

# **GIGABYTE™**

## **MJ11-EC0**

AMD EPYC™ Embedded 3000 Series Processor Motherboard

### **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 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 <http://esupport.gigabyte.com/> to create a new support ticket.

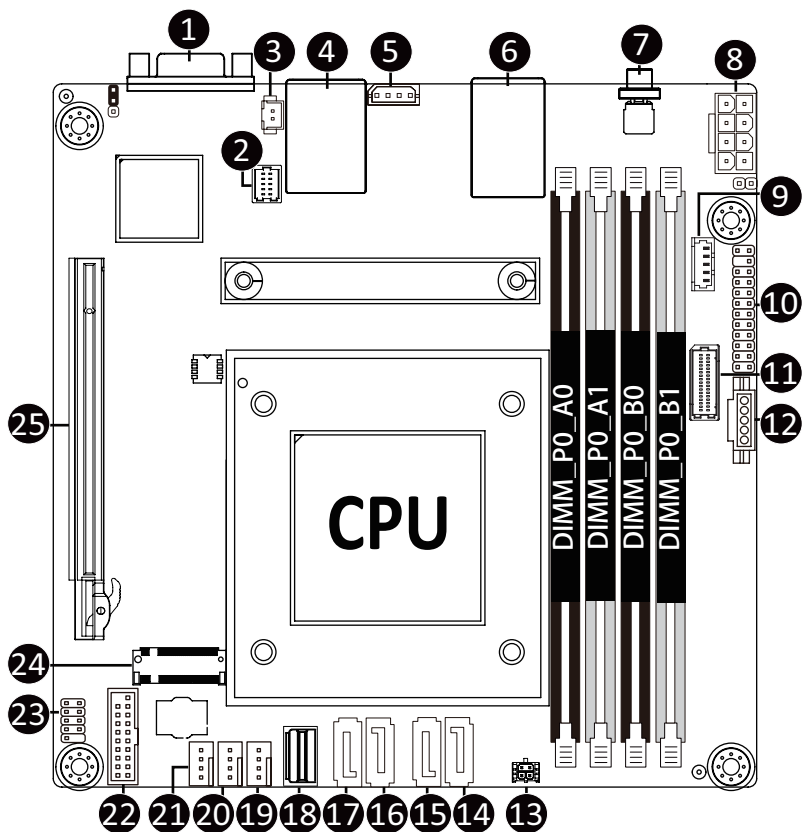
For any general sales or marketing enquires, you may message GIGABYTE server directly by email: [server.grp@gigabyte.com](mailto:server.grp@gigabyte.com).

# Table of Contents

MJ11-EC0 Motherboard Layout.....	5
Block Diagram .....	7
Chapter 1 Hardware Installation .....	8
1-1 Installation Precautions .....	8
1-2 Product Specifications.....	9
1-3 Installing and Removing Memory.....	11
1-3-1 2-Channel Memory Configuration .....	11
1-3-2 Installing and Removing a Memory Module .....	12
1-3-3 DIMM Population Table .....	12
1-4 Installing and Removing the M.2 SSD Module.....	13
1-5 Back Panel Connectors.....	14
1-6 Internal Connectors.....	15
1-7 Jumper Settings .....	23
Chapter 2 BIOS Setup .....	24
2-1 The Main Menu .....	26
2-2 Advanced Menu .....	29
2-2-1 Trusted Computing .....	30
2-2-2 PSP Firmware Versions.....	32
2-2-3 AST2500 Super IO Configuration .....	33
2-2-4 S5 RTC Wake Settings.....	35
2-2-5 Serial Port Console Redirection .....	36
2-2-6 CPU Configuration.....	39
2-2-7 PCI Subsystem Settings.....	40
2-2-8 USB Configuration .....	42
2-2-9 NVMe Configuration .....	44
2-2-10 SATA Configuration.....	45
2-2-11 AMD CBS .....	46
2-2-12 Network Stack Configuration .....	62
2-2-13 iSCSI Configuration .....	63
2-2-14 T1s Auth Configuration .....	64
2-2-15 Intel(R) I210 Gigabit Network Connection .....	65
2-2-16 VLAN Configuration.....	67
2-2-17 MAC IPv4 Network Configuration .....	69
2-2-18 MAC IPv6 Network Configuration .....	70
2-3 Chipset Setup Menu.....	72
2-3-1 North Bridge .....	73

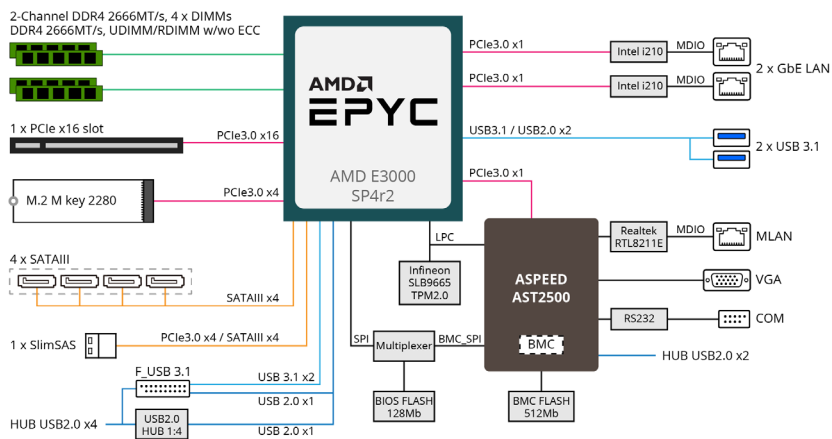
2-3-2	Error Management.....	74
2-4	Server Management Menu.....	75
2-4-1	System Event Log .....	77
2-4-2	View FRU Information .....	78
2-4-3	BMC Network Configuration .....	79
2-4-4	IPv6 BMC Network Configuration .....	80
2-5	Security Menu .....	81
2-5-1	Secure Boot .....	82
2-6	Boot Menu.....	85
2-7	Save & Exit Menu.....	87
2-8	ABL POST Codes .....	88
2-8-1	StartProcessorTestPoints .....	88
2-8-2	Memory test points .....	88
2-8-3	PMU Test Points .....	88
2-8-4	Original Post Code .....	89
2-8-5	CPU test points.....	90
2-8-6	Topology test points.....	90
2-8-7	Extended memory test point.....	90
2-8-8	Gnb Earlier init.....	91
2-8-9	PMU test points .....	94
2-8-10	ABL0 test points .....	94
2-8-11	ABL5 test points .....	94
2-9	Agesa POST Codes.....	98
2-9-1	Universal Post Code.....	98
2-9-2	[0xA1XX] For CZ only memory Postcodes.....	98
2-9-3	S3 Interface Post Code .....	101
2-9-4	PMU Post Code.....	101
2-9-5	[0xA5XX] assigned for AGESA PSP Module .....	101
2-9-6	[0xA9XX, 0xAAXX] assigned for AGESA NBIO Module.....	104
2-9-7	[0xACXX] assigned for AGESA CCX Module .....	106
2-9-8	[0xADXX] assigned for AGESA DF Module.....	107
2-9-9	[0xAFXX] assigned for AGESA FCH Module.....	107
2-10	BIOS POST Beep code (AMI standard).....	109
2-10-1	PEI Beep Codes .....	109
2-10-2	DXE Beep Codes .....	109

# MJ11-EC0 Motherboard Layout



Item	Code	Description
1	VGA	VGA Port
2	80H	80 Debug Port
3	BAT	Battery Cable Connector
4	USB3_MLAN	Server Management LAN Port (Top)/ USB3.1 Ports (Bottom)
5	IPMB	IPMB Connector
6	LAN1_2	GbE Ethernet LAN Port #1 Support NCSI (Top)/ GbE Ethernet LAN Port #2 (Bottom)
7	SW_PWR_ID	Power Button (Top)/ ID Button with LED (Bottom)
8	P12V_AUX1	2x4 Pin 12V Power Connector
9	SGPIO1	SATA SGPIO Connector
10	FP_1	Front Panel Header
11	BP_1	HDD Back Plane Board Connector
12	PMBUS	PMBus Connector
13	DC_IN1	2x2 Pin 5VSB/PSON Power Connector
14	SATA0	SATA III 6Gb/s Connector #0
15	SATA1	SATA III 6Gb/s Connector #1
16	SATA2	SATA III 6Gb/s Connector #2
17	SATA3	SATA III 6Gb/s Connector #3
18	SL_SAS	SlimLine SAS 4i Connector (SATA III/ PCIe Signal)
19	CPU0_FAN	CPU Fan Connector
20	SYS_FAN1	System Fan Connector #1
21	SYS_FAN2	System Fan Connector #2
22	F_USB3	Front Panel USB 3.1 Connector
23	COM1	Serial Port Header
24	M2_M	M.2 slot (PCIe Gen3 x4, Support NGFF-2280)
25	PCIE_1	PCIe x16 Slot (Gen3 x16)

# Block Diagram



# Chapter 1 Hardware Installation










## 1-1 Installation Precautions




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

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



## 1-2 Product Specifications

 CPU	<ul style="list-style-type: none"> <li>◆ AMD EPYC™ 3151 SoC processor</li> <li>◆ Single processor, 7nm, TDP 45W</li> <li>◆ Processor Frequency: 2.7GHz-2.9GHz</li> <li>◆ Up to 4-core, 8 threads per processor</li> <li>◆ 2MB L2 Cache, 16MB L3 Cache</li> </ul>
 Chipset	<ul style="list-style-type: none"> <li>◆ System on Chip</li> </ul>
 Memory	<ul style="list-style-type: none"> <li>◆ 4 x DIMM slots</li> <li>◆ DDR4 memory supported only</li> <li>◆ Dual Channel memory architecture</li> <li>◆ UDIMM, UDIMM ECC, RDIMM modules up to 128GB supported</li> <li>◆ Memory speed: Up to 2666 MHz</li> </ul>
 Onboard Graphics	<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>
 LAN	<ul style="list-style-type: none"> <li>◆ 2 x 1GbE LAN ports (Intel® I210-AT)</li> <li>◆ 1 x 10/100/1000 management LAN</li> </ul>
 Expansion Slots	<ul style="list-style-type: none"> <li>◆ 1 x PCIe x16 (Gen3 x16 bus) slot</li> </ul>
 Storage Interface	<ul style="list-style-type: none"> <li>◆ 1 x SlimSAS (with 4 x SATA 6Gb/s or PCIe Gen3 x4) connector</li> <li>◆ 4 x SATA 6Gb/s ports</li> <li>◆ 1 x M.2 slot: <ul style="list-style-type: none"> <li>- M-key</li> <li>- PCIe Gen3 x4</li> <li>- Supports NGFF-2280 cards</li> </ul> </li> </ul>
 Internal I/O Connectors	<ul style="list-style-type: none"> <li>◆ 1 x 2 x 4-pin 12V power connector</li> <li>◆ 1 x 2 x 2-pin 5VSB/PSON power connector</li> <li>◆ 1 x SlimSAS connector</li> <li>◆ 1 x M.2 slot</li> <li>◆ 1 x CPU fan header</li> <li>◆ 2 x System fan headers</li> <li>◆ 1 x USB 3.0 header</li> <li>◆ 1 x COM1 header</li> <li>◆ 1 x Front panel header</li> <li>◆ 1 x IPMB connector</li> <li>◆ 1 x PMBUS connector</li> <li>◆ 1 x Clear CMOS jumper</li> </ul>
 Rear I/O Connectors	<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 POWER button with LED</li> <li>◆ 1 x ID button with LED</li> </ul>

 TPM	<ul style="list-style-type: none"> <li>◆ Onboard INFINEON SLB9665</li> </ul>
 Board Management	<ul style="list-style-type: none"> <li>◆ Aspeed® AST2500 management controller</li> <li>◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface</li> </ul>
 Form Factor	<ul style="list-style-type: none"> <li>◆ Mini-ITX</li> <li>◆ 170W x 170D (mm)</li> </ul>
GIGABYTE reserves the right to make any changes to the product specifications and product-related information without prior notice.	

## 1-3 Installing and Removing Memory

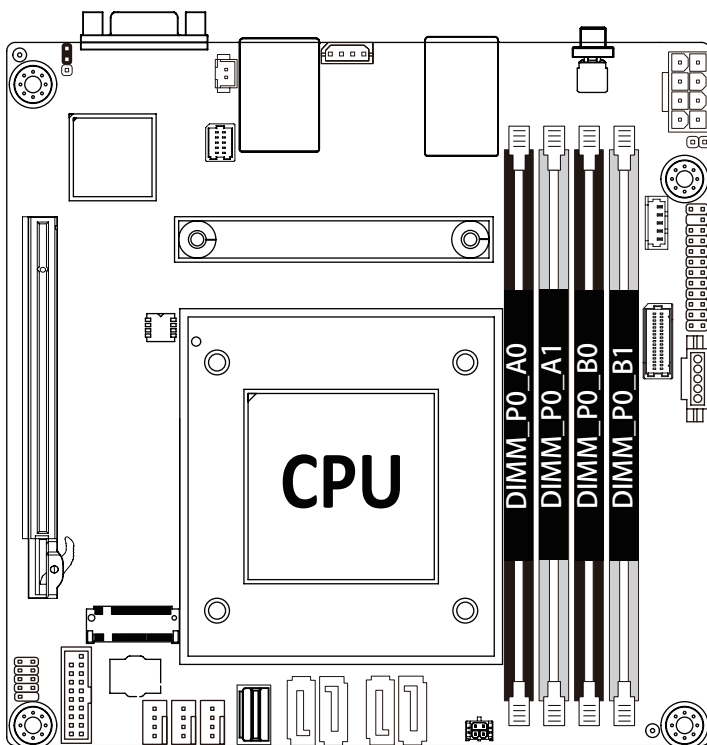


Read the following guidelines before you begin to install the memory:

- Make sure that the motherboard supports the memory. It is recommended 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.

### 1-3-1 2-Channel Memory Configuration

This motherboard provides 4 DDR4 memory sockets and supports 2-Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory.



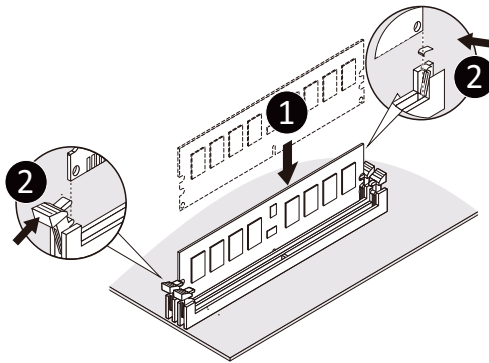
### 1-3-2 Installing and Removing a Memory Module



Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.  
Be sure to install DDR4 DIMMs on to this motherboard.

Follow these instructions to install a DIMM module:

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



### 1-3-3 DIMM Population Table

UDIMM/RDIMM Maximum Frequency Supported Table

Slots	DIMMs Populated	DIMM		Frequency (MT/s)
		1R	2R 2DR 2S2R 2S4R	1.2V
2	1	1	--	2667
		--	1	2400
	2	2	--	2133
		1	1	1866
		--	2	1866



**Note:**

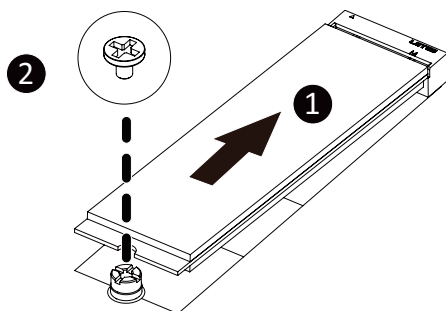
- Memory capacity 64GB/channel
- When populating DIMMs into a channel, slot numbers having the suffix "1" must be populated first, then followed by slot numbers having the suffix "0".

## 1-4 Installing and Removing the M.2 SSD Module

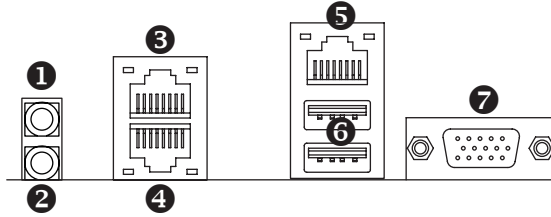
Follow the steps below to install an optional M.2 SSD module on your motherboard.

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

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



# 1-5 Back Panel Connectors



## ❶ Power Button

Press the button to turn on/off the system.

## ❷ ID button with LED

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

## ❸ RJ-45 LAN Port #1

The Gigabit Ethernet LAN port provides Internet connection at up to 1 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

## ❹ RJ-45 LAN Port #2

The Gigabit Ethernet LAN port provides Internet connection at up to 1 Gbps data rate. See the section below for a description of the states of the LAN port LEDs.

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

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

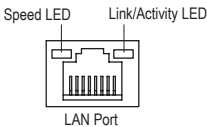
## ❻ USB 3.1 Ports

The USB port supports the USB 3.0 specification. Use this port for USB devices such as a USB keyboard/mouse, USB printer, USB flash drive etc.

## ❼ VGA Port

Connect to a monitor device.

## 10/100/1000 LAN and ID Button LEDs



10/100/1000 LAN Speed LED:

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

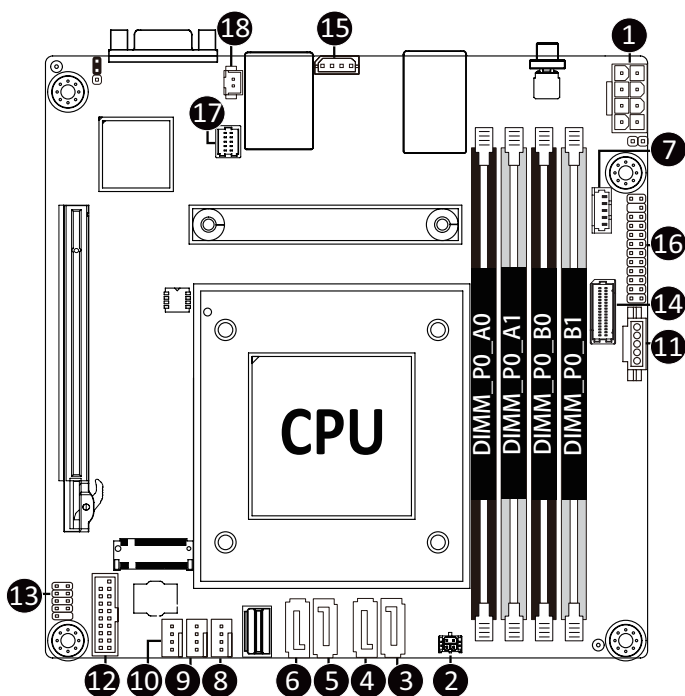
ID Button/ LED:

State	Description
Blue On	System identification is active.
Off	System identification is disabled.



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

## 1-6 Internal Connectors



1) P12V_AUX1	11) PMBUS
2) DC_IN1	12) F_USB3
3) SATA0	13) COM1
4) SATA1	14) BP_1
5) SATA2	15) IPMB
6) SATA3	16) FP_1
7) SGPIO1	17) 80H
8) CPU0_FAN	18) BAT
9) SYS_FAN1	
10) SYS_FAN2	



Read the following guidelines before connecting external devices:

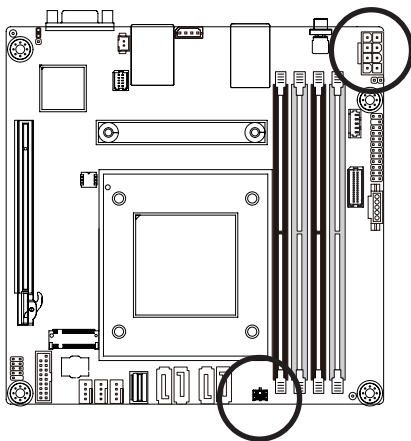
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the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

**1/2) P12V\_AUX1/DC\_IN1 (2x4 12V Power Connector & 2x2 5VSB/PSON Power Connector)**

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

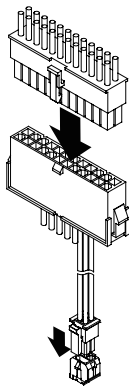
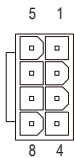


To meet expansion requirements, it is recommended that a power supply that can withstand high power consumption be used (500W or greater). If a power supply is used that does not provide the required power, the result can lead to an unstable or unbootable system.



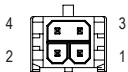
P12V\_AUX1

Pin No.	Definition
1	GND
2	GND
3	GND
4	GND
5	P12VA
6	P12VA
7	P12VA
8	P12VA



DC\_IN1 (Note)

Pin No.	Definition
1	GND
2	PS_ON
3	PWRGD
4	5VSB

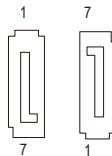
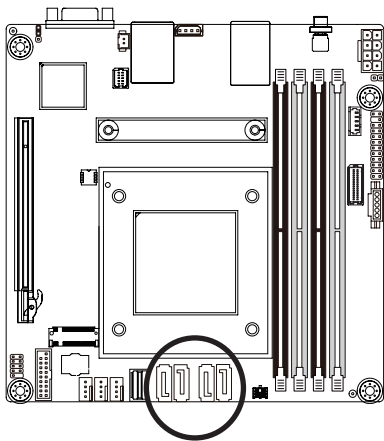


Note:  
Attach power cable to 4-pin power connector as illustration.



**3/4/5/6) SATA0/SATA1/SATA2/SATA3 (SATA 6Gb/s Connectors)**

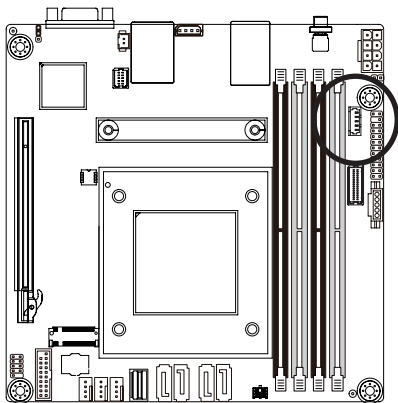
The SATA connectors conform to SATA 6Gb/s standard and are compatible with SATA 3Gb/s standard.  
Each SATA connector supports a single SATA device.



Pin No.	Definition
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND

**7) SGPIO1 (SATA SGPIO) Connector**

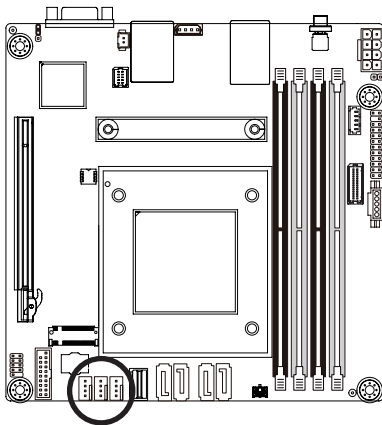
Serial General Purpose Input/Output (SGPIO) is a communication method used between a host bus adapter (HBA) and a main board.



Pin No.	Definition
1	Data In
2	GND
3	Data Out
4	Load
5	Clock

### 8/9/10) CPU0\_FAN//SYS\_FAN1//SYS\_FAN2 (CPU FAN/System FAN Headers)

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



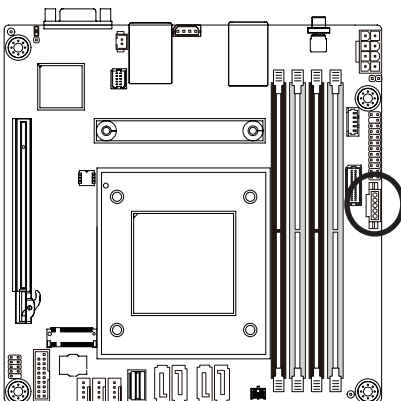
Pin No.	Definition
1	GND
2	P12V
3	FAN_TACH
4	FAN_PWM



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

### 11) PMBus Connector

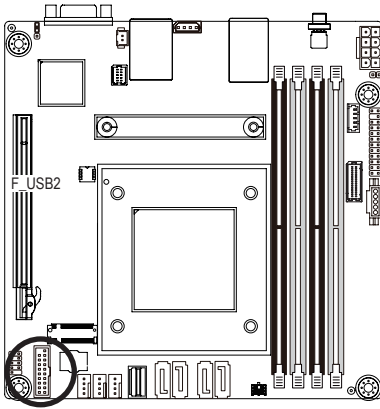
The Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



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

## 12) F\_USB3 (USB 3.1 Connector)

The connector/header conform to USB 3.1 specification. Each USB connector/header can provide two USB ports via an optional USB bracket. For purchasing the optional USB bracket, please contact the local dealer.

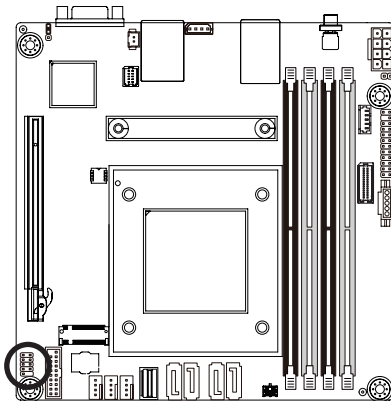


USB 3.1 Connector

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

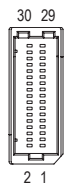
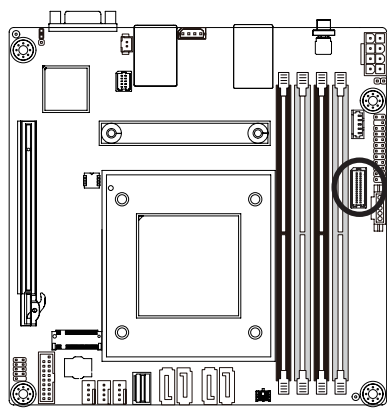
## 13) COM1 (Serial Port Header)

The COM header can provide one serial port via an optional COM port cable. For purchasing the optional COM port cable, please contact the local dealer.



Pin No.	Definition
1	DCD
2	SIN
3	SOUT
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI
10	NC

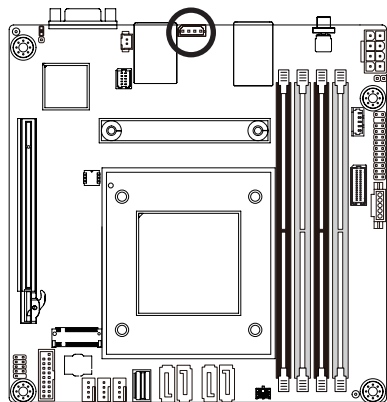
14) BP\_1 (HDD Backplane Board Header)



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

15) IPMB (Intelligent Platform Management Bus) Connector

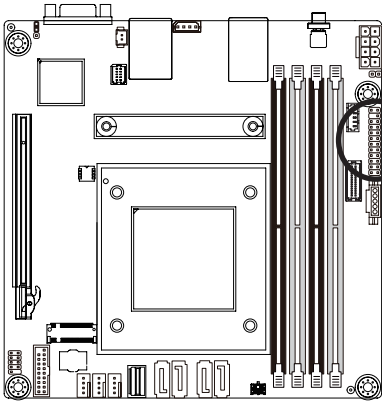
The Intelligent Platform Management Bus Communications Protocol defines a byte-level transport for transferring Intelligent Platform Management Interface Specification (IPMI) messages between intelligent I2C devices.



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

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

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

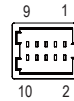
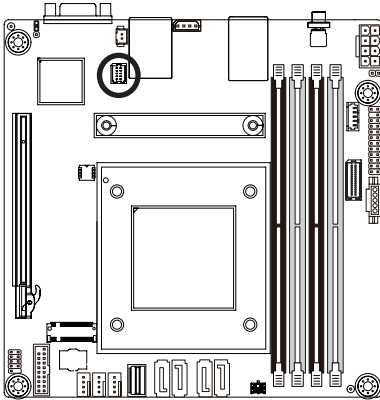


Pin No.	Definition	Pin No.	Definition
1	Power LED+	2	5VSB
3	NC	4	ID LED+
5	Power LED-	6	ID LED-
7	HDD LED+	8	F_SYSRDY
9	HDD LED- (GND)	10	SYS_STATUS-
11	PWR_BTN	12	LAN1 Active LED+
13	GND	14	LAN1 Link LED-
15	Reset Button	16	SMBus Data
17	GND	18	SMBus Clock
19	ID Button	20	Case Open
21	GND	22	LAN2 Active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



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

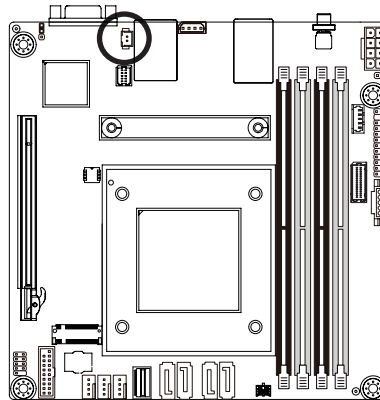
### 17) 80H (80 Debug Port)



Pin No.	Definition
1	CLOCK
2	GND
3	LPC_FRAME
4	LPC_LAD0
5	RESET
6	LPC_LAD1
7	LPC_LAD3
8	LPC_LAD2
9	P3V3
10	LPC_IRQ

### 18) BAT (Battery Socket)

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

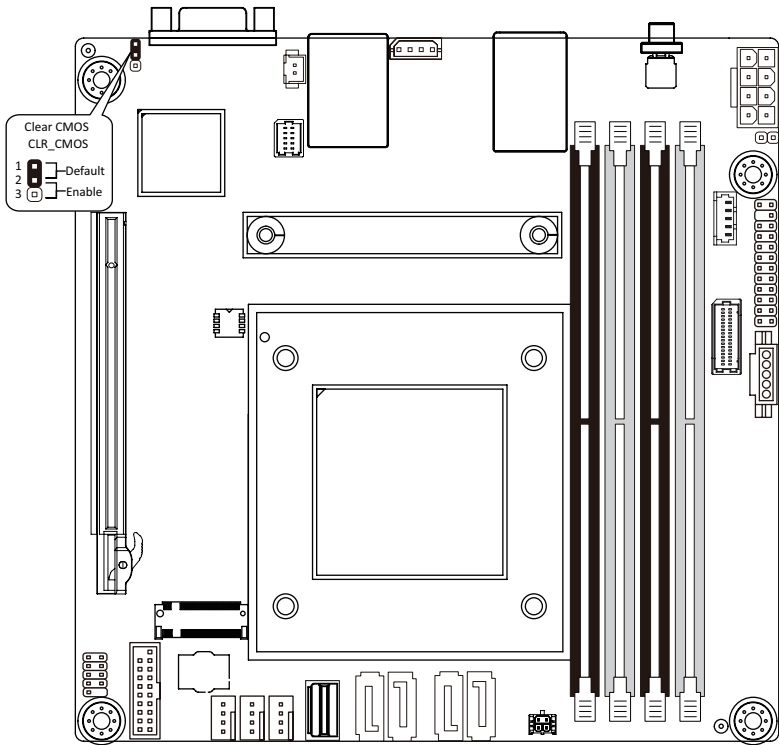


Pin No.	Definition
1	Battery+
2	GND



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

# 1-7 Jumper Settings



Jumper Name	Jumper Setting
Clear CMOS	1-2: Normal operation. (Default) 2-3: Clear CMOS data.

## Chapter 2 BIOS Setup

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

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



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

### BIOS Setup Program Function Keys

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



■ **Main**

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

■ **Advanced**

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

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

■ **Chipset**

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

## 2-1 The Main Menu

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

### Main Menu Help

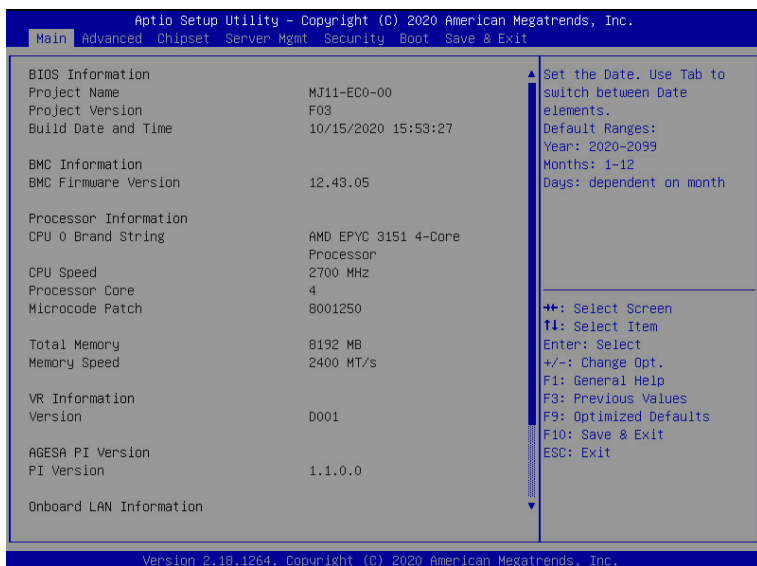
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

### Submenu Help

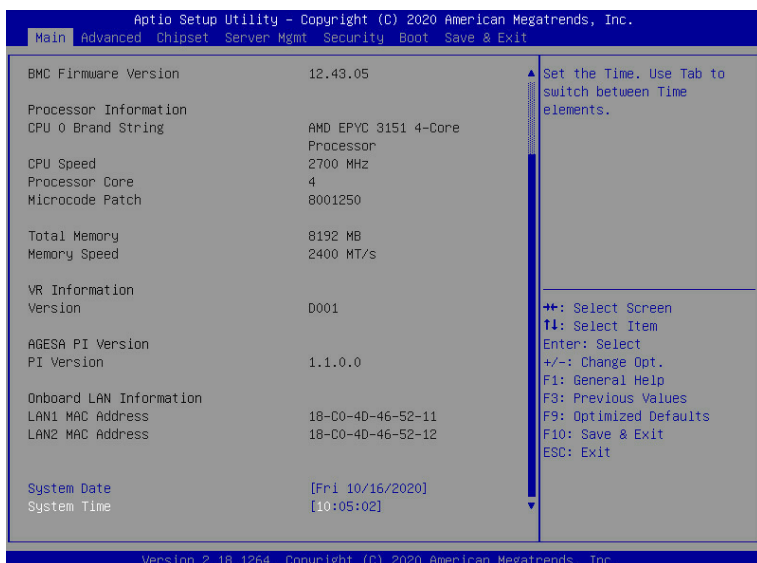
While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.



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



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



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 <sup>(Note1)</sup>	
BMC Firmware Version <sup>(Note1)</sup>	Displays BMC firmware version information.
Processor Information	
CPU0 Brand String/ CPU Speed / Processor Core / Microcode Patch	Displays the technical specifications for the installed processor(s).
Total Memory <sup>(Note2)</sup>	Displays the total memory size of the installed memory.
Memory Speed <sup>(Note2)</sup>	Displays the frequency information of the installed memory.
VR Information	
Version	Displays VR version information.

(Note1) Functions available on selected models.

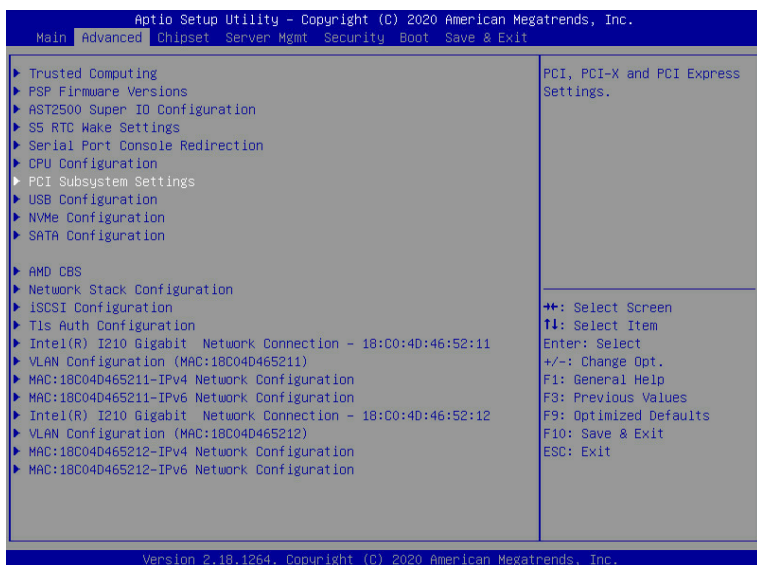
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

Parameter	Description
AGESA PI Version	
PI Version	Displays AGESA PI version information.
Onboard LAN Information	
LAN1 MAC Address <sup>(Note)</sup>	Displays LAN MAC address information.
LAN2 MAC Address <sup>(Note)</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.

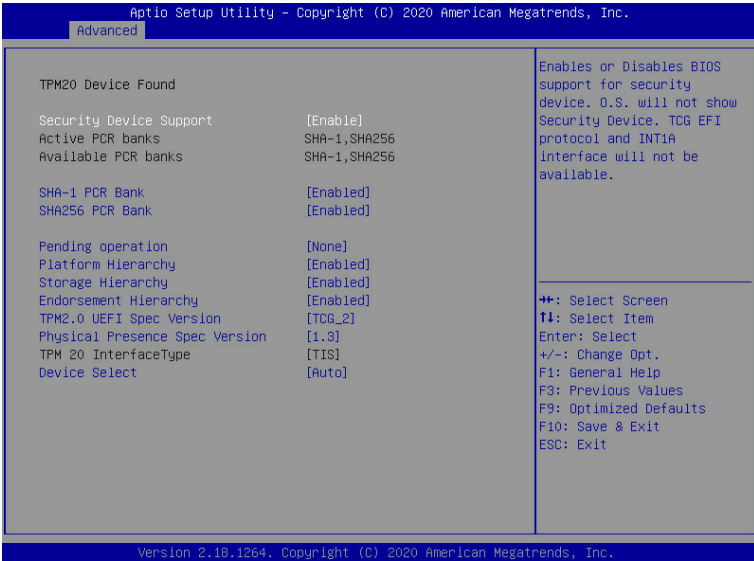
(Note) The number of LAN ports listed will depend on the motherboard / system model.

## 2-2 Advanced Menu

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



## 2-2-1 Trusted Computing

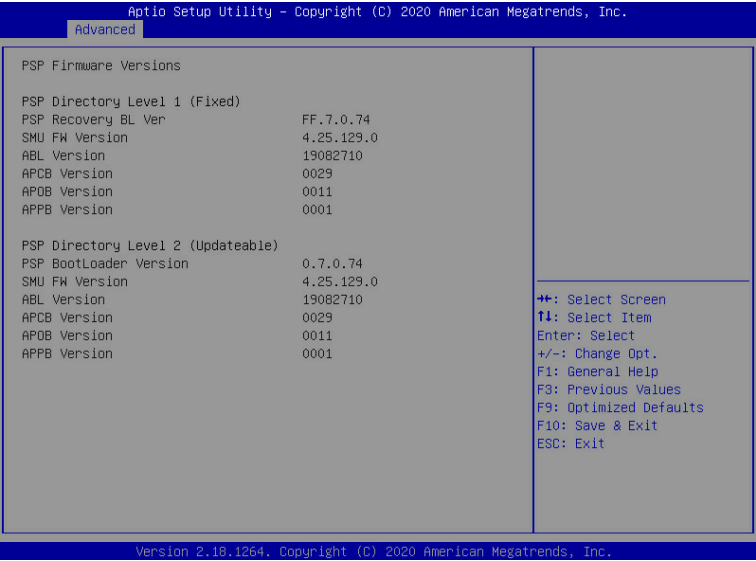


Parameter	Description
TPM20 Device Found	
Security Device Support	Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. Options available: Enable, Disable. Default setting is <b>Enable</b> .
Active PCR banks	Displays active Platform Configuration Register (PCR) banks.
Available PCR banks	Displays available PCR banks.
SHA-1 PCR Bank	Enable/Disable SHA-1 PCR bank. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
SHA256 PCR Bank	Enable/Disable SHA256 PCR bank. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Pending operation	Schedule an operation for the security device. NOTE: Your computer will reboot during restart in order to change the state of a security device. Options available: None, TPM Clear. Default setting is <b>None</b> .
Platform Hierarchy	Enable/Disable platform hierarchy. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

Parameter	Description
Storage Hierarchy	Enable/Disable storage hierarchy. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Endorsement Hierarchy	Enable/Disable endorsement hierarchy. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
TPM2.0 UEFI Spec Version	Selects the TCG2 spec version support. Options available: TCG_1_2, TCG_2. Default setting is <b>TCG2</b> .
Physical Presence Spec Version	Selects the physical presence spec version. Options available: 1.2, 1.3. Default setting is <b>1.3</b> .
TPM 20 InterfaceType	Displays the TPM 2.0 interface type.
Device Select	Selects the TPM device. Options available: TPM 1.2, TPM 2.0, Auto. Default setting is <b>Auto</b> .

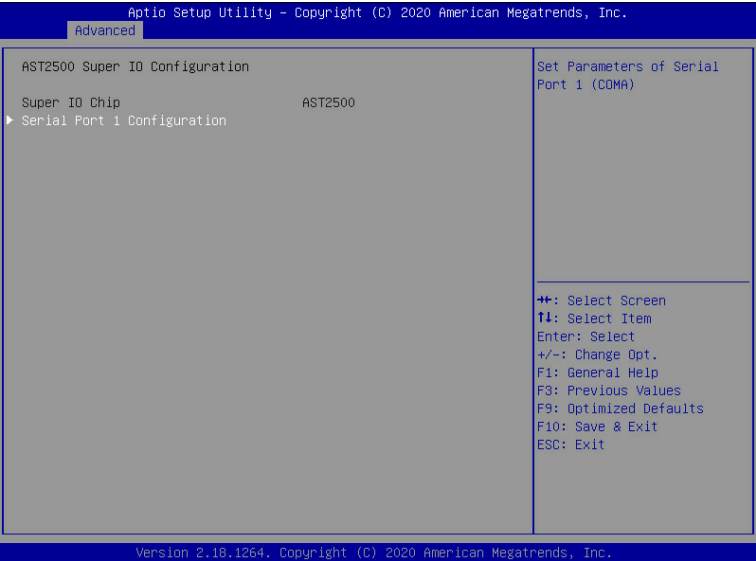
## 2-2-2 PSP Firmware Versions

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



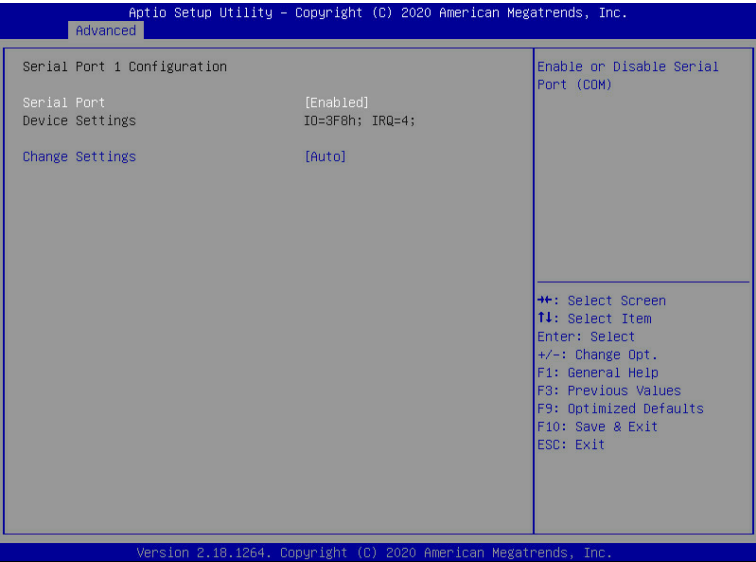


### 2-2-3 AST2500 Super IO Configuration



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

### 2-2-3-1 Serial Port 1 Configuration



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

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

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

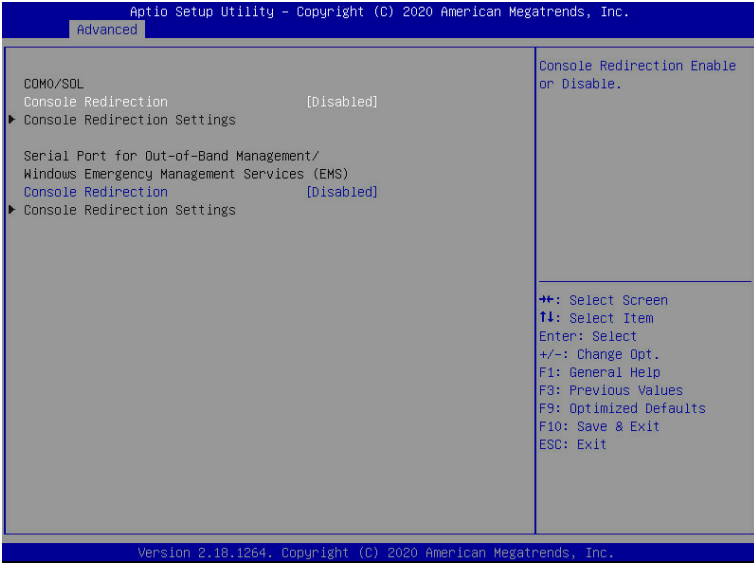
2-2-4 S5 RTC Wake Settings



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

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

## 2-2-5 Serial Port Console Redirection



Parameter	Description
COM0/Serial Over LAN Console Redirection <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>
COM0/Serial Over LAN Console Redirection Settings	<p>Press [Enter] to configure advanced items.</p> <p><b>Please note that this item is configurable when COM0/Serial Over LAN 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.

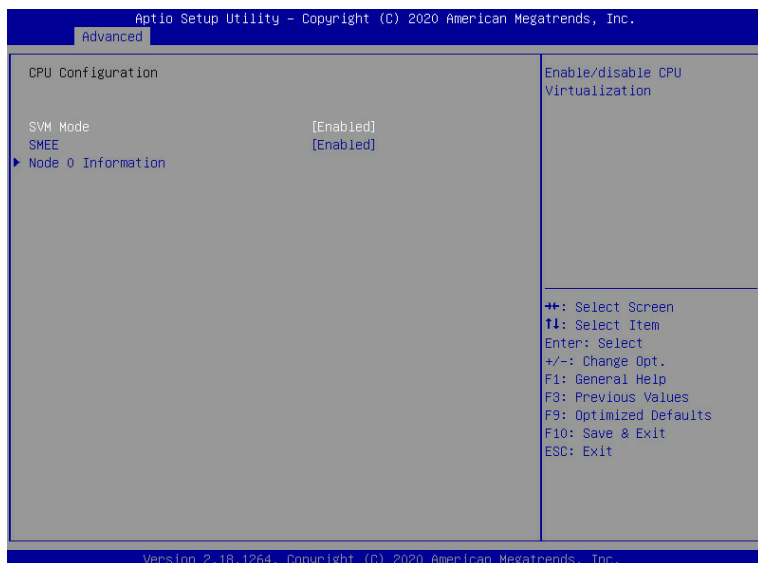
Parameter	Description
COM01/Serial Over LAN Console Redirection Settings (continued)	<ul style="list-style-type: none"> <li>◆ Parity <ul style="list-style-type: none"> <li>– A parity bit can be sent with the data bits to detect some transmission errors.</li> <li>– Even: parity bit is 0 if the num of 1's in the data bits is even.</li> <li>– Odd: parity bit is 0 if num of 1's in the data bits is odd.</li> <li>– Mark: parity bit is always 1. Space: Parity bit is always 0.</li> <li>– Mark and Space Parity do not allow for error detection.</li> <li>– Options available: None, Even, Odd, Mark, Space. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ Stop Bits <ul style="list-style-type: none"> <li>– Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.</li> <li>– Options available: 1, 2. Default setting is <b>1</b>.</li> </ul> </li> <li>◆ Flow Control <ul style="list-style-type: none"> <li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.</li> <li>– Options available: None, Hardware RTS/CTS. Default setting is <b>None</b>.</li> </ul> </li> <li>◆ VT-UTF8 Combo Key Support <ul style="list-style-type: none"> <li>– Enable/Disable the VT-UTF8 Combo Key Support.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Recorder Mode<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 KeyPad 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
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: COM0/SOL. Default setting is <b>COM0/SOL</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>VT-UTF8</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>◆ 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>

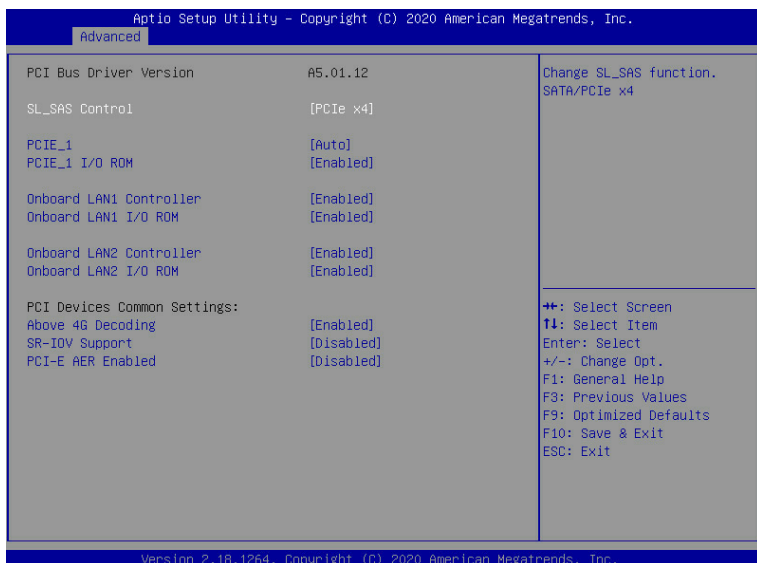
(Note) Advanced items prompt when this item is defined.

## 2-2-6 CPU Configuration



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

## 2-2-7 PCI Subsystem Settings



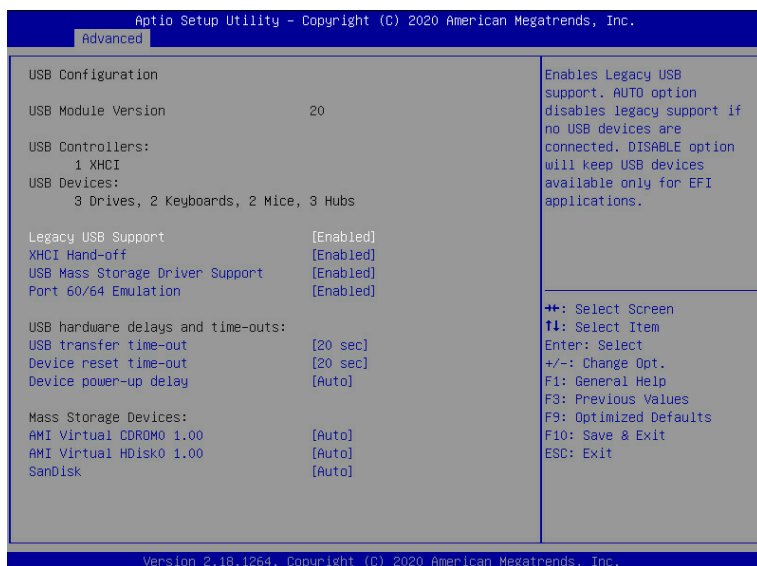
Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SL_SAS Control	Change the SL_SAS function. Options available: Disabled, SATA, PCIe x4. Default setting is <b>PCIe x4</b> .
PCIE_1 Lanes Configuration	Change the PCIe lanes. Options available: Disabled, Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is <b>Auto</b> .
PCIE_1 I/O ROM	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Onboard LAN 1/2 Controller <sup>(Note1)</sup>	Enable/Disable the onboard LAN devices. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Onboard LAN 1/2 ROM <sup>(Note1)</sup>	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. 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). Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

(Note1) This section is dependent on the available LAN controller.



Parameter	Description
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
PCI-E AER Enabled	Enable/Disable the PCI-E AER (Advanced Error Reporting) function. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .

## 2-2-8 USB Configuration

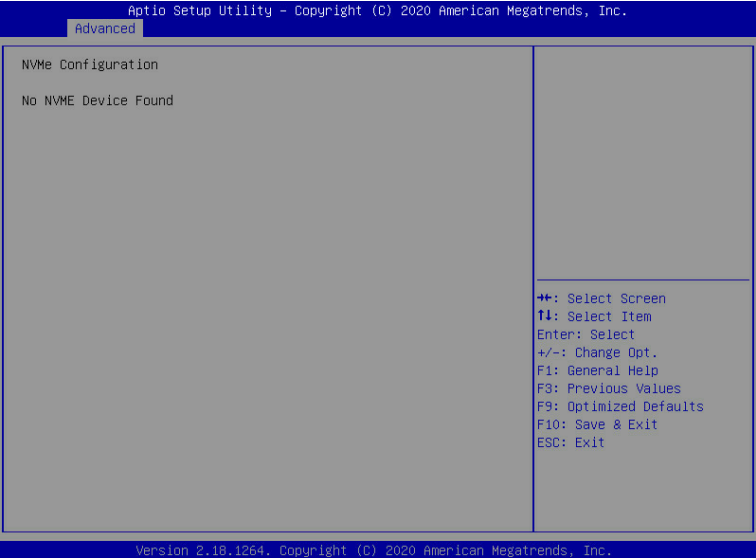


Parameter	Description
USB Configuration	
USB Module Version	Displays the USB module version information.
USB Controllers	Displays the supported USB controllers.
USB Devices:	Displays the USB devices connected to the system.
Legacy USB Support	Enable/Disable the Legacy USB support function. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. Options available: Auto, Enabled, Disabled. Default setting is <b>Enabled</b> .
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. 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. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .

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

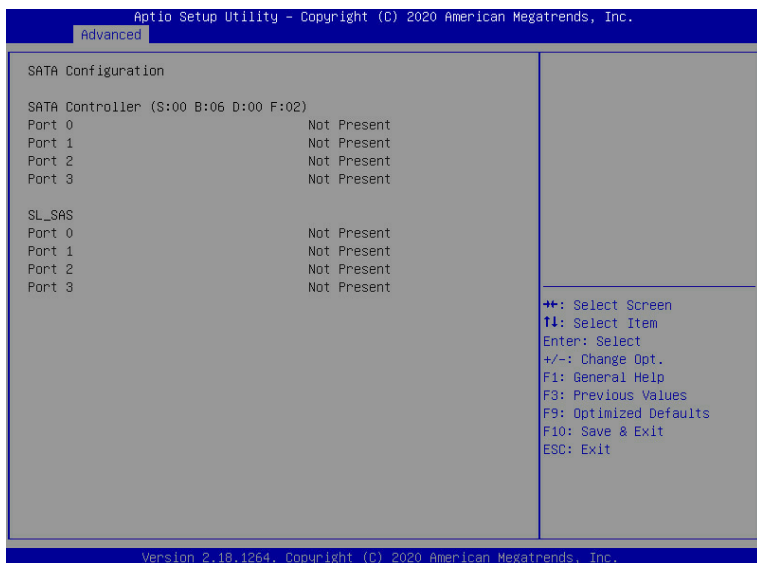
Parameter	Description
Port 60/64 Emulation	<p>Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OS.</p> <p>Options available: Enabled, Disabled. Default setting is <b>Enabled</b>.</p>
USB hardware delays and time-outs	
USB transfer time-out	<p>Selects the time-out value for USB Control/Bulk/Interrupt transfers.</p> <p>Options available: 1 sec, 5 sec, 10 sec, 20 sec.</p> <p>Default setting is <b>20 sec</b>.</p>
Device reset time-out	<p>Selects the time-out value during a USB mass storage device reset.</p> <p>Options available: 10 sec, 20 sec, 30 sec, 40 sec.</p> <p>Default setting is <b>20 sec</b>.</p>
Device power-up delay	<p>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.</p> <p>Options available: Auto, Manual. Default setting is <b>Auto</b>.</p>
Mass Storage Devices	Displays the mass storage devices available on the system.

## 2-2-9 NVMe Configuration



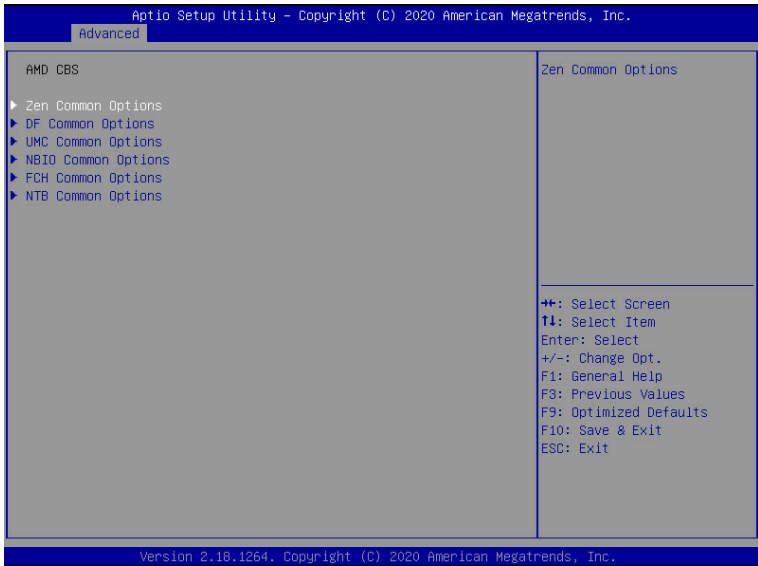
Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system.

## 2-2-10 SATA Configuration



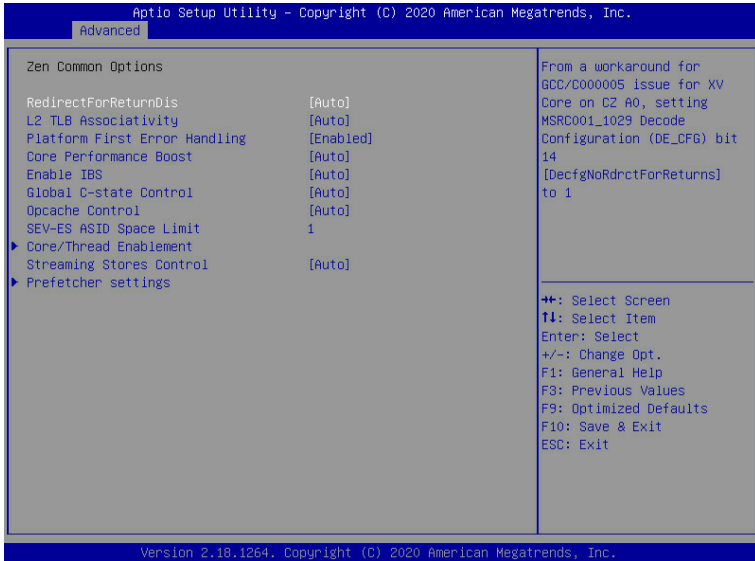
Parameter	Description
SATA Configuration	Displays the installed HDD devices information. System will automatically detect HDD type.

## 2-2-11 AMD CBS



Parameter	Description
AMD CBS	
Zen Common Options	Press [Enter] for configuration of advanced items.
DF Common Options	Press [Enter] for configuration of advanced items.
UMC Common Options	Press [Enter] for configuration of advanced items.
NBIO Common Options	Press [Enter] for configuration of advanced items.
FCH Common Options	Press [Enter] for configuration of advanced items.
NTB Common Options	Press [Enter] for configuration of advanced items.

## 2-2-11-1 Zen Common Options

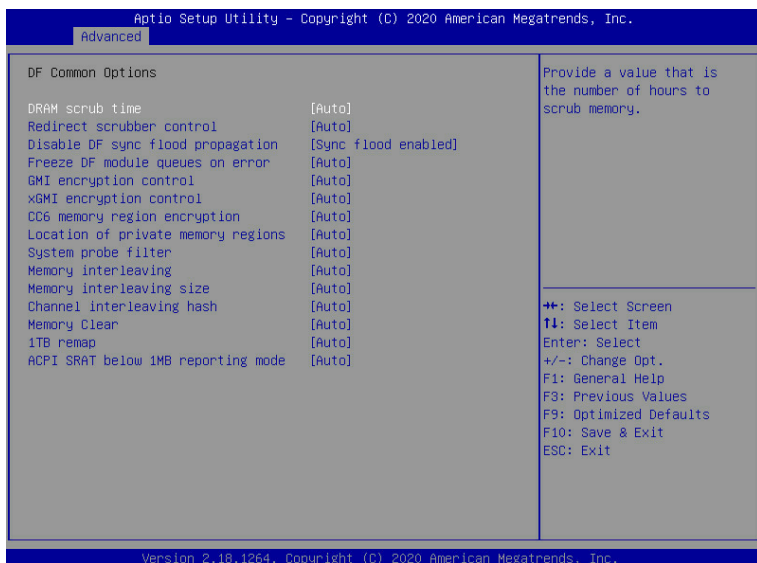


Parameter	Description
Zen Common Options	
RedirectForReturnDis	From a workaround for GCC/C000005 issue for XV Core on C2 A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrctForReturns] to 1. Options available: Auto, 1, 0. Default setting is <b>Auto</b> .
L2 TLB Associativity	0 - L2 TLB ways [11:8] are fully associative. 1 - L2 TLB ways [11:8] are 4K-only Options available: 0, 1, Auto. Default setting is <b>Auto</b> .
Platform First Error Handling	Enable/Disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Core Performance Boost	Enable/Disable the Core Performance Boost function. Options available: Auto, Disabled. Default setting is <b>Auto</b> .
Enable IBS	Enable/Disable IBS. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Global C-State Control	Controls the IO based C-state generation and DF C-states. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Opcache Control	Enable/Disable the Opcache control. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
SEV-ES ASID Space Limit C	The SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. The valid values for this field are from 0x1 (1) to 0x10 (16). Default setting is 1.

Parameter	Description
Core/Thread Enablement	<p>Allows you to disagree or agree enabling processor cores and threads. When agreed, you can control the number of cores to be used, and whether to enable or disable Symmetric Multithreading Technology (SMT) support.</p> <ul style="list-style-type: none"> <li>◆ Downcore Control <ul style="list-style-type: none"> <li>– Options available: Auto, ONE(1+0), TWO(1+1), TWO(2+0), THREE(3+0), FOUR(2+2), FOUR(4+0), SIX(3+3). Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ SMTEN <ul style="list-style-type: none"> <li>– Disable: Single hardware thread per core.</li> <li>– Auto: Two hardware threads per core.</li> <li>– Options available: Disable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
Streaming Stores Control	<p>Enable/Disable the Streaming Stores functionality. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</p>
Prefetcher settings	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ L1 Stream HW Prefetcher <ul style="list-style-type: none"> <li>– Enable/Disable L1 Stream HW Prefetcher.</li> <li>– Options available: Auto, Enable, Disable. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ L2 Stream HW Prefetcher <ul style="list-style-type: none"> <li>– Enable/Disable L2 Stream HW Prefetcher.</li> <li>– Options available: Auto, Enable, Disable. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>



## 2-2-11-2 DF Common Options



Parameter	Description
DF Common Options	
DRAM scrub time	Provide a value that is the number of hours to scrub memory. Options available: Auto, Disabled, 1 hour, 4 hours, 8 hours, 16 hours, 24 hours, 48 hours. Default setting is <b>Auto</b> .
Redirect scrubber control	Enable/Disable the Redirect scrubber control feature. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Disable DF sync flood propagation	Enable/Disable DF Sync Flood propagation. Options available: Auto, Sync flood disabled, Sync flood enabled. Default setting is <b>Auto</b> .
Freeze DF module queues on error	Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
GMI encryption control	Enable/Disable GMI link encryption. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
xGMI encryption control	Enable/Disable xGMI link encryption. 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. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Location of private memory regions	Controls whether or not the private memory regions (PSP, SMU and CC6) are at the top of DRAM or distributed. Options available: Auto, Distributed, Consolidated. Default setting is <b>Auto</b> .
System probe filter	Enable/Disable System probe filter. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .

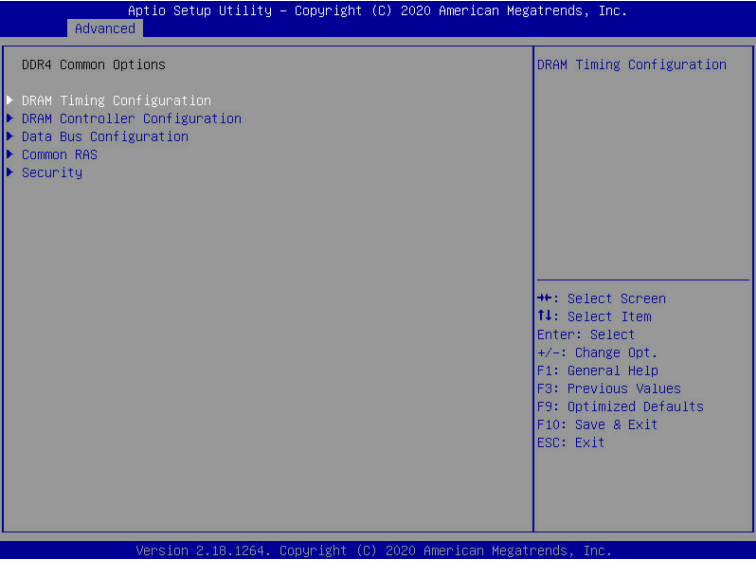
Parameter	Description
Memory interleaving	Controls the fabric level memory interleaving. Note that channel, die, and socket has requirements on memory populations and it will be ignored if the memory doesn't support the selected option. Options available: Auto, None, Channel, Die Socket. Default setting 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). Options available: Auto, 256Bytes, 512Bytes, 1KB, 2KB. Default setting is <b>Auto</b> .
Channel interleaving hash	Controls whether or not the address bits are hashed during channel interleave mode. This field should not be used unless the interleaving is set to channel and the interleaving size is 256 or 512 bytes. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Memory Clear	Enable/Disable the Memory Clear feature. When this feature is disabled, BIOS does not implement MemClear after memory training (only if non-ECC DIMMs are used). Options available: Auto, Enabled, Disabled. 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. Options available: Auto, Do not remap, Attempt to remap. Default setting is <b>Auto</b> .
ACPI SRAT below 1MB reporting mode	Controls whether or not 0xA0000 - 1MB is reported as DRAM in the SRAT. Options available: Auto, Do not report, Report as DRAM. Default setting is <b>Auto</b> .

### 2-2-11-3 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.
Memory MBIST	Press [Enter] for configuration of advanced items.

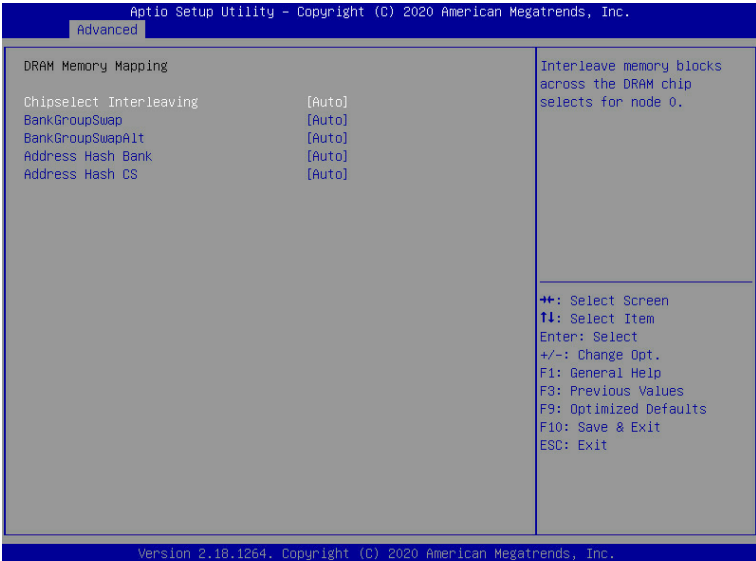
### 2-2-11-3-1 DDR4 Common Options



Parameter	Description
DDR4 Common Options	
DRAM Timing Configuration	<p>Press [Enter] to enable / disable restrictions for DDR4 frequency and voltage programming. Memory speeds will be capped at AMD guidelines.</p> <ul style="list-style-type: none"><li>◆   Decline</li><li>◆   Accept<ul style="list-style-type: none"><li>– Overclock: Enable/Disable Memory Overclock Settings.</li><li>– Options available: Auto, Enabled. Default setting is <b>Auto</b>.</li></ul></li></ul>
DRAM Controller Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"><li>◆ DRAM Power Options<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></li><li>◆ Cmd2T<ul style="list-style-type: none"><li>– Selects the Cmd2T mode on ADDR/CMD.</li><li>– Options available: Auto, 1T, 2T. Default setting is <b>Auto</b>.</li></ul></li><li>◆ Gear Down Mode<ul style="list-style-type: none"><li>– Enable/Disable the Gear Down Mode function.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul></li></ul>

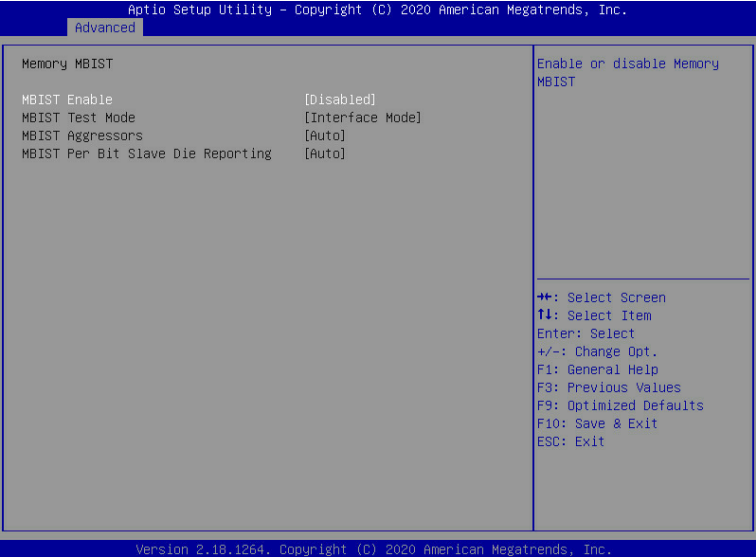
Parameter	Description
Data Bus Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>• Data Bus Configuration User Controls <ul style="list-style-type: none"> <li>– Specifies the mode for drive strength to Auto or Manual.</li> <li>– Options available: Auto, Manual. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
Common RAS	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>• Data Poisoning <ul style="list-style-type: none"> <li>– Enable/Disable the Data Poisoning function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>• RCD Parity <ul style="list-style-type: none"> <li>– Enable/Disable the RCD Parity function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>• DRAM Address Command Parity Retry <ul style="list-style-type: none"> <li>– Enable/Disable the DRAM Address Command Parity Retry function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>• Max Parity Error Replay <ul style="list-style-type: none"> <li>– Configures the Max Parity Error Replay. (0~0x3f).</li> <li>– Default setting is 8.</li> <li>– <b>Please note that this item is configurable when DRAM Address Command Parity Retry is set to Enabled.</b></li> </ul> </li> <li>• Write CRC Enable <ul style="list-style-type: none"> <li>– Enable/Disable the Write CRC function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>• Disable Memory Error Injection <ul style="list-style-type: none"> <li>– Options available: False, True. Default setting is <b>True</b>.</li> </ul> </li> <li>• ECC Configuration <ul style="list-style-type: none"> <li>– DRAM ECC Symbol Size <ul style="list-style-type: none"> <li>» Configures the DRAM ECC Symbol Size.</li> <li>» Options available: Auto, x4, x8. Default setting is <b>Auto</b>.</li> </ul> </li> <li>– DRAM ECC Enable <ul style="list-style-type: none"> <li>» Enable/Disable DRAM ECC. When set to Auto, it will set ECC to enable.</li> <li>» Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul> </li> </ul>
Security	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>• TSME <ul style="list-style-type: none"> <li>– Enable/Disable transparent secure memory encryption.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>• Data Scramble <ul style="list-style-type: none"> <li>– Enable/Disable Data Scrambling.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>

## 2-2-11-3-2 DRAM Memory Mapping



Parameter	Description
DRAM Memory Mapping	
Chipselect Interleaving	Interleave memory blocks across the DRAM chip selects for node 0. 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. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
BankGroupSwapAlt	Configures the BankGroupSwapAlt. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Address Hash Bank	Enable/Disable bank address hashing. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .
Address Hash CS	Enable/Disable CS address hashing. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .

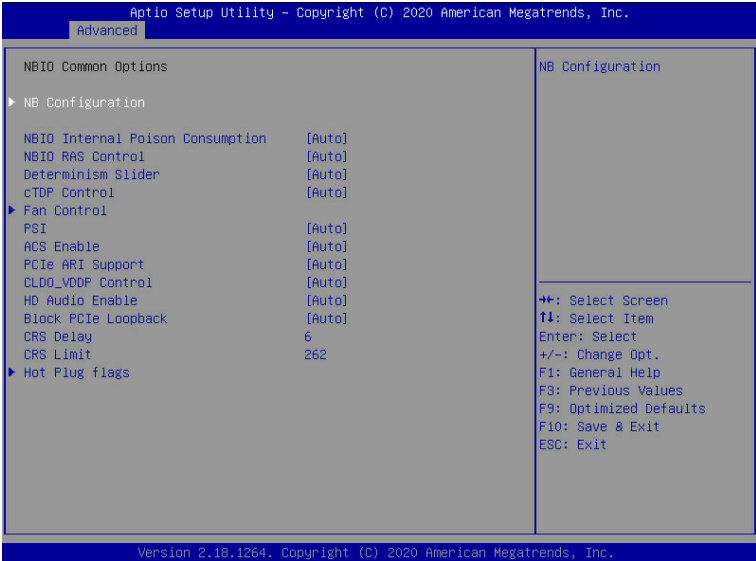
### 2-2-11-3-3 Memory MBIST



Parameter	Description
Memory MBIST	
MBIST Enable	Enable/Disable the Memory MBIST function. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
MBIST Test Mode <sup>(Note)</sup>	Selects MBIST Test Mode. Options available: Interface Mode, Data Eye Mode. Default setting is <b>Interface Mode</b> . – <b>Interface Mode</b> : Tests Single and Multiple CS transactions and Basic Connectivity. – <b>Data Eye Mode</b> : Measures Voltage vs. Timing.
MBIST Aggressors <sup>(Note)</sup>	Enable/Disable MBIST Aggressor test. 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. Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b> .

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

## 2-2-11-4 NBIO Common Options

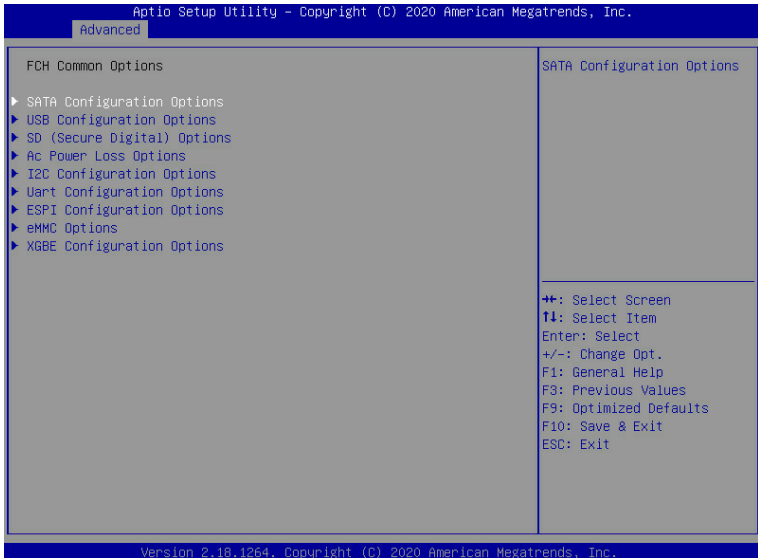


Parameter	Description
NBIO Common Options	
NB Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"><li>◆ IOMMU<ul style="list-style-type: none"><li>– Enable/Disable the IOMMU function.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul></li><li>◆ Concurrent Training<ul style="list-style-type: none"><li>– Enable/Disable Concurrent Training.</li><li>– Options available: Auto, False, True. Default setting is <b>Auto</b>.</li></ul></li></ul>
NBIO Internal Poison Consumption	<p>Enable/Disable NBIO Internal Poison Consumption.</p> <p>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</p>
NBIO RAS Control	<p>Enable/Disable NBIO RAS Control.</p> <p>Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</p>
Determinism Slider	<p>Specifies the system determinism.</p> <p>Options available: Auto, Power, Performance. Default setting is <b>Auto</b>.</p>
cTDP Control	<p>Selects use the fused TDP or set customized TDP. **TDP is used to define the RC thermal model only**</p> <p>Options available: Auto, Manual. Default setting is <b>Auto</b>.</p>
Fan Control	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"><li>◆ Fan Control<ul style="list-style-type: none"><li>– Options available: Auto, Manual. Default setting is <b>Auto</b>.</li></ul></li></ul>



Parameter	Description
PSI	Enable/Disable PSI. Options available: Auto, Disable. Default setting is <b>Auto</b> .
ACS Enable	Enable/Disable ACS support. Options available: Auto, Enable, Disabled. Default setting is <b>Auto</b> .
PCIe ARI Support	Enable/Disable Alternative Routing-ID Interpretation. Options available: Auto, Enable, Disable. Default setting is <b>Auto</b> .
CLD0_VDDP Control	Options available: Auto, Manual. Default setting is <b>Auto</b> .
HD Audio Enable	Enable/Disable HD Audio. Options available: Auto, Enable, Disabled. Default setting is <b>Auto</b> .
Block PCIe Loopback	Enable/Disable the Block PCIe loopback mode for hot plug slots. Options available: Auto, Enable, Disable. Default setting is <b>Auto</b> .
CRS Delay	Set the CRS delay for hot plug ports.
CRS Limit	Set the CRS limit for hot plug ports.
Hot Plug flags	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ Ignore sideband <ul style="list-style-type: none"> <li>– Enable/Disable the sideband function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Disable L1 w/a <ul style="list-style-type: none"> <li>– Enable/Disable the L1 w/a function.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Disable BridgeDis <ul style="list-style-type: none"> <li>– Enable/Disable BridgeDis update based on sideband.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Toggle RRC Enable <ul style="list-style-type: none"> <li>– Enable/Disable Toggle RRC during hot plug events.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Toggle RRC Enable <ul style="list-style-type: none"> <li>– Enable/Disable register control of BridgeDis only follows DL_Active.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>

## 2-2-11-5 FCH Common Options

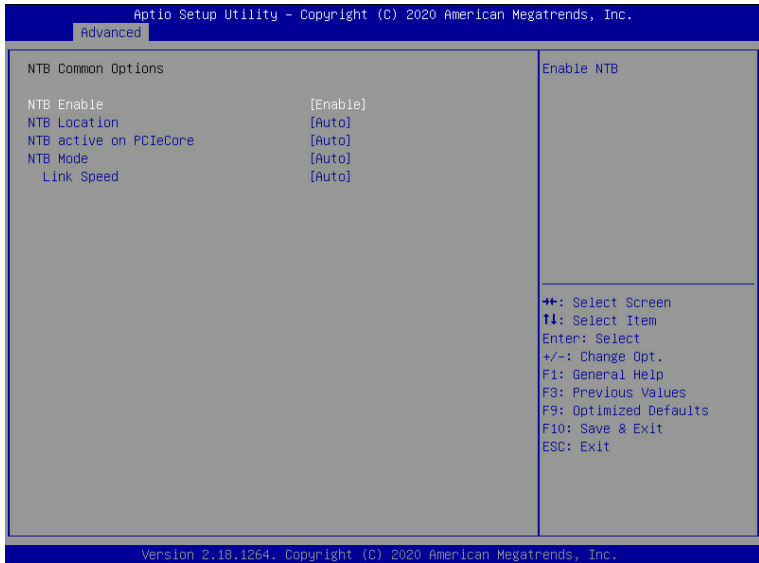


Parameter	Description
FCH Common Options	
SATA Configuration Options	Press [Enter] for configuration of advanced items.
	◆ SATA Controller <ul style="list-style-type: none"><li>– Enable/Disable OnChip SATA controller.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
	◆ Sata RAS Support <ul style="list-style-type: none"><li>– Enable/Disable Sata RAS Support.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
	◆ Sata Disabled AHCI Prefetch Function <ul style="list-style-type: none"><li>– Enable/Disable Sata Disabled AHCI Prefetch Function.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
	◆ Aggressive SATA Device Sleep Port 0 <ul style="list-style-type: none"><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
	◆ Aggressive SATA Device Sleep Port 1 <ul style="list-style-type: none"><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
USB Configuration Options	Press [Enter] for configuration of advanced items.
	◆ XHCI Controller enable <ul style="list-style-type: none"><li>– Enable/Disable USB3 controller.</li><li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul>
	◆ MCM USB enable <ul style="list-style-type: none"><li>– XHCI Controller1 enable (die1)<ul style="list-style-type: none"><li>» Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li></ul></li></ul>

Parameter	Description
USB Configuration Options (continued)	<ul style="list-style-type: none"> <li>– XHCI2 enable (MCM1/Die0) <ul style="list-style-type: none"> <li>» Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>– XHCI3 enable (MCM1/Die1) <ul style="list-style-type: none"> <li>» Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
SD (Secure Digital) Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ SD Configuration Mode <ul style="list-style-type: none"> <li>– Selects the SD mode.</li> <li>– Options available: Disabled, Ver2.0, SdDump, Auto (Version 2.0 + Low Speed). Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
AC Power Loss Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ AC Loss Control <ul style="list-style-type: none"> <li>– Selects the AC Loss Control Method.</li> <li>– Options available: Always Off, Always On, Reserved, Previous. Default setting is <b>Always On</b>.</li> </ul> </li> </ul>
I2C Configuration Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ I2C 0/1/2/3/4/5 Enable <ul style="list-style-type: none"> <li>– Enable/Disable I2C 0/1/2/3/4/5.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
Uart Configuration Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ Uart 0 Enable <ul style="list-style-type: none"> <li>– Uart 0 has no HW FC if Uart 2 is enabled.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Uart 0 Legacy Options <ul style="list-style-type: none"> <li>– Options available: Disabled, 0x2E8, 0x2F8, 0x3E8, 0x3F8. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Uart 1 Enable <ul style="list-style-type: none"> <li>– Uart 1 has no HW FC if Uart 3 is enabled.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Uart 1 Legacy Options <ul style="list-style-type: none"> <li>– Options available: Disabled, 0x2E8, 0x2F8, 0x3E8, 0x3F8. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Uart 2 Enable (no HW FC) <ul style="list-style-type: none"> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Uart 3 Enable (no HW FC) <ul style="list-style-type: none"> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
ESPI Configuration Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ ESPI Enable <ul style="list-style-type: none"> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>

Parameter	Description
eMMC Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ eMMC/SD Configure <ul style="list-style-type: none"> <li>– Options available: Disabled, SD Normal Speed, SD High Speed, SD UHSI-SDR50, SD UHSI-DDR50, SD UHSI-SDR104, eMMC Emmc Backward Compatibility, eMMC High Speed SDR, eMMC High Speed DDR, eMMC HS200, eMMC HS400, eMMC HS300, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Driver Type <ul style="list-style-type: none"> <li>– Bios will select MS driver for SD selections.</li> <li>– Options available: AMD eMMC Driver, MS Driver, MS EMMC Driver, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ eMMC Boot <ul style="list-style-type: none"> <li>– Options available: Disabled, Enabled, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
XGBE Configuration Options	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> <li>◆ AMD XGBE Controller 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> <li>– Enable/Disable Ethernet Controller 0/1/2/3/4/5/6/7.</li> <li>– Options available: Auto, Enabled, Disabled. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ AMD XGBE DIE 0/1 Configuration speed <ul style="list-style-type: none"> <li>– Options available: 10G/1G/100M, 2.5G. Default setting is <b>10G/1G/100M</b>.</li> </ul> </li> </ul>

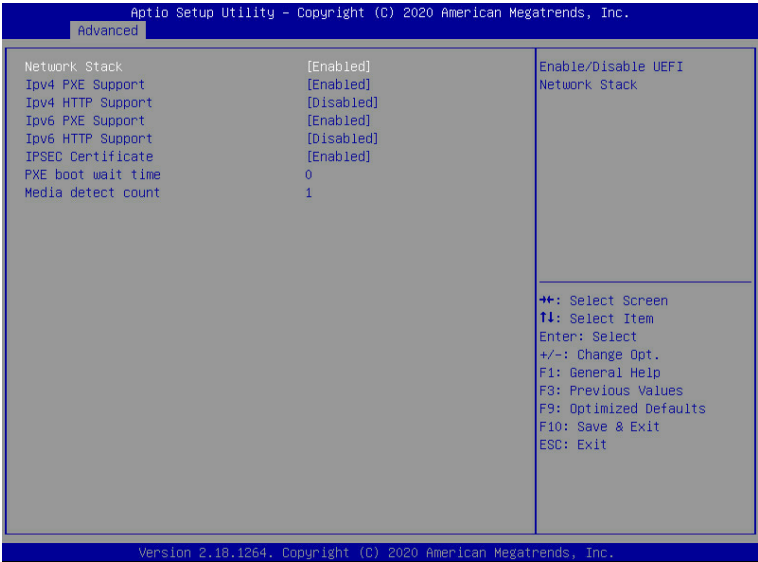
## 2-2-11-6 NTB Common Options



Parameter	Description
NTB Common Options	
NTB Enable	Options available: Auto, Enable. Default setting is <b>Auto</b> .
NTB Location <sup>(Note)</sup>	Options available: Auto, Socket0-Die0, Socket0-Die1, Socket0-Die2, Socket0-Die3, Socket1-Die0, Socket1-Die1, Socket1-Die2, Socket1-Die3. Default setting is <b>Auto</b> .
NTB active on PCIeCore <sup>(Note)</sup>	NTB enable on PCIe Core. Options available: Auto, Core0, Core1. Default setting is <b>Auto</b> .
NTB Mode <sup>(Note)</sup>	Selects NTB Mode (Core0, Port0). Options available: NTB Disabled, NTB Primary, NTB Secondary, NTB Random, Auto. Default setting is <b>Auto</b> .
Link Speed <sup>(Note)</sup>	Selects Link Speed for NTB Mode (Core0, Port0). Options available: Max Speed, Gen 1, Gen 2, Gen 3, Auto. Default setting is <b>Auto</b> .

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

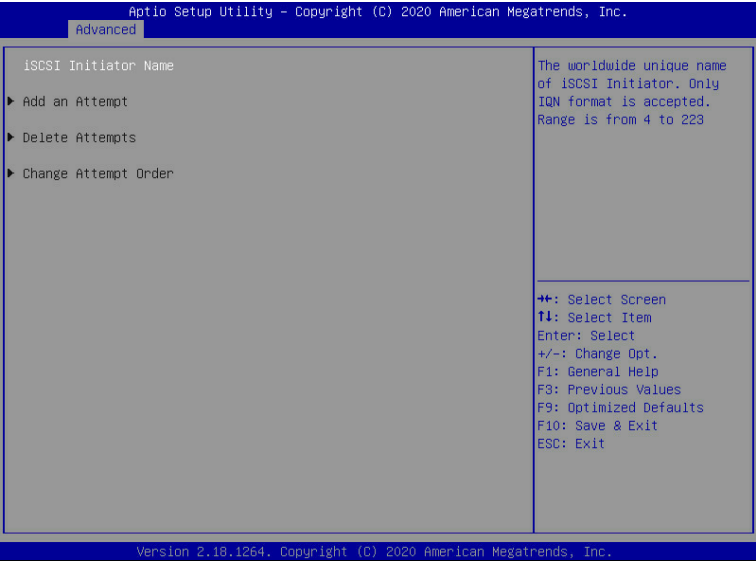
## 2-2-12 Network Stack Configuration



Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Ipv4 PXE Support <sup>(Note)</sup>	Enable/Disable the Ipv4 PXE feature. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Ipv4 HTTP Support <sup>(Note)</sup>	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Ipv6 PXE Support <sup>(Note)</sup>	Enable/Disable the Ipv6 PXE feature. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Ipv6 HTTP Support <sup>(Note)</sup>	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
IPSEC Certificate <sup>(Note)</sup>	Enable/Disable the IPSEC Certificate feature. 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. 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. Press the <+> / <-> keys to increase or decrease the desired values.

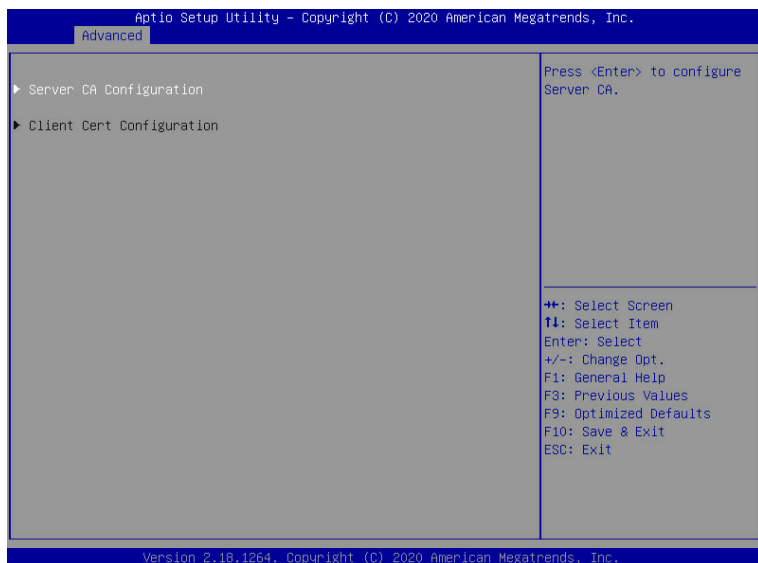
(Note) This item appears when **Network Stack** is set to **Enabled**.

## 2-2-13 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.

## 2-2-14 T1s 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 <p>Input digit character in 1111111-2222-3333-4444-1234567890ab format.</p> </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.



## 2-2-15 Intel(R) I210 Gigabit Network Connection

Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.		
Advanced		
▶ NIC Configuration		Click to configure the network device port.
Blink LEDs	0	
UEFI Driver	Intel(R) PRO/1000 7.5.11 PCI-E	
Adapter PBA	200214-007	
Device Name	Intel(R) I210 Gigabit Network Connection	
Chip Type	Intel i210	
PCI Device ID	1533	
PCI Address	03:00:00	
Link Status	[Disconnected]	↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
MAC Address	18:00:4D:46:52:11	
Virtual MAC Address	00:00:00:00:00:00	

Version 2.18.1264. Copyright (C) 2020 American Megatrends, Inc.

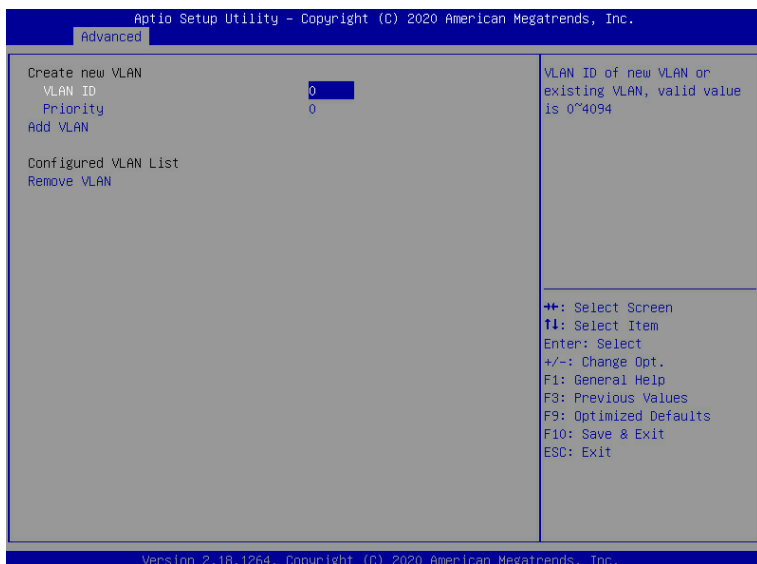
Aptio Setup Utility - Copyright (C) 2020 American Megatrends, Inc.		
Advanced		
Link Speed	[Auto Negotiated]	Specifies the port speed used for the selected boot protocol.
Wake On LAN	[Enabled]	

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

Version 2.18.1264. Copyright (C) 2020 American Megatrends, Inc.

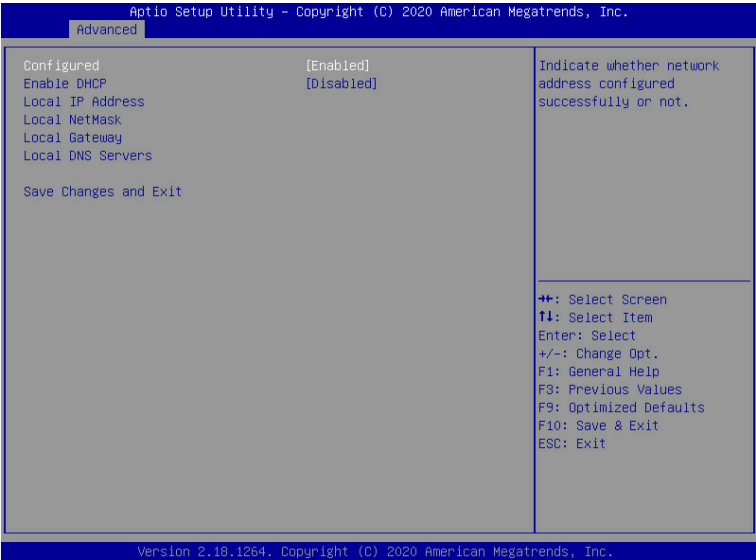
Parameter	Description
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>♦ Link Speed <ul style="list-style-type: none"> <li>– Allows for automatic link speed adjustment.</li> <li>– Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 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. 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.

## 2-2-16 VLAN Configuration



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

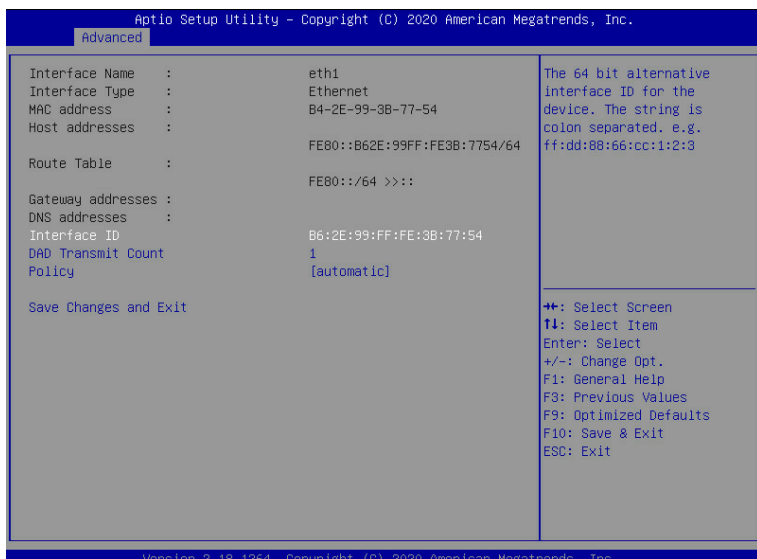
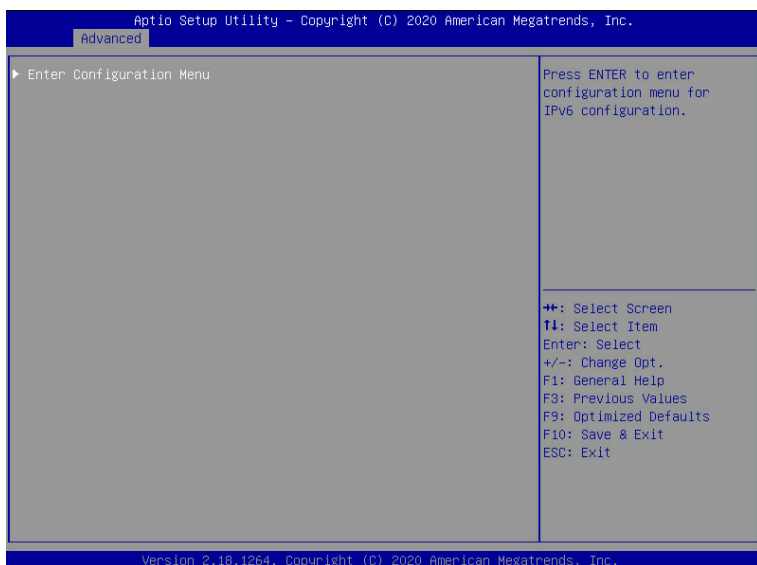
## 2-2-17 MAC IPv4 Network Configuration



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**.

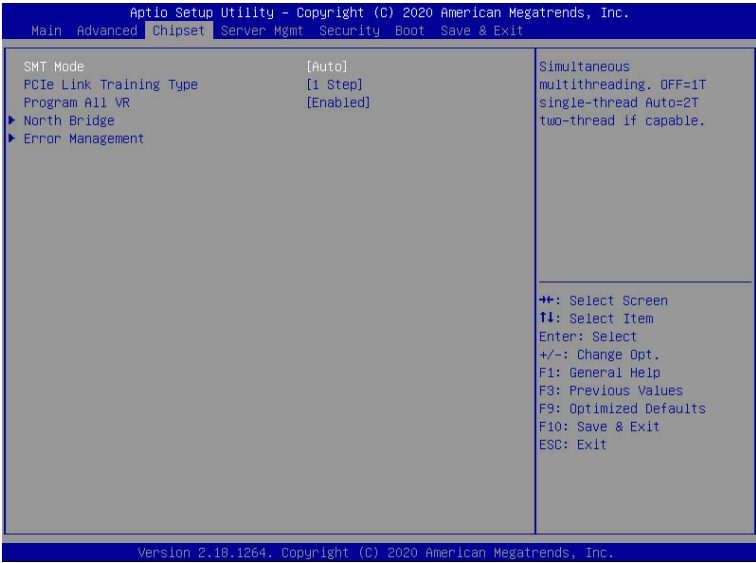
## 2-2-18 MAC IPv6 Network Configuration



Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Displays the MAC Address information.</li> <li>◆ Interface ID <ul style="list-style-type: none"> <li>– 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>◆ DAD Transmit Count <ul style="list-style-type: none"> <li>– 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>◆ Policy <ul style="list-style-type: none"> <li>– Options available: automatic, manual. Default setting is <b>automatic</b>.</li> </ul> </li> <li>◆ Save Changes and Exit <ul style="list-style-type: none"> <li>– Press [Enter] to save all configurations.</li> </ul> </li> </ul>

## 2-3 Chipset Setup Menu

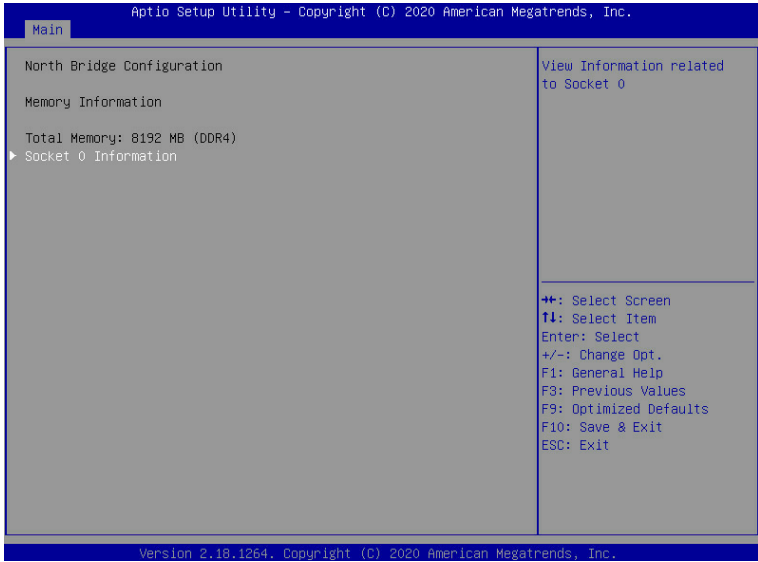
Chipset Setup menu displays submenu options for configuring the function of the North Bridge. Select a submenu item, then press <Enter> to access the related submenu screen.



Parameter	Description
SMT Mode	Simultaneous multithreading. Off=1T single-thread; Auto=2T two-thread if capable. Options available: Off, Auto. Default setting is <b>Auto</b> .
PCIe Link Training Type	Configures the PCIe Link training in 1 or 2 steps. Options available: 1 Step, 2 Step. Default setting is <b>1 Step</b> .
Program All VR	Enable/Disable program all VR on MB. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
North Bridge	Press [Enter] for configuration of advanced items.
Error Management	Press [Enter] for configuration of advanced items.



## 2-3-1 North Bridge



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

## 2-3-2 Error Management



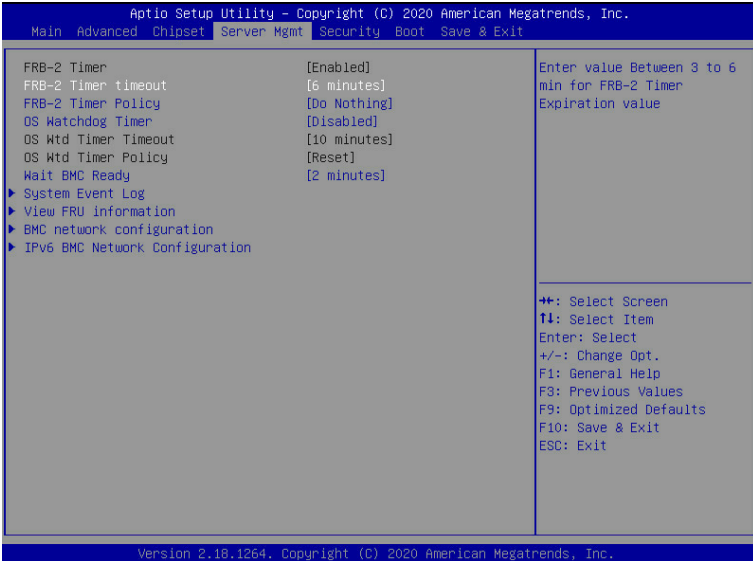
Parameter	Description
Error Management	
Platform First Error Handling	Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
MCA Error Threshold Count	Specifies the MCA Error Threshold Count. Options available: 0, 1, 5, 10, 100, 1000. Default setting is <b>10</b> .
DRAM Address/Command Parity with Replay	
RCD Parity	Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
DRAM Address Command Parity Retry	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Max Parity Error Replay <sup>(Note1)</sup>	Sets the max parity error replay. (Valid range 2 to 8).
DRAM Write Data CRC with Replay	
Write CRC Enable	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
DRAM Write CRC Enable and Retry Limit <sup>(Note2)</sup>	Options available: Enabled, Disabled. Default setting is <b>Disabled</b> .
Max Write CRC Error Replay <sup>(Note3)</sup>	Sets the max write CRC error replay. (Valid range 2 to 8).

(Note1) This item appears when **DRAM Address Command Parity Retry** is set to **Enabled**.

(Note2) This item appears when **Write CRC Enable** is set to **Enabled**.

(Note3) This item appears when **DRAM Write CRC Enable and Retry Limit** is set to **Enabled**.

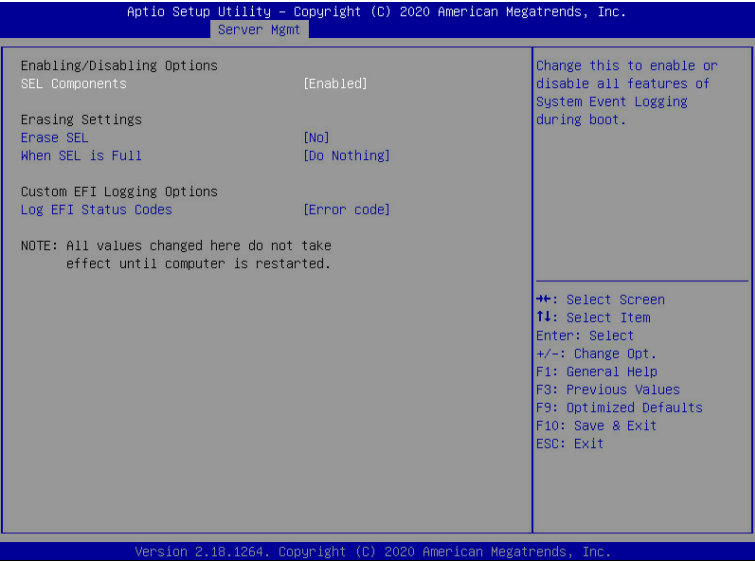
## 2-4 Server Management Menu



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

Parameter	Description
Wait BMC Ready	Configures time to wait BMC ready. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is <b>2 minutes</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.

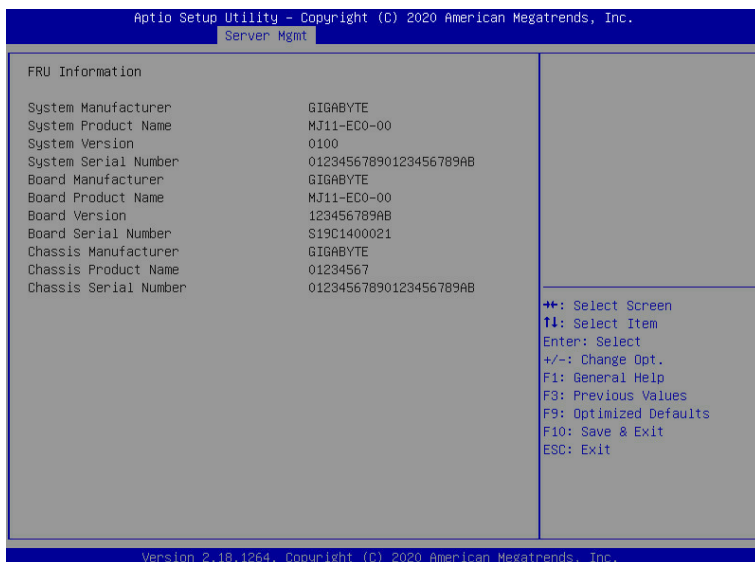
# 2-4-1 System Event Log



Parameter	Description
Enabling / Disabling Options	
SEL Components	Change this item to enable or disable all features of System Event Logging during boot. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
Erasing Settings	
Erase SEL	Choose options for erasing SEL. 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. Options available: Do Nothing, Erase 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). Options available: Disabled, Both, Error code, Progress code. Default setting is <b>Error code</b> .

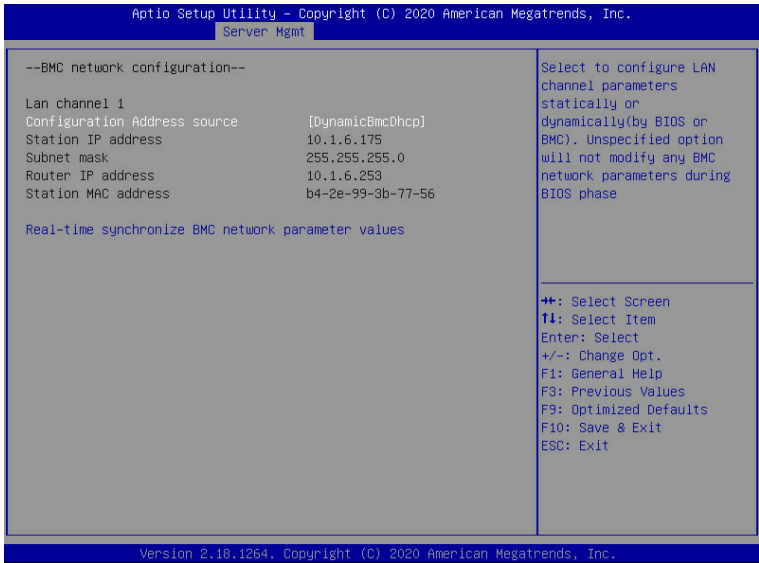
## 2-4-2 View FRU Information

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



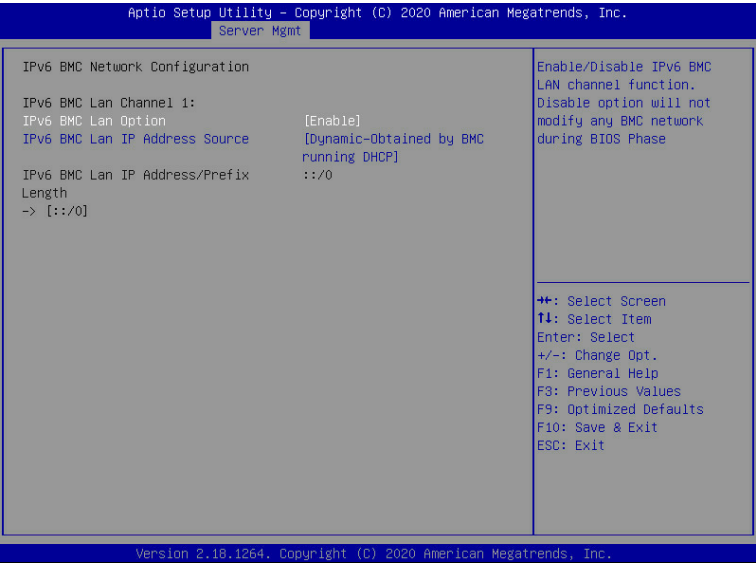
(Note) The model name will vary depends on the product you purchased

## 2-4-3 BMC 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. Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is <b>DynamicBmcDhcp</b> .
Station IP address	Displays IP Address information.
Subnet mask	Displays Subnet Mask information. 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 synchronize BMC network parameter values	Press [Enter] to synchronize the BMC network parameter values.

## 2-4-4 IPv6 BMC Network Configuration

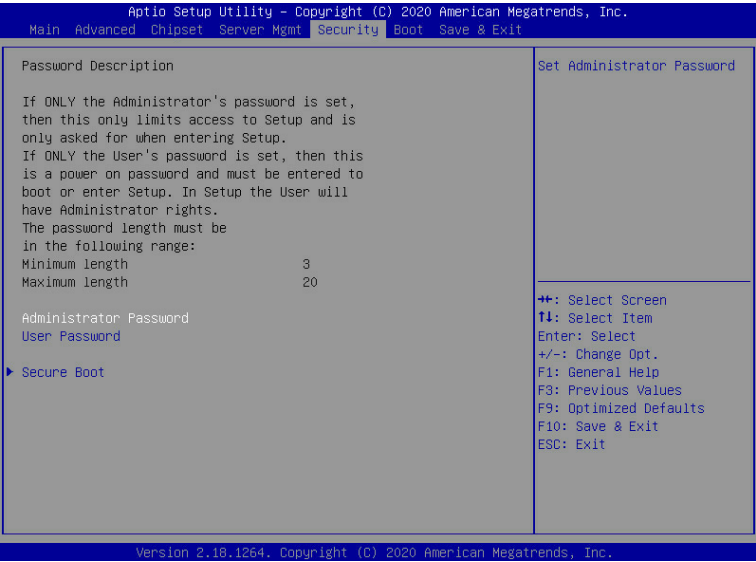


Parameter	Description
IPv6 BMC network configuration	
IPv6 BMC Lan Channel 1	
IPv6 BMC Lan Option	Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase. Options available: Unspecified, Disable, Enable. Default setting is <b>Enable</b> .
IPv6 BMC Lan IP Address Source	Selects to configure LAN channel parameters statically or dynamically (by BIOS or BMC). 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.



# 2-5 Security Menu

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



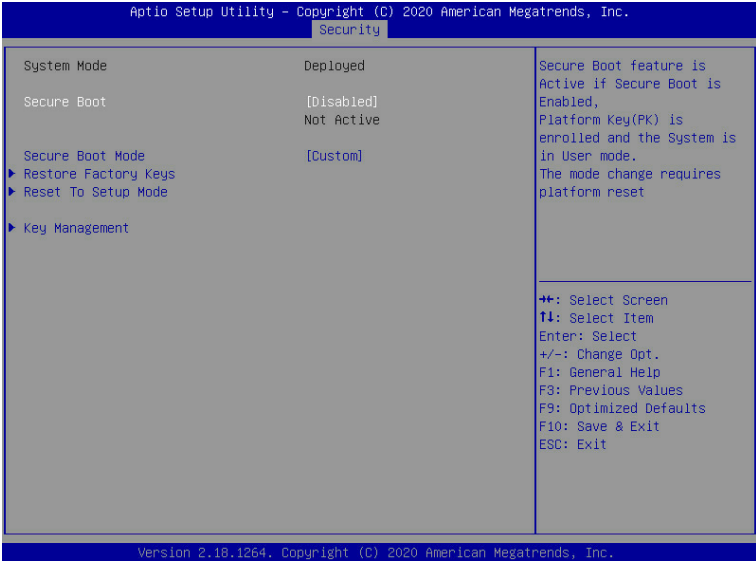
There are two types of passwords that you can set:

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

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

## 2-5-1 Secure Boot

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



Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. 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. When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases. When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database. 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.
Reset to Setup Mode	Press [Enter] to reset the system mode to Setup mode.

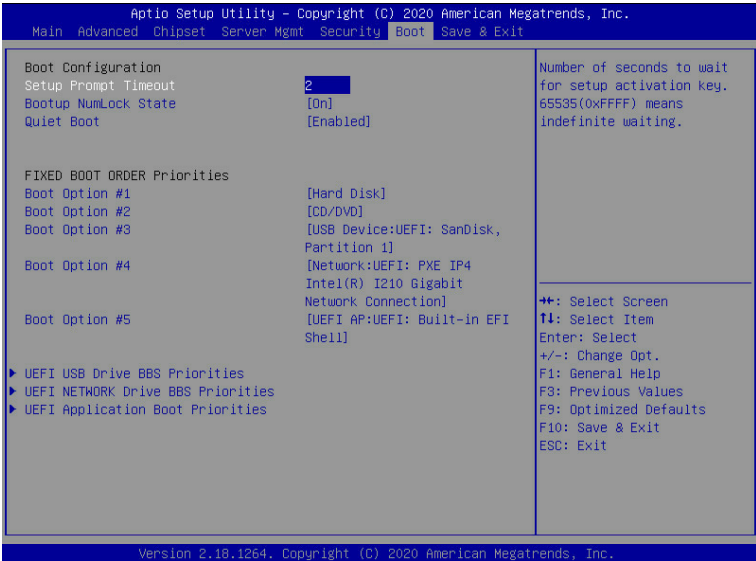
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	<p>Press [Enter] to configure advanced items.</p> <p><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>◆ Factory Key Provision <ul style="list-style-type: none"> <li>– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li>– Options available: Enabled, Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Restore Factory Keys <ul style="list-style-type: none"> <li>– Installs all factory default keys. It will force the system in User Mode.</li> <li>– Options available: Yes, No.</li> </ul> </li> <li>◆ Reset To Setup Mode <ul style="list-style-type: none"> <li>– Press [Enter] to reset the system mode to Setup mode.</li> </ul> </li> <li>◆ Export Secure Boot variables <ul style="list-style-type: none"> <li>– Press [Enter] to export all Secure Boot Keys and key variables.</li> </ul> </li> <li>◆ Enroll Efi Image <ul style="list-style-type: none"> <li>– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li>◆ Device Guard Ready</li> <li>◆ Remove 'UEFI CA' from DB <ul style="list-style-type: none"> <li>– Press [Enter] to remove Microsoft UEFI CA from Secure Boot DB</li> </ul> </li> <li>◆ Restore DB defaults <ul style="list-style-type: none"> <li>– Restore DB variable to factory defaults.</li> </ul> </li> <li>◆ Secure Boot variable <ul style="list-style-type: none"> <li>– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li>◆ Platform Key (PK) <ul style="list-style-type: none"> <li>– Displays the current status of the Platform Key (PK).</li> <li>– Press [Enter] to configure a new PK.</li> <li>– Options available: Details, Export, Update, Delete.</li> </ul> </li> <li>◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li>– Displays the current status of the Key Exchange Key Database (KEK).</li> <li>– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li>– Options available: Details, Export, Update, Append, Delete.</li> </ul> </li> <li>◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li>– Displays the current status of the Authorized Signature Database.</li> <li>– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li>– Options available: Details, Export, Update, Append, Delete.</li> </ul> </li> <li>◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li>– Displays the current status of the Forbidden Signature Database.</li> <li>– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li>– Options available: Details, Export, Update, Append, Delete.</li> </ul> </li> </ul>

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

## 2-6 Boot Menu

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

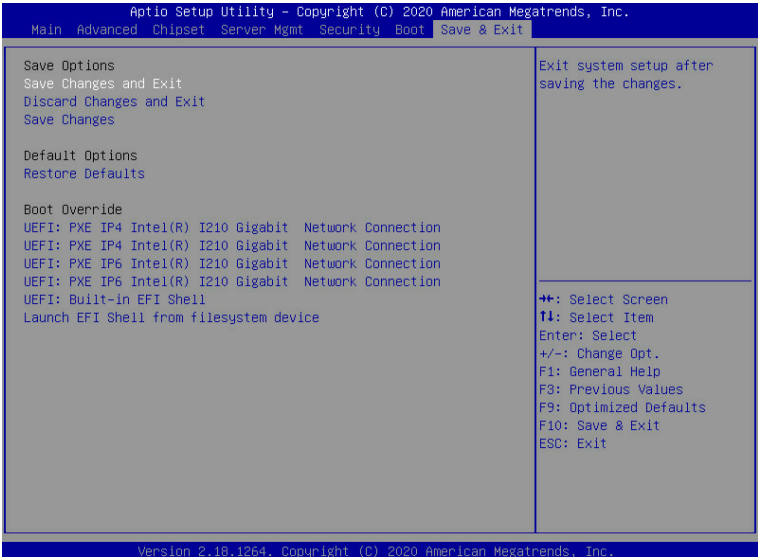


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off. Default setting is <b>Off</b> .
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled, Disabled. Default setting is <b>Enabled</b> .
FIXED BOOT ORDER Priorities	
Press [Enter] to configure the boot priority. By default, the server searches for boot devices in the following sequence:	
Boot Option #1 / #2 / #3 / #4 / #5	<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>

Parameter	Description
UEFI USB Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Application Boot Priorities	Press [Enter] to configure the boot priority.

# 2-7 Save & Exit Menu

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



Parameter	Description
Save Options	
Save Changes and Exit	Saves changes made and closes the BIOS setup. Options available: Yes, No.
Discard Changes and Exit	Discards changes made and exits the BIOS setup. Options available: Yes, No.
Save Changes	Saves changes done so far to any of the setup options. 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. 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 file system devices.

## 2-8 ABL POST Codes

### 2-8-1 StartProcessorTestPoints

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

### 2-8-2 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

### 2-8-3 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

## 2-8-4 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

## 2-8-5 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

## 2-8-6 Topology test points

ProcTopologyEntry	0xE071
ProcTopologyDone	0xE07C

## 2-8-7 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

## 2-8-8 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 Initializiation	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
Abl3ProgramUmcKeys	0xE0C2
ABL 3 DF Finial Initialization	0xE0C3
ABL 3 Execute Synchronization Function	0xE0C4
ABL 3 Debug Synchronization Function	0xE0C5
ABL 3 Error Detected	0xE0C6
ABL 3 Global memroy error detected	0xE0C7
ABL 4 Initialiation - 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	

## 2-8-9 PMU test points

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

## 2-8-10 ABL0 test points

Abl0Begin	0xE0FC
ABL 0 End	0xE0FD

## 2-8-11 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
AblbBegin	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 Support 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 Unknown Response 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 communication 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 Unsupproted 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 Latency 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

## 2-9 Agesa POST Codes

### 2-9-1 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

### 2-9-2 [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

### 2-9-3 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

### 2-9-4 PMU Post Code

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

### 2-9-5 [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 MboxBiosCmdRsmlInfo	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 MboxBiosCmdRsmlInfo 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

## 2-9-6 [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	
APB DXE Entry	0xA922
APB 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
GfxIntfInfoTableInterfaceCZ entry	0xA98A
GfxIntfInfoTableInterfaceCZ 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

## 2-9-7 [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

## 2-9-8 [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

## 2-9-9 [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

## 2-10 BIOS POST Beep code (AMI standard)

### 2-10-1 PEI Beep Codes

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

### 2-10-2 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