

# **GIGABYTE™**

# **H252-3C0**

HCI Server – Intel UP 2U 4 Nodes Server with 12 x SATA/SAS

## **User Manual**

Rev. 1.0

## **Copyright**

© 2021 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.

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

## **Disclaimer**

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

## **Documentation Classifications**

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

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

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

## **For More Information**

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




For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: <http://reseller.b2b.gigabyte.com>

For further technical assistance, please contact your GIGABYTE representative or visit <https://esupport.gigabyte.com/> to create a new support ticket

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

## Conventions

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

	<b>NOTE!</b> Gives bits and pieces of additional information related to the current topic.
	<b>CAUTION!</b> Gives precautionary measures to avoid possible hardware or software problems.
	<b>WARNING!</b> Alerts you to any damage that might result from doing or not doing specific actions.

## Server Warnings and Cautions

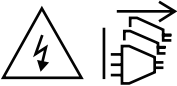
Before installing a server, be sure that you understand the following warnings and cautions.



### WARNING!

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

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug all the power cords from the power supplies to disconnect power to the equipment.



- Shock Hazard! Disconnect all power supply cords before servicing.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.



### WARNING!

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



### WARNING!

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



### WARNING!

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



### WARNING!

**This equipment is intended to be used in Restrict Access Location. The access can only be gained by Skilled person.**

**Only authorized by well trained professional person can access the restrict access location.**



### CAUTION!

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

## Electrostatic Discharge (ESD)



### **CAUTION!**

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

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

**System power on/off:** To remove power from system, you must remove the system from rack. Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

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

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

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

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

**CAUTION!**

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

# Table of Contents

Chapter 1	Hardware Installation .....	11
1-1	Installation Precautions .....	11
1-2	Product Specifications .....	12
1-3	System Block Diagram .....	17
Chapter 2	System Appearance .....	19
2-1	Front View .....	19
2-2	Rear View .....	19
2-3	Front Panel LED and Buttons .....	20
2-4	System LAN LEDs .....	21
2-5	Hard Disk Drive LEDs .....	22
2-6	Power Supply Unit (PSU) LED .....	23
Chapter 3	System Hardware Installation .....	25
3-1	Installing the Hard Disk Drive .....	26
3-2	Removing the Node .....	28
3-3	Removing Chassis Cover .....	29
3-4	Removing and Installing the Fan Duct .....	30
3-5	Installing the CPU and Heat Sink .....	31
3-6	Installing Memory .....	33
3-6-1	Eight Channel Memory Configuration .....	33
3-6-2	Installing the Memory .....	34
3-6-3	Memory Population Table .....	34
3-6-4	Processor and Memory Module Matrix Table .....	35
3-6-5	Intel Optane DCPMM DIMM Population Rule .....	36
3-7	Installing the PCI Expansion Card .....	37
3-8	Replacing the Fan Module .....	40
3-9	Replacing the Power Supply .....	41
3-10	Cable Routing .....	42
Chapter 4	Motherboard Components .....	47
4-1	Motherboard Components .....	47
4-2	Jumper Setting .....	48
Chapter 5	BIOS Setup .....	49
5-1	The Main Menu .....	51
5-2	Advanced Menu .....	54
5-2-1	Trusted Computing .....	55

5-2-2	Serial Port Console Redirection .....	56
5-2-3	SIO Configuration .....	60
5-2-4	PCI Subsystem Settings .....	61
5-2-5	USB Configuration .....	62
5-2-6	Network Stack Configuration .....	63
5-2-7	Post Report Configuration .....	64
5-2-8	NVMe Configuration .....	65
5-2-9	Chipset Configuration .....	66
5-2-10	Tls Auth Configuration .....	67
5-2-11	iSCSI Configuration .....	68
5-2-12	Intel(R) I350 Gigabit Network Connection .....	69
5-2-13	VLAN Configuration .....	71
5-2-14	Driver Health .....	72
5-3	Chipset Setup Menu .....	73
5-3-1	Processor Configuration .....	74
5-3-2	Common RefCode Configuration .....	77
5-3-3	UPI Configuration .....	78
5-3-4	Memory Configuration .....	79
5-3-5	IIO Configuration .....	83
5-3-6	Advanced Power Management Configuration .....	85
5-3-7	PCH Configuration .....	88
5-3-8	Miscellaneous Configuration .....	90
5-3-9	Server ME Configuration .....	91
5-3-10	Runtime Error Logging .....	92
5-3-11	Power Policy .....	94
5-4	Server Management Menu .....	96
5-4-1	System Event Log .....	98
5-4-2	View FRU Information .....	99
5-4-3	BMC VLAN Configuration .....	100
5-4-4	BMC Network Configuration .....	101
5-4-5	IPv6 BMC Network Configuration .....	102
5-5	Security Menu .....	103
5-5-1	Secure Boot .....	104
5-6	Boot Menu .....	106
5-6-1	UEFI NETWORK Drive BBS Priorities .....	108
5-7	Save & Exit Menu .....	109
5-8	BIOS POST Codes .....	111
5-8-1	AMI Standard - PEI .....	111
5-8-2	AMI Standard - DXE .....	111
5-8-3	AMI Standard - ERROR .....	113
5-8-4	Intel UPI POST Codes .....	114



5-8-5	Intel UPI Error Codes .....	114
5-8-6	Intel MRC POST Codes .....	115
5-8-7	Intel MRC Error Codes .....	115
5-8-8	Intel PM POST Codes .....	116
5-8-9	Intel PM POST Codes .....	116
5-9	BIOS POST Beep code (AMI standard) .....	117
5-9-1	PEI Beep Codes .....	117
5-9-2	DXE Beep Codes .....	117

This page intentionally left blank

# Chapter 1 Hardware Installation

## 1-1 Installation Precautions

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







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

# 1-2 Product Specifications



## NOTE:

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

 CPU	<ul style="list-style-type: none"><li>◆ 3rd Generation Intel® Xeon® Scalable Processors</li><li>◆ Intel® Xeon® Platinum Processor, Intel® Xeon® Gold Processor, Intel® Xeon® Silver Processor</li><li>◆ 10nm technology, CPU TDP up to 270W</li></ul>
	<b>Per Node:</b> <ul style="list-style-type: none"><li>◆ 1 x LGA 4189</li></ul>
 Socket	<b>Total:</b> <ul style="list-style-type: none"><li>◆ 4 x LGA 4189</li><li>◆ Socket P+</li></ul>
 Chipset	<ul style="list-style-type: none"><li>◆ Intel® C621A Express Chipset</li></ul>
 Memory	<b>Per Node:</b> <ul style="list-style-type: none"><li>◆ 8 x DIMM slots</li></ul> <b>Total:</b> <ul style="list-style-type: none"><li>◆ 32 x DIMM slots</li><li>◆ DDR4 memory supported only</li><li>◆ 8-Channel memory architecture</li><li>◆ RDIMM modules up to 64GB supported</li><li>◆ LRDIMM modules up to 128GB supported</li><li>◆ 3DS RDIMM/LRDIMM modules up to 256GB supported</li><li>◆ Memory speed: Up to 3200 MHz</li></ul>
 LAN	<b>Per Node:</b> <ul style="list-style-type: none"><li>◆ 2 x 1Gb/s BASE-T LAN ports (Intel® I350-AT2)</li><li>◆ 1 x Dedicated management port</li></ul> <b>Total:</b> <ul style="list-style-type: none"><li>◆ 8 x 1GbE LAN ports (1 x Intel® I350-AM2)</li><li>◆ 4 x Dedicated management ports</li><li>◆ 1 x 10/100/1000 *CMC global management port</li></ul> <p>◆ *CMC: Chassis Management Controller, to monitor all status of computing nodes</p>
 Video	<ul style="list-style-type: none"><li>◆ Integrated in Aspeed® AST2500</li><li>◆ 2D Video Graphic Adapter with PCIe bus interface</li><li>◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM</li></ul> <p>Management chip on CMC board:</p> <ul style="list-style-type: none"><li>◆ Integrated in Aspeed® AST2520A2-GP</li></ul>



## Storage

### Per node:

- ◆ 3 x 3.5" SATA/SAS hot-swappable SSD bays
- ◆ 1 x SATA DOM

### Total:

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



## Expansion Slots

### Per node:

- ◆ 2 x Low profile half-length slots with PCIe x16 (Gen4 x16 bus)
- ◆ 1 x OCP 2.0 mezzanine slot with PCIe Gen3 x8 bandwidth (Type1, P1, P2 with NCSI supported)

### Total:

- ◆ 8 x Low profile half-length slots with PCIe x16 (Gen4 x16 bus)
- ◆ 4 x OCP 2.0 mezzanine slots with PCIe Gen3 x8 bandwidth (Type1, P1, P2 with NCSI supported)



## Internal I/O

### Per Node:

- ◆ 1 x USB 3.0 header
- ◆ 1 x SATA DOM
- ◆ 1 x TPM header
- ◆ 1 x OCP 2.0 mezzanine slots
- ◆ 1 x Front panel header
- ◆ 1 x Back plane board header
- ◆ 1 x IPMB connector
- ◆ 1 x Clear CMOS jumper
- ◆ 1 x BIOS recovery jumper



#### Front I/O

**Per node:**

- ◆ 1 x Power button with LED
- ◆ 1 x ID button with LED
- ◆ 1 x Status LED

**Total:**

- ◆ 4 x Power button with LED
- ◆ 4 x ID button with LED
- ◆ 4 x Status LED
- ◆ \*1 x CMC status LED

\*Only one CMC status LED per system



#### Rear I/O

**Per node:**

- ◆ 2 x USB 3.0
- ◆ 1 x VGA
- ◆ 2 x RJ45
- ◆ 1 x MLAN
- ◆ 1 x ID LED

**Total:**

- ◆ 8 x USB 3.0
- ◆ 4 x VGA
- ◆ 8 x RJ45
- ◆ 4 x MLAN
- ◆ 4 x ID LEDs
- ◆ \*1 x CMC global management port

\*Only one CMC global management port per system



#### Backplane I/O

- ◆ Front side\_CBPH0C3: 12 x SATA/SAS ports Speed and bandwidth: SATA 6Gb/s or SAS 12Gb/s per port



#### TPM

- ◆ 1 x TPM header with SPI interface
- ◆ Optional TPM2.0 kit: CTM010





## Power Supply

- ◆ 2 x 1600W redundant PSUs
- ◆ 80 PLUS Platinum
  
- ◆ AC Input:
  - 100-127V~/ 12A, 47-63Hz
  - 200-219V~/ 10A, 47-63Hz
  - 220-240V~/ 10A, 47-63Hz
  
- ◆ DC Output:
  - Max 1000W/ 100-127V~
    - +12V/ 83A
    - +12Vsb/ 3A
  - Max 1800W/ 200-240V
    - +12V/ 148A
    - +12Vsb/ 3A
  - Max 1968W/ 200-240V
    - +12V/ 162A
    - +12Vsb/ 3A



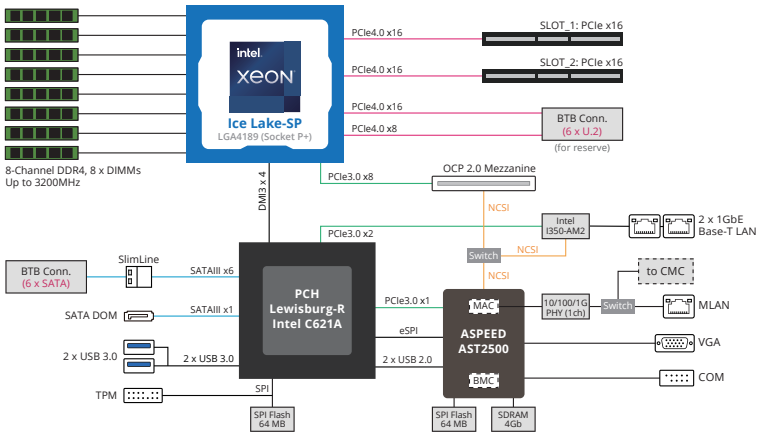
## System Management

- ◆ Aspeed® AST2500 management controller
- ◆ GIGABYTE Management Console (AMI MegaRAC SP-X) web interface
  
- ◆ Dashboard
- ◆ JAVA Based Serial Over LAN
- ◆ HTML5 KVM
- ◆ Sensor Monitor (Voltage, RPM, Temperature, CPU Status ...etc.)
- ◆ Sensor Reading History Data
- ◆ FRU Information
- ◆ SEL Log in Linear Storage / Circular Storage Policy
- ◆ Hardware Inventory
- ◆ Fan Profile
- ◆ System Firewall
- ◆ Power Consumption
- ◆ Power Control
- ◆ LDAP / AD / RADIUS Support
- ◆ Backup & Restore Configuration
- ◆ Remote BIOS/BMC/CPLD Update
- ◆ Event Log Filter
- ◆ User Management
- ◆ Media Redirection Settings
- ◆ PAM Order Settings
- ◆ SSL Settings
- ◆ SMTP Settings

 Ambient Temperature	<ul style="list-style-type: none"><li>◆ Operating temperature: 10°C to 35°C</li><li>◆ Operating humidity: 8-80% (non-condensing)</li></ul>
Relative Humidity	<ul style="list-style-type: none"><li>◆ Non-operating temperature: -40°C to 60°C</li><li>◆ Non-operating humidity: 20%-95% (non-condensing)</li></ul>
 System Dimension	<ul style="list-style-type: none"><li>◆ 2U 4 Nodes - Rear access</li><li>◆ 440mm (W) x 87.5mm (H) x 695mm (D)</li></ul>



# 1-3 System Block Diagram



This page intentionally left blank

# Chapter 2 System Appearance

## 2-1 Front View

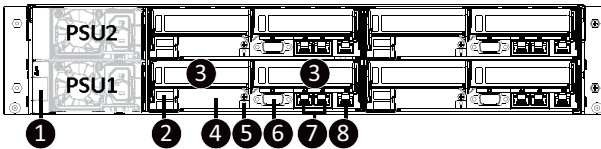


No.	Description
1.	Front Panel LEDs and Buttons



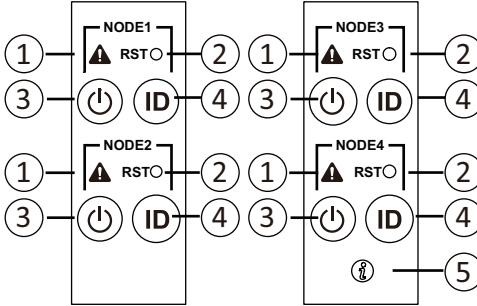
- Please Go to Chapter 2-3 Front Panel LED and Buttons for detail description of function LEDs.

## 2-2 Rear View



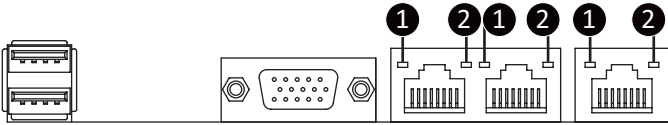
No.	Description
1.	CMC LAN Port
2.	USB 3.0 Port x 2
3.	PCIe Card Slot x 2
4.	Mezzanine Card Slot (Option/OCP 2.0)
5.	ID LED
6.	VGA Port
7.	GbE LAN Port x 2
8.	Server Management LAN Port

## 2-3 Front Panel LED and Buttons



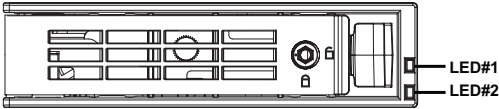
No.	Name	Color	Status	Description
1.	System Status LED	Green	On	System is operating normally.
		Amber	On	Critical condition, may indicates: System fan failure System temperature
			Blink	Non-critical condition, may indicates: Redundant power module failure Temperature and voltage issue
			Off	Non-critical condition, may indicates: Redundant power module failure Temperature and voltage issue
2.	Reset Button	--	--	Press this button to reset the system.
3.	Power button with LED	Green	On	System is powered on
		Green	Blink	System is in ACPI S1 state (sleep mode)
		N/A	Off	<ul style="list-style-type: none"> <li>System is not powered on or in ACPI S5 state (power off)</li> <li>System is in ACPI S4 state (hibernate mode)</li> </ul>
4.	ID Button with LED	Blue	On	System identification is active.
		N/A	Off	System identification is disabled.
5.	Enclosure Status LED	Green	On	System is operating normally.
		Amber	On	Critical condition, may indicates: Power module failure System fan failure Power supply voltage issue System temperature
			Blink	Non-critical condition, may indicates: Redundant power module failure Temperature and voltage issue
			Off	Non-critical condition, may indicates: Redundant power module failure Temperature and voltage issue

## 2-4 System LAN LEDs



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

## 2-5 Hard Disk Drive LEDs



RAID SKU		LED1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA)	Disk LED (LED on Back Panel)	Green	ON(*1)	OFF		BLINK (*2)	OFF
		Amber	OFF	OFF		OFF	OFF
	Removed HDD Slot (LED on Back Panel)	Green	ON(*1)	OFF		--	--
		Amber	OFF	OFF		--	--
RAID configuration (via HW RAID Card or SW RAID Card)	Disk LED	Green	ON	OFF		BLINK (*2)	OFF
		Amber	OFF	ON	(Low Speed: 2 Hz)	OFF	OFF
	Removed HDD Slot	Green	ON(*1)	OFF	(*3)	--	--
		Amber	OFF	ON	(*3)	--	--

LED 2	HDD Present	No HDD
Green	ON	OFF

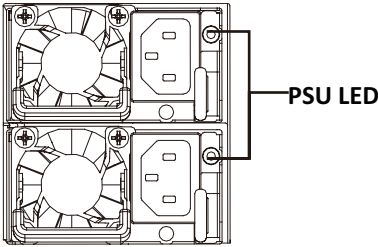
**NOTE:**

\*1: Depends on HBA/Utility Spec.

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

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

## 2-6 Power Supply Unit (PSU) LED



State	Description
OFF	Indicates no AC power to all power supplies
1Hz Blink GREEN	Indicates AC present/ only standby on/ Cold redundant mode
2Hz Blink GREEN	Indicates power supply firmware in updating mode
Amber	Indicates AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power Indicates power supply critical event causing shut down: failure, OCP, OVP, Fan Fail, UVP
1Hz Blink Amber	Indicates power supply warning events where the power supply continues to operate: high temp, high power, high current, slow fan

This page intentionally left blank



## Chapter 3 System Hardware Installation



### Pre-installation Instructions

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

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

### 3-1 Installing the Hard Disk Drive

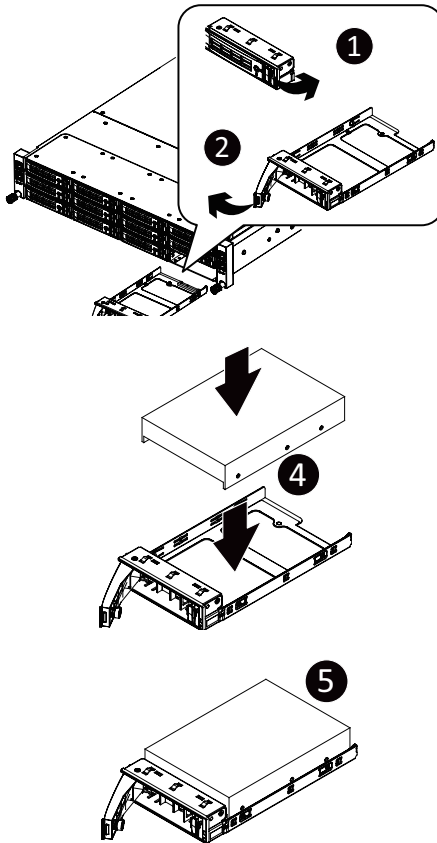


Read the following guidelines before you begin to install the Hard disk drive:

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

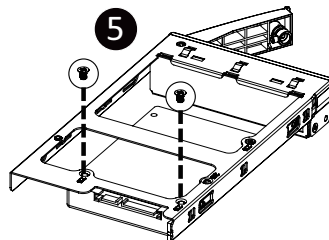
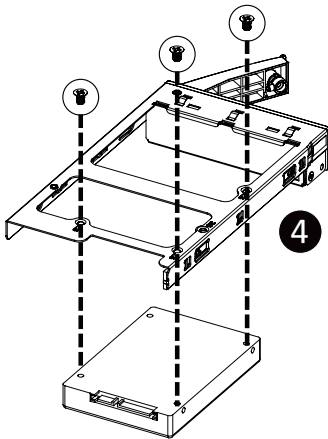
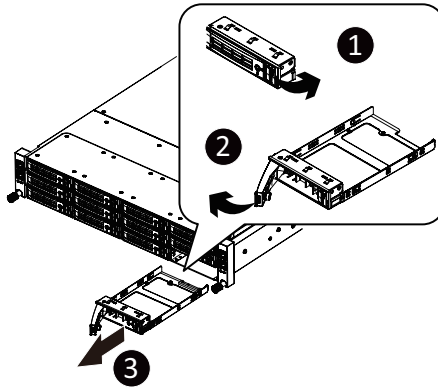
Follow these instructions to install a 3.5" hard disk drive:

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



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

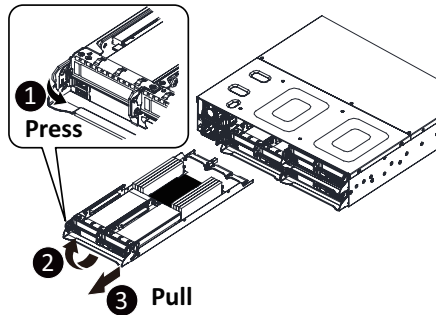
1. Press the release button.
2. Extend the locking lever.
3. Pull the locking lever in the direction indicated to remove the HDD tray.
4. Align the hard disk drive with the positioning stub on the HDD tray.
5. Secure the hard disk drive with five screws.
6. Reinsert the HDD tray into the slot and close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



## 3-2 Removing the Node

Follow these instructions to remove a node:

1. Press the release retaining clip on the right side of the node along the direction of the arrow,
2. Pulling out the node using its handle.



### 3-3 Removing Chassis Cover

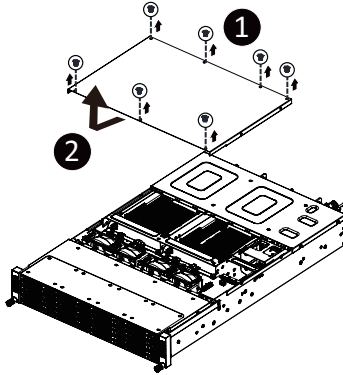


Before you remove or install the system cover

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

Follow these instructions to remove the system cover:

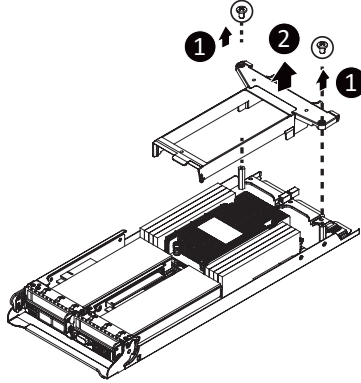
1. Loosen and remove the seven screws securing the middle cover.
2. Slide the cover to the rear of the system and remove the cover in the direction of the arrow.



### 3-4 Removing and Installing the Fan Duct

Follow these instructions to remove/install the fan duct:

1. Remove the four screws securing the fan ducts.
2. Lift up to remove the fan ducts
3. To install the fan duct, align the fan duct with the guiding groove. Push down the fan duct into chassis until its firmly seats, then install the four screws to secure the fan ducts in place.



## 3-5 Installing the CPU and Heat Sink



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

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



### **WARNING!**

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

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

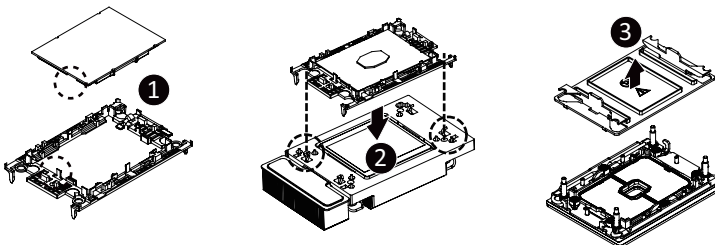
1. Align the processor to the carrier so that the gold triangle on the processor aligns with the triangle on the carrier, and then install the processor into the carrier.

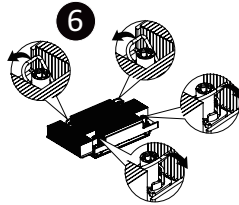
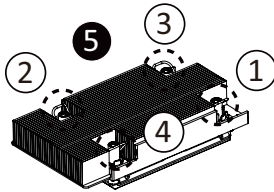
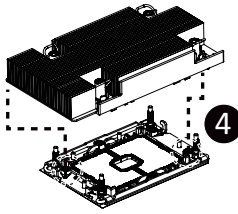
**NOTE:** Apply thermal compound evenly on the top of the CPU.

2. Carefully flip the heatsink over. Align the carrier assembly so that the triangle on the carrier aligns with the triangle on the heatsink, and then install the carrier assembly onto the bottom of the heatsink.
3. Remove the CPU socket cover.

**NOTE:** Save and replace the CPU socket cover if the processor is removed from its socket.

4. Align the heatsink to the CPU socket using the guide pins and make sure the gold triangle is in the correct orientation. Then place the heatsink onto the top of the CPU socket.
  5. Secure the heatsink by tightening the screws in sequential order (1→2→3→4).
- NOTE:** When removing the heatsink, loosen the screws in reverse order (4→3→2→1).





- To install/remove the Intel heatsink use a T30-Lobe screwdriver or drill bit with a screw torque of 8.0 +/- 0.5kgf\*cm (8lbf\*in).



## 3-6 Installing Memory

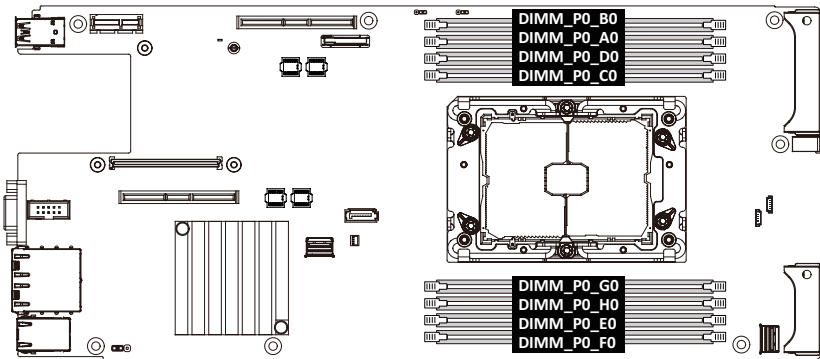


Read the following guidelines before you begin to install the memory:

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

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

This motherboard provides 8 DDR4 memory sockets and supports Eight Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory. Enabling eight Channel memory mode will be eight times of the original memory bandwidth.



### 3-6-2 Installing the Memory

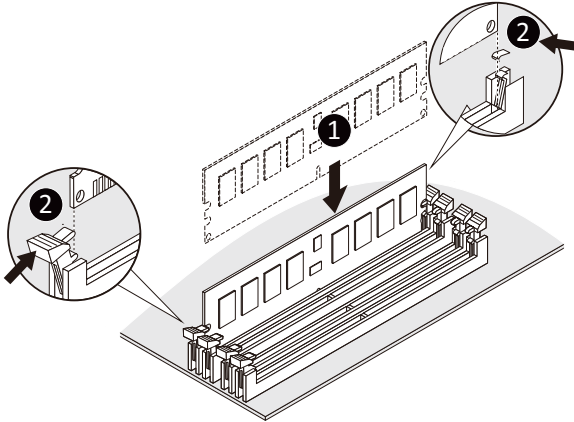


Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on this motherboard.

Follow these instructions to install the Memory:

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



### 3-6-3 Memory Population Table

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V); Slots per Channel(SPC) and DIMM per Channel (DPC)
		8Gb	16Gb	1DPC 1.2V
RDIMM	SRx8	8GB	16GB	3200
RDIMM	SRx4	16GB	32GB	
RDIMM	DRx8	16GB	32GB	
RDIMM	DRx4	32GB	64GB	
RDIMM 3DS	(4R/8R)x4	2H-64GB	2H-128GB	
		4H-128GB	4H-256GB	
LRDIMM	QRx4	64GB	128GB	
LRDIMM 3DS	(4R/8R)x4	4H-128GB	2H-128GB	
			4H-256GB	

NOTE!

- DIMM must be populated in sequential alphabetic order, starting with DIMM0.
- When only one DIMM is used, it must be populated in memory slot DIMM0.

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

Memory Q'ty	CPU0							
	B0	A0	D0	C0	G0	H0	E0	F0
1 DIMM		v						
2 DIMM		v					v	
4 DIMM		v		v	v		v	
8 DIMM	v	v	v	v	v	v	v	v

**NOTE!**

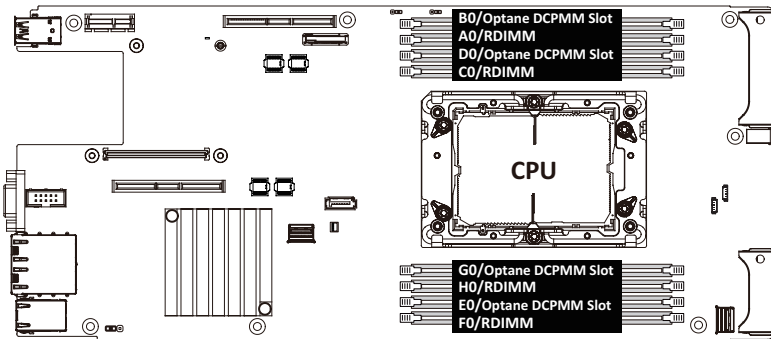
- There should be at least one DDR4 DIMM per socket.
- If only one DIMM is populated in a channel, then populate it in the slot furthest away from CPU of that channel.
- Channel 0's on each memory controller must be populated with same total capacity per channel (if populated).

### 3-6-5 Intel Optane DCPMM DIMM Population Rule

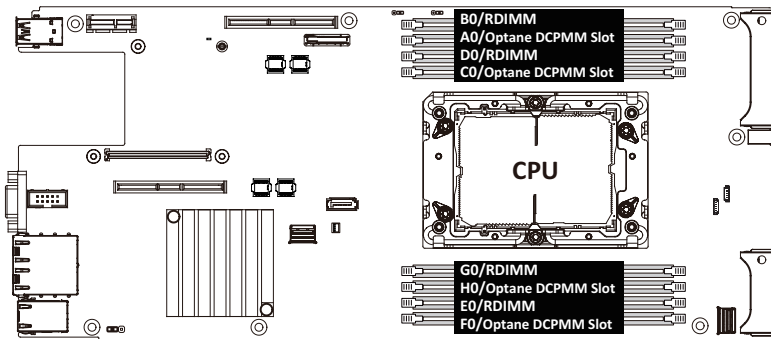
Thermal conditions for DCPMM DIMM support:

- The ambient temperature must be at or below 35°C
- The 3rd Generation Intel® Xeon® Scalable Processors used must have a maximum TDP of 270W
- A maximum of 4 pcs 512G DCPMM may be installed
  - You must install one RDIMM into any slot #0 of CPU0 before installing the DCPMM.
  - The DCPMM must be installed into the DIMM slot #0 next to the corresponding RDIMM in slot #0 (e.g. if RDIMM is installed into DIMM slot A0, the DCPMM must be installed into DIMM slot B0)

#### Configuration 1



#### Configuration 2



### 3-7 Installing the PCI Expansion Card



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

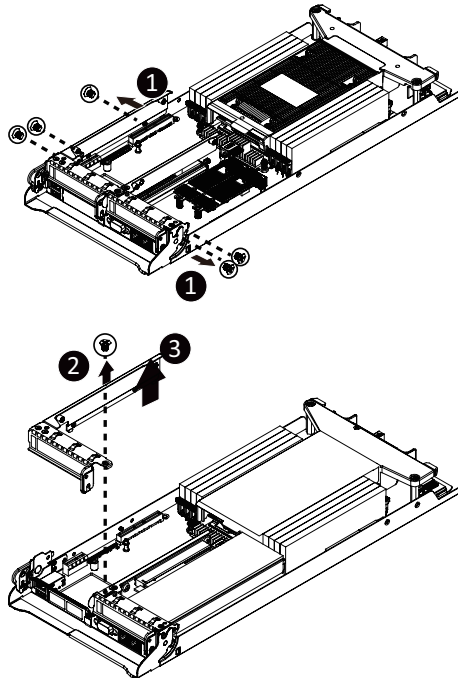
Failure to observe these warnings could result in personal injury or damage to equipment.

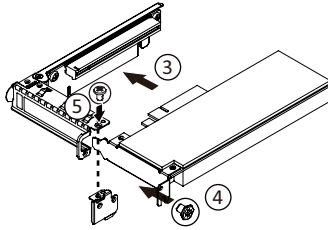
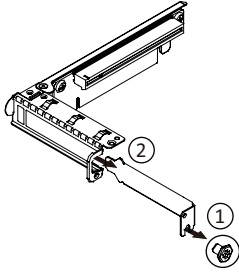


- The PCI riser assembly does not include a riser card or any cabling as standard. To install a PCI card, a riser card must be installed.

Follow these instructions to install the left PCI Expansion card:

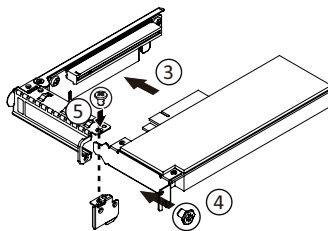
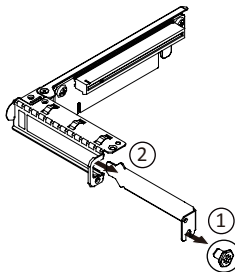
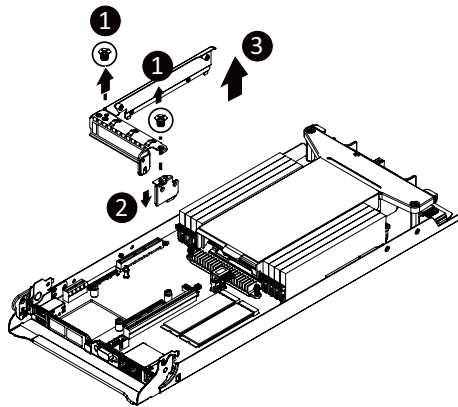
1. Remove the five screws securing the riser bracket to the system.
2. Remove the the screw securing the riser bracket to the system.
3. Lift up the riser bracket out of system.
4. Align the PCIe card to the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCI card connector.
5. Secure the PCIe card with a screw.
6. Reverse steps 1 - 3 to install the riser bracket back into the system.





**Follow these instructions to install the right PCI Expansion card:**

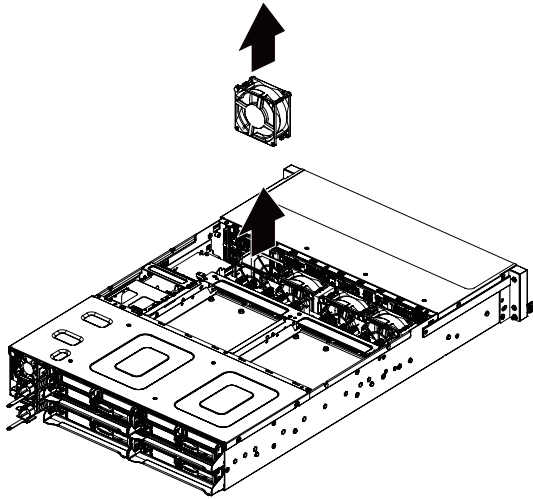
1. Remove the two screws on the riser bracket to the system.
2. Lift up the riser bracket out of system.
3. Remove the screw securing the side bracket to the riser bracket.
4. Remove the side bracket
5. Align the PCIe card to the riser guide slot and push in the direction of the arrow until the PCIe card sits in the PCI card connector.
6. Secure the PCIe card with a screw.
7. Install the side bracket to the riser bracket.
8. Secure the side bracket to the riser bracket with a screw.
9. Reverse steps 1 - 2 to install the riser bracket back into the system.



## 3-8 Replacing the Fan Module

Follow these instructions to replace the fan assembly:

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

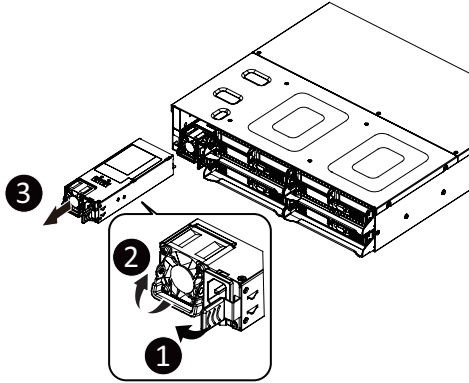




## 3-9 Replacing the Power Supply

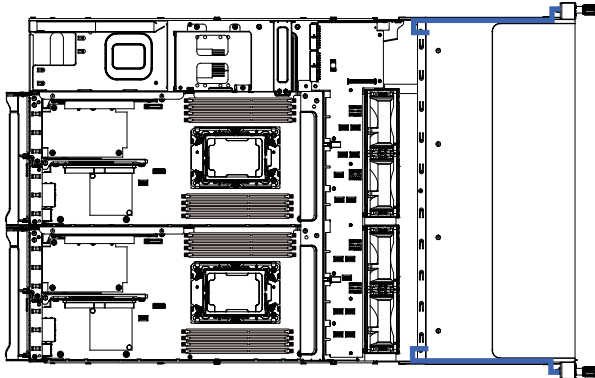
Follow these instructions to replace the power supply:

1. Pull up the power supply handle and press the retaining clip on the right side of the power supply along the direction of the arrow. At the same time, pull out the power supply by using its handle.
2. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.

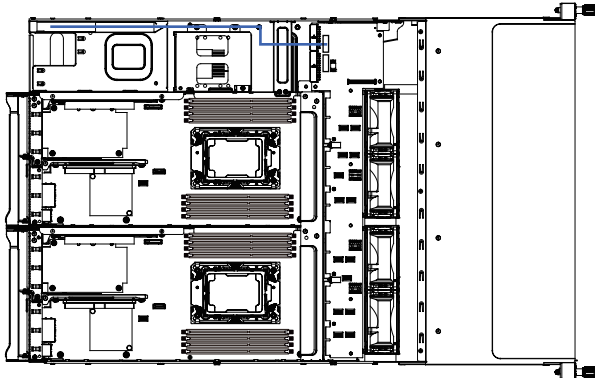


# 3-10 Cable Routing

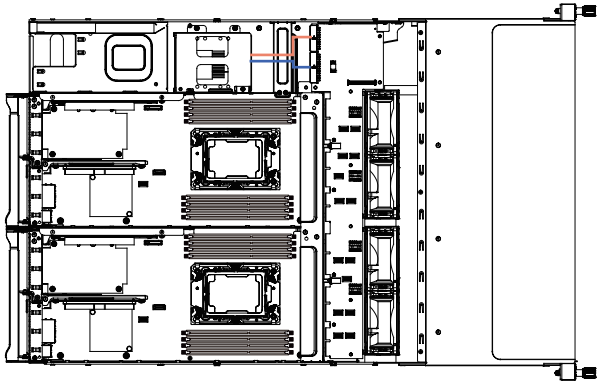
## Front Panel IO Cable



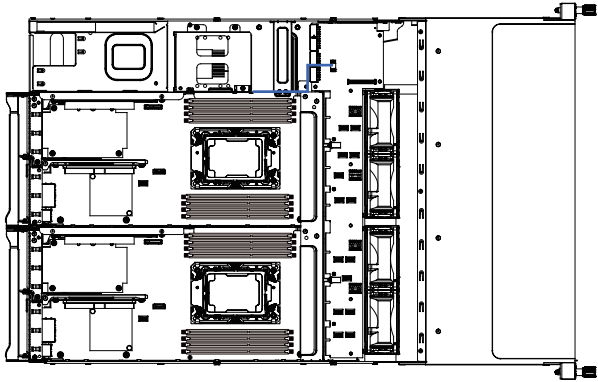
## Rear LAN Cable



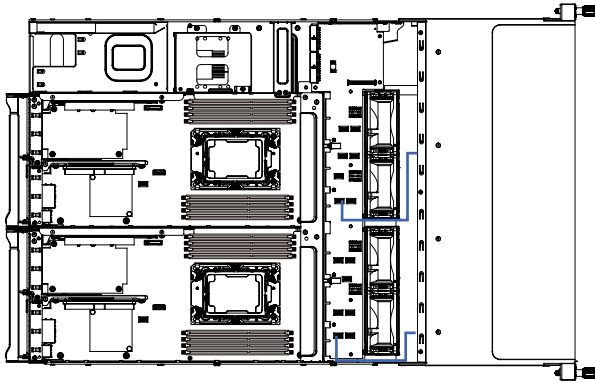
**HDD Back Plane Board Power Cable (Top/Bottom Middle Board)**



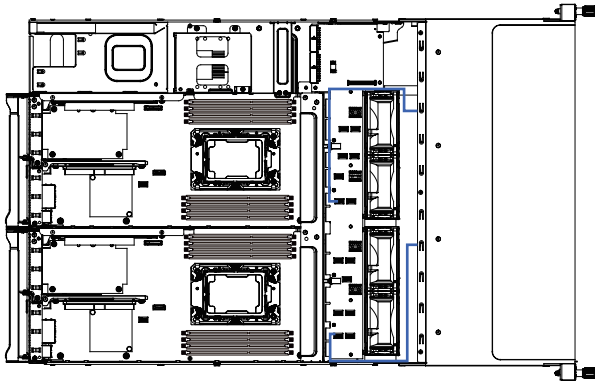
**HDD Back Plane Board Signal Cable**



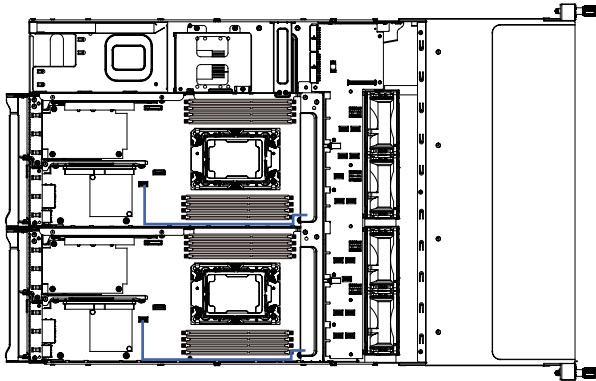
**On-Board SATA Cable (Top/Middle Board to Back Plane Board)**



**On-Board SATA Cable (Bottom/Middle Board to Back Plane Board)**



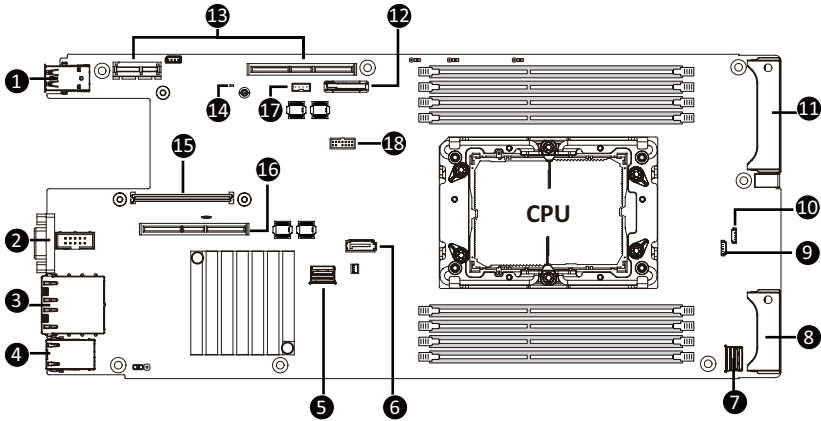
On-Board SATA Cable (Motherboard)





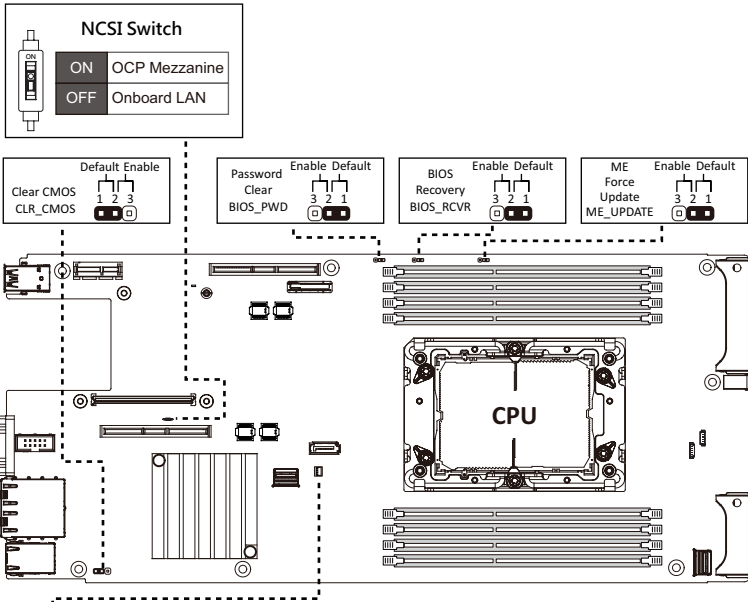
# Chapter 4 Motherboard Components

## 4-1 Motherboard Components



Item	Description
1	USB 3.0 Port x 2
2	VGA Port
3	GbE LAN Port x 2
4	Server Management LAN Port
5	SlimLine SAS Connector (SL4_SATA0/SATA)
6	SATA 6Gb/s Connector
7	SlimLine SAS Connector (SL4_SATA1/SATA)
8	Power & PCIe/SATA Connector
9	SGPIO Connector (SGPB1)
10	SGPIO Connector (SGPA1)
11	Power & PCIe/SATA Connector
12	System Battery
13	Riser Slot #1
14	BMC Readiness LED
15	OCP Mezzanine Connector (OCP 2.0/Gen3 x16)
16	Riser Slot #2
17	VROC Upgrade Module Connector
18	TPM Module Connector (SPI Interface)

# 4-2 Jumper Setting



MB_SW		ON	OFF
1	S3_MASK	Stop initial power on when BMC is not ready	Normal [Default]
2	PMBUS_SEL	PCH	BMC [Default]
3	SMB_SEL	BMC	PCH [Default]
4	ME_RCVR	ME Recovery mode	Normal [Default]



## 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.)

# 5-1 The Main Menu

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

## Main Menu Help

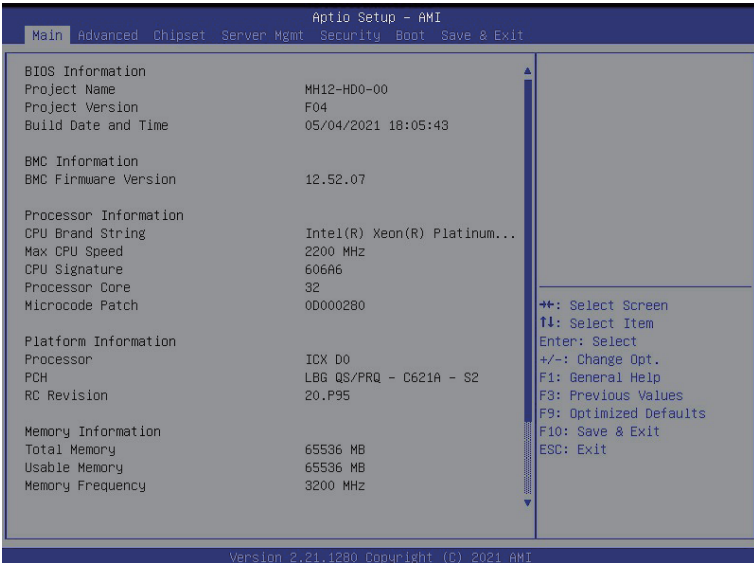
The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

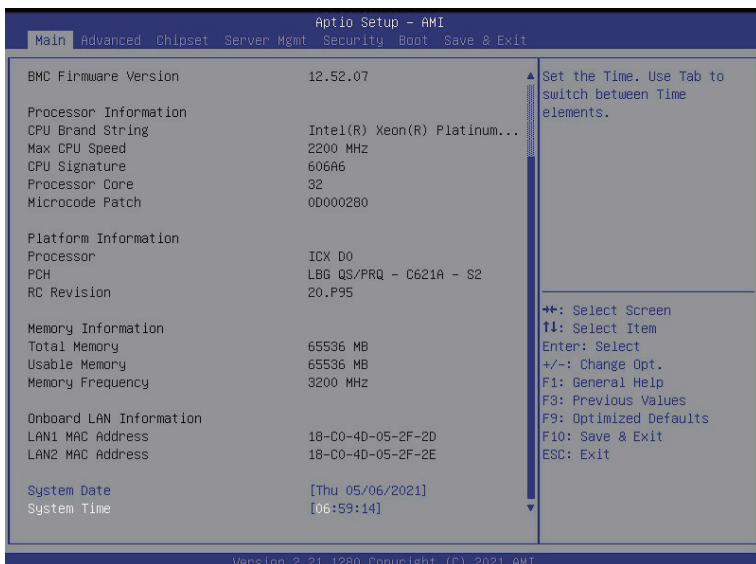
## Submenu Help

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



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





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

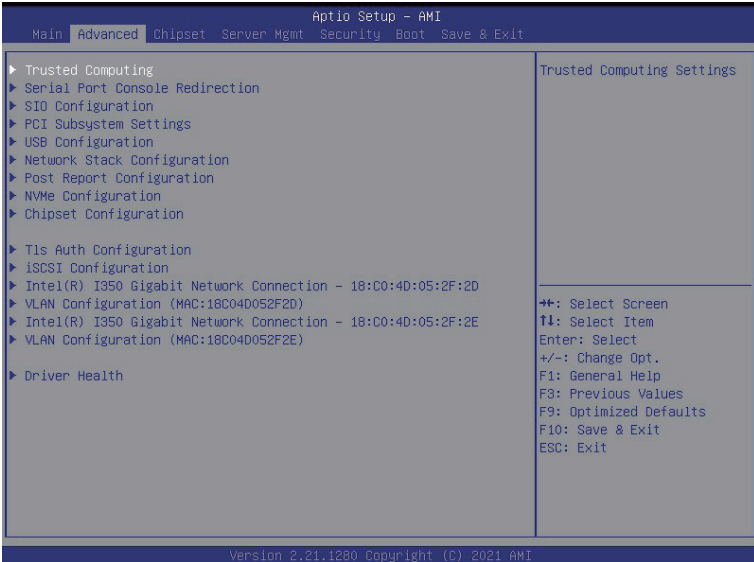
(Note1) This section will display capacity and frequency information of the memory that the customer has installed.

Parameter	Description
Onboard LAN Information	
LAN1 MAC Address <sup>(Note2)</sup>	Displays LAN MAC address information.
LAN2 MAC Address <sup>(Note2)</sup>	Displays LAN MAC address information.
System Time	Sets the system time following the hour-minute-second format.

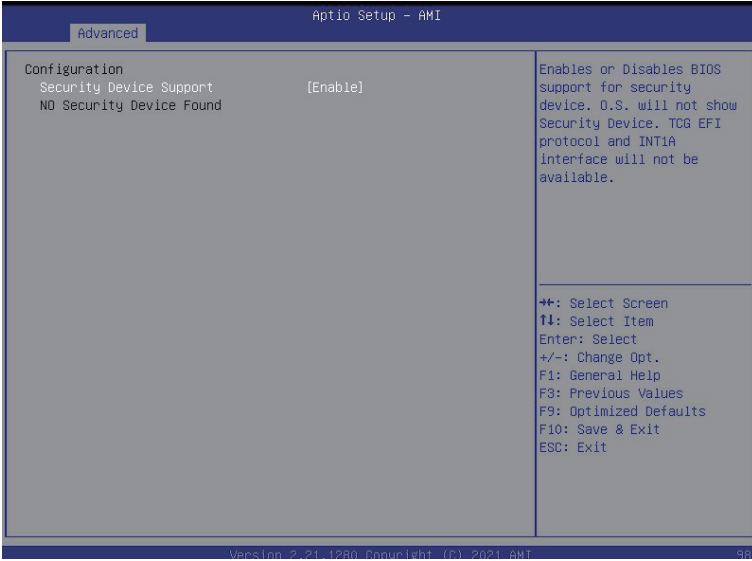
(Note2) The number of LAN ports listed will depend on the motherboard / system model.

## 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	
Security Device Support	Enable/Disable the TPM support feature. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Current Status Information	Displays current TPM status information.

## 5-2-2 Serial Port Console Redirection



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

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



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

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

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

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

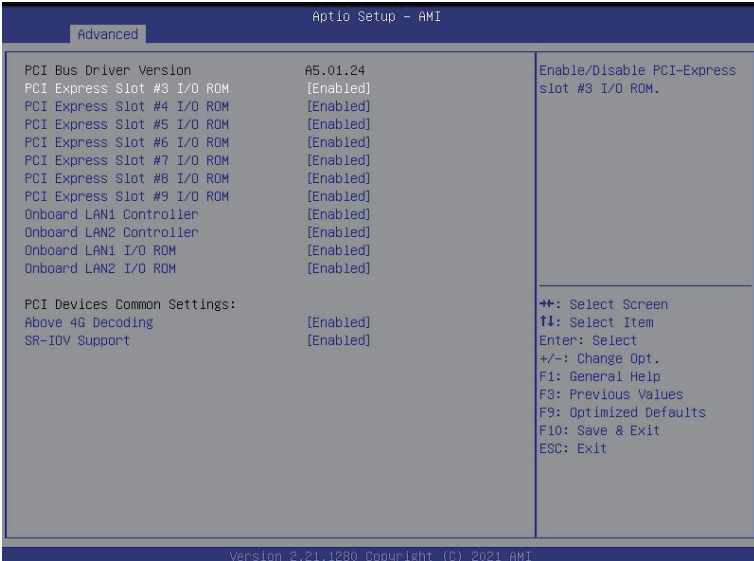
Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	<ul style="list-style-type: none"><li>◆ Flow Control<ul style="list-style-type: none"><li>– Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop'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

### 5-2-3 SIO Configuration



Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Use This Device <ul style="list-style-type: none"> <li>– When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port.</li> <li>– Options available: Enabled/Disabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Current: <ul style="list-style-type: none"> <li>– Displays the serial port base I/O address and IRQ.</li> </ul> </li> <li>◆ Possible: <ul style="list-style-type: none"> <li>– Configures the serial port base I/O address and IRQ.</li> </ul> </li> </ul>
[*Active*] Serial Port	Use Automatic Settings IO=3F8h; IRQ=4; DMA; IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; Default setting is <b>Use Automatic Settings</b> .

## 5-2-4 PCI Subsystem Settings

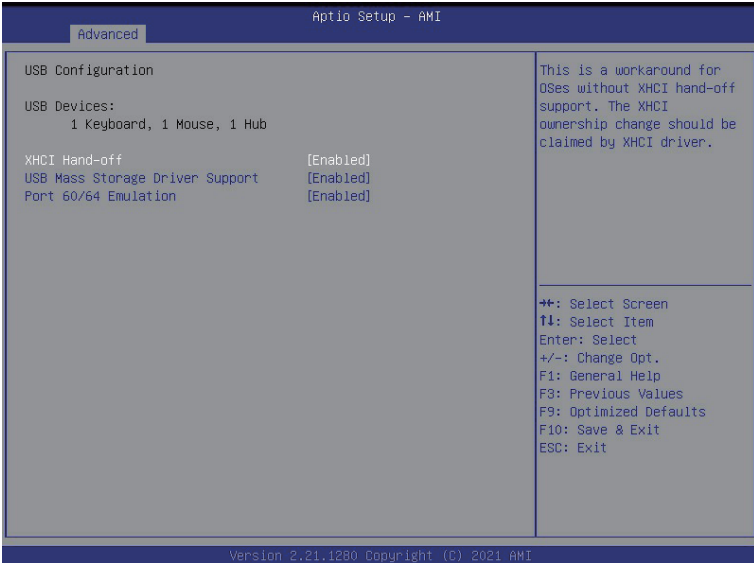


Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
Onboard LAN1 / LAN2 Controller <sup>(Note2)</sup>	Enable/Disable the onboard LAN1 / LAN2 devices. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Onboard LAN1 / LAN2 I/O ROM <sup>(Note2)</sup>	Enable/Disable the onboard LAN1 / LAN2 devices, and initializes device expansion ROM. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
PCI Express Slot # I/O ROM <sup>(Note1)</sup>	When enabled, this setting will initialize the device expansion ROM for the related PCI-E slot. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
PCI Devices Common Settings	
Above 4G Decoding	Enable/Disable memory mapped I/O to 4GB or greater address space (Above 4G Decoding). Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .

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

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

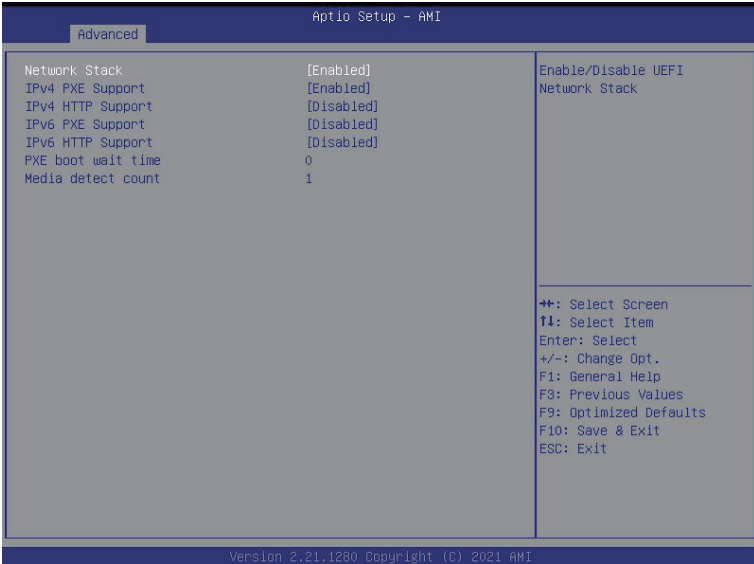
## 5-2-5 USB Configuration



Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
USB Mass Storage Driver Support <sup>(Note)</sup>	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Port 60/64 Emulation	Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OS. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .

(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. Default setting is <b>Enabled</b> .
IPv4 PXE Support	Enable/Disable the Ipv4 PXE feature. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
IPv4 HTTP Support	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .
IPv6 PXE Support	Enable/Disable the Ipv6 PXE feature. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .
IPv6 HTTP Support	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use <+> / <-> or numeric keys to set the value.
Media detect count	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. Default setting is <b>Enabled</b> .

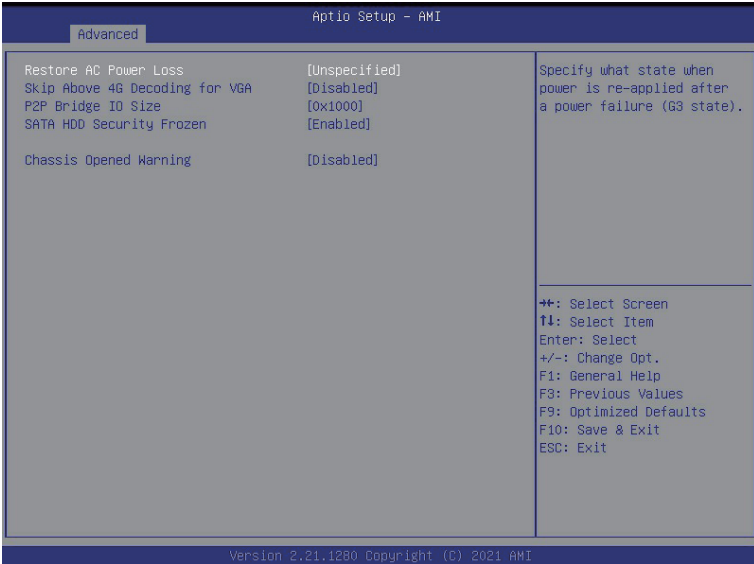


## 5-2-8 NVMe Configuration



Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system
NVMe OPROM Select	Options available: BIOS Build-In/NVMe Device. Default setting is <b>BIOS Build-In</b> .
NVMe #	Press [Enter] for advanced configuration.

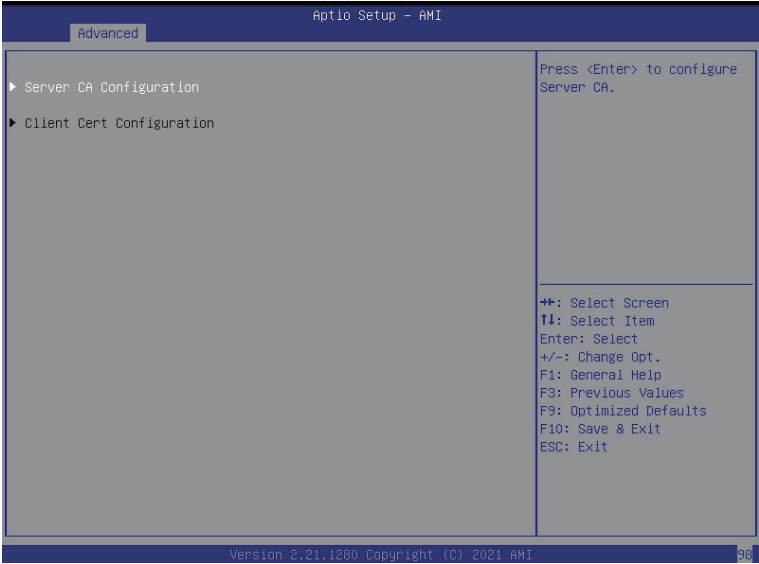
## 5-2-9 Chipset Configuration



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

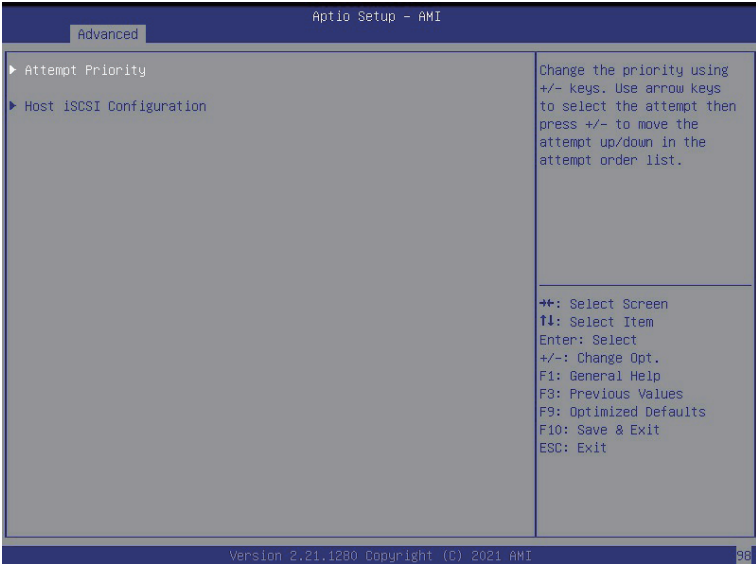
(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

## 5-2-10 Tls Auth Configuration



Parameter	Description
Save CA Configuration	Press [Enter] for configuration of advanced items.
Client Cert Configuration	Press [Enter] for configuration of advanced items.

## 5-2-11 iSCSI Configuration



Parameter	Description
Attempt Priority	Press [Enter] for configuration of advanced items.
Host iSCSI Configuration	Press [Enter] for configuration of advanced items.

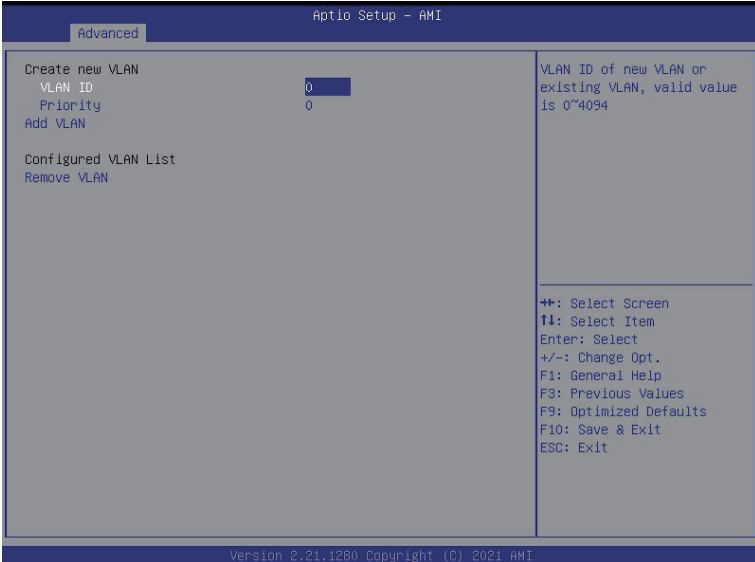
## 5-2-12 Intel(R) I350 Gigabit Network Connection

Advanced Aptio Setup - AMI		
<p>▶ NIC Configuration</p> <p>Blink LEDs 0</p> <p>UEFI Driver Intel(R) PRO/1000 7.5.11 ...            Adapter PBA 140422-008            Device Name Intel(R) I350 Gigabit Net...            Chip Type Intel I350            PCI Device ID 1521            PCI Address 02:00:00</p> <p>Link Status [Disconnected]</p> <p>MAC Address 18:00:40:8F:FF:D1            Virtual MAC Address 00:00:00:00:00:00</p>		<p>Click to configure the network device port.</p> <hr/> <p>→+: Select Screen            ↑↓: Select Item            Enter: Select            +/-: Change Opt.            F1: General Help            F3: Previous Values            F9: Optimized Defaults            F10: Save &amp; Exit            ESC: Exit</p>
Version 2.21.1280 Copyright (C) 2021 AMI		

Advanced Aptio Setup - AMI		
<p>Link Speed [Auto Negotiated]            Wake On LAN [Enabled]</p>		<p>Specifies the port speed used for the selected boot protocol.</p> <hr/> <p>→+: Select Screen            ↑↓: Select Item            Enter: Select            +/-: Change Opt.            F1: General Help            F3: Previous Values            F9: Optimized Defaults            F10: Save &amp; Exit            ESC: Exit</p>
Version 2.21.1280 Copyright (C) 2021 AMI		

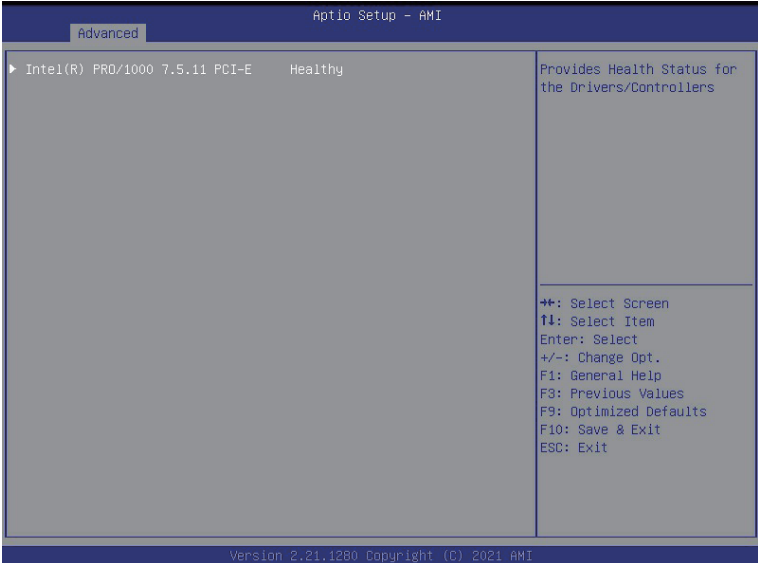
Parameter	Description
NIC Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Link Speed <ul style="list-style-type: none"> <li>– Allows for automatic link speed adjustment.</li> <li>– Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full,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

## 5-2-13 VLAN Configuration



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

## 5-2-14 Driver Health



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

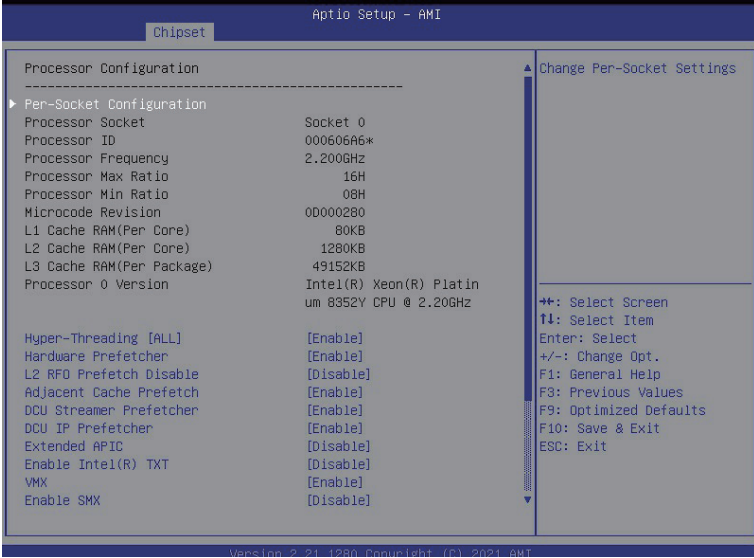


### 5-3 Chipset Setup Menu

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



### 5-3-1 Processor Configuration



Parameter	Description
Processor Configuration	
Pre-Socket Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ CPU Socket 0 Configuration <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items.</li> </ul> </li> <li>◆ Core Disable Bitmap(Hex) <ul style="list-style-type: none"> <li>– Number of Cores to enable. 0 means all cores. FFFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.</li> </ul> </li> </ul>
Processor Socket / Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM / L2 Cache RAM / L3 Cache RAM / Processor Version	Displays the technical specifications for the installed processor(s).
Hyper-Threading [All]	<p>The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance.</p> <p>Options available: Enable/Disable. Default setting is <b>Enable</b>.</p>
Hardware Prefetcher	<p>Select whether to enable the speculative prefetch unit of the processor.</p> <p>Options available: Enable/Disable. Default setting is <b>Disable</b>.</p>
L2 RF0 Prefetch Disable	Options available: Enable/Disable. Default setting is <b>Disable</b> .
Adjacent Cache Prefetch	<p>When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched.</p> <p>Options available: Enable/Disable. Default setting is <b>Enable</b>.</p>
DCU Streamer Prefetcher	<p>Prefetches the next L1 data line based upon multiple loads in same cache line.</p> <p>Options available: Enable/Disable. Default setting is <b>Enable</b>.</p>
DCU IP Prefetcher	<p>Prefetches the next L1 Data line based upon sequential load history.</p> <p>Options available: Enable/Disable. Default setting is <b>Enable</b>.</p>
Extended APIC	<p>Enable/Disable extended APIC support. Note: This will enabled VT-d automatically if x2APIC is enabled.</p> <p>Options available: Enable/Disable. Default setting is <b>Disable</b>.</p>
Enable Intel(R) TXT	<p>Enable/Disable the Intel Trusted Execution Technology support function.</p> <p>Options available: Enable/Disable. Default setting is <b>Disable</b>.</p>

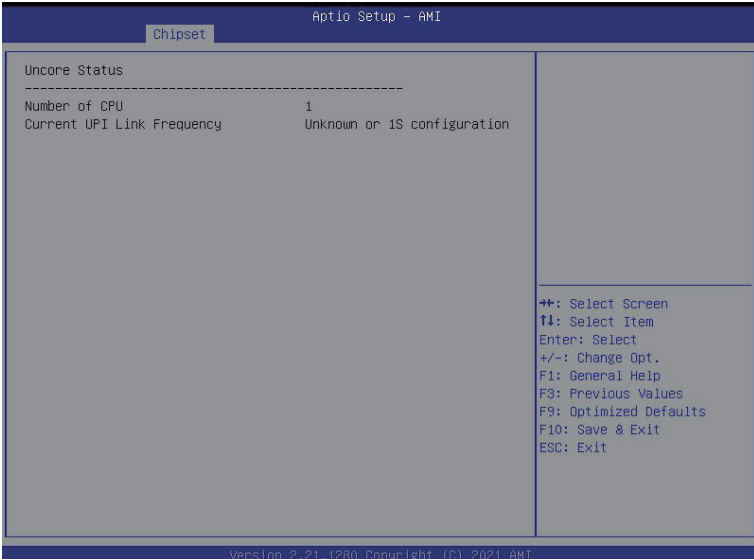
Parameter	Description
VMX (Vanderpool Technology)	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Enable SMX	Enable/Disable the Safer Mode Extensions Options available: Enable/Disable. Default setting is <b>Enable</b> .
AES-NI	Enable/Disable the AES-NI (Intel Advanced Encryption Standard New Instructions) support function. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Debug Coosent	ASD support. Options available: Enable/Disable. Default setting is <b>Disable</b> .
Total Memory Encryption	Enable/Disable Total Memory Encryption. Options available: Enable/Disable. Default setting is <b>Disabled</b> .

### 5-3-2 Common RefCode Configuration



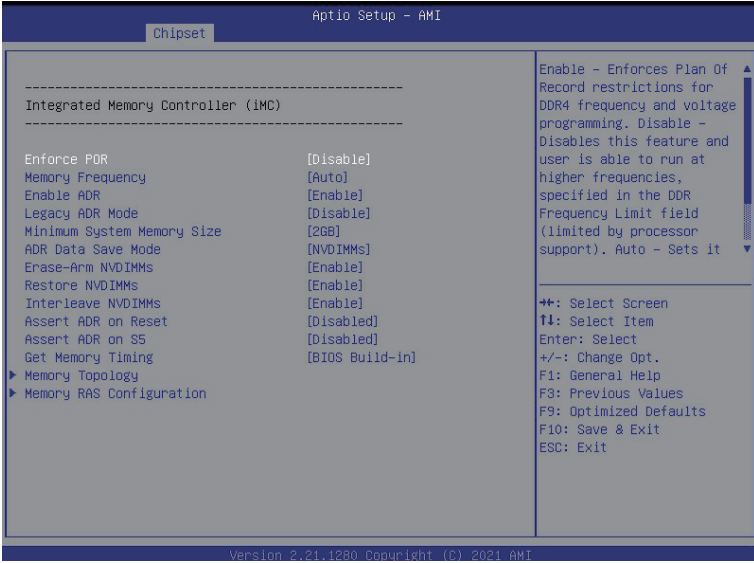
Parameter	Description
Common RefCode Configuration	
MMIO High Base	Selects the MMIO High Base setting. Options available: 56T, 40T, 32T, 24T, 16T, 4T, 1T/512G/3584T. Default setting is <b>4T</b> .
MMIO High Granularity Size	Selects the allocation size used to assign mmioh resources. Total mmioh space can be up to 32xgranularity. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation. Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is <b>1024G</b> .
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enable, Disable. Default setting is <b>Disable</b> .
Numa (Non-Uniform Memory Access)	Enable/Disable Non-uniform Memory Access (NUMA) support to improve the system performance. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Virtual Numa	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors. Options available: Enable/Disable. Default setting is <b>Enable</b> .

### 5-3-3 UPI Configuration



Parameter	Description
UPI Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Uncore Status <ul style="list-style-type: none"> <li>– Press [Enter] to view the UPI status.</li> </ul> </li> <li>◆ Link Frequency Select <ul style="list-style-type: none"> <li>– Selects the UPI link frequency.</li> <li>– Options available: 9.6GB/s, 10.4GB/s, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ SNC (Sub NUMA) <ul style="list-style-type: none"> <li>– Enable/Disable Sub NUMA Cluster function.</li> <li>– Options available: Disable, Enable SNC2 (2-clusters). Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Stale AtoS <ul style="list-style-type: none"> <li>– Enable/Disable Stale A to S directory optimization.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ LLC dead line alloc <ul style="list-style-type: none"> <li>– Enable/Disable fill dead lines in LLC.</li> <li>– Options available: Disable, Enable, Auto. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Uncore General Configuration	

### 5-3-4 Memory Configuration



Parameter	Description
<b>Integrated Memory Controller (iMC)</b>	
Enforce POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. When set to Auto, the system sets it to the MRC default settings. Options available: POR, Disable. Default setting is <b>Disable</b> .
Memory Frequency	Configures the maximum memory frequency. Options available: Auto, 1200, 1333, 1400, 1600, 1800, 1866, 2000, 2133, 2200, 2400, 2600, 2666, 2800, 2933, 3000, 3200, 3400-OvrClk, 3466-OvrClk, 3600-OvrClk, 3733-OvrClk, 3800-OvrClk, 4000-OvrClk, 4200-OvrClk, 4266-OvrClk, 4400-OvrClk, 4800-OvrClk. Default setting is <b>Auto</b> .
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable/Disable. Default setting is <b>Enable</b> .

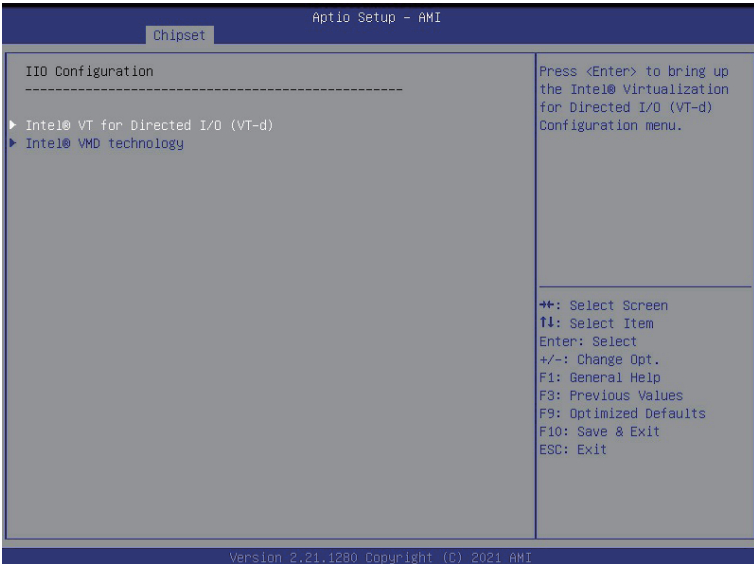
Parameter	Description
Legacy ADR Mode	Enable/Disable the Legacy ADR Mode. Options available: Enable/Disable. Default setting is <b>Disable</b> .
Minimum System Memory Size	Minimum system memory size assigned as system memory when only JEDEC NVDIMMs are present. Options available: 2GB, 4GB, 6GB, 8GB. Default setting is <b>8GB</b> .
ADR Data Save Mode	Specifies the Data Save Mode for ADR. Batterybacked or Type 01 NVDIMM. Options available: Disable, Batterybacked DIMMs, NVDIMMs. Default setting is <b>NVDIMMs</b> .
Erase-ARM NVDIMMs	Enable/Disable Erasing and Arming NVDIMMs. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Restore NVDIMMs	Enable/Disable Automatic restoring of NVDIMMs. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Interleave NVDIMMs	Controls if NVDIMMs are interleaved together or not. Options available: Enable/Disable. Default setting is <b>Enable</b> .
Assert ADR on Reset	Enable/Disable Assert ADR on Reset. Options available: Enable/Disable. Default setting is <b>Disable</b> .
Assert ADR on S5	Enable/Disable Assert ADR on S5. Options available: Enable/Disable. Default setting is <b>Disable</b> .
Get Memory Timing	Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .



Parameter	Description
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory RAS Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ RAS Type <ul style="list-style-type: none"> <li>– Displays the RAS type.</li> </ul> </li> <li>◆ New SDDC Mode <ul style="list-style-type: none"> <li>– Enable 48B SDDC ECC from ICX C0 Onwards.</li> <li>– Options available: Disabled/Enabled. Default setting is <b>Enabled</b>.</li> </ul> </li> <li>◆ Mirror Mode <ul style="list-style-type: none"> <li>– Full Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect.</li> <li>– Options available: Disabled/ Full Mirror Mode/Partial Mirror Mode. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Correctable Error Threshold <ul style="list-style-type: none"> <li>– Correctable Error Threshold (1-32767) used for sparing, tagging, and leaky bucket.</li> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Trigger SW Error Threshold <ul style="list-style-type: none"> <li>– Enable/Disable Sparing trigger SW Error Match Threshold..</li> <li>– Options available: Disabled/ Full Mirror Mode/Partial Mirror Mode. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Sparing SW Error Match Threshold <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Correctable Error Time Window. <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket time window based ini. <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket low bit <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ Leaky bucket high bit <ul style="list-style-type: none"> <li>– Press the &lt;+&gt; / &lt;-&gt; keys to increase or decrease the desired values.</li> </ul> </li> <li>◆ ADDDC Sparing <ul style="list-style-type: none"> <li>– Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ Column Correction Disable <ul style="list-style-type: none"> <li>– Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

Parameter	Description
Memory RAS Configuration	<ul style="list-style-type: none"><li>◆ ADDDC Sparing<ul style="list-style-type: none"><li>– Default setting is <b>Disabled</b>.</li></ul></li><li>◆ Column Correction Disable<ul style="list-style-type: none"><li>– Default setting is <b>Disable</b>.</li></ul></li><li>◆ Set PMem Die Sparing<ul style="list-style-type: none"><li>– Default setting is <b>Enabled</b>.</li></ul></li><li>◆ Patrol Scrub<ul style="list-style-type: none"><li>– Default setting is <b>Disabled</b>.</li></ul></li></ul>

### 5-3-5 IIO Configuration

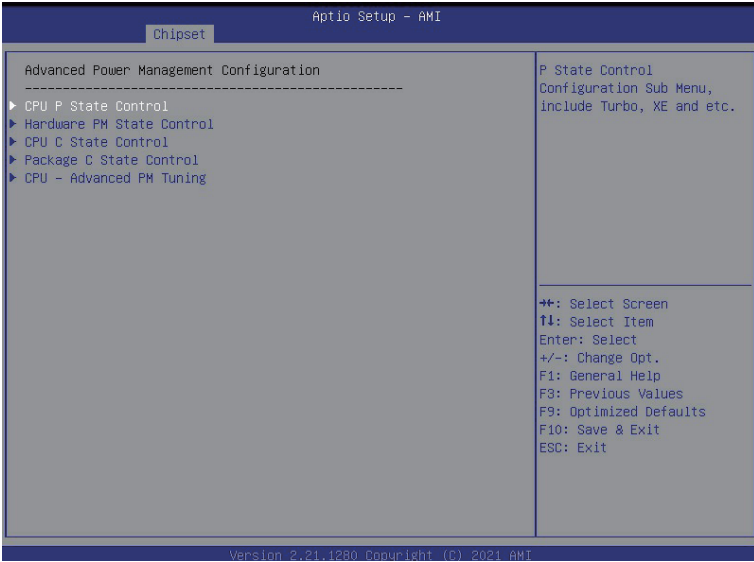


Parameter	Description
IIO Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel® VT for Directed I/O (VT-d) <ul style="list-style-type: none"> <li>– Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ ACS Control <ul style="list-style-type: none"> <li>– Enable: Programs ACS only to Chipset PCIe Root Ports Bridges.</li> <li>– Disable: Programs ACS to all PCIe bridges.</li> <li>– Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ DMA Control Opt-In Flag <ul style="list-style-type: none"> <li>– Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG AG in DRMA table in ACPI. Not compatible with Direct Device Assignment (DDA).</li> <li>– Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Interrupt Remapping <ul style="list-style-type: none"> <li>– Enable/Disable the interrupt remapping support function.</li> <li>– Options available: Enable/Disable/Auto. Default setting is <b>Auto</b>.</li> </ul> </li> </ul>
Intel® VT for Directed I/O (VT-d)	

Parameter	Description
Intel® VT for Directed I/O (VT-d) (continued)	<ul style="list-style-type: none"> <li>◆ X2APIC Opt Out <ul style="list-style-type: none"> <li>– Enable/Disable X2APIC Opt Out bit.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Pre-boot DMA Protection <ul style="list-style-type: none"> <li>– Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and if VTD_INFO_PPI is installed in PEI.)</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>
Intel® VMD technology	<p data-bbox="373 346 713 373">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Intel® VMD technology<sup>(Note1)</sup></li> <li>◆ Intel® VMD Configuration <ul style="list-style-type: none"> <li>– Enable/Disable the Intel VMD support function.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

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

### 5-3-6 Advanced Power Management Configuration



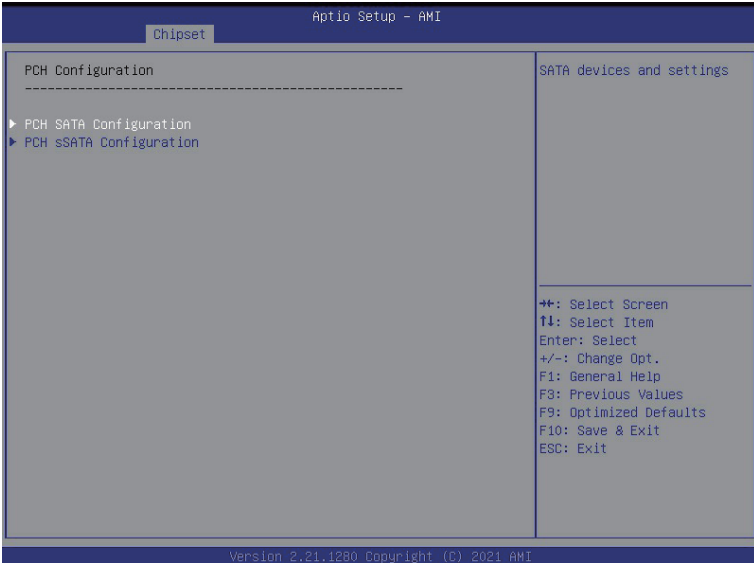
Parameter	Description
Advanced Power Management Configuration	

Parameter	Description
CPU P State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ SpeedStep (Pstates) <ul style="list-style-type: none"> <li>– Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Activate SST-BF<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– This option allows SST-BT to be enabled.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Configure SST-BF <ul style="list-style-type: none"> <li>– This option allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Turbo Mode <ul style="list-style-type: none"> <li>– 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.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>

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

Parameter	Description
Hardware PM State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Hardware P-States <ul style="list-style-type: none"> <li>– When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States).</li> <li>– In Native mode, the processor hardware chooses a P-state based on OS guidance.</li> <li>– In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance).</li> <li>– Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is <b>Native Mode</b>.</li> </ul> </li> </ul>
CPU C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Enable Monitor MWAIT <ul style="list-style-type: none"> <li>– Allows Monitor and MWAIT instructions.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ CPU C6 Report <ul style="list-style-type: none"> <li>– Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced power-saving state than C1.</li> <li>– Options available: Disable/Enable/Auto. Default setting is <b>Auto</b>.</li> </ul> </li> <li>◆ Enhanced Halt State (C1E) <ul style="list-style-type: none"> <li>– Core C1E auto promotion control. Takes effect after reboot.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Package C State Control	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Package C State <ul style="list-style-type: none"> <li>– Configures the state for the C-State package limit.</li> <li>– Options available: C0/C1 state, C2 state, C6(non Retention) state, , Auto. Default setting is <b>C0/C1 state</b>.</li> </ul> </li> </ul>
CPU-Advanced PM Tuning	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ Energy Perf BIAS <ul style="list-style-type: none"> <li>– Press [Enter] to configure advanced items.</li> </ul> </li> <li>◆ Power Performance Tuning <ul style="list-style-type: none"> <li>– Option available: OS Controls EPB/BIOS Controls EPB/PECI Controls EPB. Default setting is <b>BIOS Controls EPB</b>.</li> </ul> </li> <li>◆ ENERGY_PERF_BIAS_CFG mode<sup>(Note)</sup> <ul style="list-style-type: none"> <li>– Option available: Performance/Balanced Performance/Balanced Power/Power.</li> <li>– Default setting is <b>Performance</b>.</li> </ul> </li> </ul>

### 5-3-7 PCH Configuration



Parameter	Description
PCH Configuration	<p>Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li>◆ SATA Controller               <ul style="list-style-type: none"> <li>- Enable/Disable SATA controller.</li> <li>- Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Configure SATA as               <ul style="list-style-type: none"> <li>- Configures on chip SATA type.</li> <li>- AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time.</li> </ul> </li> </ul>
PCH SATA Configuration	<ul style="list-style-type: none"> <li>- RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time.</li> <li>- Options available: AHCI/RAID. Default setting is <b>AHCI</b>.</li> <li>◆ Alternate Device ID on RAID<sup>(Note 1)</sup> <ul style="list-style-type: none"> <li>- Enable/Disable Alternate Device ID on RAID mode.</li> <li>- Options available: Enable/Disable. Default setting is Disabled</li> </ul> </li> <li>◆ SATA Port 0/1/2/3/4/5/6/7               <ul style="list-style-type: none"> <li>- The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type.</li> </ul> </li> </ul>

(Note 1) Only appears when HDD sets to **RAID Mode**.



Parameter	Description
PCH SATA Configuration (continued)	<ul style="list-style-type: none"> <li>◆ Port 0/1/2/3/4/5/6/7 <ul style="list-style-type: none"> <li>– Enable/Disable Port 0/1/2/3/4/5/6/7 device.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Hot Plug (for Port 0/1/2/3/4/5/6/7)<sup>(Note 2)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable HDD Hot-Plug function.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Spin Up Device (for Port 0/1/2/3/4/5/6/7)<sup>(Note 2)</sup> <ul style="list-style-type: none"> <li>– On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>
PCH sSATA Configuration	<ul style="list-style-type: none"> <li>◆ sSATA Controller <ul style="list-style-type: none"> <li>– Enable/Disable sSATA controller.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Configure sSATA as <ul style="list-style-type: none"> <li>– Configures on chip SATA type.</li> <li>– AHCI Mode: When set to AHCI, the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time.</li> <li>– RAID Mode: When set to RAID, the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time.</li> <li>– Options available: AHCI/RAID. Default setting is <b>AHCI</b>.</li> </ul> </li> <li>◆ Alternate Device ID on RAID<sup>(Note 1)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable Alternate Device ID on RAID mode.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disabled</b>.</li> </ul> </li> <li>◆ sSATA Port 0/1/2/3 <ul style="list-style-type: none"> <li>– The category identifies sSATA hard drives that are installed in the computer. System will automatically detect HDD type.</li> </ul> </li> <li>◆ Port 0/1/2/3 <ul style="list-style-type: none"> <li>– Enable/Disable Port 0/1/2/3/4/5 device.</li> <li>– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Hot Plug (for Port 0/1/2/3/4/5)<sup>(Note 2)</sup> <ul style="list-style-type: none"> <li>– Enable/Disable HDD Hot-Plug function.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> <li>◆ Spin Up Device (for Port 0/1/2/3)<sup>(Note 2)</sup> <ul style="list-style-type: none"> <li>– On an edge detect from 0 to 1, the PCH starts a COM reset initialization to the device.</li> <li>– Options available: Enable/Disable. Default setting is <b>Disabled</b>.</li> </ul> </li> </ul>

(Note 1) Only appears when HDD sets to **RAID** Mode.

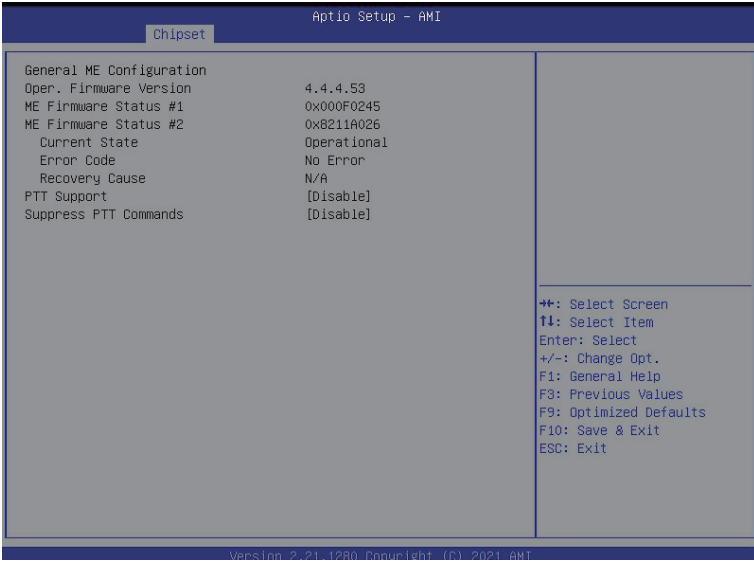
(Note 2) Only Supported when HDD is in **AHCI** or **RAID** Mode.

### 5-3-8 Miscellaneous Configuration



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

### 5-3-9 Server ME Configuration



Parameter	Description
General ME Configuration	
Oper. Firmware Version	Displays the operational firmware version.
ME Firmware Status #1/#2	Displays ME Firmware status information.
Current State (for ME Firmware)	Displays ME Firmware current status information.
Error Code (for ME Firmware)	Displays ME Firmware status error code.
Recovery Cause (for ME Firmware)	Displays ME Firmware recovery cause.
PTT Support	Displays if the system supports the Intel® Platform Trust Technology.
Suppress PTT Commands	Displays if the system supports to Bypass TPM2 commands submitting to PTT Firmware.

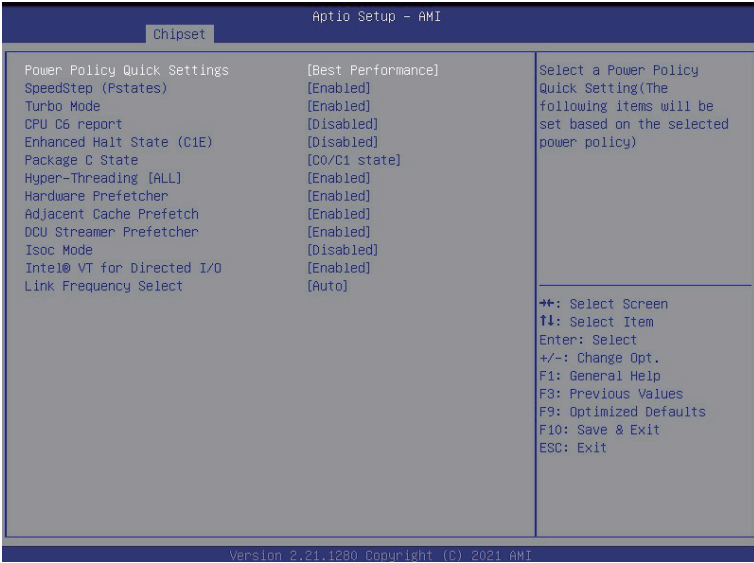
### 5-3-10 Runtime Error Logging



Parameter	Description
Runtime Error Logging	
System Errors	Enable/Disable system error logging function. Options available: Enable/Disable. Default setting is <b>Enable</b> .
S/W Error Injection Support	Enable/Disable software injection error logging function. Options available: Enable/Disable. Default setting is <b>Disable</b> .
Whea Settings	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ WHEA (Windows Hardware Error Architecture) Support <ul style="list-style-type: none"> <li>- Enable/Disable WHEA Support.</li> <li>- Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>
Memory Error Enabling	Press [Enter] to configure advanced items. <ul style="list-style-type: none"> <li>◆ Memory Error <ul style="list-style-type: none"> <li>- Enable/Disable Memory Error.</li> <li>- Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Memory Corrected Error <ul style="list-style-type: none"> <li>- Enable/Disable Memory Corrected Error.</li> <li>- Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li>◆ Uncorrected Error disable Memory <ul style="list-style-type: none"> <li>- Enable/Disable the Memory that triggers Uncorrected Error.</li> <li>- Options available: Enable/Disable. Default setting is <b>Disable</b>.</li> </ul> </li> </ul>

Parameter	Description
PCIe Error Enabling	<p data-bbox="309 142 642 166">Press [Enter] to configure advanced items.</p> <ul style="list-style-type: none"> <li data-bbox="309 170 841 225">◆ PCIE Error <ul style="list-style-type: none"> <li data-bbox="341 202 841 225">– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 230 923 313">◆ Uncorrected Error <ul style="list-style-type: none"> <li data-bbox="341 261 923 285">– Enables and escalates Uncorrectable/Recoverable Errors to error pins.</li> <li data-bbox="341 290 841 313">– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 318 841 401">◆ Fatal Error Enable <ul style="list-style-type: none"> <li data-bbox="341 349 749 373">– Enables and escalates Fatal Errors to error pins.</li> <li data-bbox="341 377 841 401">– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 406 841 489">◆ Assert NMI on SERR <ul style="list-style-type: none"> <li data-bbox="341 437 645 460">– Enable/Disable SERR propagation.</li> <li data-bbox="341 465 841 489">– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> <li data-bbox="309 493 841 577">◆ Assert NMI on PERR <ul style="list-style-type: none"> <li data-bbox="341 525 645 548">– Enable/Disable PERR propagation.</li> <li data-bbox="341 553 841 577">– Options available: Enable/Disable. Default setting is <b>Enable</b>.</li> </ul> </li> </ul>

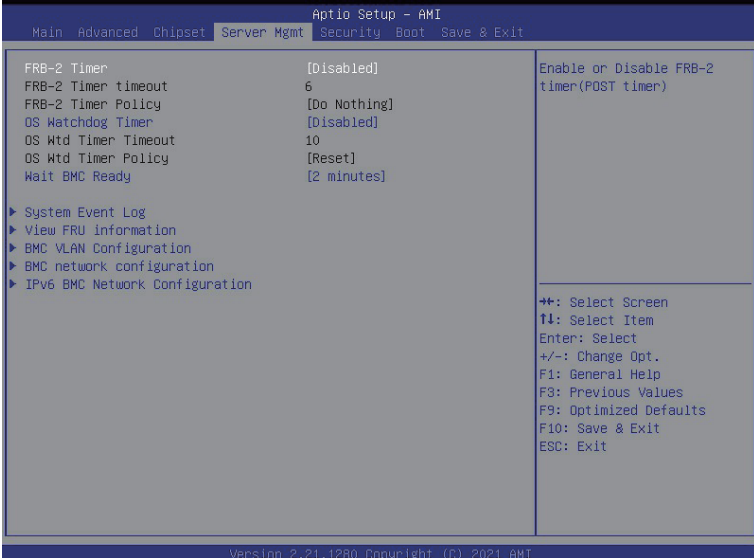
### 5-3-11 Power Policy



Parameter	Description
Power Policy Quick Settings	Selects a Power Policy Quick Setting. Options available: Standard, Best Performance, Energy Efficient, Turbo Lock. Default setting is <b>Best Performance</b> .
SpeedStep (Pstates)	Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Turbo Mode	When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
CPU C6 report	Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced powersaving state than C1. Options available: Disabled, Enabled, Auto. Default setting is <b>Disabled</b> .
Enhanced Halt State (C1E)	Core C1E auto promotion control. Takes effect after reboot. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .

Parameter	Description
Package C State	Configures the state for the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is <b>C0/C1 state</b> .
Hyper-Threading [ALL]	The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enabled/Disabled. Default setting is <b>Disabled</b> .
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
DCU Streamer Prefetcher	Prefetches the next L1 data line based upon multiple loads in same cache line. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enabled, Disabled. Default setting is <b>Disabled</b> .
Intel® VT for Directed I/O (VT-d)	Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. Options available: Enabled/Disabled. Default setting is <b>Enabled</b> .
Link Frequency Select	Selects the UPI link frequency. Options available: 9.6GB/s, 10.4GB/s, 11.2GB/s, Auto. Default setting is <b>Auto</b> .

## 5-4 Server Management Menu



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



Parameter	Description
OS Wtd Timer Policy	Configure OS Watchdog Timer Policy. Options available: Reset, Do Nothing, Power Down, Power Cycle. Default setting is <b>Reset</b> . <b>Please note that this item is configurable when OS Watchdog Timer is set to Enabled.</b>
Wait BMC Ready	POST wait BMC ready and reboot system. Options available: Disabled, 2 minutes, 4 minutes, 6 minutes. Default setting is <b>2 minutes</b> .
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the advanced items.
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.

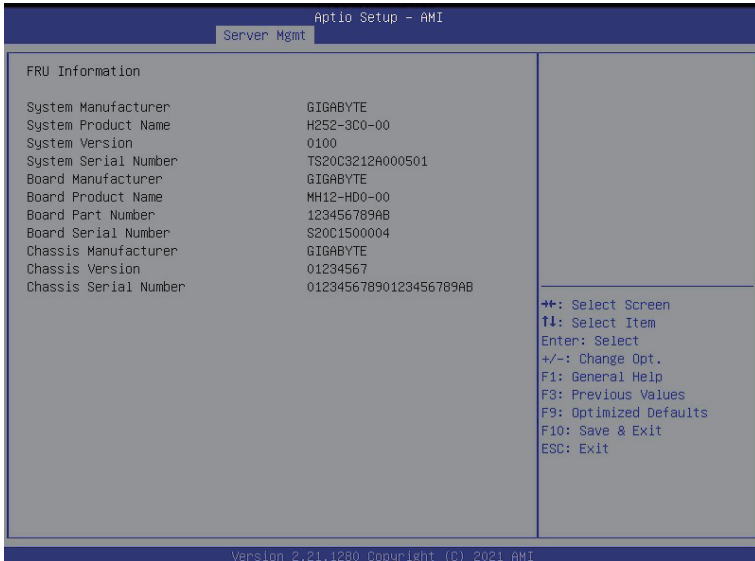
## 5-4-1 System Event Log



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

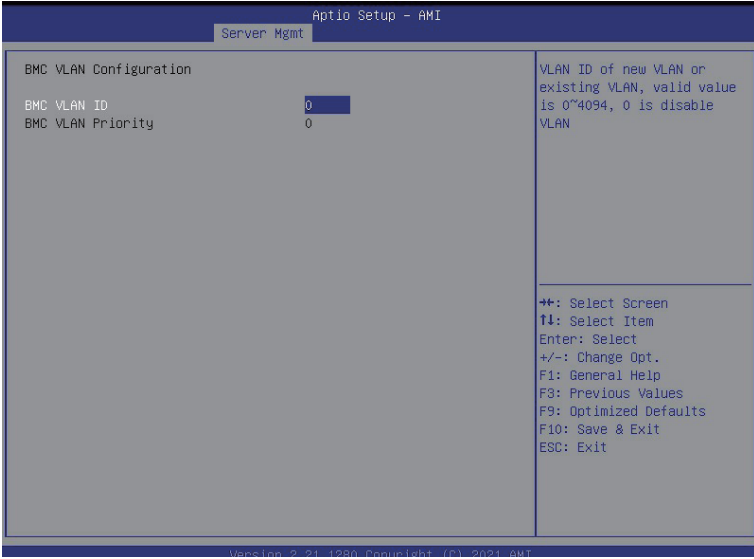
## 5-4-2 View FRU Information

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.



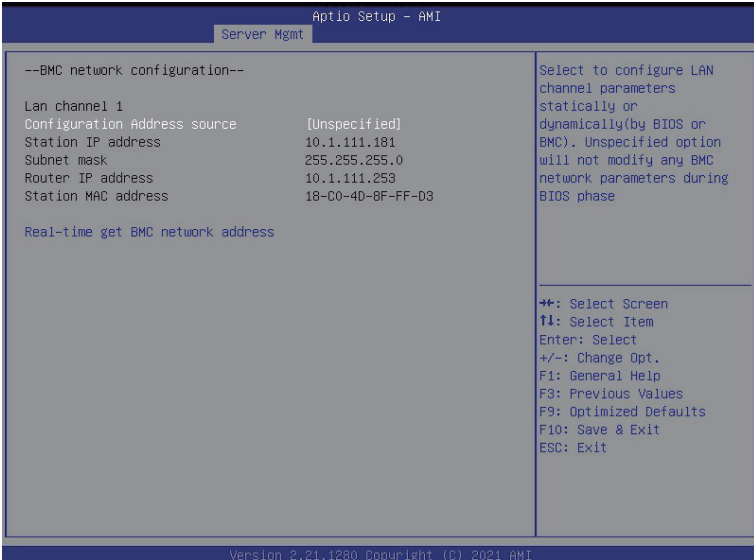
(Note) The model name will vary depends on the product you purchased

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

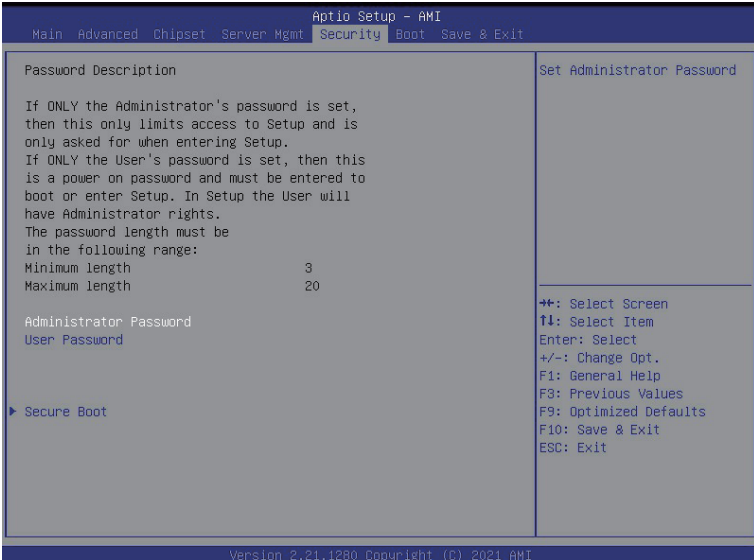
## 5-4-5 IPv6 BMC Network Configuration



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, Enable, Disable. Default setting is <b>Enable</b> .
IPv6 BMC Lan IP Address Source	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Options available: Unspecified, Static, Dynamic-Obtained by BMC running DHCP. Default setting is <b>Dynamic-Obtained by BMC running DHCP</b> .
IPv6 BMC Lan IP Address/Prefix Length	Check if the IPv6 BMC LAN IP address matches those displayed on the screen.

## 5-5 Security Menu

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



There are two types of passwords that you can set:

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

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

## 5-5-1 Secure Boot

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



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

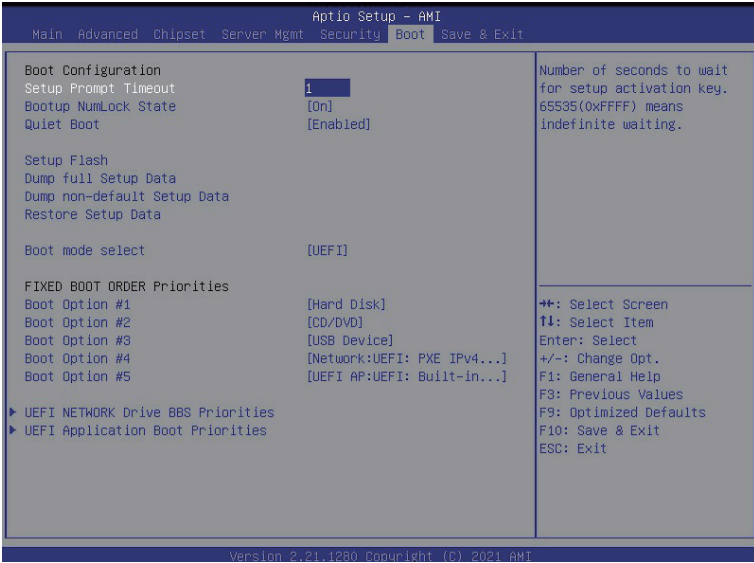
(Note) Advanced items prompt when this item is set to **Custom**.



Parameter	Description
Key Management	<p data-bbox="335 156 665 180">Press [Enter] to configure advanced items.</p> <p data-bbox="335 185 936 235"><b>Please note that this item is configurable when Secure Boot Mode is set to Custom.</b></p> <ul style="list-style-type: none"> <li data-bbox="335 243 946 352">◆ Factory Key Provision <ul style="list-style-type: none"> <li data-bbox="367 266 946 321">– Allows to provision factory default Secure Boot keys when system is in Setup Mode.</li> <li data-bbox="367 326 899 352">– Options available: Enabled/Disabled. Default setting is <b>Disabled</b>.</li> </ul> </li> <li data-bbox="335 357 931 431">◆ Restore Factory Keys <ul style="list-style-type: none"> <li data-bbox="367 381 931 404">– Installs all factory default keys. It will force the system in User Mode.</li> <li data-bbox="367 409 601 431">– Options available: Yes/No.</li> </ul> </li> <li data-bbox="335 435 904 517">◆ Enroll Efi Image <ul style="list-style-type: none"> <li data-bbox="367 459 904 517">– Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db).</li> </ul> </li> <li data-bbox="335 522 702 572">◆ Restore DB defaults <ul style="list-style-type: none"> <li data-bbox="367 545 702 572">– Restore DB variable to factory defaults.</li> </ul> </li> <li data-bbox="335 577 899 627">◆ Secure Boot variable <ul style="list-style-type: none"> <li data-bbox="367 600 899 627">– Displays the current status of the variables used for secure boot.</li> </ul> </li> <li data-bbox="335 631 803 736">◆ Platform Key (PK) <ul style="list-style-type: none"> <li data-bbox="367 655 803 682">– Displays the current status of the Platform Key (PK).</li> <li data-bbox="367 686 680 713">– Press [Enter] to configure a new PK.</li> <li data-bbox="367 718 611 736">– Options available: Set New.</li> </ul> </li> <li data-bbox="335 741 946 878">◆ Key Exchange Keys (KEK) <ul style="list-style-type: none"> <li data-bbox="367 765 946 846">– Displays the current status of the Key Exchange Key Database (KEK).</li> <li data-bbox="367 851 909 878">– Press [Enter] to configure a new KEK or load additional KEK from storage devices.</li> <li data-bbox="367 882 675 901">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 882 909 1019">◆ Authorized Signatures (DB) <ul style="list-style-type: none"> <li data-bbox="367 906 909 932">– Displays the current status of the Authorized Signature Database.</li> <li data-bbox="367 937 946 987">– Press [Enter] to configure a new DB or load additional DB from storage devices.</li> <li data-bbox="367 992 675 1019">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1023 904 1160">◆ Forbidden Signatures (DBX) <ul style="list-style-type: none"> <li data-bbox="367 1047 904 1074">– Displays the current status of the Forbidden Signature Database.</li> <li data-bbox="367 1078 893 1128">– Press [Enter] to configure a new dbx or load additional dbx from storage devices.</li> <li data-bbox="367 1133 675 1160">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1165 931 1301">◆ Authorized TimeStamps (DBT) <ul style="list-style-type: none"> <li data-bbox="367 1188 931 1215">– Displays the current status of the Authorized TimeStamps Database.</li> <li data-bbox="367 1219 909 1270">– Press [Enter] to configure a new DBT or load additional DBT from storage devices.</li> <li data-bbox="367 1274 675 1301">– Options available: Set New/Append.</li> </ul> </li> <li data-bbox="335 1306 920 1434">◆ OsRecovery Signatures <ul style="list-style-type: none"> <li data-bbox="367 1329 920 1356">– Displays the current status of the OsRecovery Signature Database.</li> <li data-bbox="367 1361 888 1411">– Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices.</li> <li data-bbox="367 1415 675 1434">– Options available: Set New/Append.</li> </ul> </li> </ul>

## 5-6 Boot Menu

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



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

Parameter	Description
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	<p data-bbox="399 200 955 227">Press [Enter] to configure the boot priority.</p> <p data-bbox="399 232 955 290">By default, the server searches for boot devices in the following sequence:</p> <ol data-bbox="436 294 955 435" style="list-style-type: none"> <li data-bbox="436 294 955 321">1. Hard drive.</li> <li data-bbox="436 326 955 352">2. CD-COM/DVD drive.</li> <li data-bbox="436 357 955 384">3. USB device.</li> <li data-bbox="436 388 955 415">4. Network.</li> <li data-bbox="436 420 955 435">5. UEFI.</li> </ol>
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot priority.
UEFI Application Boot Priorities	Press [Enter] to configure the boot priority.

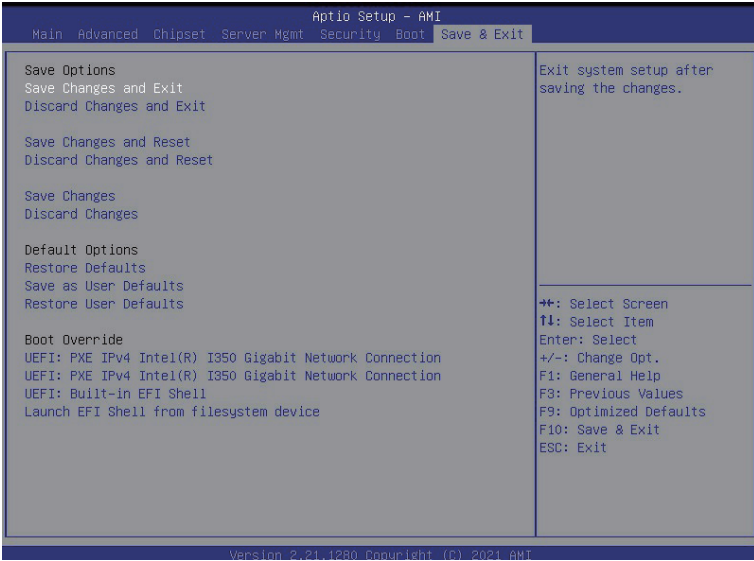
## 5-6-1 UEFI NETWORK Drive BBS Priorities

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



## 5-7 Save & Exit Menu

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



Parameter	Description
Save Options	
Save Changes and Exit	Saves changes made and closes the BIOS setup. Options available: Yes/No.
Discard Changes and Exit	Discards changes made and exits the BIOS setup. Options available: Yes/No.
Save Changes and Reset	Restarts the system after saving the changes made. Options available: Yes/No.
Discard Changes and Reset	Restarts the system without saving any changes. Options available: Yes/No.
Save Changes	Saves changes made in the BIOS setup. Options available: Yes/No.
Discard Changes	Discards changes made and closes the BIOS setup. Options available: Yes/No.

Parameter	Description
Default Options	
Restore Defaults	<p>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.</p> <p>Options available: Yes/No.</p>
Save as User Defaults	<p>Saves the changes made as the user default settings.</p> <p>Options available: Yes/No.</p>
Restore User Defaults	<p>Loads the user default settings for all BIOS setup parameters.</p> <p>Options available: Yes/No.</p>
Boot Override	<p>Press [Enter] to configure the device as the boot-up drive.</p>

## 5-8 BIOS POST Codes

### 5-8-1 AMI Standard - PEI

PEI_CORE_STARTED	0x10
PEI_CAR_CPU_INIT	0x11
PEI_CAR_NB_INIT	0x15
PEI_CAR_SB_INIT	0x19
PEI_MEMORY_SPD_READ	0x2B
PEI_MEMORY_PRESENCE_DETECT	0x2C
PEI_MEMORY_TIMING	0x2D
PEI_MEMORY_CONFIGURING	0x2E
PEI_MEMORY_INIT	0x2F
PEI_MEMORY_INSTALLED	0x31
PEI_CPU_INIT	0x32
PEI_CPU_CACHE_INIT	0x33
PEI_CPU_AP_INIT	0x34
PEI_CPU_BSP_SELECT	0x35
PEI_CPU_SMM_INIT	0x36
PEI_MEM_NB_INIT	0x37
PEI_MEM_SB_INIT	0x3B
PEI_DXE_IPL_STARTED	0x4F
DXE_CORE_STARTED	0x60
//Recovery	
PEI_RECOVERY_AUTO	0xF0
PEI_RECOVERY_USER	0xF1
PEI_RECOVERY_STARTED	0xF2
PEI_RECOVERY_CAPSULE_FOUND	0xF3
PEI_RECOVERY_CAPSULE_LOADED	0xF4
//S3	
PEI_S3_STARTED	0xE0
PEI_S3_BOOT_SCRIPT	0xE1
PEI_S3_VIDEO_REPOST	0xE2
PEI_S3_OS_WAKE	0xE3

### 5-8-2 AMI Standard - DXE

DXE_CORE_STARTED	0x60
DXE_NVRAM_INIT	0x61
DXE_SBRUN_INIT	0x62
DXE_CPU_INIT	0x63
DXE_NB_HB_INIT	0x68
DXE_NB_INIT	0x69
DXE_NB_SMM_INIT	0x6A

DXE_SB_INIT	0x70
DXE_SB_SMM_INIT	0x71
DXE_SB_DEVICES_INIT	0x72
DXE_ACPI_INIT	0x78
DXE_CSM_INIT	0x79
DXE_BDS_STARTED	0x90
DXE_BDS_CONNECT_DRIVERS	0x91
DXE_PCI_BUS_BEGIN	0x92
DXE_PCI_BUS_HPC_INIT	0x93
DXE_PCI_BUS_ENUM	0x94
DXE_PCI_BUS_REQUEST_RESOURCES	0x95
DXE_PCI_BUS_ASSIGN_RESOURCES	0x96
DXE_CON_OUT_CONNECT	0x97
DXE_CON_IN_CONNECT	0x98
DXE_SIO_INIT	0x99
DXE_USB_BEGIN	0x9A
DXE_USB_RESET	0x9B
DXE_USB_DETECT	0x9C
DXE_USB_ENABLE	0x9D
DXE_IDE_BEGIN	0xA0
DXE_IDE_RESET	0xA1
DXE_IDE_DETECT	0xA2
DXE_IDE_ENABLE	0xA3
DXE_SCSI_BEGIN	0xA4
DXE_SCSI_RESET	0xA5
DXE_SCSI_DETECT	0xA6
DXE_SCSI_ENABLE	0xA7
DXE_SETUP_VERIFYING_PASSWORD	0xA8
DXE_SETUP_START	0xA9
DXE_SETUP_INPUT_WAIT	0xAB
DXE_READY_TO_BOOT	0xAD
DXE_LEGACY_BOOT	0xAE
DXE_EXIT_BOOT_SERVICES	0xAF
RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN	0xB0
RT_SET_VIRTUAL_ADDRESS_MAP_END	0xB1
DXE_LEGACY_OPROM_INIT	0xB2
DXE_RESET_SYSTEM	0xB3
DXE_USB_HOTPLUG	0xB4
DXE_PCI_BUS_HOTPLUG	0xB5
DXE_NVRAM_CLEANUP	0xB6
DXE_CONFIGURATION_RESET	0xB7



### 5-8-3 AMI Standard - ERROR

PEI_MEMORY_INVALID_TYPE	0x50
PEI_MEMORY_INVALID_SPEED	0x50
PEI_MEMORY_SPD_FAIL	0x51
PEI_MEMORY_INVALID_SIZE	0x52
PEI_MEMORY_MISMATCH	0x52
PEI_MEMORY_NOT_DETECTED	0x53
PEI_MEMORY_NONE_USEFUL	0x53
PEI_MEMORY_ERROR	0x54
PEI_MEMORY_NOT_INSTALLED	0x55
PEI_CPU_INVALID_TYPE	0x56
PEI_CPU_INVALID_SPEED	0x56
PEI_CPU_MISMATCH	0x57
PEI_CPU_SELF_TEST_FAILED	0x58
PEI_CPU_CACHE_ERROR	0x58
PEI_CPU_MICROCODE_UPDATE_FAILED	0x59
PEI_CPU_NO_MICROCODE	0x59
PEI_CPU_INTERNAL_ERROR	0x5A
PEI_CPU_ERROR	0x5A
PEI_RESET_NOT_AVAILABLE	0x5B
//Recovery	
PEI_RECOVERY_PPI_NOT_FOUND	0xF8
PEI_RECOVERY_NO_CAPSULE	0xF9
PEI_RECOVERY_INVALID_CAPSULE	0xFA
//S3 Resume	
PEI_MEMORY_S3_RESUME_FAILED	0xE8
PEI_S3_RESUME_PPI_NOT_FOUND	0xE9
PEI_S3_BOOT_SCRIPT_ERROR	0xEA
PEI_S3_OS_WAKE_ERROR	0xEB
DXE_CPU_ERROR	0xD0
DXE_NB_ERROR	0xD1
DXE_SB_ERROR	0xD2
DXE_ARCH_PROTOCOL_NOT_AVAILABLE	0xD3
DXE_PCI_BUS_OUT_OF_RESOURCES	0xD4
DXE_LEGACY_OPROM_NO_SPACE	0xD5
DXE_NO_CON_OUT	0xD6
DXE_NO_CON_IN	0xD7
DXE_INVALID_PASSWORD	0xD8
DXE_BOOT_OPTION_LOAD_ERROR	0xD9
DXE_BOOT_OPTION_FAILED	0xDA
DXE_FLASH_UPDATE_FAILED	0xDB
DXE_RESET_NOT_AVAILABLE	0xDC

#### 5-8-4 Intel UPI POST Codes

Initialize KTIRC ininput structure default values	0xA0
Collect info such as SBSP, Boot Mode, Reset type etc	0xA1
Setup IO SADs in SBSP to access the config space	0xA2
Setup up minimum path between SBSP & other sockets Add the node to the tree Parse the LEP of the discovered socket Check if the system has the supported topology Setup the boot path for the parent which is not directly connected to Legacy CPU Setup path from SBSP to the new found node	0xA3
Setup IO SADs in PBSP to access the config space	0xA4
System configurations that require some kind of reset	0xA5
Sync up with PBSPs	0xA6
Topology discovery and route calculation	0xA7
Program final route	0xA8
Program final IO SAD setting	0xA9
Protocol layer and other Uncore settings	0xAA
Transition links to full speed operation	0xAB
Phy layer settings	0xAC
Link layer settings	0xAD
Coherency Settings	0xAE
KTIRC is done	0xAF

#### 5-8-5 Intel UPI Error Codes

When system BSP tries to setup path for remote sockets or sends a Boot_Go command to remote socket in SetupSbspPathToAllSockets() or SyncUpPbspForReset(). If the remote socket(s) hasn't checked-in, assert; it is a fatal condition, this error will be logged. No retry. <i>RC Behavior: System Halt</i>	0xD8
When SBSP tries to add this remote socket into system topology tree in SetupSbspPathToAllSockets(), there are some errors occur in the data structure. No retry. <i>RC Behavior: The current Socket is not added to the tree.</i> When SBSP setups the boot path for the parent which is not directly connected to Legacy CPU in SetupSbspPathToAllSockets(). The Child is not an immediate neighbor of Parent. No retry.	0xDA
SAD setup error <i>RC Behavior: System Halt</i>	0xDB

Unsupported topology <i>RC Behavior: System Halt</i>	0xDC
SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry. <i>RC Behavior: System Halt</i>	0xDD

### 5-8-6 Intel MRC POST Codes

Detect DIMM population	0xB0
Set DDR frequency	0xB1
Gather remaining SPD data	0xB2
Program registers on the memory controller level	0xB3
Evaluate RAS modes and save rank information	0xB4
Program registers on the channel level	0xB5
DDRIO Initialization	0xB6
Train DDR	0xB7
Initialize CLTT/OLTT	0xB8
Hardware memory test and init	0xB9
Execute memory init	0xBA
Program memory map and interleaving	0xBB
Program RAS configuration	0xBC
Rank margin tool	0xBD
MRC is done	0xBF

### 5-8-7 Intel MRC Error Codes

No memory was detected	0xE8
Memory test failure	0xEB
Different dimm types are detected installed in the system	0xED
Number of HAs found in system greater than MAX_HA defined in MRC build	0xEE
Indicates a CLTT table structure error	0xEF
Invalid VR mode, unable to set DRAM VDD	0xF0
Failure occurred reserving memory for IOT	0xF1
Reference code assert	0xF2
Unsupported MC frequency set	0xF3
Unable to get current MC frequency	0xF4

### 5-8-8 Intel PM POST Codes

Start of PPM structure initialization	0xD0
PPM CSR programming	0xD1
PPM MSR programming	0xD2
Start of PState transition init	0xD3
PPM exit	0xD4
PPM On ready to boot event	0xD5

### 5-8-9 Intel PM POST Codes

Start of IIO early Initialization	0xE0
Pre Link training	0xE1
Start of Gen3 EQ training	0xE2
Start of PState transition init	0xE3
Gen3 parameters override	0xE4
End of IIO Early Initialization	0xE5
Start of IIO Late initialization	0xE6
PCIE port initialization	0xE7
IOAPIC initialization	0xE8
VTD initialization	0xE9
IOAT initialization	0xEA
DFX initialization	0xEB
NTB initialization	0xEC
Security Initialization	0xED
IIO late initialization	0xEE
IIO On ready to boot event	0xEF

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

### 5-9-1 PEI Beep Codes

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

### 5-9-2 DXE Beep Codes

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