

## 5-3-3-1-2 CAD Bus Configuration



| Parameter                            | Description  |
|--------------------------------------|--|
| CAD Bus Configuration                |  |
| CAD Bus Timing User Controls         | Setup time on CAD bus signals to Auto or Manual.<br>Options available: Auto/Manual. Default setting is <b>Auto</b> .     |
| CAD Bus Drive Strength User Controls | Drive Strength on CAD bus signals to Auto or Manual.<br>Options available: Auto/Manual. Default setting is <b>Auto</b> . |

### 5-3-3-1-3 Data Bus Configuration



| Parameter                            | Description   |
|--------------------------------------|---|
| Data Bus Configuration               |   |
| Data Bus Configuration User Controls | Specifies the mode for drive strength to Auto or Manual. Options available: Auto/Manual. Default setting is <b>Auto</b> . |

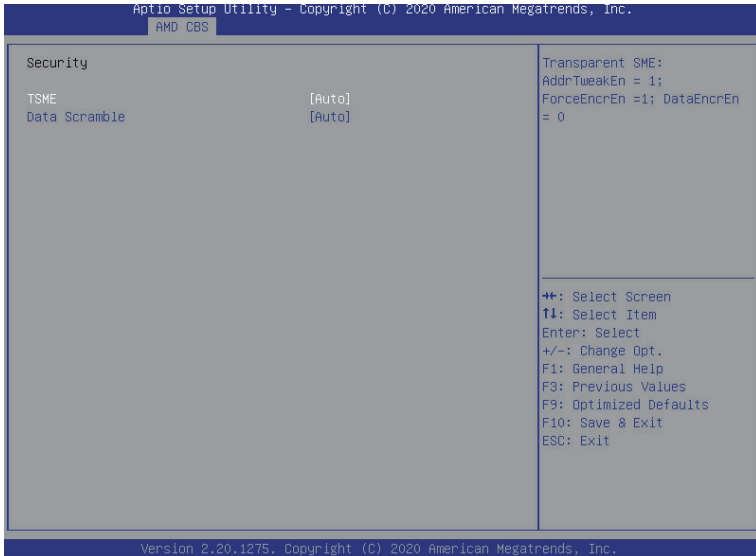
### 5-3-3-1-4 Common RAS



| Parameter                             | Description  |
|---------------------------------------|--|
| Common RAS                            |  |
| Data Poisoning                        | Enable/Disable the Data Poisoning function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| DRAM Post Package Repair              | Enable/Disable the DRAM Post Package Repair function.<br>Options available: Enabled/Disabled. Default setting is <b>Auto</b> .   |
| RCD Parity                            | Enable/Disable the RCD Parity function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| DRAM Address Command Parity Retry     | Enable/Disable the DRAM Address Command Parity Retry function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| Max Parity Error Replay               | Configures the Max Parity Error Replay. (0-0x3f)<br>Default setting is <b>8</b> .<br><b>Please note that this item is configurable when DRAM Address Command Parity Retry is set to Enabled.</b> |
| Write CRC Enable                      | Enable/Disable the Write CRC function.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| DRAM Write CRC Enable and Retry Limit | Enable/Disable DRAM Write CRC Enable and Retry Limit.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .<br>Configures the Max Write CRC Error Replay. (0-0x3f)     |
| Max Write CRC Error Replay            | Default setting is <b>8</b> .<br><b>Please note that this item is configurable when DRAM Write CRC Enable and Retry Limit is set to Enabled.</b>   |

| Parameter                      | Description   |
|--------------------------------|---|
| Disable Memory Error Injection | Options available: False/True. Default setting is <b>True</b> .   |
| ECC Configuration              | <p data-bbox="396 189 732 213">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="396 221 954 299">◆ DRAM ECC Symbol Size <ul style="list-style-type: none"> <li data-bbox="434 247 783 271">– Configures the DRAM ECC Symbol Size.</li> <li data-bbox="434 272 926 296">– Options available: Auto, x4, x8, x16. Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="396 307 954 417">◆ DRAM ECC Enable <ul style="list-style-type: none"> <li data-bbox="434 333 942 388">– Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable.</li> <li data-bbox="434 393 954 448">– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li data-bbox="396 453 954 561">◆ DRAM UECC Retry <ul style="list-style-type: none"> <li data-bbox="434 479 742 503">– Enable/Disable DRAM UECC Retry.</li> <li data-bbox="434 508 954 561">– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul> |

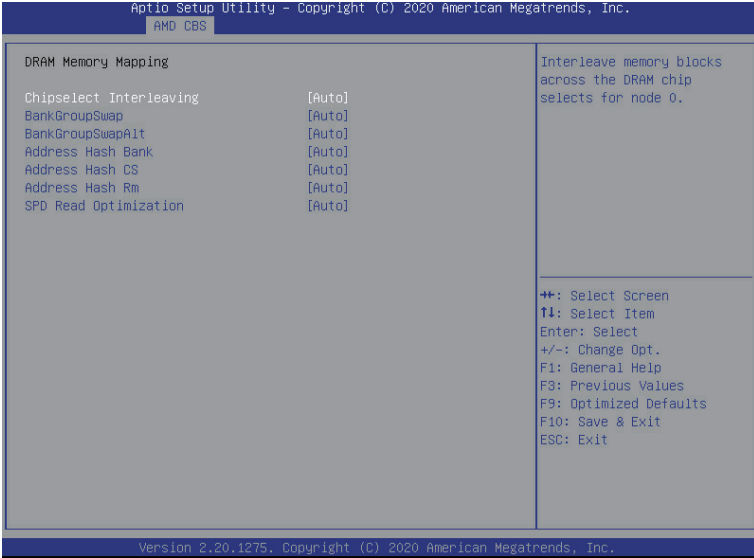
### 5-3-3-1-5 Security



| Parameter     | Description   |
|---------------|---|
| Security      |   |
| TSME          | Enable/Disable Transparent SME.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| Data Scramble | Enable/Disable Data Scrambling.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |



### 5-3-3-2 DRAM Memory Mapping



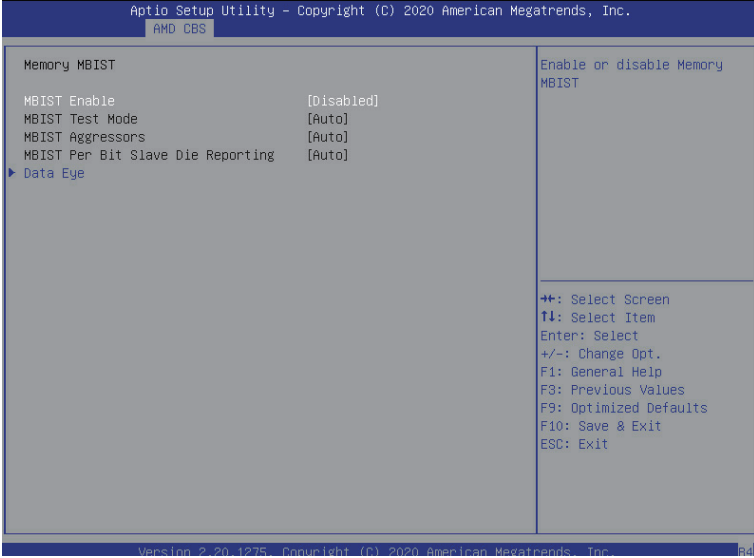
| Parameter               | Description   |
|-------------------------|---|
| DRAM Memory Mapping     |   |
| Chipselect Interleaving | Interleave memory blocks across the DRAM chip selects for CPU 0.<br>Options available: Auto/Disabled. Default setting is <b>Auto</b> .  |
| BankGroupSwap           | Configures the BankGroupSwap. BankGroupSwap (BGS) is a new memory mapping option in AGESA that alters how applications get assigned to physical locations within the memory modules. When this option sets to Auto, it is null: No help string.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| BankGroupSwapAlt        | Configures the BankGroupSwapAlt.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Address Hash Bank       | Enable/Disable bank address hashing.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Address Hash CS         | Enable/Disable CS address hashing.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>  |
| Address Hash Rm         | Enable/Disable RM address hashing.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>  |
| SPD Read Optimization   | Enable/Disable SPD Read Optimization.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>   |

### 5-3-3-3 NVDIMM



| Parameter | Description  |
|-----------|--|
| NVDIMM    | Disable NVDIMM-N feature for memory margin tool.<br>Options available: No, Yes. Default setting is <b>No</b> . |

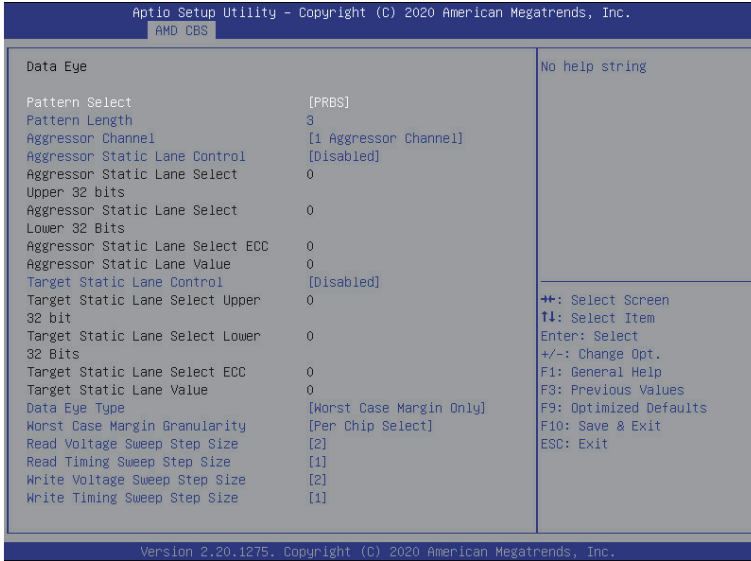
### 5-3-3-4 Memory MBIST



| Parameter   | Description  |
|---|--|
| Memory MBIST  |  |
| MBIST Enable  | Enable/Disable the Memory MBIST function.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .   |
| MBIST Test Mode <sup>(Note)</sup>                   | Selects MBIST Test Mode.<br><b>Interface Mode:</b> Tests Single and Multiple CS transactions and Basic Connectivity.<br><b>Data Eye Mode:</b> Measures Voltage vs. Timing.<br>Options available: Auto, Both, Interface Mode, Data Eye Mode. Default setting is <b>Auto</b> . |
| MBIST Aggressors <sup>(Note)</sup>                  | Enable/Disable MBIST Aggressor test.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| MBIST Per Bit Slave Die Reporting <sup>(Note)</sup> | Enable/Disable to report 2D data eye results in ABL log for each DQ, Chipselect, and Channel.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .  |
| Data Eye  | Press [Enter] to configure advanced items.   |

(Note) This item appears when **MBIST Enable** is set to **Enabled**.

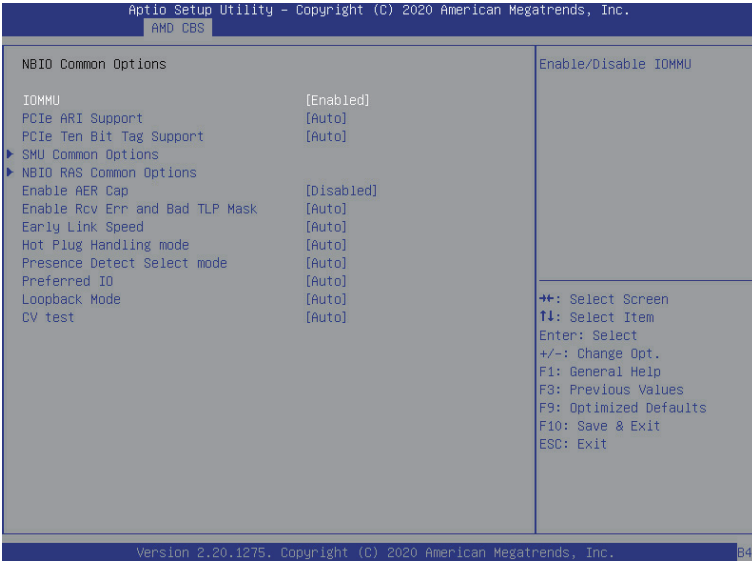
## 5-3-3-4-1 Data Eye



| Parameter                                  | Description  |
|--|--|
| Data Eye                                   |  |
| Pattern Select                             | Options available: PRBS, SSO, Both. Default setting is <b>PRBS</b> .   |
| Pattern Length                             | Determines the pattern length. The possible options are N=3....12.   |
| Aggressor Channel                          | This item helps read the aggressors channels.<br>Options available: Disabled, 1 Aggressor Channel, 3 Aggressor Channels, 7 Aggressor Channels. Default setting is <b>1 Aggressor Channel</b> . |
| Aggressor Static Lane Control              | Enable/Disable the Aggressor Static Lane Control function.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .  |
| Aggressor Static Lane Select Upper 32 bits | This item is configurable when <b>Aggressor Static Lane Control</b> is set to <b>Enabled</b> .   |
| Aggressor Static Lane Select Lower 32 bits | This item is configurable when <b>Aggressor Static Lane Control</b> is set to <b>Enabled</b> .   |
| Aggressor Static Lane Select ECC           | This item is configurable when <b>Aggressor Static Lane Control</b> is set to <b>Enabled</b> .   |
| Aggressor Static Lane Value                | This item is configurable when <b>Aggressor Static Lane Control</b> is set to <b>Enabled</b> .   |
| Target Static Lane Control                 | Enable/Disable the Target Static Lane Control function.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .   |

| Parameter                               | Description   |
|---|---|
| Target Static Lane Select Upper 32 bits | This item is configurable when <b>Target Static Lane Control</b> is set to <b>Enabled</b> .   |
| Target Static Lane Select Lower 32 bits | This item is configurable when <b>Target Static Lane Control</b> is set to <b>Enabled</b> .   |
| Target Static Lane Select ECC           | This item is configurable when <b>Target Static Lane Control</b> is set to <b>Enabled</b> .   |
| Target Static Lane Value                | This item is configurable when <b>Target Static Lane Control</b> is set to <b>Enabled</b> .   |
| Data Eye Type                           | This item determines which results are expected to be captured for Data Eye. Options available: 1D Voltage Sweep, 1D Timing Sweep, 2D Full Data Eye, Worst Case Margin Only. Default setting is <b>Worst Case Margin Only</b> . |
| Worst Case Margin Granularity           | Configures Worst Case Margin Granularity. Options available: Per Chip Select, Per Nibble. Default setting is <b>Worst Case Margin Only</b> .  |
| Read Voltage Sweep Step Size            | Configures the step size for read Data Eye voltage sweep. Options available: 1, 2, 4. Default setting is <b>2</b> .   |
| Read Timing Sweep Step Size             | Configures the step size for read Data Eye timing sweep. Options available: 1, 2, 4. Default setting is <b>1</b> .  |
| Write Voltage Sweep Step Size           | Configures the step size for write Data Eye voltage sweep. Options available: 1, 2, 4. Default setting is <b>2</b> .  |
| Write Timing Sweep Step Size            | Configures the step size for write Data Eye timing sweep. Options available: 1, 2, 4. Default setting is <b>1</b> .   |

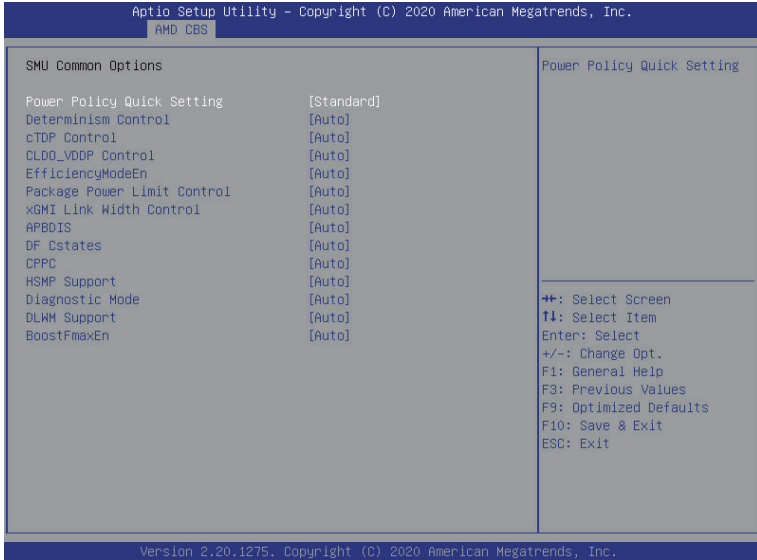
### 5-3-4 NBIO Common Options



| Parameter                | Description   |
|--------------------------|---|
| NBIO Common Options      |   |
| IOMMU                    | Enable/Disable the IOMMU function.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .   |
| PCIe ARI Support         | Enable/Disable Alternative Routing-ID Interpretation.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                   |
| PCIe Ten Bit Tag Support | Enable/Disable PCIe ten bit tags for supported devices. (Auto=Disabled)<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| SMU Common Options       | Press [Enter] for configuration of advanced items.  |
| NBIO RAS Common Options  | Press [Enter] for configuration of advanced items.  |
| Enable AER Cap           | Enable/Disable Advanced Error Reporting Capability.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                     |
| Early Link Speed         | Configures Early Link Speed.<br>Options available: Auto, Gen1, Gen2. Default setting is <b>Auto</b> .   |

| Parameter                   | Description  |
|-----------------------------|--|
| Hot Plug Handling mode      | Controls the Hot Plug Handling mode.<br>Options available: Auto, A0 Mode, OS First (No Error Handling), OS First (Error Handling-Not Implemented), Firmware First (Not Implemented).<br>Default setting is <b>Auto</b> . |
| Presence Detect Select mode | Controls the Presence Detect Select mode.<br>Options available: Auto, OR, AND. Default setting is <b>Auto</b> .  |
| Preferred IO Device         | Configures Preferred IO Device.<br>Options available: Auto, Manual. Default setting is <b>Auto</b> .   |
| Loopback Mode               | Enabled/Disabled PCIe Loopback mode.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| CV test                     | Set this to Enabled to support running PCIECV tool.<br>Auto: preserve hardware defaults.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |

### 5-3-4-1 SMU Common Options

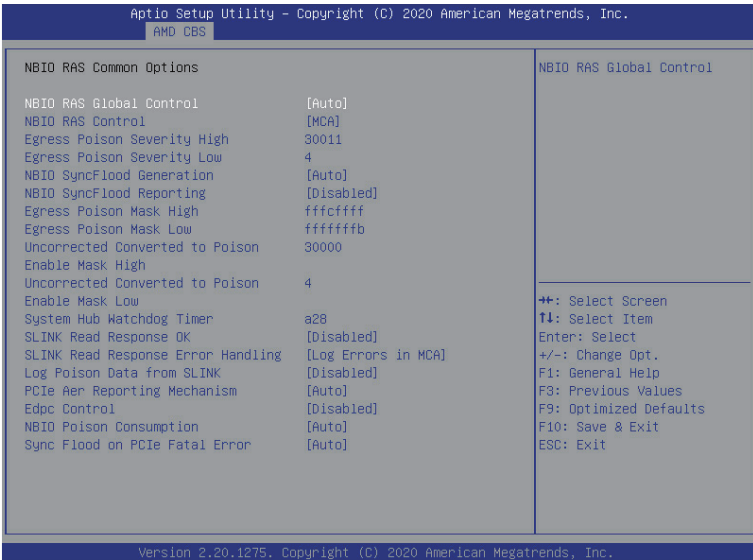


| Parameter                   | Description   |
|-----------------------------|---|
| SMU Common Options          |   |
| Power Policy Quick Setting  | Options available: Standard, Best Performance, Energy Efficient. Default setting is <b>Standard</b> .   |
| Determinism Control         | Selects use the fused Determinism or set customized Determinism. Options available: Auto/Manual. Default setting is <b>Auto</b> .                                     |
| cTDP Control                | Selects use the fused TDP or set customized TDP. **TDP is used to define the RC thermal model only** Options available: Auto/Manual. Default setting is <b>Auto</b> . |
| CLD0_VDDP Control           | Options available: Auto/Manual. Default setting is <b>Auto</b> .  |
| EfficiencyModeEn            | Options available: Auto/Enabled. Default setting is <b>Auto</b> .   |
| Package Power Limit Control | Selects use the fused PPT or set customized PPT. **PPT will be used as the ASIC power limit** Options available: Auto/Manual. Default setting is <b>Auto</b> .        |
| xGMI Link Width Control     | Options available: Auto/Enabled. Default setting is <b>Auto</b> .   |
| APBDIS                      | Options available: Auto, 0, 1. Default setting is <b>Auto</b> .   |



| <b>Parameter</b> | <b>Description</b>  |
|------------------|---|
| DF Cstates       | Enable/Disable DF C-states.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .               |
| CPPC             | Enable/Disable the CPPC feature.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .          |
| HSMP Support     | Select HSMP support enable or disable.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .    |
| Diagnostic Mode  | Select Diagnostic Mode enable or disable.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |
| BoostFmaxEn      | Options available: Auto/Enabled. Default setting is <b>Auto</b> .   |

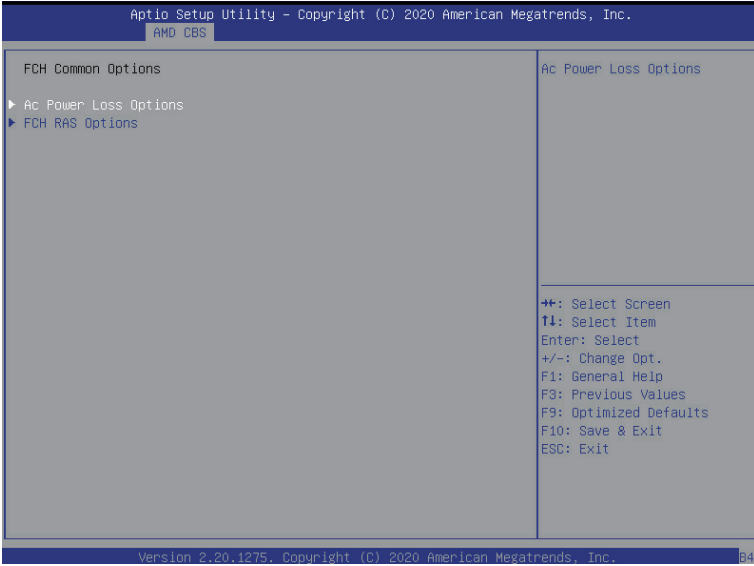
## 5-3-4-2 NBIO RAS Common Options



| Parameter                    | Description  |
|------------------------------|--|
| NBIO RAS Common Options      |  |
| NBIO RAS Global Control      | Options available: Auto/Manual. Default setting is <b>Auto</b> .   |
| NBIO RAS Control             | Options available: Disabled, MCA, Legacy. Default setting is <b>MCA</b> .  |
| Egress Poison Serverity High | Configures the Egress Poison High Serverity. Each bit set to 1 enables High servery on the associated IOHC egress port. A bit of 0 indicates LOW servery.            |
| Egress Poison Serverity Low  | Configures the Egress Poison Low Servery. Each bit set to 1 enables High servery on the associated IOHC egress port. A bit of 0 indicates LOW servery.               |
| NBIO SyncFlood Generation    | The value may be used to mask SyncFlood caused by NBIO RAS options. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                     |
| NBIO SyncFlood Reporting     | The value may be used to enanle SyncFlood reporting to APML. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .                               |
| Egress Poison Mask High      | Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions. |
| Egress Poison Mask Low       | Enables mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions. |

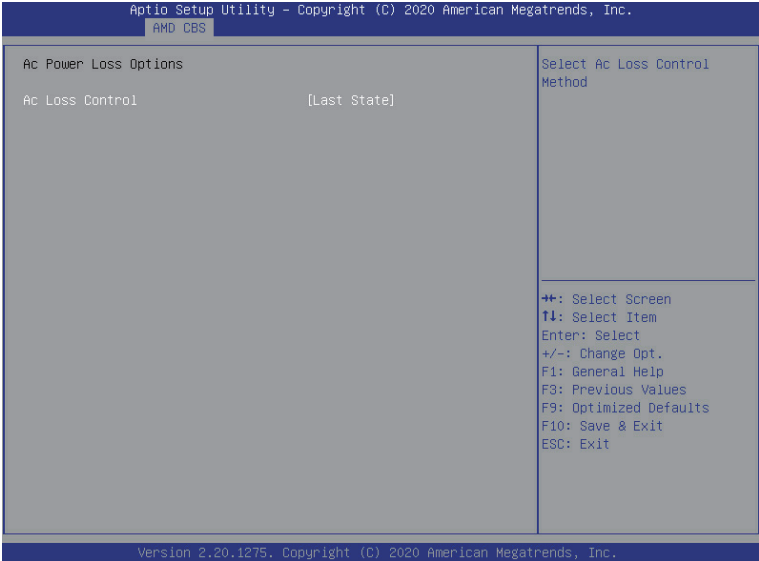
| Parameter  | Description  |
|--|--|
| Uncorrected Converted to Poison Enable Mask High | Enables mask for masking of uncorrectable parity errors on internal arrays.  |
| Uncorrected Converted to Poison Enable Mask Low  | Enables mask for masking of uncorrectable parity errors on internal arrays.  |
| System Hub Watchdog Timer                        | Specifies the timer interval of the SYSHUB Watchdog timer in milliseconds.   |
| SLINK Read Response OK                           | This item specifies whether SLINK read response errors are converted to an Okay response.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> . |
| SLINK Read Response Error Handling               | Options available: Enabled, Trigger MCOMMIT Error, Log Errors in MCA.<br>Default setting is <b>Log Errors in MCA</b> .   |
| Log Poison Data from SLINK                       | Enable/Disable the Log Poison Data from SLINK feature.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .                                    |
| PCIe Aer Reporting Mechanism                     | Selects the method of reporting AER errors from PCI Express.<br>Options available: Auto, Firmware First, OS First, MCA.<br>Default setting is <b>Auto</b> .            |
| Edpc Control                                     | Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b> .   |
| NBIO Poison Consumption                          | Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .   |
| Sync Flood on PCIe Fatal Error                   | Options available: Auto, True, False. Default setting is <b>Auto</b> .   |

### 5-3-5 FCH Common Options



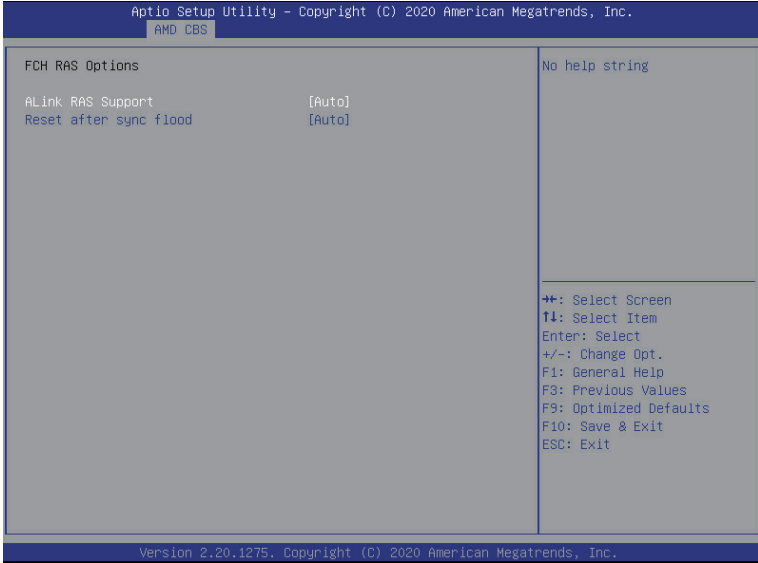
| Parameter             | Description  |
|-----------------------|--|
| FCH Common Options    |  |
| AC Power Loss Options | Press [Enter] for configuration of advanced items. |
| FCH RAS Options       | Press [Enter] for configuration of advanced items. |

### 5-3-5-1 AC Power Loss Options



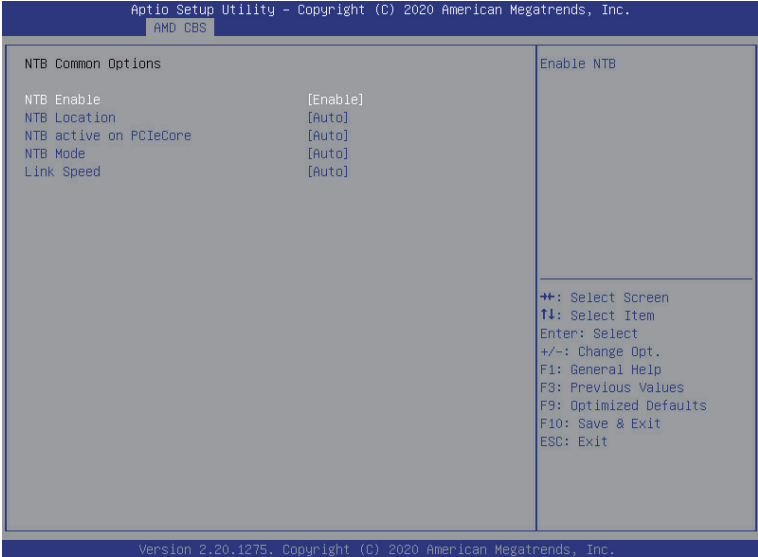
| Parameter             | Description  |
|-----------------------|--|
| AC Power Loss Options |  |
| AC Loss Control       | Selects the AC Loss Control Method.<br>Options available: Power Off, Power On, Last State.<br>Default setting is <b>Last State</b> . |

### 5-3-5-2 FCH RAS Options



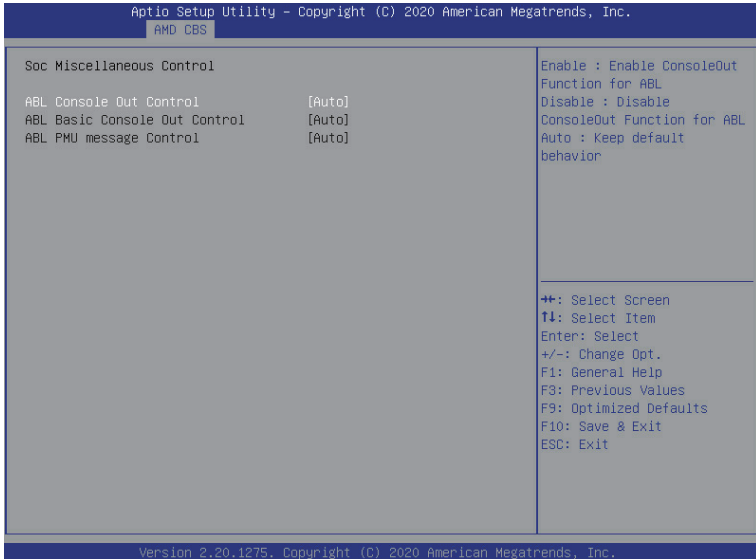
| Parameter              | Description   |
|------------------------|---|
| FCH RAS Options        |   |
| ALink RAS Support      | Enable/Disable the ALink RAS Support.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .                                     |
| Reset after sync flood | Enables AB to forward downstream sync-flood message to system controller.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |

### 5-3-6 NTB Common Options



| Parameter          | Description   |
|--------------------|---|
| NTB Common Options |   |
| NTB Enable         | Options available: Auto/Enabled. Default setting is <b>Auto</b> . |

### 5-3-7 SOC Miscellaneous Control



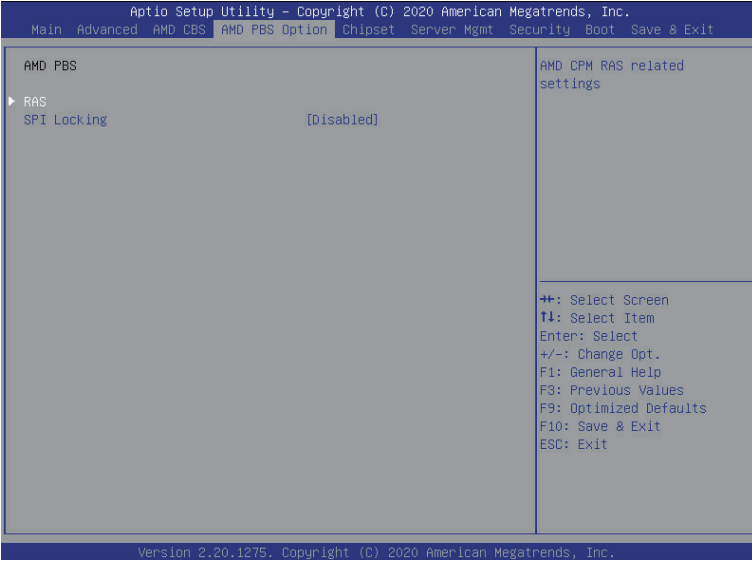
| Parameter                                 | Description  |
|---|--|
| SOC Miscellaneous Control                 |  |
| ABL Console Out Control                   | Enable/Disable the ConsoleOut function for ABL.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .    |
| ABL PMU message Control <sup>(Note)</sup> | To Control the total number of PMU debug messages.<br>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> . |

(Note) This item appears when **ABL Console Out Control** is set to **Enabled**.



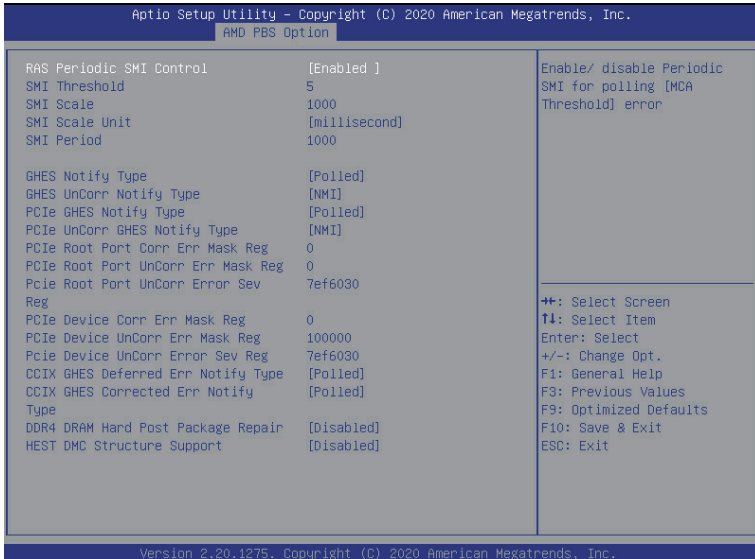
## 5-4 AMD PBS Menu

AMD PBS Option menu displays submenu options for configuring the function of AMD PBS. Select a submenu item, then press [Enter] to access the related submenu screen.



| Parameter   | Description   |
|-------------|---|
| RAS         | Press [Enter] for configuration of advanced items.  |
| SBI Locking | Enable/Disable SBI Locking for protect ROM part.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> . |

## 5-4-1 RAS

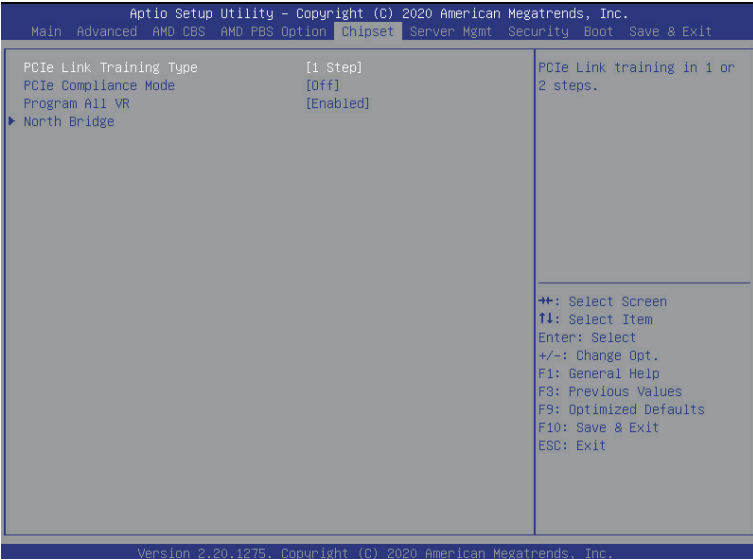


| Parameter                        | Description   |
|----------------------------------|---|
| RAS Periodic SMI Control         | Enable/Disable the Periodic SMI for polling [MCA Threshold] error. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> . |
| SMI Threshold                    | Configures the SMI Threshold value.   |
| SMI Scale                        | Configures the SMI Scale value.   |
| SMI Scale Unit                   | Defines the unit of time scale. Options available: millisecond, second, minute. Default setting is <b>millisecond</b> .                     |
| SMI Period                       | Configures the SMI Period.  |
| GHES Notify Type                 | Selects the Notification type for deferred/ corrected errors. Options available: Polled/SCI. Default setting is <b>Polled</b> .             |
| GHES UnCorr Notify Type          | Selects the Notification type for uncorrected errors. Options available: Polled/NMI. Default setting is <b>NMI</b> .                        |
| PCIe GHES Notify Type            | Selects the Notification type for PCIe corrected errors. Options available: Polled/SCI. Default setting is <b>Polled</b> .                  |
| PCIe UnCorr GHES Notify Type     | Selects the Notification type for PCIe uncorrected errors. Options available: Polled/NMI. Default setting is <b>NMI</b> .                   |
| PCIe Root Port Corr Err Mask Reg | Initialize the PCIe AER Corrected Error Mask register of Root Port.   |

| Parameter                           | Description   |
|-------------------------------------|---|
| PCIe Root Port UnCorr Err Mask Reg  | Initialize the PCIe AER Uncorrected Error Mask register of Root Port.   |
| PCIe Root Port UnCorr Err Sev Reg   | Initialize the PCIe AER Uncorrected Error Severity register of Root Port.   |
| PCIe Device Corr Err Mask Reg       | Initialize the PCIe AER Corrected Error Mask register of PCIe device.   |
| PCIe Device UnCorr Err Mask Reg     | Initialize the PCIe AER Uncorrected Error Mask register of PCIe device.   |
| PCIe Device UnCorr Err Sev Reg      | Initialize the PCIe AER Uncorrected Error Severity register of PCIe device.   |
| CCIX GHES Deferred ERR Notify Type  | Selects the Notification type for CCIX deferred error.<br>Options available: Polled/SCI. Default setting is <b>Polled</b> .   |
| CCIX GHES Corrected Err Notify Type | Selects the Notification type for CCIX corrected error.<br>Options available: Polled/SCI. Default setting is <b>Polled</b> .  |
| DDR4 DRAM Hard Post Package Repair  | This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> . |
| HEST DMC Structure Support          | HEST DMC (Deferred Machine Check) Structure Support.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .   |

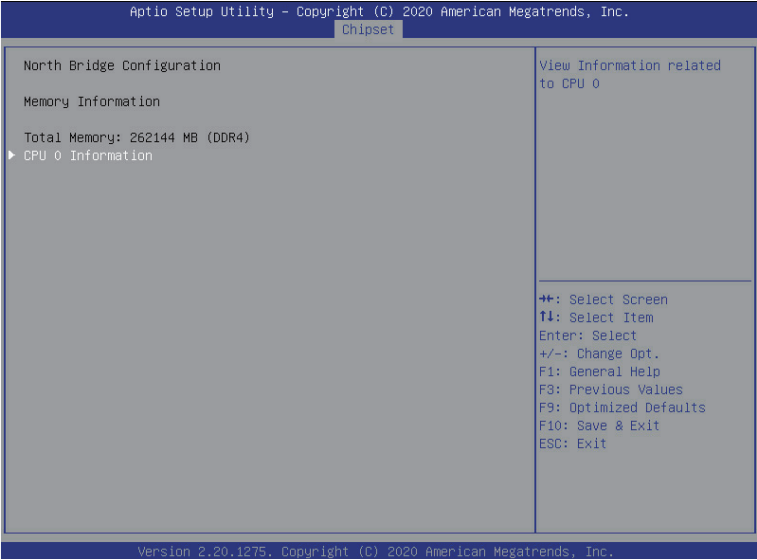
## 5-5 Chipset Setup Menu

Chipset Setup menu displays submenu options for configuring the function of the North Bridge. Select a submenu item, then press <Enter> to access the related submenu screen.



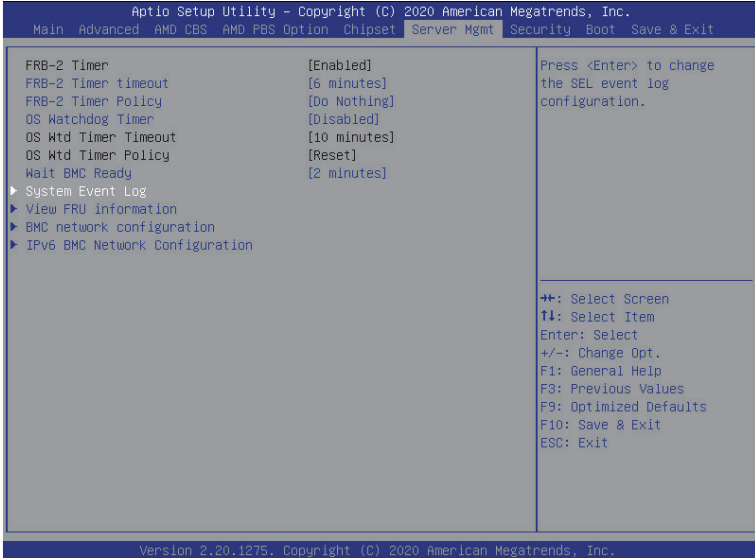
| Parameter               | Description   |
|-------------------------|---|
| PCIe Link Training Type | Configures the PCIe Link training in 1 or 2 steps.<br>Options available: 1 Step/2Step. Default setting is <b>1 Step</b> . |
| PCIe Compliance Mode    | Options available: On/Off. Default setting is <b>Off</b> .  |
| Program All VR          | Enable/Disable program all VR on MB.<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .          |
| North Bridge            | Press [Enter] for configuration of advanced items.  |

# 5-5-1 North Bridge



| Parameter                  | Description   |
|----------------------------|---|
| North Bridge Configuration |   |
| Memory Information         |   |
| Total Memory               | Displays the total memory information.              |
| CPU0 Information           | Press [Enter] to view information related to CPU 0. |

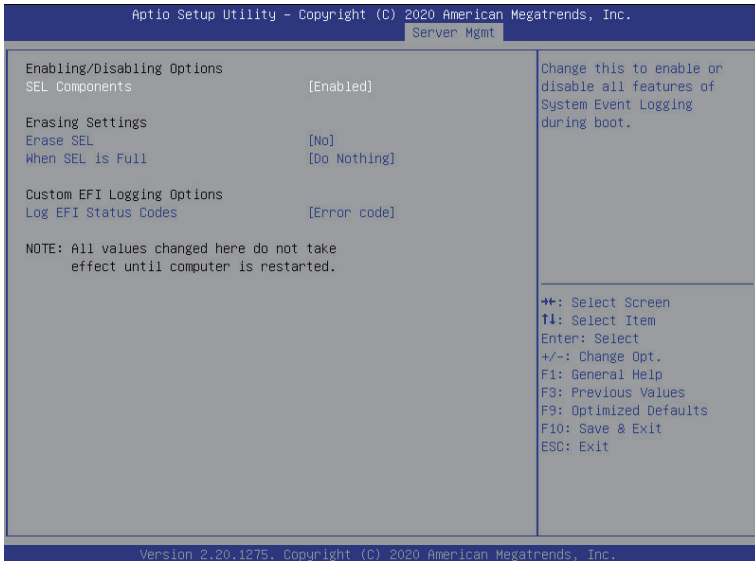
## 5-6 Server Management Menu



| Parameter            | Description  |
|----------------------|--|
| FRB-2 Timer          | Enable/Disable FRB-2 timer (POST timer).<br>Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .   |
| FRB-2 Timer timeout  | Configures the FRB2 Timer timeout.<br>Options available: 3 minutes, 4 minutes, 5 minutes, 6 minutes. Default setting is <b>6 minutes</b> .<br><b>Please note that this item is configurable when FRB-2 Timer is set to Enabled.</b>      |
| FRB-2 Timer Policy   | Configures the FRB2 Timer policy.<br>Options available: Do Nothing, Reset, Power Down. Default setting is <b>Do Nothing</b> .<br><b>Please note that this item is configurable when FRB-2 Timer is set to Enabled.</b>                   |
| OS Watchdog Timer    | Enable/Disable OS Watchdog Timer function.<br>Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .  |
| OS Wtd Timer Timeout | Configures OS Watchdog Timer.<br>Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is <b>10 minutes</b> .<br><b>Please note that this item is configurable when OS Watchdog Timer is set to Enabled.</b> |
| OS Wtd Timer Policy  | Configure OS Watchdog Timer Policy.<br>Options available: Reset, Do Nothing, Power Down. Default setting is <b>Reset</b> .<br><b>Please note that this item is configurable when OS Watchdog Timer is set to Enabled.</b>                |

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

## 5-6-1 System Event Log

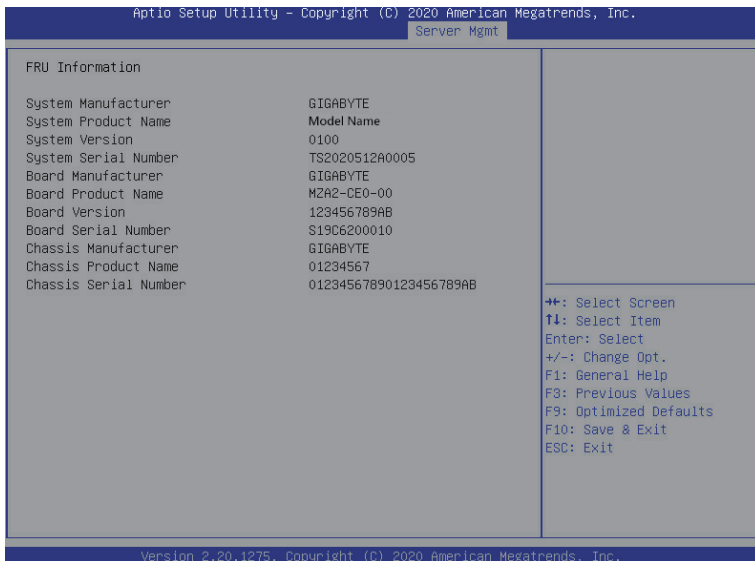


| Parameter                    | Description   |
|------------------------------|---|
| Enabling / Disabling Options |   |
| SEL Components               | Change this item to enable or disable all features of System Event Logging during boot.<br>Options available: Enabled/Disabled. Default setting is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



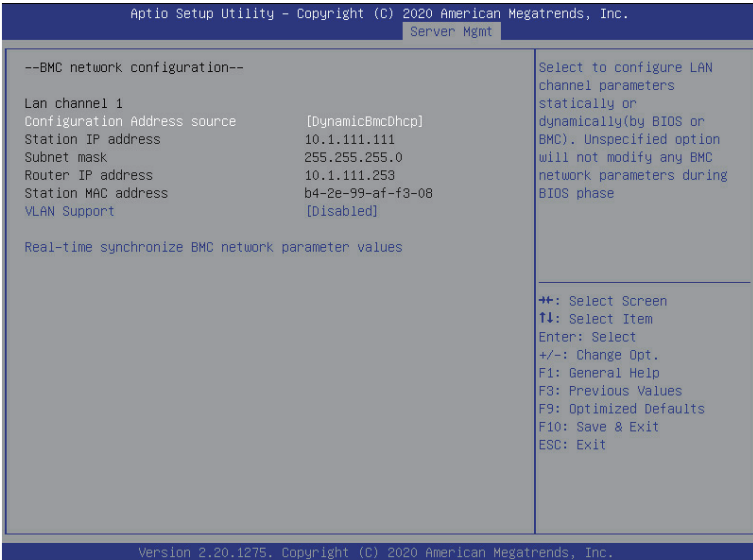
## 5-6-2 View FRU Information

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.



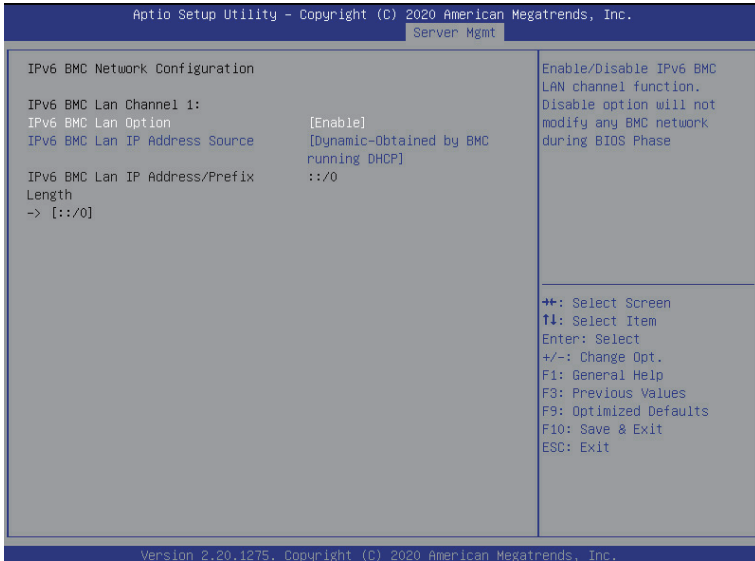
(Note) The model name will vary depends on the product you purchased

### 5-6-3 BMC Network Configuration



| Parameter                         | Description   |
|-----------------------------------|---|
| BMC network configuration         |   |
| Lan Channel 1                     |   |
| Configuration Address source      | Selects to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase.<br>Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is <b>DynamicBmcDhcp</b> . |
| Station IP address                | Displays IP Address information.  |
| Subnet mask                       | Displays Subnet Mask information.<br>Please note that the IP address must be in three digitals, for example, 192.168.000.001.   |
| Router IP address                 | Displays the Router IP Address information.   |
| Station MAC address               | Displays the MAC Address information.   |
| Real-time get BMC network address | Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.  |

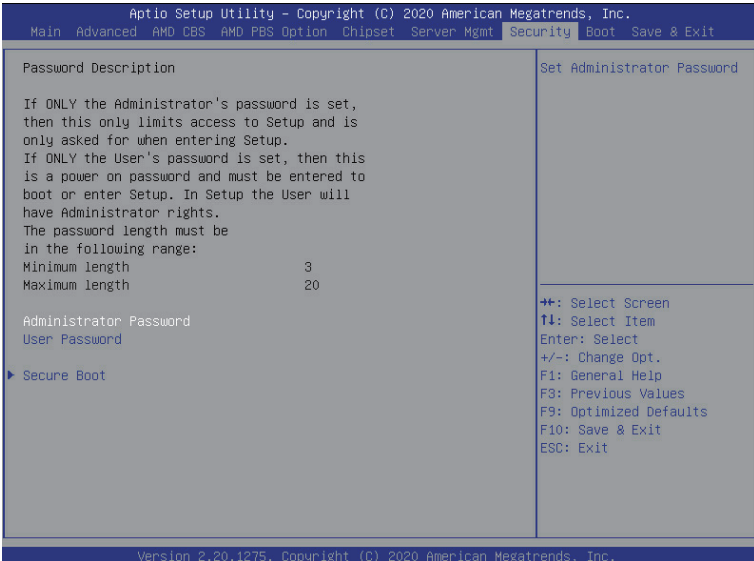
## 5-6-4 IPv6 BMC Network Configuration



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

## 5-7 Security Menu

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



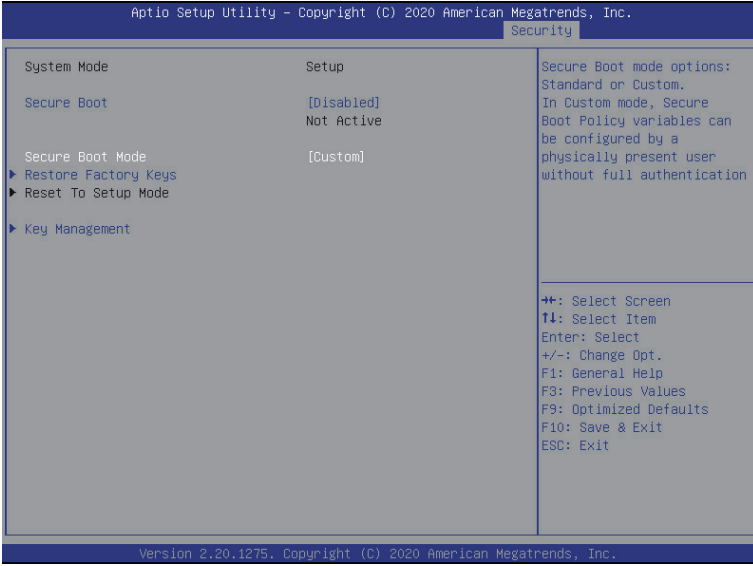
There are two types of passwords that you can set:

- 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.             |

## 5-7-1 Secure Boot

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



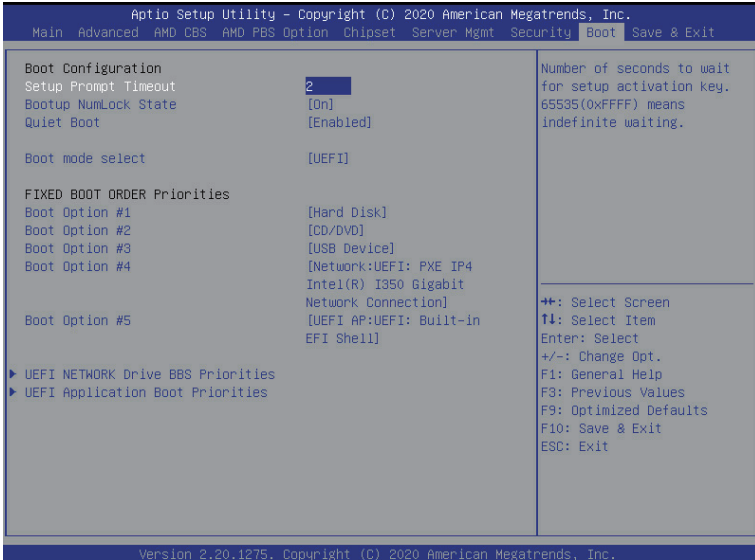
| Parameter                          | Description  |
|------------------------------------|--|
| System Mode                        | Displays if the system is in User mode or Setup mode.  |
| Secure Boot                        | Enable/ Disable the Secure Boot function.<br>Options available:Enabled/Disabled.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

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

| Parameter      | Description  |
|----------------|--|
| Key Management | <p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235"><b>Please note that this item is configurable when Secure Boot Mode is set to Custom.</b></p> <ul style="list-style-type: none"> <li data-bbox="335 243 941 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 941 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li data-bbox="367 326 899 352">– Options available: Enabled/Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="335 357 925 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 925 404">– Installs all factory default keys. It will force the system in User Mode.</li> <li data-bbox="367 409 601 431">– Options available: Yes/No.</li> </ul> </li> <li data-bbox="335 435 899 517">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 459 899 517">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li data-bbox="335 522 696 572">◆ Restore DB defaults <ul style="list-style-type: none"> <li data-bbox="367 545 696 572">– Restore DB variable to factory defaults.</li> </ul> </li> <li data-bbox="335 577 893 627">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 600 893 627">– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li data-bbox="335 631 803 736">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 655 803 682">– Displays the current status of the Platform Key (PK).</li> <li data-bbox="367 686 675 713">– Press [Enter] to configure a new PK.</li> <li data-bbox="367 718 611 736">– Options available: Set New.</li> </ul> </li> <li data-bbox="335 741 941 878">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 765 941 846">– Displays the current status of the Key Exchange Key Database (KEK).</li> <li data-bbox="367 851 904 878">– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li data-bbox="367 882 675 901">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 882 904 1019">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 906 904 932">– Displays the current status of the Authorized Signature Database.</li> <li data-bbox="367 937 941 987">– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li data-bbox="367 992 675 1019">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1023 899 1160">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1047 899 1074">– Displays the current status of the Forbidden Signature Database.</li> <li data-bbox="367 1078 888 1128">– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li data-bbox="367 1133 675 1160">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1165 925 1301">◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li data-bbox="367 1188 925 1215">– Displays the current status of the Authorized TimeStamps Database.</li> <li data-bbox="367 1219 904 1270">– Press [Enter] to configure a new DBT or load additional DBT from storage devices.</li> <li data-bbox="367 1274 675 1301">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1306 915 1434">◆ OsRecovery Signatures <ul style="list-style-type: none"> <li data-bbox="367 1329 915 1356">– Displays the current status of the OsRecovery Signature Database.</li> <li data-bbox="367 1361 888 1411">– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.</li> <li data-bbox="367 1415 675 1434">– Options available: Set New/Append.</li> </ul> </li> </ul> |

## 5-8 Boot Menu

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



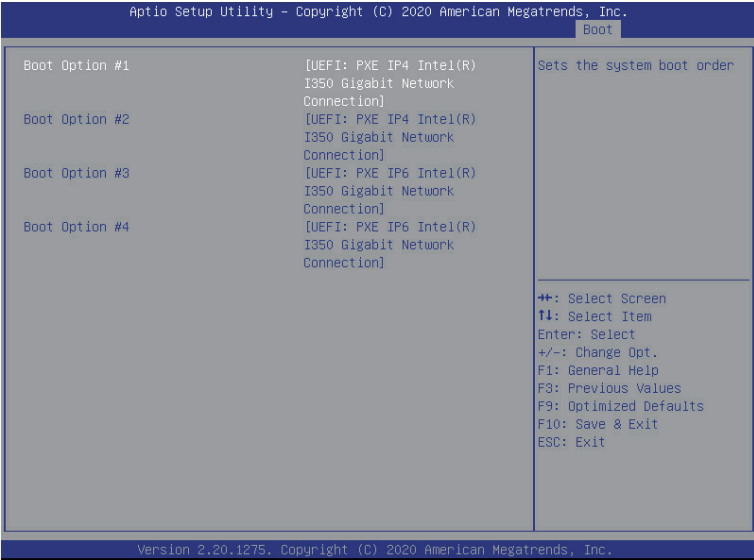
| Parameter            | Description   |
|----------------------|---|
| Boot Configuration   |   |
| Setup Prompt Timeout | Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.<br>Press the numeric keys to input the desired values. |
| Bootup NumLock State | Enable/Disable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

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



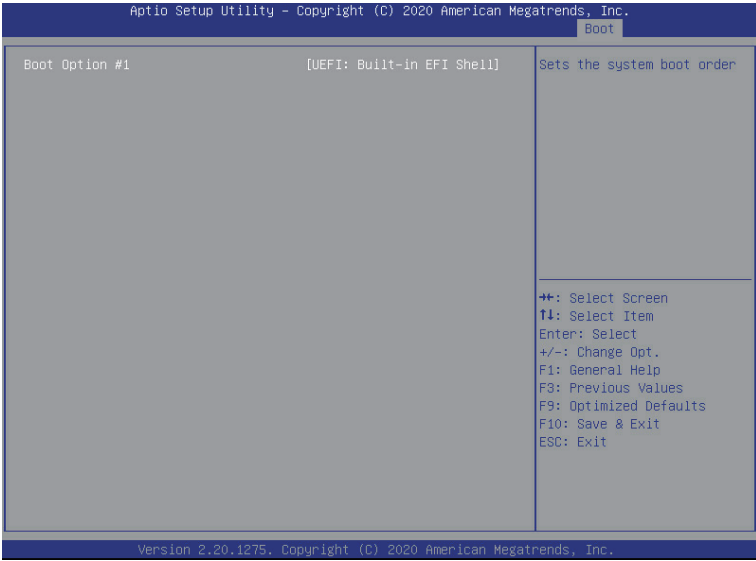
## 5-8-1 UEFI NETWORK Drive BBS Priorities

The UEFI network drive BBS priorities submenu allows you to specify the boot device priority from the available UEFI network drives during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



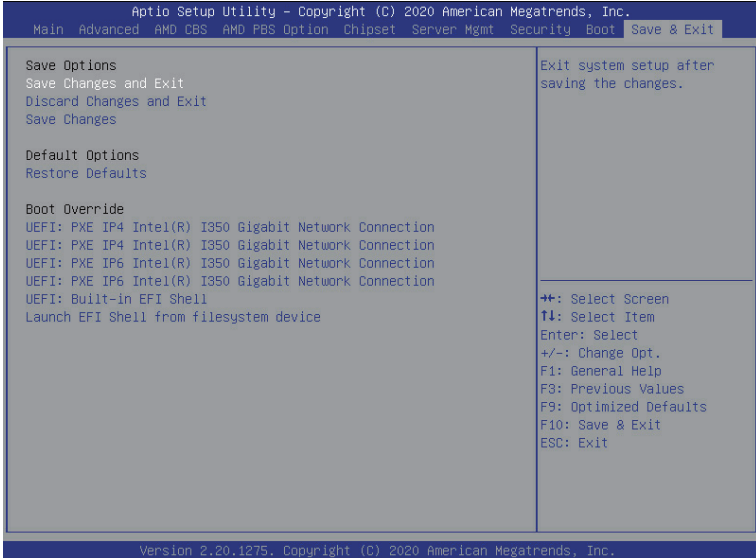
## 5-8-2 UEFI Application Boot Priorities

The UEFI application boot priorities submenu allows you to specify the boot device priority from the available UEFI applications during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



## 5-9 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 Changes 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                            | Saves changes done so far to any of the setup options.<br>Options available: Yes/No.  |
| Default Options                         |   |
| 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. |
| Boot Override                           | Press [Enter] to configure the device as the boot-up drive.   |
| Launch EFI Shell from filesystem device | Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.  |

## 5-10 ABL POST Codes

### 5-10-1 StartProcessorTestPoints

|   |        |
|---|--------|
| Entry used for range testing for @b Processor related TPs | 0xE000 |
|---|--------|

### 5-10-2 Memory test points

|  |        |
|--|--------|
| Memory structure initialization (Public interface) | 0xE001 |
| SPD Data processing (Public interface)             | 0xE002 |
| Memory configuration (Public interface) Phase 1    | 0xE003 |
| DRAM initialization                                | 0xE004 |
| ProcMemSPDChecking                                 | 0xE005 |
| ProcMemModeChecking                                | 0xE006 |
| Speed and TCL configuration                        | 0xE007 |
| ProcMemSpdTiming                                   | 0xE008 |
| ProcMemDramMapping                                 | 0xE009 |
| ProcMemPlatformSpecificConfig                      | 0xE00A |
| ProcMemPhyCompensation                             | 0xE00B |
| ProcMemStartDcts                                   | 0xE00C |
| ProcMemBeforeDramInit (Public interface)           | 0xE00D |
| ProcMemPhyFenceTraining                            | 0xE00E |
| ProcMemSynchronizeDcts                             | 0xE00F |
| ProcMemSystemMemoryMapping                         | 0xE010 |
| ProcMemMtrrConfiguration                           | 0xE011 |
| ProcMemDramTraining                                | 0xE012 |
| ProcMemBeforeAnyTraining(Public interface)         | 0xE013 |

### 5-10-3 PMU Test Points

|  |        |
|--|--------|
| ABL Mem - PMU - Before PMU Firmware load | 0xE014 |
| ABL Mem - PMU - After PMU Firmware load  | 0xE015 |
| ABL Mem - PMU Populate SRAM Timing       | 0xE016 |
| ABL Mem - PMU Populate SRAM Config       | 0xE017 |
| ABL Mem - PMU Write SRAM Msg Block       | 0xE018 |
| ABL Mem - Wait for Phy Cal Complete      | 0xE019 |
| ABL Mem - Phy Cal Complete               | 0xE01A |
| ABL Mem - PMU Start                      | 0xE01B |
| ABL Mem - PMU Started                    | 0xE01C |
| ABL Mem - PMU Waiting for Complete       | 0xE01D |
| ABL Mem - PMU Stage Dec Init             | 0xE01E |
| ABL Mem - PMU Stage Training Wr Lvl      | 0xE01F |
| ABL Mem - PMU Stage Training Rx En       | 0xE020 |
| ABL Mem - PMU Stage Training Rd Dqs      | 0xE021 |
| ABL Mem - PMU Stage Training Rd 2D       | 0xE022 |

|                                    |        |
|------------------------------------|--------|
| ABL Mem - PMU Stage Training Wr 2D | 0xE023 |
| ABL Mem - PMU Queue Empty          | 0xE024 |
| ABL Mem - PMU US message Start     | 0xE025 |
| ABL Mem - PMU US message End       | 0xE026 |
| ABL Mem - PMU Complete             | 0xE027 |
| ABL Mem - PMU - After PMU Training | 0xE028 |
| ABL Mem - PMU - Before Disable PMU | 0xE029 |

### 5-10-4 Original Post Code

|  |        |
|--|--------|
| ProcMemTransmitDqsTraining                                     | 0xE02A |
| ABL Mem - Start write sweep                                    | 0xE02B |
| ABL Mem - Set Transmit DQ delay                                | 0xE02C |
| ABL Mem - Write test pattern                                   | 0xE02D |
| ABL Mem - Read Test pattern                                    | 0xE02E |
| ABL Mem - Compare Test pattern                                 | 0xE02F |
| ABL Mem - Update results                                       | 0xE030 |
| ABL Mem - Start Find passing window                            | 0xE031 |
| ABL Mem - ProcMemMaxRdLatencyTraining                          | 0xE032 |
| ABL Mem - Start sweep  | 0xE033 |
| ABL Mem - Set delay  | 0xE034 |
| ABL Mem - Write test pattern                                   | 0xE035 |
| ABL Mem - Read Test pattern                                    | 0xE036 |
| ABL Mem - Compare Test pattern                                 | 0xE037 |
| ABL Mem - Online Spare init                                    | 0xE038 |
| ABL Mem - Chip select Interleave Init                          | 0xE039 |
| ABL Mem - Node Interleave Init                                 | 0xE03A |
| ABL Mem - Channel Interleave Init                              | 0xE03B |
| ABL Mem - ECC initialization                                   | 0xE03C |
| ABL Mem - Platform Specific Init                               | 0xE03D |
| ABL Mem - Before callout for "AgesaReadSpd"                    | 0xE03E |
| ABL Mem - After callout for "AgesaReadSpd"                     | 0xE03F |
| ABL Mem - Before optional callout "AgesaHookBeforeDramInit"    | 0xE040 |
| ABL Mem - After optional callout "AgesaHookBeforeDramInit"     | 0xE041 |
| ABL Mem - Before optional callout "AgesaHookBeforeDQSTraining" | 0xE042 |
| ABL Mem - After optional callout "AgesaHookBeforeDQSTraining"  | 0xE043 |
| ABL Mem - Before optional callout "AgesaHookBeforeDramInit"    | 0xE044 |
| ABL Mem - After optional callout "AgesaHookBeforeDramInit"     | 0xE045 |
| ABL Mem - After MemDataInit                                    | 0xE046 |
| ABL Mem - Before InitializeMCT                                 | 0xE047 |
| ABL Mem - Before LV DDR3                                       | 0xE048 |
| ABL Mem - Before InitMCT                                       | 0xE049 |

|                                      |        |
|--------------------------------------|--------|
| ABL Mem - Before OtherTiming         | 0xE04A |
| ABL Mem - Before UMAMemTyping        | 0xE04B |
| ABL Mem - Before SetDqsEccTmgs       | 0xE04C |
| ABL Mem - Before MemClr              | 0xE04D |
| ABL Mem - Before On DIMM Thermal     | 0xE04E |
| ABL Mem - Before DMI                 | 0xE04F |
| ABL MEM - End of phase 3 memory code | 0xE050 |

### 5-10-5 CPU test points

|                                     |        |
|-------------------------------------|--------|
| Entry point CPU init after training | 0xE051 |
| Exit point CPU init after training  | 0xE052 |
| Entry point CPU APOB CCX map init   | 0xE053 |
| Exit point CPU APOB CCX map init    | 0xE054 |
| Entry point CPU Optimized boot init | 0xE055 |
| Exit point CPU Optimized boot init  | 0xE056 |
| Entry point CPU APOB EDC info init  | 0xE057 |
| Exit point CPU APOB EDC info init   | 0xE058 |

### 5-10-6 Topology test points

|                   |        |
|-------------------|--------|
| ProcTopologyEntry | 0xE071 |
| ProcTopologyDone  | 0xE07C |

### 5-10-7 Extended memory test point

|  |        |
|--|--------|
| ProcMemSendMRS2  | 0xE080 |
| Sedding MRS3   | 0xE081 |
| Sending MRS1   | 0xE082 |
| Sending MRS0   | 0xE083 |
| Continuous Pattern Read  | 0xE084 |
| Continuous Pattern Write   | 0xE085 |
| Mem: 2d RdDqs Training begin   | 0xE086 |
| Mem: Before optional callout to platform BIOS to change External Vref during 2d Training | 0xE087 |
| Mem: After optional callout to platform BIOS to change External Vref during 2d Training  | 0xE088 |
| Configure DCT For General use begin  | 0xE089 |
| Configure DCT For training begin   | 0xE08A |
| Configure DCT For Non-Explicit   | 0xE08B |
| Configure to Sync channels   | 0xE08C |
| Allocate C6 Storage  | 0xE08D |
| Before LV DDR4   | 0xE08E |
| Before LV DDR3   | 0xE08F |

### 5-10-8 Gnb Earlier init

|                                    |        |
|------------------------------------|--------|
| TP0x90                             | 0xE090 |
| GNB earlier interface              | 0xE091 |
| GNB internal debug code            | 0xE092 |
| GNB internal debug code            | 0xE093 |
| GNB internal debug code            | 0xE094 |
| GNB internal debug code            | 0xE095 |
| GNB internal debug code            | 0xE096 |
| GNB internal debug code            | 0xE097 |
| GNB internal debug code            | 0xE098 |
| GNB internal debug code            | 0xE099 |
| GNB internal debug code            | 0xE09A |
| GNB internal debug code            | 0xE09B |
| GNB internal debug code            | 0xE09C |
| GNB internal debug code            | 0xE09D |
| GNB internal debug code            | 0xE09E |
| GNB internal debug code            | 0xE09F |
| TP0xA0                             | 0xE0A0 |
| GNB internal debug code            | 0xE0A1 |
| GNB internal debug code            | 0xE0A2 |
| GNB internal debug code            | 0xE0A3 |
| GNB internal debug code            | 0xE0A4 |
| GNB internal debug code            | 0xE0A5 |
| GNB internal debug code            | 0xE0A6 |
| GNB internal debug code            | 0xE0A7 |
| GNB internal debug code            | 0xE0A8 |
| GNB internal debug code            | 0xE0A9 |
| GNB internal debug code            | 0xE0AA |
| GNB internal debug code            | 0xE0AB |
| GNB internal debug code            | 0xE0AC |
| GNB internal debug code            | 0xE0AD |
| GNB internal debug code            | 0xE0AE |
| GNB internal debug code            | 0xE0AF |
| Abl1Begin                          | 0xE0B0 |
| ABL 1 Initialization               | 0xE0B1 |
| ABL 1 DF Early                     | 0xE0B2 |
| ABL 1 DF Pre Training              | 0xE0B3 |
| ABL 1 Debug Synchronization        | 0xE0B4 |
| ABL 1 Error Detected               | 0xE0B5 |
| ABL 1 Global memory error detected | 0xE0B6 |
| ABL 1 End                          | 0xE0B7 |

|   |        |
|---|--------|
| ABL 2 Begin                                   | 0xE0B8 |
| ABL 2 Initialization                          | 0xE0B9 |
| ABL 2 After Training                          | 0xE0BA |
| ABL 2 Debug Synchronization                   | 0xE0BB |
| ABL 2 Error detected                          | 0xE0BC |
| ABL 2 Global memory error detected            | 0xE0BD |
| ABL 2 End                                     | 0xE0BE |
| ABL 3 Begin                                   | 0xE0BF |
| ABL 3 Initialization                          | 0xE0C0 |
| ABL 3 GMI/xGMI Initialization Stage 1         | 0xB1C0 |
| ABL 3 GMI/xGMI Initialization Stage 1 Warning | 0xF1C0 |
| ABL 3 GMI/xGMI Initialization Stage 2 Error   | 0xE2C0 |
| ABL 3 GMI/xGMI Initialization Stage 2         | 0xB2C0 |
| ABL 3 GMI/xGMI Initialization Stage 2 Warning | 0xF2C0 |
| ABL 3 GMI/xGMI Initialization Stage 2 Error   | 0xE3C0 |
| ABL 3 GMI/xGMI Initialization Stage 3         | 0xB3C0 |
| ABL 3 GMI/xGMI Initialization Stage 3 Warning | 0xF3C0 |
| ABL 3 GMI/xGMI Initialization Stage 3 Error   | 0xE4C0 |
| ABL 3 GMI/xGMI Initialization Stage 4         | 0xB4C0 |
| ABL 3 GMI/xGMI Initialization Stage 4 Warning | 0xF4C0 |
| ABL 3 GMI/xGMI Initialization Stage 4 Error   | 0xE5C0 |
| ABL 3 GMI/xGMI Initialization Stage 5         | 0xB5C0 |
| ABL 3 GMI/xGMI Initialization Stage 5 Warning | 0xF5C0 |
| ABL 3 GMI/xGMI Initialization Stage 5 Error   | 0xE6C0 |
| ABL 3 GMI/xGMI Initialization Stage 6         | 0xB6C0 |
| ABL 3 GMI/xGMI Initialization Stage 6 Warning | 0xF6C0 |
| ABL 3 GMI/xGMI Initialization Stage 6 Error   | 0xE7C0 |
| ABL 3 GMI/xGMI Initialization Stage 7         | 0xE8C0 |
| ABL 3 GMI/xGMI Initialization Stage 8         | 0xE9C0 |
| ABL 3 GMI/xGMI Initialization Stage 9         | 0xF9C0 |
| ABL 3 GMI/xGMI Initialization Stage 9 Error   | 0xEAC0 |
| ABL 3 GMI/xGMI Initialization Stage 10        | 0xFAC0 |
| ABL 3 GMI/xGMI Initialization Stage 10 Error  | 0xE0C1 |
| Abi3ProgramUmcKeys                            | 0xE0C2 |
| ABL 3 DF Final Initialization                 | 0xE0C3 |
| ABL 3 Execute Synchronization Function        | 0xE0C4 |
| ABL 3 Debug Synchronization Function          | 0xE0C5 |
| ABL 3 Error Detected                          | 0xE0C6 |
| ABL 3 Global memory error detected            | 0xE0C7 |
| ABL 4 Initialization - cold boot              | 0xE0C8 |
| ABL 4 Memory test - cold boot                 | 0xE0C9 |



|   |        |
|---|--------|
| ABL 4 APOB Initialization - cold boot                         | 0xE0CA |
| ABL 4 Finalize memory settings - cold boot                    | 0xE0CB |
| ABL 4 CPU Initialize Optimized Boot - cold boot               | 0xE0CC |
| ABL 4 Gmi Pcie Training - cold boot                           | 0xE0CD |
| ABL 4 Cold boot End   | 0xE0CE |
| ABL 4 Initialization - Resume boot                            | 0xE0CF |
| ABL 4 Resume End  | 0xE0D0 |
| ABL 4 End Cold/Resume boot                                    | 0xE0D1 |
| ABL 2 memory initialization                                   | 0xE0D2 |
| ABL 3 memory initialization                                   | 0xE0D3 |
| ABL 3 End   | 0xE0D4 |
| ABL 1 Enter Memory Flow                                       | 0xE0D5 |
| Memory flow memory clock synchronization                      | 0xE0D6 |
| IfAmdReadEventLogEntry  | 0xE0D7 |
| Exiting from AmdReadEventLog                                  | 0xE0D8 |
| Entry to AmdGetApicId   | 0xE0D9 |
| Exiting from AmdGetApicId                                     | 0xE0DA |
| Entry to AmdGetPciAddress                                     | 0xE0DB |
| Exiting from AmdGetPciAddress                                 | 0xE0DC |
| Entry to AmdIdentifyCore                                      | 0xE0DD |
| TExiting from AmdIdentifyCore                                 | 0xE0DE |
| After IDS calls out to run code on an AP                      | 0xE0DF |
| After IDS calls out to run code on an AP                      | 0xE0E0 |
| Before IDS calls out to get IDS data                          | 0xE0E1 |
| After IDS calls out to get IDS data                           | 0xE0E2 |
| Before the heap manager calls out to allocate a buffer        | 0xE0E3 |
| After the heap manager calls out to allocate a buffer         | 0xE0E4 |
| Before the heap manager calls out to deallocate a buffer      | 0xE0E5 |
| After the heap manager calls out to deallocate a buffer       | 0xE0E6 |
| Before the heap manager calls out to locate a buffer          | 0xE0E7 |
| After the heap manager calls out to locate a buffer           | 0xE0E8 |
| Memory flow P-State synchronization                           | 0xE0E9 |
| After the BSP calls out to run code on an AP                  | 0xE0EA |
| Before the BSP calls out to run code on an AP                 | 0xE0EB |
| After the BSP calls out to run code on an AP                  | 0xE0EC |
| Before the S3 save code calls out to allocate a buffer        | 0xE0ED |
| After the S3 save code calls out to allocate a buffer         | 0xE0EE |
| Before the memory S3 save code calls out to allocate a buffer | 0xE0EF |
| After the memory S3 save code calls out to allocate a buffer  | 0xE0F0 |
| Before the memory code calls out to locate a buffer           | 0xE0F1 |
| After the memory code calls out to locate a buffer            | 0xE0F2 |

|   |        |
|---|--------|
| Before the memory code calls out to locate a buffer | 0xE0F3 |
| After the memory code calls out to locate a buffer  | 0xE0F4 |
| Before the memory code calls out to locate a buffer | 0xE0F5 |
| After the memory code calls out to locate a buffer  | 0xE0F6 |
| Before the memory code calls out to locate a buffer | 0xE0F7 |
| After the memory code calls out to locate a buffer  | 0xE0F8 |
| Ready to boot event                                 |        |

### 5-10-9 PMU test points

|                            |        |
|----------------------------|--------|
| Failed PMU training        | 0xE0F9 |
| End of phase 1 memory code | 0xE0FA |
| End of phase 2 memory code | 0xE0FB |

### 5-10-10 ABL0 test points

|           |        |
|-----------|--------|
| Abl0Begin | 0xE0FC |
| ABL 0 End | 0xE0FD |

### 5-10-11 ABL5 test points

|   |        |
|---|--------|
| ABL 5 End   | 0xE100 |
| sume boot   | 0xE101 |
| ABL 6 End   | 0xE102 |
| ABL 6 Initialization  | 0xE103 |
| End of phase 1b memory code   | 0xE104 |
| ABL 1b memory initialization  | 0xE105 |
| ABL 6 Global memroy error detected                                  | 0xE106 |
| ABL 1b Debug Synchronization Function                               | 0xE107 |
| ABL 4b Debug Synchronization Function                               | 0xE108 |
| Ab1bBegin   | 0xE109 |
| Ab4bBegin   | 0xE10A |
| BSP encountered HMAC fail on APOB Header                            | 0xE10B |
| ABL Error General ASSERT  | 0xE2A0 |
| Unknown Error   | 0xE2A1 |
| ABL Error Log Inig Error  | 0xE2A2 |
| ABL Error for On DIMM thermal Heap allocation error                 | 0xE2A3 |
| ABL Error for memory test error                                     | 0xE2A4 |
| ABL Error while executing memory test error                         | 0xE2A5 |
| ABL Error DDR Post Package Repair Mem Auto Heap Alloc error         | 0xE2A6 |
| ABL Error for DDR Post Package repair Apob Heap Alloc error         | 0xE2A7 |
| ABL Error for DDR Post Package Repair No PPR Table Heap Alloc error | 0xE2A8 |
| ABL Error for Ecc Mem Auto Aloc Error error                         | 0xE2A9 |
| ABL Error for Soc Scan Heap Alloc error                             | 0xE2AB |

|   |        |
|---|--------|
| ABL Error for Soc Scan No Die error                                     | 0xE2AC |
| ABL Error for Nb Tech Heap Alloc error                                  | 0xE2AD |
| ABL Error for No Nb Constructor error                                   | 0xE2AE |
| ABL Error for No Tech Constructor error                                 | 0xE2AE |
| ABL Error for ABL1b Auto Allocation error                               | 0xE2B0 |
| ABL Error for ABL1b No NB Constructor error                             | 0xE2B1 |
| ABL Error for ABL2 No Nb Constructor error                              | 0xE2B2 |
| ABL Error for ABL3 Auto Allocation error                                | 0xE2B3 |
| ABL Error for ABL3 No Nb Constructor error                              | 0xE2B4 |
| ABL Error for ABL1b General error                                       | 0xE2B5 |
| ABL Error for ABL2 General error  | 0xE2B6 |
| ABL Error for ABL3 General error  | 0xE2B7 |
| ABL Error for Get Target Speed error                                    | 0xE2B8 |
| ABL Error for Flow P1 Family Support error                              | 0xE2B9 |
| ABL Error for No Valid Ddr4 Dimms error                                 | 0xE2BA |
| ABL Error for No Dimm Present error                                     | 0xE2BB |
| ABL Error for Flow P2 Family Supprot error                              | 0xE2BC |
| ABL Error for Heap Deallocation for PMU Sram Msg Block error            | 0xE2BD |
| ABL Error for DDR Recovery error  | 0xE2BE |
| ABL Error for RRW Test error  | 0xE2BF |
| ABL Error for On Die Thermal error                                      | 0xE2C1 |
| ABL Error for Heap Allocation For Dct Struct Amd Ch Def structure error | 0xE2C2 |
| ABL Error for Heap Allocation for PMU SRAM Msg block error              | 0xE2C3 |
| ABL Error for Heap Phy PLL lock Flure error                             | 0xE2C4 |
| ABL Error for Pmu Training error  | 0xE2C5 |
| ABL Error for Failure to Load or Verify PMU FW error                    | 0xE2C6 |
| ABL Error for Allocate for PMU SRAM Msg Block No Init error             | 0xE2C7 |
| ABL Error for Failure BIOS PMU FW Mismatch AGESA PMU FW version error   | 0xE2C8 |
| ABL Error for Deallocate for PMU SRAM Msg Block error                   | 0xE2CA |
| ABL Error for Module Type Mismatch RDIMM error                          | 0xE2CB |
| ABL Error for Module type Mismatch LRDIMM error                         | 0xE2CC |
| ABL Error for MEm Auto NVDIM error                                      | 0xE2CD |
| ABL Error for Unknowm Responce error                                    | 0xE2CE |
| ABL Error for Over Clock Error RRW Test Results Error                   | 0xE2CF |
| ABL Error for Over Clock Error PMU Training Error                       | 0xE2D0 |
| ABL Error for ABL1 General Error  | 0xE2D1 |
| ABL Error for ABL2 General Error  | 0xE2D2 |
| ABL Error for ABL3 General Error  | 0xE2D3 |
| ABL Error for ABL4 General Error  | 0xE2D4 |

|  |        |
|--|--------|
| ABL Error over clock Mem Init Error                                | 0xE2D5 |
| ABL Error over clock Mem Other Error                               | 0xE2D6 |
| ABL Error for ABL6 General Error                                   | 0xE2D7 |
| ABL Error Event Log Error  | 0xE2D8 |
| ABL Error FATAL ABL1 Log Error                                     | 0xE2D9 |
| ABL Error FATAL ABL2 Log Error                                     | 0xE2DA |
| ABL Error FATAL ABL3 Log Error                                     | 0xE2DB |
| ABL Error FATAL ABL4 Log Error                                     | 0xE2DC |
| ABL Error Slave Sync function execution Error                      | 0xE2DD |
| ABL Error Slave Sync communicaton with data set to master Error    | 0xE2DE |
| ABL Error Slave broadcast communication from master to slave Error | 0xE2DF |
| ABL Error FATAL ABL6 Log Error                                     | 0xE2E0 |
| ABL Error Slave Offline Error                                      | 0xE2E1 |
| ABL Error Slave Informs Master Error Info Error                    | 0xE2E2 |
| ABL Error Error Heap Locate for PMU SRAM Msg Block Error           | 0xE2E3 |
| ABL Error ABL2 Auto Error  | 0xE2E4 |
| ABL Error Flow P3 Family support Error                             | 0xE2E5 |
| ABL Error Abl 4 Gen Error  | 0xE2EB |
| ABL Error MBIST Heap Allocation Error                              | 0xE2EC |
| ABL Error MBIST Results Error                                      | 0xE2EE |
| ABL Error NO Dimm Smcus Info Error                                 | 0xE2EE |
| ABL Error Por Max Freq Table Error                                 | 0xE2EF |
| ABL Error Unsuppoted DIMM Config Error                             | 0xE2F0 |
| ABL Error No Ps Table Error  | 0xE2F1 |
| ABL Error Cad Bus Timing Not Found Error                           | 0xE2F2 |
| ABL Error Data Bus Timing Not Found Error                          | 0xE2F3 |
| ABL Error LrDIMM IBT Not Found Error                               | 0xE2F4 |
| ABL Error Unsuppote Dimm Config Max Freq Error Error               | 0xE2F5 |
| ABL Error Mr0 Not Found Error                                      | 0xE2F6 |
| ABL Error Obt Pattern Not found Error                              | 0xE2F7 |
| ABL Error Rc10 Op Speed Not FOUnd Error                            | 0xE2F8 |
| ABL Error Rc2 Ibt Not Found Error                                  | 0xE2F9 |
| ABL Error Rtt Not Found Error                                      | 0xE2FA |
| ABL Error Checksum ReStrt Results Error                            | 0xE2FB |
| ABL Error No Chipselect Results Error                              | 0xE2FC |
| ABL Error No Common Cas Latency Results Error                      | 0xE2FD |
| ABL Error Cas Latecnyc exceeds Taa Max Error                       | 0xE2FE |
| ABL Error Nvdimm Arm Mismatch Power Policy Error                   | 0xE2FF |
| ABL Error Nvdimm Arm Mismatch Power Source Error                   | 0xE300 |
| ABL Error ABL 1 Mem Init Error                                     | 0xE301 |

|   |        |
|---|--------|
| ABL Error ABL 2 Mem Init Error                        | 0xE302 |
| ABL Error ABL 4 Mem Init Error                        | 0xE303 |
| ABL Error ABL 6 Mem Init Error                        | 0xE304 |
| ABL Error ABL 1 error repor Error                     | 0xE305 |
| ABL Error ABL 2 error repor Error                     | 0xE306 |
| ABL Error ABL 3 error repor Error                     | 0xE307 |
| ABL Error ABL 4 error repor Error                     | 0xE308 |
| ABL Error ABL 6 error repor Error                     | 0xE30A |
| ABL Error message slave sync function execution Error | 0xE30B |
| ABL Error slave offline Error                         | 0xE30C |
| ABL Error Sync Master Error                           | 0xE30D |
| ABL Error Slave Informs Master Info Message Error     | 0xE30E |
| ABL Error General Assert Error                        | 0xE30F |
| ABL Error No Dimms On Any Channel in sysem            | 0xE310 |
| ABL Alert PMU Major Message captured                  | 0xE311 |
| ABL Alert PMU REsults Rx Timing captured              | 0xE312 |
| ABL Alert PMU REsults Tx Timing captured              | 0xE313 |
| ABL Alert PMU REsults Rx Vref captured                | 0xE314 |
| ABL Alert PMU REsults Tx Vref captured                | 0xE315 |
| EndAgesas   | 0xEFFF |

## 5-11 Agesa POST Codes

### 5-11-1 Universal Post Code

|                        |        |
|------------------------|--------|
| Universal ACPI entry   | 0xA001 |
| Universal ACPI exit    | 0xA002 |
| Universal ACPI abort   | 0xA003 |
| Universal SMBIOS entry | 0xA004 |
| Universal SMBIOS exit  | 0xA005 |
| Universal SMBIOS abort | 0xA006 |

### 5-11-2 [0xA1XX] For CZ only memory Postcodes

|  |        |
|--|--------|
| Memory structure initialization (Public interface) | 0xA101 |
| SPD Data processing (Public interface)             | 0xA102 |
| Memory configuration (Public interface)            | 0xA103 |
| DRAM initialization                                | 0xA104 |
| TpProcMemSPDChecking                               | 0xA105 |
| TpProcMemModeChecking                              | 0xA106 |
| Speed and TCL configuration                        | 0xA107 |
| TpProcMemSpdTiming                                 | 0xA108 |
| TpProcMemDramMapping                               | 0xA109 |
| TpProcMemPlatformSpecificConfig                    | 0xA10A |
| TPProcMemPhyCompensation                           | 0xA10B |
| TpProcMemStartDcts                                 | 0xA10C |
| (Public interface)                                 | 0xA10D |
| TpProcMemPhyFenceTraining                          | 0xA10E |
| TpProcMemSynchronizeDcts                           | 0xA10F |
| TpProcMemSystemMemoryMapping                       | 0xA110 |
| TpProcMemMtrrConfiguration                         | 0xA111 |
| TpProcMemDramTraining                              | 0xA112 |
| (Public interface)                                 | 0xA113 |
| TpProcMemWriteLevelizationTraining                 | 0xA114 |
| Below 800Mhz first pass start                      | 0xA115 |
| Above 800Mhz second pass start                     | 0xA116 |
| Target DIMM configured                             | 0xA117 |
| Prepare DIMMS for WL                               | 0xA118 |
| Configure DIMMS for WL                             | 0xA119 |
| TpProcMemReceiverEnableTraining                    | 0xA11A |
| Start sweep loop                                   | 0xA11B |
| Set receiver Delay                                 | 0xA11C |
| Write test pattern                                 | 0xA11D |
| Read test pattern                                  | 0xA11E |
| Compare test pattern                               | 0xA11F |

|  |        |
|--|--------|
| Calculate MaxRdLatency per channel                   | 0xA120 |
| TpProcMemReceiveDqsTraining                          | 0xA121 |
| Set Write Data delay                                 | 0xA122 |
| Write test pattern                                   | 0xA123 |
| Start read sweep                                     | 0xA124 |
| Set Receive DQS delay                                | 0xA125 |
| Read Test pattern                                    | 0xA126 |
| Compare Test pattern                                 | 0xA127 |
| Update results                                       | 0xA128 |
| Start Find passing window                            | 0xA129 |
| TpProcMemTransmitDqsTraining                         | 0xA12A |
| Start write sweep                                    | 0xA12B |
| Set Transmit DQ delay                                | 0xA12C |
| Write test pattern                                   | 0xA12D |
| Read Test pattern                                    | 0xA12E |
| Compare Test pattern                                 | 0xA12F |
| Update results                                       | 0xA130 |
| Start Find passing window                            | 0xA131 |
| TpProcMemMaxRdLatencyTraining                        | 0xA132 |
| Start sweep  | 0xA133 |
| Set delay  | 0xA134 |
| Write test pattern                                   | 0xA135 |
| Read Test pattern                                    | 0xA136 |
| Compare Test pattern                                 | 0xA137 |
| Online Spare init                                    | 0xA138 |
| Bank Interleave Init                                 | 0xA139 |
| Node Interleave Init                                 | 0xA13A |
| Channel Interleave Init                              | 0xA13B |
| ECC initialization                                   | 0xA13C |
| Platform Specific Init                               | 0xA13D |
| Before callout for "AgesaReadSpd"                    | 0xA13E |
| After callout for "AgesaReadSpd"                     | 0xA13F |
| Before optional callout "AgesaHookBeforeDramInit"    | 0xA140 |
| After optional callout "AgesaHookBeforeDramInit"     | 0xA141 |
| Before optional callout "AgesaHookBeforeDQSTraining" | 0xA142 |
| After optional callout "AgesaHookBeforeDQSTraining"  | 0xA143 |
| Before optional callout "AgesaHookBeforeDramInit"    | 0xA144 |
| After optional callout "AgesaHookBeforeDramInit"     | 0xA145 |
| After MemDataInit                                    | 0xA146 |
| Before InitializeMCT                                 | 0xA147 |
| Before LV DDR3                                       | 0xA148 |

|  |        |
|--|--------|
| Before InitMCT   | 0xA149 |
| Before OtherTiming   | 0xA14A |
| Before UMAMemTyping  | 0xA14B |
| Before SetDqsEccTmgs   | 0xA14C |
| Before MemClr  | 0xA14D |
| Before On DIMM Thermal   | 0xA14E |
| Before DMI   | 0xA14F |
| End of memory code   | 0xA150 |
| Entry point S3Init   | 0xA151 |
| Sending MRS2   | 0xA180 |
| Sedding MRS3   | 0xA181 |
| Sending MRS1   | 0xA182 |
| Sending MRS0   | 0xA183 |
| Continuous Pattern Read  | 0xA184 |
| Continuous Pattern Write   | 0xA185 |
| Mem: 2d RdDqs Training begin   | 0xA186 |
| Mem: Before optional callout to platform BIOS to change External Vref during 2d Training | 0xA187 |
| Mem: After optional callout to platform BIOS to change External Vref during 2d Training  | 0xA188 |
| Configure DCT For General use begin  | 0xA189 |
| Configure DCT For training begin   | 0xA18A |
| Configure DCT For Non-Explicit   | 0xA18B |
| Configure to Sync channels   | 0xA18C |
| Allocate C6 Storage  | 0xA18D |
| Before LV DDR4   | 0xA18E |
| // BR CPU  |        |
| BR before AP launch  | 0xA190 |
| Install AP launched PPI  | 0xA191 |
| BR after AP launch   | 0xA192 |
| Before CPU PM  | 0xA193 |
| Enable IO Cstate   | 0xA194 |
| Enable C6  | 0xA195 |
| Install CCX PEI complete PPI   | 0xA196 |
| BR CPU memory done call back entry   | 0xA197 |
| Before APM weights   | 0xA198 |
| After APM weights  | 0xA199 |
| BR CPU memory done call back end   | 0xA19A |
| BR Init Mid entry  | 0xA19B |
| BR enable APM  | 0xA19C |
| BR Init Mid install protocol   | 0xA19D |



|                                  |        |
|----------------------------------|--------|
| BR Init Mid end                  | 0xA19E |
| BR Init Late entry               | 0xA19F |
| BR Init Late install protocol    | 0xA1A0 |
| BR Init Late end                 | 0xA1A1 |
| BR DXE install complete protocol | 0xA1A2 |
| UNB install complete PPI         | 0xA1A3 |
| UNB AfterApLaunch callback entry | 0xA1A4 |
| UNB AfterApLaunch callback end   | 0xA1A5 |

### 5-11-3 S3 Interface Post Code

|   |        |
|---|--------|
| Before the S3 save code calls out to allocate a buffer        | 0xA1EC |
| After the S3 save code calls out to allocate a buffer         | 0xA1ED |
| Before the memory S3 save code calls out to allocate a buffer | 0xA1EE |
| After the memory S3 save code calls out to allocate a buffer  | 0xA1EF |
| Before the memory code calls out to locate a buffer           | 0xA1F0 |
| After the memory code calls out to locate a buffer            | 0xA1F1 |
| Before the memory code calls out to locate a buffer           | 0xA1F2 |
| After the memory code calls out to locate a buffer            | 0xA1F3 |
| Before the memory code calls out to locate a buffer           | 0xA1F4 |
| After the memory code calls out to locate a buffer            | 0xA1F5 |
| Before the memory code calls out to locate a buffer           | 0xA1F6 |
| After the memory code calls out to locate a buffer            | 0xA1F7 |

### 5-11-4 PMU Post Code

|                     |        |
|---------------------|--------|
| Failed PMU training | 0xA1F9 |
|---------------------|--------|

### 5-11-5 [0xA5XX] assigned for AGESA PSP Module

|   |        |
|---|--------|
| // PSP V1 Modules   |        |
| PspPeiV1 entry  | 0xA501 |
| PspPeiV1 exit   | 0xA502 |
| MemoryDiscoveredPpiCallback entry                               | 0xA503 |
| MemoryDiscoveredPpiCallback exit                                | 0xA504 |
| PspDxeV1 entry  | 0xA507 |
| PspDxeV1 exit   | 0xA508 |
| PspDxeV1 PspPciEnumerationCompleteCallBack entry                | 0xA50A |
| PspDxeV1 PspPciEnumerationCompleteCallBack exit                 | 0xA50B |
| PspDxeV1 ready to boot entry                                    | 0xA50C |
| PspDxeV1 ready to boot exit                                     | 0xA50D |
| PspSmmV1 entry  | 0xA50E |
| PspSmmV1 exit   | 0xA50F |
| PspSmmV1 SwSmiCallBack entry, build the S3 save area for resume | 0xA510 |

|   |        |
|---|--------|
| PspSmmV1 SwSmiCallBack exit, build the S3 save area for resume  | 0xA511 |
| PspSmmV1 BspSmmResumeVector entry                               | 0xA512 |
| PspSmmV1 BspSmmResumeVector exit                                | 0xA513 |
| PspSmmV1 ApSmmResumeVector entry                                | 0xA514 |
| PspSmmV1 ApSmmResumeVector exit                                 | 0xA515 |
| PspP2CmboxV1 entry  | 0xA516 |
| PspP2CmboxV1 exit   | 0xA517 |
| // PSP V2 Modules   |        |
| PspPeiV2 entry  | 0xA521 |
| PspPeiV2 exit   | 0xA522 |
| PspDxeV2 entry  | 0xA523 |
| PspDxeV2 exit   | 0xA524 |
| PspDxeV2 PspMpServiceCallBack entry                             | 0xA525 |
| PspDxeV2 PspMpServiceCallBack exit                              | 0xA526 |
| PspDxeV2 FlashAccCallBack entry                                 | 0xA527 |
| PspDxeV2 FlashAccCallBack exit                                  | 0xA528 |
| PspDxeV2 ready to boot entry                                    | 0xA529 |
| PspDxeV2 ready to boot exit                                     | 0xA52A |
| PspDxeV2 exit boot service entry                                | 0xA52B |
| PspDxeV2 exit boot service exit                                 | 0xA52C |
| PspSmmV2 entry  | 0xA52D |
| PspSmmV2 exit   | 0xA52E |
| PspSmmV2 SwSmiCallBack entry, build the S3 save area for resume | 0xA52F |
| PspSmmV2 SwSmiCallBack exit, build the S3 save area for resume  | 0xA530 |
| PspSmmV2 BspSmmResumeVector entry                               | 0xA531 |
| PspSmmV2 BspSmmResumeVector exit                                | 0xA532 |
| PspSmmV2 ApSmmResumeVector entry                                | 0xA533 |
| PspSmmV2 ApSmmResumeVector exit                                 | 0xA534 |
| PspP2CmboxV2 entry  | 0xA535 |
| PspP2CmboxV2 exit   | 0xA536 |
| TpPspRecoverApcbFail  | 0xA537 |
| // PSP fTpm modules   |        |
| PspfTpmPei entry  | 0xA540 |
| PspfTpmPei exit   | 0xA541 |
| PspfTpmPei memory callback entry                                | 0xA542 |
| PspfTpmPei memory callback exit                                 | 0xA543 |
| PspfTpmDxe entry  | 0xA544 |
| PspfTpmDxe exit   | 0xA545 |
| // P2C mailbox Handling [0xA59X]                                |        |
| PspP2Cmbox Command SpiGetAttrib Handling entry                  | 0xA591 |

|   |        |
|---|--------|
| PspP2Cmbox Command SpiSetAttrib Handling entry    | 0xA592 |
| PspP2Cmbox Command SpiGetBlockSize Handling entry | 0xA593 |
| PspP2Cmbox Command SpiReadFV Handling entry       | 0xA594 |
| PspP2Cmbox Command SpiWriteFV Handling entry      | 0xA595 |
| PspP2Cmbox Command SpiEraseFV Handling entry      | 0xA596 |
| PspP2Cmbox Command Handling exit                  | 0xA59E |
| PspP2Cmbox Command Handling Fail exit             | 0xA59F |
| // C2P mailbox Handling                           |        |
| PSP C2P mailbox entry base [0xA5BX   Cmd]         | 0xA5B0 |
| Before send C2P command MboxBiosCmdDramInfo       | 0xA5B1 |
| Before send C2P command MboxBiosCmdSmmInfo        | 0xA5B2 |
| Before send C2P command MboxBiosCmdSleep SxInfo   | 0xA5B3 |
| Before send C2P command MboxBiosCmdRsmInfo        | 0xA5B4 |
| Before send C2P command MboxBiosCmdQueryCap       | 0xA5B5 |
| Before send C2P command MboxBiosCmdBootDone       | 0xA5B6 |
| Before send C2P command MboxBiosCmdClearS3Sts     | 0xA5B7 |
| Before send C2P command MboxBiosCmdS3DataInfo     | 0xA5B8 |
| Before send C2P command MboxBiosCmdNop            | 0xA5B9 |
| Before send C2P command MboxBiosCmdHSTIQuery      | 0xA5C4 |
| Before send C2P command MboxBiosCmdClrSmmLock     | 0xA5C7 |
| Before send C2P command MboxBiosCmdPciInfo        | 0xA5C8 |
| Before send C2P command MboxBiosCmdGetVersion     | 0xA5C9 |
| PSP C2P mailbox exit base [0xA5DX   Cmd]          | 0xA5D0 |
| Wait C2P command MboxBiosCmdDramInfo finished     | 0xA5D1 |
| Wait C2P command MboxBiosCmdSmmInfo finished      | 0xA5D2 |
| Wait C2P command MboxBiosCmdSleep SxInfo finished | 0xA5D3 |
| Wait C2P command MboxBiosCmdRsmInfo finished      | 0xA5D4 |
| Wait C2P command MboxBiosCmdQueryCap finished     | 0xA5D5 |
| Wait C2P command MboxBiosCmdBootDone finished     | 0xA5D6 |
| Wait C2P command MboxBiosCmdClearS3Sts finished   | 0xA5D7 |
| Wait C2P command MboxBiosCmdS3DataInfo finished   | 0xA5D8 |
| Wait C2P command MboxBiosCmdNop finished          | 0xA5D9 |
| Wait C2P command MboxBiosCmdHSTIQuery finished    | 0xA5E4 |
| Wait C2P command MboxBiosCmdClrSmmLock finished   | 0xA5C7 |
| Wait C2P command MboxBiosCmdPciInfo finished      | 0xA5C8 |
| Wait C2P command MboxBiosCmdGetVersion finished   | 0xA5C9 |
| // fTPM command Handling [0xA5FX]                 |        |
| PspfTpm send TPM command entry                    | 0xA5F0 |
| PspfTpm send TPM command exit                     | 0xA5F1 |
| PspfTpm receive TPM command entry                 | 0xA5F2 |
| PspfTpm receive TPM command exit                  | 0xA5F3 |

## 5-11-6 [0xA9XX, 0xAAXX] assigned for AGESA NBIO Module

|                                |        |
|--------------------------------|--------|
| // NbioBase                    |        |
| AmdNbioBase PEIM driver entry  | 0xA900 |
| AmdNbioBase PEIM driver exit   | 0xA901 |
| AmdNbioBase DXE driver entry   | 0xA902 |
| AmdNbioBase DXE driver exit    | 0xA903 |
| // PCIe                        |        |
| AmdNbioPcie PEIM driver entry  | 0xA904 |
| AmdNbioPcie PEIM driver exit   | 0xA905 |
| AmdNbioPcie DXE driver entry   | 0xA906 |
| AmdNbioPcie DXE driver exit    | 0xA907 |
| // GFX                         |        |
| AmdNbioGfx PEIM driver entry   | 0xA908 |
| AmdNbioGfx PEIM driver exit    | 0xA909 |
| AmdNbioGfx DXE driver entry    | 0xA90A |
| AmdNbioGfx DXE driver exit     | 0xA90B |
| // IOMMU                       |        |
| AmdNbiolommu DXE driver entry  | 0xA90C |
| AmdNbiolommu DXE driver exit   | 0xA90D |
| // ALIB                        |        |
| AmdNbioALIB DXE driver entry   | 0xA90E |
| AmdNbioALIB DXE driver exit    | 0xA90F |
| // SMU                         |        |
| AmdSmuV8 PEIM driver entry     | 0xA910 |
| AmdSmuV8 PEIM driver exit      | 0xA911 |
| AmdSmuV8 DXE driver entry      | 0xA912 |
| AmdSmuV8 DXE driver exit       | 0xA913 |
| AmdSmuV9 PEIM driver entry     | 0xA914 |
| AmdSmuV9 PEIM driver exit      | 0xA915 |
| AmdSmuV9 DXE driver entry      | 0xA916 |
| AmdSmuV9 DXE driver exit       | 0xA917 |
| AmdSmuV10 PEIM driver entry    | 0xA918 |
| AmdSmuV10 PEIM driver exit     | 0xA919 |
| AmdSmuV10 DXE driver entry     | 0xA91A |
| AmdSmuV10 DXE driver exit      | 0xA91B |
| // IOMMU PEIM                  |        |
| AmdNbiolommu PEIM driver entry | 0xA920 |
| AmdNbiolommu PEIM driver exit  | 0xA921 |
| // APB DXE                     |        |
| APCB DXE Entry                 | 0xA922 |
| APCB DXE Exit                  | 0xA923 |

|  |        |
|--|--------|
| // APCB SMM                                    |        |
| APCB SMM Entry                                 | 0xA924 |
| APCB SMM Exit                                  | 0xA925 |
| // [0xA950, 0xA99F] NBIO PPI/PROTOCOL Callback |        |
| NbioTopologyConfigureCallback entry            | 0xA950 |
| NbioTopologyConfigureCallback exit             | 0xA951 |
| MemoryConfigDoneCallbackPpi entry              | 0xA952 |
| MemoryConfigDoneCallbackPpi exit               | 0xA953 |
| DxioInitializationCallbackPpi entry            | 0xA954 |
| DxioInitializationCallbackPpi exit             | 0xA955 |
| DispatchSmuV9Callback entry                    | 0xA956 |
| DispatchSmuV9Callback exit                     | 0xA957 |
| DispatchSmuV10Callback entry                   | 0xA958 |
| DispatchSmuV10Callback exit                    | 0xA959 |
| AmdPcieMisclnit Event entry                    | 0xA95A |
| AmdPcieMisclnit Event exit                     | 0xA95B |
| NbioBaseHookReadyToBoot Event entry            | 0xA95C |
| NbioBaseHookReadyToBoot Event exit             | 0xA95D |
| NbioBaseHookPciO Event entry                   | 0xA95E |
| NbioBaseHookPciO Event exit                    | 0xA95F |
| // [0xA980, 0xA99F] BR GNB Task                |        |
| GnbEarlyInterfaceCZ entry                      | 0xA970 |
| GnbEarlyInterfaceCZ exit                       | 0xA971 |
| PcieConfigurationInit entry                    | 0xA972 |
| PcieConfigurationInit exit                     | 0xA973 |
| GnbEarlierInterfaceCZ entry                    | 0xA974 |
| GnbEarlierInterfaceCZ exit                     | 0xA975 |
| PcieEarlyInterfaceCZ entry                     | 0xA976 |
| PcieEarlyInterfaceCZ exit                      | 0xA977 |
| PciePostEarlyInterfaceCZ entry                 | 0xA978 |
| PciePostEarlyInterfaceCZ exit                  | 0xA979 |
| GfxConfigPostInterfaceCZ entry                 | 0xA97A |
| GfxConfigPostInterfaceCZ exit                  | 0xA97B |
| GfxPostInterfaceCZ entry                       | 0xA97C |
| GfxPostInterfaceCZ exit                        | 0xA97D |
| GnbPostInterfaceCZ entry                       | 0xA97E |
| GnbPostInterfaceCZ exit                        | 0xA97F |
| PciePostInterfaceCZ entry                      | 0xA980 |
| PciePostInterfaceCZ exit                       | 0xA981 |
| GnbEnvInterfaceCZ entry                        | 0xA982 |
| GnbEnvInterfaceCZ exit                         | 0xA983 |

|                                  |        |
|----------------------------------|--------|
| GfxConfigEnvInterface entry      | 0xA984 |
| GfxConfigEnvInterface exit       | 0xA985 |
| GfxEnvInterfaceCZ entry          | 0xA986 |
| GfxEnvInterfaceCZ exit           | 0xA987 |
| GfxMidInterfaceCZ entry          | 0xA988 |
| GfxMidInterfaceCZ exit           | 0xA989 |
| GfxIntInfoTableInterfaceCZ entry | 0xA98A |
| GfxIntInfoTableInterfaceCZ exit  | 0xA98B |
| PcieMidInterfaceCZ entry         | 0xA98C |
| PcieMidInterfaceCZ exit          | 0xA98D |
| GnbMidInterfaceCZ entry          | 0xA98E |
| GnbMidInterfaceCZ exit           | 0xA98F |
| GnbSmuMidInterfaceCZ entry       | 0xA990 |
| GnbSmuMidInterfaceCZ exit        | 0xA991 |
| InvokeAmdInitLate entry          | 0xA992 |
| InvokeAmdInitLate exit           | 0xA993 |
| GnbSmuServiceRequestV8 entry     | 0xA994 |
| GnbSmuServiceRequestV8 exit      | 0xA995 |

### 5-11-7 [0xACXX] assigned for AGESA CCX Module

|                                      |        |
|--------------------------------------|--------|
| CCX IDS IDS_HOOK_CCX_AFTER_AP_LAUNCH | 0xAC10 |
| CCX PEI entry                        | 0xAC50 |
| CCX downcore entry                   | 0xAC51 |
| CCX DXE entry                        | 0xAC55 |
| CCX MP service callback entry        | 0xAC56 |
| CCX Read To Boot callback entry      | 0xAC57 |
| CCX SMM entry                        | 0xAC5D |
| CCX PEI start to launch APs for S3   | 0xAC70 |
| CCX PEI end of launching APs for S3  | 0xAC71 |
| CCX start to launch AP               | 0xAC90 |
| CCX launch AP is ended               | 0xAC91 |
| CCX launch AP abort                  | 0xAC92 |
| CCX MP service abort                 | 0xAC93 |
| CCX cac weights                      | 0xAC94 |
| CCX PEI exit                         | 0xACE0 |
| CCX downcore exit                    | 0xACE1 |
| CCX DXE exit                         | 0xACE5 |
| CCX MP service callback exit         | 0xACE6 |
| CCX Read To Boot callback exit       | 0xACE7 |
| CCX SMM exit                         | 0xACED |

### 5-11-8 [0xADXX] assigned for AGESA DF Module

|                        |        |
|------------------------|--------|
| DF PEI entry           | 0xAD50 |
| DF DXE entry           | 0xAD55 |
| DF Ready to Boot entry | 0xAD56 |
| DF PEI exit            | 0xADE0 |
| DF DXE exit            | 0xADE5 |
| DF Ready to Boot exit  | 0xADE6 |

### 5-11-9 [0xAFXX] assigned for AGESA FCH Module

|                                   |        |
|-----------------------------------|--------|
| FCH InitReset dispatch point      | 0xAF01 |
| FCH InitEnv dispatch point        | 0xAF06 |
| FCH InitMid dispatch point        | 0xAF07 |
| FCH InitLate dispatch point       | 0xAF08 |
| FCH Inits3Early dispatch point    | 0xAF0B |
| FCH Inits3Late dispatch point     | 0xAF0C |
| FCH Inits3Early dispatch finished | 0xAF0D |
| FCH Inits3Late dispatch finished  | 0xAF0E |
| FCH Pei Entry                     | 0xAF10 |
| FCH Pei Exit                      | 0xAF11 |
| FCH MultiFch Pei Entry            | 0xAF12 |
| FCH MultiFch Pei Exit             | 0xAF13 |
| FCH Dxe Entry                     | 0xAF14 |
| FCH Dxe Exit                      | 0xAF15 |
| FCH MultiFch Dxe Entry            | 0xAF16 |
| FCH MultiFch Dxe Exit             | 0xAF17 |
| FCH Smm Entry                     | 0xAF18 |
| FCH Smm Exit                      | 0xAF19 |
| FCH Smm Dispatcher Entry          | 0xAF20 |
| FCH Smm Dispatcher Exit           | 0xAF21 |
| FCH InitReset HwAcpi              | 0xAF40 |
| FCH InitReset AB Link             | 0xAF41 |
| FCH InitReset LPC                 | 0xAF42 |
| FCH InitReset SPI                 | 0xAF43 |
| FCH InitReset eSPI                | 0xAF44 |
| FCH InitReset SD                  | 0xAF45 |
| FCH InitReset eMMC                | 0xAF46 |
| FCH InitReset SATA                | 0xAF47 |
| FCH InitReset USB                 | 0xAF48 |
| FCH InitReset xGbE                | 0xAF49 |
| FCH InitReset HwAcpiP             | 0xAF4F |
| FCH InitEnv HwAcpi                | 0xAF50 |

|                         |        |
|-------------------------|--------|
| FCH InitEnv AB Link     | 0xAF51 |
| FCH InitEnv LPC         | 0xAF52 |
| FCH InitEnv SPI         | 0xAF53 |
| FCH InitEnv eSPI        | 0xAF54 |
| FCH InitEnv SD          | 0xAF55 |
| FCH InitEnv eMMC        | 0xAF56 |
| FCH InitEnv SATA        | 0xAF57 |
| FCH InitEnv USB         | 0xAF58 |
| FCH InitEnv xGbE        | 0xAF59 |
| FCH InitEnv HwAcpiP     | 0xAF5F |
| FCH InitMid HwAcpi      | 0xAF60 |
| FCH InitMid AB Link     | 0xAF61 |
| FCH InitMid LPC         | 0xAF62 |
| FCH InitMid SPI         | 0xAF63 |
| FCH InitMid eSPI        | 0xAF64 |
| FCH InitMid SD          | 0xAF65 |
| FCH InitMid eMMC        | 0xAF66 |
| FCH InitMid SATA        | 0xAF67 |
| FCH InitMid USB         | 0xAF68 |
| FCH InitMid xGbE        | 0xAF69 |
| FCH InitLate HwAcpi     | 0xAF70 |
| FCH InitLate AB Link    | 0xAF71 |
| FCH InitLate LPC        | 0xAF72 |
| FCH InitLate SPI        | 0xAF73 |
| FCH InitLate eSPI       | 0xAF74 |
| FCH InitLate SD         | 0xAF75 |
| FCH InitLate eMMC       | 0xAF76 |
| FCH InitLate SATA       | 0xAF77 |
| FCH InitLate USB        | 0xAF78 |
| FCH InitLate xGbE       | 0xAF79 |
| End of TP range for FCH | 0xAFFF |
| Last defined AGESA PCs  | 0xFFFF |



## 5-12 BIOS POST Beep code (AMI standard)

### 5-12-1 PEI Beep Codes

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

### 5-12-2 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      |

This page intentionally left blank