

GIGABYTE™

MB12-CE0

Intel® Xeon® D-1700 Processor Server Motherboard

User Manual

Rev. 1.0

Copyright

© 2022 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.

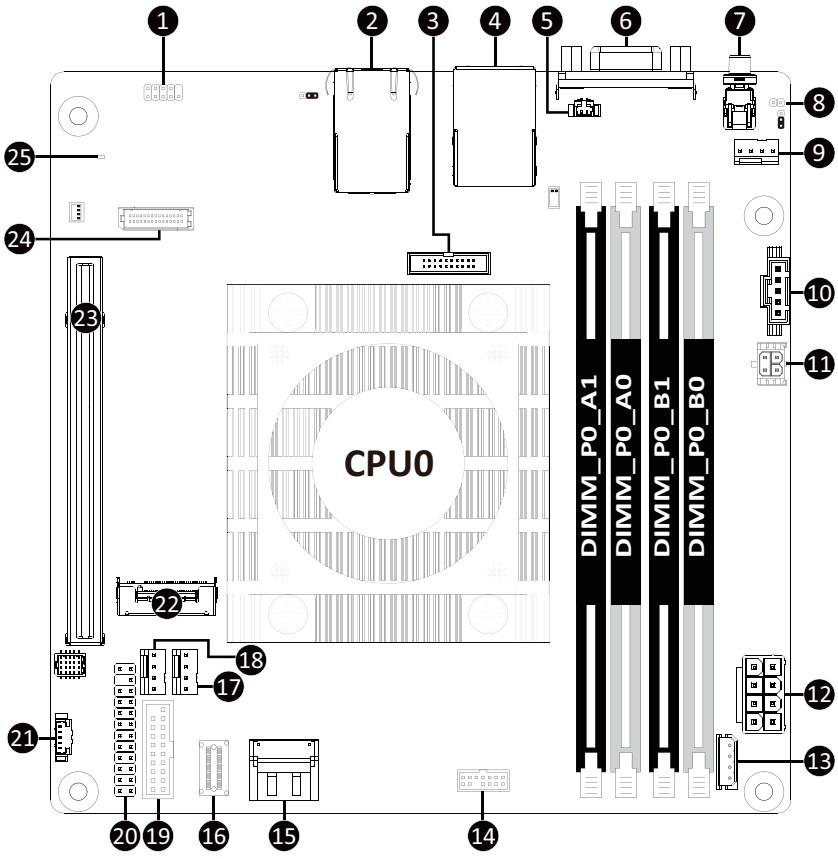
For any general sales or marketing enquires, you may message GIGABYTE server directly by email: server.grp@gigabyte.com.

Table of Contents

MB12-CE0 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 Dual-Channel Memory Configuration	11
1-3-2 Installing and Removing a Memory Module	12
1-3-3 DIMM Population Table	12
1-4 Installing the M.2 SSD Module.....	13
1-5 Back Panel Connectors.....	14
1-6 Internal Connectors.....	15
1-7 Jumper Settings	24
Chapter 2 BIOS Setup	25
2-1 The Main Menu	27
2-2 Advanced Menu	29
2-2-1 Trusted Computing	30
2-2-2 Serial Port Console Redirection	31
2-2-3 SIO Configuration	35
2-2-4 PCI Subsystem Settings.....	36
2-2-5 USB Configuration.....	38
2-2-6 Network Stack Configuration	39
2-2-7 Post Report Configuration	40
2-2-8 NVMe Configuration	41
2-2-9 Chipset Configuration.....	42
2-2-10 Tls Auth Configuration	43
2-2-11 All Cpu Information.....	44
2-2-12 Emulation Configuration	45
2-2-13 iSCSI Configuration.....	46
2-2-14 Intel(R) I210 Gigabit Network Connection	47
2-2-15 VLAN Configuration.....	49
2-2-16 MAC IPv6 Network Configuration.....	50
2-2-17 MAC IPv4 Network Configuration.....	51
2-2-18 Driver Health.....	52
2-3 Chipset Menu	53
2-3-1 Processor Configuration	54

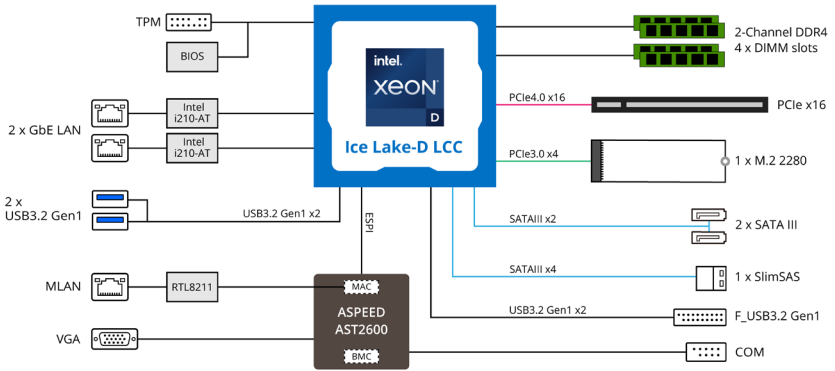
2-3-2	Common RefCode Configuration	56
2-3-3	UPI Configuration	57
2-3-4	Memory Configuration	58
2-3-5	IIO Configuration	60
2-3-6	Advanced Power Management Configuration	62
2-3-7	PCH-IO Configuration.....	64
2-3-8	Miscellaneous Configuration	66
2-3-9	Server ME Configuration	67
2-3-10	Runtime Error Logging	68
2-3-11	Power Policy.....	69
2-4	Server Management Menu.....	71
2-4-1	System Event Log	73
2-4-2	View FRU Information	74
2-4-3	BMC VLAN Configuration.....	75
2-4-4	BMC Network Configuration.....	76
2-4-5	IPv6 BMC Network Configuration	77
2-5	Security Menu	78
2-5-1	Secure Boot	79
2-6	Boot Menu.....	82
2-7	Save & Exit Menu.....	84
2-8	BIOS Recovery	86
2-9	BIOS POST Beep code (AMI standard).....	87
2-9-1	PEI Beep Codes	87
2-9-2	DXE Beep Codes	87

MB12-CE0 Motherboard Layout



Item	Code	Description
1	COM	Serial Port Header
2	LAN_1	1GbE LAN Port #1 (Top)/1GbE LAN Port #2 (Bottom)
3	CN_NCSI	NCSI Connector
4	USB3_MLAN	Server Management LAN Port (Top)/USB 3.0 Ports (Bottom)
5	BAT	Battery Cable Connector
6	VGA_1	VGA Connector
7	SW_ID	ID Button with LED
8	CASE_OPEN	Case Open Intrusion Alert Header
9	SYS_FAN1	System Fan Connector #1
10	PMBUS	PMBus Connector
11	DC_IN	2x2 Pin 5VSB/PSON Power Connector
12	P12V1	2x4 Pin 12V Power Connector
13	IPMB1	IPMB Connector
14	SPL_TPM	TPM Connector
15	SATA_0_1	SATA 6Gb/s Connector #0/#1
16	SL_SAS0	Slimline Connector (SATA 6Gb/s Signal)
17	CPU0_FAN	CPU Fan Connector
18	SYS_FAN2	System Fan Connector #2
19	F_USB3_1	Front Panel USB 3.0 Connector
20	FP_1	Front Panel Header
21	SGPIO	SATA SGPIO Connector
22	M2_0	M.2 Slot (PCIe Gen3 x4, Support NGFF-2280)
23	PCIE_1	PCIe x16 Slot (Gen4 x16)
24	BP_1	HDD Backplane Board Connector
25	LED_BMC	BMC Firmware Readiness LED

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.
- To avoid any potential short circuit of the DIMM slots, please remove any stand-offs from the chassis that will be located underneath the DIMM slots, before installing the motherboard into the chassis.

1-2 Product Specifications



NOTE:

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

 Form Factor	<ul style="list-style-type: none">◆ ATX◆ 170W x 170D (mm)
 CPU	<ul style="list-style-type: none">◆ Intel® Xeon® D-1700 processor families◆ Default CPU setting: Intel® Xeon® D-1739◆ Based Frequency 3GHz, max turbo 3.5GHz◆ 8 cores, 15MB LLC Cache◆ 83W TDP
 Chipset	<ul style="list-style-type: none">◆ System on Chip
 Memory	<ul style="list-style-type: none">◆ 4 x DIMM slots◆ DDR4 memory supported only◆ 2-channel memory architecture◆ RDIMM module up to 32GB per DIMM slot◆ Total 128GB capacity◆ 1.2V modules: 2933 (2DPC) MHz
 LAN	<ul style="list-style-type: none">◆ 2 x 1GbE LAN ports (1 x Intel® I210-AT)◆ 1 x 10/100/1000 management LAN
 Onboard Graphics	<ul style="list-style-type: none">◆ Integrated in Aspeed® AST2600◆ 2D Video Graphic Adapter with PCIe bus interface◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
 Storage Interface	<ul style="list-style-type: none">◆ 1 x SlimSAS for 4 x SATA 6Gb/s ports◆ 2 x 7-pin SATA 6Gb/s ports
 RAID	<ul style="list-style-type: none">◆ Intel® SATA RAID 0/1/10/5
 Expansion Slots	<ul style="list-style-type: none">◆ 1 x PCIe x16 (Gen4 x16 bus) slot ◆ 1 x M.2 slot:<ul style="list-style-type: none">- M-key- PCIe Gen3 x4 per slot- Supports 2280 cards



**Internal I/O
Connectors**

- ◆ 1 x 4-pin power connector
- ◆ 1 x 8-pin 12V power connector
- ◆ 1 x M.2 slot
- ◆ 2 x 7-pin SATA 6Gb/s ports
- ◆ 1 x SlimSAS connector
- ◆ 1 x USB 3.2 Gen1 connector
- ◆ 1 x CPU fan header
- ◆ 2 x System fan headers
- ◆ 1 x TPM header
- ◆ 1 x Front panel header
- ◆ 1 x JTAG BMC header
- ◆ 1 x Clear CMOS jumper
- ◆ 1 x IPMB connector
- ◆ 1 x PMBus connector
- ◆ 1 x SGPIO connector
- ◆ 1 x COM (RS-232)



**Rear I/O
Connectors**

- ◆ 2 x USB 3.2 Gen1
- ◆ 1 x VGA
- ◆ 2 x RJ45
- ◆ 1 x MLAN
- ◆ 1 x ID button with LED



TPM

- ◆ 1 x TPM Header with SPI Interface
- ◆ Optional TPM2.0 kit: CTM010



**Board
Management**

- ◆ Aspeed® AST2600 Management Controller
- ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) Web Interface



**Operating
Properties**

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

1-3 Installing and Removing Memory

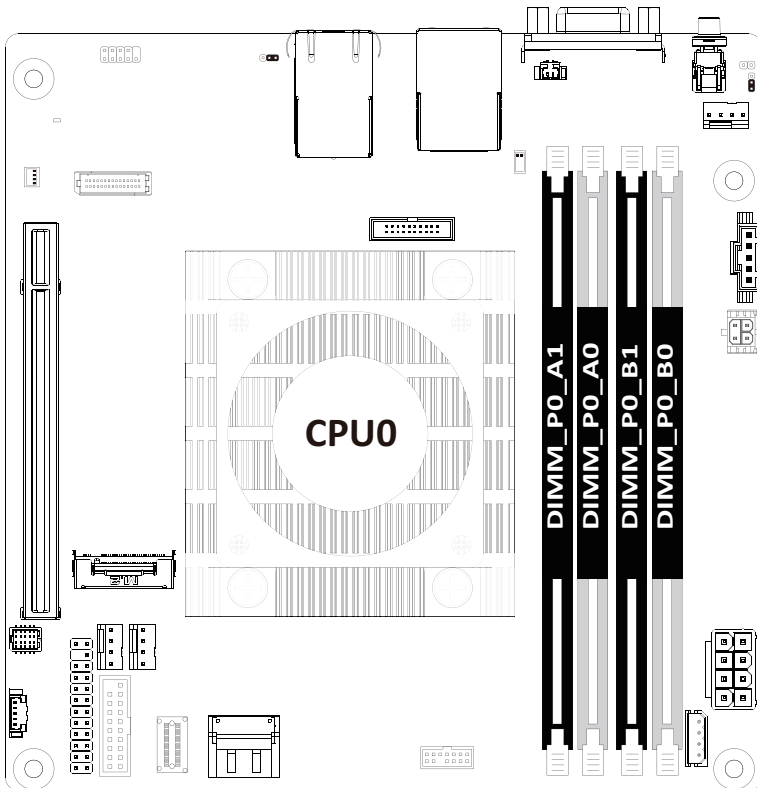


Read the following guidelines before you begin to install the memory:

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

1-3-1 Dual-Channel Memory Configuration

This motherboard provides 4 DDR4 memory slots and supports Dual-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

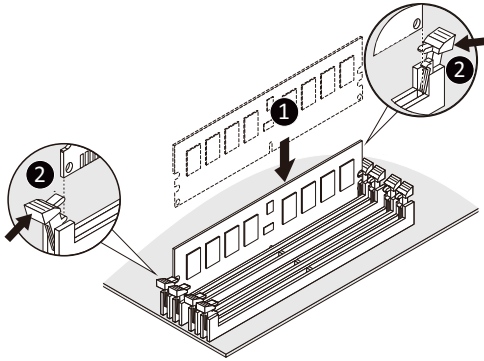


Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on 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

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V); DIMM per Channel (DPC)
		8Gb	16Gb	2DPC
RDIMM	SRx8	8GB	16GB	2933
	SRx4	16GB	32GB	
	DRx8	16GB	32GB	
	DRx4	32GB	64GB	
ECC UDIMM	SRx8	8GB	16GB	2666
	DRx8	16GB	32GB	
non-ECC UDIMM	SRx16	4GB	8GB	
	SRx8	8GB	16GB	
	DRx8	16GB	32GB	



Note:

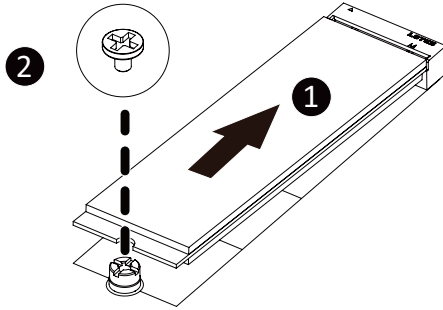
- When only one DIMM is used, it must be populated in memory slot DIMM0.

1-4 Installing the M.2 SSD Module

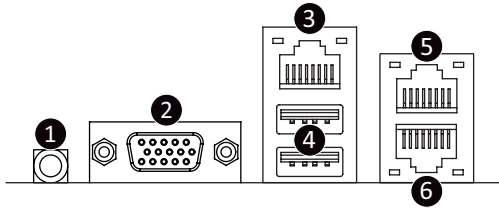
Follow the steps below to install a M.2 SSD module on your motherboard.

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

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



1-5 Back Panel Connectors



1 ID button with LED

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

2 VGA Port

Connect to a monitor device.

3 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.

4 USB 3.0 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.

5 1GbE 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.

6 1GbE 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.

LAN and ID Button LEDs

Speed LED Link/Activity LED



10/100/1000 LAN LED:

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

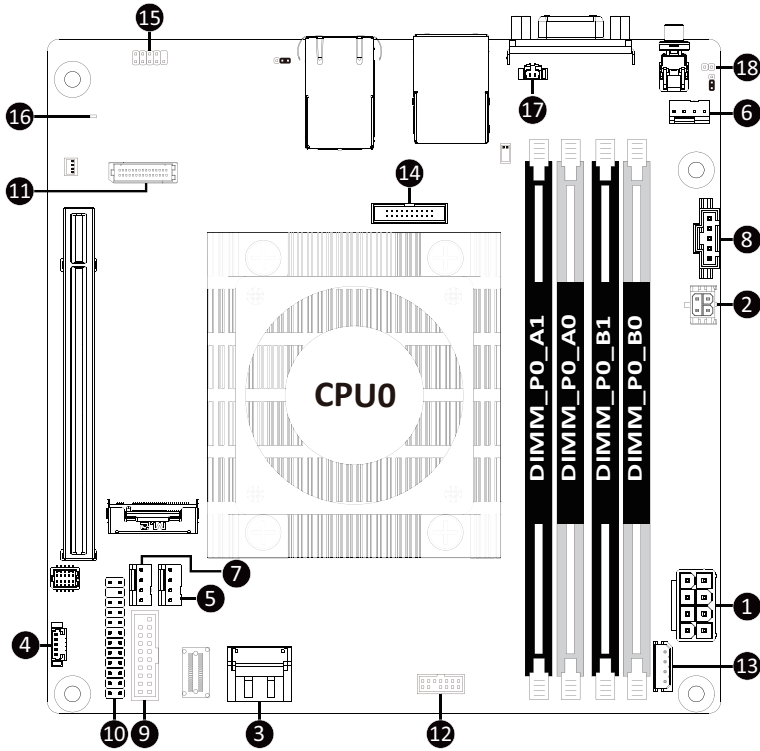
ID button/LED:

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) P12V1	11) BP_1
2) DC_IN	12) SPI_TPM
3) SATA_0_1	13) IPMB1
4) SGPIO	14) CN_NCSI
5) CPU0_FAN	15) COM
6) SYS_FAN1	16) LED_BMC
7) SYS_FAN2	17) BAT
8) PMBUS	18) CASE_OPEN
9) F_USB3_1	
10) FP_1	



Read the following guidelines before connecting external devices:

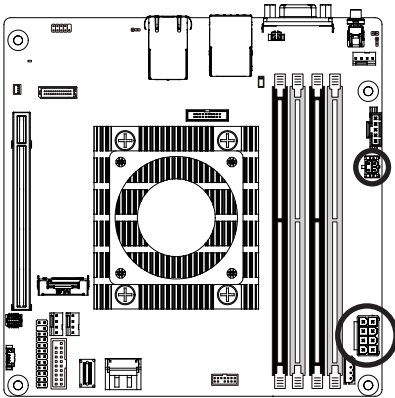
- First make sure your devices are compliant with the connectors you wish to connect.
- Before installing the devices, be sure to turn off the devices and your computer. Unplug the power cord from the power outlet to prevent damage to the devices.
- After installing the device and before turning on the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

1/2) P12V1/DC_IN (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. Using a power converter cable between a 4-pin power connector and a 24-pin ATX power connector is required.

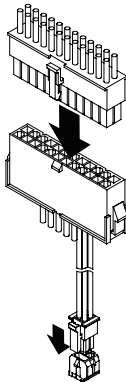


To meet expansion requirements, it is recommended that a power supply that can withstand high power consumption be used (500W or greater). If a power supply is used that does not provide the required power, the result can lead to an unstable or unbootable system.



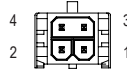
P12V1

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



DC_IN^(Note)

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

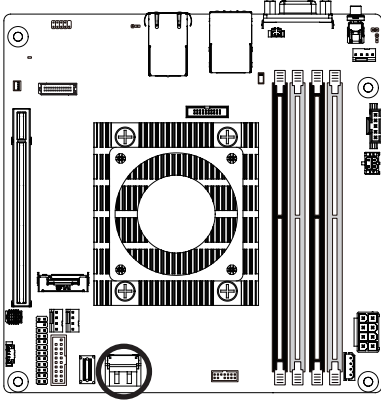


Note:

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

3) SATA_0_1 (SATA III 6Gb/s Connectors)

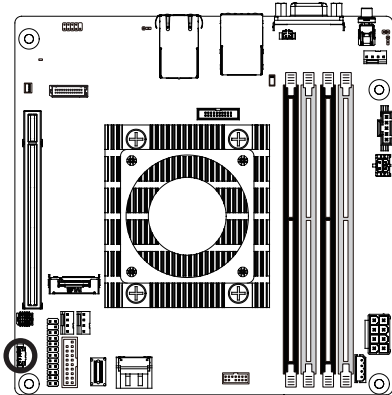
The SATA connectors conform to SATA III 6Gb/s standard and are compatible with SATA 3Gb/s standard. Each SATA connector supports a single SATA device.



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

4) SGPIO (SATA SGPIO Connector)

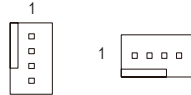
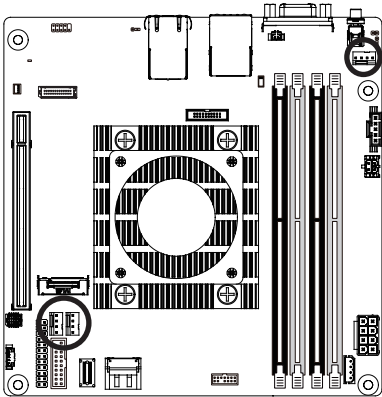
Serial General Purpose Input/Output (SGPIO) is a communication method used between a host bus adapter (HBA) and a main board.



Pin No.	Definition
1	DATAOUT
2	GND
3	NC
4	Load
5	Clock

5/6/7) CPU_FAN/SYS_FAN1/SYS_FAN2 (Fan Headers)

The motherboard has one 2-pin CPU fan header (CPU_FAN), and five 4-pin (SYS_FAN) system fan headers. Most fan headers possess a foolproof insertion design. When connecting a fan cable, be sure to connect it in the correct orientation (the black connector wire is the ground wire). The motherboard supports CPU fan speed control, which requires the use of a CPU fan with fan speed control design. For optimum heat dissipation, it is recommended that a system fan be installed inside the chassis.



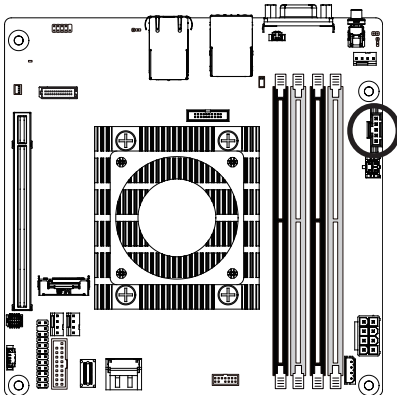
Pin No.	Definition
1	GND
2	+12V
3	Sense
4	Speed Control



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

8) PMBus Connector

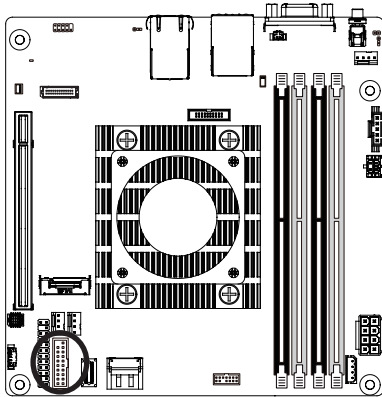
The Power Management Bus (PMBus) is a variant of the System Management Bus (SMBus) which is targeted at digital management of power supplies.



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

9) F_USB3_1 (Front Panel USB 3.0 Connector)

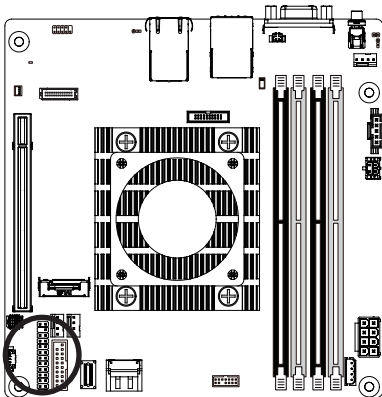
The connector/header conform to USB 3.0 specification. Each USB connector/header can provide two USB ports via an optional USB bracket. For purchasing the optional USB bracket, please contact the local dealer.



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

10) FP_1 (Front Panel Header)

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

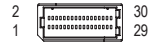
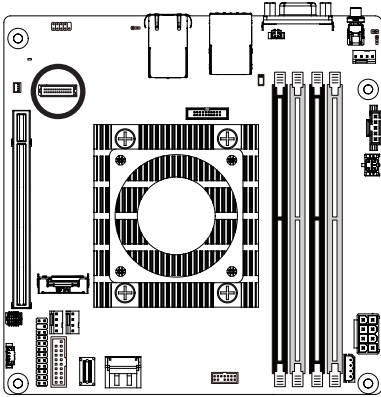


Pin No.	Definition	Pin No.	Definition
1	Power LED+	2	5V Standby
3	No Pin	4	ID LED+
5	Power LED-	6	ID LED-
7	HDD LED+	8	System Status LED+
9	HDD LED-	10	System Status LED -
11	Power Button	12	LAN1 Active LED+
13	GND	14	LAN1 Link LED-
15	Reset Button	16	SMBus Data
17	GND	18	SMBus Clock
19	ID Button	20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



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

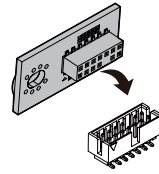
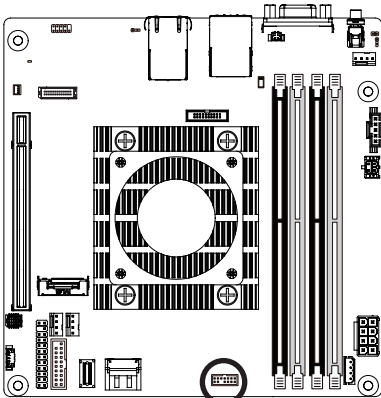
11) BP_1 (HDD Backplane Board Connector)



Pin No.	Definition	Pin No.	Definition
1	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	12C_DEV_RST
21	PH_HP_SCL0	22	GND
23	PH_HP_SDA0	24	GND
25	PH_HP_SCL1	26	GND
27	PH_HP_SDA1	28	GND
29	P3V3_AUX	30	P3V3_AUX

12) SPI_TPM (Trusted Platform Module Connector)

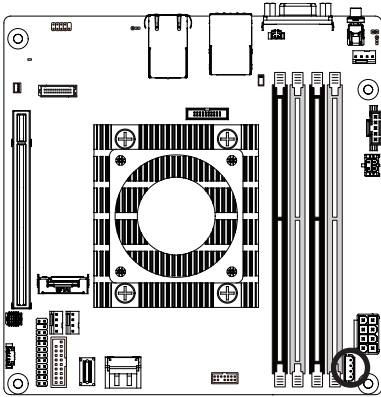
Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.



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

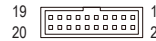
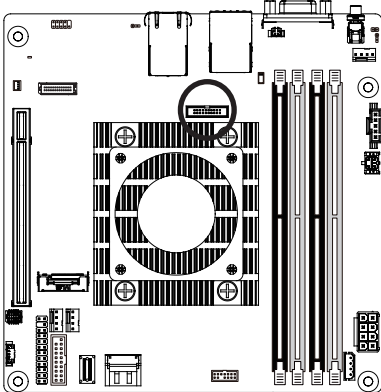
13) IPMB1 (Intelligent Platform Management Bus) Connector

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	Data
3	GND
4	VCC

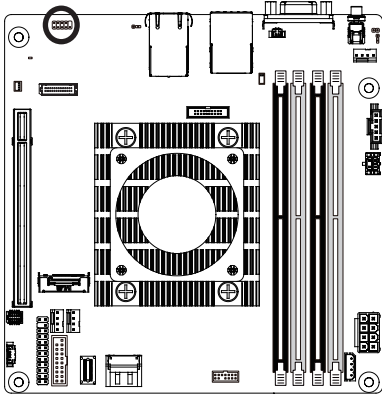
14) CN_NCSI (NCSI Connector)



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

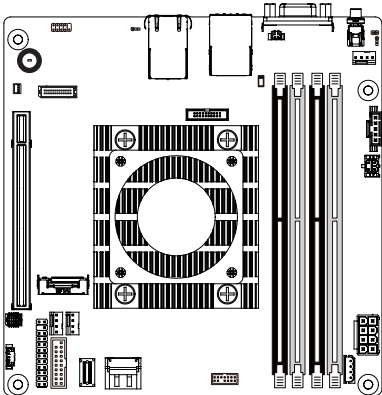
15) COM (Serial Port Header)

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

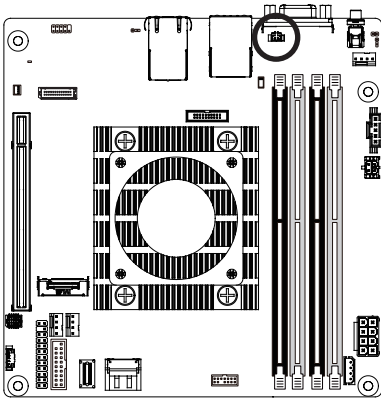
16) LED_BMC (BMC Firmware Readiness LED)



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

17) BAT (Battery Cable Connector)

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.



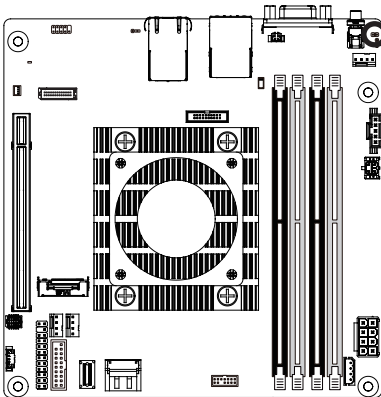
Pin No.	Definition
1	Battery+
2	GND



- 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.

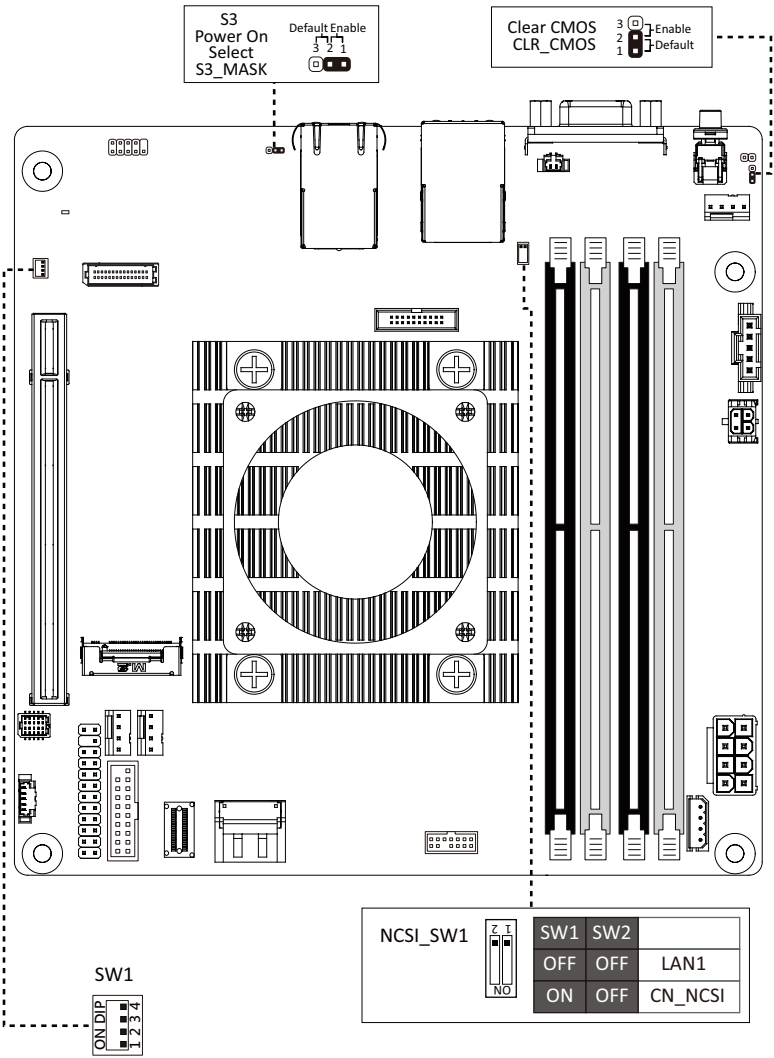
18) CASE_OPEN (Case Open Intrusion Alert Header)

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



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

1-7 Jumper Settings



SW1		ON	OFF
1	ME UPDATE	Force ME update	Normal [Default]
2	Password Clean	Clear supervisor password	Normal [Default]
3	BIOS RCVR	BIOS recovery mode	Normal [Default]
4	ME RCVR	ME recovery mode	Normal [Default]

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 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 Platform Controller Hub.

■ **Server Management**

Server additional features enabled/disabled setup menus.

■ **Security**

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

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

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

■ **Boot**

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

■ **Save & Exit**

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

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

2-1 The Main Menu

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

Main Menu Help

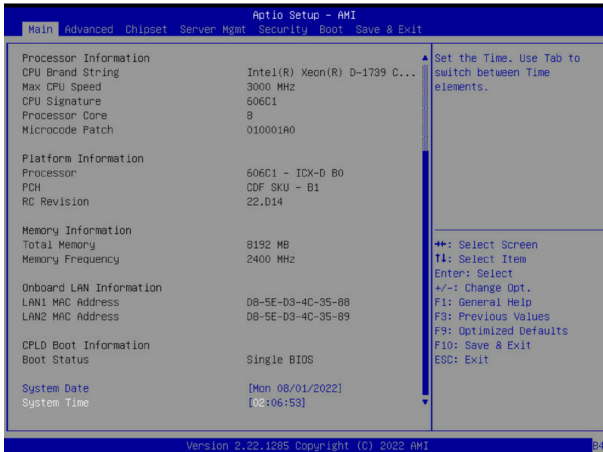
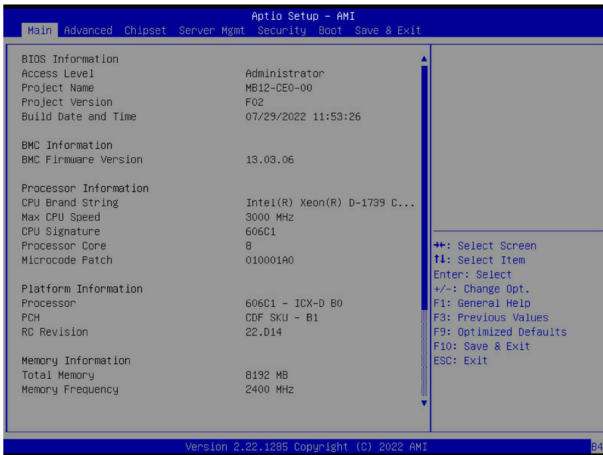
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

Submenu Help

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



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



Parameter	Description
BIOS Information	
Access Level	Displays the privileges level 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 ^(Note1)	
BMC Firmware Version	Displays BMC firmware version information.
Processor Information	
CPU Brand String/ Max CPU Speed / CPU Signature/ Processor Core/ Microcode Patch	Displays the technical information for the installed processor.
Platform Information	
Processor/ PCH/ RC Revision	Displays the information for the installed platform.
Memory Information ^(Note2)	
Total Memory	Displays the total memory size of the installed memory.
Memory Frequency	Displays the frequency information of the installed memory.
Onboard LAN Information	
LAN# MAC Address ^(Note3)	Displays LAN MAC address information.
ME FW Version	Displays ME Firmware version.
System Language	Option: English.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

(Note1) Functions available on selected models.

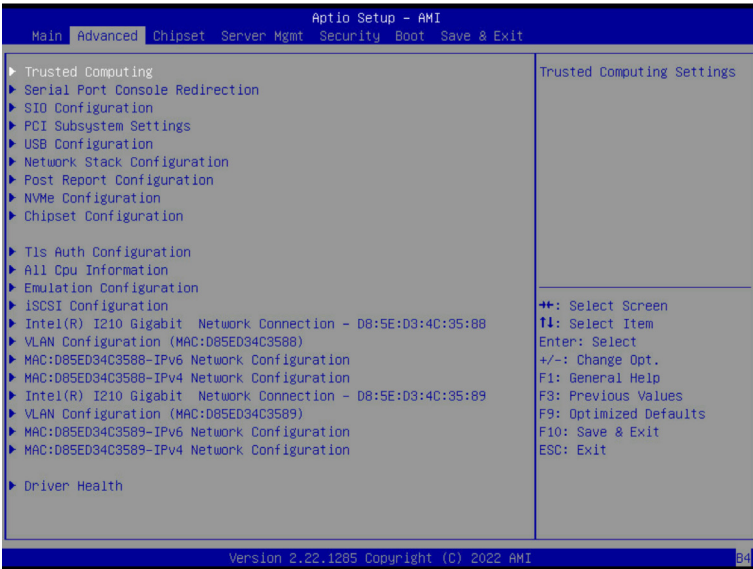
(Note2) This section will display capacity and frequency information of the memory that the customer has installed.

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

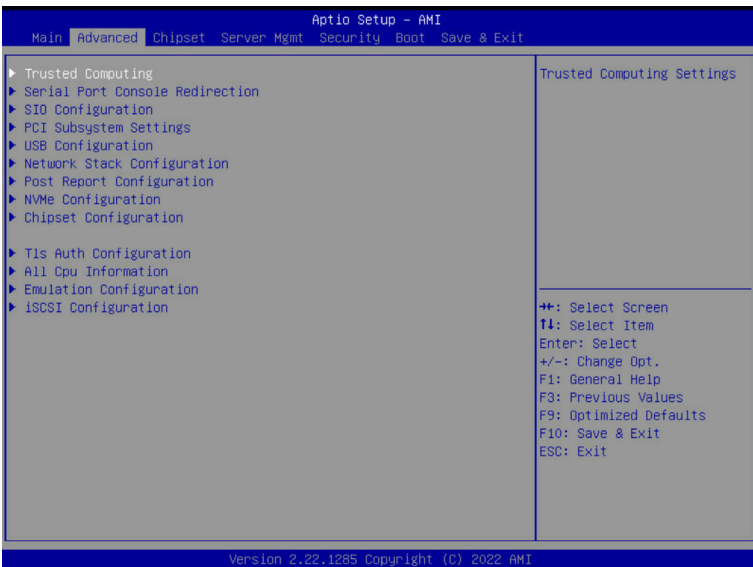
2-2 Advanced Menu

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

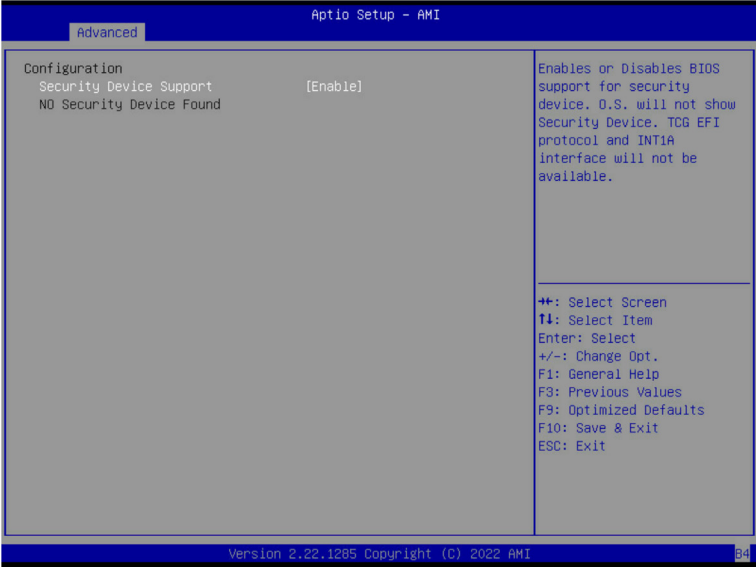
When Boot Mode Select is set to UEFI (Default)



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

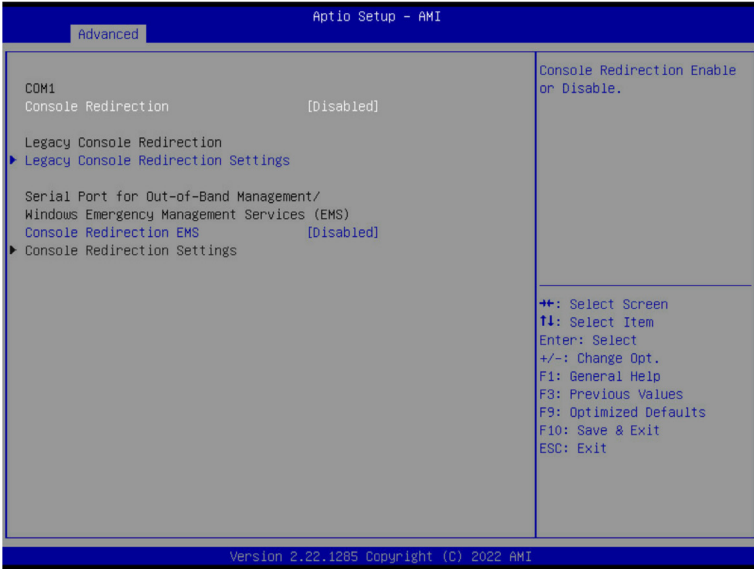


2-2-1 Trusted Computing



Parameter	Description
Configuration	
Security Device Support	<p>Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>

2-2-2 Serial Port Console Redirection



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

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

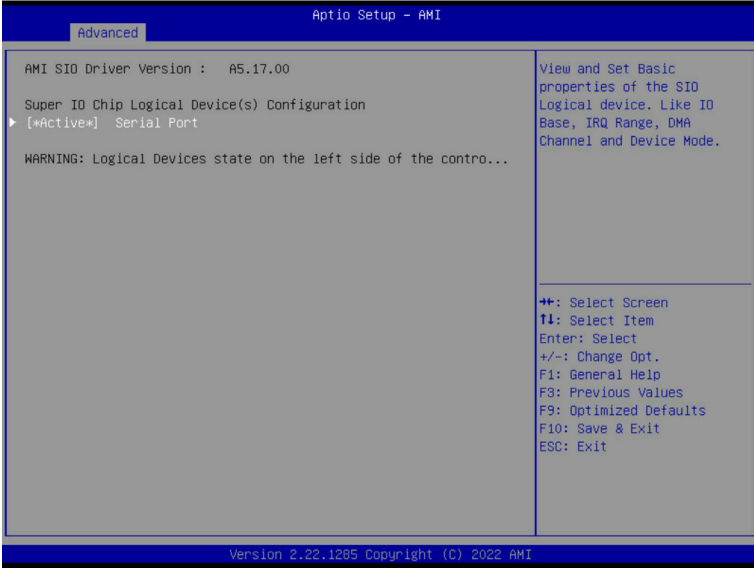
Parameter	Description
COM Console Redirection Settings (continued)	<ul style="list-style-type: none"> ◆ Parity <ul style="list-style-type: none"> – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: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

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

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

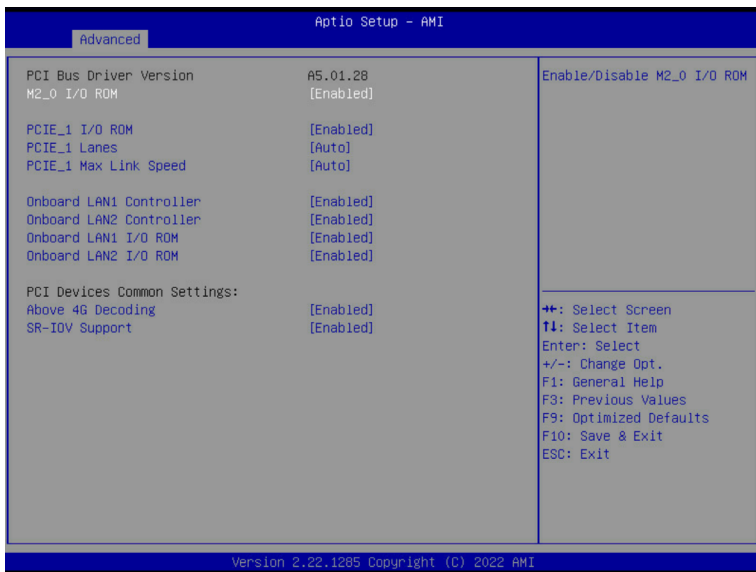
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	<ul style="list-style-type: none">◆ Flow Control EMS<ul style="list-style-type: none">– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' 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.– Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is None.

2-2-3 SIO Configuration



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

2-2-4 PCI Subsystem Settings



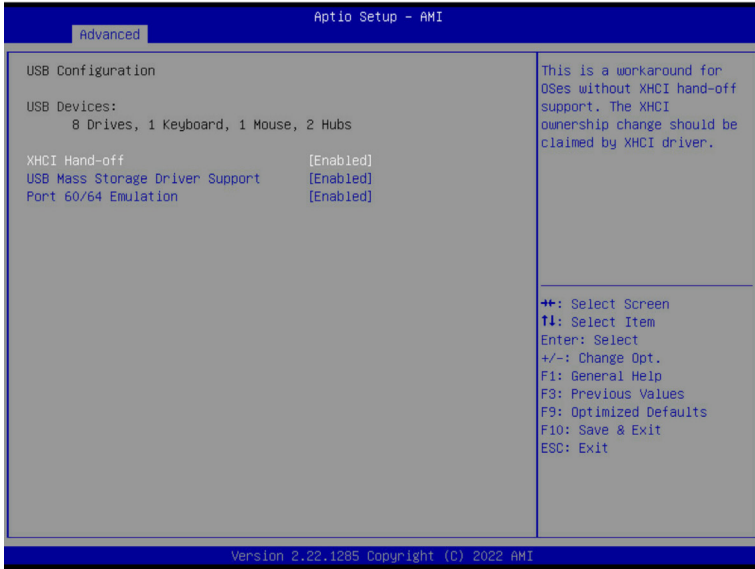
Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
M2_0 I/O ROM	Enable/Disable M2_0 I/O ROM. Options available: Enabled, Disabled. Default setting is Enabled .
PCI_E_# I/O ROM ^(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled, Disabled. Default setting is Enabled .
PCI_E_# Lanes ^(Note1)	Change the PCIe lanes. Options available: Auto, x16, x8x8, x8x4x4, x4x4x8, x4x4x4x4. Default setting is Auto .
PCI_E_# Max Link Speed ^(Note1)	Change the PCIe max link speed. Options available: Auto, Gen1, Gen2, Gen3, Gen4. Default setting is Auto .
Onboard LAN# Controller ^(Note2)	Enable/Disable the onboard LAN devices. Options available: Enabled, Disabled. Default setting is Enabled .
Onboard LAN# I/O ROM ^(Note2)	Enable/Disable the onboard LAN devices, and initializes device expansion ROM. Options available: Enabled, Disabled. Default setting is Enabled .

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

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

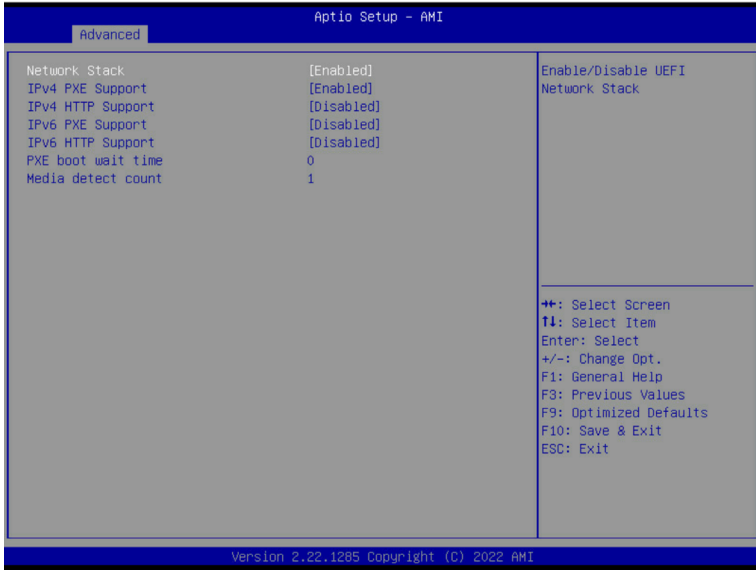
Parameter	Description
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled, Disabled. Default setting is Enabled .
SR-IOV Support	If the system has SR-IOV capable PCIe devices, this item Enable/Disable Single Root IO Virtualization Support. Options available: Enabled, Disabled. Default setting is Enabled .

2-2-5 USB Configuration



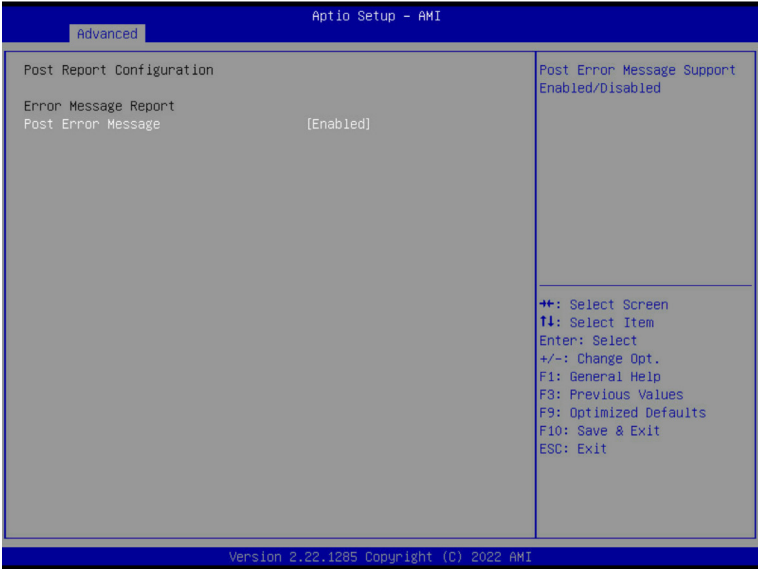
Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Disabled, Enabled. Default setting is Enabled .
USB Mass Storage Driver Support	Enable/Disable USB Mass Storage Driver Support Options available: Disabled, Enabled. Default setting is Enabled .
Port 60/64 Emulation	Enable/Disable I/O port 60h/64h emulation support. Options available: Disabled, Enabled. Default setting is Enabled .

2-2-6 Network Stack Configuration



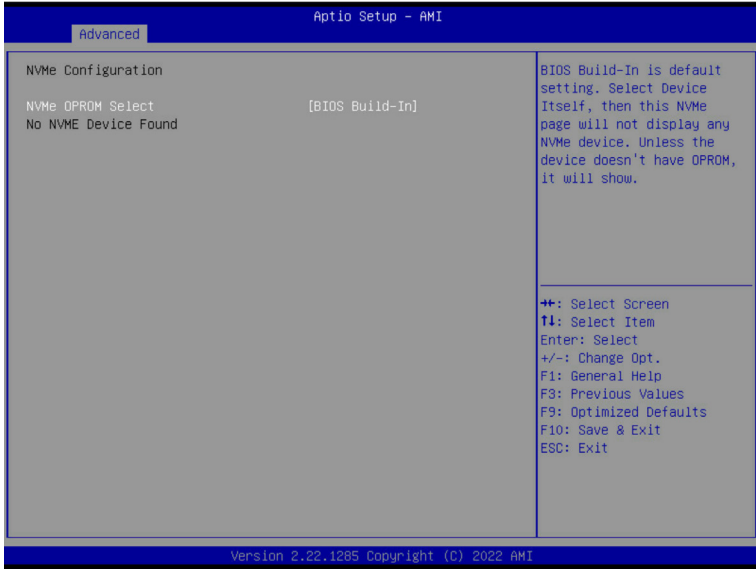
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled, Disabled. Default setting is Enabled .
IPv4 PXE Support	Enable/Disable the IPv4 PXE feature. Options available: Enabled, Disabled. Default setting is Enabled .
IPv4 HTTP Support	Enable/Disable the IPv4 HTTP feature. Options available: Enabled, Disabled. Default setting is Disabled .
IPv6 PXE Support	Enable/Disable the IPv6 PXE feature. Options available: Enabled, Disabled. Default setting is Disabled .
IPv6 HTTP Support	Enable/Disable the IPv6 HTTP feature. Options available: Enabled, Disabled. Default setting is Disabled .
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Press the <+> / <-> keys to increase or decrease the desired values.
Media detect count	Number of times the presence of media will be checked. Press the <+> / <-> keys to increase or decrease the desired values.

2-2-7 Post Report Configuration



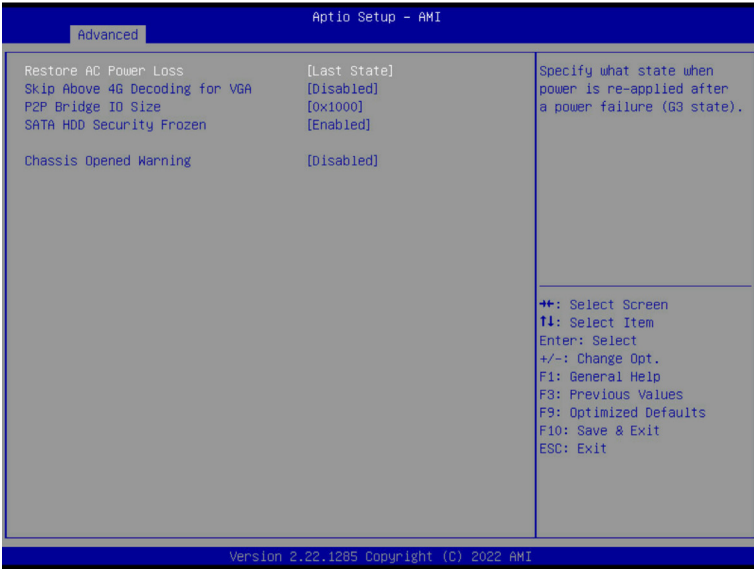
Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled, Disabled. Default setting is Enabled .

2-2-8 NVMe Configuration



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

2-2-9 Chipset Configuration



Parameter	Description
Restore on AC Power Loss ^(Note)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
Skip Above 4G Decoding for VGA	Enable/Disable 64bit capable devices to be decoded in Skip Above 4G Address VGA Space. Options available: Enabled, Disabled. Default setting is Disabled .
P2P Bridge IO Size	Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is 0x1000 .
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: Enabled, Disabled. Default setting is Enabled .
Chassis Opened Warning	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is Disabled .

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

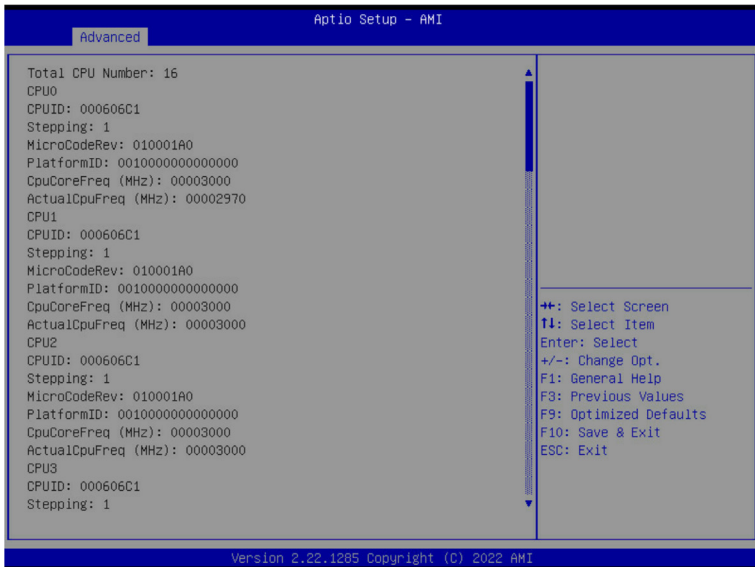
2-2-10 Tls Auth Configuration



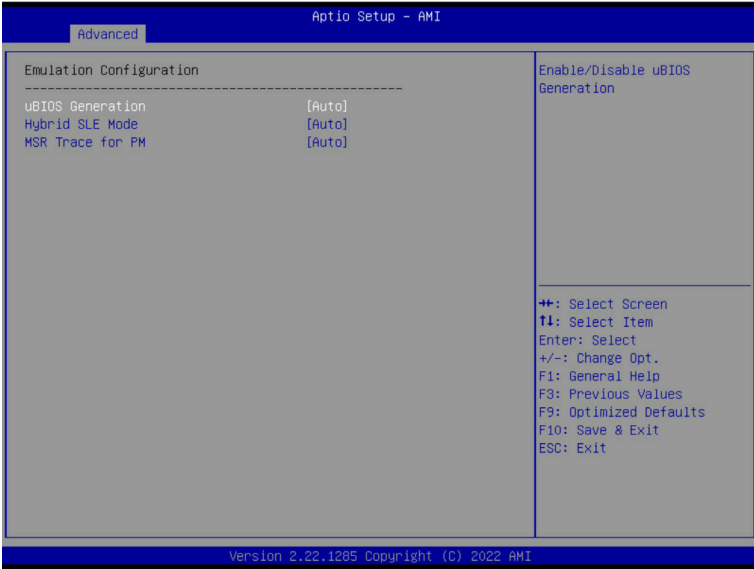
Parameter	Description
Server CA Configuration	<p>Press [Enter] for configuration of advanced items.</p> <ul style="list-style-type: none"> ◆ Enroll Cert <ul style="list-style-type: none"> – Press [Enter] to enroll a certificate <ul style="list-style-type: none"> • Enroll Cert Using File • Cert GUID 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

2-2-11 All Cpu Information

This page is a simple display page for all CPU information. Items on this window are non-configurable.

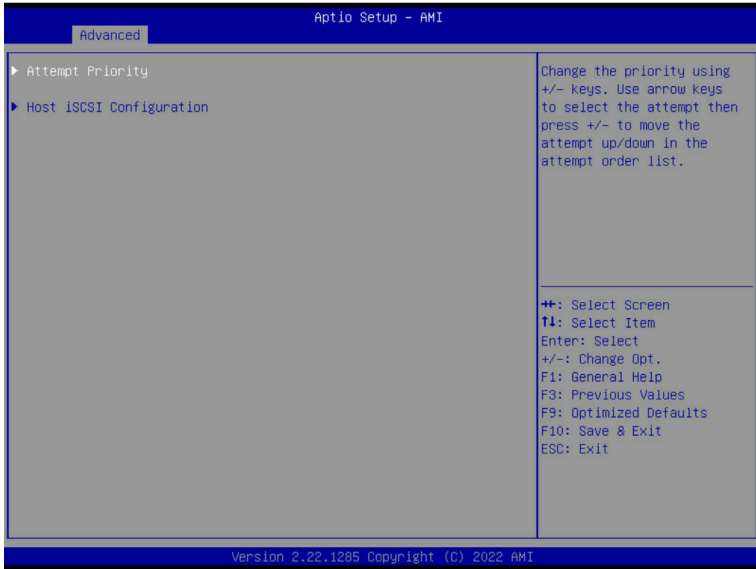


2-2-12 Emulation Configuration



Parameter	Description
uBIOS Generation	Enable/Disable uBIOS generation. Options available: Disable, Enable, Auto. Default setting is Auto .
Hybrid SLE Mode	Enable/Disable Hybrid system level emulation mode. Options available: Disable, Enable, Auto. Default setting is Auto .
MSR Trace for PM	Enable/Disable MSR trace for power management in uBIOS. Options available: Disable, Enable, Auto. Default setting is Auto .

2-2-13 iSCSI Configuration



Parameter	Description
Attempt Priority	<p>Press [Enter] configure advanced items.</p> <ul style="list-style-type: none"> ◆ Attempt Priority <ul style="list-style-type: none"> – Options available: Host Attempt, Redfish Attempt. Default setting is Host Attempt. ◆ Commit Changes and Exit
Host iSCSI Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ iSCSI Initiator Name <ul style="list-style-type: none"> – Only IQN format is accepted. Range: from 4 to 223 ◆ Add an Attempt ◆ Delete Attempts ◆ Change Attempt Order

2-2-14 Intel(R) I210 Gigabit Network Connection

Aptio Setup - AMI

Advanced

<p>► NIC Configuration</p> <p>Blink LEDs 0</p> <p>UEFI Driver Intel(R) PRO/1000 7.5.11 ...</p> <p>Adapter PBA 140724-006</p> <p>Device Name Intel(R) I210 Gigabit Ne...</p> <p>Chip Type Intel i210</p> <p>PCI Device ID 1533</p> <p>PCI Address 01:00:00</p> <p>Link Status [Connected]</p> <p>MAC Address D8:5E:D3:4C:95:88</p> <p>Virtual MAC Address 00:00:00:00:00:00</p>		<p>Click to configure the network device port.</p>
		<p>++: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F3: Previous Values</p> <p>F9: Optimized Defaults</p> <p>F10: Save & Exit</p> <p>ESC: Exit</p>

Version 2.22.1285 Copyright (C) 2022 AMI

Aptio Setup - AMI

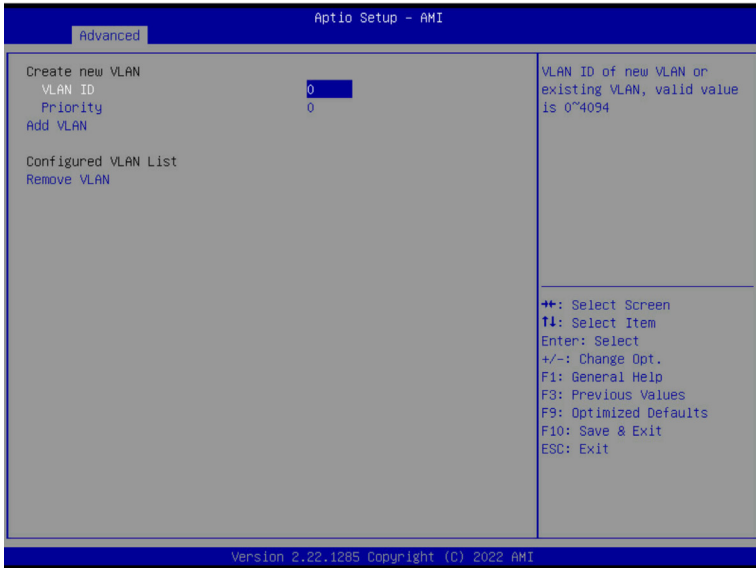
Advanced

<p>Link Speed [Auto Negotiated]</p> <p>Wake On LAN [Enabled]</p>		<p>Specifies the port speed used for the selected boot protocol.</p>
		<p>++: Select Screen</p> <p>↑↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F3: Previous Values</p> <p>F9: Optimized Defaults</p> <p>F10: Save & Exit</p> <p>ESC: Exit</p>

Version 2.22.1285 Copyright (C) 2022 AMI

Parameter	Description
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Link Speed <ul style="list-style-type: none"> – Specifies the port speed used for the selected boot protocol. – Options available: Auto Negotiated, 10Mbps Half, 10Mbps Full, 100Mbps Half, 100Mbps Full. Default setting is Auto Negotiated. ◆ Wake On LAN <ul style="list-style-type: none"> – 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. – Options available: Enabled, Disabled. Default setting is Enabled.
Blink LEDs	<p>Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).</p>
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

2-2-15 VLAN Configuration



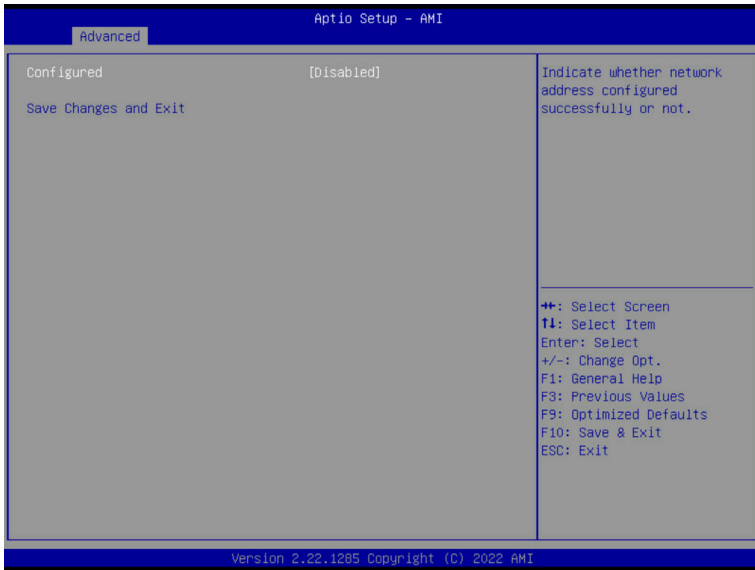
Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Create new VLAN ◆ VLAN ID <ul style="list-style-type: none"> – Sets VLAN ID for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the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

2-2-16 MAC IPv6 Network Configuration



Parameter	Description
Enter Configuration Menu	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Displays the MAC Address information. ◆ Interface ID <ul style="list-style-type: none"> – The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3. ◆ DAD Transmit Count <ul style="list-style-type: none"> – 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. ◆ Policy <ul style="list-style-type: none"> – Options available: automatic, manual. Default setting is automatic. ◆ Save Changes and Exit <ul style="list-style-type: none"> – Press [Enter] to save all configurations.

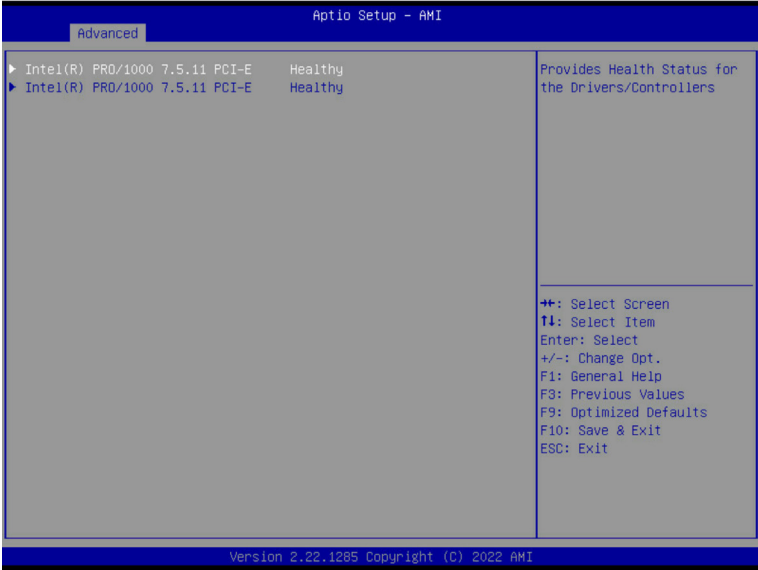
2-2-17 MAC IPv4 Network Configuration



Parameter	Description
Configured	Indicates whether network address is configured successfully or not. Options available: Enabled, Disabled. Default setting is Disabled .
Enable DHCP ^(Note)	Options available: Enabled, Disabled. Default setting is Disabled .
Local IP Address ^(Note)	Press [Enter] to configure local IP address.
Local NetMask ^(Note)	Press [Enter] to configure local NetMask.
Local Gateway ^(Note)	Press [Enter] to configure local Gateway
Local DNS Servers ^(Note)	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**.

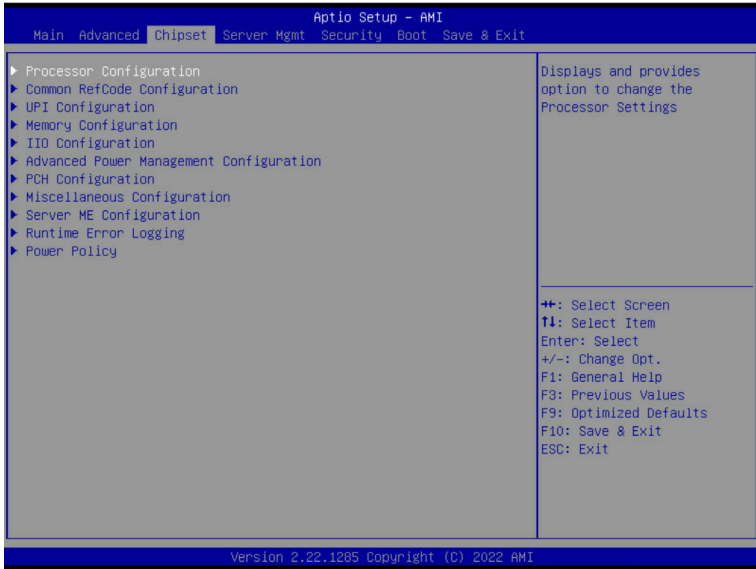
2-2-18 Driver Health



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

2-3 Chipset Menu

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



2-3-1 Processor Configuration

Aptio Setup - AMI

Chipset

Processor Configuration		Change Per-Socket Settings

▶ Per-Socket Configuration		
Processor Socket	Socket 0	
Processor ID	000606C1*	
Processor Frequency	3.000GHz	
Processor Max Ratio	1EH	
Processor Min Ratio	08H	
Microcode Revision	010001A0	
L1 Cache RAM(Per Core)	80KB	
L2 Cache RAM(Per Core)	1280KB	
L3 Cache RAM(Per Package)	15360KB	
Processor 0 Version	Intel(R) Xeon(R) D-1739	

Hyper-Threading [ALL]	[Enable]	++: Select Screen
Hardware Prefetcher	[Enable]	T1: Select Item
Adjacent Cache Prefetch	[Enable]	Enter: Select
DCU Streamer Prefetcher	[Enable]	+/-: Change Opt.
DCU IP Prefetcher	[Enable]	F1: General Help
Extended APIC	[Disable]	F3: Previous Values
Enable Intel(R) TXT	[Disable]	F9: Optimized Defaults
VMX	[Enable]	F10: Save & Exit
Enable SMX	[Disable]	ESC: Exit
AES-NI	[Enable]	

Version 2.22.1285 Copyright (C) 2022 AMI

Aptio Setup - AMI

Chipset

Processor ID	000606C1*	▲ Enable/Disable Total Memory Encryption (TME)
Processor Frequency	3.000GHz	
Processor Max Ratio	1EH	
Processor Min Ratio	08H	
Microcode Revision	010001A0	
L1 Cache RAM(Per Core)	80KB	
L2 Cache RAM(Per Core)	1280KB	
L3 Cache RAM(Per Package)	15360KB	
Processor 0 Version	Intel(R) Xeon(R) D-1739	

Hyper-Threading [ALL]	[Enable]	
Hardware Prefetcher	[Enable]	
Adjacent Cache Prefetch	[Enable]	
DCU Streamer Prefetcher	[Enable]	
DCU IP Prefetcher	[Enable]	
Extended APIC	[Disable]	
Enable Intel(R) TXT	[Disable]	
VMX	[Enable]	
Enable SMX	[Disable]	
AES-NI	[Enable]	

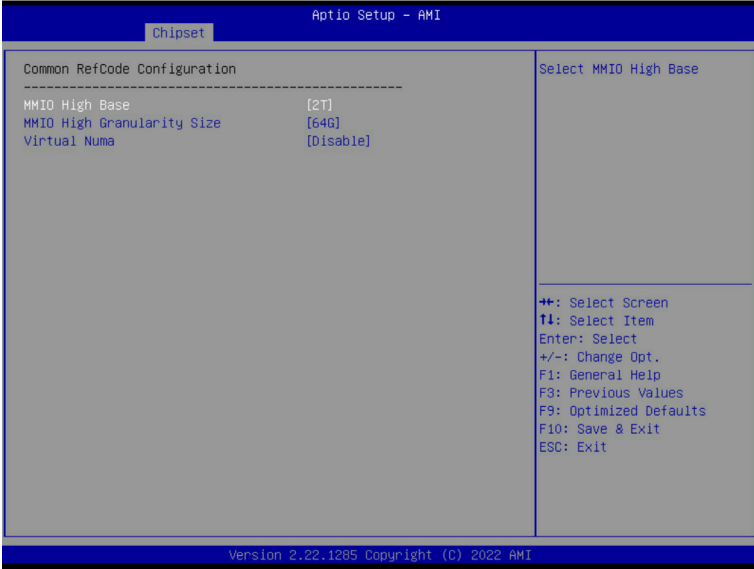
TME, TME-MT, TDX		

Total Memory Encryption (TME)	[Disabled]	++: Select Screen T1: Select Item Enter: Select +/-: Change Opt. F1: General Help F3: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit

Version 2.22.1285 Copyright (C) 2022 AMI

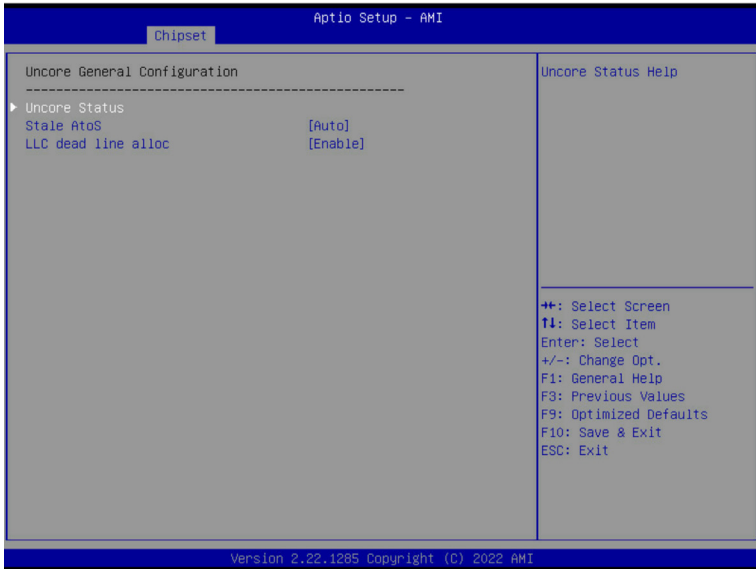
Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ CPU Socket 0 Configuration <ul style="list-style-type: none"> – Core Disable Bitmap(Hex) <ul style="list-style-type: none"> • Number of Cores to enable. 0 means all cores. FFFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.
Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Per Core) / L3 Cache RAM(Per Package) / Processor # Version	Displays the technical specifications for the installed processor(s).
Hyper-Threading [All]	<p>The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Hardware Prefetcher	<p>Select whether to enable the speculative prefetch unit of the processor.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Adjacent Cache Prefetch	<p>When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
DCU Streamer Prefetcher	<p>Enable/Disable DCU streamer prefetcher.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
DCU IP Prefetcher	<p>Enable/Disable DCU IP Prefetcher.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Extended APIC	<p>Enable/Disable extended APIC support. Note: The VT-d will be enabled automatically when x2APIC is enabled.</p> <p>Options available: Enable, Disable. Default setting is Disable.</p>
Enable Intel(R) TXT	<p>Enable/Disable the Intel Trusted Execution Technology support function.</p> <p>Options available: Enable, Disable. Default setting is Disable.</p>
VMX (Vanderpool Technology)	<p>Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Enable SMX	<p>Enable/Disable the Safer Mode Extensions (SMX) support function.</p> <p>Options available: Enable, Disable. Default setting is Disable.</p>
AES-NI	<p>Enable/Disable the AES-NI support.</p> <p>Options available: Enable, Disable. Default setting is Enable.</p>
Total Memory Encryption (TME)	<p>Enable/Disable total memory encryption (TME).</p> <p>Options available: Enabled, Disabled. Default setting is Disabled.</p>

2-3-2 Common RefCode Configuration



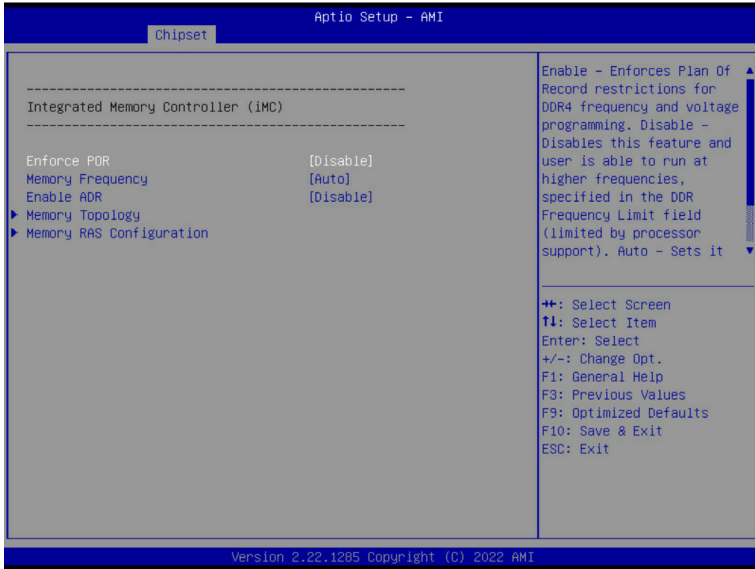
Parameter	Description
Common RefCode Configuration	
MMIO High Base	Selects the MMIO High Base setting. Options available: 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T. Default setting is 56T .
MMIO High Granularity Size	Selects the allocation size used to assign memory-mapped I/O (MMIO) resources. Total mmio space can be up to 32x granularity. Per stack mmio resource assignments are multiples of the granularity where 1 unit per stack is the default allocation. Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is 256G .
Virtual Numa	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors. Options available: Enable, Disable. Default setting is Disable .

2-3-3 UPI Configuration



Parameter	Description
UnCore General Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ UnCore Status <ul style="list-style-type: none"> – Press [Enter] to view the UnCore status. ◆ Stale AtoS <ul style="list-style-type: none"> – Enable/Disable Stale A to S directory optimization. – Options available: Disable, Enable, Auto. Default setting is Auto. ◆ LLC dead line alloc <ul style="list-style-type: none"> – Enable/Disable fill dead lines in LLC. – Options available: Disable, Enable, Auto. Default setting is Enable.

2-3-4 Memory Configuration



Parameter	Description
Integrated Memory Controller (iMC)	
Enforce POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. Options available: POR, Disable. Default setting is Disable .
Memory Frequency	Configures the maximum memory frequency. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Default setting is Auto .
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable, Disable. Default setting is Disable .
Legacy ADR Mode ^(Note)	Enable/Disable the Legacy ADR Mode. Options available: Enable, Disable. Default setting is Disable .
Minimum System Memory Size ^(Note)	Configures the minimum memory size. Options available: 2GB, 4GB, 6GB, 8GB. Default setting is 2GB .
Memory Topology	Press [Enter] to view memory topology with DIMM population information.

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

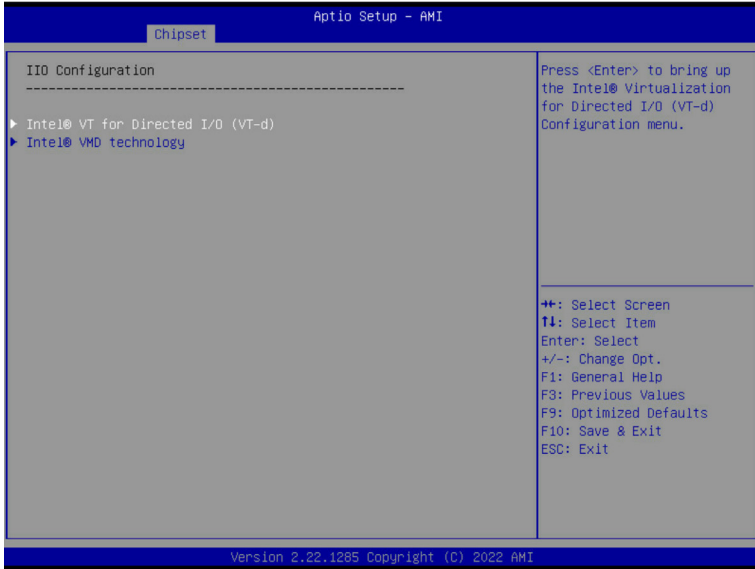
Parameter	Description
Memory RAS Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Mirror Mode <ul style="list-style-type: none"> – Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch. – Options available: Disabled, Full Mirror Mode, Partial Mirror Mode. Default setting is Disabled. ◆ Correctable Error Threshold <ul style="list-style-type: none"> – Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket. – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Trigger SW Error Threshold <ul style="list-style-type: none"> – Enable/Disable Sparing trigger SW Error Match Threshold. – Options available: Disabled, Enabled. Default setting is Disabled. ◆ Leaky bucket time window based interface <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Disabled. ◆ Leaky bucket low bit <ul style="list-style-type: none"> – Configures leaky bucket low bit (1-63). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket high bit <ul style="list-style-type: none"> – Configures leaky bucket high bit (1-63). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ ADDDC Sparing <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Disabled. ◆ Enable ADDDC Error Injection^(Note1) <ul style="list-style-type: none"> – Options available: Disabled, Enabled. Default setting is Enabled. ◆ Column Correction Disable^(Note2) <ul style="list-style-type: none"> – Options available: Disable, Enable. Default setting is Disable. ◆ Patrol Scrub <ul style="list-style-type: none"> – Options available: Disabled, Enabled, Enable at End of POST. Default setting is Disabled. ◆ Patrol Scrub Interval^(Note3) <ul style="list-style-type: none"> – Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto.

(Note1) This item appears when **ADDDC Sparing** is set to **Enabled**.

(Note2) This item is configurable when **ADDDC Sparing** is set to **Enabled**.

(Note3) This item appears when **Patrol Scrub** is set to **Enabled**.

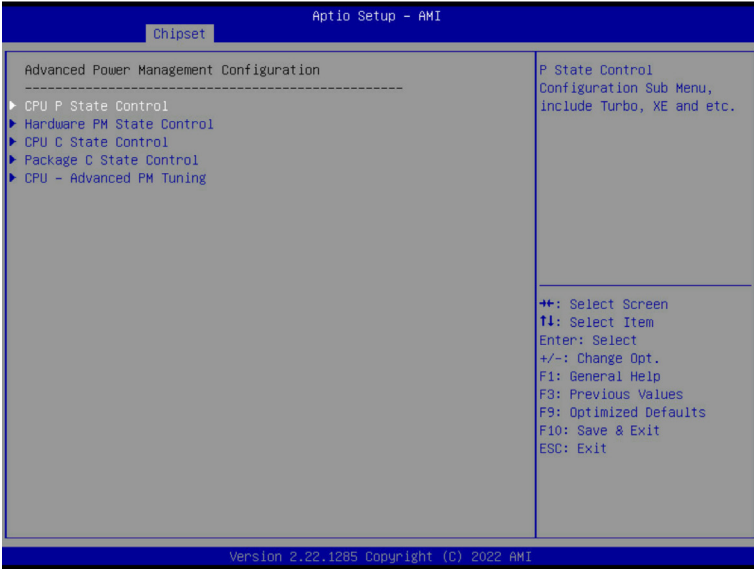
2-3-5 IIO Configuration



Parameter	Description
IIO Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Intel® VT for Directed I/O <ul style="list-style-type: none"> – Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. – Options available: Enable, Disable. Default setting is Enable. ◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> – Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA). – Options available: Enable, Disable. Default setting is Disable. ◆ Intel® VT for Directed I/O (VT-d) <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ Interrupt Remapping <ul style="list-style-type: none"> – Enable/Disable the interrupt remapping support function. – Options available: Auto, Enable, Disable. Default setting is Auto. ◆ x2APIC Opt Out <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ Pre-boot DMA Protection <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable. ◆ PCIe ACSCTL <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable.

Parameter	Description
Intel® VMD technology	<p data-bbox="373 142 710 166">Press [Enter] to configure advanced items.</p> <ul data-bbox="373 170 954 285" style="list-style-type: none"><li data-bbox="373 170 954 194">◆ Intel® VMD for Volume Management Device on Socket 0<ul data-bbox="416 199 954 285" style="list-style-type: none"><li data-bbox="416 199 954 222">– VMD Config for PCH ports/ IOU 0<ul data-bbox="437 227 954 285" style="list-style-type: none"><li data-bbox="437 227 954 250">• Enable/Disable Intel® VMD<li data-bbox="437 255 954 285">• Options available: Enable, Disable. Default setting is Disable.

2-3-6 Advanced Power Management Configuration

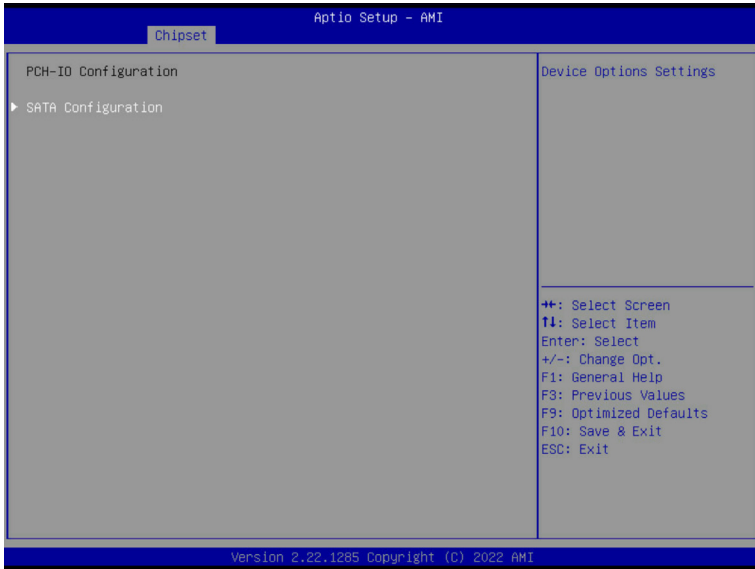


Parameter	Description
Advanced Power Management Configuration	
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ SpeedStep (Pstates) <ul style="list-style-type: none"> – Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. – Options available: Enable, Disable. Default setting is Enable. ◆ Turbo Mode <ul style="list-style-type: none"> – When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. – Options available: Enable, Disable. Default setting is Enable.

Parameter	Description
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Hardware P-States <ul style="list-style-type: none"> – When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States). – In Native mode, the processor hardware chooses a P-state based on OS guidance. – In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance). – Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is Native Mode.
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Enable Monitor MWAIT <ul style="list-style-type: none"> – Allows Monitor and MWAIT instructions. – Options available: Enable, Disable. Default setting is Enable. ◆ CPU C6 Report <ul style="list-style-type: none"> – Enable/Disable CPU C6(ACPI C3) report to OS. – Options available: Disable, Enable, Auto. Default setting is Disable. ◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> – Core C1E auto promotion control. Takes effect after reboot. – Options available: Enable, Disable. Default setting is Disable.
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Package C State <ul style="list-style-type: none"> – Configures the state for the C-State package limit. – Options available: C0/C1 state, C2 state, C6(non Retention) state, Auto. Default setting is Auto.
CPU - Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Energy Perf BIAS <ul style="list-style-type: none"> – Enters the Energy Perf BIAS submenu. <ul style="list-style-type: none"> » Power Performance Tuning <ul style="list-style-type: none"> • Options available: OS Controls EPB, BIOS Controls EPB, PECCI Controls EPB. Default setting is OS Controls EPB. » Energy_PERF_BIAS_CFG mode^(Note) <ul style="list-style-type: none"> • Options available: Performance, Balanced Performance, Balanced Power, Power. Default setting is Performance.

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

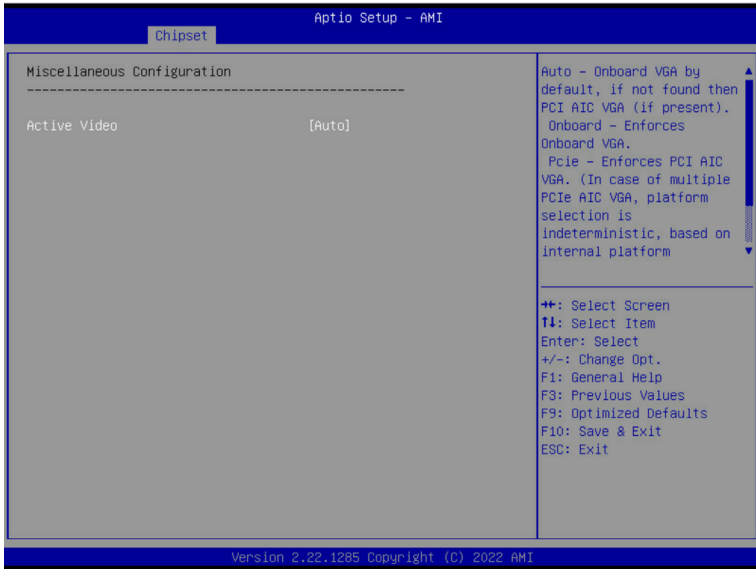
2-3-7 PCH-IO Configuration



Parameter	Description
SATA Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> ◆ Controller 2 SATA Configuration <ul style="list-style-type: none"> – SATA Configuration <ul style="list-style-type: none"> » Enable/Disable SATA device. » Options available: Enabled, Disabled. Default setting is Enabled. – SATA Mode Selection <ul style="list-style-type: none"> » Determines how SATA controller(s) operate. » Options available: AHCI, RAID. Default setting is AHCI. – SATA Port # <ul style="list-style-type: none"> » Port # <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Enabled. » Hot Plug <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Enabled. » Spin Up Device <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Disabled.

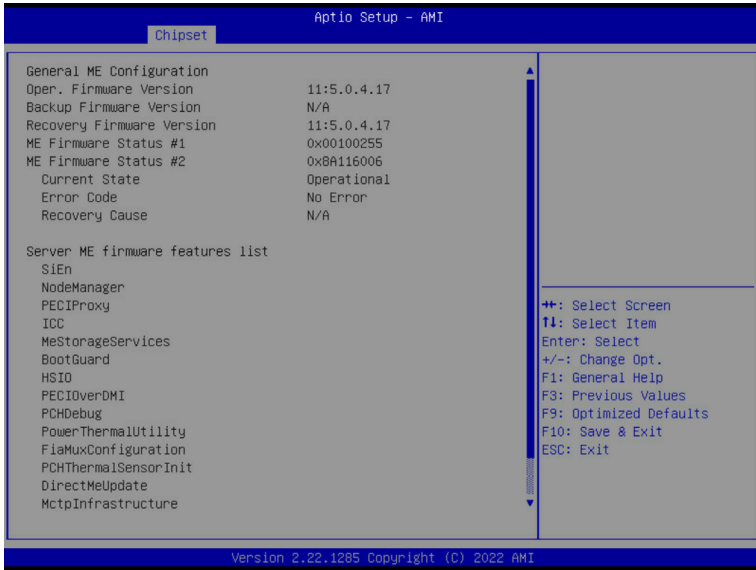
Parameter	Description
SATA Configuration (continued)	<ul style="list-style-type: none"> ◆ Controller 3 SATA Configuration <ul style="list-style-type: none"> – SATA Configuration <ul style="list-style-type: none"> » Enable/Disable SATA device. » Options available: Enabled, Disabled. Default setting is Enabled. – SATA Port 0 <ul style="list-style-type: none"> » Port 0 <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Enabled. » Hot Plug <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Enabled. » Spin Up Device <ul style="list-style-type: none"> • Options available: Enabled, Disabled. Default setting is Disabled.

2-3-8 Miscellaneous Configuration



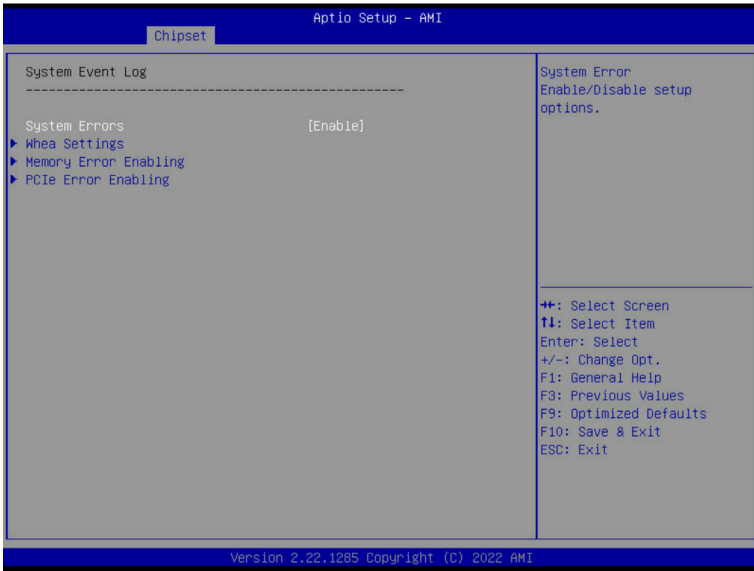
Parameter	Description
Miscellaneous Configuration	
Active Video	Selects the active video type. Options available: Auto, Onboard Device, PCIE Device. Default setting is Auto .

2-3-9 Server ME Configuration



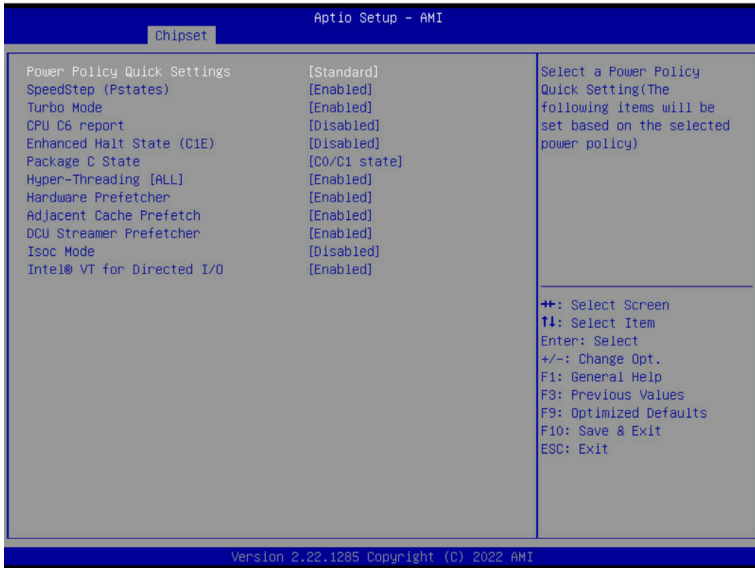
Parameter	Description
General ME Configuration	Displays the operational firmware information.

2-3-10 Runtime Error Logging



Parameter	Description
System Event Log	
System Errors	Enable/Disable system error setup. Options available: Disable, Enable, Auto. Default setting is Enable .
Whea Settings	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ WHEA Support <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable.
Memory Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ Memory Error <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable. ◆ Memory Corrected Error <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Enable ◆ Uncorrected Error disable Memory <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable
PCIe Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> ◆ PCIe Error <ul style="list-style-type: none"> – Options available: Enable, Disable. Default setting is Disable.

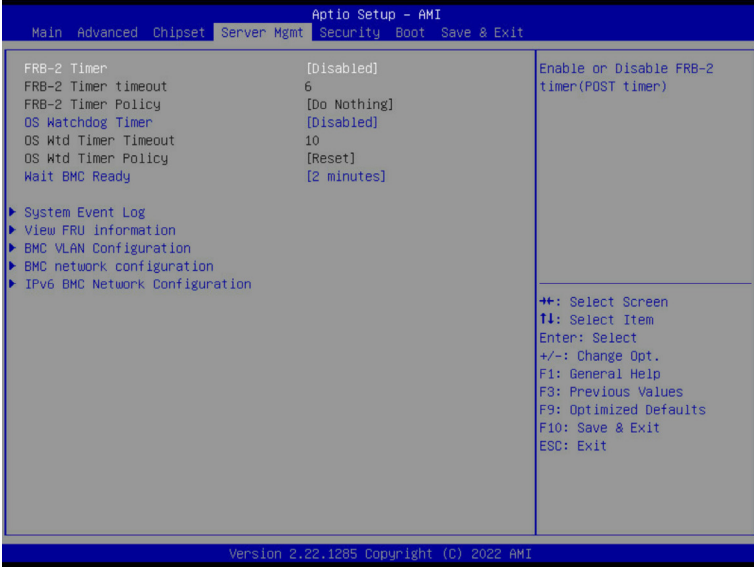
2-3-11 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient, Turbo Lock. Default setting is Standard .
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enabled, Disabled. Default setting is Enabled .
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enabled, Disabled. Default setting is Enabled .
CPU C6 report	Enable/Disable the BIOS to enable the report from the CPU C6 state (ACPI C3) to the OS. Options available: Disabled, Enabled, Auto. Default setting is Disabled .
Enhanced Halt State (C1E)	Enable/Disable the C1E support for lower power consumption. Takes effect after reboot. Options available: Enabled, Disabled. Default setting is Disabled .
Package C State	Configures the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, Auto. Default setting is C0/C1 state .

Parameter	Description
Hyper-Threading [ALL]	The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance. Options available: Enabled, Disabled. Default setting is Enabled .
Hardware Prefetcher	Options available: Enabled, Disabled. Default setting is Enabled .
Adjacent Cache Prefetch	Options available: Enabled, Disabled. Default setting is Enabled .
DCU Streamer Prefetcher	Options available: Enabled, Disabled. Default setting is Enabled .
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enabled, Disabled. Default setting is Disabled .
Intel® VT for Directed I/O (VT-d)	Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. Options available: Enabled, Disabled. Default setting is Enabled .

2-4 Server Management Menu



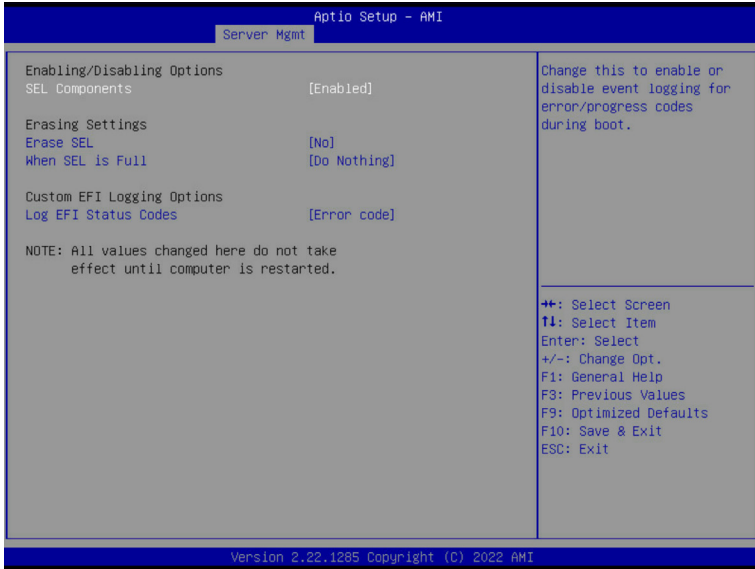
Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, Disabled. Default setting is Disabled .
FRB-2 Timer timeout ^(Note1)	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is 6 .
FRB-2 Timer Policy ^(Note1)	Configures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

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

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

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

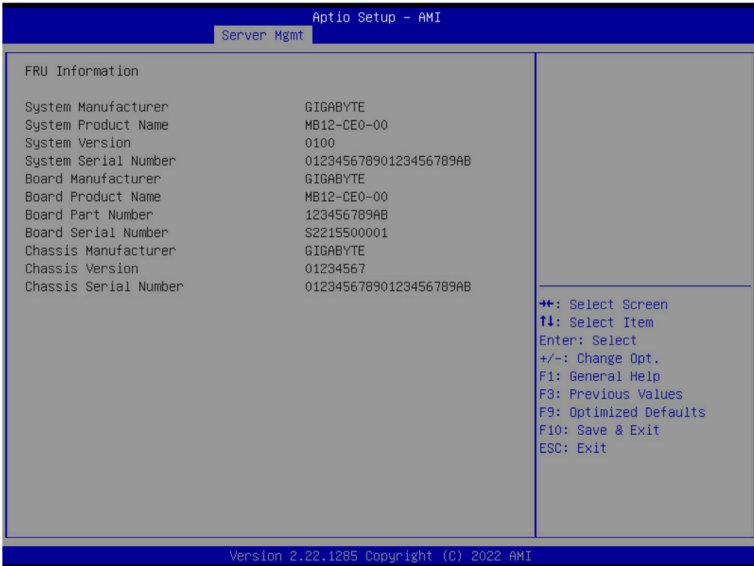
2-4-1 System Event Log



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 Enabled .
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: No Yes, On next reset Yes, On every reset. Default setting is No .
When SEL is Full	Choose options for reactions to a full SEL. Options available: Do Nothing, Erase Immediately, Delete Oldest Record. Default setting is Do Nothing .
Custom EFI Logging Options	
Log EFI Status Codes	Enable/Disable the logging of EFI Status Codes (if not already converted to legacy). Options available: Disabled, Both, Error code, Progress code. Default setting is Error code .

2-4-2 View FRU Information

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



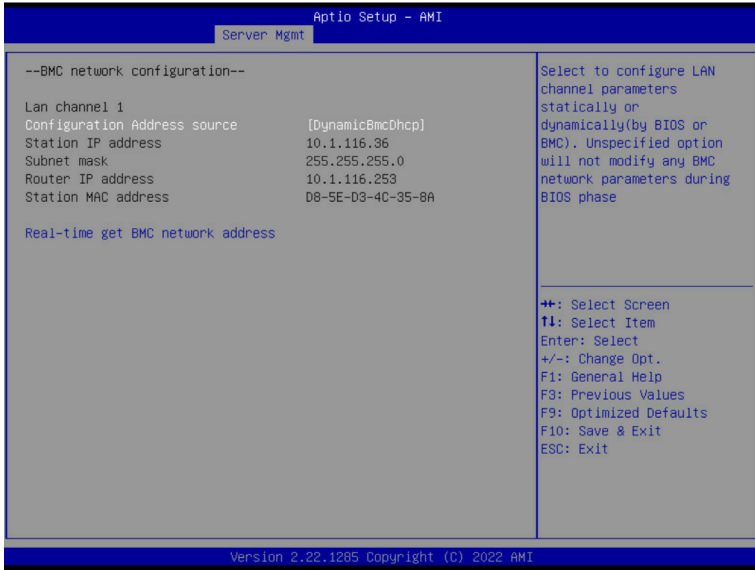
(Note) The model name will vary depends on the product you purchased

2-4-3 BMC VLAN Configuration



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

2-4-4 BMC Network Configuration



Parameter	Description
BMC network configuration	
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 DynamicBmcDhcp .
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 get BMC network address	Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.

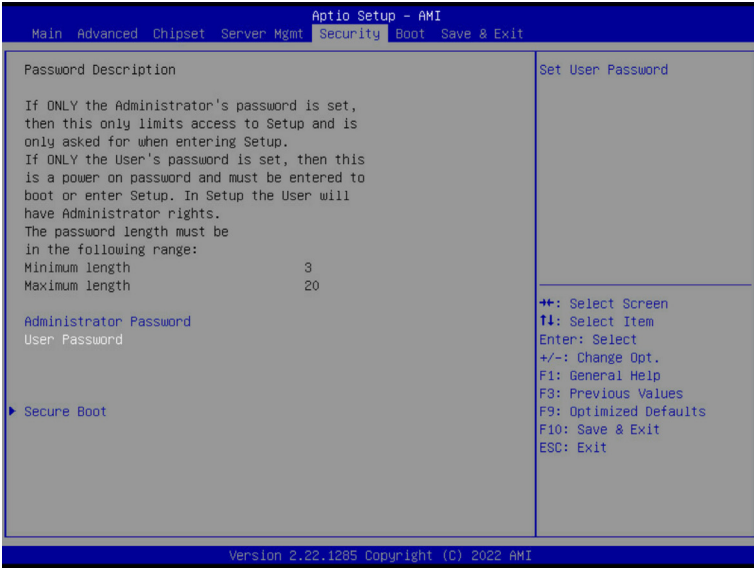
2-4-5 IPv6 BMC Network Configuration



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

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 Disabled .
Secure Boot Mode ^(Note)	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before 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 Custom .
Restore Factory Keys	Forces the system to user mode and installs factory default Secure Boot key database.
Reset To Setup Mode	Reset the system to Setup Mode.

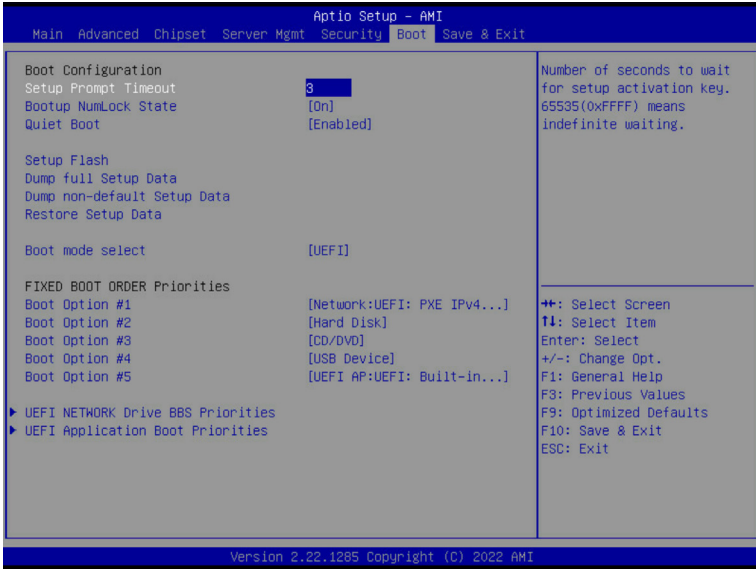
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235">Please note that this item is configurable when Secure Boot Mode is set to Custom.</p> <ul style="list-style-type: none"> <li data-bbox="335 243 941 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 941 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode. <li data-bbox="367 326 904 352">– Options available: Enabled, Disabled. Default setting is Disabled. <li data-bbox="335 357 925 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 925 404">– Installs all factory default keys. It will force the system in User Mode. <li data-bbox="367 409 606 431">– Options available: Yes, No. <li data-bbox="335 435 654 517">◆ Reset To Setup Mode <ul style="list-style-type: none"> <li data-bbox="367 459 654 482">– Reset the system to Setup Mode. <li data-bbox="367 487 606 517">– Options available: Yes, No. <li data-bbox="335 522 899 603">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 545 899 603">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). <li data-bbox="335 608 936 682">◆ Export Secure Boot variables <ul style="list-style-type: none"> <li data-bbox="367 631 936 682">– Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device. <li data-bbox="335 686 893 744">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 710 893 744">– Displays the current status of the variables used for secure boot. <li data-bbox="335 749 803 854">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 773 803 796">– Displays the current status of the Platform Key (PK). <li data-bbox="367 801 675 824">– Press [Enter] to configure a new PK. <li data-bbox="367 829 601 854">– Options available: Update. <li data-bbox="335 859 941 995">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 882 941 906">– Displays the current status of the Key Exchange Key Database (KEK). <li data-bbox="367 911 904 964">– Press [Enter] to configure a new KEK or load additional KEK from storage devices. <li data-bbox="367 969 670 995">– Options available: Update, Append. <li data-bbox="335 1000 941 1136">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 1023 904 1047">– Displays the current status of the Authorized Signature Database. <li data-bbox="367 1052 941 1105">– Press [Enter] to configure a new DB or load additional DB from storage devices. <li data-bbox="367 1110 670 1136">– Options available: Update, Append. <li data-bbox="335 1141 899 1277">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1165 899 1188">– Displays the current status of the Forbidden Signature Database. <li data-bbox="367 1193 888 1246">– Press [Enter] to configure a new dbx or load additional dbx from storage devices. <li data-bbox="367 1251 670 1277">– Options available: Update, Append. <li data-bbox="335 1282 931 1411">◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li data-bbox="367 1306 931 1329">– Displays the current status of the Authorized TimeStamps Database. <li data-bbox="367 1334 904 1387">– Press [Enter] to configure a new DBT or load additional DBT from storage devices. <li data-bbox="367 1392 670 1411">– Options available: Update, Append.

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

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.

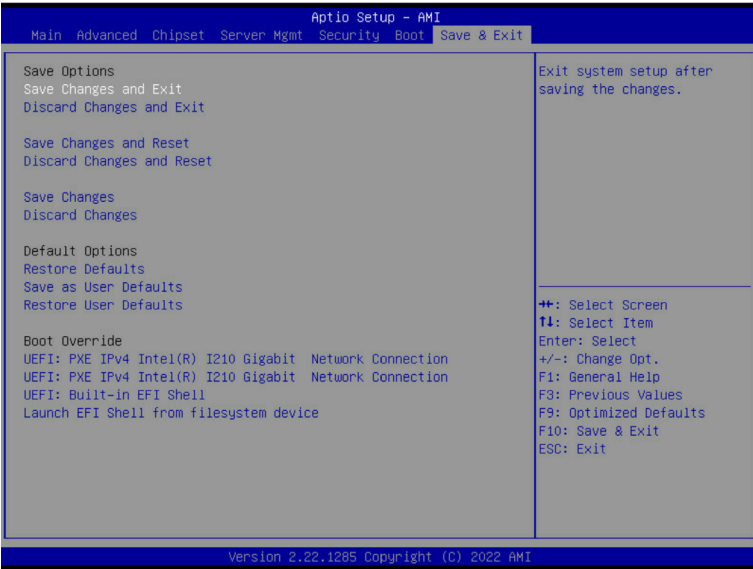


Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On, Off.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

Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	<p>Press [Enter] to configure the boot priority. By default, the server searches for boot devices in the following sequence:</p> <ol style="list-style-type: none"> 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
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 and Reset	Restarts the system after saving the changes made. Options available: Yes, No.
Discard Changes and Reset	Restarts the system without saving any changes. Options available: Yes, No.
Save Changes	Saves changes done so far to any of the setup options. Options available: Yes, No.
Discard Changes	Discards changes made and closes the BIOS setup. Options available: Yes, No.
Default Options	

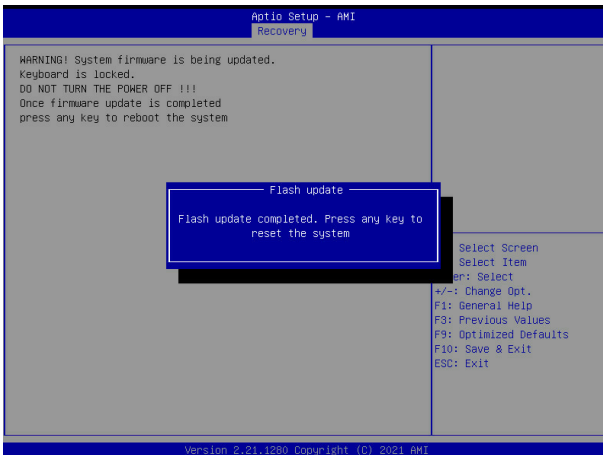
Parameter	Description
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly. Options available: Yes, No.
Save as User Defaults	Saves the changes made as the user default settings. Options available: Yes, No.
Restore User Defaults	Loads the user default settings for all BIOS setup parameters. 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 BIOS Recovery

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

Recovery Instruction:

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



2-9 BIOS POST Beep code (AMI standard)

2-9-1 PEI Beep Codes

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

2-9-2 DXE Beep Codes

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