GIGABYTE™

MS24-SU1

Motherboard
- Intel® Xeon® 6700/6500
- Series Processors R1S - CEB UP

User Manual

Rev. 1.0

Copyright

© 2026 Giga Computing TECHNOLOGY CO., LTD. All rights reserved.
The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

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

Documentation Classifications

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

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

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

For More Information

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

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

Table of Contents

Chapter 1 Hardware Installation 5

1-1 Installation Precautions 5

1-2 Product Specifications 6

1-3 Block Diagram 9

1-4 Motherboard Layout 10

1-5 Installing and Removing the CPU and Heat Sink 12

1-6 Installing and Removing Memory 13

1-6-1 8-Channel Memory Configuration 13

1-6-2 Installing and Removing the Memory Module 14

1-6-3 Processor and Memory Module Matrix Table 14

1-6-4 Memory Population Table 14

1-7 Installing the M.2 SSD Module 15

1-8 Back Panel Connectors 16

1-9 Internal Connectors 17

1-10 Jumper Settings 25

Chapter 5 BIOS Setup 26

5-1 The Main Menu 28

5-2 Advanced Menu 31

5-2-1 Trusted Computing 32

5-2-2 Serial Port Console Redirection 33

5-2-3 SIO Configuration 36

5-2-4 PCI Subsystem Settings 37

5-2-5 USB Configuration 40

5-2-6 Network Stack Configuration 41

5-2-7 Post Report Configuration 42

5-2-8 KMS Policy Configuration 43

5-2-9 NVMe Configuration 45

5-2-10 Chipset Configuration 46

5-2-11 Tls Auth Configuration 48

5-2-12 iSCSI Configuration 49

5-2-13 Intel(R) I210 Gigabit Network Connection 50

5-2-14 VLAN Configuration 52

5-2-15 MAC IPv6 Network Configuration 53

5-2-16 MAC IPv4 Network Configuration 54

5-2-17 Driver Health 55

5-3 Chipset Menu 56

5-3-1 Processor Configuration 57

5-3-2 Common RefCode Configuration 60
5-3-3 UPI Configuration 61
5-3-4 Memory Configuration 63
5-3-5 IIO Configuration 66
5-3-6 Advanced Power Management Configuration 68
5-3-7 Miscellaneous Configuration 71
5-3-8 Runtime Error Logging Settings 72
5-3-9 Power Policy 74
5-4 Server Management Menu 76
5-4-1 System Event Log 78
5-4-2 View FRU Information 79
5-4-3 BMC VLAN Configuration 80
5-4-4 BMC Network Configuration 81
5-4-5 IPv6 BMC Network Configuration 82
5-5 Security Menu 83
5-5-1 Secure Boot 84
5-6 Boot Menu 87
5-7 Save & Exit Menu 89
5-8 BIOS Recovery 91

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

NOTE:

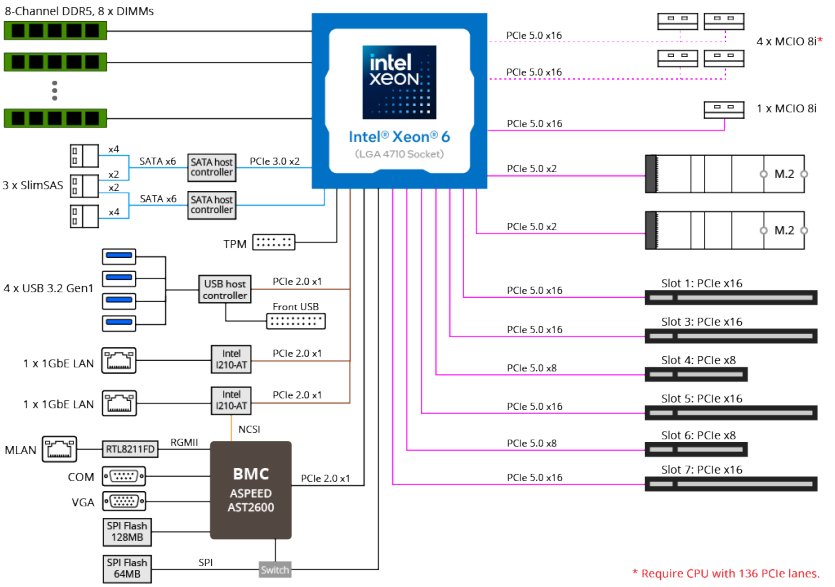
We reserve the right to make any changes to the product specifications and product-related information without prior notice.

Form Factor (WxD, mm)	◆ CEB ◆ 304.8 x 266.7
CPU	◆ Intel® Xeon® 6 Processors - Intel® Xeon® 6700-Series Processors - Intel® Xeon® 6500-Series Processors ◆ Single processor, TDP up to 350W
Socket	◆ 2 x LGA 4710 ◆ Socket E2
Chipset	◆ System on Chip
Memory	◆ 8 x DIMM slots [1] ◆ Support DDR5 RDIMM/MRDIMM [2] ◆ 8-Channel memory per processor ◆ RDIMM: Up to 6400 MT/s ◆ MRDIMM: Up to 8000 MT/s [1] MRDIMMs are only supported only on select Intel® Xeon® 6 Processors with P-cores.
LAN	◆ 2 x 1Gb/s LAN (2 x Intel® I210-AT) - Support NCSI function ◆ 1 x 10/100/1000 Mbps Management LAN
Video	◆ Integrated in ASPEED® AST2600 - 1 x VGA port
Audio	◆ N/A
Storage Interface	**MCIO:** ◆ 1 x MCIO 8i for 2 x Gen5 NVMe ◆ 4 x MCIO 8i for 8 x Gen5 NVMe [1] **SlimSAS:** ◆ 3 x SlimSAS 4i for 12 x SATA **M.2:** ◆ 1 x M.2 (2280/22110), PCIe Gen3 x4 ◆ 2 x M.2 (2280/22110), PCIe Gen5 x2 ◆ [1] Require CPU with 136 PCIe lanes.
RAID	◆ Onboard VROC key header

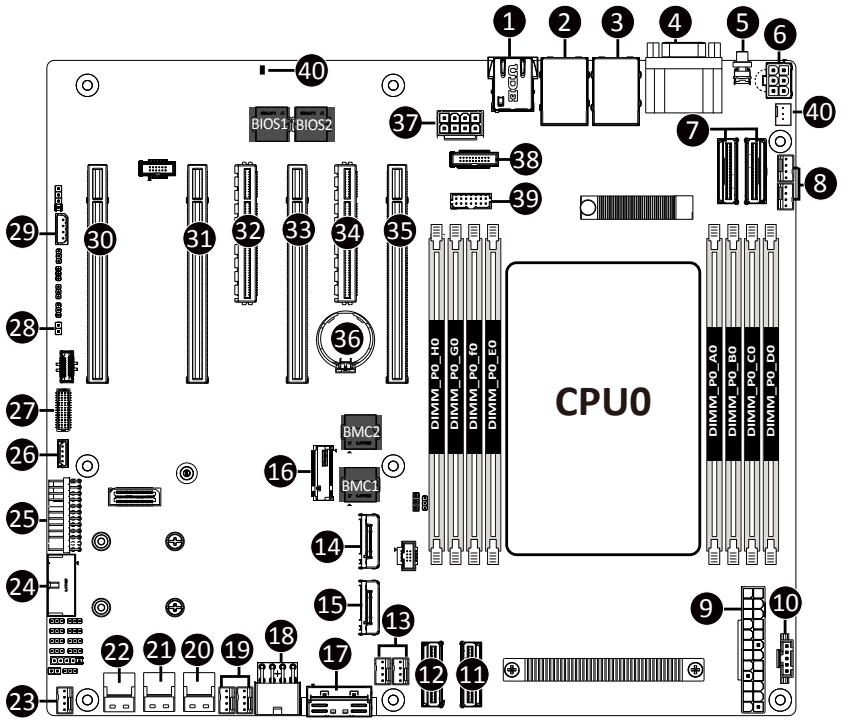
PCIe Expansion Slots	◆ Slot_7: PCIe x16 (Gen5 x16) ◆ Slot_6: PCIe x8 (Gen5 x8) [1] ◆ Slot_5: PCIe x16 (Gen5 x16) ◆ Slot_4: PCIe x8 (Gen5 x8)[1] ◆ Slot_3: PCIe x16 (Gen5 x16) ◆ Slot_1: PCIe x16 (Gen5 x16) ◆ ◆ 1 x MCIO 8i (Gen5 x8) ◆ 4 x MCIO 8i (Gen5 x8) [1] ◆ [1] Require CPU with 136 PCIe lanes.
Internal I/O	◆ 1 x 24-pin ATX main power connector ◆ 2 x 8-pin ATX 12V power connectors (for CPU) ◆ 1 x 6-pin ATX 12V power connector (for PCIe slot) ◆ 1 x 4-pin CPU fan header ◆ 1 x 3-pin CPU fan header ◆ 6 x System fan headers ◆ 1 x USB 3.2 Gen1 x2 header ◆ 2 x M.2 slots ◆ 5 x MCIO 8i connectors ◆ 3 x SlimSAS 4i connectors ◆ 1 x VROC connector ◆ 1 x NCSI connector ◆ 1 x Front panel header ◆ 1 x Backplane board header ◆ 1 x PMBus header ◆ 1 x IPMB header ◆ 1 x TPM header ◆ 1 x PRoT connector (**only enabled on RoT SKU**)
Rear I/O Connectors	◆ 4 x USB 3.2 Gen1 ports (Type-A) ◆ 1 x VGA port ◆ 1 x Serial port ◆ 2 x RJ45 ports ◆ 1 x MLAN port ◆ 1 x ID button with LED
Security Modules	◆ 1 x TPM header with SPI interface - **Optional** TPM2.0 kit: CTM010 ◆ 1 x PRoT connector (**only enabled on RoT SKU**)

Board Management	◆	ASPEED® AST2600 Baseboard Management Controller
	◆	GIGABYTE Management Console web interface
PSU Connectors	◆	1 x 24-pin ATX main power connector
	◆	2 x 8-pin ATX 12V power connectors (for CPU)
	◆	1 x 6-pin ATX 12V power connector (for PCIe slot)
Operating Properties	◆	Operating temperature: 10°C to 40°C
	◆	Operating humidity: 8-80% (non-condensing)
	◆	Non-operating temperature: -40°C to 60°C
	◆	Non-operating humidity: 20%-95% (non-condensing)

1-3 Block Diagram



1-4 Motherboard Layout



No.	Code	Description
1	MLAN	Sever Management LAN Port
2	USB3_LAN1	1GbE LAN Port #1(Top) / USB 3.2 Gen1 Type-A Ports(Bottom)
3	USB3_LAN2	1GbE LAN Port #2(Top) / USB 3.2 Gen1 Type-A Ports(Bottom)
4	COM1_VGA	Serial Port(Top) / VGA Port(Bottom)
5	SW_ID	ID Button with LED
6	P12V_AUX1	2x3 Pin 12V Power Connector
7	U2_P0_7CA/U2_P0_7GE	MCIO Connector (PCIe Gen5)
8	CPU0_FAN/SYS_FAN5	CPU Fan Connector / System Fan Connector #5
9	ATX	2x12 Pin Main Power Connector
10	PMBUS	PMBus Connector
11	U2_P0_9CA	MCIO Connector (PCIe Gen5)
12	U2_P0_9GE	MCIO Connector (PCIe Gen5)
13	SYS_FAN3/SYS_FAN4	System Fan Connector#3 / #4
14	M2_1	M.2 Slot (PCIe Gen5 x2, Support NGFF-2280/22110)
15	M2_0	M.2 Slot (PCIe Gen5 x2, Support NGFF-2280/22110)
16	PROT	PRot Module Connector
17	U1_P0_5GE	MCIO Connector (PCIe Gen5)
18	P12V_CPU1	2x4 Pin 12V Power Connector
19	SYS_FAN2/SYS_FAN1	System Connector #2 /#1
20	SL_SATA1	Slimline Connector #1
21	SL_SATA2	Slimline Connector #2
22	SL_SATA3	Slimline Connector #3
23	SYS_FAN6	System Connector #6
24	F_USB3_1	Front Panel USB 3.2 Gen1 Connector
25	FP_1	Front Panel Header
26	SW_RAID	VROC Module Connector
27	BP_1	HDD Backplane Board Connector
28	Case Open	Case Open Intrusion Alert Header
29	IPMB	IPMB Connector
30	PCIE_1	PCIe x16 Slot (Gen5 x16)
31	PCIE_3	PCIe x16 Slot (Gen5 x16)
32	PCIE_4	PCIe x16 Slot (Gen5 x8)
33	PCIE_5	PCIe x16 Slot (Gen5 x16)
34	PCIE_6	PCIe x16 Slot (Gen5 x8)
35	PCIE_7	PCIe x16 Slot (Gen5 x16)
36	BAT	Battery Socket
37	P12V_CPU2	2x4 Pin 12V Power Connector
38	CN_NCSI	NCSI Connector
39	SPI_TPM	TPM Connector
40	LED_BMC	BMC Firmware Readiness LED
41	FAN1_PWR	CPU Fan Power Connector

1-5 Installing and Removing the CPU and Heat Sink

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

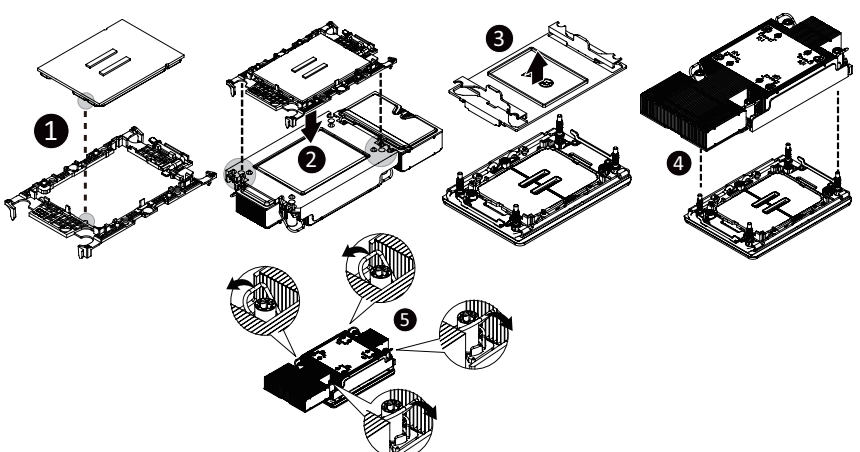
- Make sure that the motherboard supports the CPU.
- Always turn off the computer and unplug the power cord from the power outlet before installing the CPU to prevent hardware damage.
- Unplug all cables from the power outlets.
- Disconnect all telecommunication cables from their ports.
- Place the system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

WARNING!

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

Follow these instructions to install the CPU:

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



Note:

- When installing the heatsink to CPU, use T30-Lobe driver to tighten 4 captive nuts in sequence as 1-4.
- Please refer to the Heatsink Label for the screw tightening torque value.
- The illustrations of the heat-sink installation shown are for reference only.

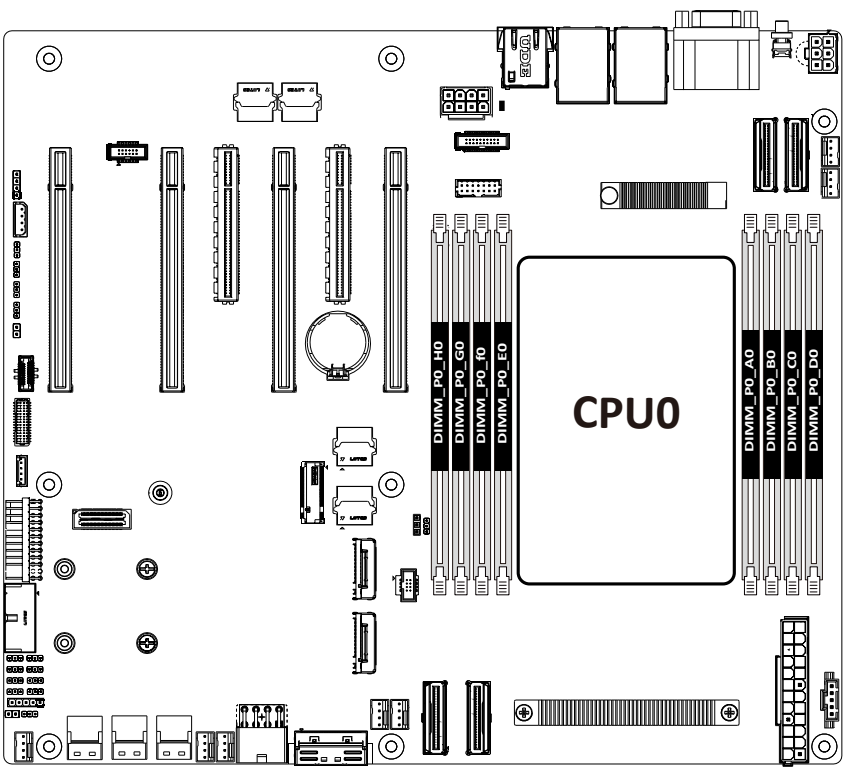
1-6 Installing and Removing Memory

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.

1-6-1 8-Channel Memory Configuration

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

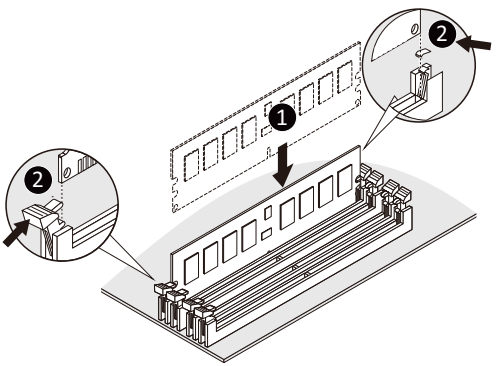


1-6-2 Installing and Removing the Memory Module

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

Follow these instructions to install a DIMM module:

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



1-6-3 Processor and Memory Module Matrix Table

Memory Q'ty for each CPU	CPU0							
	H0	G0	F0	E0	A0	B0	C0	D0
1 DIMM					V			
4 DIMM		V		V	V		V	
	V		V			V		V
8 DIMM	V	V	V	V	V	V	V	V

1-6-4 Memory Population Table

For detailed memory population guidelines, click the link below to view the Memory Population Table.

Note:
When only one DIMM per channel is used, it must be populated in memory slot DIMM1.

1-7 Installing the M.2 SSD Module

WARNING

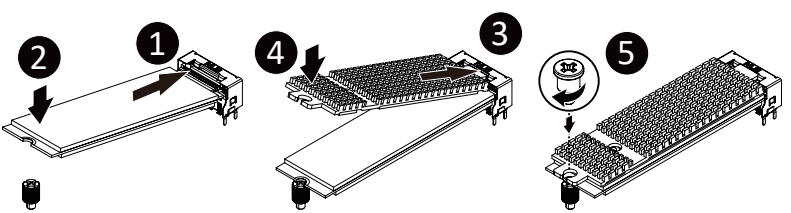
Installation of the thermal pad over the M.2 device is required when installing an M.2 device. Lack of the thermal pad may result in the system overheating and throttle the system performance.

CAUTION

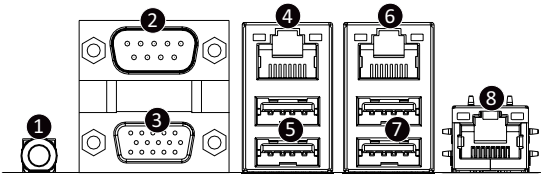
The position of the stand-off screw will depend on the size of the M.2 device. The stand-off screw is pre-installed for 22110 cards as standard. Refer to the size of the M.2 device and change the position of the stand-off screw accordingly.

Follow these instructions to install the M.2 device and heat sink:

1. Insert the M.2 device into the M.2 connector.
2. Press down on the M.2 device.
3. Install the thermal pad of the M.2 device to the M.2 device.
4. Press down on the thermal pad.
5. Secure the M.2 device and its thermal pad to the motherboard with a single screw.
6. Reverse steps 1-5 to remove the M.2 device.



1-8 Back Panel Connectors



❶ ID button with LED

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

❷ Serial Port

Connect to serial-based mouse or data processing devices.

❸ VGA Port

Connect to a monitor device.

❹ 1 GbE 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.

❺❼ USB 3.2 Gen1 Ports

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

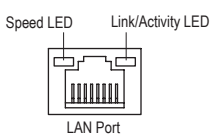
❻ 1 GbE LAN Port #2

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.

❽ 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.

LAN and ID Button LEDs



ID button/LED:

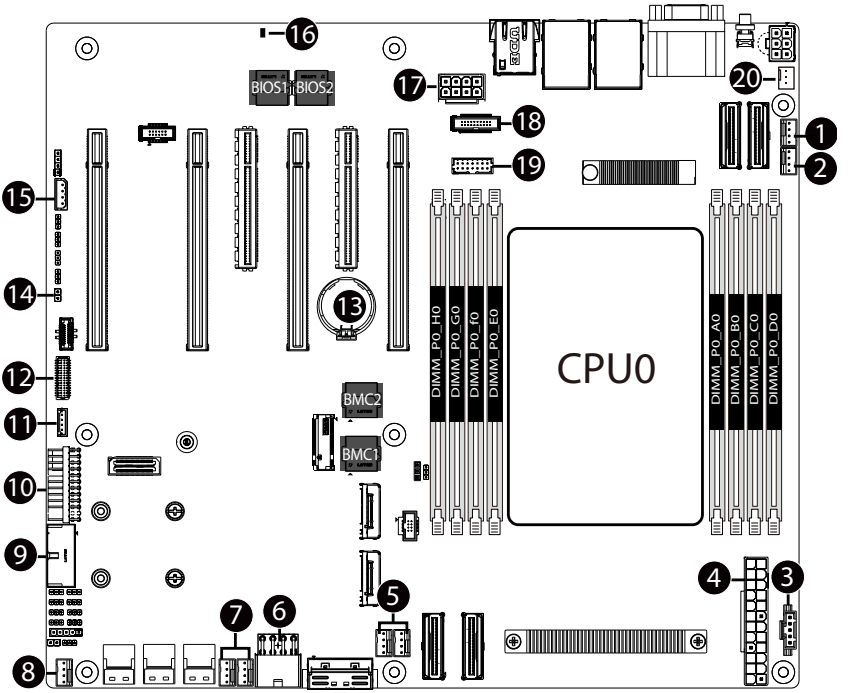
State	Description
Blue On	System identification is active
Off	System identification is disabled

10/100/1000 LAN LED:

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

- 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.

1-9 Internal Connectors



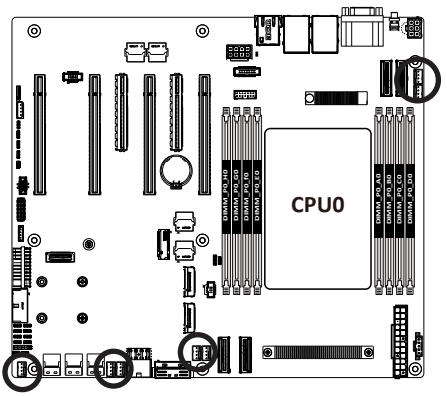
1)	CPU0_FAN	11)	SW_RAID
2)	SYS_FAN5	12)	BP_1
3)	PMBUS	13)	BAT
4)	ATX	14)	CASE_OPEN
5)	SYS_FAN3/SYS_FAN4	15)	IPMB
6)	P12V_CPU1	16)	LED_BMC
7)	SYS_FAN2/SYS_FAN1	17)	P12V_CPU2
8)	SYS_FAN6	18)	CN_NCSI
9)	F_USB3_1	19)	SPI_TPM
10)	FP_1	20)	FAN_PWR

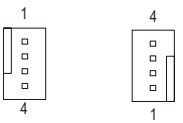
Read the following guidelines before connecting external devices:

- 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.

1/2/5/7/8) CPU0_FAN/SYS_FAN5/SYS_FAN3//SYS_FAN4/SYS_FAN2/SYS_FAN1/SYS_FAN6 (FAN Headers)

The motherboard has one 4-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.



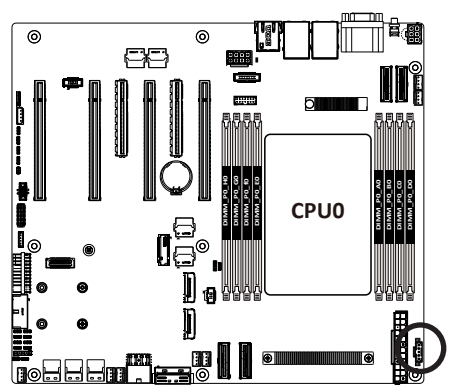


Pin No.	Definition
1	GND
2	+12V
3	Sense
4	Speed Control

- 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.

3) PMBus Connector

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



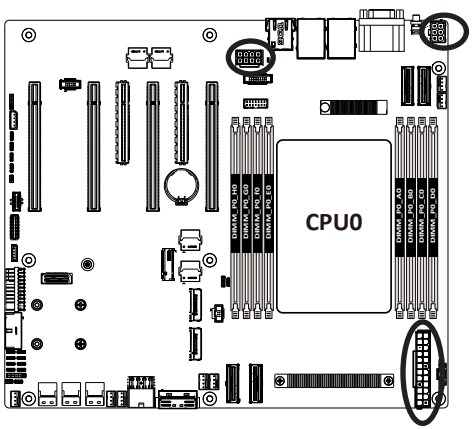
Pin No.	Definition
1	PMBus Clock
2	PMBus Data
3	PMBus Alert
4	GND
5	3.3V Sense

4/6/18/20) ATX/P12V_CPU2/P12V_CPU1/P12V_AUX1

(2x12 Main Power Connector, 2x4 12V Power Connector and 2x3 12V Power Connector)

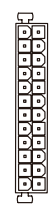
With the use of the power connector, the power supply can supply enough stable power to all the components on the motherboard. Before connecting the power connector, first make sure the power supply is turned off and all devices are properly installed. The power connector possesses a foolproof design.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

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



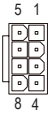
P12V_AUX1/P12V_CPU1

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



ATX

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

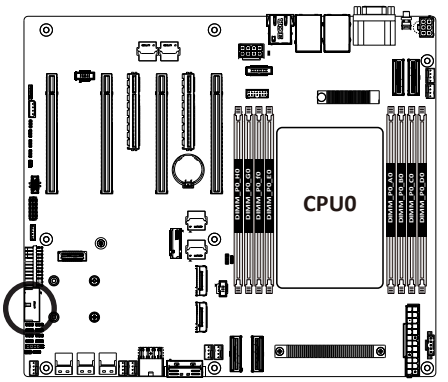


P12V_CPU2

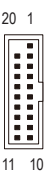
Pin No.	Definition
1	GND
2	GND
3	GND
4	GND
5	+12V
6	+12V
7	+12V
8	+12V

9) F_USB3_1 (USB 3.2 Gen1 Connector)

The connector/header conform to USB 2.0/ 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.



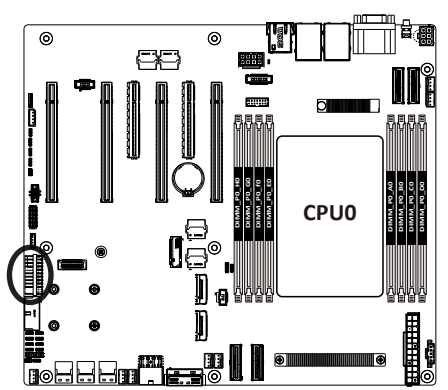
USB 3.0 Connector



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

10) FP_1 (Front Panel Header)

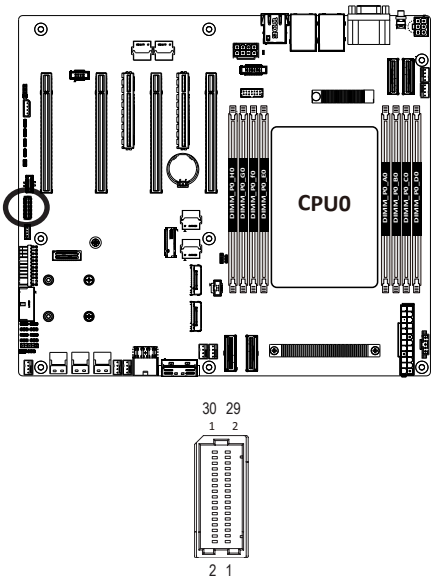
Connect the power switch, reset switch, speaker, chassis intrusion switch/sensor and system status indicator on the chassis to this header according to the pin assignments below. Note the positive and negative pins before connecting the cables.



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 Actve LED+
23	NMI Switch	24	LAN2 Link LED-
*Note: Pin 7 & Pin 9 are reserved for Gigabyte systems.			

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.

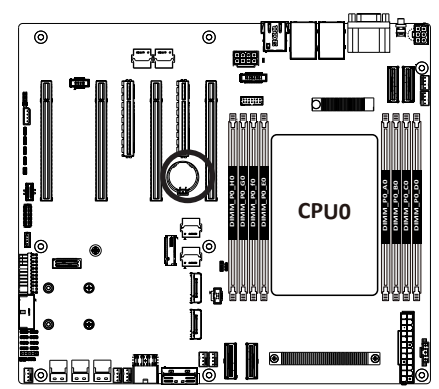
12) BP_1 (HDD Backplane Board Header)

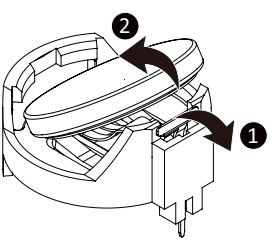


Pin No.	Definition	Pin No.	Definition
1	HP_ALERT_L	2	BPMI DIN/OUT
3	GND	4	BPMI DIN/IN
5	BPMI_LOAD	6	GND
7	BPMI_CLK	8	PLD_Program_EN
9	GLED_AMB_N	10	GLED_GRN_N
11	FAN_IRQ_N	12	Reserved
13	BP_SCL	14	GND
15	BP_SDA	16	BP_RST_N
17	SMB_U2_TMP_SCL	18	GND
19	SMB_U2_TMP_SDA	20	I2C_DEV_RST
21	PH_HP_SCL0	22	GND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

13) BAT (Battery Socket)

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

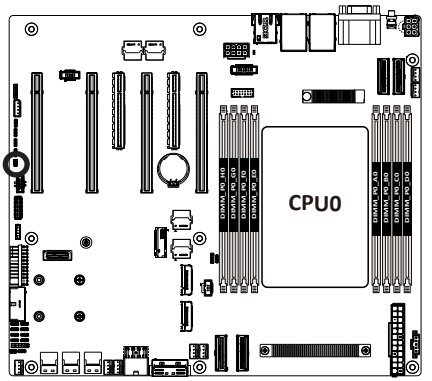




- Always turn off your computer and unplug the power cord before replacing the battery.
- Replace the battery with an equivalent one. Danger of explosion if the battery is replaced with an incorrect model.
- Contact the place of purchase or local dealer if you are not able to replace the battery by yourself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

14) 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.

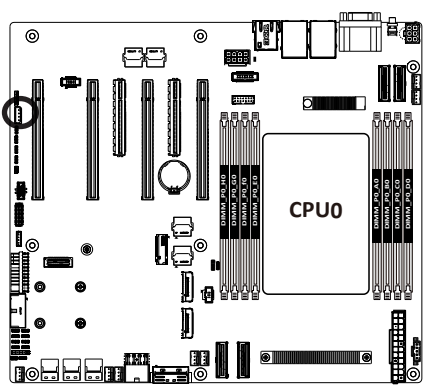


Open: Normal Operation (Default)

Closed: Active Chassis Intrusion Alert

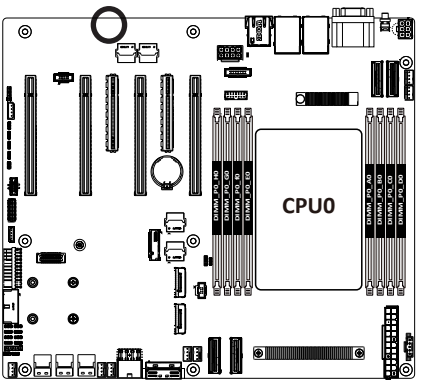
15) IPMB (Intelligent Platform Management Bus) Connector

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.



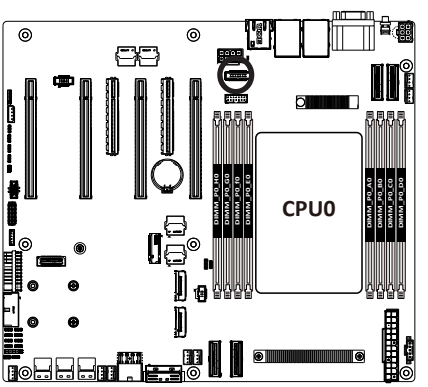
Pin No.	Definition
1	Clock
2	GND
3	Data
4	VCC

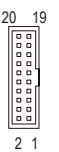
16) LED_BMC (BMC Firmware Readiness LED)



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

18) CN_NCSI (NCSI Connector)

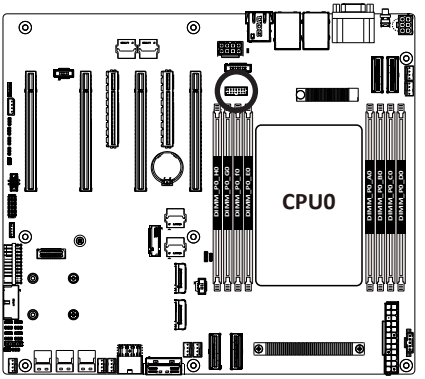


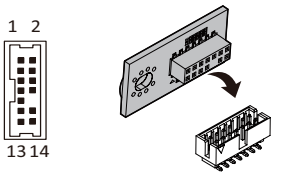


Pin No.	Definition	Pin No.	Definition
1	NCSI_CLK	2	GND
3	NCSI_RX_D0	4	GND
5	NCSI_RX_D1	6	GND
7	NCSI_CRS_DV	8	GND
9	NCSI_RX_ER	10	GND
11	P3V3_AUX	12	GND
13	NCSI_TX_D1	14	GND
15	NCSI_TX_D0	16	GND
17	NCSI_TX_EN	18	GND
19	NCSI_PRESENT	20	P3V3_AUX

19) SPI_TPM (Trusted Platform Module Connector)

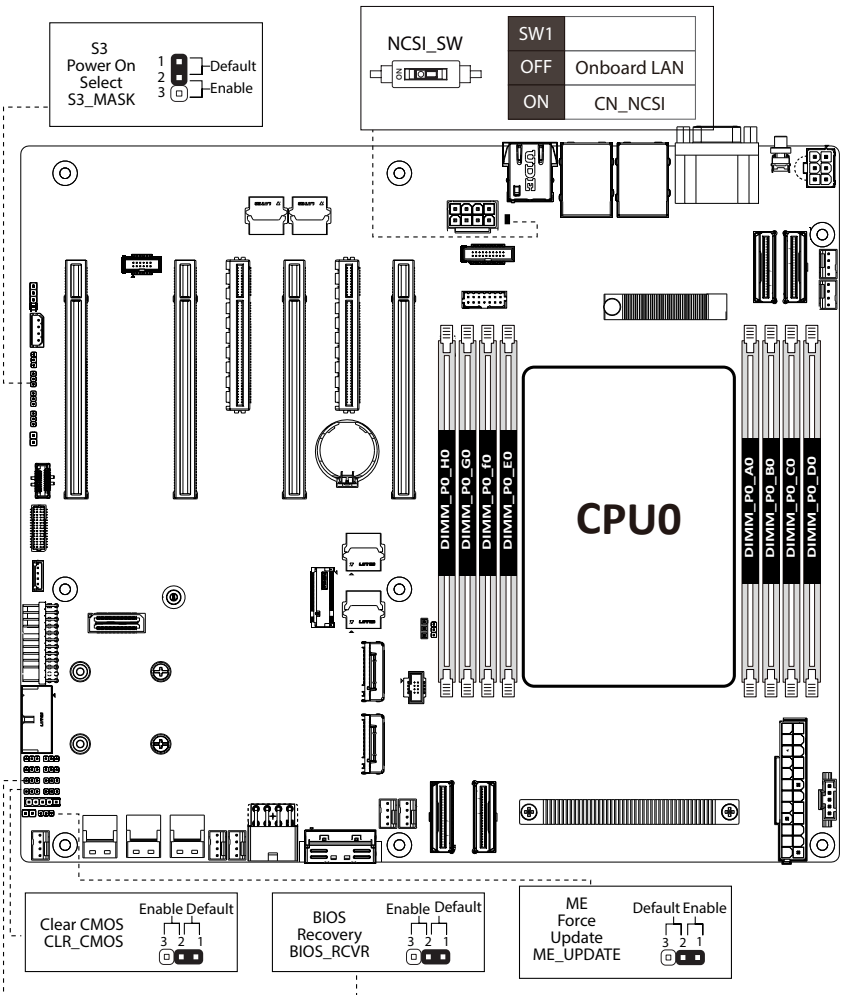
Trusted Platform Module (TPM) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.





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

1-10 Jumper Settings



Chapter 5 BIOS Setup

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

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

- BIOS flashing is potentially risky, if you do not encounter any problems when using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 4 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

<←><→>	Move the selection bar to select the screen
<↑><↓>	Move the selection bar to select an item
<+>	Increase the numeric value or make changes
<->	Decrease the numeric value or make changes
<Enter>	Execute command or enter the submenu
<Esc>	Main Menu: Exit the BIOS Setup program 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.)
  NOTE! BIOS setting changes require a system reboot to take effect.

5-1 The Main Menu

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

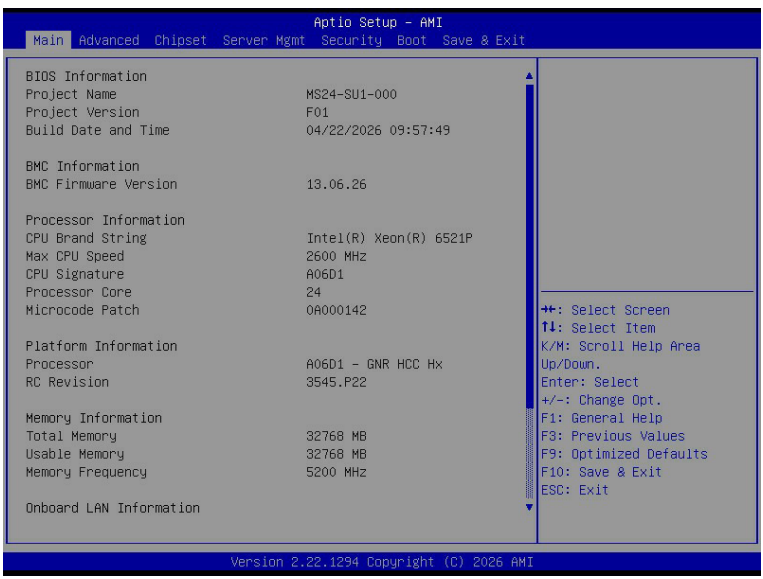
Main Menu Help

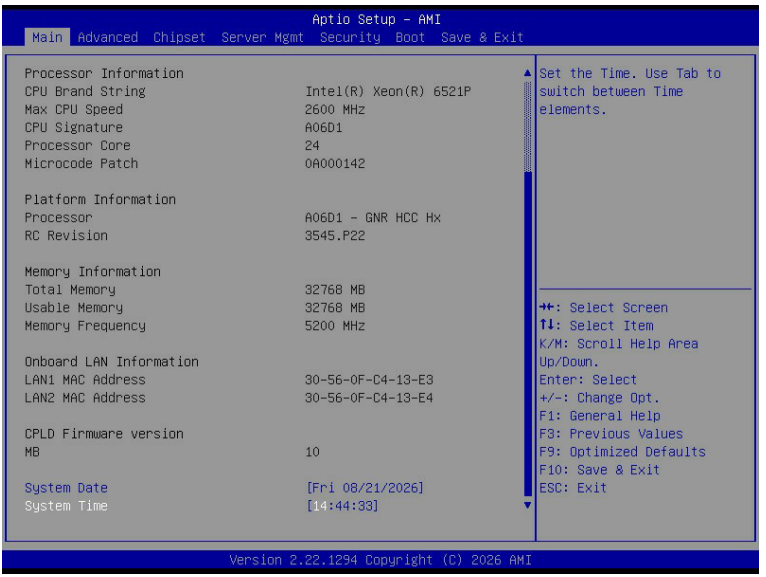
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

Submenu Help

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

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





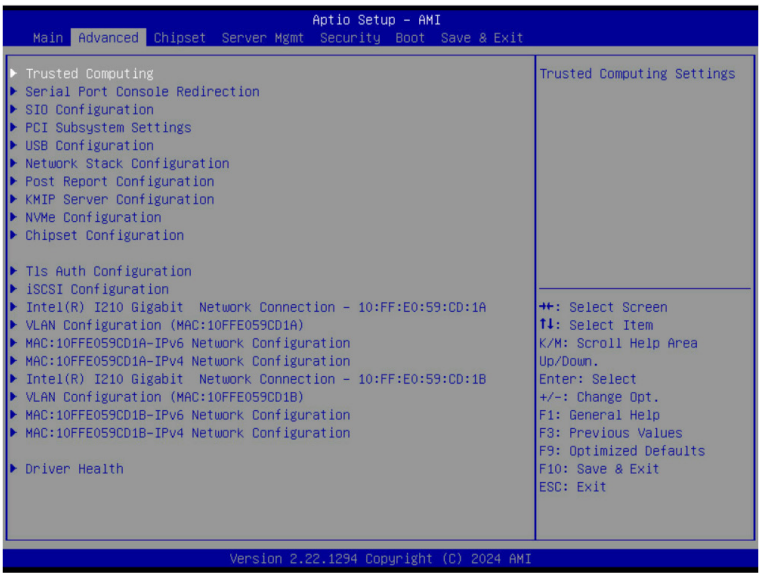
Parameter	Description
Project Name	Displays the project name information.
Project Version	Displays version number of the BIOS setup utility.
Build Date and Time	Displays the date and time when the BIOS setup utility was created.
BMC Information	
BMC Firmware Version	Displays BMC firmware version information.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

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

Parameter	Description
CPLD Firmware version	
MB/location	Displays CPLD firmware version 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.

5-2 Advanced Menu

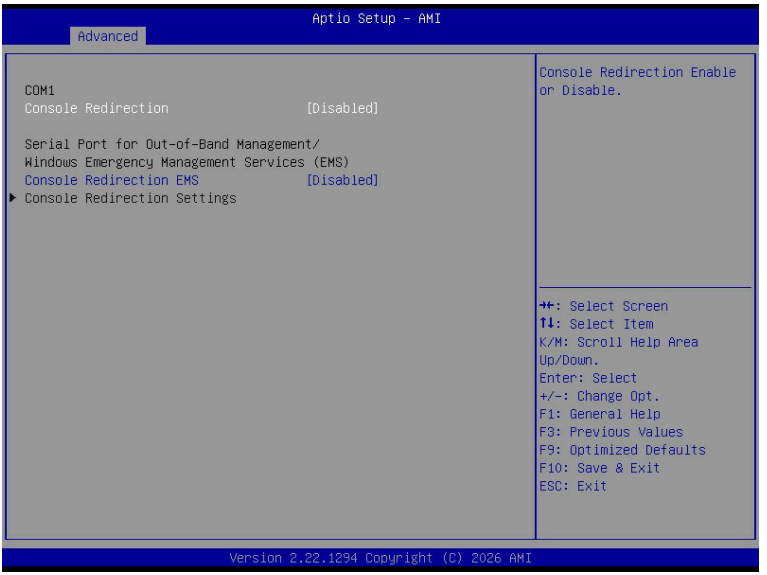
The Advanced Menu displays submenu options for configuring the function of various hardware components. Select a submenu item, then press <Enter> to access the related submenu screen.



5-2-1 Trusted Computing

Parameter	Description
Configuration	
TPM v1.2 Support	Enable/Disable BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available. Options available: Disabled, **Enabled**.

5-2-2 Serial Port Console Redirection



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

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

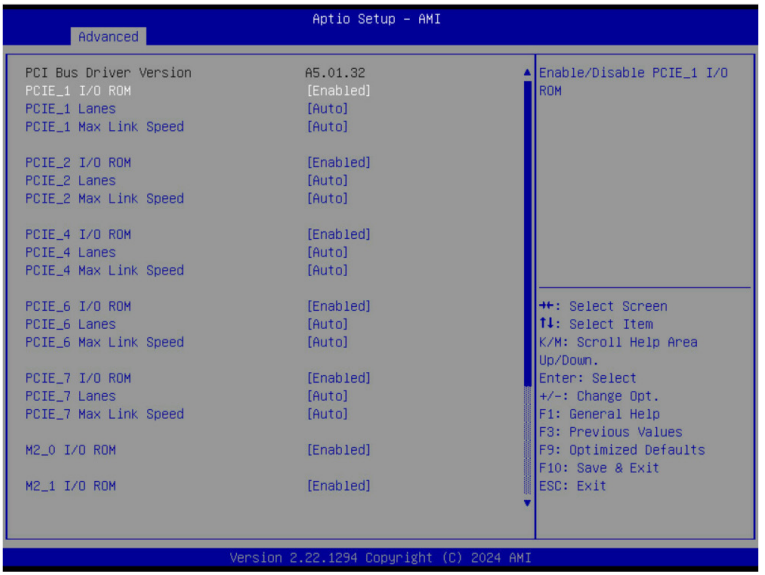
Parameter	Description
COM1 Console Redirection Settings (continued)	◆ Parity – A parity bit can be sent with the data bits to detect some transmission errors. – Even: parity bit is 0 if the num of 1's in the data bits is even. – Odd: parity bit is 0 if num of 1's in the data bits is odd. – Mark: parity 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. ◆ Stop Bits – 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. ◆ Flow Control – 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. ◆ VT-UTF8 Combo Key Support – Enable/Disable the VT-UTF8 Combo Key Support. – Options available: **Enabled**, Disabled. ◆ Recorder Mode – When this mode enabled, only texts will be send. This is to capture Terminal data. – Options available: Enabled, **Disabled**. ◆ Resolution 100x31 – Enable/Disable extended terminal resolution. – Options available: **Enabled**, Disabled. ◆ Putty KeyPad – Selects Function Key and KeyPad on Putty. – Options available: **VT100**, LINUX, XTERMR6, SC0, ESCN, VT400.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection(Note)	EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management. Options available: Enabled, **Disabled**.

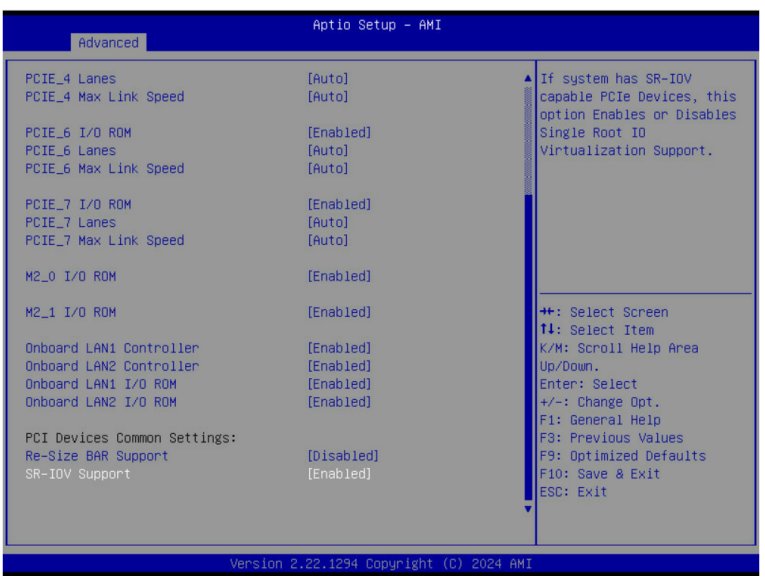
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.** ◆ Out-of-Band Mgmt Port – Microsoft Windows Emergency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Default setting is **COM1**. ◆ Terminal Type EMS – Selects a terminal type to be used for console redirection. – Options available: VT100, **VT100PLUS**, VT-UTF8, ANSI. ◆ Bits per second EMS – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 57600, **115200**. ◆ Flow Control EMS – 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.

5-2-3 SIO Configuration

Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	
[*Active*] Serial Port	Press [Enter] to configure advanced items. ◆ Use This Device – 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. ◆ Logical Device Settings/Current: – Displays the serial port base I/O address and IRQ. ◆ Possible: – Configures the serial port base I/O address and IRQ. **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;

5-2-4 PCI Subsystem Settings



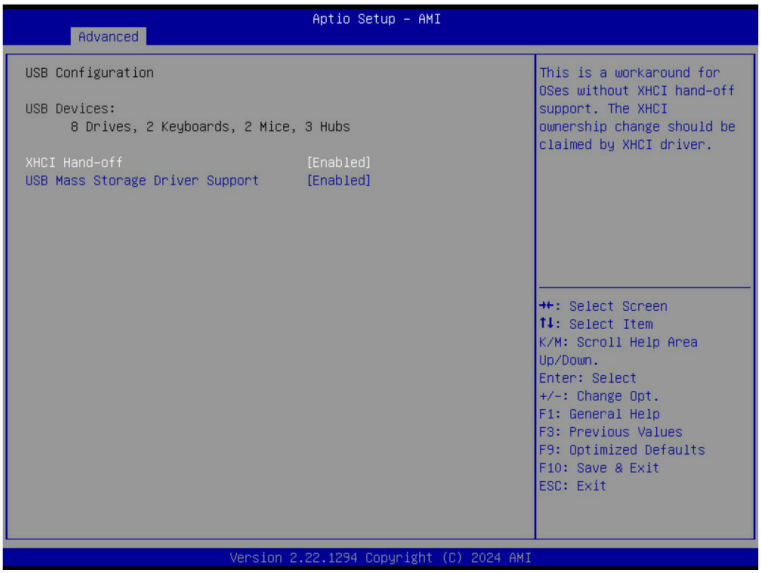


Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
SLOT_# I/O ROM(Note1)	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: **Enabled**, Disabled.
SLOT_# Data Link Feature Exchange function(Note1)	Enable/Disable SLOT Data Link Feature Exchange function. Options available: Disabled, Enabled, **Auto**.
SLOT_# PXE Boot(Note1)	Options available: Disabled, **Enabled**.
SLOT_# Lanes(Note1)	Change the PCIe lanes. Default setting is **Auto**.
SLOT_#_Max Link Speed(Note1)	Configure PCIe max link speed. Options available: **Auto**, Gen1, Gen2, Gen3, Gen4, Gen5.
M2A/B I/O ROM(Note2)	Enable/Disable M2 I/O ROM. Options available: **Enabled**, Disabled.
M2A/B Data Link Feature Exchange function(Note2)	Enable/Disable M2 Data Link Feature Exchange function. Options available: Disabled, Enabled, **Auto**.
M2A/B PXE Boot(Note2)	Options available: Disabled, **Enabled**.
M2A/B Lanes(Note2)	Change the M2 PCIe lanes. Default setting is **Auto**.
M2A/B Max Link Speed(Note2)	Configure M2 PCIe max link speed. Options available: **Auto**, Gen1, Gen2, Gen3, Gen4, Gen5.
LAN I/O ROM(Note3)	Enable/Disable the LAN devices, and initializes device expansion ROM. Options available: **Enabled**, Disabled.
LAN Data Link Feature Exchange function(Note3)	Enable/Disable LAN Data Link Feature Exchange function. Options available: Disabled, Enabled, **Auto**.
LAN PXE Boot(Note3)	Options available: Disabled, **Enabled**.
LAN_Max Link Speed(Note3)	Configure LAN PCIe max link speed. Options available: **Auto**, Gen1, Gen2, Gen3, Gen4, Gen5.
M2C I/O ROM	Enable/Disable M2C I/O ROM. Options available: **Enabled**, Disabled.
M2C Data Link Feature Exchange function	Enable/Disable M2C Data Link Feature Exchange function. Options available: Disabled, Enabled, **Auto**.
M2C PXE Boot	Options available: Disabled, **Enabled**.
M2C Max Link Speed	Configure M2C PCIe max link speed. Options available: **Auto**, Gen1, Gen2, Gen3, Gen4, Gen5.

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

Parameter	Description
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable 64 bit capable Devices to be Decoded in Above 4G Address Space (Only if system supports 64 bit PCI decoding). Options available: **Enabled**, Disabled.
Re-Size BAR Support	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support. Options available: Enabled, **Disabled**.
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.

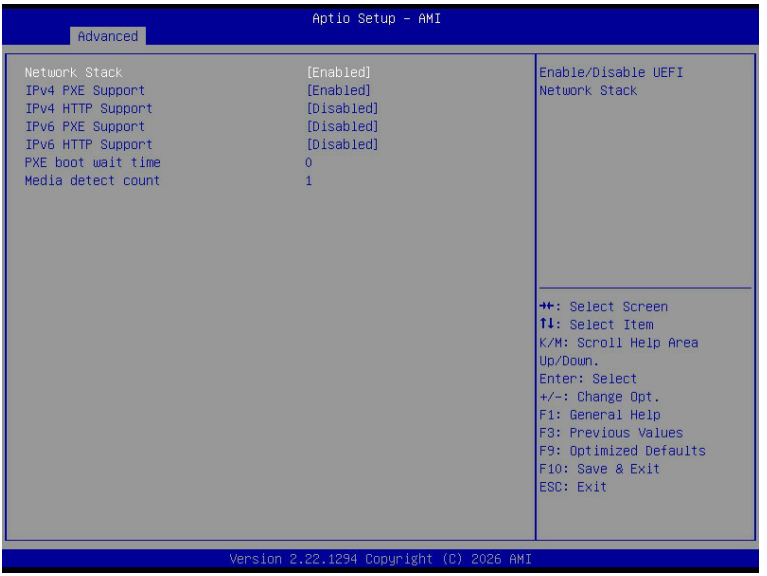
5-2-5 USB Configuration



Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: **Enabled**, Disabled.
USB Mass Storage Driver Support(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: **Enabled**, Disabled.

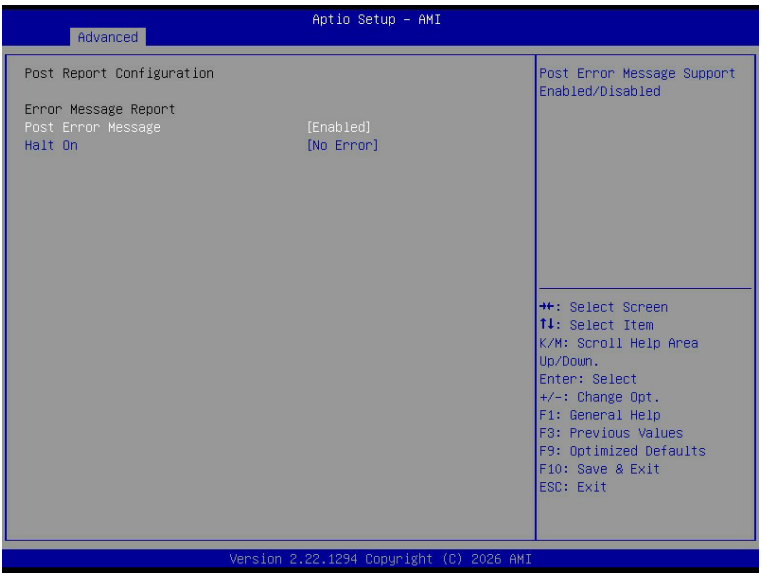
(Note) This item is present only if you attach USB devices.

5-2-6 Network Stack Configuration



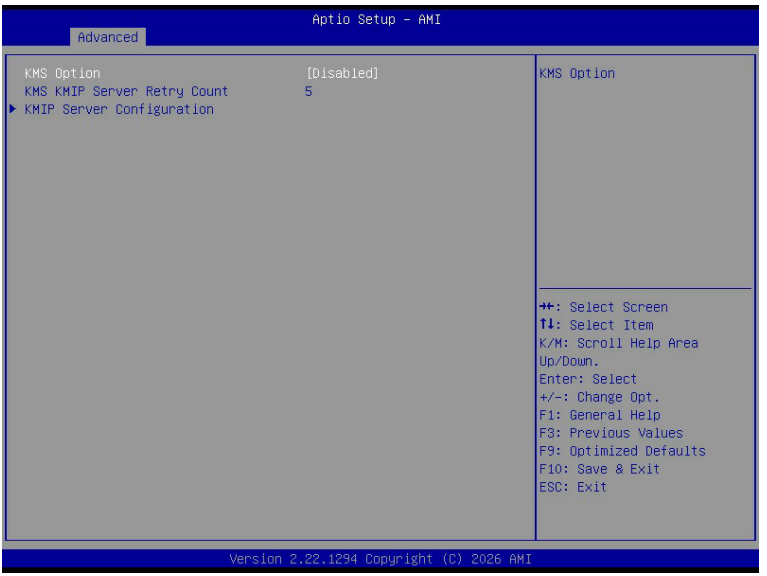
Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: **Enabled**, Disabled.
Ipv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: **Enabled**, Disabled.
Ipv4 HTTP Support	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled, **Disabled**.
Ipv6 PXE Support	Enable/Disable the Ipv6 PXE feature. Options available: Enabled, **Disabled**.
Ipv6 HTTP Support	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled, **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.

5-2-7 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.
Halt On	Options available: **No Error**, All Error.

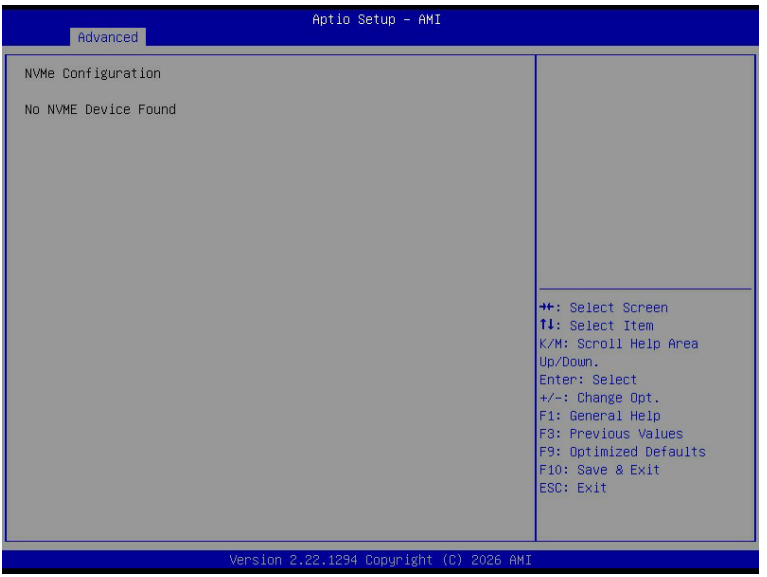
5-2-8 KMS Policy Configuration



Parameter	Description
KMS Option	Options available: **Disabled**, KMS with KMIP.
KMS KMIP Server Retry Count	Define KMS KMIP Server Retry Count.
KMIP Server Configuration	Press [Enter] to configure advanced items. ◆ KMIP Server IP address – Enter IP4 address in dotted-decimal notation. ◆ KMIP TCP Port number – Enter KMIP TCP Port number 100...9999. – Default setting is **5696**. ◆ Time Zone – Enter the correct time zone for this server. – Default setting is **GMT+8**. ◆ Client Credentials – Use User and password credentials to authenticate the client. – Options available: Disabled, **Enabled**. ◆ Client UserName – Enter Client identity: UserName. – Name Length: 0-63 characters. ◆ Client Password – Enter Client identity: Password. – Password Length: 0-31 characters.

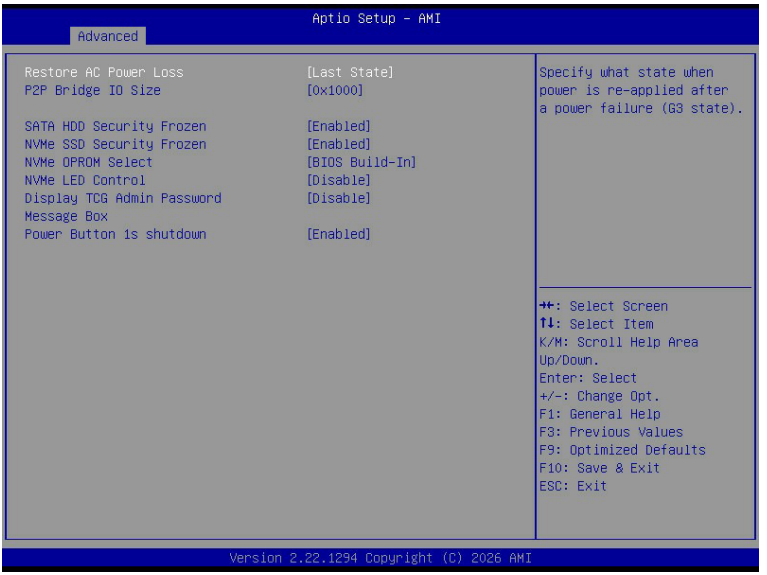
Parameter	Description
KMIP Server Configuration (continued)	◆ KMS TLS Certificate / Size – CA Certificate/ Client Private Key/ Client Certificate. » Enroll factory defaults or load the KMS TLS certificates from the file.

5-2-9 NVMe Configuration



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

5-2-10 Chipset Configuration

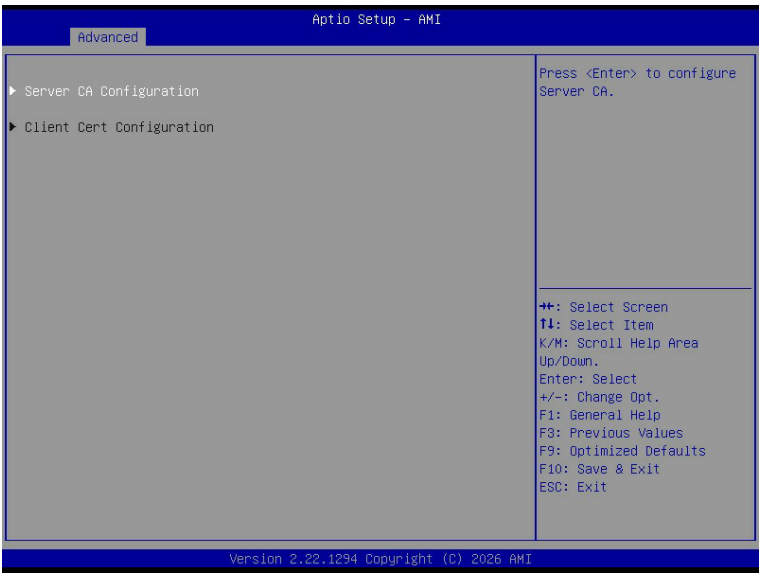


Parameter	Description
Restore on AC Power Loss(Note)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
P2P Bridge IO Size	Specifies P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, **0x1000**.
SATA HDD Security Frozen	Enable/Disable this item to send freeze lock command to SATA HDD. Options available: **Enabled**, Disabled.
NVMe SSD Security Frozen	Attempt to send freeze lock command to NVMe SSDs during boot. Options available: **Enabled**, Disabled.
NVMe OPROM Select	BIOS Build-In is default setting. Select Device Itself, then this NVMe page will not display any device. Unless the device doesn't have OPROM. Options available: **BIOS Build-In**, NVMe Device, Disables.
NVMe LED Control	Enable/Disable allow user control NVMe LED. It only available the NVMe device direct connect to CPU. Default setting is **Disable**.

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

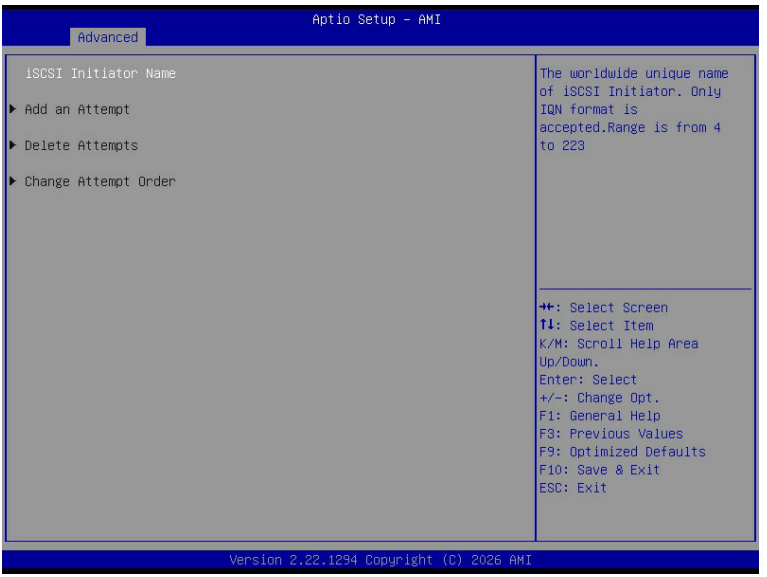
Parameter	Description
Display TCG Admin Password Message Box	Enable/Disable allow user control TCG Admin Password Message Box display at POST or not. Options available: **Disable**, Enable.
Power Button is shutdown	Enable/Disable Press power button 1 sec shutdown before entering OS. Options available: Disabled, **Enabled**.

5-2-11 Tls Auth Configuration



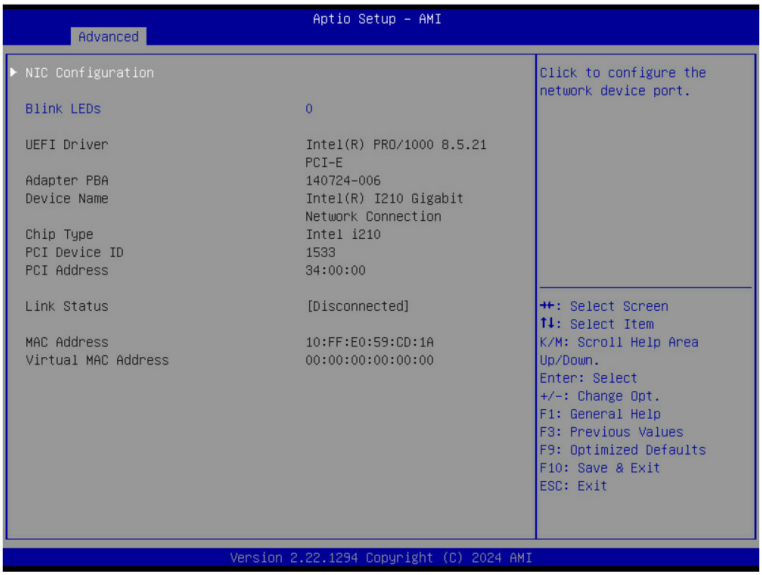
Parameter	Description
Server CA Configuration	Press [Enter] for configuration of advanced items. ◆ Enroll Cert – Press [Enter] to enroll a certificate • Enroll Cert Using File • Cert GUID Input digit character in 1111111-2222-3333-4444-1234567890ab format. – Commit Changes and Exit – Discard Changes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

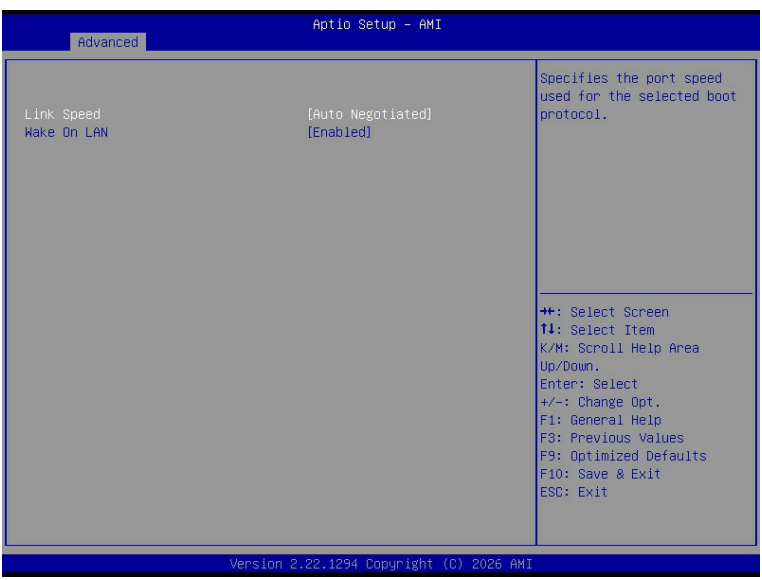
5-2-12 iSCSI Configuration



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

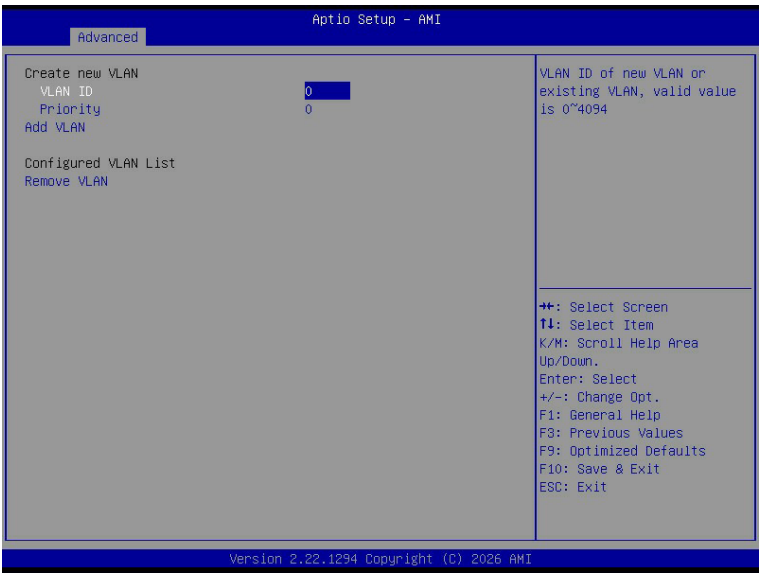
5-2-13 Intel(R) I210 Gigabit Network Connection





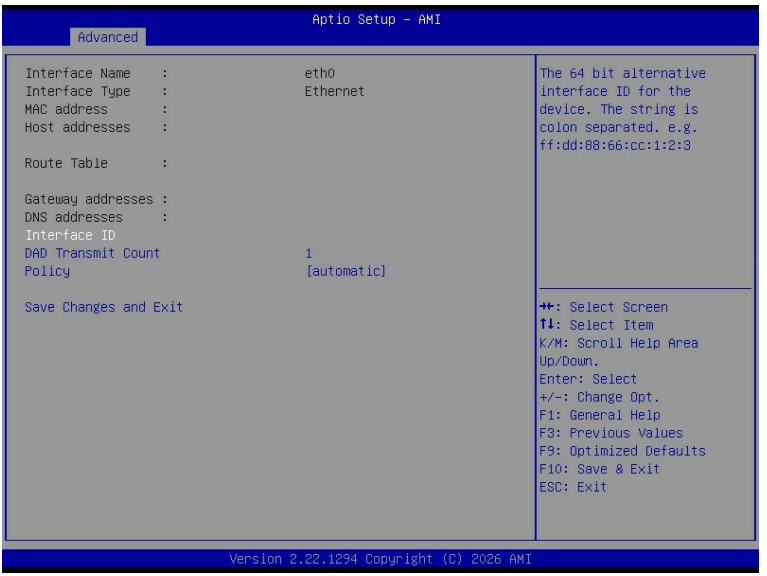
Parameter	Description
NIC Configuration	Press [Enter] to configure advanced items. ◆ Link Speed – Allows for automatic link speed adjustment. – Options available: **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. ◆ Wake On LAN – Enables power on of the system via LAN. Note 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.
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values (up to 15 seconds).
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

5-2-14 VLAN Configuration



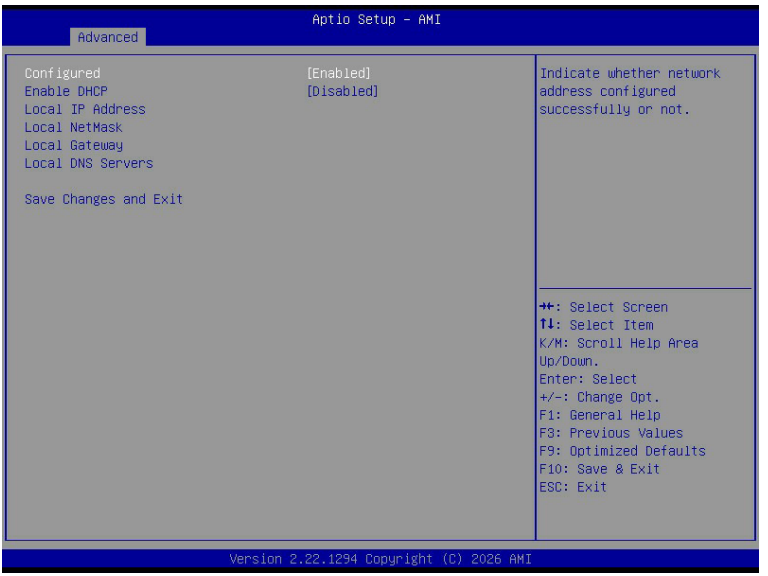
Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Create new VLAN ◆ VLAN ID – Sets VLAN ID for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the desired values. – The valid range is from 0 to 4094. ◆ Priority – Sets 802.1Q 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 – Press [Enter] to create a new VLAN or update an existing VLAN. ◆ Configured VLAN List ◆ Remove VLAN – Press [Enter] to remove an existing VLAN.

5-2-15 MAC IPv6 Network Configuration



Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Displays the MAC Address information. ◆ Interface ID – 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 – 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 – Options available: **automatic**, manual. ◆ Save Changes and Exit – Press [Enter] to save all configurations.

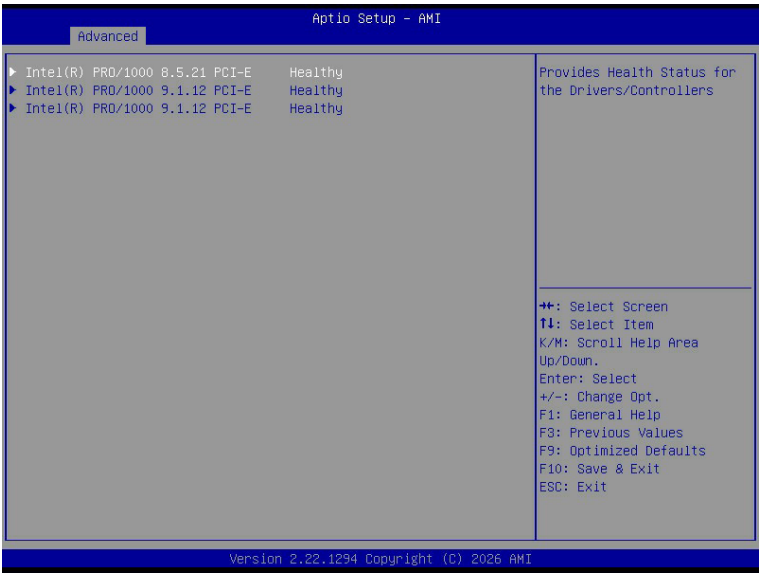
5-2-16 MAC IPv4 Network Configuration



Parameter	Description
Configured	Indicates whether network address is configured successfully or not. Options available: Enabled, **Disabled.**
Enable DHCP(Note)	Options available: Enabled, **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**.

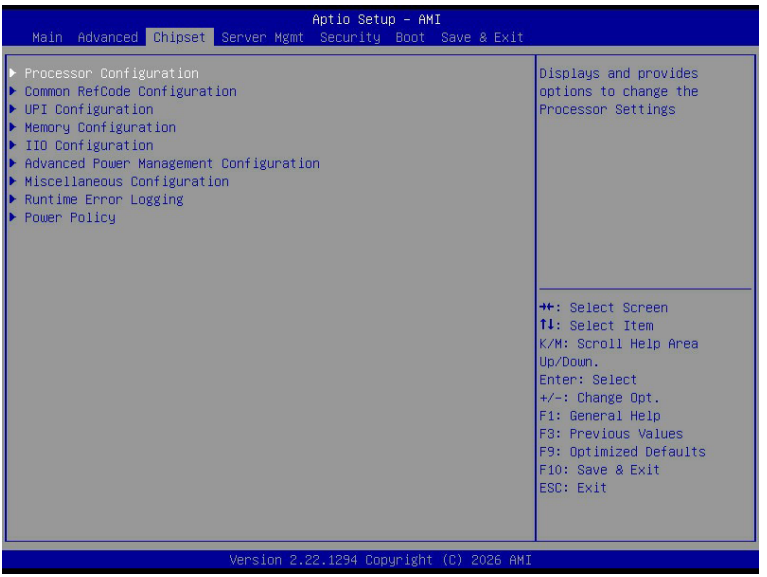
5-2-17 Driver Health



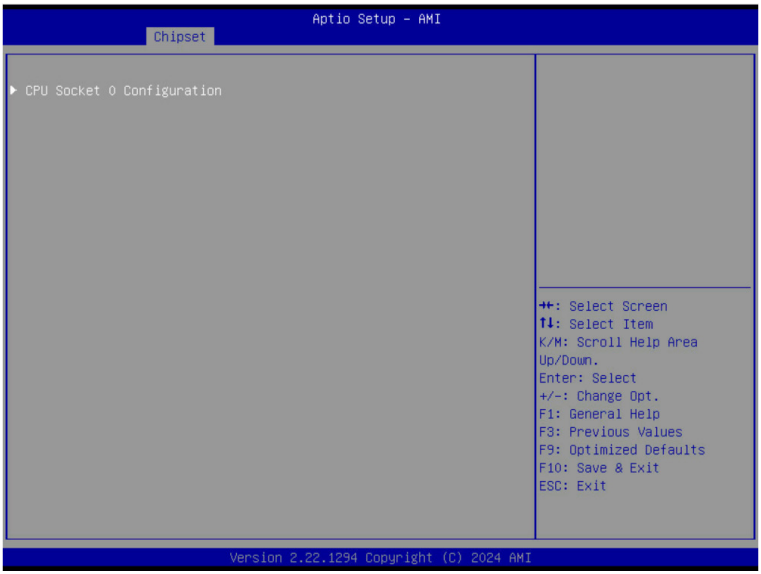
Parameter	Description
Driver Health	Displays driver health status of the devices/controllers if installed

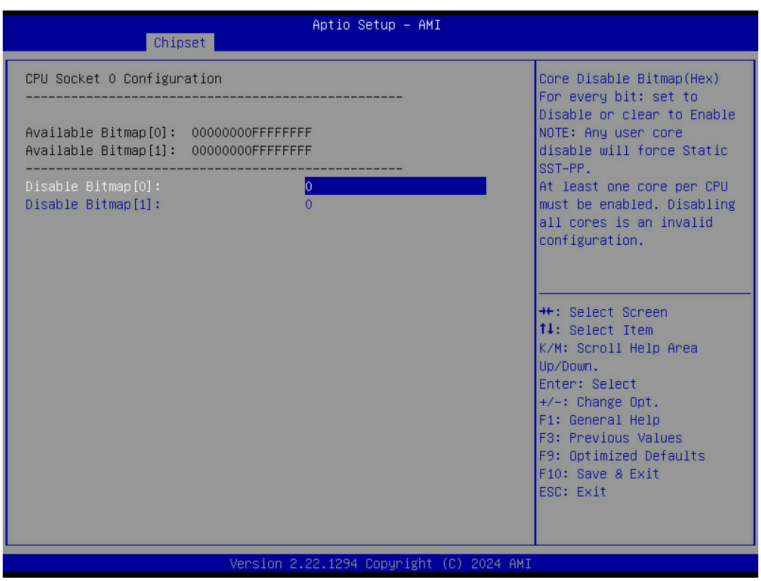
5-3 Chipset Menu

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



5-3-1 Processor Configuration



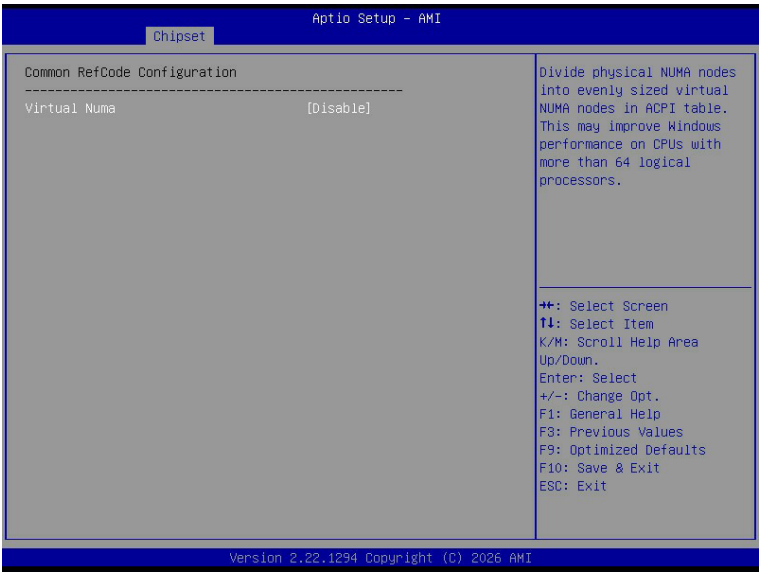


Parameter	Description
Processor Configuration	
Pre-Socket Configuration	Press [Enter] to configure advanced items. ◆ CPU Socket 0/1 Configuration – Core Disable Bitmap(Hex) • Number of Cores to enable. 0 means all cores. FFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.
Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM(Per Core) / L2 Cache RAM(Package) / L3 Cache RAM(Per Package) / Processor # Version	Displays the technical specifications for the installed processor(s).
Enable LP [Global]	Enables Logical processor (Software Method to Enable/Disable Logical Processor threads). Options available: **ALL LPs**, Single LP.
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: **Enable**, Disable.
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: **Enable**, Disable.
DCU Streamer Prefetcher	Enable/Disable DCU streamer prefetcher. Options available: Enable, Disable, **Auto**.
DCU IP Prefetcher	Enable/Disable DCU IP Prefetcher. Options available: **Enable**, Disable.
LLC Prefetch	Enable/Disable LLC Prefetch on all threads. Options available: **Disable**, Enable.
Homeless Prefetch	Enable/Disable Homeless Prefetch on all threads, Auto will skip the register programming and keep the hardware default setting. Options available: Disable, Enable, **Auto**.
FB Thread Slicing	Enable/Disable FB (Full Buffer) Thread Slicing per thread. Options available: **Disable**, Enable.
AMP Prefetch	Options available: **Enable**, Disable.
Enable Intel(R) TXT	Enable/Disable the Intel Trusted Execution Technology support function. Options available: Enable, **Disable.**
VMX	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: **Enable**, Disable.
Enable SMX	Enable/Disable the Safer Mode Extensions (SMX) support function. Options available: Enable, **Disable**.

Parameter	Description
AES-NI	Enable/Disable the AES-NI support. Options available: Disable, **Enable**.
UMONITOR	Enable/Disable UMONITOR support. Options available: **Disable**, Enable.
Debug Consent	Options available: **Disable**, Enable.
Memory Encryption (TME)	Enable/Disable memory encryption (TME). Options available: **Disabled**, Enabled.
Total Memory Encryption Multi-Tenant (TME-MT)	Options available: **Disabled**, Enabled.
Memory integrity	Options available: **Disabled**, Enabled.
Trust Domain Extension (TDX)(Note)	Options available: **Disabled**, Enabled.
Trust Domain Extensions - Connect (TDX Connect)	Options available: **Disabled**, Enabled.
TDX Secure Arbitration Mode Loader (SEAM Loader)	Options available: **Disabled**, Enabled.
TME-MT/TDX Key split	Designate number of bits for TDX usage. The rest will be used by TME-MT.
SGX error code [HEX]	Shows hexadecimal SGX internal error code.
SGX Factory Reset	Perform SGX Factory Reset, on subsequent boot: delete all registration data, if SGX enabled will force Initial Platform Establishment flow. Options available: **Disabled**, Enabled.
SW Guard Extension (SGX)	Options available: **Disabled**, Enabled.
SGX Package Info In-Band Access	Options available: **Disabled**, Enabled.
SGX PRMRR Size Requested	Default setting is **Auto**.
In-Field Scan (IFS)	Press [Enter] to configure advanced items. ◆ Enable SAF(Note) – Options available: **Disabled**, Enabled. ◆ SAF PRMRR Size Requested – Configures SAF size region inside of PRM - just a constituent that may not be equal to the total PRM size.

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

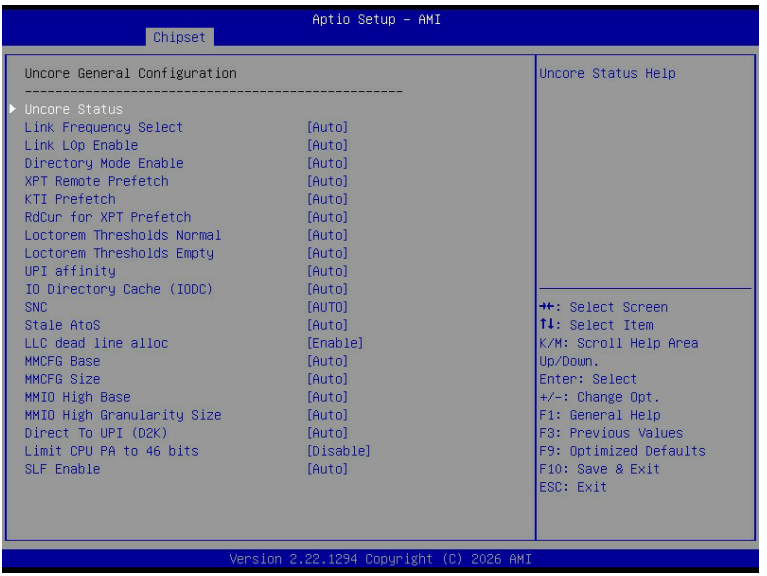
5-3-2 Common RefCode Configuration



Parameter	Description
Common RefCode Configuration	
Virtual Numa(Note)	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors. Options available: Enable, **Disable**.
Number of Virtual Numa Nodes	The number of virtual NUMA nodes per physical NUMA nodes. 0 means automatically set the number of virtual NUMA nodes base on system configuration. 1 equals disabling virtual NUMA.

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

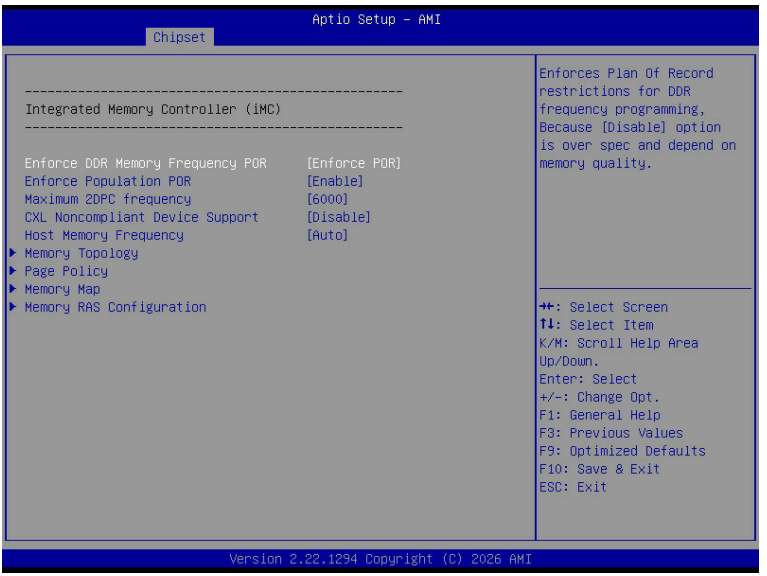
5-3-3 UPI Configuration



Parameter	Description
UPI General Configuration	Press [Enter] to configure advanced items. ◆ Uncore Status – Press [Enter] to view the Uncore status. ◆ Link Frequency Select – Selects the UPI link frequency. – Options available: 16.0GT/s, 20.0GT/s, 24.0GT/s, **Auto**, Use Per Link Setting. ◆ Link L0p Enable – Options available: Disable, Enable, **Auto**. ◆ Directory Mode Enable – Options available: Disable, Enable, **Auto**. ◆ XPT Remote Prefetch – Options available: Disable, Enable, **Auto**. ◆ KTI Prefetch – Options available: Disable, Enable, **Auto**. ◆ RdCur for XPT Prefetch – Options available: Disable, Enable, **Auto**. ◆ Loctorem Thresholds Normal – Options available: Disable, **Auto**, Low, Medium, High. ◆ Loctorem Thresholds Empty – Options available: Disable, **Auto**, Low, Medium, High. ◆ UPI affinity – Options available: Disable, Enable, **Auto**.

Parameter	Description
UPI General Configuration	◆ IO Directirt Cache (IODC) – Options available: Disable, **Auto**, Enable for Remote InvItoM Hybrid Push, Enable for Remote InItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, Enable for Remote InvItoM and Remote WCiLF. ◆ SNC – Default setting is **Auto**. ◆ Stale AtoS – Enable/Disable Stale A to S directory optimization. – Options available: Disable, Enable, **Auto**. ◆ LLC dead line alloc – Enable/Disable fill dead lines in LLC. – Options available: Disable, **Enable**, Auto. ◆ MMCFG Base – Options available: 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, **Auto**. ◆ MMCFG Size – Options available: 64M, 128M, 256M, 512M, 1G, 2G, **Auto**. ◆ MMIO High Base – Options available: 248T, 120T, 88T, 60T, 30T, 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, **Auto**. ◆ MMIO High Granularity Size – Selects the allocation size used to assign mmioh resources. – Options available: 1G, 4G, 16G, 32G, 64G, 256G, 1024G, 4096G, **Auto**. ◆ Limit CPU PA to 46 bits – Options available: **Disable**, Enable, Auto. ◆ SLF Enable – Options available: Disable, Enable, **Auto**.

5-3-4 Memory Configuration



Parameter	Description
Integrated Memory Controller (iMC)	
Enforce DDR Memory Frequency POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR frequency programming. Options available: **Enforce POR**, Enforce Stretch Goals, Disable.
Enforce Population POR	Options available: Disable, **Enable**.
Maximum 2DPC frequency	Select maximum frequency for 2DPC systems. Options available: 5200, **6000**.
CXL Noncompliant Device Support	Options available: Enable, **Disable**.
Host Memory Frequency	Maximum Host DDR Memory Frequency Selections in MT/s. If the AUTO option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. Options available: **Auto**, 4800, 5200, 5600, 6000, 6400.
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Page Policy	Press [Enter] to configure advanced items. ◆ Page Policy – Selects DRAM page policy. – Options available: Auto, Closed, **Adaptive**.

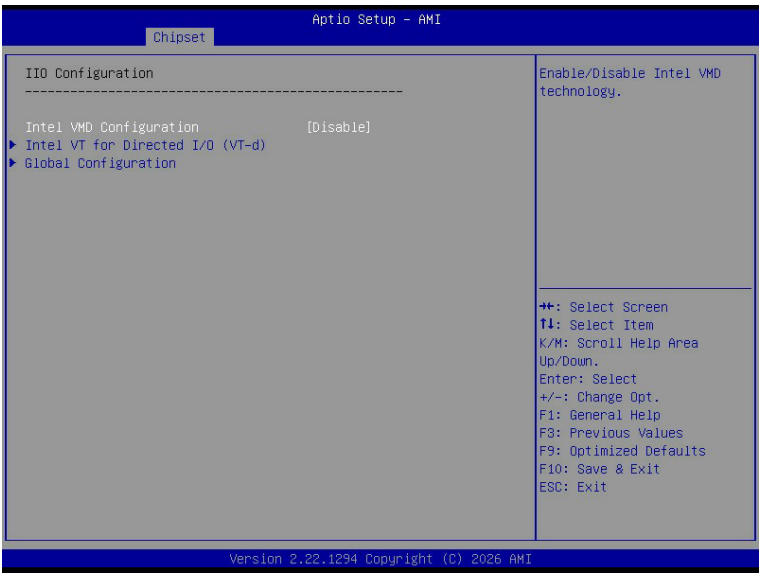
Parameter	Description
Memory Map(Note)	Press [Enter] to configure advanced items. ◆ Intel(R) Flat Memory Mode Support. – Options available: Enabled, **Disabled**. ◆ DDR CXL Heterogeneous Interleave support. – Options available: Enabled, **Disabled**. ◆ In Memory Directory (Dir Backed RSF) with IODC mode – Options available: Enabled, **Disabled**.
Memory RAS Configuration	Press [Enter] to configure advanced items. ◆ Mirror Mode – 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. ◆ UEFI ARM Mirror – Imitate behavior of UEFI based Address Rang Mirror with setup option. – Options available: **Disabled**, Enabled. ◆ Mirror TAD0 – Enable Mirror om entire memory for TAD0. – Options available: Enabled, **Disabled**. ◆ Correctable Error Threshold – Correctable Error Threshold (0x01-0x7fff) used for sparing, and leaky bucket. – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket time window based interface(Note1) – Enable/Disable leaky bucket time window based interface. – Options available: Disabled, Enabled. Default setting is **Disabled**. ◆ Leaky bucket time window based interface Hour – Leaky bucket time window based interface hour used for DDR (0-24). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket time window based interface Minute – Leaky bucket time window based interface minute used for DDR (0-60). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ Leaky bucket low bit – Configures leaky bucket low bit (0x1 - 0x29). – Press the <+> / <-> keys to increase or decrease the desired values.

(Note) Advanced items prompt when HBM CPU is installed.

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

Parameter	Description
Memory RAS Configuration (continued)	◆ Leaky bucket high bit – Configures leaky bucket high bit (0x1 - 0x29). – Press the <+> / <-> keys to increase or decrease the desired values. ◆ ADDDC Sparing(Note) – Enable/Disable ADDDC Sparing. – Options available: **Disabled**, Enabled. ◆ Enable ADDDC Error Injection – Options available: Disabled, **Enabled**. ◆ Patrol Scrub – Options available: Disabled, **Enable at End of POST**. ◆ Patrol Scrub Interval – Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto. ◆ DDR5 ECS – Options available: Disabled, **Enabled**, Enable ECS with Result Collection.

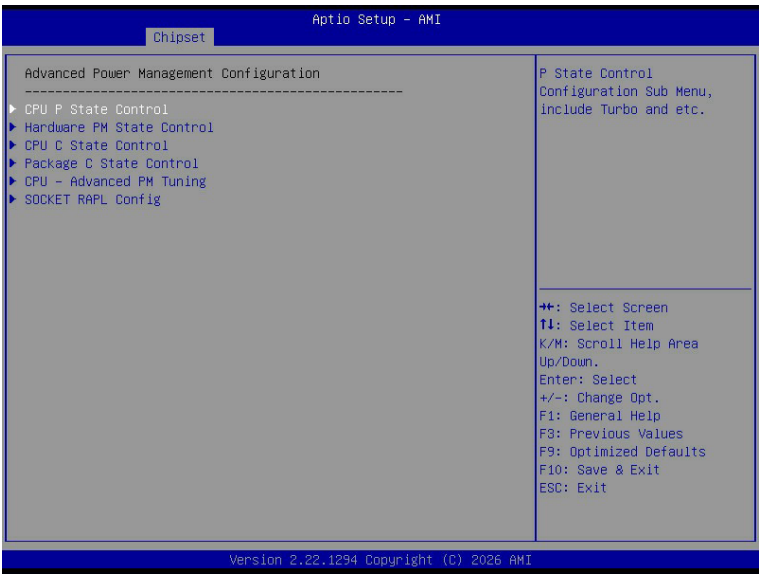
5-3-5 IIO Configuration



Parameter	Description
IIO Configuration	
Intel® VMD Configuration(Note)	Enable/Disable Intel® VMD technology. Options available: **Disable**, Enable.
Intel® VMD for Non-Hotplug NVMe	Enable/Disable Intel® VMD for Non-Hotplug NVMe. Options available: **Disable**, Enable.
Intel VT for Directed I/O (VT-d)	Press [Enter] to configure advanced items. ◆ Enable IOMMU Virtualization Support – Options available: **Enable**, Disable. ◆ DMA Control Opt-In Flag – Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA). – Options available: Enable, **Disable**. ◆ Pre-boot DMA Protection – Options available: Enable, **Disable**. ◆ PCIe ACSCTL(Note) – Options available: Enable, **Disable**. ◆ Source Validation – Options available: **Disabled**, Enabled. ◆ Translation Blocking – Options available: **Disabled**, Enabled.

Parameter	Description
Intel VT for Directed I/O (VT-d)	◆ P2P Request Redirect – Options available: Disabled, **Enabled**. ◆ P2P Completion Redirect – Options available: Disabled, **Enabled**. ◆ Upstream Forwarding Enable – Options available: Disabled, **Enabled**. ◆ Cache Allocation – Options available: **Enable**, Disable. ◆ PRS Capability for PCIe – Options available: Disable, Enable, **Auto**.
Global Configuration	Press [Enter] to configure advanced items. ◆ Allocating Write Flows – Options available: Non-Allocating, **Allocating**. ◆ 10-bit Tag Support – Options available: Disable, **Auto**, Force Enable. ◆ Max Read Request Size – Options available: Auto, 128B, 256B, 512B, 1024B, 2048B, **4096B**. ◆ Relaxed Ordering – Options available: Disable, **Enable**.

5-3-6 Advanced Power Management Configuration



Parameter	Description
CPU P State Control	Press [Enter] to configure advanced items. ◆ AVX License Pre-Grant Override(Note) – Options available: **Disable**, Enable. ◆ AVX ICCP pre-grant level – Options available: **128 Heavy**, 256 Light, 256 Heavy, 512 Light, 512 Heavy, AMX. ◆ AVX P1 – Options available: **Nominal**, Level 1, Level 2. ◆ 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: Disable, **Enable**. ◆ EIST PSD Function – Options available: **HW_ALL**, SW_ALL. ◆ Boot performance mode – Select the performance state that the BIOS will set before OS hand off. – Options available: **Max Performance**, Max Efficiency.

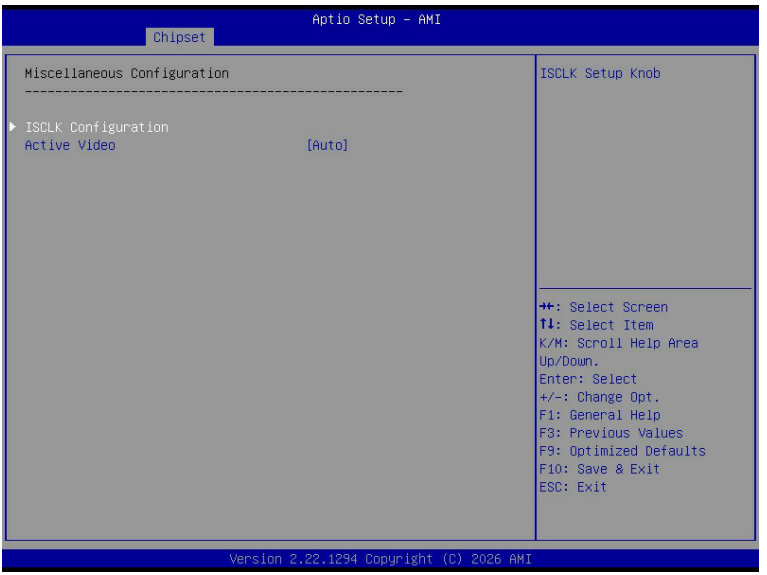
(Note) Advanced items prompt when this item is defined.

Parameter	Description
CPU P State Control (continued)	◆ 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: Disable, **Enable**. ◆ Energy Efficient Turbo – Options available: Disable, **Enable**. ◆ Perf P-Limit – Press [Enter] to configure advanced items. » Perf P-Limit • Options available: **Disable**, Enable.
Hardware PM State Control	Press [Enter] to configure advanced items. ◆ Hardware P-State – 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. ◆ HardwarePM Interrupt – Options available: **Disable**, Enable. ◆ Native ASPM – Options available: **Auto**, Enabled, Disabled.
CPU C State Control	Press [Enter] to configure advanced items. ◆ Monitor MWAIT – Options available: Disable, **Enable**. ◆ C1 to C1e Promotion – CPU will promote C1 request to C1e state. – Options available: Disable, **Enable**. ◆ ACPI C6x Enumeration – Options available: Disable, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, **Auto**. ◆ C6x to C1 Demotion – Options available: **Disable**, Enable. ◆ C1 Undemotion to C6x – Options available: **Disable**, Enable.
Package C State Control	Press [Enter] to configure advanced items. ◆ Package C State – Configures the state for the C-State package limit. – Options available: C0/C1 state, C2 state, C6(non Retention) state, No Limit, **Auto**.

Parameter	Description
CPU - Advanced PM Tuning	Press [Enter] to configure advanced items. ◆ Uncore Freq Ratio (COMPUTE/IO) – 0: Set dynamic Uncore frequency range from max and min fused values. Otherwise Uncore will run at a constant frequency ratio, the UFS algorithm will be disabled, but physical limits may still reduce frequency. ◆ Uncore Freq Control – Options available: Mode 0, **Mode 1** ◆ Energy Perf BIAS – Press [Enter] to configure advanced items. » Power Performance Tuning • Options available: **OS Controls EPB**, BIOS Controls EPB, PECI Controls EPB. » Energy_PERF_BIAS_CFG mode(Note) • Options available: Performance, **Balanced Performance**, Balanced Power, Power. » Workload Configuration • Options available: **Balanced**, I/O sensitive. ◆ Latency Optimized Mode – Options available: **Disable**, Enabled, Auto.
SOCKET RAPL Config	Press [Enter] to configure advanced items. ◆ PL1 Power Limit – Press the <+> / <-> keys to increase or decrease the desired values. ◆ PL1 Timer Window – Options available: **1**, 1.25, 1.5, 1.75, 2, 2.5, 3, 3.5, 4, 5. ◆ PL2 Power Limit – Press the <+> / <-> keys to increase or decrease the desired values. ◆ PL2 Timer Window – Options available: **0.012**, 0.014, 0.016, 0.02, 0.023, 0.027, 0.031, 0.039.

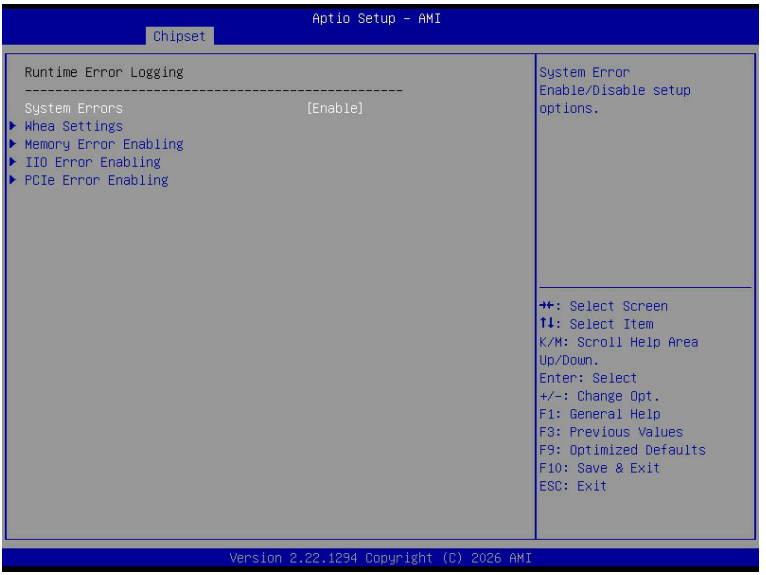
(Note) This item is configurable when **Power Performance Tuning** is set to **BIOS Controls EPB**.

5-3-7 Miscellaneous Configuration



Parameter	Description
Miscellaneous Configuration	
ISCLK Configuration	Press [Enter] to configure advanced items. ◆ SSC1/SSC2 Enable – Options available: Disable, **Enable**.
Active Video	Selects the active video type. Options available: **Auto**, Onboard Device, PCIE Device, Specific PCIE Device.

5-3-8 Runtime Error Logging Settings

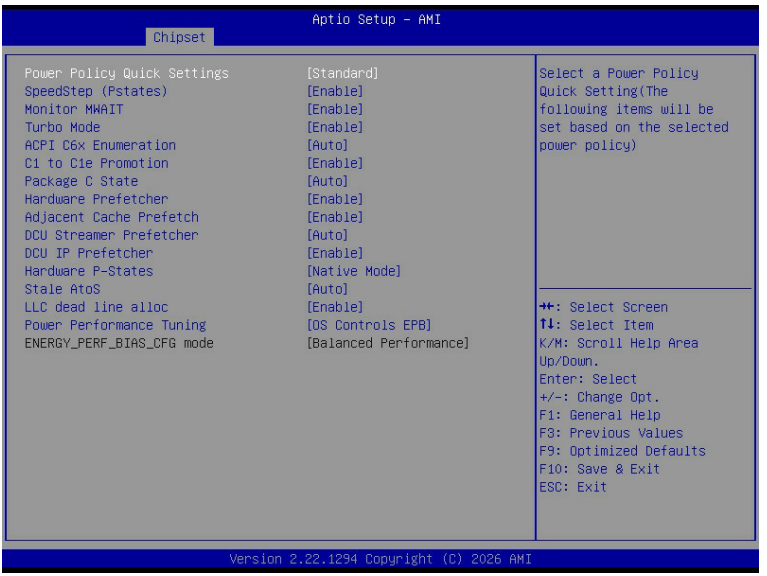


Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: **Enable**, Disable.
Whea Settings	Press [Enter] to configure advanced items. ◆ WHEA (Windows Hardware Error Architecture) Support – Enable/Disable WHEA Support. – Options available: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

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

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

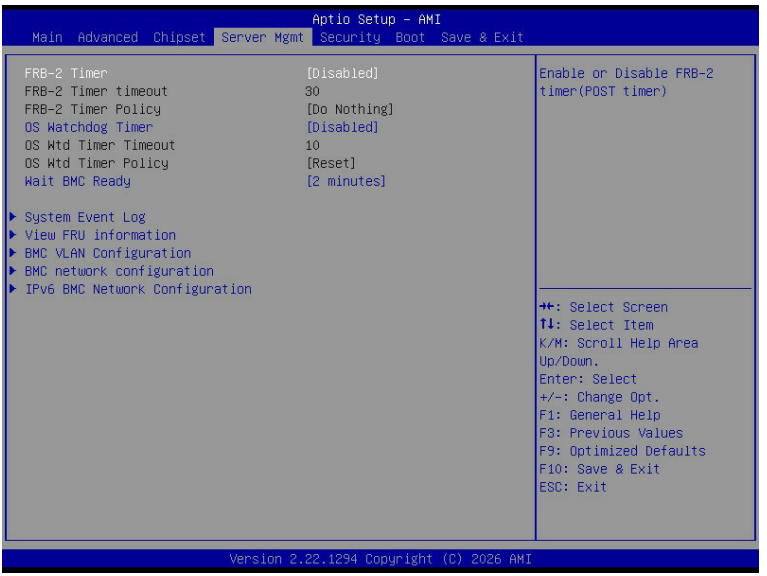
5-3-9 Power Policy



Parameter	Description
Power Policy Quick Settings(Note)	Selects a Power Policy Quick Setting. Options available: **Standard**, Best Performance, Energy Efficient.
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: **Enable**, Disable.
Monitor MWAIT	Allows Monitor and MWAIT instructions. Options available: **Enable**, Disable.
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: **Enable**, Disable.
ACPI C6x Enumeration	Options available: Disable,C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, **Auto**.
C1 to C1e Promotion	Options available: Disable, **Enable**.
Package C State	Configures the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, **Auto**.
Hardware Prefetcher	Options available: **Enable**, Disable.
Adjacent Cache Prefetch	Options available: **Enable**, Disable.

Parameter	Description
DCU Streamer Prefetcher	Options available: Enable, Disable, **Auto**.
DCU IP Prefetcher	Options available: **Enable**, Disable.
Hardware P-States	Options available: Disable, **Native Mode**, Out of Band Mode, Native Mode with No Legacy Support.
Stale Atos	Options available: Disable, Enable, **Auto**.
LLC dead line alloc	Options available: Disable, **Enable**, Auto.
Power Performance Tuning	Options available: **OS Controls EPB**, BIOS Controls EPB, PECI Controls EPB.
ENERGY_PERF_BIAS_CFG mode	Options available: Performance, **Balanced Performance,** Balanced Power, Power.
Hyper-Performance	Options available: Disable, Level 1, Level 2, Level 3, **Maximum**.
Turbo Frequency Lock	Options available: **Disable**, Enable.

5-4 Server Management Menu

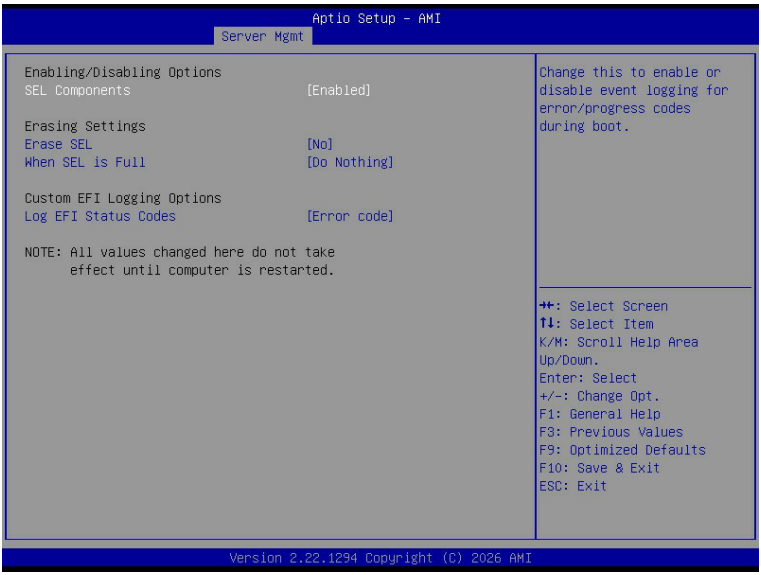


Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled, **Disabled**.
FRB-2 Timer[Note1] timeout	Configures the FRB2 Timer timeout. The value is between 1 to 30 minutes. Default setting is **30**.
FRB-2 Timer Policy[Note1]	Configures the FRB2 Timer policy. Options available: **Do Nothing**, Reset, Power Down, Power Cycle.
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled, **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.
Wait BMC Ready	POST wait BMC ready and reboot system. Options available: Disabled, **2 minutes**, 4 minutes, 6 minutes.
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the FRU information.

(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
BMC VLAN Configuration	Press [Enter] to configure advanced items.
BMC network Configuration	Press [Enter] to configure advanced items.
IPv6 BMC Network Configuration	Press [Enter] to configure advanced items.

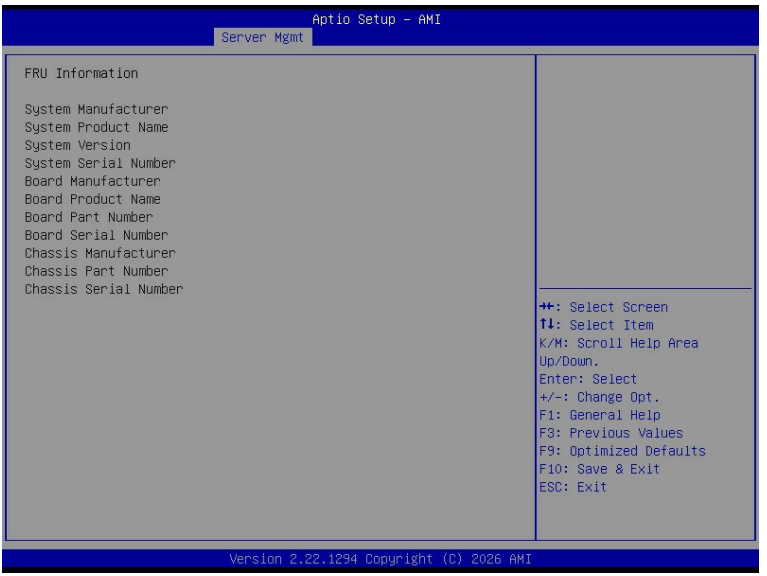
5-4-1 System Event Log



Parameter	Description
Enabling / Disabling Options	
SEL Components	Change this item to enable or disable all features of System Event Logging during boot. Options available: **Enabled**, Disabled.
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: **No**, Yes, On next reset, Yes, On every reset.
When SEL is Full	Choose options for reactions to a full SEL. Options available: **Do Nothing**, Erase Immediately, Delete Oldest Record.
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.

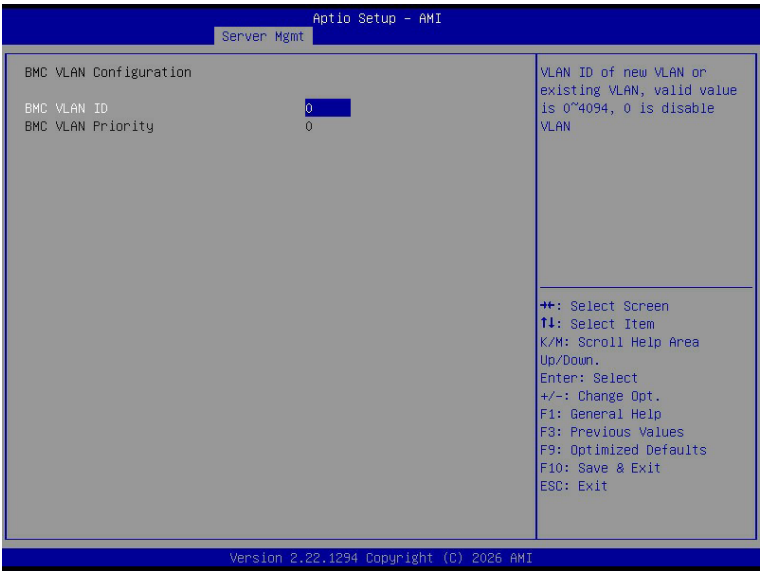
5-4-2 View FRU Information

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



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

5-4-3 BMC VLAN Configuration

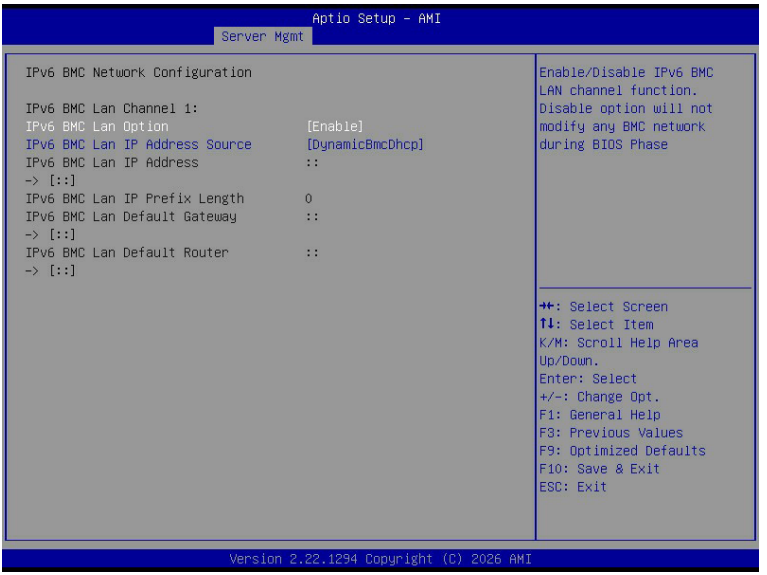


Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority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

5-4-4 BMC Network Configuration

Parameter	Description
BMC network configuration	
Select NCSI and Dedicated LAN	Options available: Do Nothing, Model1(Dedicated), Model2(NCSI), **Mode3(Failover)**.
Lan Channel 1	
Configuration Address source	Selects to configure LAN channel parameters statically or dynamically (DHCP). Options available: Unspecified, Static, **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.

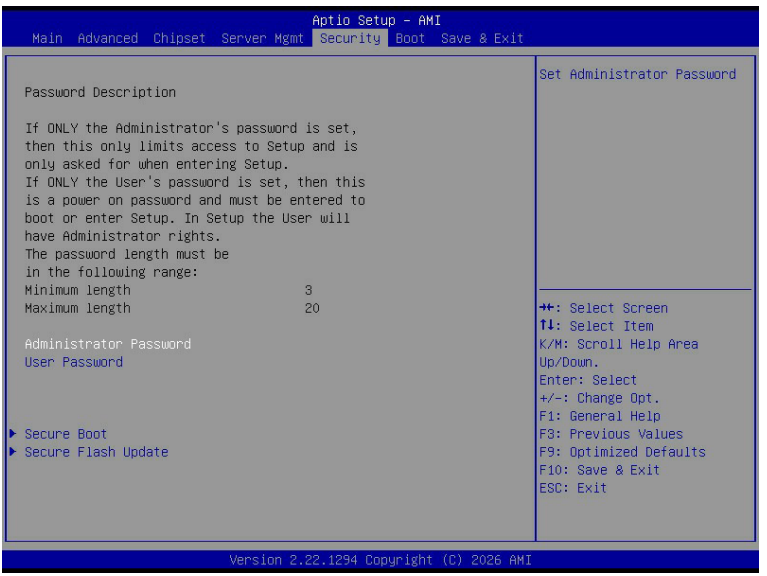
5-4-5 IPv6 BMC Network Configuration



Parameter	Description
IPv6 BMC network configuration	
IPv6 BMC Lan Channel 1	
IPv6 BMC Lan Option	Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase. Options available: Unspecified, Disable, **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**.
IPv6 BMC Lan IP Address/ Prefix Length	Check if the IPv6 BMC LAN IP address matches those displayed on the screen.

5-5 Security Menu

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



There are two types of passwords that you can set:

- Administrator Password

  Entering this password will allow the user to access and change all settings in the Setup Utility.

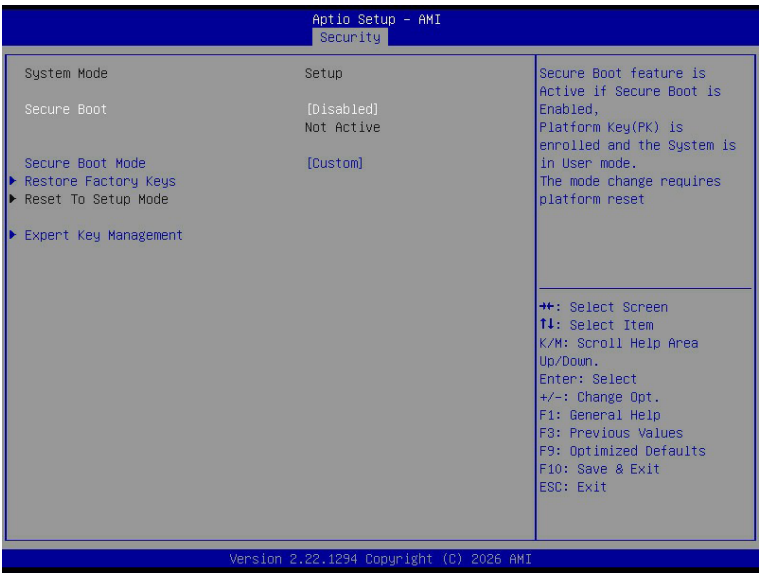
- User Password

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

5-5-1 Secure Boot

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

If your Operating System is not supporting Secure Boot, the system will hang when starting the Operating System.



Parameter	Description
System Mode	Displays if the system is in User mode or Setup mode.
Secure Boot	Enable/ Disable the Secure Boot function. Options available: Enabled, **Disabled**.
Secure Boot Mode(Note)	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all files being loaded before the Operating System loads to the login screen have not been tampered with. 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.
Restore Factory Keys	Forces the system to user mode and installs factory default Secure Boot key database.
Reset To Setup Mode	Reset the system to Setup Mode.

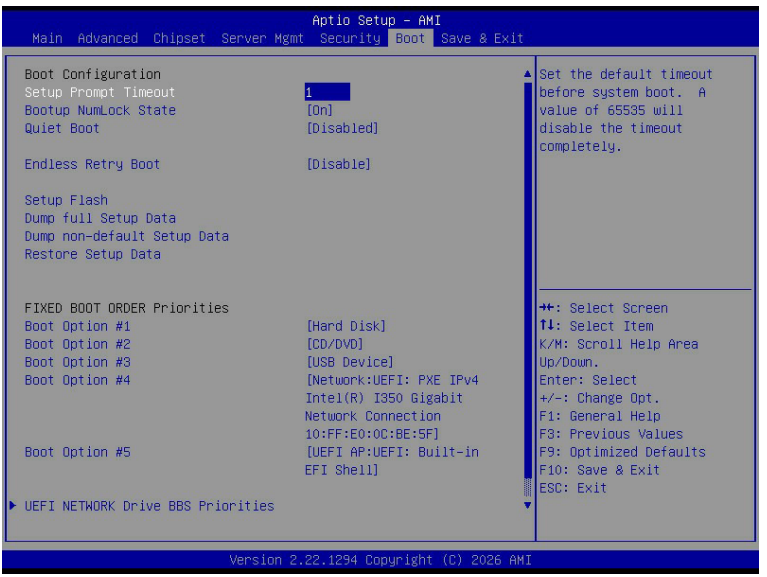
(Note) Advanced items prompt when this item is set to **Custom**.

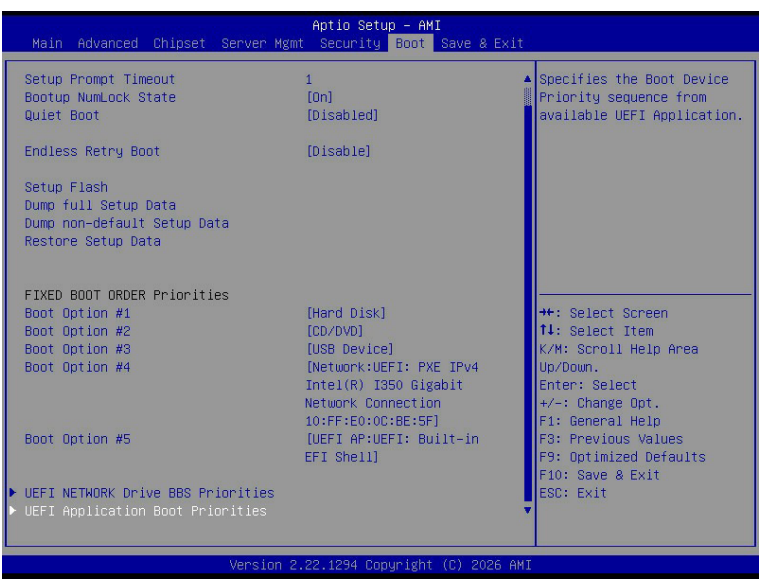
Parameter	Description
Key Management	Press [Enter] to configure advanced items. **Please note that this item is configurable when Secure Boot Mode is set to Custom.** ◆ Factory Key Provision – Allows to provision factory default Secure Boot keys when system is in Setup Mode. – Options available: Enabled,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

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

5-6 Boot Menu

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

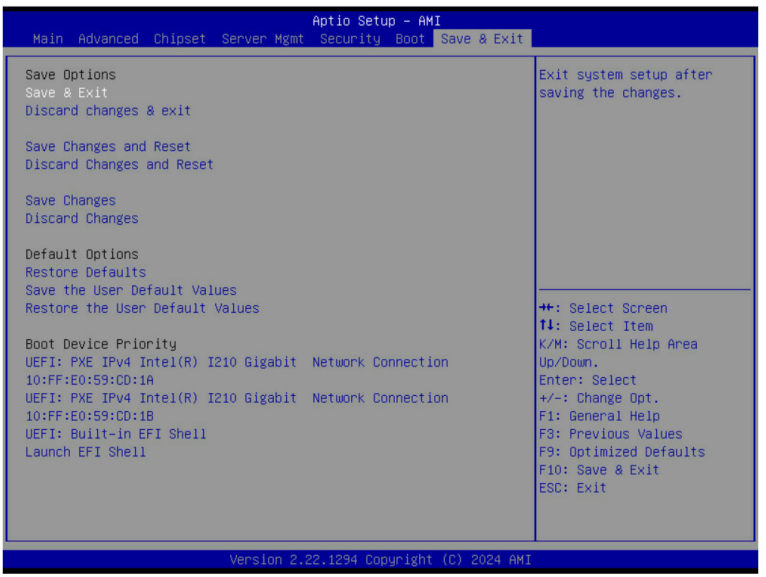




Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: **On**, Off.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

5-7 Save & Exit Menu

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



Parameter	Description
Save Options	
Save and Exit	Saves changes made and closes the BIOS setup. 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	

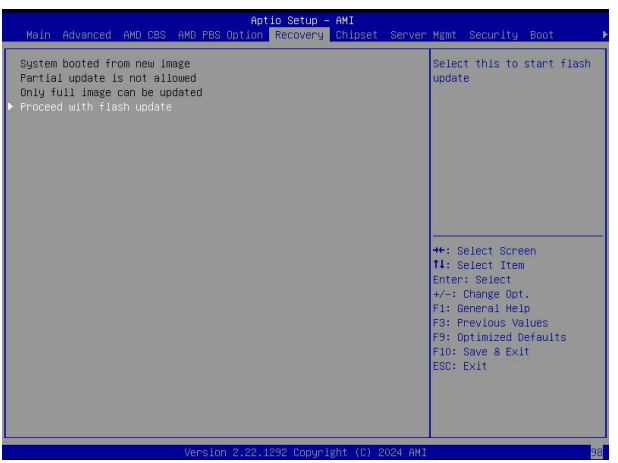
Parameter	Description
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system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

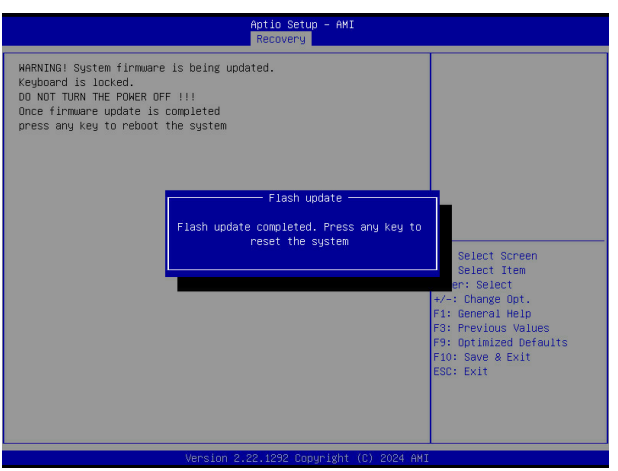
5-8 BIOS Recovery

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

Recovery Instruction:

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





Designed by