SB102-HK

Storage Barebone
User's Manual

UM_SB102-HK_v1.2_082624

Document Release History

Release Date	Version	Update Content
January, 2024	1	Released to public.
January, 2024	1.1	Update PSU spec.
August, 2024	1.2	Add Note to the top cover section.

Table of Contents

Preface i
Safety Instructions ii
About This Manual iv
Chapter 1. Product Features 1
1.1 Box Contents 1
1.1.1 Accessory Bag Contents 2
1.2 Specifications 3
1.3 System Block Diagram 4
1.4 Features 5
Chapter 2. Hardware Setup 8
2.1 Central Processing Unit 8
2.1.1 Installation 8
2.2 System Memory 14
2.2.1 Placement 14
2.2.2 DIMM Population 15
2.2.3 Installation 17
2.3 Top Cover 18
2.4 Power Supply Unit 19
2.4.1 Installation 19
2.4.2 LED Indicator 19
2.5 Fan 20
2.6 Air Duct 21
2.7 Disk Drive 22
2.7.1 Disk Drive: 2.5-inch 22
2.7.2 LED Indicator 23
2.8 Riser Card 24
2.9 M.2 Card 25
2.10 OCP Card 26
2.11 Slide Rail 27
Chapter 3. Hardware Settings 31
3.1 Block Diagram 31
3.2 Placement 32
3.3 Content List 33
3.4 Input and Output Panel 35

3.5 Onboard LED Indicator 36
3.6 Connector Definition 37
3.7 Jumper Setup 49
3.8 Drive Backplane: 4 Bay 50
3.8.1 Placement 50
3.8.2 Connector 51
3.8.3 LED Indicator 53
3.8.4 Jumper Setting 54
3.8.5 Switch Setting 55
3.8.6 Application Setting 56
3.8.6.1 HOST Select 56
3.8.6.2 MCIO-8i I2C input Setting 56
Chapter 4. BIOS Configuration Settings 57
4.1 Navigation Keys 57
4.2 BIOS Menu 58
4.2.1 Menu 58
4.2.2 Startup 58
4.3 Main 59
4.3.1 Main 59
4.4 Advanced 60
4.4.1 Trusted Computing 60
4.4.2 ACPI Settings 60
4.4.3 Redfish Host Interface Settings 60
4.4.4 AST2600 Super IO Configuration 61
4.4.5 Serial Port Console Redirection 61
4.4.6 Option ROM Dispatch Policy 61
4.4.7 PCI Subsystem Settings 62
4.4.8 Network Stack Configuration 62
4.4.9 T1s Auth Configuration 62
4.4.10 RAM Disk Configuration 63
4.4.11 VLAN Configuration (MAC:BA8B593F29EE) 63
4.4.12 MAC:BA8B593F29EE-IPv4 Network Configuration 63
4.4.13 MAC:BA8B593F29EE-IPv6 Network Configuration 63
4.5 Platform Configuration 64
4.5.1 PCH-IO Configuration 64

4.5.2 Server ME Configuration 66
4.5.3 Runtime Error Logging 66
4.5.4 IIO Error Enabling 68
4.5.5 PCIe Error Enabling 69
4.5.6 Error Control Setting 70
4.5.7 Crash Log Enabling 71
4.5.8 DWR Configuration 71
4.6 Socket Configuration 72
4.6.1 Processor Configuration 72
4.6.2 Uncore Configuration 73
4.6.3 Memory Configuration 75
4.6.4 IIO Configuration 77
4.6.5 Advanced Power Management Configuration 89
4.7 Server Mangement 93
4.7.1 System Event Log 94
4.7.2 BMC Network Configuration 94
4.8 Security 95
4.9 Boot 96
4.10 Save & Exit 99
4.11 BIOS Update Process 100
4.12 BIOS Post Code 101
Chapter 5. Technical Support 107

Copyright © 2023 AIC®, Inc. All Rights Reserved.

This document contains proprietary information about AIC® products and is not to be disclosed or used except in accordance with applicable agreements.

Preface

Copyright

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photo-static, recording or otherwise, without the prior written consent of the manufacturer.

Trademarks

All products and trade names used in this document are trademarks or registered trademarks of their respective holders.

Changes

The material in this document is for information purposes only and is subject to change without notice.

Warning

1. A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Disclaimer

AIC® shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither AIC® or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Instruction Symbols

Special attention should be given to the instruction symbols below.

NOTE	This symbol indicates that there is an explanatory or supplementary instruction.
CAUTION	This symbol denotes possible hardware impairment. Upmost precaution must be taken to prevent serious hardware damage.
WARNING	This symbol serves as a warning alert for potential body injury. The user may suffer possible injury from disregard or lack of attention.

Safety Instructions

Before you commence, please attentively read the following important discretions below. All cautions and warnings on the equipment or in the manuals should be circumspectly noted and reviewed.

Always ground yourself to prevent static electricity.
請全程接地，以防止靜電。
请全程接地，以防止静电。
Всегда заземляйте себя, чтобы избежать статического электричества.
Aard jezelf altijd om statische elektriciteit te voorkomen.

- Firmly ground yourself at all times when installing or assembling the internal components of the server. Most of electronic components in the server are highly sensitive to electrical static discharge.
- Use a solid grounding wrist strap and distinctively place all electronic components in static-shielded devices to prevent static. Grounding wrist straps can be purchased in any electronic supply store.
- Confirm that the power source is turned off and then disconnect the power cords from your system before performing any type of installation or manual servicing. A sudden surge of power could severely damage the sensitive electronic components.
- Do not precipitously open the system's top cover. If you must open the cover for maintenance purposes, only a trained technician should be allowed to proceed this action. Integrated circuits on computer boards are highly sensitive to static electricity. Before operating a board or integrated circuit, touch an unpainted portion of the system unit chassis for a couple of seconds to discharge any static electricity on your body.

Place the server in a stable environment.
請將伺服器放置在穩定的環境中。
请将伺服器放置在稳定的环境中。
Поместите сервер в стабильную среду.
Plaats de server in een stabiele omgeving.

- Place this equipment on a stable surface when installing. A small mild drop or fall could cause fatal injury to both the equipment and the person handling the equipment.
- Please keep this equipment away from humidity to prevent vast rust and disintegration.
- Carefully and accurately mount the equipment into the rack. Uneven mechanical loading may lead to hazardous consequences.
- This equipment is to be installed for operation in an environment with maximum ambient temperature below 35°C.
- Review the environment before performing any installation or servicing. Keep the equipment away from hazardous and uneven grounds.
- This server must be installed only in Restricted Access Locations.

Handle equipment with care.
請謹慎操作設備。
请谨慎操作设备。
Обращайтесь с оборудованием осторожно.
Behandel de apparatuur voorzichtig.

- Do not cover the openings of the system. The openings on the system are for air convection, which intentionally protect the equipment from overheating.
- Never pour any liquid into ventilation openings of the system. This could cause catastrophic fire or electrical shock.

- Ensure that the voltage of the power source is within the specification on the label when connecting the equipment to the power outlet. The current load and output power of loads must be within the specification.
- This equipment must be firmly connected to reliable grounding before usage. Pay special attention to power supplied other than direct connections, e.g. using of power strips.
- Place the power cord out of the way of foot traffic. Do not place anything over the power cord. The power cord must be rated for the product, voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product.

Pay attention to hardware maintenance.
注意硬體維護。
注意硬体维护。
Обратите внимание на обслуживание оборудования.
Besteed aandacht aan hardware-onderhoud.

- If the equipment is not used for a long time, disconnect the equipment from mains to avoid being damaged by transient over-voltage.
- Module and drive bays must not be empty. They must have a dummy cover.
- Never open the equipment without professional assistance. For safety reasons, only qualified service personnel should open the equipment.
- If one of the following situations arise, the equipment should be checked and tested by service personnel:
  1. The power cord or plug is damaged.
  2. Liquid has penetrated the equipment.
  3. The equipment has been exposed to moisture.
  4. The equipment does not work well or will not work according to its user manual.
  5. The equipment has been dropped and/or damaged.
  6. The equipment has obvious signs of breakage.
  7. Please disconnect this equipment from the AC outlet before cleaning. Do not use liquid or detergent for cleaning. The use of a moisture sheet or cloth is recommended for cleaning.

CAUTION
The equipment intended for installation should be placed in Restricted Access Location.

CAUTION
There will be a risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. After performing any installation or servicing, make sure the enclosure is correct in position before turning on the power.

CAUTION
This unit may have more than one power supply. Disconnect all power sources before maintenance to avoid electric shock.

About This Manual

Thank you for selecting and purchasing the SB102-HK.
This user's manual is provided for professional technicians to perform easy hardware setup, basic system configurations and quick software startup. This document pellucidly presents a brief overview of the product design, device installation and firmware settings for SB102-HK. For the latest version of this user's manual, please refer to the AIC® website: https://www.aicipc.com/en/productdetail/51413.

Chapter 1 Product Features

SB102-HK is a flexible storage server barebone that is specifically designed to accommodate diverse corporations and enterprises for managing heavy workloads and multiple applications.

Chapter 2 Hardware Setup

This chapter displays an easy installation guide for assembling the hardware in this product. Utmost caution for proceeding to set up the hardware is highly advised. Most of the components are highly fragile and vulnerable to exterior influence. Do not endanger the device by placing the device in an unstable environment.

Chapter 3 Motherboard Settings

This chapter elaborates the overall layout of the server motherboard, including multifarious connectors, jumpers and LED descriptions. These descriptions assist users to configure different settings and functions of the motherboard, as well as to confirm the placement of each connector and jumper.

Chapter 4 BIOS Configuration Settings

This chapter introduces the key features of BIOS, including the descriptions and option keys for diverse functions. These details provide users to effortlessly navigate and configure the input/output devices.

Chapter 5 BMC Configuration Settings

This chapter illustrates the diverse functions of IPMI BMC, including the details on logging into the web page and assorted definitions. These descriptions are helpful in configuring various functions through Web GUI without entering the BIOS setup. For more information of BMC configurations, please refer to IPMI BMC (Aspeed AST2500) User's Manual for a more detailed description.

Chapter 6 Technical Support

For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: https://www.aicipc.com/en/index. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

SB102-HK is a high density storage server that includes motherboard, chassis, power supply and disk drive. For more information about our product, please visit our website at https://www.aicipc.com/en/index.

Before removing the subsystem from the shipping carton, visually inspect the physical condition of the shipping carton. Exterior damage to the shipping carton may indicate that the contents of the carton are damaged. If any damage is found, do not remove the components; contact the dealer where the subsystem was purchased for further instructions. Before continuing, first unpack the subsystem and verify that the number of components in the shipping carton is accurate and in good condition.

1.1 Box Contents

This product contains the components listed below.

Please confirm the number and the condition of the components before installation.

	Pre-installed into the system	Number
✓	1600W redundant power supply 80+ Platinum/Titanium	1+1
✓	2.5-inch hot swap disk drive tray	12
✓	Heat sink	2
✓	Easy swap fan 8 x 40x56mm	8
✓	AIC® Horkos motherboard	1
	Accessory Item	**Number**
✓	EPE foam for front board: 575*420*105H	1
✓	EPE foam for rear board: 575*420*105H	1
✓	EPE foam for front tray: 575*300*145H	1 set
✓	EPE foam for rear tray: 575*300*145H	1 set
✓	EPE pad for Rail Box: 125*100*60T	2
✓	EPE pad for heatsink: 125*100*100H	1 set
✓	Power cord	vary per region
✓	28-inch tool-less slide rail assembly	1

Product features are subject to change without notice.

1.1.1 Accessory Bag Contents

Item	Part No.	Description	Number
ACCESSORY_PACKAGE	M06-1519-032X01	MCB	1 set
SCREW/MECH	H38K0P305004	K(+),M3X5L,NI	2 pcs
MINI DP TO VGA dongle	G6-A00000130	TC&C/MINI DP MALE TO VGA FEMALE(DB15)/ L230MM/32AWG	1 pcs
CPU carrier E1A	CM1-00006699	OTHER/WNMEC00-0NNK1-EH	2 pcs
CPU carrier E1B	CM1-00006947	OTHER/WNMEC00-0NNK2-EH	2 pcs
CPU heatsink under 250 watts	H50HP0A-0023	L=118MM, W=79MM,H=24.5MM/ TIM=TC-5288	2 pcs
CPU heatsink over 250 watts	H50VC0C-0003	L=118MM, W=78MM,H=24.7MM/ TIM=TC-5288	2 pcs

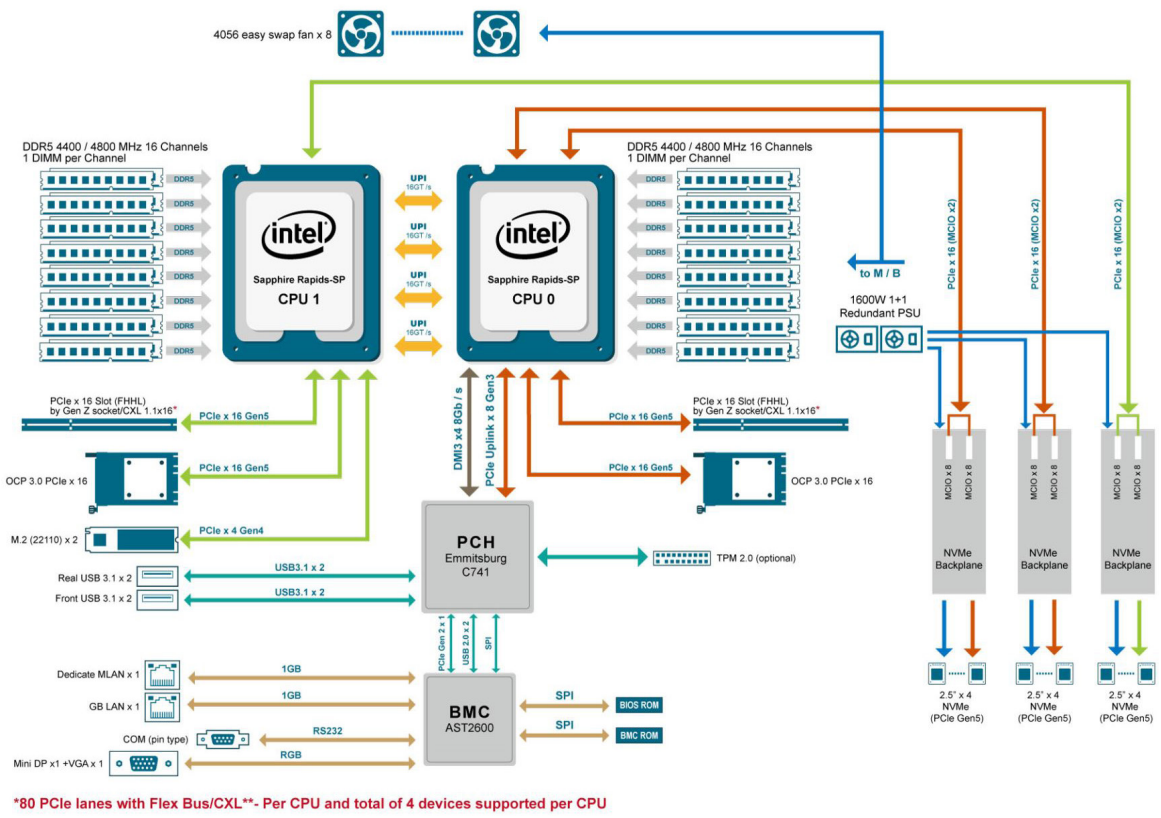
Product features are subject to change without notice.

1.2 Specifications

Dimensions (W x D x H)	mm : 438 x 800 x 43.75		
	inches : 17.2 x 33.5 x 1.75		
Motherboard	AIC Server Board HK		
Processor	Processor Support	• 4th Gen Intel® Xeon® Scalable Processors (Sapphire Rapids) • 5th Gen Intel® Xeon® Scalable Processors (Emerald Rapids) • Supports CPU TDP up to 350W **Please contact AIC Technical Support for more info/details about optimized CPUs and specialized system.*	
	Socket Type	Socket E (LGA 4677)	
Chipset Support	Intel® Emmitsburg PCH (C741 Chipset)		
System Memory	• DDR5 4800MHz (1DPC) • DDR5 5600MHz (1DPC) 4400MTS (2DPC) by Emerald Rapids CPU • Total 32 memory slots; 16 slots per CPU (2DPC)		
Front Panel	• 1 x System power on/off button/LED • 1 x System reset button • 1 x System ID button/LED • 1 x System alert (BMC) • 1 x USB 3.0		
Drive Bays	External	2.5" hot swap	12 x PCIe Gen5 NVMe
	Internal	M.2	2 x M.2/M-Key/22110/2280 (PCIe Gen4)
Backplane	3 x 4-bay NVMe PCIe Gen 5		
Expansion Slots	PCIe 5.0	• 2 x PCIe X16 slots (FHHL) • 2 x OCP 3.0 bays (PCIe X16 width)	
Rear I/O	LAN	1 x GbE RJ45 dedicated BMC management	
	USB	2 x USB 3.2 Gen1 Type A	
	Video Output	1 x Mini DisplayPort	
	Serial Port	1 x RJ45 (COM)	
Power Supply	• 1600W redundant power supply 80+ Platinum/Titanium		
System Cooling	8 x 40x56mm easy swap fans ABS material plastic air-duct (clear)		

Riser Card (included)	G3-A00001149	2 x PCIe 5.0 x16 cable CEM	
System BIOS	BIOS Type	AMI UEFI BIOS	
	BIOS Features	• ACPI • PXE • WOL • AC loss recovery • BIOS recovery • IPMI 2.0 KCS mode interface	• SRIOV • SMBIOS • TPM • Serial console redirection • PCIe hotplug
On-board Devices	SATA	Intel® Emmitsburg PCH on-chip solution • M.2: 2 x M.2/M-Key/22110/2280 (PCIe Gen4)	
	BMC	Aspeed AST2600 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN • HTML5 • Redfish • SMASH Support	
	Network Controllers	Realtek RTL8211E for BMC dedicated management port	
	Graphics	Aspeed AST2600 Advanced PCIe Graphics & Remote Management Processor • PCIe Graphic/2D Controller • 1920x1200@60Hz 32bpp	
Environmental Specifications	• Storage temperature : -10ºC(14ºF) ~ 60ºC(140ºF) • Operating temperature : 0ºC(32ºF) ~ 35ºC(95ºF) • Storage operating humidity : 5%~95% non-condensing		
Gross Weight	(w/ PSU & Rail)	kgs : 20	
		lbs : 44	
Packaging Dimensions	(W x D x H)	mm : 595 x 1115 x 239	
		inches : 23.4 x 43.9 x 9.4	
Mounting	Standard	28" tool-less slide rail	

1.3 System Block Diagram



*80 PCIe lanes with Flex Bus/CXL**- Per CPU and total of 4 devices supported per CPU

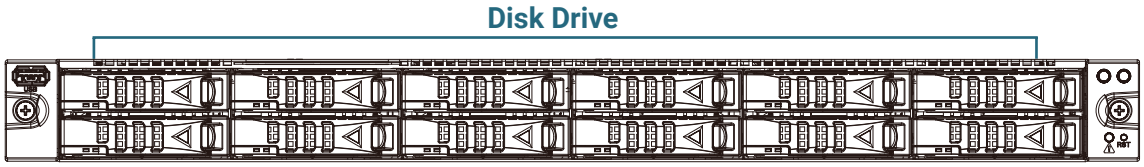
1.4 Features

SB102-HK is a reliable 1U storage server barebone with 12 hot swap drives bays. This product is designed to accommodate the AIC-patented serverboard, Horkos, which supports dual 4th Gen Intel® Xeon® Scalable Processors and 32 DDR5 DIMM to offer greater performance, efficiency and utility for our customers. Featuring Intel® Emmitsburg PCH Chipset, which is emphasized for its accelerated speed and expansion, this product enhances these advantages by integrating flexible IO usage and system expansion into to provide greater bandwidth and utilization.

In addition to the noteworthy features of the barebone, SB102-HK provides immediate and efficient management with Onboard Baseboard Management Controller and greater I/O extension. Featuring IPMI 2.0 and Aspeed AST2600 Advanced PCIe Graphics, the server board offers support for iKVM, Media Redirection, Smash Support, IPMI over LAN and Serial over LAN.

- 1U all-flash server solution
- 12 x 2.5” front hot-swappable NVMe bays
- Supports dual 4th Gen Intel® Xeon® Scalable Processors
  (codename: Sapphire Rapids)
- 32x DDR5 RDIMM and 4x PCIe Gen5 extensions

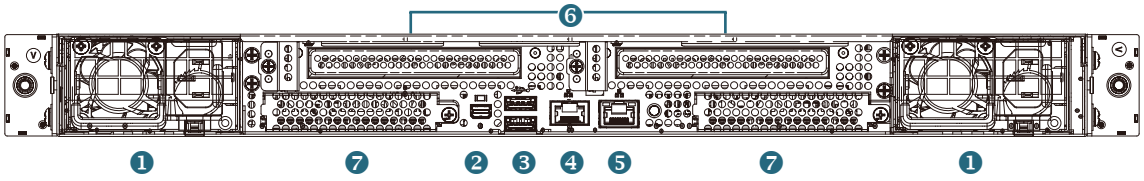
Front Panel



System LED Indicator and switch

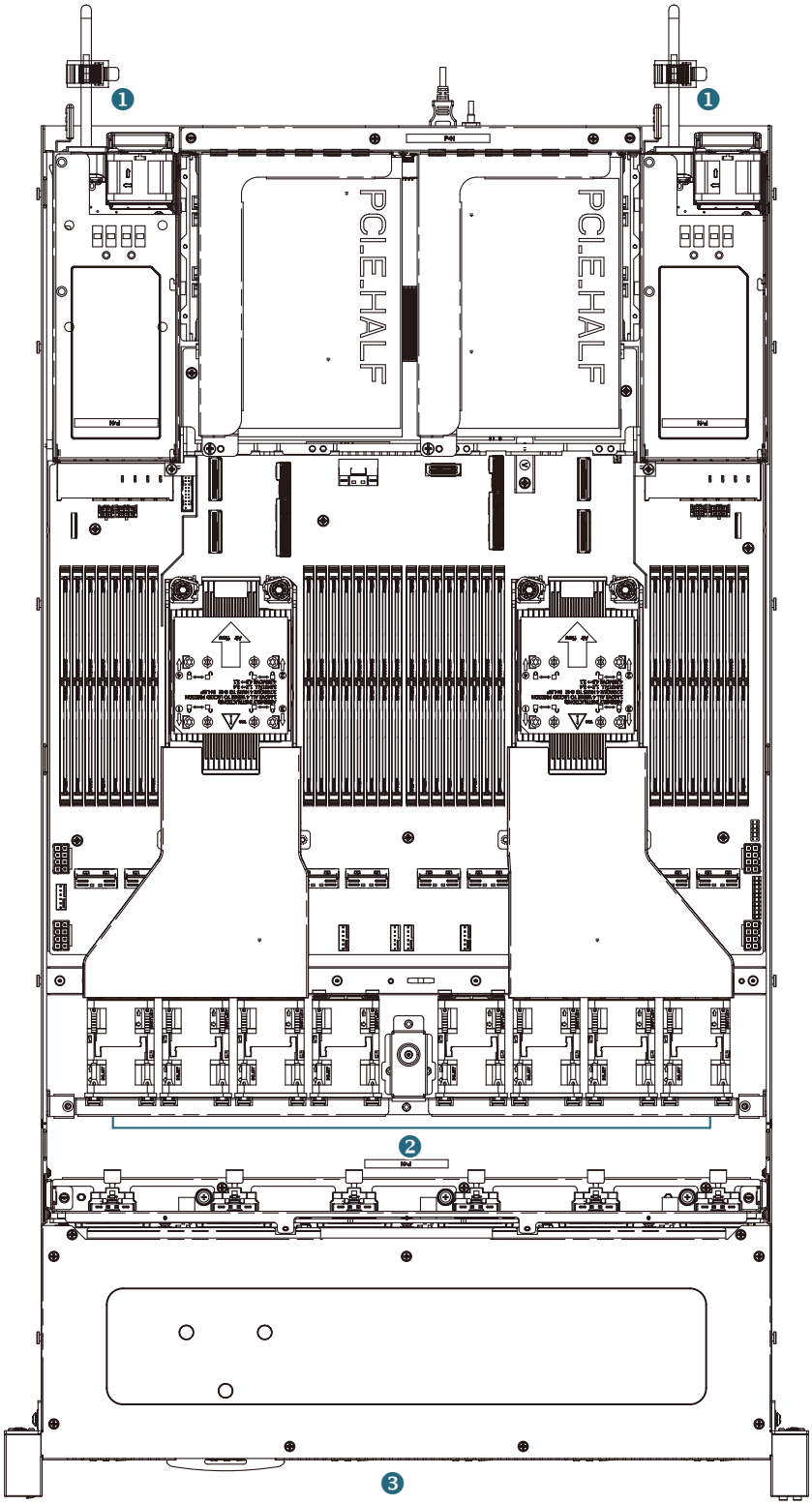
Item	Description	Item	Description
	System Power Button & LED (Green)	RST	System Reset Button
	System ID Button & LED (Blue)		System Alert LED (Red)

Rear Panel



Item	Description
1	1600W redundant power supply 80+ Platinum/Titanium
2	1 x mini-display port connector
3	2 x USB 3.0 Type A
4	1 x external RJ45 COM port
5	1 x Gbe RJ45 dedicated BMC management
6	2 x PCIe 5.0 x16 slots (FHHL)
7	2 x OCP 3.0 bays (PCIe X16 width)

Top View



Item	Description
1	1600W redundant power supply 80+ Platinum/Titanium
2	8 x 40x56mm easy swap fans
3	12 x 2.5-inch hot swap disk drive

Chapter 2. Hardware Setup

This chapter provides the graphic detail and basic instruction for hardware installation. Turn off the system and unplug all peripheral devices before proceeding.

2.1 Central Processing Unit

The serverboard supports dual Xeon scalable processors and 1+1 Socket E (LGA-4677).

2.1.1 Installation

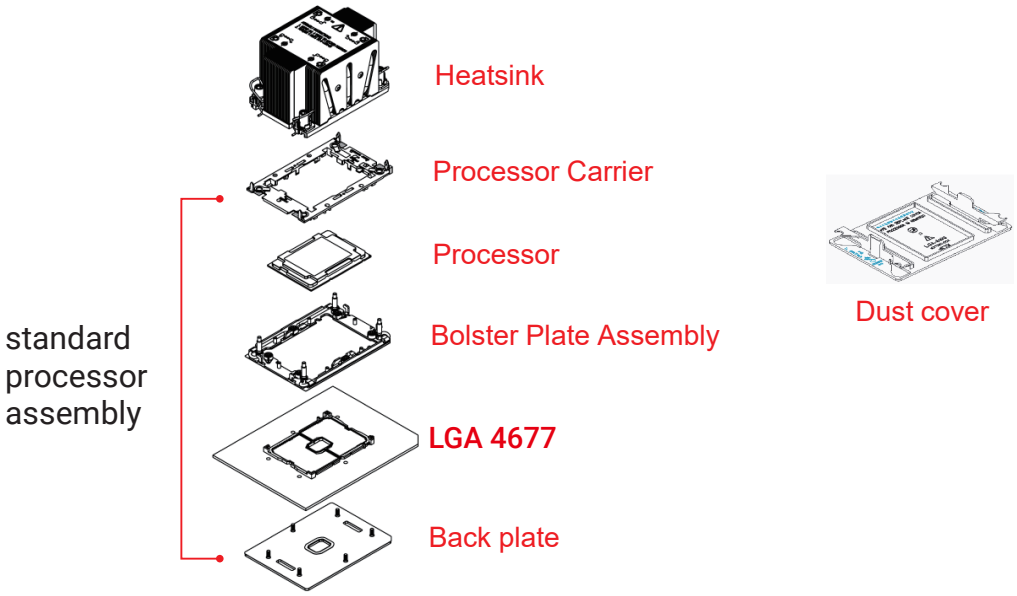
To ensure a safe and easy setup, you need to prepare before installation:

- ☑ a T30 torque screwdriver
- ☑ ESD wrist strap/mat and conductive foam pad
- ☑ Safe and stable environment

CAUTION
The pins of the processor socket are vulnerable and easily susceptible to damage if fingers or any foreign objects are pressed against them. Please keep the socket protective cover on when the processor is not installed.

CAUTION
When unpacking a processor, hold the processor only by its edges to avoid touching the contacts.

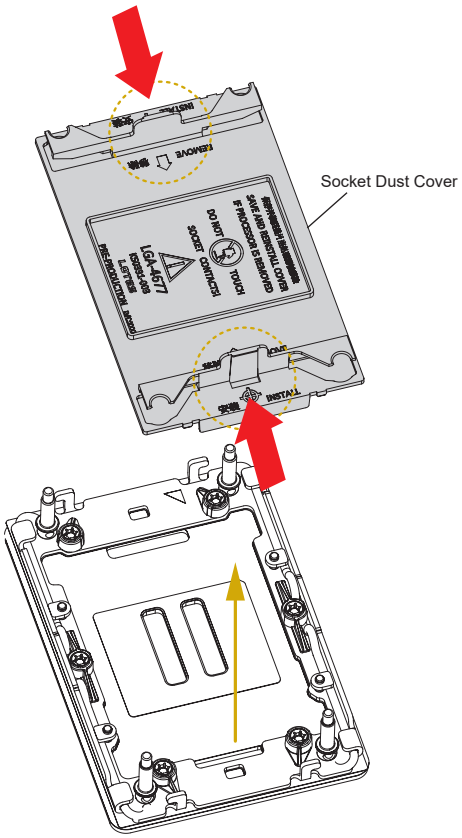
Standard Processor Assembly:
A standard processor assembly is comprised of 5 components: processor carrier, processor, bolster plate assembly, socket and back plate.



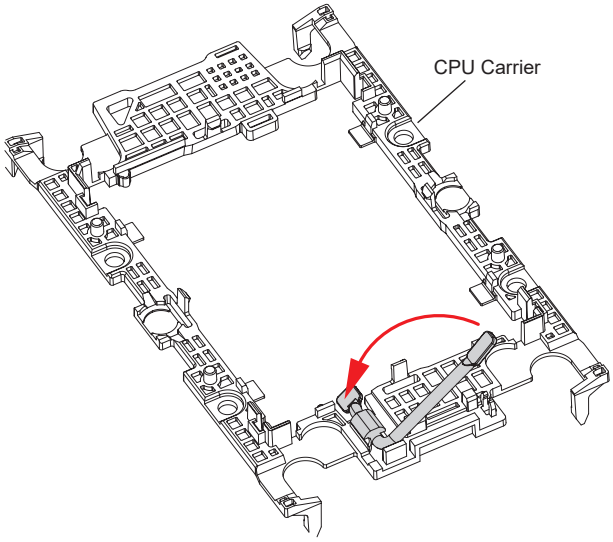
This information is provided for professional technicians only.

Procedure:

① Remove the dust cover. Push the tab inward on both sides to remove.

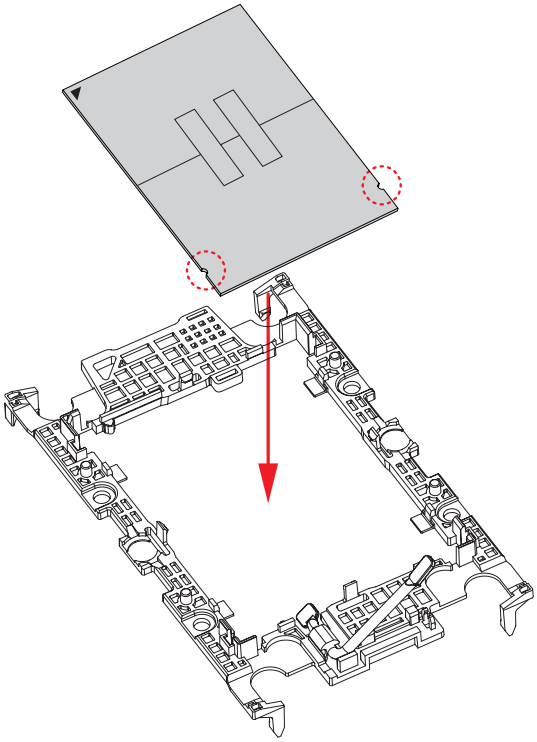


② Release the handle on the CPU carrier.

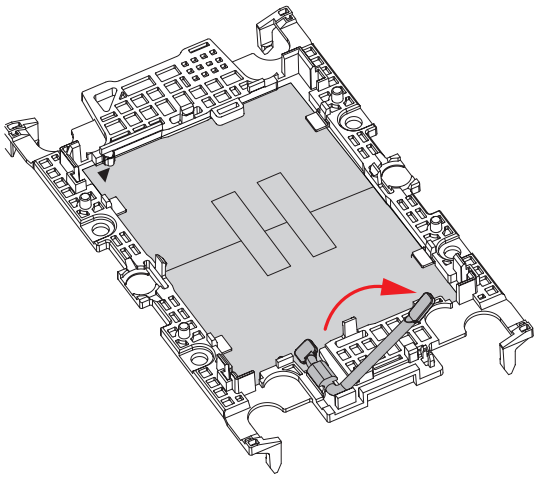


③ Insert the CPU into the CPU carrier. Carefully align and insert on side of the CPU and then the other.

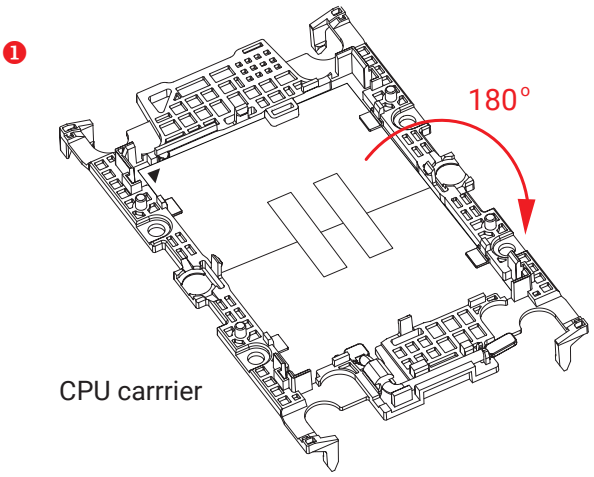
> **NOTE**
> Must ensure to match the direction and the notch of the CPU with the carrier.

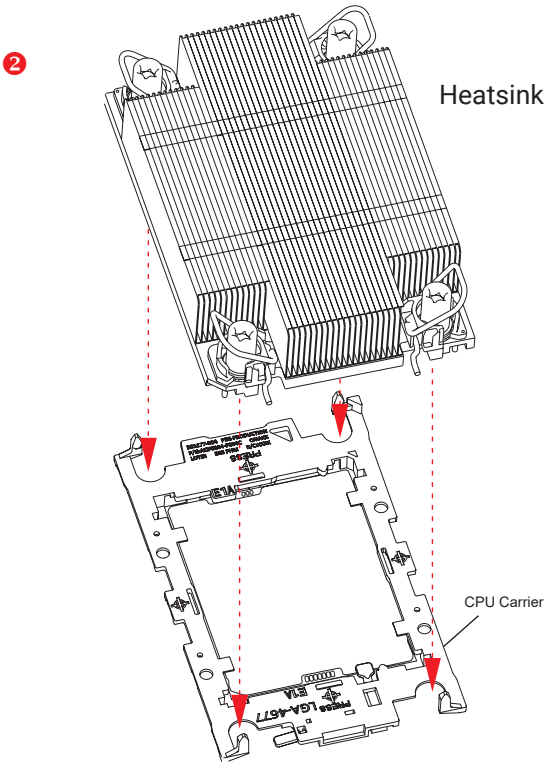


④ Close the handle after inserting the CPU.



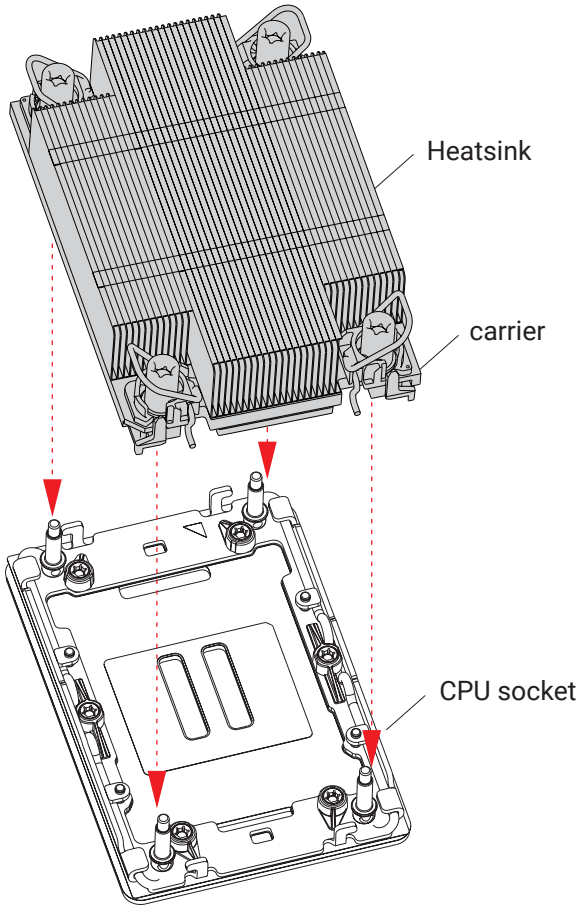
⑤ Reverse the CPU carrier to 180 degrees and attach the heat sink onto the CPU carrier with the Syringe thermal paste.



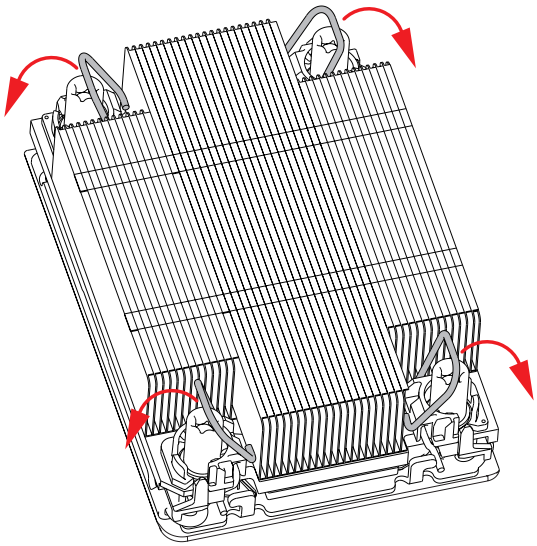


⑥ Install the assembled heatsink and CPU carrier onto the CPU socket.

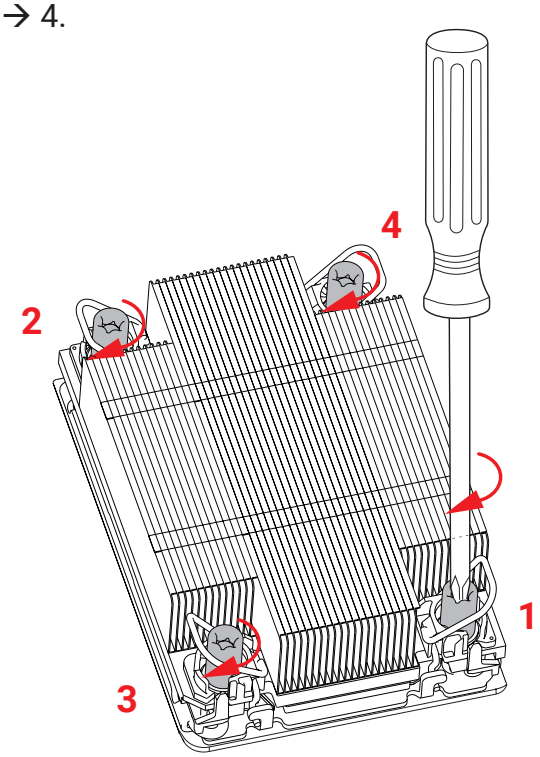
CAUTION
Failure to tighten the heat sink screws in the specified order may cause damage to the processor socket assembly. Heat sink screws is recommended to be tightened to 8 in-lbs torque, but can be tightened to 12 in-lbs torque according to the indicated order on the top of the heatsink label.



⑦ Press the rotating wire located on the four corners of the heat sink to latch position to secure the heat sink.



⑧ Please use a T-30 torque driver tighten the nuts in the four corners of the heat sink labeled in the order 1 → 2 → 3 → 4.



This information is provided for professional technicians only.

2.2 System Memory

2.2.1 Placement

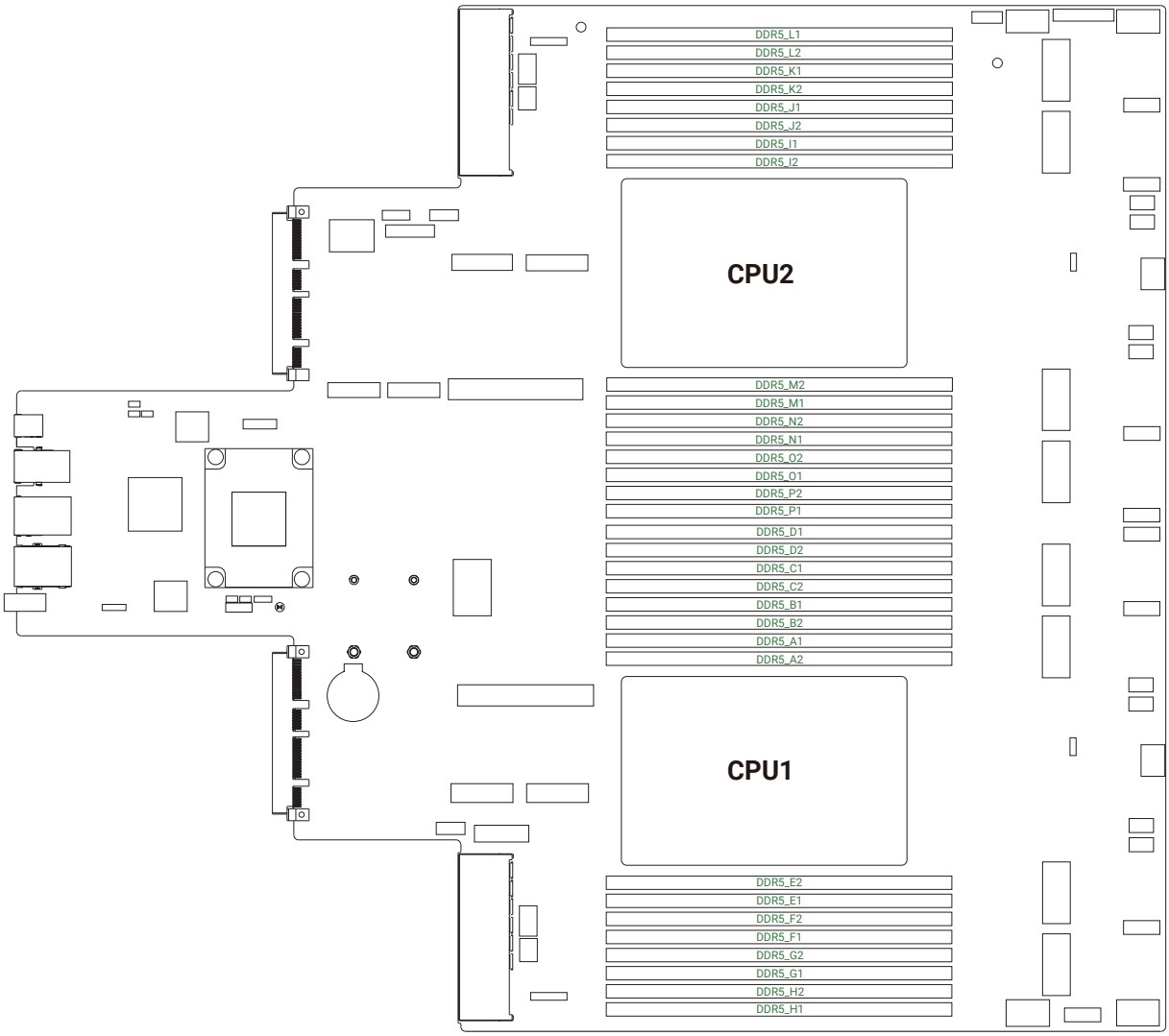
The DIMMs are displayed on the Horkos board as DDR5_L1/DDR5_L2/DDR5_K1/DDR5_K2/DDR5_J1/DDR5_J2/DDR5_I1/DDR5_I2/ DDR5_M2/DDR5_M1/DDR5_N2/DDR5_N1/DDR5_O2/DDR5_O1/DDR5_P2/DDR5_P1/ DDR5_D1/DDR5_D2/DDR5_C1/DDR5_C2/DDR5_B1/DDR5_B2/DDR5_A1/DDR5_A2/ DDR5_E2/DDR5_E1/DDR5_F2/DDR5_F1/DDR5_G2/DDR5_G1/DDR5_H2/DDR5_H1

To ensure satisfactory performance, you need to:

☑ Verify the DIMM type:

This product supports DDR5 RDIMM

☑ Verify if all of the DIMMs installed are of the same DIMM type to avoid memory failure and loss of performance speed.



2.2.2 DIMM Population

NOTE

Rules to abide by before installation:

- Must install at least one DDR5 DIMM per socket.
- If only one DIMM is populated in a channel, you must install it in the slot furthest away from the CPU.
- Must populate DIMM1 before DIMM2.

The symbol # in the graph below indicates that the DIMM slot is populated.

1 CPU Configuration

Placement		DIMM Number														
		1	1	1	1	2	2	4	6	6	6	6	8	12	12	16
CPU1	A1	#				#		#	#	#		#	#	#	#	#
	A2													#		#
	B1			#						#	#	#	#	#	#	#
	B2														#	#
	C1						#	#	#	#	#		#	#	#	#
	C2													#		#
	D1								#		#	#	#	#	#	#
	D2														#	#
	E1		#				#	#	#	#	#		#	#	#	#
	E2													#		#
	F1				#				#		#	#	#	#	#	#
	F2														#	#
	G1					#		#	#	#		#	#	#	#	#
	G2													#		#
	H1									#	#	#	#	#	#	#
	H2														#	#

2 CPU Configurations

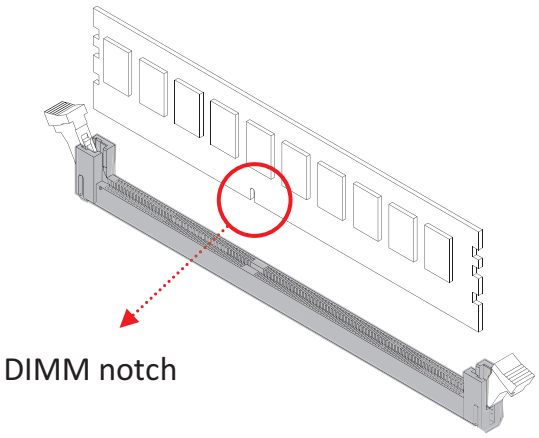
Placement		DIMM Number														
		1	1	1	1	2	2	4	6	6	6	6	8	12	12	16
CPU1	A1	#				#		#	#	#		#	#	#	#	#
	A2													#		#
	B1			#						#	#	#	#	#	#	#
	B2														#	#
	C1						#	#	#	#	#		#	#	#	#
	C2													#		#
	D1								#		#	#	#	#	#	#
	D2														#	#
	E1		#				#	#	#	#	#		#	#	#	#
	E2													#		#
	F1				#				#		#	#	#	#	#	#
	F2														#	#
	G1					#		#	#	#		#	#	#	#	#
	G2													#		#
	H1									#	#	#	#	#	#	#
	H2														#	#

Placement		DIMM Number														
		1	1	1	1	2	2	4	6	6	6	6	8	12	12	16
CPU2	I1	#				#		#	#	#		#	#	#	#	#
	I2													#		#
	J1			#						#	#	#	#	#	#	#
	J2														#	#
	K1						#	#	#	#	#		#	#	#	#
	K2													#		#
	L1								#		#	#	#	#	#	#
	L2														#	#
	M1		#				#	#	#	#	#		#	#	#	#
	M2													#		#
	N1				#				#		#	#	#	#	#	#
	N2														#	#
	O1					#		#	#	#		#	#	#	#	#
	O2													#		#
	P1									#	#	#	#	#	#	#
	P2														#	#

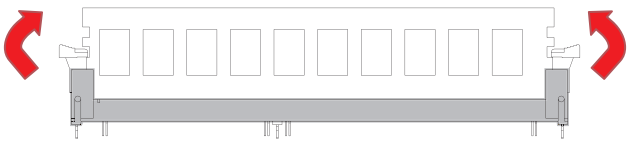
2.2.3 Installation

Step 1 Unlock the DIMM socket by pressing the retaining clips outward.

Step 2 Insert the memory module into the slot. Make sure that the DIMM notch is accurately positioned.

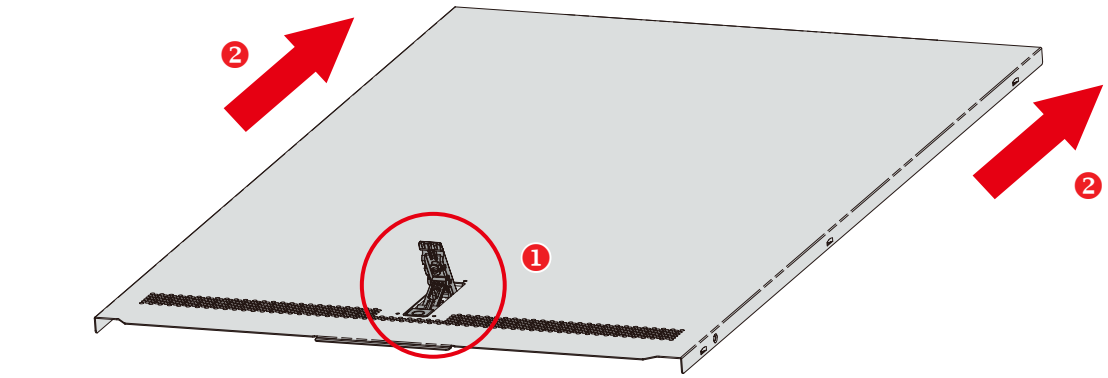


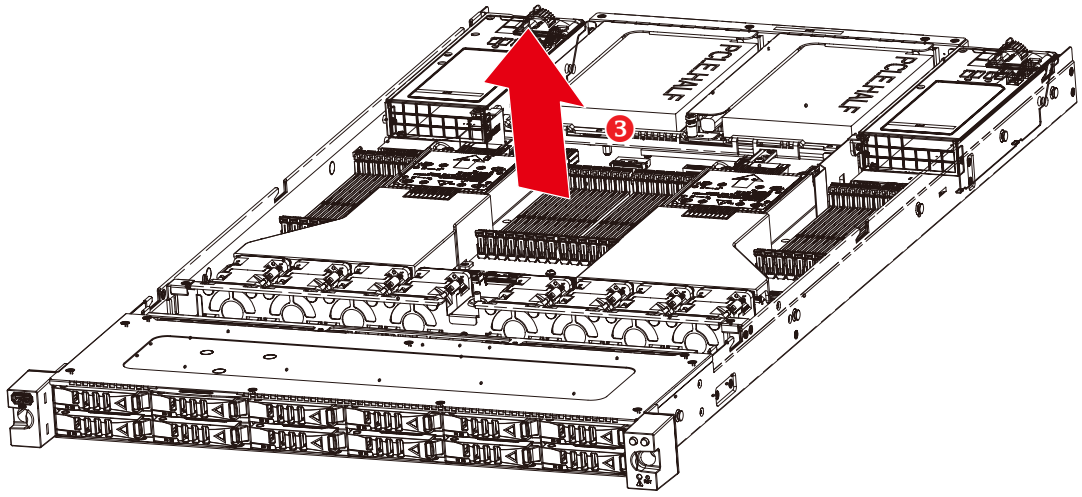
Step 3 Close the retaining clips to complete installation.



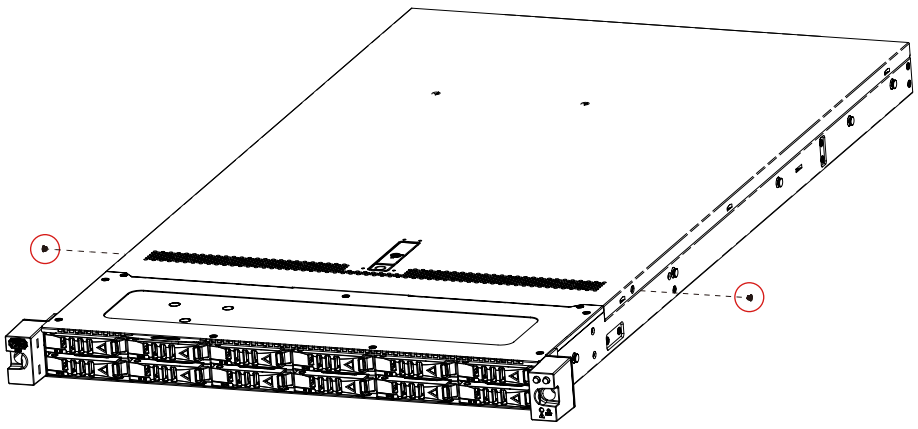
2.3 Top Cover

① Press the release tab on the top cover.
② Slide the top cover towards the rear of the system barebone.
③ Lift the top cover upward to remove.





The screws in the red circle below are for transportation secure. After removing the cover for the first time, there is no necessary to fasten the screws back to the chassis.

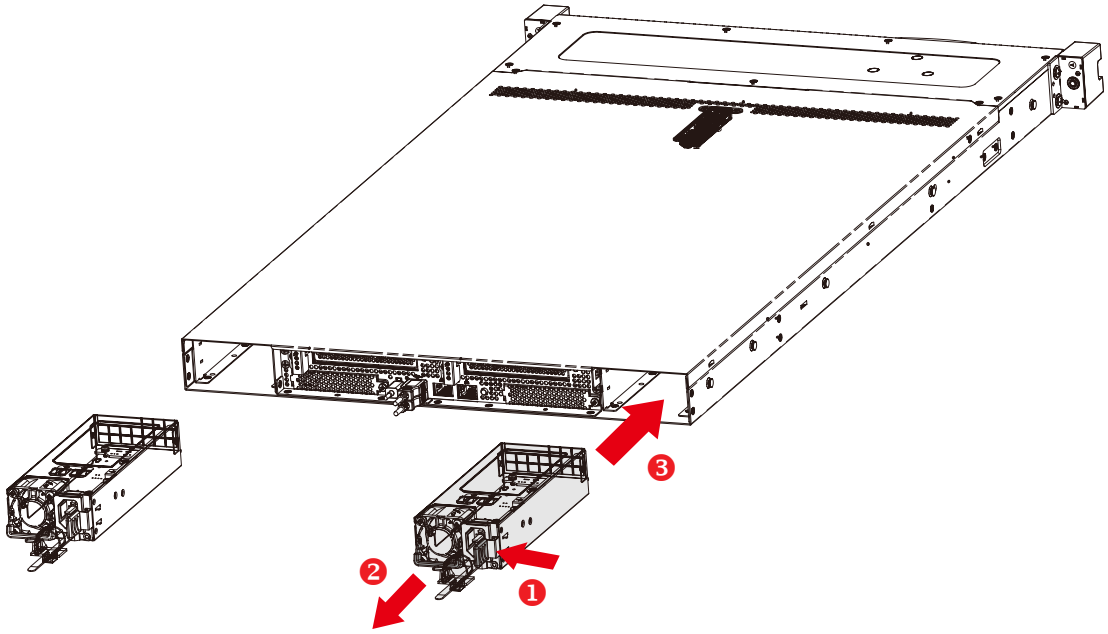


This information is provided for professional technicians only.

2.4 Power Supply Unit

2.4.1 Installation

① Press the ejector to release the module.
② Pull the handle to remove the module out of the chassis.
③ Push the replaced power supply unit into the chassis. Ensure that the module is hooked into the cage.



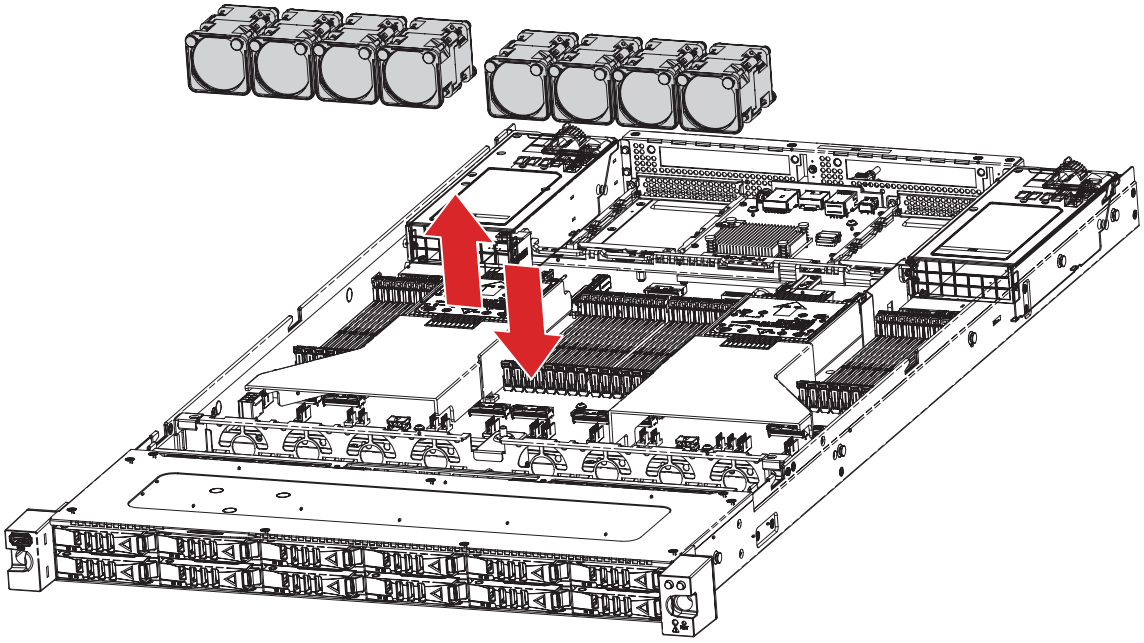
2.4.2 LED Indicator

Color	Behavior	Description
Green	Solid	Output on and working normally.
	Off	No AC power to all power supplies.
	Blinking, 1Hz	AC present/ Only Vsb on (PS off) or PS in Smart redundant state/ Off line mode.
	Blinking, 2Hz	Power supply FW updating.
Amber	Solid	AC cord unplugged or AC power lost; with a second power supply in parallel still with AC input power.
	Solid	Power supply critical event causing a shutdown; failure, OCP, OVP, fan fail.
	Blinking, 1Hz	Power supply warning events where the power supply continues to operate high temp, high power, high current, slow fan.

This information is provided for professional technicians only.

2.5 Fan

① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Unplug the fan cables and connectors from the server board.
③ Pull the top fan out of the chassis.

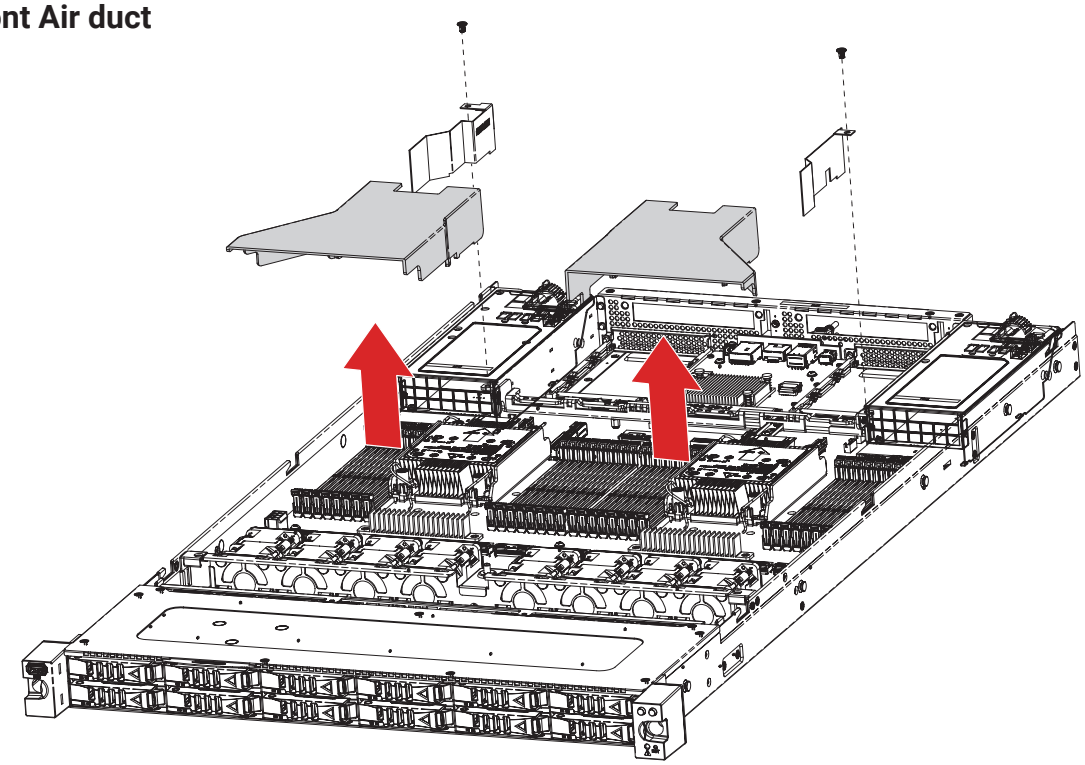


This information is provided for professional technicians only.

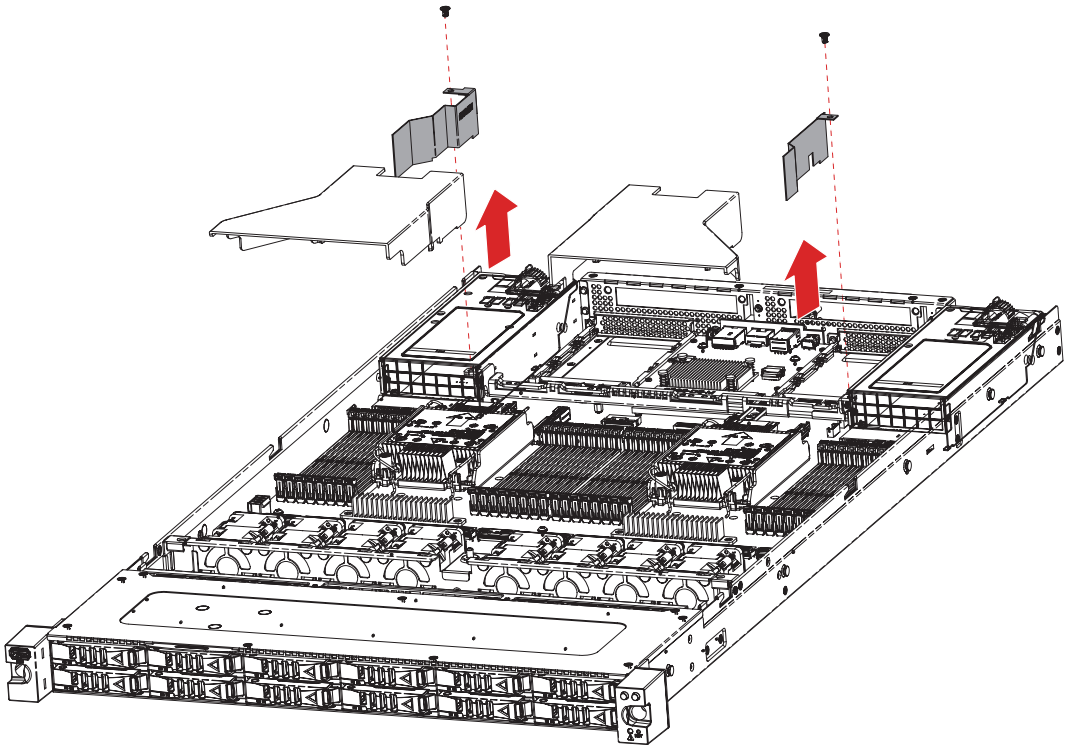
2.6 Air Duct

① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Lift the front air duct upward to remove.
③ Dislodge the screws on the rear air duct and lift the air duct upward to remove.

Front Air duct



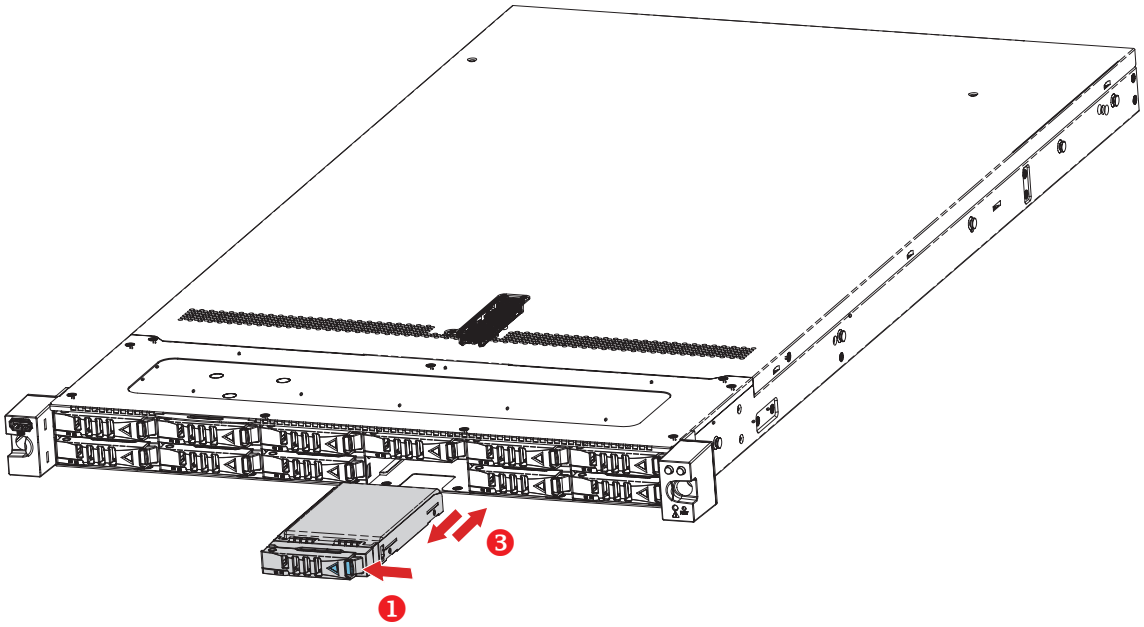
Rear Air duct



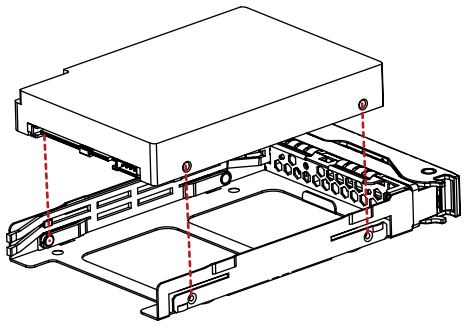
2.7 Disk Drive

2.7.1 Disk Drive: 2.5-inch

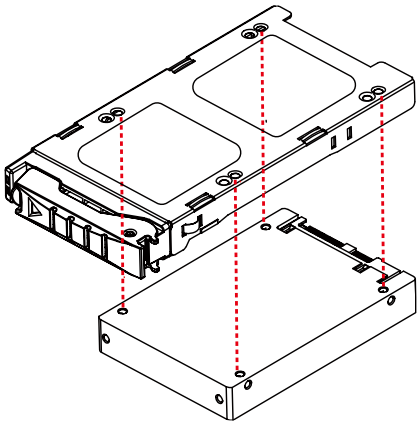
① Press the ejector on the tray to release the handle.
② Pull the tray handle completely outward.
③ Pull the drive tray out of the chassis.



④ Insert the disk drive into the tray. Ensure that the dimples on the tray match the disk drive. For additional assurance, fasten the screws * 4 on the tray to secure the disk drive.



dimple placement



screw placement

⑤ Push the tray with the installed disk drive into the end of the drive slot in the chassis.
⑥ Close the tray handle.

This information is provided for professional technicians only.

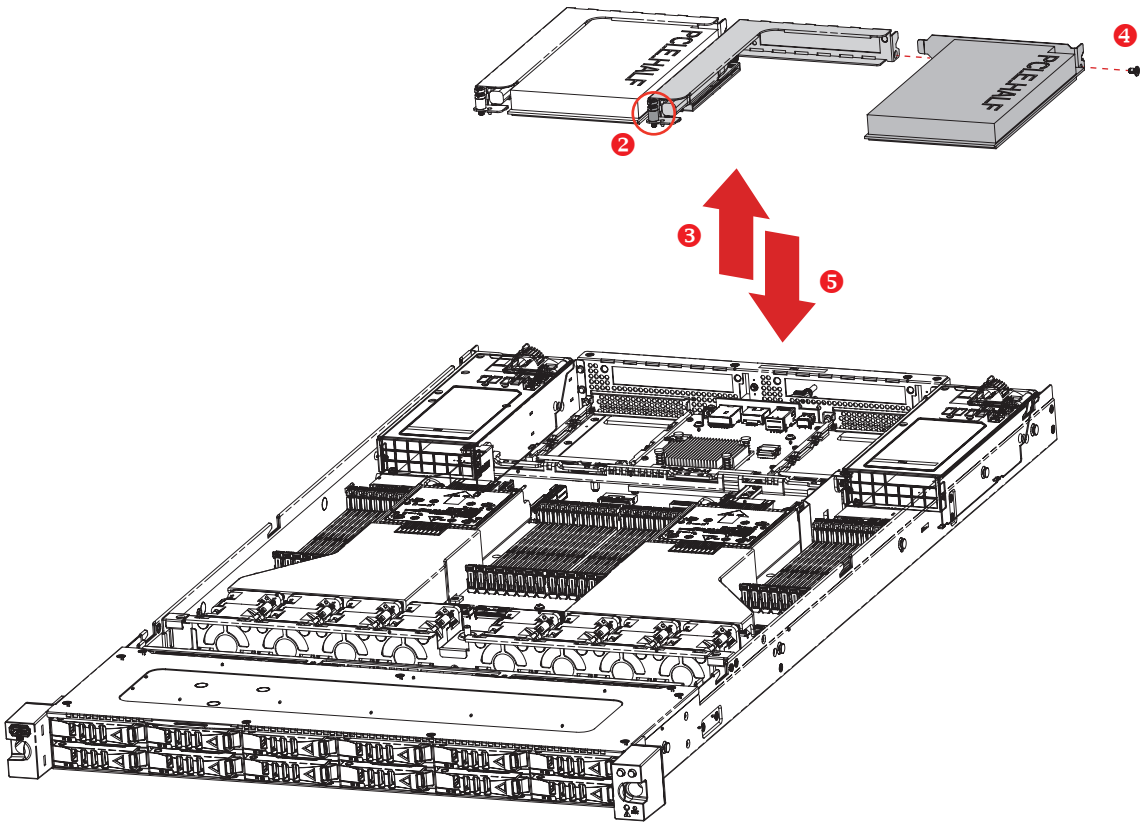
2.7.2 LED Indicator

NVMe

Indicator	Color	Behavior	Description
HDD Activity LEDs	Blue	On	HDD is present.
		Blinking	HDD Activity is detected or External control.
	---	Off	HDD is not connected.
HDD Fail LEDs	Yellow	On	HDD Fault
	Yellow	Blinking	HDD Rebuild
	---	Off	Normal
HDD Locate LED	Green	On	HDD Locate
	---	Off	Normal

2.8 Riser Card

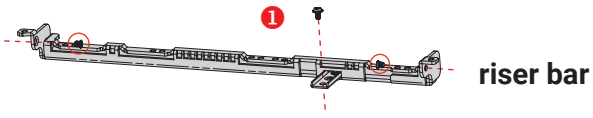
① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Loosen the captive screw.
③ Pull up the riser card and insert the PCIe card into the card slot.
④ Fasten the screw to secure the PCIe card.
⑤ Insert the replaced riser card into the appropriate card slot. Ensure that the card is properly aligned.

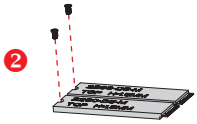


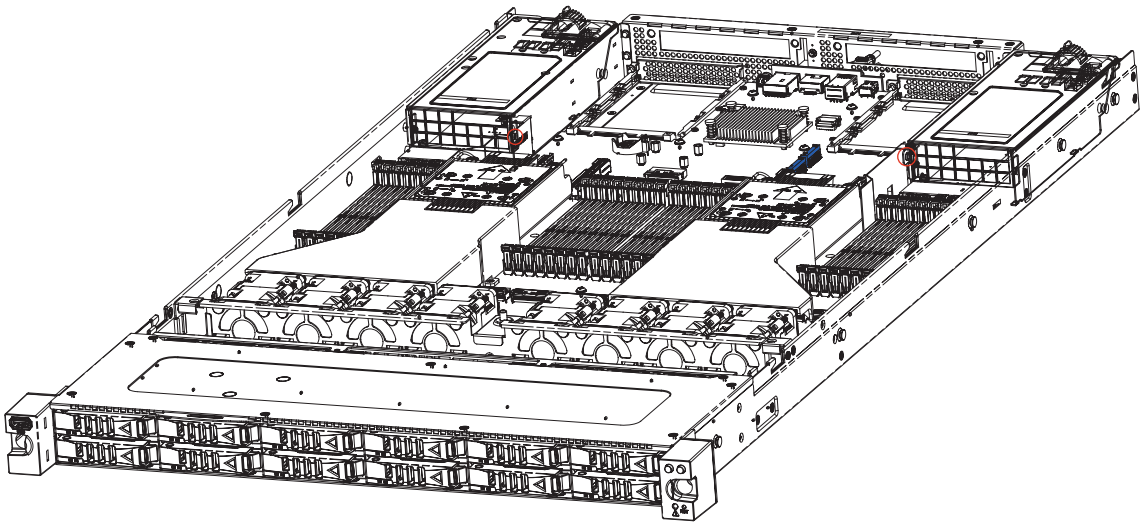
This information is provided for professional technicians only.

2.9 M.2 Card

① Dislodge the screws to remove the riser bar.
② Align and insert the M.2 card into the socket. Ensure the size of your M.2 card match the corresponding standoff on the serverboard.
③ Fasten the screws to secure the M.2 card.
④ Securing the riser bar by fastening the screws to complete the setup.



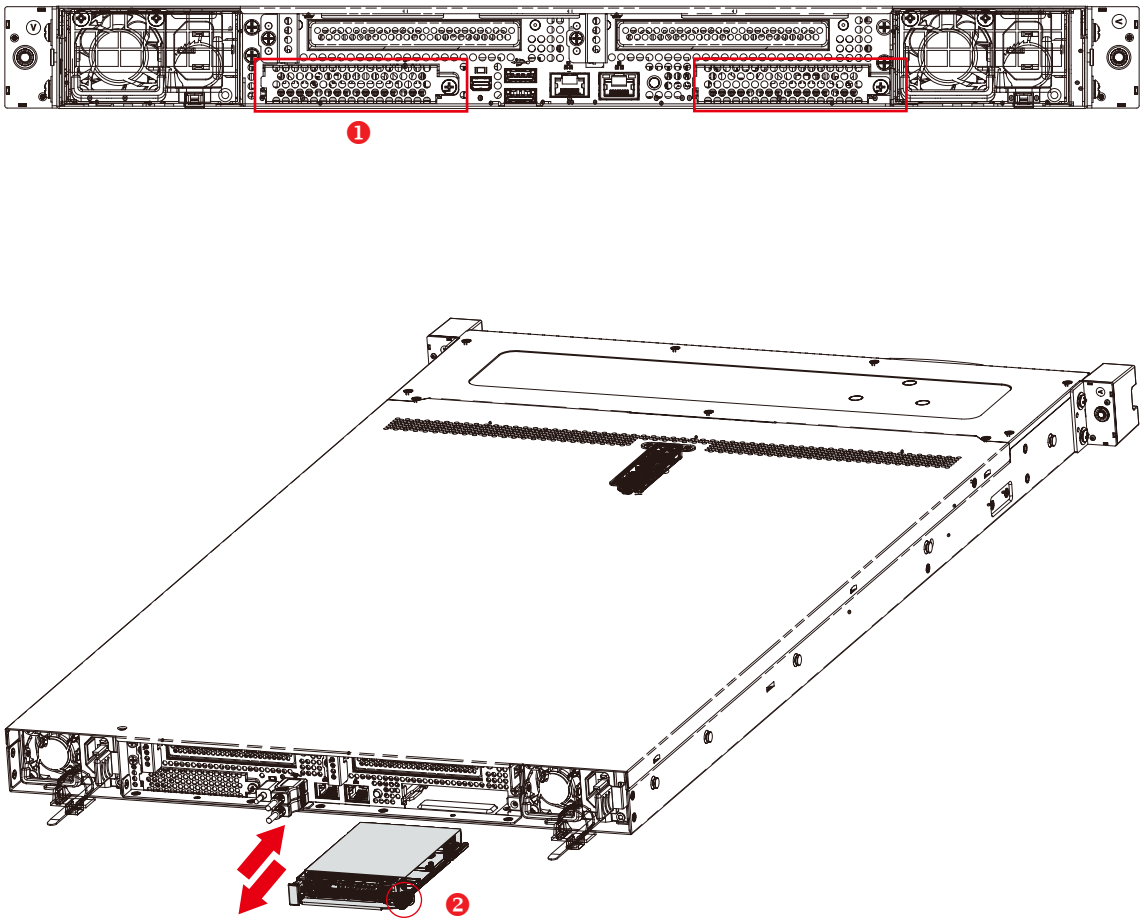




This information is provided for professional technicians only.

2.10 OCP Card

① Remove the metal cover of the OCP 3.0 slot.
② Loosen the thumb screw and pull the OCP card out of chassis.



This information is provided for professional technicians only.

2.11 Slide Rail

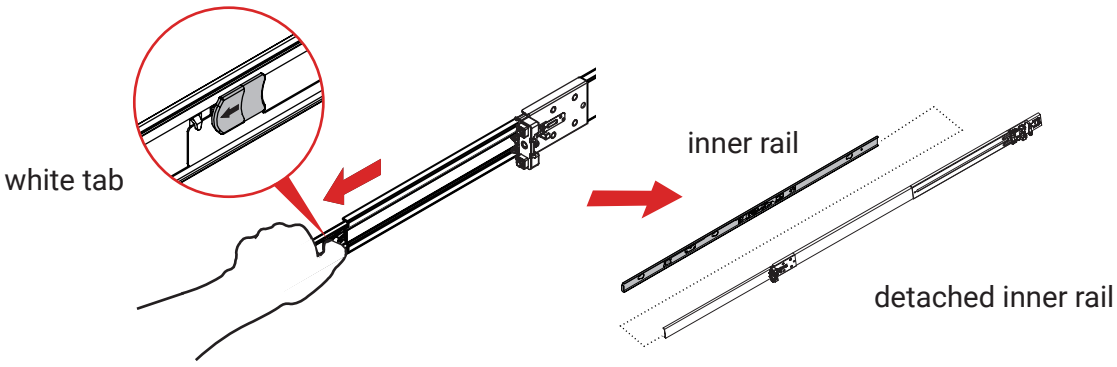
NOTE

This section provides a basic instruction for mounting the slide rail onto the system. Tool-less rails vary per order. The rail in this manual may not exactly match the rail for your system. Please refer to the specifications or quick installation guide that came with your purchased product.

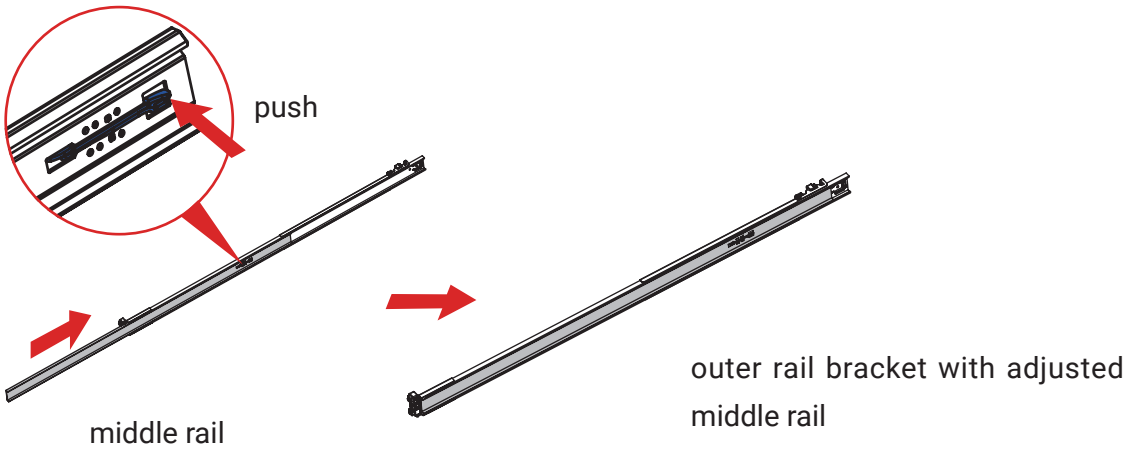
CAUTION

They rack may tilt and fall due to incorrect installation or placed on uneven grounds. The rack must be placed in a flat surface before you begin to slide the system barebone in for servicing.

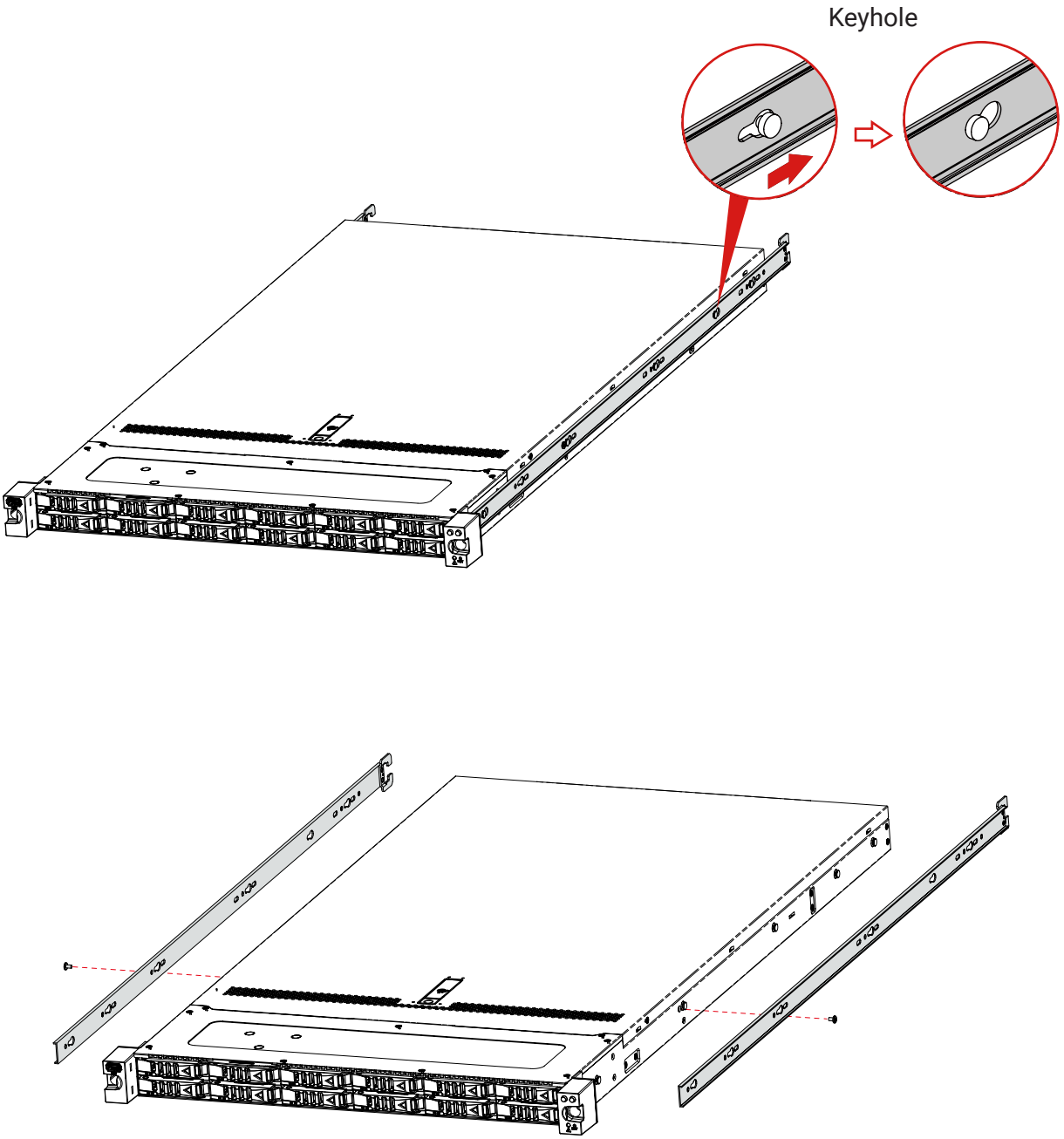
1. Pull the inner rail out of the slide rail until it clicks.
2. Detach the inner rail completely from the slide rail by pulling the white tab forward.



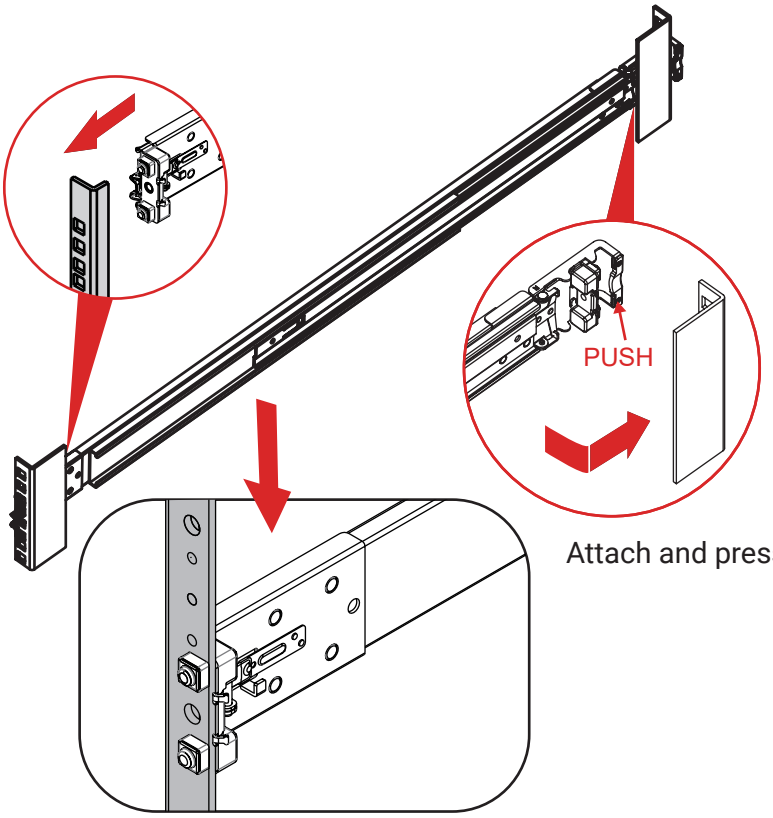
3. After the inner rail is dislodged, adjust the middle rail back to its original position by pushing the tab on the middle rail.



4. Install the inner rail onto the system barebone. Lock the keyholes and secure the screws on sides of the system.



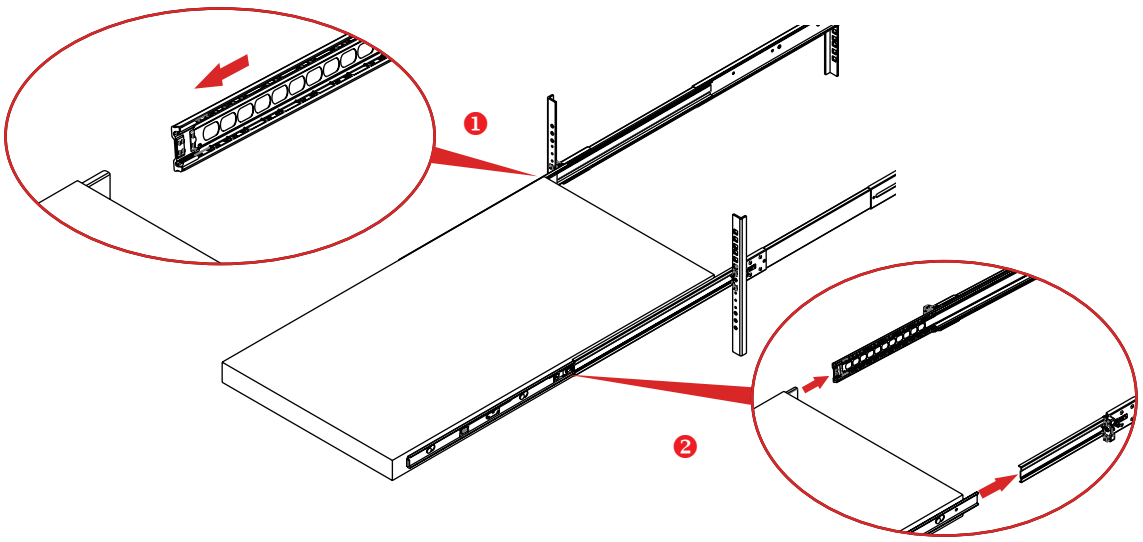
5. Continue installing the outer rail bracket to the mounting frame. Attach the outer rail assembling to the frame and press the bracket to form a rack on both ends. Repeat to fully mount the bracket assembly on the other side.



Attach and press bracket.

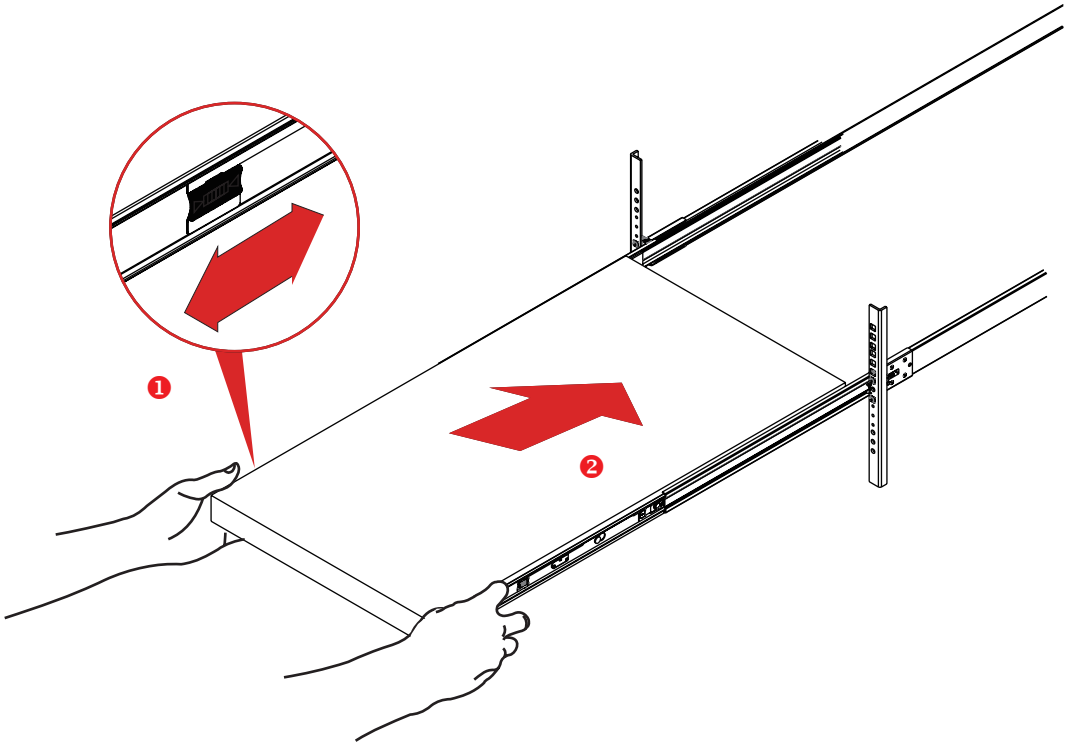
bracket secured.

6. Pull out the middle channel until the ball bearing retainer is locked forward.



NOTE
Verify ball bearing retainer is locked forward.

7. Slide the release tab and push barebone into rack. Make sure the barebone is completely installed onto the rack.

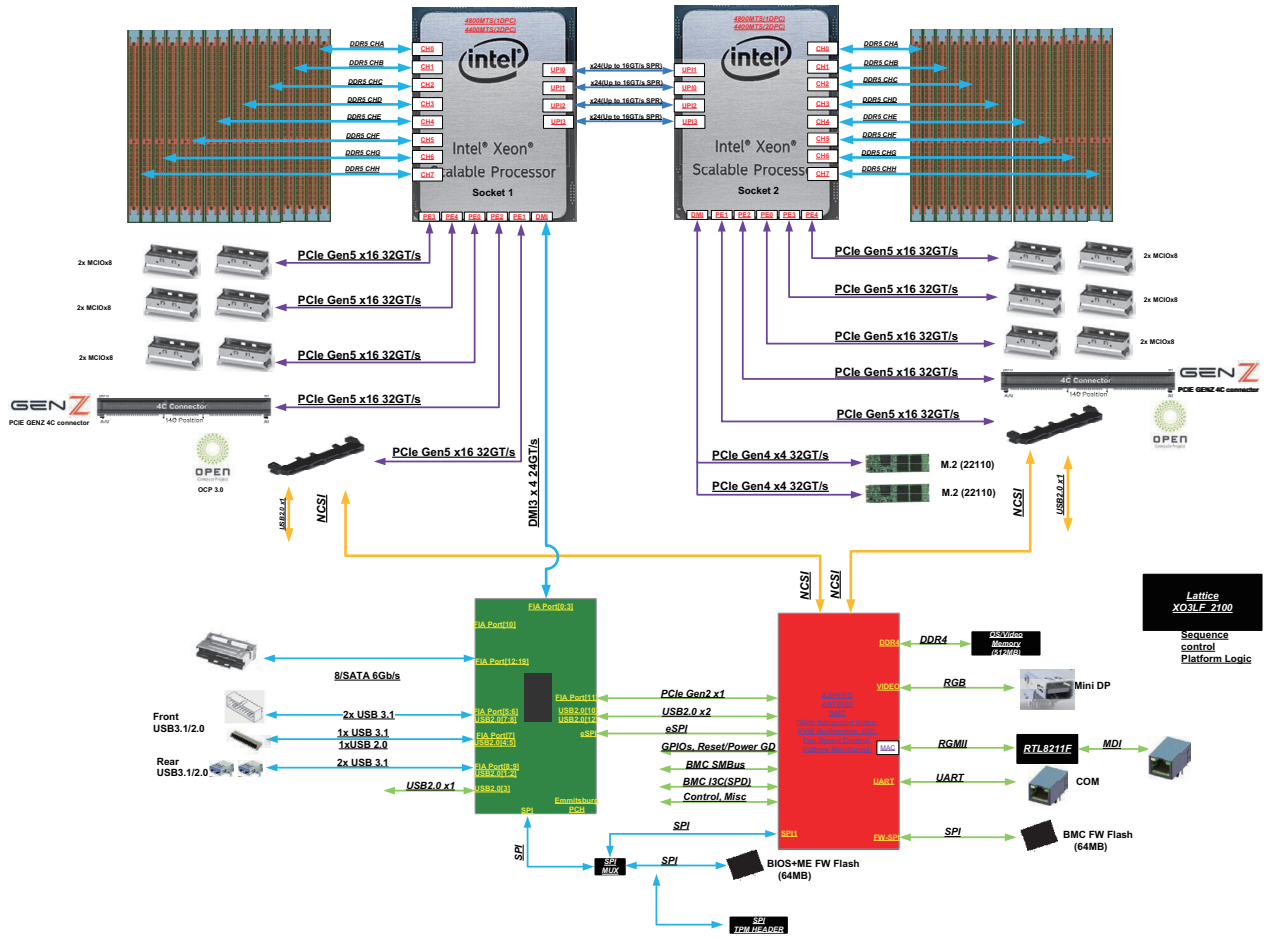


This information is provided for professional technicians only.

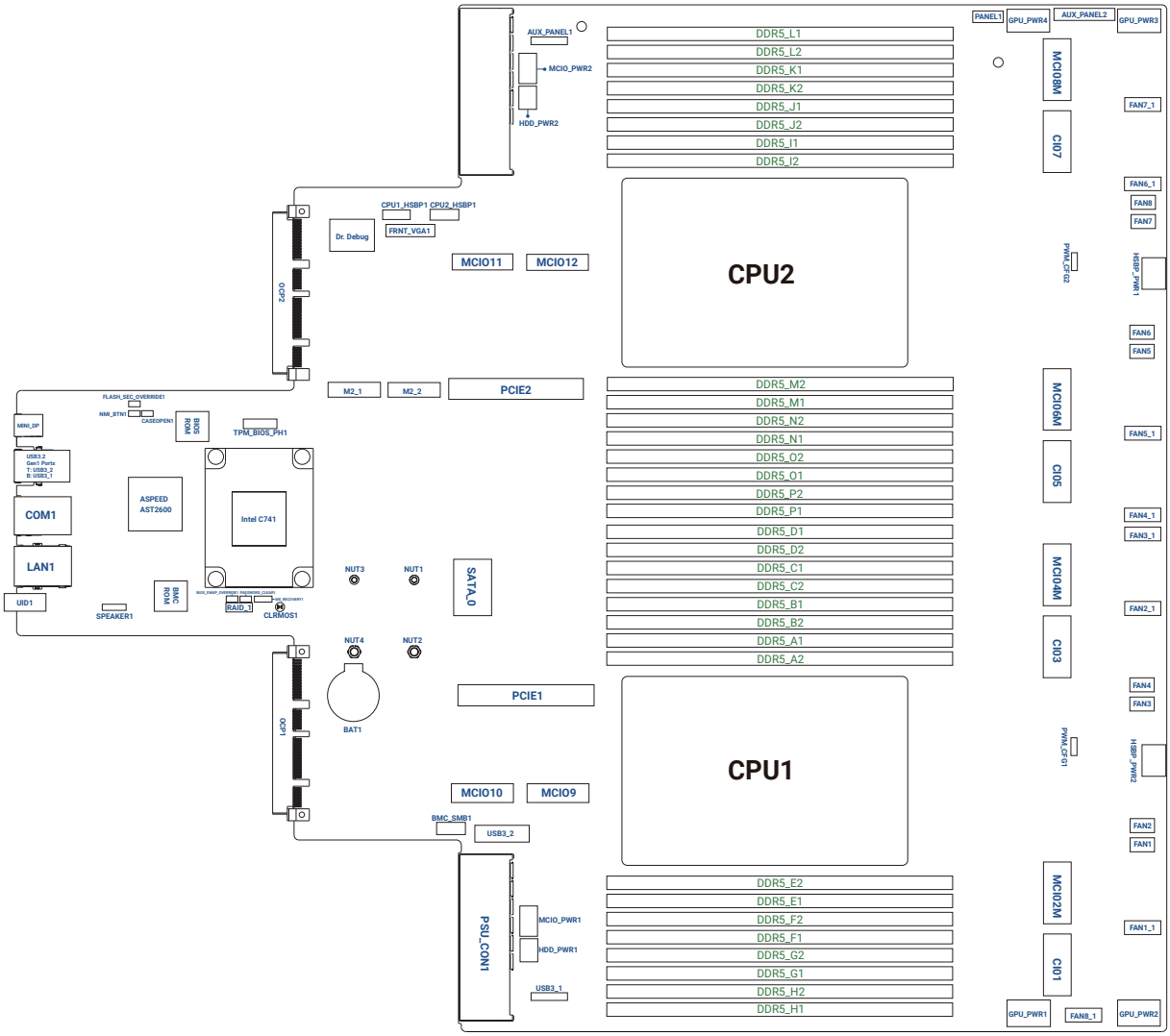
Chapter 3. Hardware Settings

This section provides illustrations that display the internal jumpers, connectors, and system LED indicators on the Tucana motherboard. The motherboard layout and essential connectors are listed below for your reference.

3.1 Block Diagram



3.2 Placement

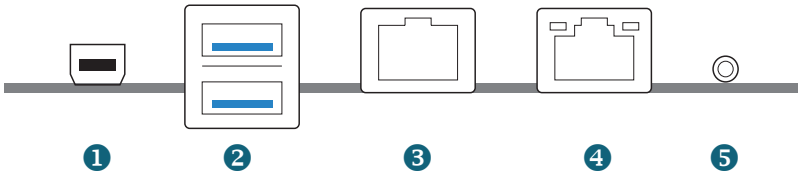


3.3 Content List

Item	Placement	Item	Placement
Non Maskable Interrupt Button	NMI_BTN1	System Fan Connector	FAN7_1 (for 1U system)
Flash Override Jumper	FLASH_SEC_ OVERRIDE1	Mini Cool Edge IO Connector	MCIO7
Chassis Intrusion Header	CASEOPEN1	2 x 288-pin DDR5 DIMM Slots	DDR5_I1, DDR5_ J1
TPM-SPI Header	TPM_BIOS_PH1	System Fan Connector	FAN6_1 (for 1U system)
OCP 3.0 Gen5 x16 Mezzanine Card Slot	OCP2	System Fan Connector	FAN8 (for 2U system)
M.2 Socket (Type 2280/22110)	M2_1	System Fan Connector	FAN7 (for 2U system)
M.2 Socket (Type 2280/22110)	M2_2	2 x 288-pin DDR5 DIMM Slots	DDR5_I2, DDR5_J2
Backplane PCI Express Hot-Plug Connector	CPU1_HSBP1	PWM Configuration Header	PWM_CFG2
Front VGA Header	FRNT_VGA1	HDD Backplane Power Connector	HSBP_PWR1
Backplane PCI Express Hot-Plug Connector	CPU2_HSBP1	LGA 4677 CPU Socket	CPU2
PSU Power Connector	PSU_CON2	2 x 288-pin DDR5 DIMM Slots	DDR5_M2, DDR5_N2
Mini Cool Edge IO Connector	MCIO11	System Fan Connector	FAN6 (for 2U system)
Mini Cool Edge IO Power Connector	MCIO_PWR2	System Fan Connector	FAN5 (for 2U system)
Auxiliary Panel Header	AUX_PANEL1	Mini Cool Edge IO Connector	MCIO6
HDD Power Connector	HDD_PWR2	2 x 288-pin DDR5 DIMM Slots	DDR5_M1, DDR5_N1
Mini Cool Edge IO Connector	MCIO12	System Fan Connector	FAN5_1 (for 1U system)
PCI Express 5.0 x16 Slot	PCIE2	2 x 288-pin DDR5 DIMM Slots	DDR5_O2, DDR5_P2
2 x 288-pin DDR5 DIMM Slots	DDR5_K1, DDR5_ L1	Mini Cool Edge IO Connector	MCIO5
2 x 288-pin DDR5 DIMM Slots	DDR5_K2, DDR5_ L2	2 x 288-pin DDR5 DIMM Slots	DDR5_O1, DDR5_P1
System Panel Header	PANEL1	System Fan Connector	FAN4_1 (for 1U system)
GPU Power Connector	GPU_PWR4	System Fan Connector	FAN3_1 (for 1U system)
Auxiliary Panel Header	AUX_PANEL2	2 x 288-pin DDR5 DIMM Slots	DDR5_C1, DDR5_D1
GPU Power Connector	GPU_PWR3	Mini Cool Edge IO Connector	MCIO4
Mini Cool Edge IO Connector	MCIO8	2 x 288-pin DDR5 DIMM Slots	DDR5_C2, DDR5_D2

Item	Placement	Item	Placement
System Fan Connector	FAN2_1 (for 1U system)	2 x 288-pin DDR5 DIMM Slots	DDR5_G2, DDR5_H2
2 x 288-pin DDR5 DIMM Slots	DDR5_A1, DDR5_B1	2 x 288-pin DDR5 DIMM Slots	DDR5_G1, DDR5_H1
Mini Cool Edge IO Connector	MCIO3	PCI Express 5.0 x16 Slot	PCIE1
System Fan Connector	FAN4 (for 2U system)	Mini Cool Edge IO Connector	MCIO9
System Fan Connector	FAN3 (for 2U system)	Mini Cool Edge IO Power Connector	MCIO_PWR1
2 x 288-pin DDR5 DIMM Slots	DDR5_A2, DDR5_B2	Front USB 3.2 Gen1 Header	USB3_1
PWM Configuration Header	PWM_CFG1	HDD Power Connector	HDD_PWR1
HDD Backplane Power Connector	HSBP_PWR2	Front USB 3.2 Gen1 Header	USB3_2
LGA 4677 CPU Socket	CPU1	PSU Power Connector	PSU_CON1
2 x 288-pin DDR5 DIMM Slots	DDR5_E2, DDR5_F2	BMC SMBus Header	BMC_SMB1
System Fan Connector	FAN2 (for 2U system)	Mini Cool Edge IO Connector	MCIO10
System Fan Connector	FAN1 (for 2U system)	SATA Connector	SATA_0
Mini Cool Edge IO Connector	MCIO2	Clear CMOS Pad	CLRMOS1
2 x 288-pin DDR5 DIMM Slots	DDR5_E1, DDR5_F1	OCP 3.0 Gen5 x16 Mezzanine Card Slot	OCP1
System Fan Connector	FAN1_1 (for 1U system)	ME Recovery Jumper	ME_RECOVERY1
Mini Cool Edge IO Connector	MCIO1	Password Reset Jumper	PASSWORD_CLEAR1
GPU Power Connector	GPU_PWR2	Virtual RAID On CPU Header	RAID_1
System Fan Connector	FAN8_1 (for 1U system)	BIOS Swap Override Jumper	BIOS_SWAP_OVERRIDE1
GPU Power Connector	GPU_PWR1	Speaker Header	SPEAKER1

3.4 Input and Output Panel

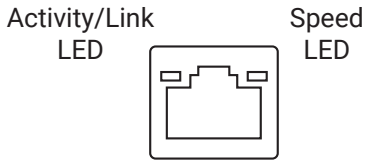


Item	Description	Item	Description
1	Mini Display Port (MINI_DP)	4	LAN RJ-45 Port (IPMI_LAN)*
2	USB 3.2 Gen1 Ports (USB3_1_2)	5	UID Switch (UID1)
3	RJ45 Serial Port (COM1)		

LAN Port LED Indications

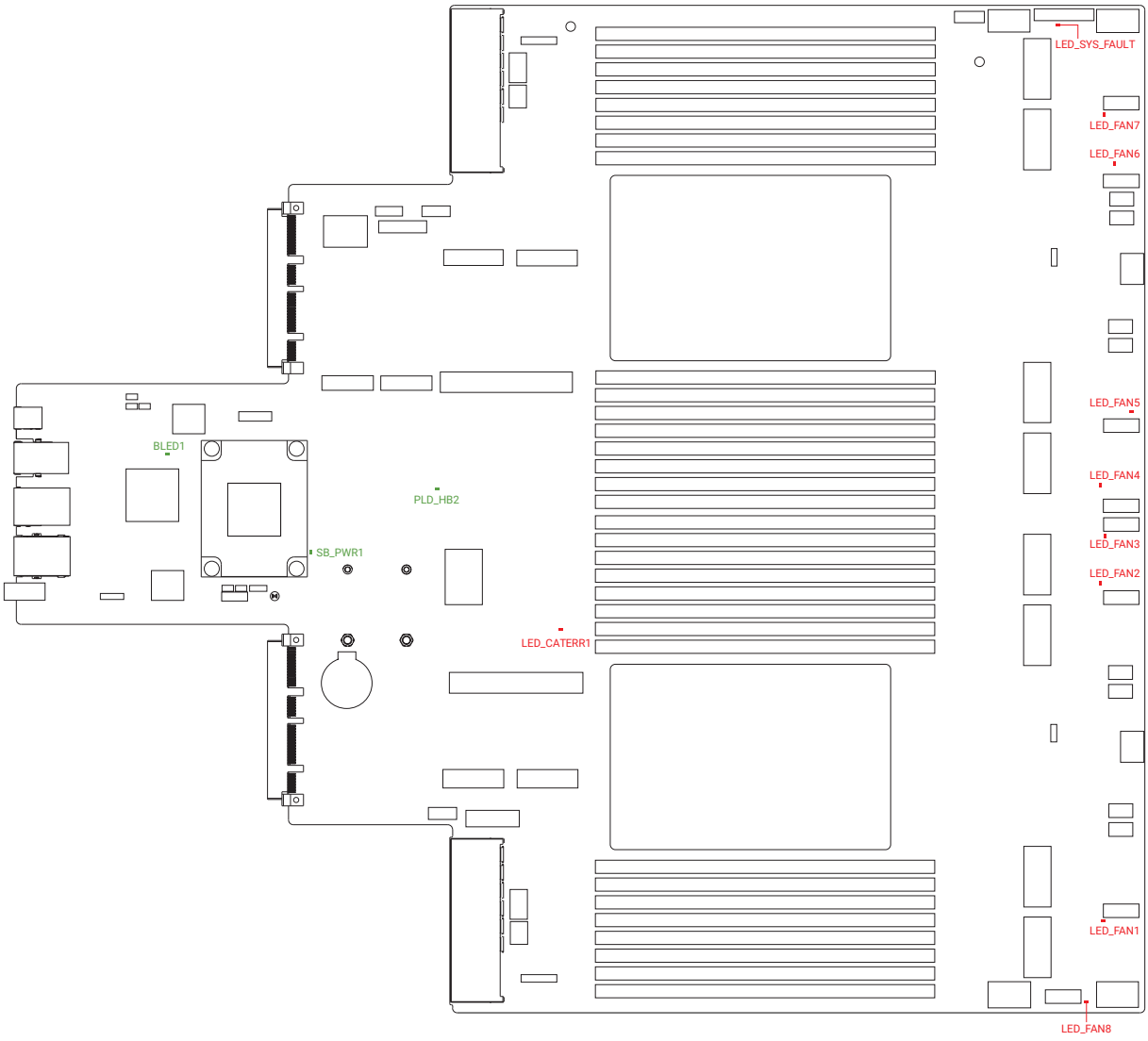
*There is an LED on each side of IPMI LAN port. Please refer to the table below for the LAN port LED indications.

LAN LED Indicator



Item	Color	Behavior
Activity/Link LED	Yellow (blinking)	Data Activity
	Off	No Link
	On	Link
Speed LED	Off	10M bps connection or no link.
	Orange	100M bps connection.
	Green	1G bps connection.

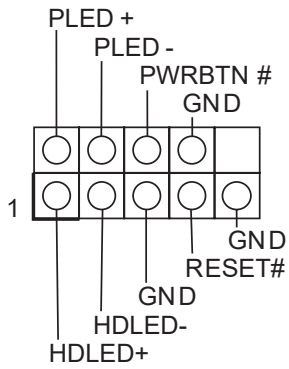
3.5 Onboard LED Indicator

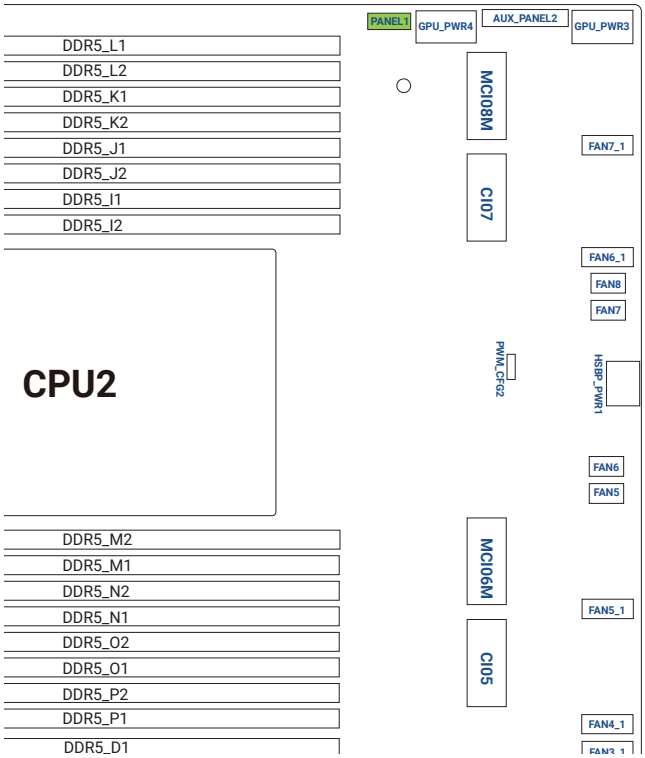


Item	Color	Description
LED_SYS_FAULT	Red	System failed
LED_FAN7	Red	FAN7 failed
LED_FAN6	Red	FAN6 failed
LED_FAN5	Red	FAN5 failed
LED_FAN4	Red	FAN4 failed
LED_FAN3	Red	FAN3 failed
LED_FAN2	Red	FAN2 failed
LED_FAN1	Red	FAN1 failed
LED_FAN8	Red	FAN8 failed
LED_CATERR1	Red	CPU CATERR failed
PLD_HB2	Green	FPGA heartbeat LED
SB_PWR1	Green	STB PWR ready
BLED1	Green	BMC heartbeat LED

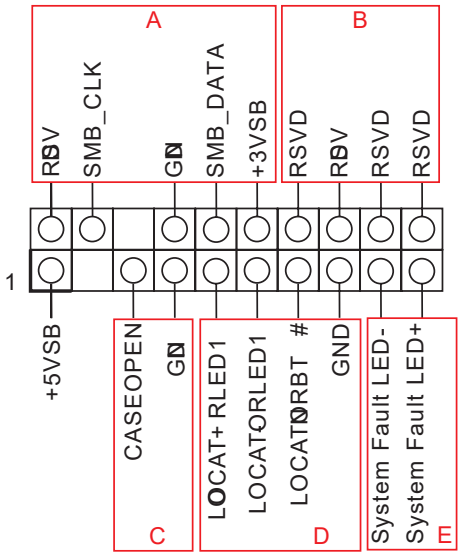
3.6 Connector Definition

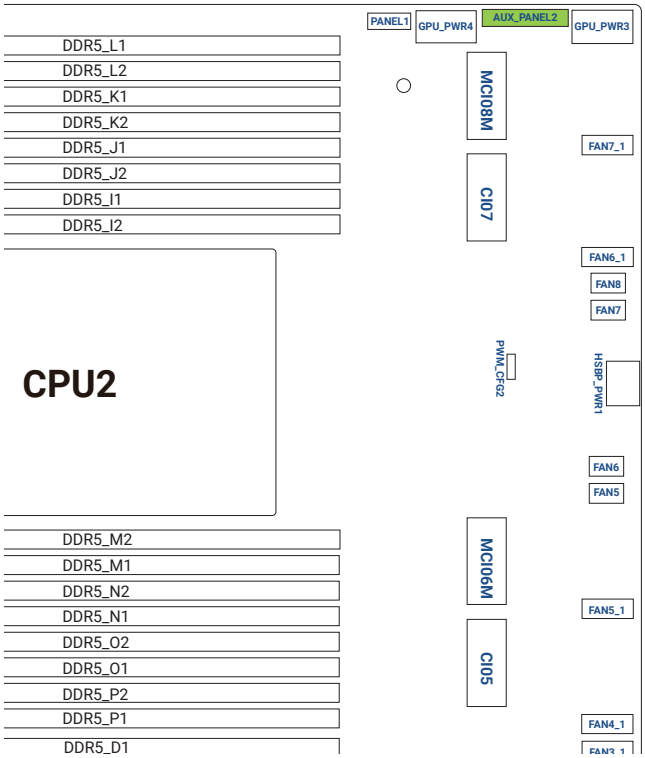
System Panel Header (PANEL1)
This is a 9-pin header that connect the power switch, reset switch and system status indicator on the chassis to this header.





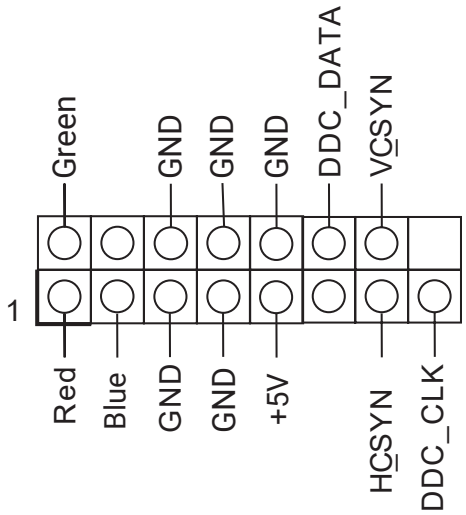
Auxiliary Panel Header (AUX PANEL2)
This is a 18-pin header that supports multiple functions on the front panel.

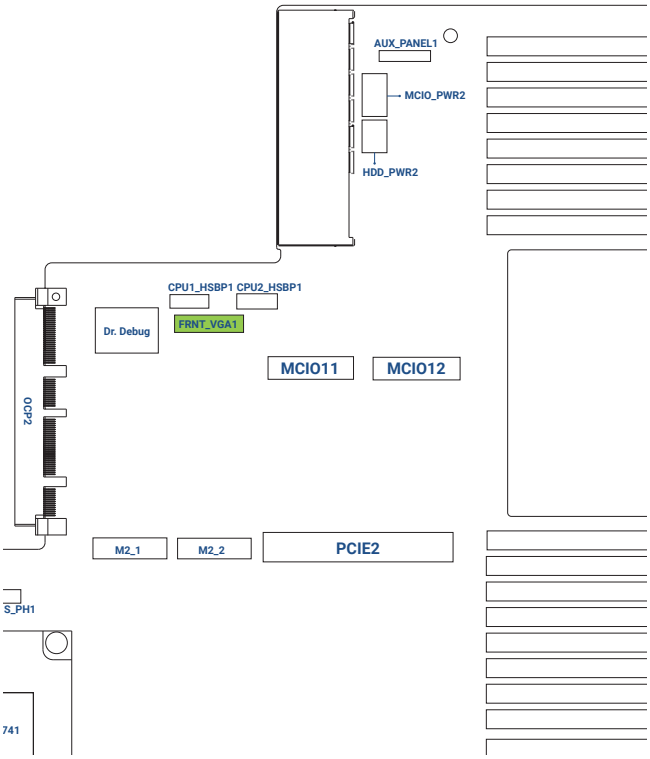




Front VGA Header (FRNT_VGA1)

This is a 15-pin connector that connect either end of VGA_2X8 cable to VGA header.

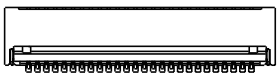


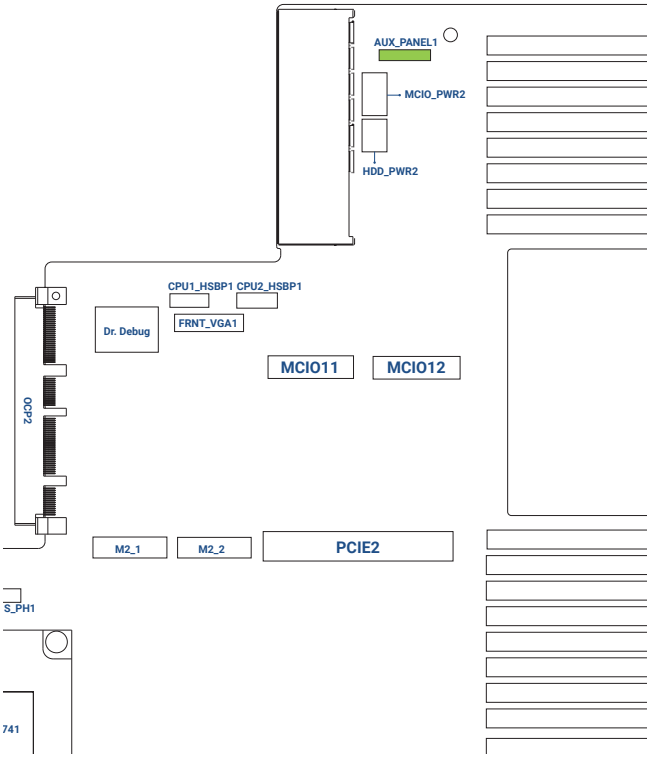


Auxiliary Panel Header (AUX_PANEL1)

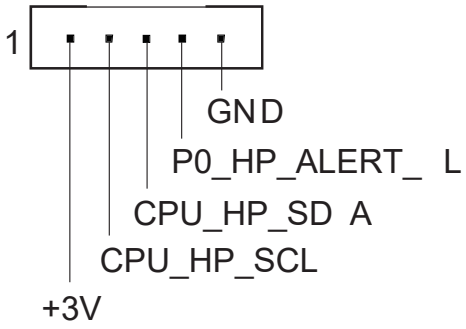
This 26-pin header supports multiple functions on the front panel, including front panel SMB, internet status indicator.

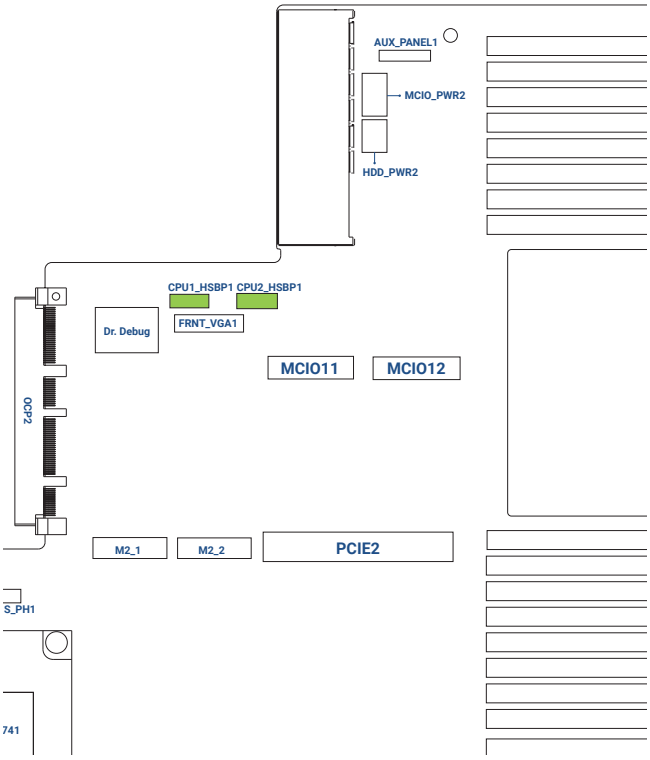
1	+3VSB
2	+3VSB
3	N/A
4	LOCATORLED+
5	PLED-
6	LOCATORLED-
7	+3V
8	N/A
9	System Fault LED-
10	HDLED-
11	PWRBTN#
12	N/A
13	GND
14	N/A
15	RESET#
16	SMB_DATA
17	SMB_CLK
18	GND
19	LOCATORBTN#
20	N/A
21	N/A
22	N/A
23	N/A
24	N/A
25	GND
26	GND



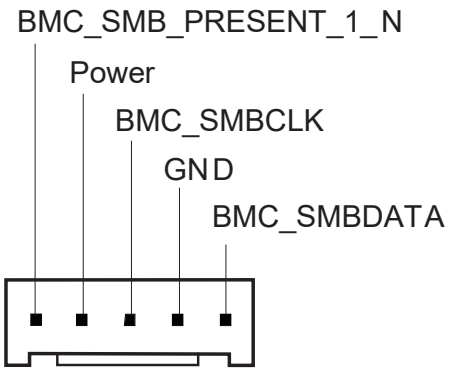


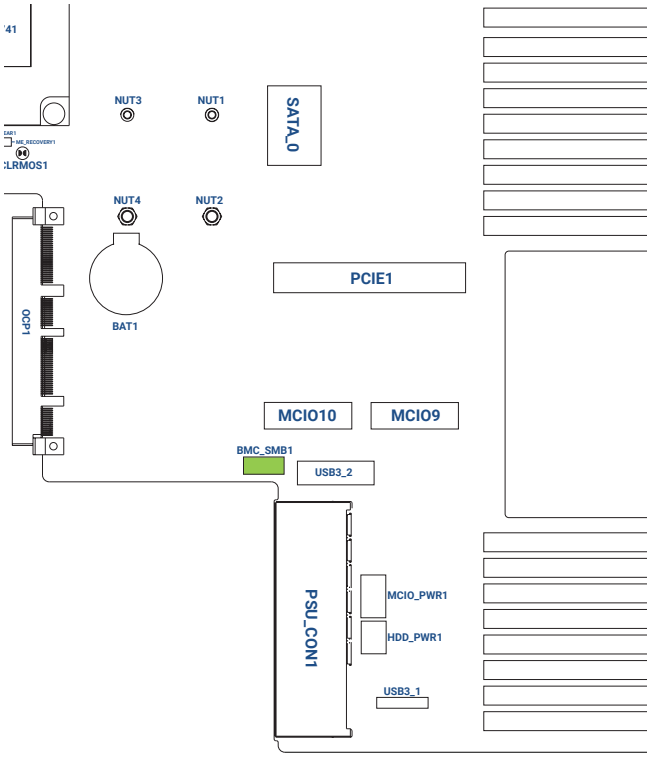
Backplane PCI Express Hot-Plug Connectors (CPU1_ HSBP1 & CPU2_ HSBP1)
These 5-pin headers are used for the hot plug feature of HDDs on the backplane.





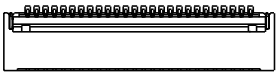
BMC SMB Headers (BMC_SMB1)
These 5-pin headers are used for the SM BUS devices.

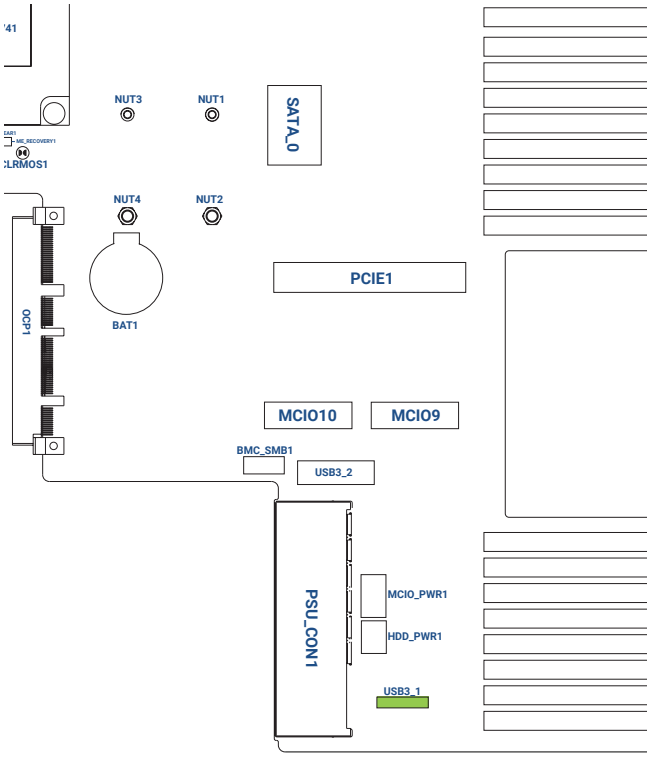




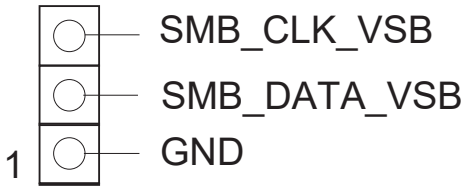
Front USB 3.2 Gen1 Header (USB3_1)
This is a 26-pin header support two USB 3.2 Gen1 ports.

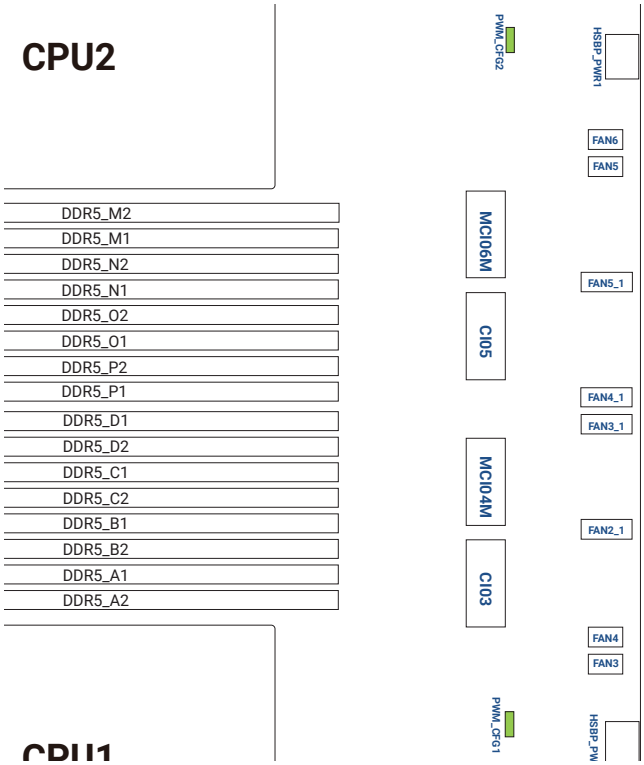
1	+3VSB
2	+3VSB
3	N/A
4	LOCATORLED+
5	PLED-
6	LOCATORLED-
7	+3V
8	N/A
9	System Fault LED-
10	HDLED-
11	PWRBTN#
12	N/A
13	GND
14	N/A
15	RESET#
16	SMB_DATA
17	SMB_CLK
18	GND
19	LOCATORBTN#
20	N/A
21	N/A
22	N/A
23	N/A
24	N/A
25	GND
26	GND



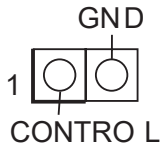


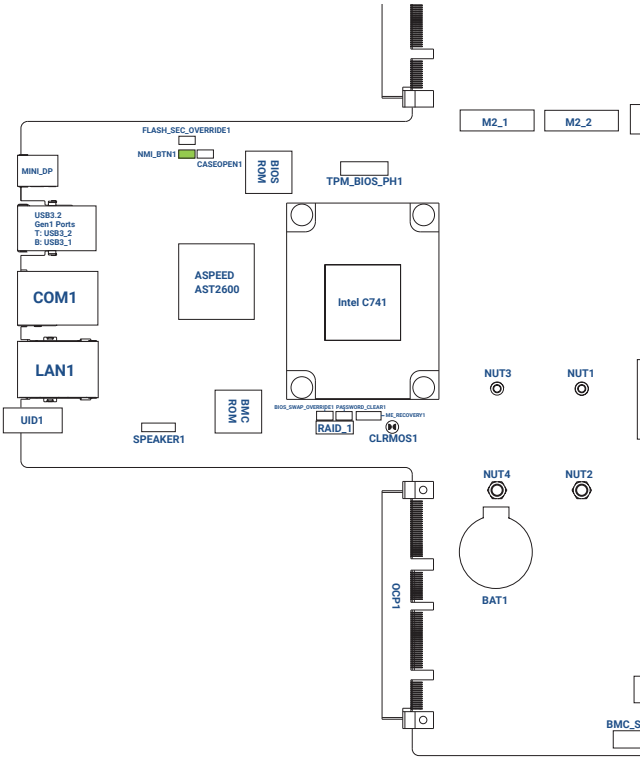
PWM Configuration Header
(PWM_CFG1 & PWM_CFG2)
These 3-pin header are used for PWM configurations.



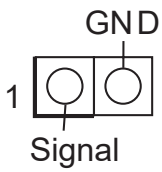


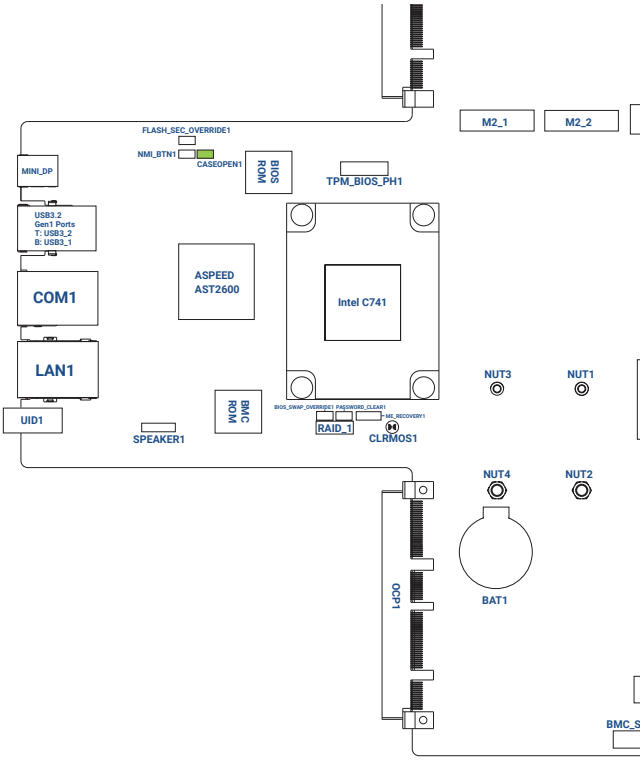
Non Maskable Interrupt Button Header (NMI_BTN1)
This is a 2-pin header that connect a NMI device.





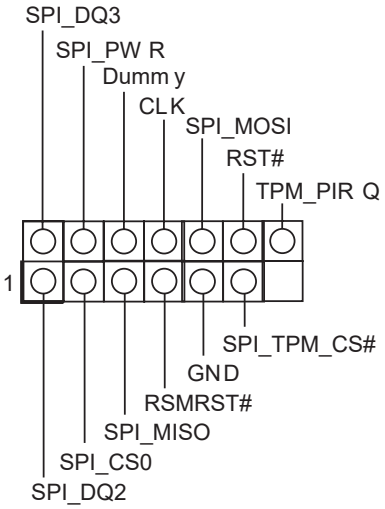
Chassis Intrusion Header (CASEOPEN1)
This motherboard supports CASE OPEN detection featurethat detects if the chassis cover has been removed. This feature requires a chassis with chassis intrusion detection design.

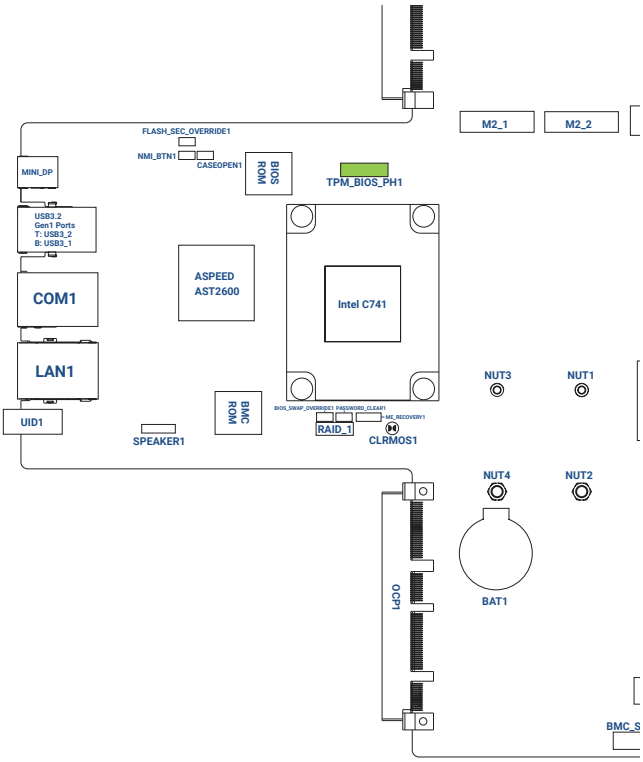




TPM-SPI Header (TPM_BIOS_PH1)

This is a 13-pin header that supports SPI Trusted Platform Module (TPM) system, which can securely store keys, digital certificates, passwords, and data.

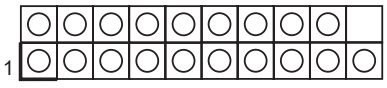


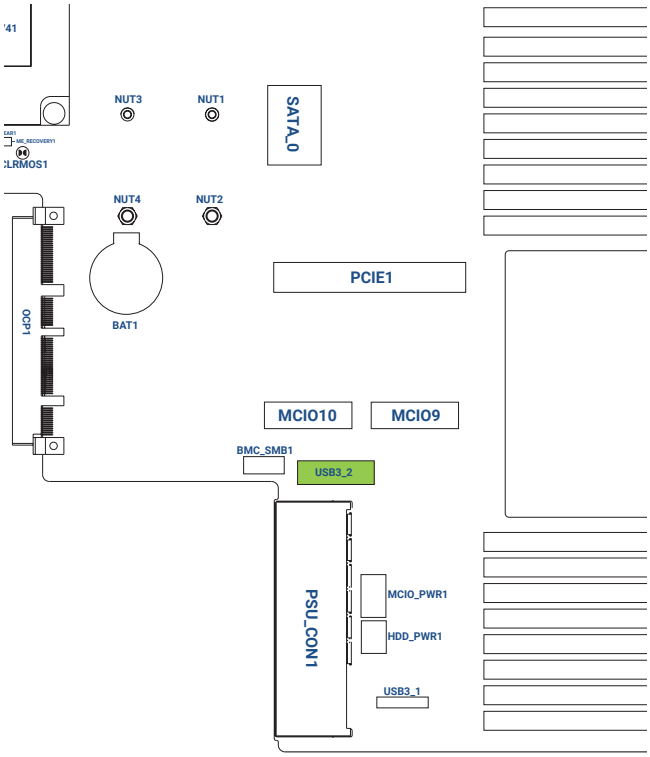


USB 3.2 Gen1 Header (USB3_2)

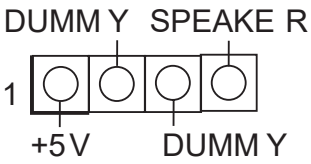
This is a 19-pin connector that can support two USB 3.2 Gen1 ports.

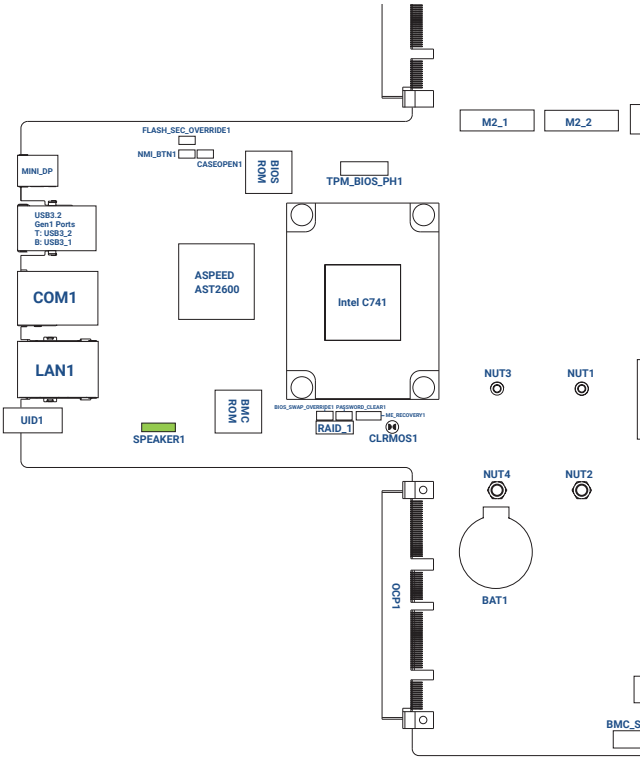
Dummy	1	11	IntA_PA_D+
IntA_PB_D+	2	12	IntA_PA_D-
IntA_PB_D-	3	13	GND
GND	4	14	IntA_PA_SSTX+
IntA_PB_SSTX+	5	15	IntA_PA_SSTX-
IntA_PB_SSTX-	6	16	GND
GND	7	17	IntA_PA_SSRX+
IntA_PB_SSRX+	8	18	IntA_PA_SSRX-
IntA_PB_SSRX-	9	19	Vbus
Vbus	10		



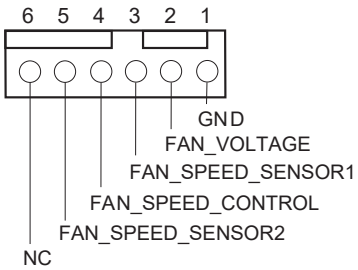


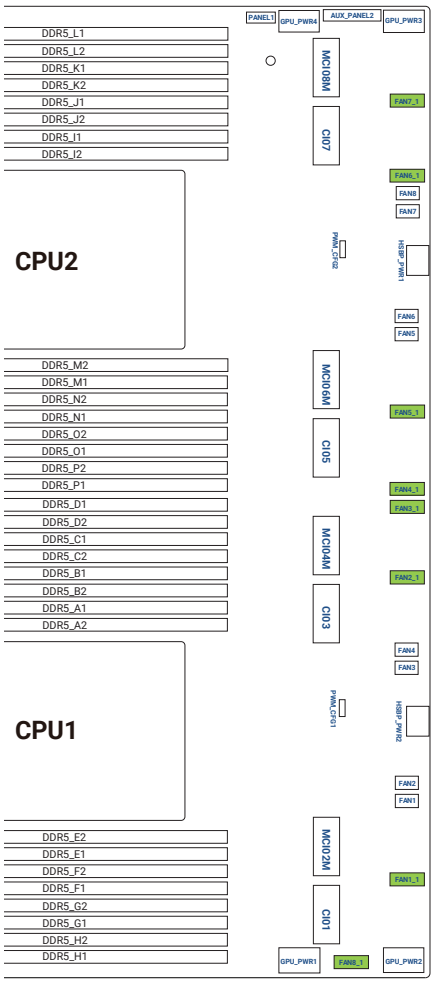
Chassis Speaker Header (SPEAKER1)
This is a 4-pin connector that connect the chassis speaker.



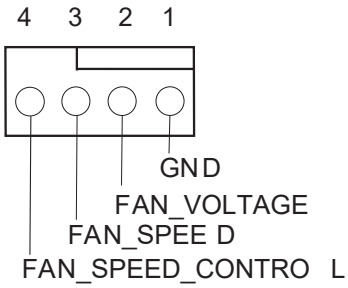


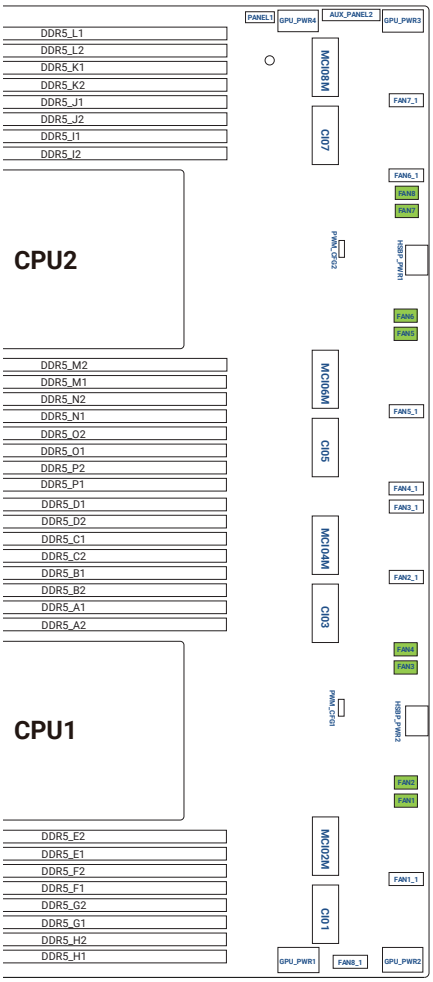
System Fan Connectors [for 1U system] (FAN1~8_1)
This is a 6-pin header that support Fan Control.(Please connect fan cables to the fan connectors and match the black wire to the ground pin.)



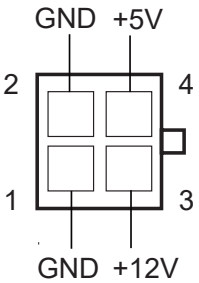


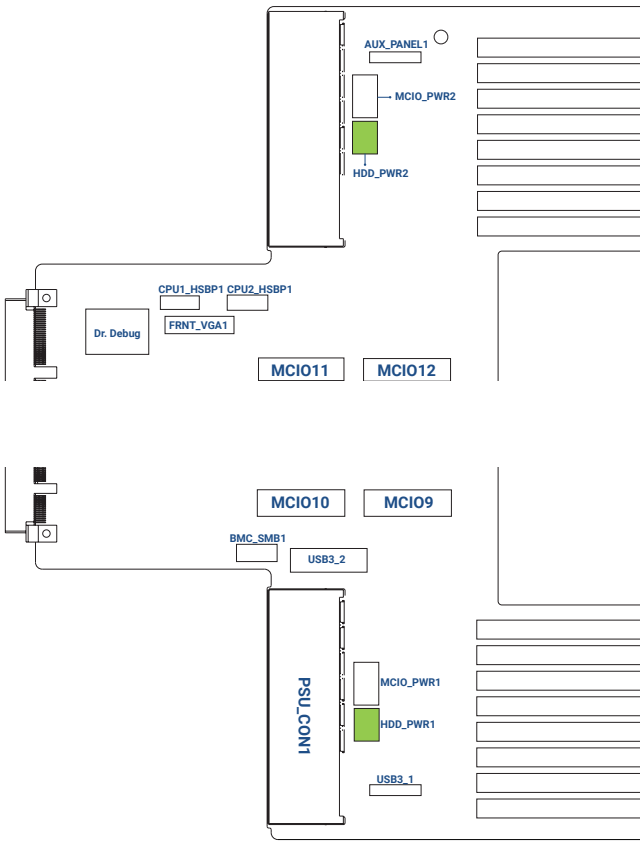
System Fan Connectors [for 2U system] (FAN1~8)
This is a 4-pin header that support Fan Control.(Please connect fan cables to the fan connectors and match the black wire to the ground pin.)





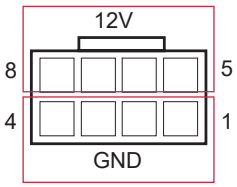
SATA Power Connector (HDD_PWR1 & HDD_PWR2)
This is a 2x2-Pin connector. Use a SATA power cable to connect this SATA Power Connector and the SATA HDD for supplying power from the motherboard, when using DC-IN mode without SATA power supply.

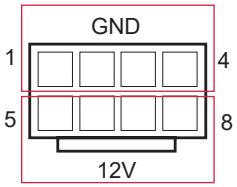


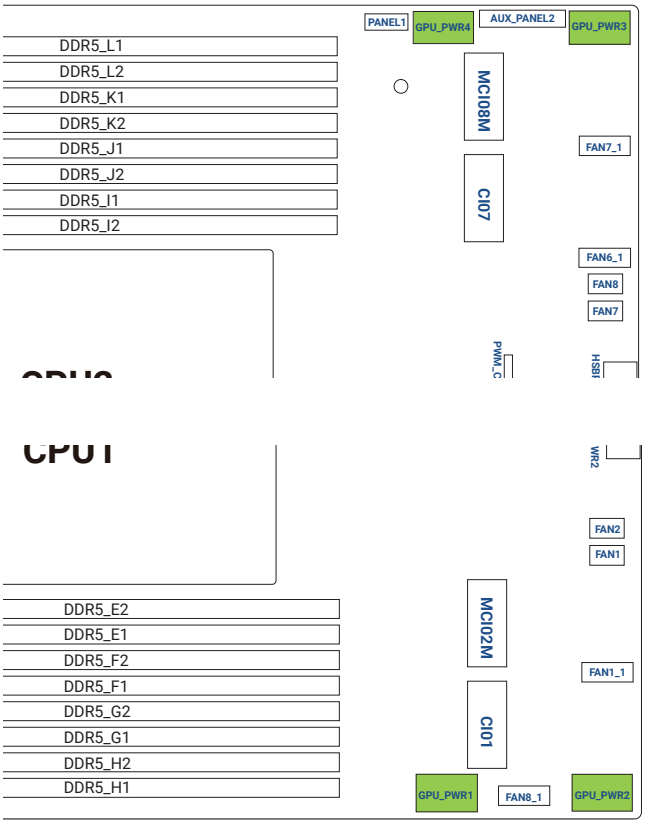


GPU Power Connectors (GPU_PWR1~4)

These are 8-pin ATX 12V GPU power connectors.

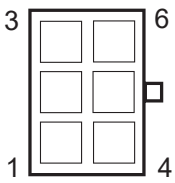




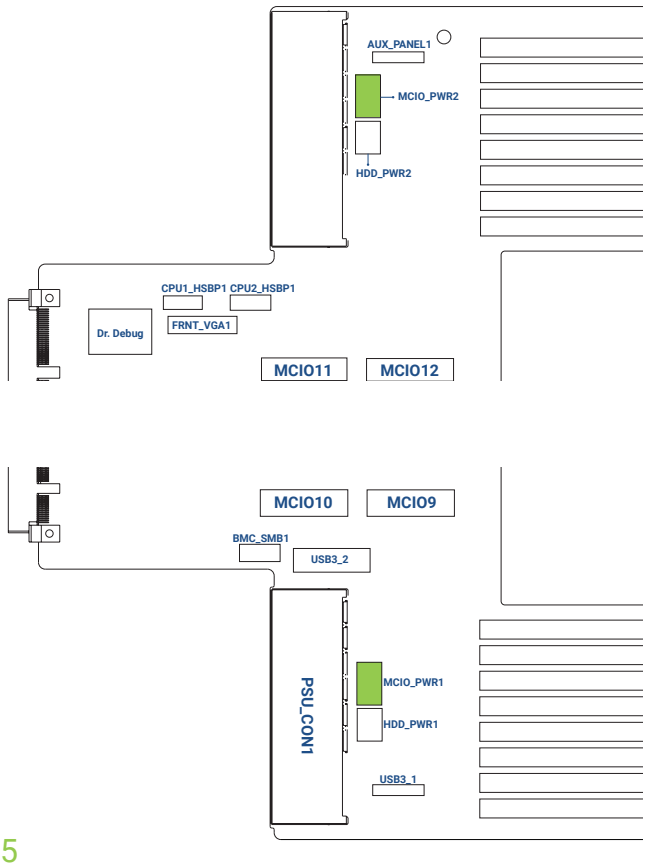


MCIO Power Connectors (MCIO_PWR1 & MCIO_PWR2)

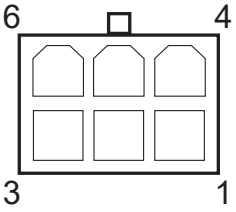
These are 2x3-pin MCIO power connectors.



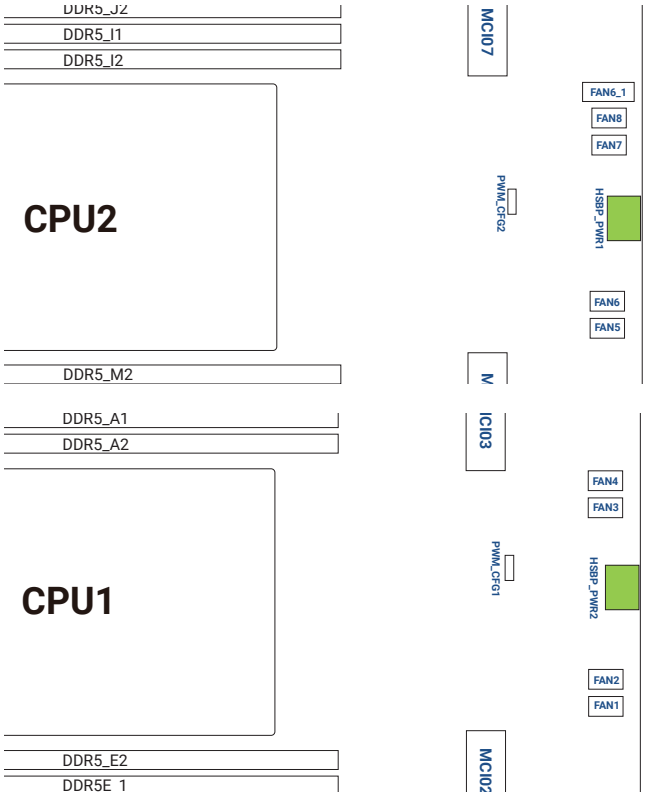
+12V	4	1	GND
+3.3V	5	2	GND
+3.3VSB	6	3	GND



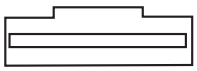
HDD Backplane Power Connector Right-Angle(HSBP_PWR1 & HSBP_PWR2)
This is a 2x3-pin connector that connect a HDD with a 6-pin power cable.

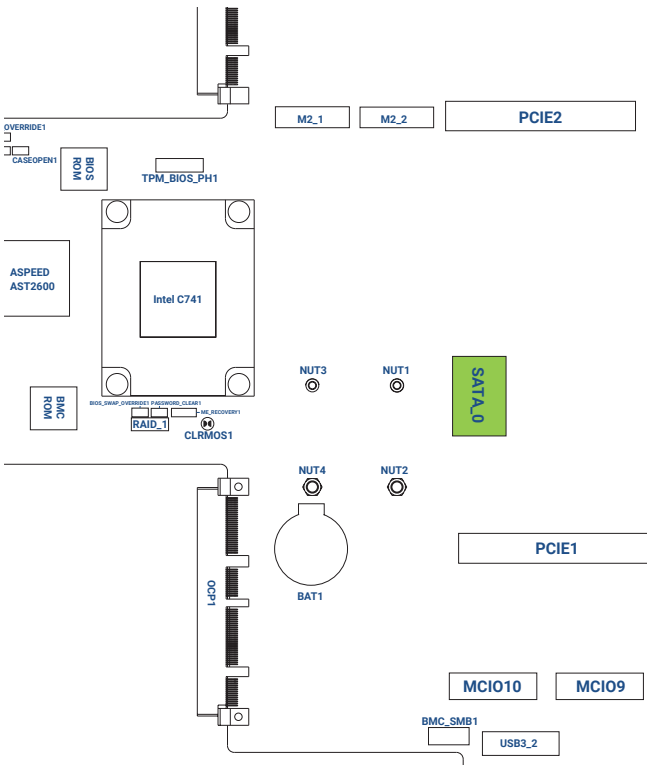


+12V	4	1	GND
+12V	5	2	GND
+12V	6	3	GND

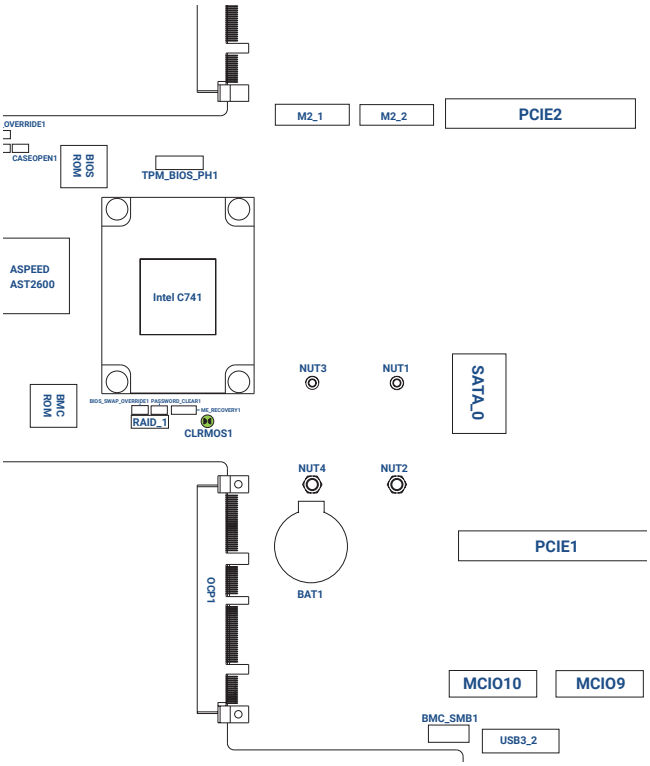


SATA Connectors Right-Angle (SATA_0)
The SATA connector supports a SATA data cable for internal storage device.

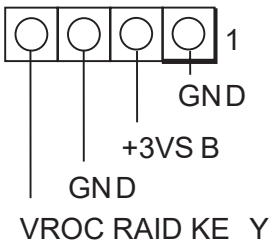


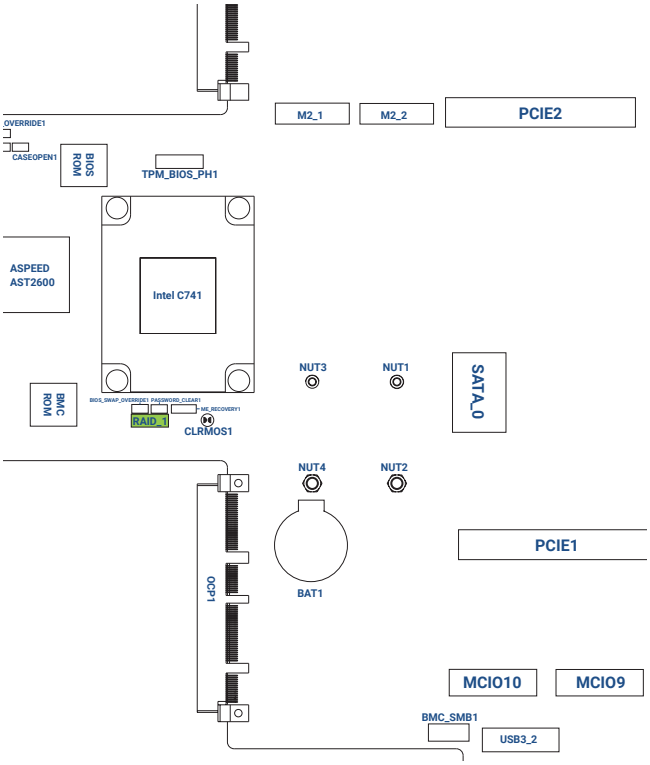


Clear CMOS Pad (CLRMOS1)
This allows user to clear the data in CMOS. To clear CMOS, take out the CMOS battery and short the Clear CMOS Pad.

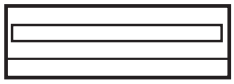


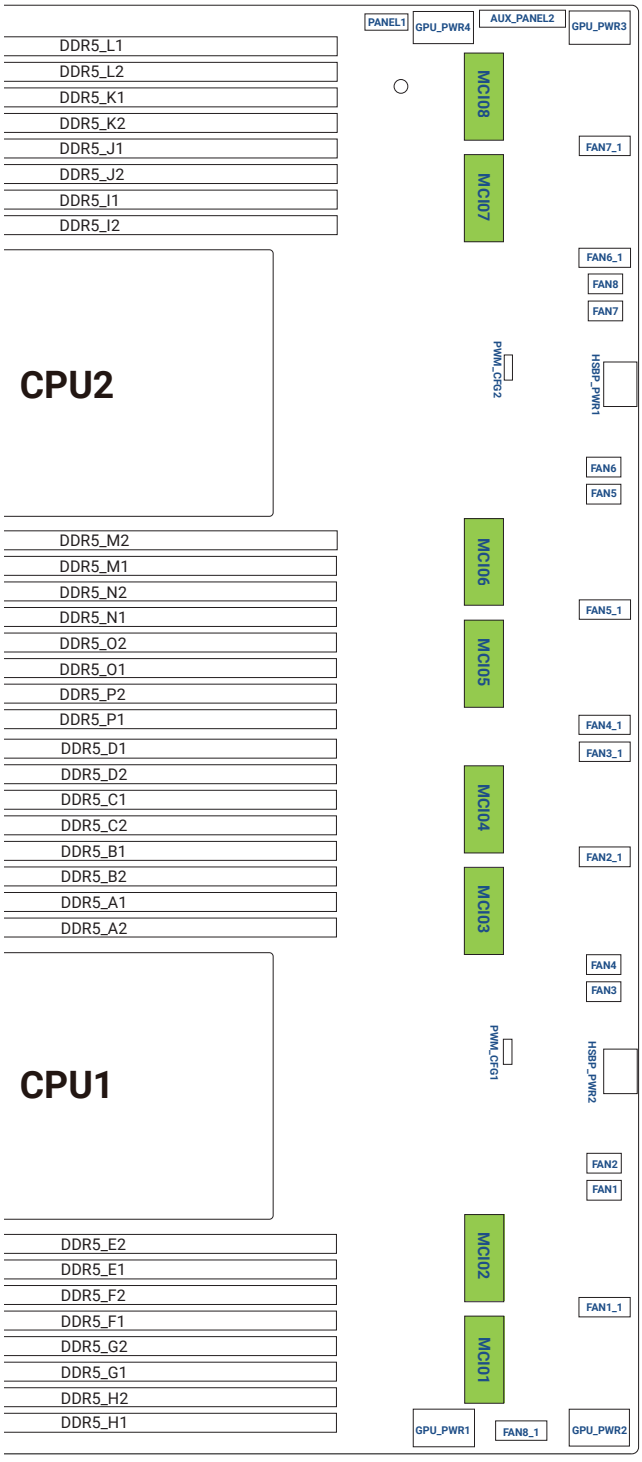
Virtual RAID On CPU Header (RAID_1)
This 4-pin connector supports Intel® Virtual RAID on CPU and NVME/AHCI RAID on CPU PCIE.





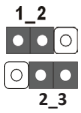
Mini Cool Edge IO x8 Connector
Right-Angle (MCIO1~8)
This motherboard supports 12 Mini Cool Edge IO 8x Connectors. Please connect these connectors to the HDD backplane board.





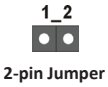
3.7 Jumper Setup

ME Recovery Jumper (3-pin ME_RECOVERY1)



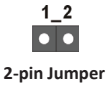
ME_RECOVERY1	Setting	
pin1-2	Normal	Default
pin2-3	ME Force Udate	

Flash Override Jumper (FLASH_SEC_OVERRIDE1)



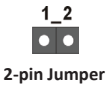
FLASH_SEC_OVERRIDE1	Setting	
Open	Enable FLASH Security	Default
Short	Disable FLASH Security	

Password Reset Jumper (2-pin PASSWORD_CLEAR1)



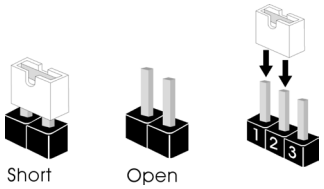
PASSWORD_CLEAR1	Setting	
Open	Password Clear	
Short	Normal Mode	Default

BIOS Swap Override Jumper (BIOS_SWAP_OVERRIDE1)

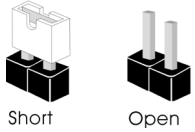


BIOS_SWAP_OVERRIDE1	Setting	
Open	Disable Override	Default
Short	Enable Override	

The illustration shows how jumpers are setup. When the jumper cap is placed on the pins, the jumper is “Short”. If no jumper cap is placed on the pins, the jumper is “Open”. The illustration shows a 3-pin jumper whose pin1 and pin2 are “Short” when a jumper cap is placed on these 2 pins.



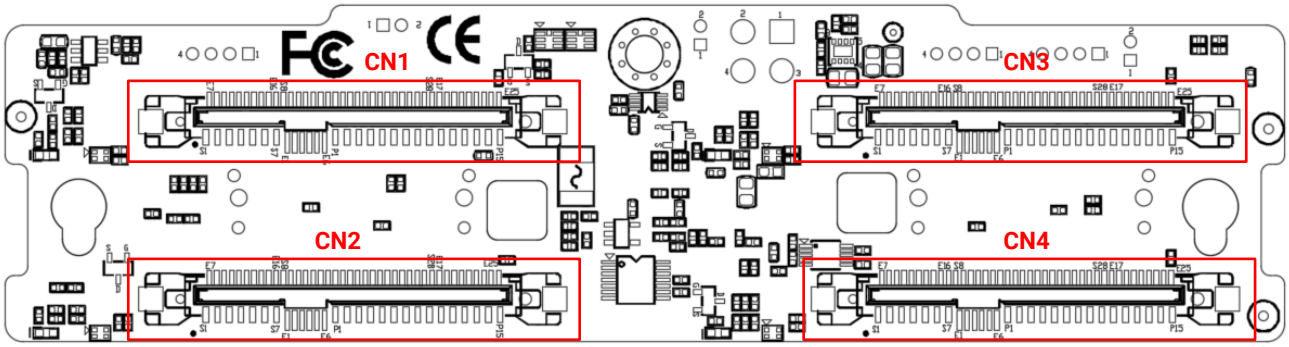
The illustration shows how jumpers are setup. When the jumper cap is placed on the pins, the jumper is “Short”. If no jumper cap is placed on the pins, the jumper is “Open”.



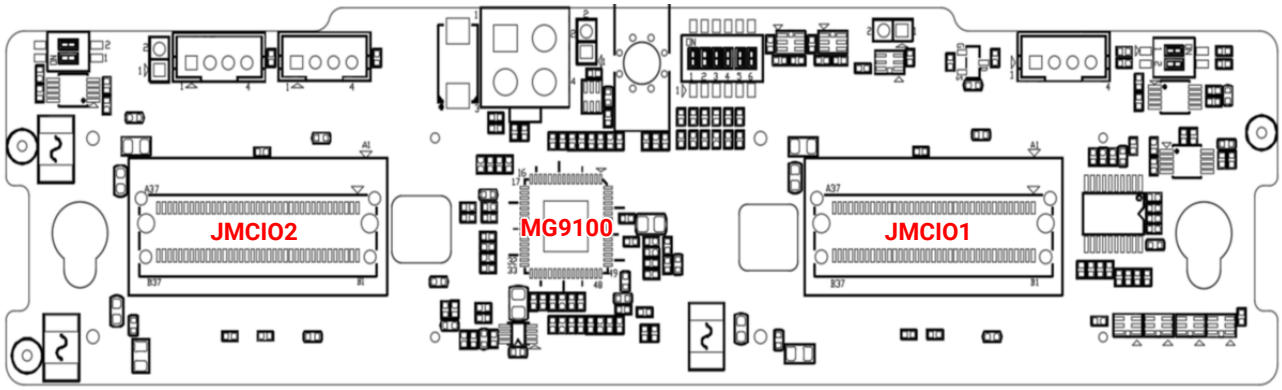
3.8 Drive Backplane: 4 Bay

3.8.1 Placement

Top view

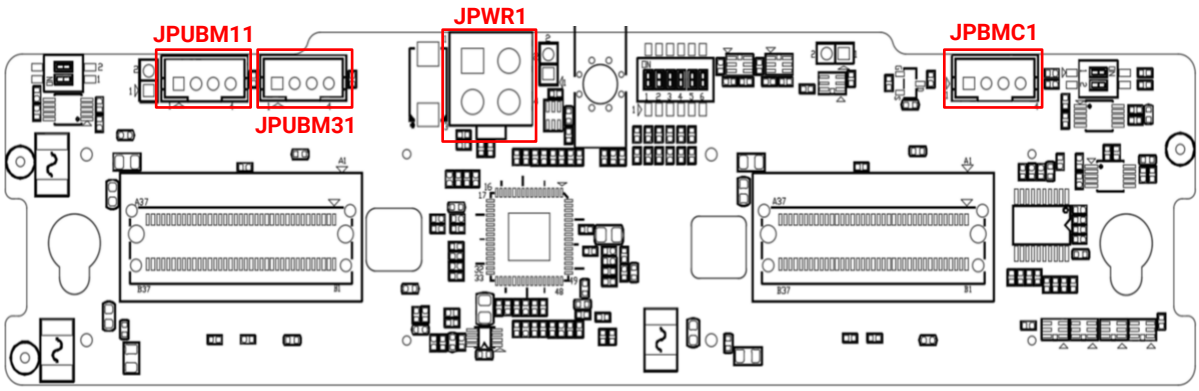


Bottom view



3.8.2 Connector

Bottom view



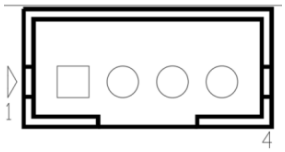
External Connectors

Connector	Description	Comments
NVMe Connection (CN1,2,3,4)	SFF-8639 SAS/PCIE Receptacle	PCIe Gen5 speed
MB PCIe Connection (JMCIO1,2)	MCIO 8i	From Host PCIe

Internal Connectors

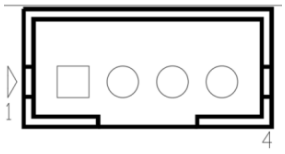
Connector	Description	Comments
Power Input (JPWR1)	2x4 pin Box Header	12V & GND
External I2C (JPUBM11)	1x4 pin Box Header	I2C Input to MG9100 –UBM1/ VPP0 I2C
External I2C (JPUBM31)	1x4 pin Box Header	I2C Input to MG9100 –UBM3/ VPP1 I2C
External I2C (JPBMC1)	1x4 pin Box Header	I2C Input to MG9100 –BMC I2C

External I2C (JPUBM11)



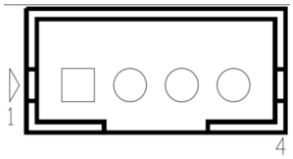
1	SHP0_SCL
2	SHP0_SDA
3	GND
4	SHPINT_OUT_N0

External I2C (JBMC1)



1	SHP1_SCL
2	SHP1_SDA
3	GND
4	SHPINT_OUT_N1

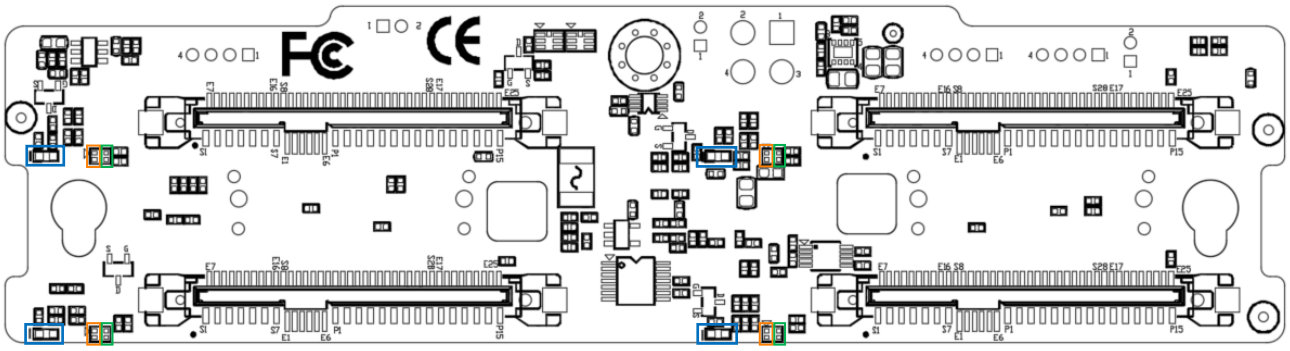
External I2C (JPUBM1)



1	BMC_SCL
2	BMC_SDA
3	GND
4	BMC_ALERT_N

3.8.3 LED Indicator

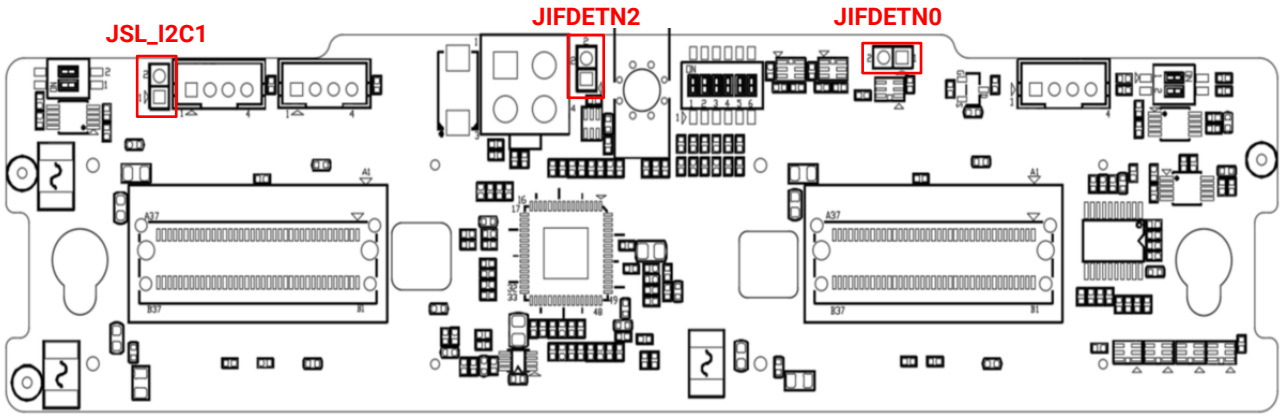
Top view



Indicator	Color	Behavior
HDD Activity LEDs	Blue (On)	HDD present
	Blue (Blinking)	HDD activity is detected.
	Off	HDD is not connected or power off status.
HDD Fail LEDs (Bi Color LED)	Green (On)	HDD Locate
	Off	NA
HDD Locate LEDs (Bi Color LED)	Yellow (On)	HDD Fault
	Yellow (Blinking)	HDD Rebuild
	Off	Normal

3.8.4 Jumper Setting

Bottom view



I2C Source Application Type Select

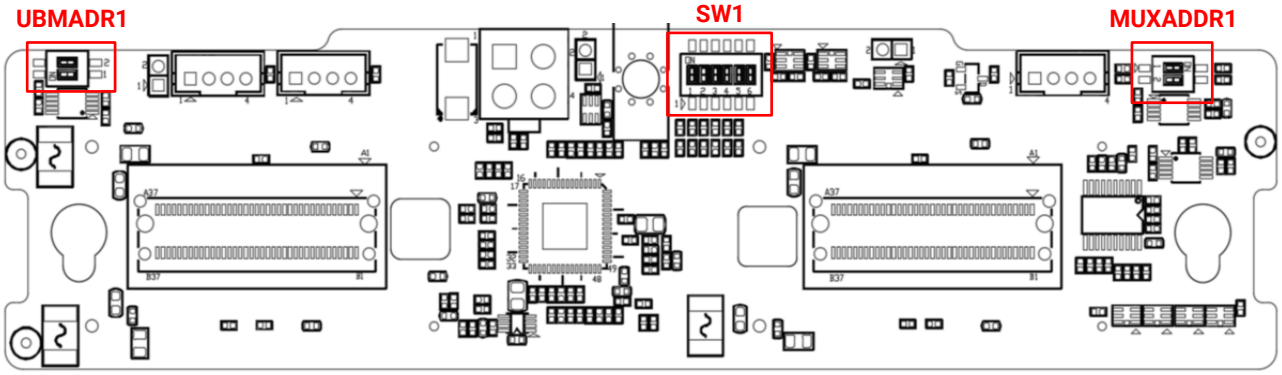
I2C MODE	JIFDET N0	JIFDET N2
UBM Application	Close	
VPP Application	Open	

MCIO I2C Mode Select

MCIO Co nnector Input MODE	JSL_I2C1
UBM/VPP/SHP to MG9100	Close
BMC I2C to HDD	Open

3.8.5 Switch Setting

Bottom view



SW1			
	LD0	LD1	LD2
VPP SMBus Address	**Pin1**	**Pin2**	**Pin3**
0x40 / 0x42 (default)	ON	ON	ON
SHP SMBus Address	**Pin1**	**Pin2**	**Pin3**
0x50 / 0x52 (default)	ON	ON	ON
VPP Table Select	**Pin4**		
Standard*(default)	OFF		
Alternative	ON		
Vendor ID	**Pin5**	**Pin6**	
UBM/INTEL*(default)	OFF	OFF	
Avago	OFF	ON	
AMD/Microsemi	ON	OFF	
UBM Only	ON	ON	

SW (ON=0/OFF=1)

Alternate VPP Strap PIN 38	VPP0_ID2/LD2 PIN 25	VPP0_ID1/LD1 PIN 24	VPP0_ID0/LD0 PIN 23	VPP0 SMB Address Drive [0-3]	VPP1 SMB Address
1	0	0	0	0x40h-0x42h	Disabled
1	0	1	0	0x44h-0x46h	Disabled
1	0	0	1	0x48h-0x4Ah	Disabled
1	0	1	1	0x4Ch-0x4Eh	Disabled

SHP0 ID	VPP#	Drives	MG9100 BMC SMBus Addr: 0xC0/0xC2/0xC4/0xC6			
			SLOT0	SLOT1	SLOT2	SLOT3
0	VPP0	4	0x40	0x40	0x42	0x42
	VPP1	0	-	-	-	-
2	VPP0	4	0x44	0x44	0x46	0x46
	VPP1	0	-	-	-	-
1	VPP0	4	0x48	0x48	0x4A	0x4A
	VPP1	0	-	-	-	-
3	VPP0	4	0x4C	0x4C	0x4E	0x4E
	VPP1	0	-	-	-	-

UBMADR1				
Device Address	**0xC0**	**0xC2**	**0xC4**	**0xC6**
Pin1	ON	OFF	ON	OFF*
Pin2	ON	ON	OFF	OFF*

MUXADDR1				
Device Address	**0xE0**	**0xE2**	**0xE4**	**0xE6**
Pin1	ON	OFF	ON	OFF*
Pin2	ON	ON	OFF	OFF*

3.8.6 Application Setting

3.8.6.1 HOST Select

Broadcom – UBM Mode

SW1						JIFDETN0	JIFDETN2
1	2	3	4	5	6	Close	
ON	ON	ON	ON	OFF	OFF		

Intel – VPP Mode

SW1						JIFDETN0	JIFDETN2
1	2	3	4	5	6	Open	
ON	ON	ON	OFF	OFF	OFF		

AMD – SHP Mode

SW1						JIFDETN0	JIFDETN2
1	2	3	4	5	6	Open	
ON	ON	ON	ON	ON	OFF		

3.8.6.2 MCIO-8i I2C input Setting

I2C Select	JSL_I2C1
HP_I2C*	Close
BMC_I2C*	Open

* HD_I2C to MG9100 Controller, BMC_I2C to HDD SMBus

Chapter 4. BIOS Configuration Settings

This chapter demonstrates how to configure the UEFI BIOS settings in your system device. You can enter the BIOS screen during system startup.

To enter BIOS configuration settings,
- Press **Esc** key during the Power-On-Self-Test (POST)

To enter BIOS after POST, you have to restart the system by using one of the three methods:
- Press **Ctrl** + **Alt** + **Delete.**
- Press the reset button on the system chassis.
- Turn the system off and on.

NOTE

- The following pages provide the details of BIOS menu. Please be noted that the BIOS menu are continually changing due to the BIOS updating. The BIOS menu provided are the most updated ones when this manual is written.
- The default value for each BIOS option key may vary per system. The [default] key is for reference only.

4.1 Navigation Keys

The navigation keys are listed below.

Function Key	Description
< ↑ > < ← > < → > < ↓ >	Select item.
< Enter >	Select and enter sub-screen.
< + > < - >	Modify selected option.
< F1 >	General help.
< F2 >	Previous Value.
< F3 >	Optimized defaults.
< F4 >	Save & Exit.
< Esc >	Exit the current menu screen.

4.2 BIOS Menu

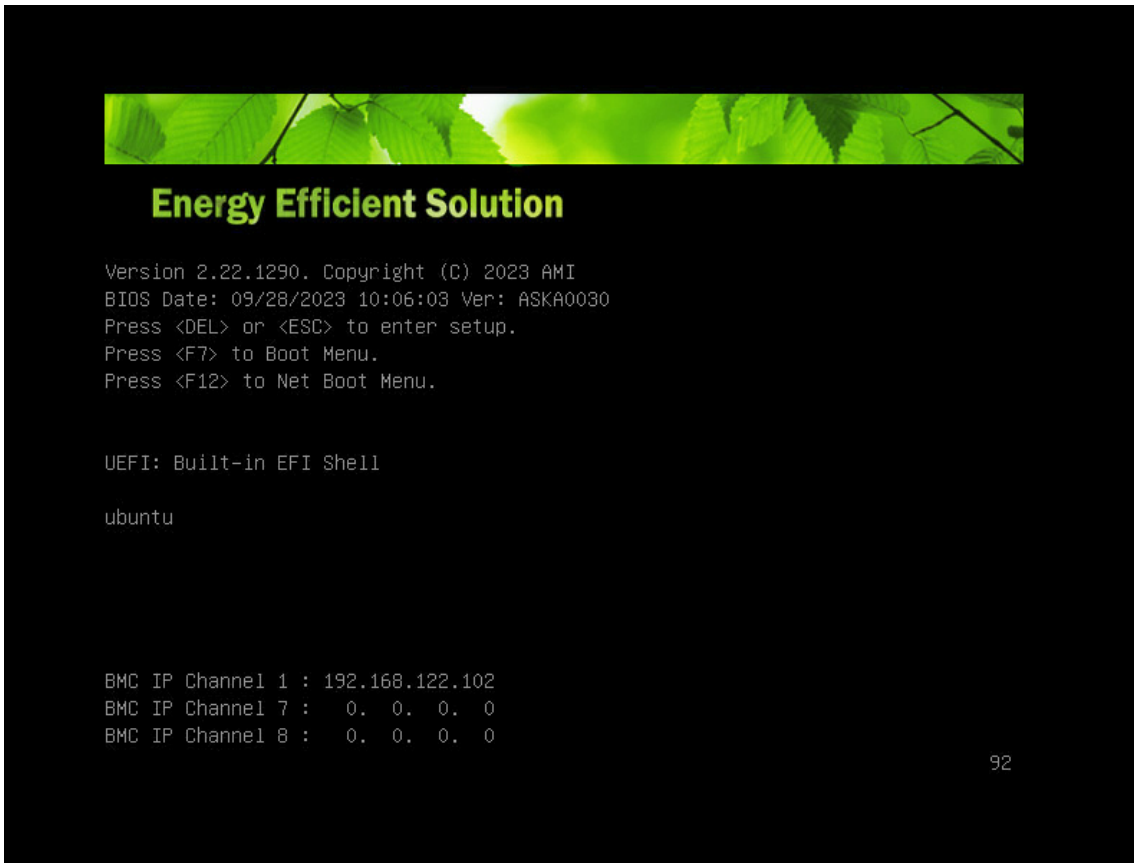
4.2.1 Menu

Press ⬅ and ➡ to select the options of the menu bar.
Press **Enter** to access the option screen.

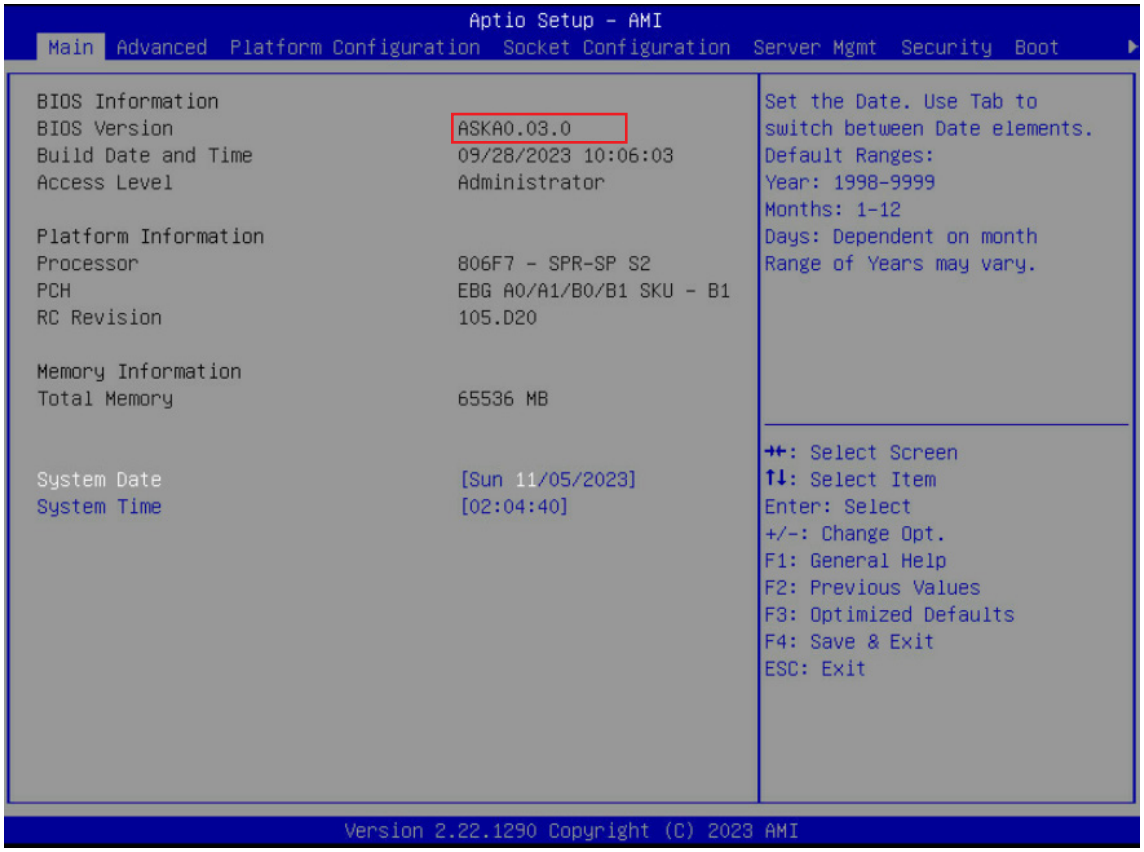
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Platform Configuration	Allows configuration of platform settings such as PCH, miscellaneous, and server ME configuration.
Socket Configuration	Allows configuration of socket settings such as processor, Common RefCode, UPI, and memory configurataion.
Server Management	Allows configuration of timer, System Event Log, and BMC network.
Security	Sets passwords and security functions.
Boot	Sets boot options such as Quick Boot or USB Boot.
Exit	Save changes and exit, discard changes and exit, discard changes, or load optimal or fail-safe defaults.

4.2.2 Startup

① Press **DEL** or **ESC** to run the BIOS setup procedure.



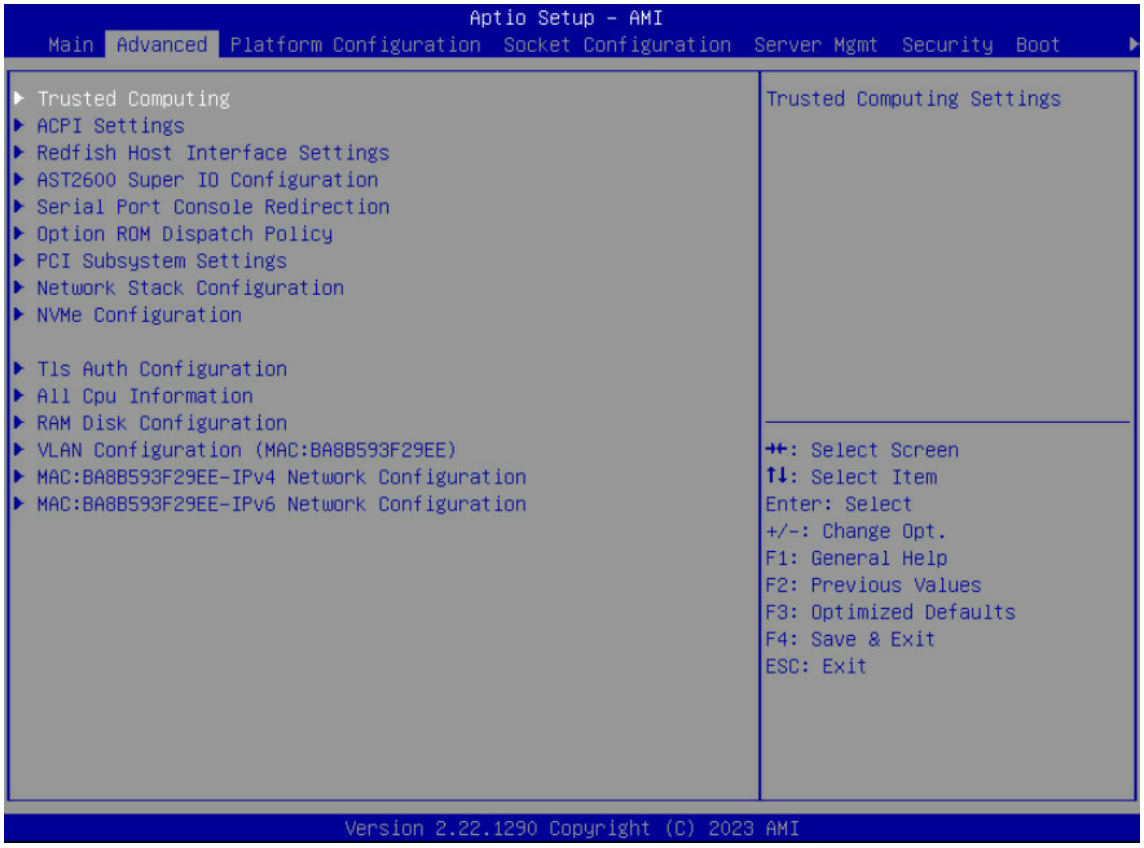
4.3 Main



4.3.1 Main

Main	
System Date	Configures the current time. Set the date. Use tab to switch between date elements.
System Time	Configures the current date. Set the time. Use tab to switch between time elements.

4.4 Advanced



4.4.1 Trusted Computing

Trusted Computing Settings.

Trusted Computing		
Security Device Support	Enables or disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.	
	▶Enable	Disable

4.4.2 ACPI Settings

System ACPI Parameters.

ACPI Settings		
Enable ACPI Auto Configuration	Enables or disables BIOS ACPI Auto Configuration.	
	Enable	▶Disable
Enable Hibernation	Enables or disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.	
	▶Enable	Disable

4.4.3 Redfish Host Interface Settings

Redfish Host Interface Parameters.

Redfish Host Interface Settings		
Redfish	Enable/Disable AMI Redfish.	
	▶Enable	Disable
Authentication mode	Select authentication mode.	
	▶Basic Authentication	Session Authentication

4.4.4 AST2600 Super IO Configuration

System Super IO Chip Parameters.

AST2600 Super IO Configuration				
Serial Port 1 Configuration	Set Parameters of Serial Port 1 (COMA)			
	Serial Port	Enables/disables Serial Port (COM)		
		▶Enable	Disable	
	Change Settings	Select an optimal settings for Super IO Device.		
		▶Auto	IO=3F8h; IRQ=4;	IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
		IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=2E8h IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
Serial Port 2 Configuration	Set Parameters of Serial Port 2 (COMB)			
	Serial Port	Enables/disables Serial Port (COM)		
		▶Enable	Disable	
	Change Settings	Select an optimal settings for Super IO Device.		
		▶Auto	IO=2F8h; IRQ=3;	IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
		IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=2E8h IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;

4.4.5 Serial Port Console Redirection

Serial Port Console Redirection.

Serial Port Console Redirection		
Console Redirection	Enables/disables console redirection.	
	Enable	▶Disable
Console Redirection EMS	Console Redirection Enable or Disable.	
	Enable	▶Disable

4.4.6 Option ROM Dispatch Policy

Option ROM Dispatch Policy.

Serial Port Console Redirection		
Restore if Failure	If system fails to boot and this option is set to 'Enabled', software will reset settings of this page as well as CSM page to its default values automatically.	
	▶Enable	Disable
Primary Video Ignore	If software will detect that due to the Policy settings, Option ROM of Primary Video Device will not dispatch, it will ignore this device policy settings, and restore it to 'Enable' automatically.	
	▶Enable	Disable

4.4.7 PCI Subsystem Settings

PCI, PCI-X and PCI Express Settings.

PCI Subsystem Settings		
Above 4G decoding	Enables/disables 64 bit capable devices to be decoded in above 4G address space (only if system supports 64 bit PCI decoding).	
	▶Enable	Disable
SR-IOV Support	If system has SR-IOV capable PCIe devices, this option enables or disables Single Root IO Virtualization Support.	
	▶Enable	Disable
BME DMA Mitigation	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked.	
	Enable	▶Disable

4.4.8 Network Stack Configuration

Network Stack Settings.

Network Stack Configuration		
Network Stack	Enables/disables UEFI Network Stack.	
	▶Enable	Disable
IPv4 PXE Support	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.	
	Enable	▶Disable
IPv4 HTTP Support	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.	
	Enable	▶Disable
IPv6 PXE Support	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.	
	Enable	▶Disable
IPv6 HTTP Support	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.	
	Enable	▶Disable
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.	
	0	
Media detect count	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.	
	1	

4.4.9 T1s Auth Configuration

Press <Enter> to select T1s Auth Configuration.

T1s Auth Configuration			
Server CA Configuration	Press <Enter> to configures server CA.		
	Enroll Cert	Press <Enter> to enroll cert.	
		Enroll Cert Using File	Enroll Cert Using File
		Cert GUID	Input digit character in 11111111-2222-3333-4444-1234567890ab format.
		Commt Changes and Exit	Commit Changes and Exit.
		Discard Changes and Extit	Discard Changes and Exit.
	Delete Cert	Press <Enter> to delete cert.	

4.4.10 RAM Disk Configuration

Press <Enter> to Adds/Removes RAM disks.

RAM Disk Configuration			
Disk Memory Type	Specifies type of memory to use from available memory pool in system to create a disk.		
	►Boot Service Data	Reserved	
Create Raw	Creates a raw RAM disk.		
	Size (Hex)	The valid RAM disk size should be multiples of RAM disk block size.	
		1	
	Create & Exit	Creates a new RAM disk with the given starting and ending address.	
	Discard & Exit	Discards and exits.	
Create from file	Creates a RAM disk from a given file.		
Remove selected RAM disk(s)	Removes selected RAM disk(s).		

4.4.11 VLAN Configuration (MAC:BA8B593F29EE)

VLAN Configuration (MAC:BA8B593F29EE)

VLAN Configuration (MAC:BA8B593F29EE)			
Enter Configuration Menu	VLAN ID	VLAN ID of new VLAN or existing VLAN, valid value is 0~4094.	
		0	
	Priority	802.1Q Priority, valid value is 0~7.	
		0	
	Add VLAN	Create a new VLAN or update existing VLAN.	
	VLAN ID: 0, Priority: 0	Select for remove	
		Enabled	►Disabled
	Remove VLAN	Remove selected VLANs.	

4.4.12 MAC:BA8B593F29EE-IPv4 Network Configuration

Configure network parameters (MAC:BA8B593F29EE)

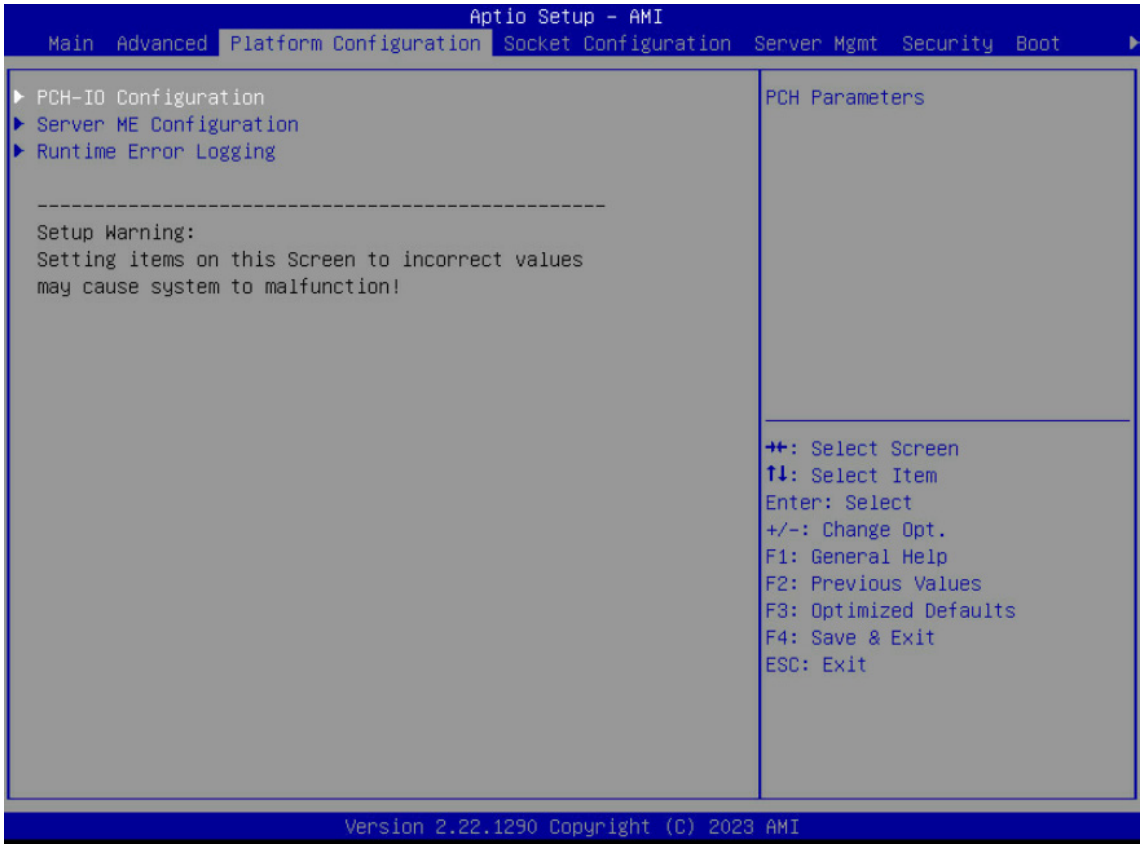
MAC:BA8B593F29EE-IPv4 Network Configuration		
Configured	Indicate whether network address configured successfully or not.	
	Enabled	►Disabled
Save Changes and Exit	Save Changes and exit.	

4.4.13 MAC:BA8B593F29EE-IPv6 Network Configuration

Configure IPv6 network parameters (MAC:BA8B593F29EE)

MAC:BA8B593F29EE-IPv6 Network Configuration			
Enter Configuration Menu	Interface ID	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3	
		B8:8B:59:FF:FE:3F:29:EE	
	DAD Transmit Count	The number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.	
		1	
	Policy	automatic or manual	
		►automatic	manual
	Save Changes and Exit	Save changes for interface ID, DAD transmit count, policy, and data in advanced configuration.	

4.5 Platform Configuration



4.5.1 PCH-IO Configuration

PCH Parameters.

PCH-IO Configuration						
SATA And RST Configuration	Device Options Settings					
	Controller 1-3 SATA and RST Configuration	SATA Controller 1 Device Options Settings.				
		SATA Configuration		SATA test settings		
				▶Enabled	Disabled	
		SATA Mode Selection		Determines how SATA controller(s) operate.		
				▶AHCI	RAID	
		SATA Test Mode		Test Mode Enable/Disable (Loop Back).		
				Enabled	▶Disabled	
		Aggressive LPM Support		Enable PCH to aggressively enter link power state.		
				▶Enabled	Disabled	
		Force SATA Gen Speed		Changes SATA Gen Speed for port.		
				Gen1	Gen2	▶Gen3
		SATA SGPIO Enable		Enable Serial GPIO for SATA controller.		
				▶Enabled	Disabled	
		SATA Port 0-7		Enable or Disable SATA Port.		
				▶Enabled	Disabled	
		SATA Port 0-7	Hot Plug	Designates this port as Hot Pluggable.		
				▶Enabled	Disabled	
			External	Marks this port as external.		
				Enabled	▶Disabled	
			Spin Up Device	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.		
				Enabled	▶Disabled	

SATA And RST Configuration	Controller 1 SATA and RST Configuration	SATA Port 0-7	Spin Up Time	Spin Up Time.			
				1 Sec	2 Sec	3 Sec	4 Sec	►5 Sec
			SATA Rx Setting	Adjust SATA DTLE DATA Values(0-15).			
				►Auto	0.0 db	0.8 db	1.6 db
				2.4 db	3.2 db	4.0 db	4.8 db
				5.6 db	6.4 db	7.2 db	8.0 db
				8.8 db	9.6 db	10.4 db	11.2 db
				12.0 db	--	--	--
			SATA Device Type	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.			
				►Hard Disk Drive		Solid State Drive	
			DITO Confiur-ation	Enable/Disable DITO Configuration.			
				Enabled		►Disabled	
	USB Configuration	USB Configuration settings					
		USB PD0 Programming		Select "Enabled" if Port Disable Override functionality is used.			
				►Enabled		Disabled	
		USB Overcurrent		Select "Enabled" for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.			
				►Enabled		Disabled	
		USB Overcurrent Lock		Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data			
				►Enabled		Disabled	
		USB Port Disable Override		Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.			
				►Disable		Select Per-Pin	
	Pch Thermal Throttling Control	Pch Thermal Throttling Control.					
		Thermal Throttling Level		Determine if use Intel suggested setting.			
				►Suggested Setting		Manual	
		DMI Thermal Setting		Determin if use Intel suggested setting.			
				►Suggested Setting		Manual	
		Sata Thermal Throttli-ng setup for Controll -er 1-3	SATA Thermal Setting	Determin if use Intel suggested setting.			
				►Suggested Setting		Manual	
	State After G3	Specify what state to go to when power is re-applied after a power failure (G3 state).					
		SO State		►S5 State		Leave power state unchanged	
	Enable/Disable ADR	Enable or disable Automatic DIMM Refresh (ADR)This is not available if eADR is enabled since eADR requires ADR to be enabled. Platform-POR: ADR disabled					
		►Platform-POR		Enabled		Disabled	
	Enable/Disable ADR Timer	Enable or disable ADR Timer. Platform-POR: ADR Timer Disabled					
		►Platform-POR		Enabled		Disabled	
	Host Partition Reset ADR Enable	Enables/Disables ADR on Host Partition Reset. Platform-POR: Disabled ADR on Host Partition Reset					
		►Platform-POR		Enabled		Disabled	
	ADR timer 1 expire time	Type desired ADR timer expire time, 0 is AUTO mode, valid values - <1, 256>. Entered time is scaled by ADR timer time unit.					
		0					

SATA And RST Configuration	ADR timer 1 time unit	Select ADR timer time unit.		
		1us	10us	100us
		1ms	10ms	100ms
		1s	10s	▶Auto
	ADR timer 2 expire time	Type desired ADR timer expire time, 0 is AUTO mode, valid values - <1, 256>. Entered time is scaled by ADR timer time unit.		
		0		
	ADR timer 2 time unit	Select ADR timer time unit.		
		1us	10us	100us
		1ms	10ms	100ms
		1s	10s	▶Auto
	Extended BIOS Range Decode	Enabling this will make memory cycles falling in a specific area to be redirected to SPI flash controller.		
		Enabled	▶Disabled	
	Thermal Trip Timer Delay	Adding delay time between CPU thermal trip propagating through PCH and PCH generating a Global Reset		
		500		
	Enable I/O Marging	Enable this option to support I/O Margin tool.		
		Enabled	▶Disabled	

4.5.2 Server ME Configuration

Configure Server ME Technology Parameters.

Server ME Configuration	
Altitude	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer.Provide the 8000h value if the altitude is unknown.
	8000
MCTP Bus Owner	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.
	0

4.5.3 Runtime Error Logging

Press <Enter> to view or change the runtime error log configuration.

Runtime Error Logging				
System Errors	System Error Enable/Disable setup options.			
	▶Enable		Disable	
RAS Log Level	RAS Log setup options.			
	None	▶MIN (BASIC_FLOW)	MID (BASIC_FLOW, FUNC_FLOW)	MID (BASIC_FLOW, FUNC_FLOW, REG)
System Memory Poison	Enable/Disable System Memory Poison.			
	▶Enable		Disable	
Viral Status	Enable/Disable Viral.			
	Enable		▶Disable	
Cloak Devhide registers from being accessible from OS	Enable/Disable OS to access Devhide registers.			
	Enable		▶Disable	
System Cloaking	When enabled, Corrected errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled.			
	Enable		▶Disable	
FatalErrDebugHalt	DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjuction with ITP as thread will halt in Fatal error flow			
	Enable		▶Disable	
Mca Bank Warm Boot Clear Errors	Enable/Disable Mca Bank Warm Boot Clear Errors.			
	▶Enable		Disable	

Shutdown Suppression	Configures Shutdown Log MCA IERR Support.			
	Disable	▶Shutdown Suppression and Log MCA IERR	Shutdown Log MCA IERR	
eMCA Settings	Press <Enter> to view or change the eMCA configuration.			
	EMCA Logging Support	Enable/Disable EMCA Logging.		
		▶Enable	Disable	
	LMCE Support	Enable/Disable Local MCE firmware support.		
		▶Enable	Disable	
	Ignore OS ELOG Opt-in	Enable/Disable Ignore OS ELOG Opt-in and log.		
		Enable	▶Disable	
	EMCA CMCI-SMI Morphing	Enable/Disable EMCA CSMI.		
		Disable	▶EMCA gen 2 CSMI	
	EMCA CMCI-SMI Threshold	Set the threshold of correctable error for signaling CMCI-CSMI		
		0		
	CSMI Dynamic Disable	[Enable] - BIOS disables CSMI when error threshold reached. [Disabled] - CSMI always on.		
		Enable	▶Disable	
	EMCA MCE-SMI Enable	Enable/Disable EMCA Uncorrected SMI for gen2.		
		Disable	▶EMCA gen 2 - MSMI	
	Corrected Error eLog	Enable/Disable Corrected Error eLog.		
		▶Enable	Disable	
	Memory Error eLog	Enable/Disable Memory Error eLog.		
		▶Enable	Disable	
	Processor Error eLog	Enable/Disable Processor Errror eLog.		
		▶Enable	Disable	
	Opportunistic Spare Core	Enable/Disable Opportunistic Spare Core support.		
		Enable	▶Disable	
	Ubox Error Mask	Mask SMI generation for Ubox Error.		
		Enable	▶Disable	
Whea Settings	Press <Enter> to view or change the WHEA configuration.			
	WHEA Support	Enable/Disable WHEA support.		
		▶Enable	Disable	
	Whea Log Memory Error	Enable/Disable Whea Log Memory Error.		
		▶Enable	Disable	
	Whea Log Processor Error	Enable/Disable Whea Log Processor Error.		
		▶Enable	Disable	
	Whea Log PCI Error	Enable/Disable Whea Log PCI Error.		
		▶Enable	Disable	
Memory Error Enabling	Press <Enter> to view or change the Memory errors enabling options.			
	Memory Corrected Error	Enable/Disable Memory Corrected Error.		
		▶Enable	Disable	
	Spare Interrupt	Spare Interrupt Selection.		
		Disable	▶SMI	Error Pin	CMCI
	Pfd	Pfd is to identify hard error out from errors. Auto indicates PFD is enabled dynamically based on system configuration.		
		Disable	▶Enable	Auto
	PMem CTLR Errors	Enable/Disable PMem CTLR Error Reporting & Logging.		
		▶Enable	Disable	
	PMem CTLR Low Priority Error Signaling	Selection of signaling for errors bucketed as Low Priority.		
		Disable	▶SMI	ERRO# Pin
	PMem CTLR High Priority Error Signaling	PMem CTLR High Priority Error Signaling.		
		Disable	▶SMI	ERRO# Pin
	Set PMem Address Range Scrub	Enable/Disable PMem DIMM Physical Address Range scrub		
		Enable	▶Disable	

Memory Error Enabling	Set PMem Host Alert Policy for Patrol Scrub	Enable/Disable signaling PMem interrupt upon receiving Uncorrectable Error for NGN Patrol Scrub.	
		▶Enable	Disable
	Enable Reporting SPA to OS	Enable Reporting SPA to OS (Only disable for MCE recovery validation).	
		▶Enable	Disable
	Set PMem Host Alert Policy for DPA Error	Configures to signal Poison or viral upon receiving DIMM Physical Address Error.	
		▶Poison	Viral

4.5.4 IIO Error Enabling

Press <Enter> to view or change the IIO errors enabling options.

IIO Error Enabling			
IIO/PCH Global Error Support	Enable/Disable IIO/PCH Error Support.		
	▶Enable	Disable	
Os Native AER Support	Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.		
	Enable	▶Disable	
IIO MCA Support	Enable/Disable IIO MCA Support.		
	▶Enable	Disable	
Clear PCC for IIO Non-Fatal Error	Enable/Disable PCC equal 0 for IIO severity 1 error.		
	Enable	▶Disable	
IIO Error Pin0 Enable	Enable/Disable IIO Error Pin0.		
	Enable	▶Disable	
IIO OOB Mode	Enable/Disable System Event Generation when Error Pin is enabled.		
	▶Enable	Disable	
IIO Error Registers Clear	Enable/Disable Clear IIO Error Registers.		
	▶Enable	Disable	
IIO eDPC Support	Enable/Disable IIO eDPC Support.		
	▶Disable	On Fatal Error	On Fatal and Non-Fatal Errors
IIO Coherent Interface Error	Enable/Disable IIO Coherent Interface Error.		
	▶Enable	Disable	
IIO IRPO protocol parity error	Enable or disable Coherent Interface protocol IIO parity error reporting.		
	▶Enable	Disable	
IIO IRPO protocol qt overflow underflow error	Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting.		
	▶Enable	Disable	
IIO IRPO protocol rcvd unexprsp	Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting.		
	▶Enable	Disable	
IIO IRPO csr acc 32b unaligned	Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting.		
	▶Enable	Disable	
IIO IRPO wrcache unceccs0 error	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting		
	▶Enable	Disable	
IIO IRPO wrcache unceccs1 error	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting		
	▶Enable	Disable	
IIO IRPO protocol rcvd poison error	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting.		
	▶Enable	Disable	
IIO IRPO wrcache correccs0 error	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.		
	▶Enable	Disable	
IIO IRPO wrcache correccs1 error	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.		
	▶Enable	Disable	

IIO Misc. Error	Enable/Disable IIO Misc. Error.	
	▶Enable	Disable
IO Vtd Error	Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.	
	▶Enable	Disable
IIO Dma Error	Enable/Disable IIO Dma Error.	
	▶Enable	Disable
PCIE Error	Enable/Disable PCIE Error.	
	▶Enable	Disable
IIO PCIE Additional Corrected Error	Enable/Disable IIO PCIE Additional Corrected Error.	
	▶Enable	Disable
IIO PCIE Additional Uncorrected Error	Enable/Disable IIO PCIE Additional Uncorrected Error.	
	▶Enable	Disable
IIO PCIE Additional Received Completion with UR	Enable/Disable Clear IIO Error Registers.	
	Enable	▶Disable
ITC/OTC CA/MA Errors	Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.	
	Enable	▶Disable
PSF UR Error	Enable/Disable Unsupported Request Error on PSF.	
	▶Enable	Disable
PMSB Router Parity Error	Enable/Disable PMSB Router Parity Error.	
	▶Enable	Disable

4.5.5 PCIe Error Enabling

Press <Enter> to view or change the PCIe errors enabling options.

PCIe Error Enabling		
Corrected Error	Enable & escalate Correctable Errors to error pins.	
	▶Enable	Disable
Uncorrected Error	Enable & escalate Uncorrectable/Recoverable to error pins.	
	▶Enable	Disable
Fatal Error Enable	Enable & escalate fatal errors to error pins.	
	▶Enable	Disable
PCIE Corrected Error Threshold Counter	Enable/Disable PCIE Corrected Error Counter.	
	Enable	▶Disable
PCIE Corrected Error Threshold	0x001 - 0x7fff	
	1	
PCIE Corrected Error Limit Check	Enable/Disable the feature to disable reporting PCIe corrected errors for a device if they exceed a given limit.	
	Enable	▶Disable
PCIE AER Corrected Errors	Enable/Disable PCIE AER Corrected Errors.	
	▶Enable	Disable
PCIE AER NonFatal Error	Enable/Disable PCIE AER NonFatal Error.	
	▶Enable	Disable
PCIE AER Fatal Error	Enable/Disable PCIE AER Fatal Error.	
	▶Enable	Disable
PCIE AER Advisory Nonfatal Error	Enable/Disable PCIE AER Advisory Nonfatal Error.	
	▶Enable	Disable
PCIE ECRC Error	Enable/Disable PCIE ECRC Error.	
	Enable	▶Disable
PCIE Surprise Link Down Error	Enable/Disable PCIE Surprise Link Down Error.	
	Enable	▶Disable
PCIE Unsupported Request Error	Enable/Disable PCIE Unsupported Request Error.	
	Enable	▶Disable

Assert NMI on SERR	On SERR, generate an NMI and log an error. **NOTE** [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.	
	▶Enable	Disable
Assert NMI on PERR	On PERR, generate an NMI and log an error. **NOTE** This option is only active if the Assert NMI on SERR option has [Enabled] selected.	
	▶Enable	Disable
Expected BER	Set the expected Bit Error Rate for all speeds.	
	34359738367	
Time Window (Gen1/2)	Set the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.	
	65535	
Time Window (Gen3/4/5)	Set the error burst protection time window for Gen3, Gen4 and Gen5 speeds. A burst of errors within the window is counted as one.	
	2	
Error Threshold (Gen1/2)	Set the error threshold for Gen1, Gen2 speeds. An event is triggered when the error count exceeds the threshold.	
	0	
Error Threshold (Gen3/4/5)	Set the error threshold for Gen3, Gen4 and Gen5 speeds. An event is triggered when the error count exceeds the threshold.	
	16	
Gen3/4/5 Re-Equalization	Enable or disable Gen3, Gen4 and Gen5 re-equalization. Applies only when operating at Gen3, Gen4 or Gen5 speeds. When an event is triggered, equalization is re-run.	
	▶Enable	Disable
Gen2 Link Degradation	Enable or disable Gen2 link degradation. Applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.	
	▶Enable	Disable
Gen3 Link Degradation	Enable or disable Gen3 link degradation. Applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.	
	▶Enable	Disable
Gen4 Link Degradation	Enable or disable Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.	
	▶Enable	Disable
Gen5 Link Degradation	Enable or disable Gen5 link degradation. Applies only when operating at Gen5 speeds. When an event is triggered, 32GT/s and higher modes are disabled.	
	▶Enable	Disable

4.5.6 Error Control Setting

Press <Enter> to view or change the Error Control Setting options.

Error Control Setting		
2LM Correctable Error Logging in m2mem	Enable or disable 2LM correctable error logging in m2mem.	
	▶Enable	Disable
Latch First Corrected Error in KTI	Enable or disable latch first corrected error in KTI.	
	Enable	▶Disable
Patrol Scrub Error Reporting	Patrol Scrub Error type selection.	
	UCNA	
LLC EWB Error Control	Control the signaling of EWB errors as UCNA or SRA0.	
	▶UCNA	SRA0

4.5.7 Crash Log Enabling

Press <Enter> to view or change the Crash Log enabling options.

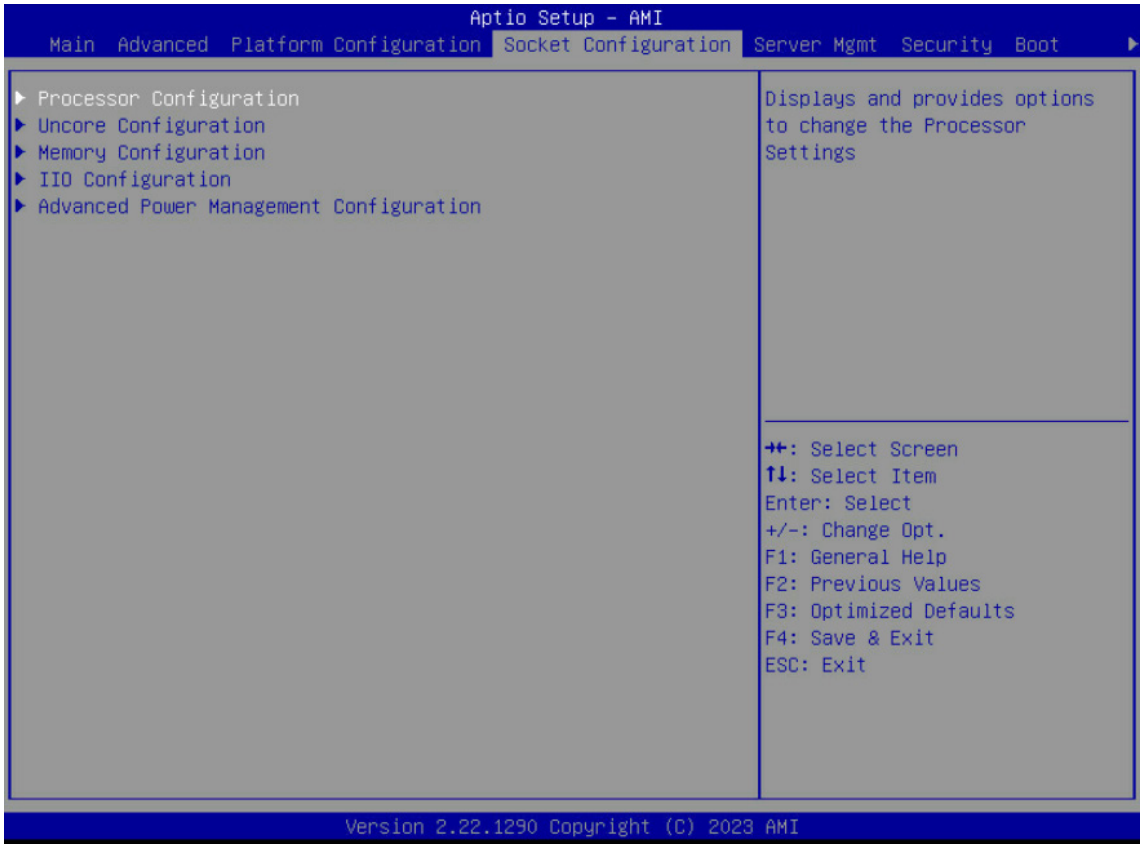
Error Control Setting			
CPU CrashLog Feature	The feature helps collecting crash data from OOBMSM SSRAM.		
	▶Auto	Enable	Disable
Core CrashLog Disable	The feature helps to disable CPU Core crash log.		
	▶no	yes	
TOR CrashLog Disable	The feature helps to disable CPU TOR crash log.		
	▶no	yes	
Uncore CrashLog Disable	The feature helps to disable CPU Uncore crash log.		
	▶no	yes	
MCERR Trigger CrashLog Disable	The feature helps to disable MCERR to trigger crash log.		
	▶no	yes	
CPU Clear CrashLog	Option to clear CPU CrashLog after collection.		
	▶Enable	Disable	
CPU Crashlog ReArm	Option to ReArm CPU CrashLog after collection.		
	▶Enable	Disable	
PCH CrashLog Feature	The feature helps collecting crash data from PMC SSRAM.		
	▶Enable	Disable	
PCH CrashLog Collect On All Reset	Option to invoke PCH CrashLog collection on all reset.		
	Enable	▶Disable	
PCH Clear CrashLog	Option to clear PCH CrashLog after collection.		
	Enable	▶Disable	
PCH ReArm CrashLog	Option to ReArm PCH CrashLog after collection.		
	▶Enable	Disable	

4.5.8 DWR Configuration

Dirty Warm Reset Configuration.

DWR Configuration		
Dirty Warm Reset	Enables/disables Dirty Warm Reset. It promotes regular reset to DWR under internal error conditions.	
	▶Enable	Disable
Ierr Global Reset	When Ierr is present in last boot, enable this knob will make BIOS do a global reset, disabled option is used in test mode only.	
	▶Enable	Disable
DWR/ IERR Error harvesting stall	When enabled, system will enter spin loop during dirty warm reset allowing manual error collection.	
	Enable	▶Disable
BMC RootPort	RootPort that BMC is connected to.	
	▶6	12

4.6 Socket Configuration



4.6.1 Processor Configuration

Displays and provides option to change the Processor Settings.

Processor Configuration			
Per-Socket Configuration	Change Per-Socket Settings.		
	CPU Socket 0/1 Configuration	0: Enable all cores. FFFFFFFFFFFFFFFF: Disable all cores.	
		NOTE At least one core per CPU must be enabled. Disabling all cores is an invalid configuration.	
		Disable Bitmap: 0	
Hardware Prefetcher	MLC Streamer Prefetcher (MSR 1A4h Bit[0]).		
	▶Enable	Disable	
Adjacent Cache Prefetch	MLC Spatial Prefetcher (MSR 1A4h Bit[1]).		
	▶Enable	Disable	
DCU Streamer Prefetcher	DCU Streamer Prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[2]).		
	▶Enable	Disable	
DCU IP Prefetcher	DCU IP Prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[3]).		
	▶Enable	Disable	
LLC Prefetcher	Enable/Disable LLC Prefetch on all threads.		
	Enable	▶Disable	
Homeless Prefetcher	Enables/Disable Homeless Prefetch on all threads, the setting Auto maps is program specific.		
	▶Auto	Enable	Disable
Extended APIC	Enables/Disable extended APIC support.		
	NOTE When enabled, VT-d & Interrupt Remapping will be automatically enabled.		
	▶Enable	Disable	

Enable Intel(R) TXT	Enable Intel(R) TXT.	
	Enable	▶Disable
VMX	Enables the Vanderpool Technology, takes effect after reboot.	
	▶Enable	Disable
Enable SMX	Enables Safer Mode Extensions.	
	Enable	▶Disable
Lock Chipset	Lock or Unlock chipset.	
	▶Enable	Disable
PPIN Control	Unlock and Enable/Disable PPIN Control.	
	Lock/Disable	▶Unlock/Enable
AES-NI	Enable/Disable AES-NI support.	
	▶Enable	Disable
Memory Encryption (TME)	Enables/Disable Memory Encryption(TME)	
	Enable	▶Disable
In Field Scan(IFS)	In Field Scan(IFS)	

4.6.2 Uncore Configuration

Displays and provides option to change the Uncore Settings.

Uncore Configuration							
Uncore General Configuration	Display and provides option to change the Uncore General Settings.						
	Uncore Status	Uncore Status Help					
	Degrade Precedence	Choose Topology Precedence to degrade features if system options are in conflict or choose Feature Precedence to degrade topology if system options are in conflict.					
		▶Topology Precedence	Feature Precedence				
	Link L0p Enable	Enable - Enables UPI L0p only when system is power limited, Disable - Reset it, Auto - Auto decides based on Si Compatibility, Full L0p enable - Always enables UPI L0p for all EPB levels.					
		▶Auto	Enable	Disable			
	Link L1 Enable	Enable - Set the c_l1_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.					
		▶Auto	Enable	Disable			
	KTI Prefetch	KTI Prefetch, Auto - Auto decides based on Si Compatibility.					
		▶Auto	Enable	Disable			
	IO Directory Cache (IODC)	IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores), Auto - Auto sets to WCiLF					
		Disable	▶Auto	Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow	Enable for Remote InvItoM Hybrid AllocNon-Alloc	Enable for Remote InvItoM and Remote WViLF
	SNC	Disable supports 1-cluster and 4-IMC way interleave. Enable SNC2 supports 2-clusters SNC and 2-way IMC interleave. Enable SNC4 supports 4-cluster and 1-IMC way interleave, Auto - Auto decides based on Si Compatibility.					
		▶AUTO	Disable	Enable SNC2 (2-clusters)			
	Stale AtoS	Stale A to S Dir optimization, Auto - Auto decides based on Si Compatibility.					
		▶Auto	Enable	Disable			
	LLC dead line alloc	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC, Auto - Auto decides based on Si Compatibility.					
		Auto	▶Enable	Disable			
	MMCFG Base	Select MMCFG Base, Auto - Auto decides based on Si Compatibility.					
		▶Auto	1G	1.5G	1.75G	2G	2.25G	3G

Uncore General Configuration	MMCFG Size	Select MMCFG Size, Auto - Auto decides based on Si Compatibility.					
		128M	256M	512M	1G	2G	►Auto
	MMIO High Base	Select MMIO High Base.					
		56T	40T	►32T	24T	16T	
		4T	2T	1T	512G	3584T	
	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.					
		1G	4G	16G	►64G	256G	1024G
Uncore Per Socket Configuration	CPU0	CPU 0 Configuration Silk Screen Equivalent -> CPU1					
		CPU 0 UPI Port 0-2	CPU 0 UPI Port 0-3 Configuration.				
			Link Diable	Disable a single UPI port. No: Not disable; Yes: Disable			
				►No	Yes		
			Current UPI Link Speed	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility			
				12.8GT/s	14.4GT/s	16.0GT/s	►Auto
		CPU 0 UPI Port 3	Link Diable	Disable a single UPI port. No: Not disable; Yes: Disable			
				No	►Yes		
			Current UPI Link Speed	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility			
				12.8GT/s	14.4GT/s	16.0GT/s	►Auto
		Bus Resources Allocation Ratio	Bus resources allocation ratio, range 0 to 8.				
			1				
		HIOP STACK DISABLE	Enables/Disables given HIOP STACK. Default is AUTO no stack is disabled. 1 - The stacks indicated by the bit locations are disabled. 0 - The stacks indicated by the bit locations are not modified. The stack order is abstracted so each bit 0 = stack 0 ... bit n = stack n. For PE numbering convention bits are incrementaly mapped from bit0 to instances PE(0->n) then PE(a->x) and HC(a->x). The bit setting for each stack can be overriden by BIOS based on CPU-knob compatibility.				
			0				
	CPU1	CPU 1 Configuration Silk Screen Equivalent -> CPU2					
		CPU 0 UPI Port 0-3	CPU 1 UPI Port 0-3 Configuration.				
			Link Diable	Disable a single UPI port. No: Not disable; Yes: Disable			
				►No	Yes		
			Current UPI Link Speed	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility			
				12.8GT/s	14.4GT/s	16.0GT/s	►Auto
		Bus Resources Allocation Ratio	Bus resources allocation ratio, range 0 to 8.				
			1				
		HIOP STACK DISABLE	Enables/Disables given HIOP STACK. Default is AUTO no stack is disabled. 1 - The stacks indicated by the bit locations are disabled. 0 - The stacks indicated by the bit locations are not modified. The stack order is abstracted so each bit 0 = stack 0 ... bit n = stack n. For PE numbering convention bits are incrementaly mapped from bit0 to instances PE(0->n) then PE(a->x) and HC(a->x). The bit setting for each stack can be overriden by BIOS based on CPU-knob compatibility.				
			0				

4.6.3 Memory Configuration

Displays and provides option to change Memory Settings.

Memory Configuration								
Enforce DDR Memory Frequency POR	Enforces Plan Of Record restriction for DDR frequency programming.							
	▶POR				Disable			
DDR PPR Type	Selects DDR Post Package Repair Type- Hard/ Soft/ Disabled. Current default is Soft PPR.							
	PPR Disabled		Hard PPR		▶Soft PPR			
Memory Frequency	Maximum Memory Frequency Selections in MT/s. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved							
	▶Auto	3200	3600	4000	4400	4800	5200	5600
Data Scrambling for DDR4/5	Enable - Enables data scrambling for DDR4 and DDR5. Disable - Disables this feature; current default is Enable.							
	▶Enable				Disable			
Allow Memory Test Correctable Error	Enable - Logs error and allows correctable errors during memory test(DIMM Rank not removed). Disable - Logs error and removes DIMM Rank.							
	▶Enable				Disable			
Scrambling Seed Low	Low 32 bits of the scrambling seed.							
	41003							
Scrambling Seed High	High 32 bits of the scrambling seed.							
	54165							
Enable FADR	Enable/Disable FADR capability in the platform.							
	Enable				▶Disable			
Enable ADR	Enables the detecting and enabling of ADR. This is not available if FADR is enabled since FADR requires ADR to be enabled.							
	▶Enable				Disable			
Legacy ADR Mode	Enable/Disable/Auto Legacy ADR mode. This is not available if eADR is enabled since eADR requires this mode to be enabled.							
	▶Auto		Enable			Disable		
NVDIMM Energy Policy	Set the energy policy for NVDIMMs.							
	▶Device-Managed				Host-Managed			
ADR Data Save Mode	Data Save Mode for ADR.							
	Disable		Batterybacked DIMMs		▶NVDIMMs		Copy to Flash	
Custom Refresh Enable	Enable/disable a custom memory refresh rate.							
	Enable				▶Disable			
DDR 2x Refresh Enable	Enable/Disable 2x Refresh. Auto= dynamically selected.							
	▶Auto		Enable			Disable		
Memory Topology	Displays memory topology with Dimm population information.							
Memory RAS Configuration	Displays and provides option to change the Memory RAS Settings.							
	Mirror Mode	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. Enabling any type of Mirror Mode will disable XPT Prefetch.							
		▶Disabled		Full Mirror Mode		Partial Mirror Mode		
	Mirror TADO	Enable Mirror on entire memory for TADO.						
		Enable			▶Disabled			
	UEFI ARM Mirror	Imitate behavior of UEFI based Address Range Mirror with setup option.						
		Enable			▶Disabled			
	Memory Correctable Error Flood Policy	[Disabled] - Don't deal with Memory CE flood.[Once] - Only First Memory CE will trigger SMI, and BIOS will disable this rank silicon side to trigger SMI.[Frequency] Disable SMI when Memory CE reaches threshold within time limits.						
		Disable		Once		▶Frequency		

Memory RAS Configuration	Correctable Error Threshold	Correctable Error Threshold (0x01 - 0x7fff) used for DDR sparing and DDR leaky bucket		
		7FFF		
	ADDDC Sparing	Enable/Disable ADDDC Sparing.		
		Enable	▶Disabled	
	Patrol Scrub	Enable/Disable Patrol Scrub.		
		▶Enable at End of POST	Disabled	
	Patrol Scrub Interval	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto!		
		24		
	DDR5 ECS	Disable: Disable ECS/Result collection. Enable: Enable ECS without Result Collection. Enable ECS with Result Collection: Enable ECS/Result Collection.		
		Disabled	▶Enabled	Enable ECS with Result Collection

4.6.4 IIO Configuration

Displays and provides option to change IIO Settings.

IIO Configuration				
Socket0 Configuration	IOU0/1/2/3/4 (IIO PCIe Port 1/2/3/4/5)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
		x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2
	DmiAsPcie (IIO PCIe Port 0)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
		x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2
	IOU6 (IIO PCIe Port 7)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
	Port 1/2/4/5 Subsystem Mode	Selects PCIe Subsystem Mode for selected slot(s)Gen4: Gen4 controller onlyGen5: Gen5 with or without mix modeAuto: Auto selectForce CXL: There is no training discovery, the attached device must also supports this mode.		
		►Gen5	Protocol Auto Negotiation	
	Port 3/0/7 Subsystem Mode	Selects PCIe Subsystem Mode for selected slot(s)Gen4: Gen4 controller onlyGen5: Gen5 with or without mix modeAuto: Auto selectForce CXL: There is no training discovery, the attached device must also supports this mode.		
		Gen5	►Protocol Auto Negotiation	
	PE0-6 Restore RO Write Perf	Restores BW in the presence of mixed RO and non-RO PCIe Writes to memory at the cost of limiting P2P BW.		
		►Auto	Enable	Disable
	DMI Restore RO Write Perf	Restores BW in the presence of mixed RO and non-RO PCIe Writes to memory at the cost of limiting P2P BW.		
		►Auto	Enable	Disable
	IIO PCIe VC1 Port Bitmap	Enable/Disable PCIe Port VC1 support.Port 0 is allocated to DMI or DMI as PCIe.Port 0 bit will have no effect in DMI mode.0 - VC1 support disabled.1 - VC1 support enabled.Example: bit 0 = IIO PCIe Port 0 ... bit n = IIO PCIe Port n.		
		0		

Socket0 Configuration	Sck0 RP Correctable Err	Applies to root ports only. Enable interrupt on correctable errors.					
		►No	Yes				
	Sck0 RP NonFatal Uncorrectalbe Err	Applies to root ports only. Enable interrupt on a non-fatal error.					
		►No	Yes				
	Sck0 RP Fatal Uncorrectable Err	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.					
		►No	Yes				
	TraceHub Configuration Menu	TraceHub Configuration Settings.					
		North Trace Hub 1-4 Enable Mode	Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software.				
			►Disabled	Target Debugger	Host Debugger		
	Port DMI	Link Speed	Choose Link Speed for this PCIe port.				
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	Gen 2 (8 GT/s)	Gen 4 (16 GT/s)
		PCI-E Port DeEmphasis	De-Emphasis control (LNKCON2[6]) for this PCIe port.				
			►-6.0 dB	-3.5 dB			
		PCI-e Port Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component.				
			Distinct	►Common			
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.				
			►Enable	Disable			
		DMI Port MPSS	Configure Max Payload Size Supported in DMI Device Capabilities register. 'Auto' keeps hardware default. If 'Auto' is not used make sure MPSS in PCH root ports is updated to the same or smaller value.				
			►Auto	128B	256B		
		PCI-E Port D-state	Set to D0 for normal operation, D3Hot to be in low-power state.				
			►D0	D3Hot			
		PCI-E Completion Timeout	Configure PCIe Completion Timeout in Device Control2 register.				
			50us to 50ms	16ms to 55ms	65ms to 210ms		
			►260ms to 900ms	1s to 3.5s	Disable		
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.				
			►Auto	Disable			
		PCI-E Port L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.				
			<1uS	1uS - 2uS	2uS - 4uS	4uS - 8uS	
			►8uS - 16uS	16uS - 32uS	32uS - 64uS	>64uS	
		MSI	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3.				
			Enable	►Disable			
		PCI-E Extended Sync	Enable / disable the Extended the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.				
			►No	Yes			
		Compliance Mode	Enable/Disable Compliance Mode for this P				
			►No	Yes			
		Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.				
			Enable	►Disable			

Socket0 Configuration	Port DMI	SRIS	Enable or Disable SRIS.			
			►No	Yes		
		ECRC Generation	Enable or Disable ECRC Generation (Error Capabilities and Control Register).			
			Enable	►Disable		
		ECRC Check	Enable or Disable ECRC Check (Error Capabilities and Control Register).			
			Enable	►Disable		
		IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
			►KTI Option	Auto	Enable for Remote InvItoM Hybrid Push	
			InvItoM AllocFlow	Enable for Remote InvItoM Hybrid AllocNonAlloc	Enable for Remote InvItoM and Remote WViLF	
		MCTP	Enable/Disable MCTP.			
			No	►Yes		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
	Port 1A	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable.			
			Auto	►Disable	Enable	
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable.			
			Enable	►Disable		
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.			
			Yes	►No		
		Link Speed	Choose link speed for this PCIe port.			
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	
			Gen 3 (8 GT/s)	Gen 4 (16 GT/s)	Gen 5 (32 GT/s)	
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.			
			►Enable	Disable		
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
			►Auto	128B	256B	512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.			
			Auto	►Disable		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge.			
			0			
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge.			
			0			
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits).			
			1			

Socket0 Configuration	Port 1A	(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge. 0
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge. 0
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 0

Socket0 Configuration	Port 2A	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable.			
			Auto	Disable	►Enable	
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable.			
			►Enable	Disable		
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.			
			Yes	►No		
		Link Speed	Choose link speed for this PCIe port.			
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	
			Gen 3 (8 GT/s)	Gen 4 (16 GT/s)	Gen 5 (32 GT/s)	
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.			
			►Enable	Disable		
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
			►Auto	128B	256B	512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.			
			Auto	►Disable		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge. 2			
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge. 8			
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits). 1			

Socket0 Configuration	Port 2A	(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge. 1
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge. 0
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 4

Socket0 Configuration	Port 3A/3C/3E/3G/4A/4C/4E/4G/5A/5C/5E/5G	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable.			
			Auto	Disable	►Enable	
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable.			
			►Enable	Disable		
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.			
			Yes	►No		
		Link Speed	Choose link speed for this PCIe port.			
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	
			Gen 3 (8 GT/s)	Gen 4 (16 GT/s)	Gen 5 (32 GT/s)	
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.			
			►Enable	Disable		
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
			►Auto	128B	256B	512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.			
			Auto	►Disable		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge. 2			
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge. 1			
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits). 1			

Socket0 Configuration	Port 3A/3C/3E/3G/4A/4C/4E/4G/5A/5C/5E/5G	(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge. 1
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge. 0
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 0

Socket1 Configuration	IOU0 (IIO PCIe Port 1)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
		x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2
	DmiAsPcie (IIO PCIe Port 0)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
		x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2
	IOU1/2/3/4/6 (IIO PCIe Port 2/3/4/5/7)	Select PCIe port Bifurcation for selected slot (s). Port Format: xDxCxBxA The port can further be x2x2		
		►Auto	x4x4x4x4	x4x4_x8
		x_x8x4x4	x_x8x_x8	x_x_x_x16
		x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4
		x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4
		x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4
		x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2
		x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2
		x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2
	Port 1/2/3/0/7 Subsystem Mode	Selects PCIe Subsystem Mode for selected slot(s)Gen4: Gen4 controller onlyGen5: Gen5 with or without mix modeAuto: Auto selectForce CXL: There is no training discovery, the attached device must also supports this mode.		
		Gen5	►Protocol Auto Negotiation	
	Port 4/5 Subsystem Mode	Selects PCIe Subsystem Mode for selected slot(s)Gen4: Gen4 controller onlyGen5: Gen5 with or without mix modeAuto: Auto selectForce CXL: There is no training discovery, the attached device must also supports this mode.		
		►Gen5	Protocol Auto Negotiation	
	PE0-6 Restore RO Write Perf	Restores BW in the presence of mixed RO and non-RO PCIe Writes to memory at the cost of limiting P2P BW.		
		►Auto	Enable	Disable
	DMI Restore RO Write Perf	Restores BW in the presence of mixed RO and non-RO PCIe Writes to memory at the cost of limiting P2P BW.		
		►Auto	Enable	Disable
	IIO PCIe VC1 Port Bitmap	Enable/Disable PCIe Port VC1 support.Port 0 is allocated to DMI or DMI as PCIe.Port 0 bit will have no effect in DMI mode.0 - VC1 support disabled.1 - VC1 support enabled.Example: bit 0 = IIO PCIe Port 0 ... bit n = IIO PCIe Port n.		
		0		

Socket1 Configuration	Sck1 RP Correctable Err	Applies to root ports only. Enable interrupt on correctable errors.			
		►No	Yes		
	Sck1 RP NonFatal Uncorrectalbe Err	Applies to root ports only. Enable interrupt on a non-fatal error.			
		►No	Yes		
	Sck1 RP Fatal Uncorrectable Err	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.			
		►No	Yes		
	TraceHub Configuration Menu	TraceHub Configuration Settings.			
		North Trace Hub 1-4 Enable Mode	Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software.		
			►Disabled	Target Debugger	Host Debugger

Socket1 Configuration	Port 1A/1C/1E/1G/4A/4C/4E/4G/5A/5C/5E/5G	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable.			
			Auto	Disable	►Enable	
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable.			
			►Enable	Disable		
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.			
			Yes	►No		
		Link Speed	Choose link speed for this PCIe port.			
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	
			Gen 3 (8 GT/s)	Gen 4 (16 GT/s)	Gen 5 (32 GT/s)	
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.			
			►Enable	Disable		
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
			►Auto	128B	256B	512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.			
			Auto	►Disable		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge.			
			2			
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge.			
			1			
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits).			
			1			
		(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge.			
			1			
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits).			
			1			

Socket1 Configuration	Port 1A/1C/1E/1G/4A/4C/4E/4G/5A/5C/5E/5G	(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge.			
			0			
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits).			
			1			
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.			
			0			
	Port 2A	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable.			
			Auto	Disable	►Enable	
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable.			
			►Enable	Disable		
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.			
			Yes	►No		
		Link Speed	Choose link speed for this PCIe port.			
			►Auto	Gen 1 (2.5 GT/s)	Gen 2 (5 GT/s)	
			Gen 3 (8 GT/s)	Gen 4 (16 GT/s)	Gen 5 (32 GT/s)	
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.			
			►Enable	Disable		
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
			►Auto	128B	256B	512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.			
			►Enable	Disable		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			►Enable	Disable		
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge.			
			2			
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge.			
			8			
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits).			
			1			
		(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge.			
			1			
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits).			
			1			
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge.			
			0			

Socket1 Configuration	Port 2A	(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 4

Socket1 Configuration	Port 3A	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable. Auto / Disable / ►Enable
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable. ►Enable / Disable
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active. Yes / ►No
		Link Speed	Choose link speed for this PCIe port. ►Auto / Gen 1 (2.5 GT/s) / Gen 2 (5 GT/s) Gen 3 (8 GT/s) / Gen 4 (16 GT/s) / Gen 5 (32 GT/s)
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register. ►Enable / Disable
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default. ►Auto / 128B / 256B / 512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default. ►Enable / Disable
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable. ►Enable / Disable
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge. 0
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge. 0
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits). 1
		(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge. 0
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge. 0
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 0

Socket1 Configuration	Port 0A/0C/0E/0G	Hot Plug Capable	This option specifies if the link is considered Hot Plug capable. Auto | ►Disable | Enable
		Surprise Hot Plug Capable	This option specifies if the link is considered Surprise Hot Plug capable. Enable | ►Disable
		PCI-E Port Link Disable	This option disables the link so that the no training occurs but the CFG space is still active. Yes | ►No
		Link Speed	Choose link speed for this PCIe port. ►Auto | Gen 1 (2.5 GT/s) | Gen 2 (5 GT/s) Gen 3 (8 GT/s) | Gen 4 (16 GT/s) | Gen 5 (32 GT/s)
		Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register. ►Enable | Disable
		PCI-E Port MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default. ►Auto | 128B | 256B | 512B
		PCI-E ASPM Support	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default. Enable | ►Disable
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable. ►Enable | Disable
		(IIO) Extra Bus Reserved	(IIO) Extra Bus Reserved for bridges behind this Root Bridge. 0
		(IIO) Reserved Memory	(IIO) Reserved Memory Range for this Root Bridge. 0
		(IIO) Reserved Memory Alignment	(IIO) Reserved Memory Alignment (0 - 31 bits). 1
		(IIO) Reserved Prefetchable Memory	(IIO) Reserved Prefetchable Memory for this Root Bridge. 0
		(IIO) Reserved Prefetchable Memory Alignment	(IIO) Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) 64 bit Reserved Prefetchable Memory	(IIO) 64 bit Reserved Prefetchable Memory Range for this Root Bridge. 0
		(IIO) 64 bit Reserved Prefetchable Memory Alignment	(IIO) 64 bit Reserved Prefetchable Memory Alignment (0 - 31 bits). 1
		(IIO) Reseved I/O	(IIO) Reseved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. 0

IOAT Configuration	All IOAT configuration options.						
	Sck0/1 IOAT Config	DSA	Select Dsa Enable/Disable.				
			►Enable	Disable			
		IAX	Select Iax Enable/Disable.				
			►Enable	Disable			
	Relaxed Ordering	Relaxed Ordering Enable/Disable.					
		►No	Yes				
Intel VT for Directed I/O (VT-d)	Press <Enter> to bring up the Intel Virtualization for Direction I/O (VT-d) Configuratioin menu.						
	Intel VT for Directed I/O	Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables. To disable VT-d, X2APIC must also be disabled.					
		►Enable	Disable				
	Interrupt Remapping	Enable/Disable VT-d Interrupt Remapping Support. To disable Interrupt Remapping, X2APIC must also be disabled.					
		►Auto	Enable	Disable			
	Pre-boot DMA Protection	Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)					
		Enable	►Disable				
	PCIe ACSCTL	Enable/Disable overwrite of PCI Access Control Services Control register in PCI root ports.					
		Enable	►Disable				
Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.						
	Intel VMD for Volume Management Device on Socket 0	VMD Config for PCH ports/ VMD Config for IOU0-4					
		Enable/Disable VMD	Enable/Disable VMD in this Stack.				
			Enable	►Diable			
	Intel VMD for Volume Management Device on Socket 1	VMD Config for PCH ports/ VMD Config for IOU0-5					
		Enable/Disable VMD	Enable/Disable VMD in this Stack.				
			Enable	►Diable			
PCI-E ASPM Support (Global)	This option can disable ASPM support in all PCIe root ports.						
	►Disable	Per-Port					
PCIe Max Read Request Size	This option can set requested Max Read Request Size in PCI hierarchy. 'Default' keeps hardware default.						
	AUTO	128B	256B	512B	1024B	2048B	►4096B
Equalization Bypass To Highest Rate	Equalization Bypss To Highest Rate Support Enable/Disable.						
	►Enable	Disable					

4.6.5 Advanced Power Management Configuration

Displays and provides to change the Power Management settings.

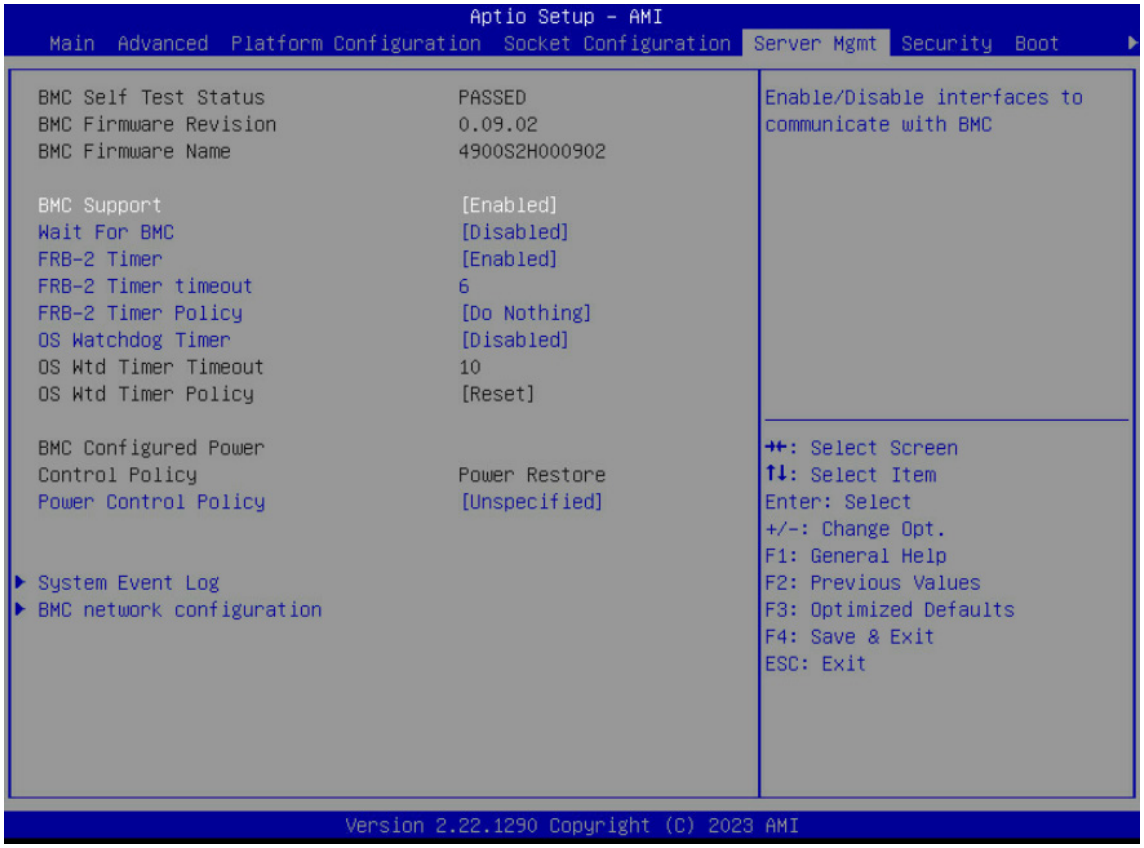
Advanced Power Management Configuration					
CPU P State Control	P State Control Configuration Sub Menu, include Turbo, XE and etc.				
	SpeedStep (Pstates)	Enable/Disable EIST (P-States).			
		▶Enable	Disable		
	EIST PSD Function	Choose HW_ALL/SW_ALL in _PSD return.			
		▶HW_ALL	SW_ALL		
	Turbo Mode	Enable/Disable processor Turbo Mode.			
		▶Enable	Disable		
Hardware PM State Control	Hardware P-States	• Disable: Hardware chooses a P-state based on OS Request (Legacy P-States). • Native Mode: Hardware chooses a P-state based on OS guidance. • Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance). **NOTE** When HWP mode is Disable or Out of Band Mode, Dynamic SST-PP,SST-BF and SST-CP will be disabled.			
		▶Native Mode	Out of Band Mode	Native Mode with No Legacy Support	Disable
Frequency Prioritization	Frequency Prioritization Control.				
	SST-CP	This knob controls whether SST-CP is enabled. When enabled it activates per core power budgeting. **NOTE** HWP Native Mode is a pre-requisite for enabling SST-CP.			
		Enable	▶Disable		
CPU C State Control	CPU C State setting.				
	Enable Monitor MWAIT	Allows Monitor and MWAIT instructions, Auto maps to Enable.			
		▶Auto	Enable	Disable	
	CPU C1 auto demotion	Allows CPU to automatically demote to C1. Takes effect after reboot.			
		▶Auto	Enable	Disable	
	CPU C6 report	Enable/Disable CPU C6(ACPI C3) report to OS, Auto maps to enable.			
		▶Auto	Enable	Disable	
	Enhanced Halt State (C1E)	Core C1E auto promotion control. Takes effect after reboot. Will be enforced to enable when Optimized Power Mode is enabled.			
		▶Enable	Disable		
Package C State Control	Package C State setting.				
	Package C State	Package C State limit, the state Auto maps is program specific.			
		▶C0/C1 state	C2 state		
		C6(non Retention) state	C6(Retention) state		
		No Limit	Auto		

CPU Thermal Management	CPU Thermal Related setting.			
	PROCHOT Modes	When a processor thermal sensor trips (either core), the PROCHOT# will be driven.		
		►Input-only	Disable	
	Thermal Monitor	Enables/disables Thermal Monitor.		
		►Enable	Disable	
	Therm-Monitor-Status Filter	Enables Filter based therm_monitor_status(IA32_THERM_STATUS[0]) reporting.		
		Enable	►Disable	
	PROCHOT RATIO	Controls the CPU response to an inbound platform assertion of xxPROCHOT# by capping to the programmed ratio. Default value 0 will allow ME to control this value. If ME does not set ratio, default 0 equates to Pn. A non-zero value will override ME setting. The min allowed ratio is defined by PLATFORM_INFO[MIN_OPERATING_RATIO].		
		0		
	TCC Activation Offset	Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated.		
		0		
CPU- Advanced PM Tuning	Setting Energy Per Bias Pwr_Ctl, PP0 Current SWL TD, SAPM etc.			
	Energy Perf BIAS	Energy Perf BIAS Sub Menu.		
		Power Performance Tuning	Options decides who Controls EPB. • In OS mode: IA32_ENERGY_PERF_BIAS is used • In BIOS mode: ENERGY_PERF_BIAS_CONFIG is used • In PECI mode: PCS53 is usedWill be enforced to BIOS controls EPB when Optimized Power Mode is enabled	
			►OS Controls EPB	BIOS Controls EPB	PECI Controls EPB
		Dynamic Loadline Switch	Dynamic Loadline Switch control. MSR 0x1FC[Bit33].	
			►Enable	Disable
		Workload Configuration	This allows optimization for the workload characterization. The three options for selection.	
			►Balanced	I/O sensitive
		Averaging Time Window	This is used to control the effective window of the average for C0 and P0 time.	
			1A	
		P0 TotalTimeThres-hold Low	The HW switching mechanism DIABLES the performance setting (0) when the totoal P0 time is less than this threshold.	
			28	
		P0 TotalTimeThres-hold High	The HW switching mechanism ENABLES the performance setting (0) when the totoal P0 time is greater than this threshold.	
			3F	
	Optimized Power Mode	Enable/Disable Optimized Power Mode.		
		Enable	►Disable	
Package Current Config	Program PRI_PLANE_CURT_CFG_CTRL_MSR 0x601 Sub Menu.			
	Current Limit Override	Disable - Default, do nothing; Enable, overrride Current limitation in 1/8 A increments.		
		Enable	►Disable	
	Lock Indication	Lock for CURRENT_LIMIT settings Move this into the Config Above.		
		►Enable	Disable	

SOCKET RAPL Config	SOCKET RAPL Configuration Sub Menu - TURBO_POWER_LIMIT CSR & MSR.							
	FAST_RAPL_ NSTRIKE_PL2_ DUTY_CYCLE	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) - 64 (25%)						
		64						
	Package RAPL Limit MSR Lock	Enable/Disable locking of Package RAPL Limit MSR and a reset will be required to unlock the register.						
		Enable			►Disable			
	Package RAPL Limit CSR Lock	Enable/Disable locking of Package RAPL Limit CSR and a reset will be required to unlock the register.						
		►Enable			Disable			
	PL1 Power Limit	PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.						
		0						
	PL1 Time Window	PL1 value in seconds. The value may vary from 0 to 448. Indicates the time window over which TDP value should be maintained.						
		►1	1.25	1.5	1.75	2	2.5	3	3.5
		4	5	6	7	8	10	12	14
		16	20	24	28	32	40	56	64
		80	96	112	128	160	192	224	256
		320	384	448	0.001	0.0012	0.0015	0.0017	0.002
		0.0024	0.003	0.0034	0.004	0.005	0.006	0.007	0.008
		0.01	0.012	0.014	0.016	0.02	0.023	0.027	0.031
		0.039	0.047	0.055	0.063	0.078	0.094	0.109	0.125
		0.156	0.188	0.219	0.25	0.313	0.375	0.438	0.5
		0.625	0.75	0.875					
	PL2 Power Limit	PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 120% * TDP							
		0							
	PL2 Time Window	PL2 value in seconds. The value may vary from 0 to 0.438. Indicates the time window over which TDP value should be maintained.							
		1	1.25	1.5	1.75	2	2.5	3	3.5
		4	5	6	7	8	10	12	14
		16	20	24	28	32	40	56	64
		80	96	112	128	160	192	224	256
		320	384	448	0.001	0.0012	0.0015	0.0017	0.002
		0.0024	0.003	0.0034	0.004	0.005	0.006	0.007	0.008
		0.01	►0.012	0.014	0.016	0.02	0.023	0.027	0.031
		0.039	0.047	0.055	0.063	0.078	0.094	0.109	0.125
		0.156	0.188	0.219	0.25	0.313	0.375	0.438	0.5
		0.625	0.75	0.875					
System Power Control (Psys)	System Power Control (Psys) Sub Menu.								
	Platform Power Balancing	Enable the platform power balancing BIOS to Pcode command.							
		Enable			►Disable				
	Platform RAPL Limit CSR Lock	Enable/Disable locking of Platform Power Limit CSR and a reset will be required to unlock the register.							
		►Enable			Disable				
	Platform RAPL Info CSR Lock	Enable/Disable locking of Platform Power Info CSR and a reset will be required to unlock the register.							
		►Enable			Disable				
	Platform RAPL Limit &Info	Configure Platform RAPL Limit and Info by Platform Power Limit and Info CSR. SKIP: Use hardware default Manual: External customer to input manually Other options: Predefined board configures (PSU Config 1: 1600W PSU, PCU Config 2: 2130W PSU)							
		►SKIP							
		ARCHERCITY 1x PSU Config 1			ARCHERCITY 1x PSU Config 2				
		ARCHERCITY 2x PSU Config 1			ARCHERCITY 2x PSU Config 2				
		ARCHERCITY 3x PSU Config 1			Manual				

System Power Control (Psys)	Platform RAPL Domain	Configure Psys socket primary and secondary by B2P mailbox PSYS_CONFIG.SKIP: Use hardware defaultManual: External customer to input manuallyARCHERCITY: Even socket is primary and odd socket is secondary			
		►SKIP	ARCHERCITY	Manual	
PMax Detector Configuration	PMax Detector Control Sub Menu.				
	PMax Config Sign	Negative: Detector will trip on higher power consumption. Positive: Detector will trip on lower power consumption.			
		►Positive	Negative		
	PMax Config Positive Offset	Input decimal correction factor to program. Valid input values are 0 to 31. Will be positive based on PMAX Config Sign value.			
		0			
	Trigger Setup	Possible selection options [0], [1], [2] [0] = Interaction disabled (default) [1] = Enable external trigger mode [2] = Enable internal trigger observability			
		0			
Memory Power & Thermal Configuration	Displays and provides option to change the Memory Settings.				
	DRAM RAPL Configuraion	DRAM RAPL Control Sub Menu.			
		DRAM RAPL Power Limit Lock CSR	This Option allows unlock/lock DRAM_ PLANE_POWER_LIMIT.pp_pwr_lim_lock. Enable - LockDisable - Unlock		
			►Enable	Disable	
		Override BW_LIMIT_TF	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled		
			0		
		CMS ENABLE DRAM PM	CMS ENABLE DRAM PM.		
			►Enable	Disable	
	Memory Thermal	Set memory thermal settings.			
		Throttling Mode	Configure Thermal Throttling Mode.		
			►CLTT	CLTT with PECI	Disable
		MEMTRIP REPORTING	If set to 0, processor will ignore all Mem Trip tree. If set to 1 processor will include all Mem Trip tree.		
			►Enable	Disable	
	Select Temperature Refresh Value	Option to manually enter Temperature refresh value. Select Manual to enter value, Auto for default.			
		►Auto	Manual		
	Dimm Temperature Offset Cooling Type	DIMM cooling type to define temperature Offset value.			
		►Air cooling	Liquid cooling (tube)	Immersion cooling	
	MEMHOT INPUT	Configue Memhot input.			
		Enable	►Disable		
	MEMHOT OUTPUT	Configure MEMHOT Output Mode options: Enable/Disable the Throt Output high, mid and low bit fields.			
		Disabled	►Enable only temphi	Enable only temphi & mid	Enable only temphi, mid and low
	Memory Power Savings Advanced Options	Advanced Settings for CKE and related Memory Power Savings Features.			
		CKE Throttling	Configures CKE Throttling.		
			►Auto	Manual	
		SREF Feature	Select manual or auto programming Self Refresh feature.		
			►Auto	Manual	
		PKGC SREF EN	Enables or disables PKGC Self Refresh.		
			►Enable	Disable	
		Data DLL Off EN	Enables or disables Data DLL Off feature of Low Power Mode.		
			►Enable	Disable	

4.7 Server Mangement



Server Management				
BMC Support	Enable/Disable interfaces to communication with BMC.			
	▶Enable	Disable		
Wait for BMC	Wait for BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.			
	Enable	▶Disable		
FRB-2 Timer	Enable or Disable FRB-2 timer (POST timer).			
	▶Enable	Disable		
FRB-2 Timer timeout	Enter value Between 1 to 30 min for FRB-2 Timer Expiration.			
	6			
FRB-2 Timer Policy	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.			
	▶Do Nothing	Reset	Power Down	Power cycle
OS Watchdog Timer	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.			
	Enable	▶Disable		
Power Control Policy	Configure how the system should respond if AC Power is lost,Reset not required as selected Power policy will be set in BMC when policy is saved.			
	Do Not Powerup	Last Power State	Power Restore	▶Unspecified

4.7.1 System Event Log

Press <Enter> to change the SEL event log configuration.

System Event Log				
SEL Components	Change this to enable or disable event logging error/progress codes during boot.			
	▶Enable	Disable		
Erase SEL	Choose options for erasing SEL.			
	Yes, on next reset	Yes, on every reset	▶No	
When SEL is Full	Choose options for reactions to full SEL.			
	▶Do Nothing	Erase Immediately	Delete oldest Record	
Log EFI Status Codes	Disables the logging of EFI Status Codes or log only error code or only progress code or both.			
	▶Error code	Progress code	Both	Disable

4.7.2 BMC Network Configuration

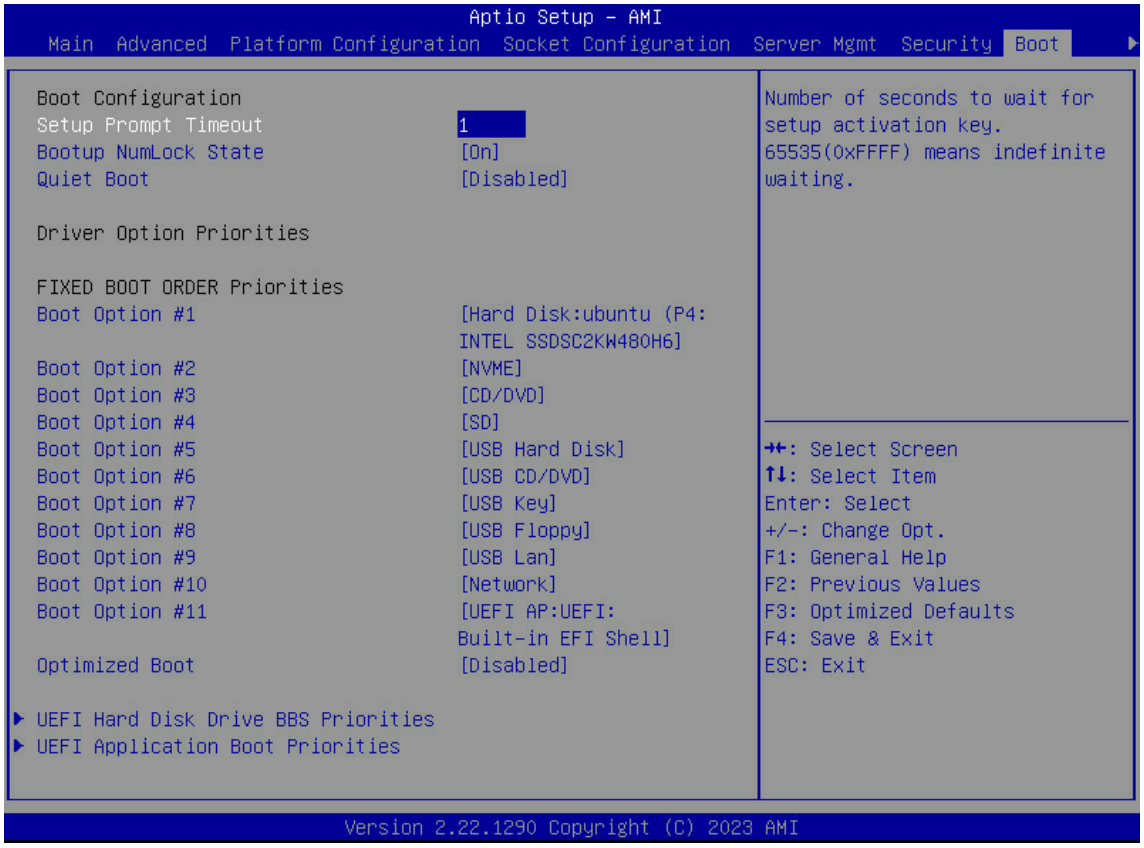
Configures BMC network parameters.

BMC Network Configuration				
Configuration Address source Lan1/2/3	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.			
	▶Unspecified	Static	DynamicBmcDhcp	DynamicBmcNon Dhcp
Configure IPv6 support				
IPv6 Support Lan1/2/3	Enables/disables LAN1 IPv6 Support			
	▶Enabled	Disabled		
Configuration Address source Lan1/2/3	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.			
	▶Unspecified	Static	DynamicBmcDhcp	
Configuration Gateway Lan1/2/3 Address source	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase			
	▶Unspecified	Static	DynamicBmcDhcp	
Configure VLAN support				
VLAN Support Lan1/2/3	Enable VLAN Support to specify the 802.1q VLAN ID.			
	▶Unspecified	Enabled	Disabled	

4.8 Security

Security			
Administrator Password	Set administer password.		
User Password	Set User Password.		
Disable Sanitize Freeze Lock	If this option is enabled, then sending Sanitize Freeze Lock command to HDDs will be skipped in next boot.		
	Enable	▶Disable	
P4:INTEL SSDSC2KW480H6	HDD Security Configuration for selected drive.		
	Set User Password	Set HDD User Password. ***Advisable to Power Cycle System after Setting Hard Disk Passwords***. Discard or Save changes option in setup does not have any impact on HDD when password is set or removed. If the 'Set HDD User Password' option is hidden, do power cycle to enable the option again.	
Secure Boot	Secure boot configuration.		
	Secure Boot	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset.	
		▶Enabled	Disabled
	Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.	
		▶Standard	Custom

4.9 Boot

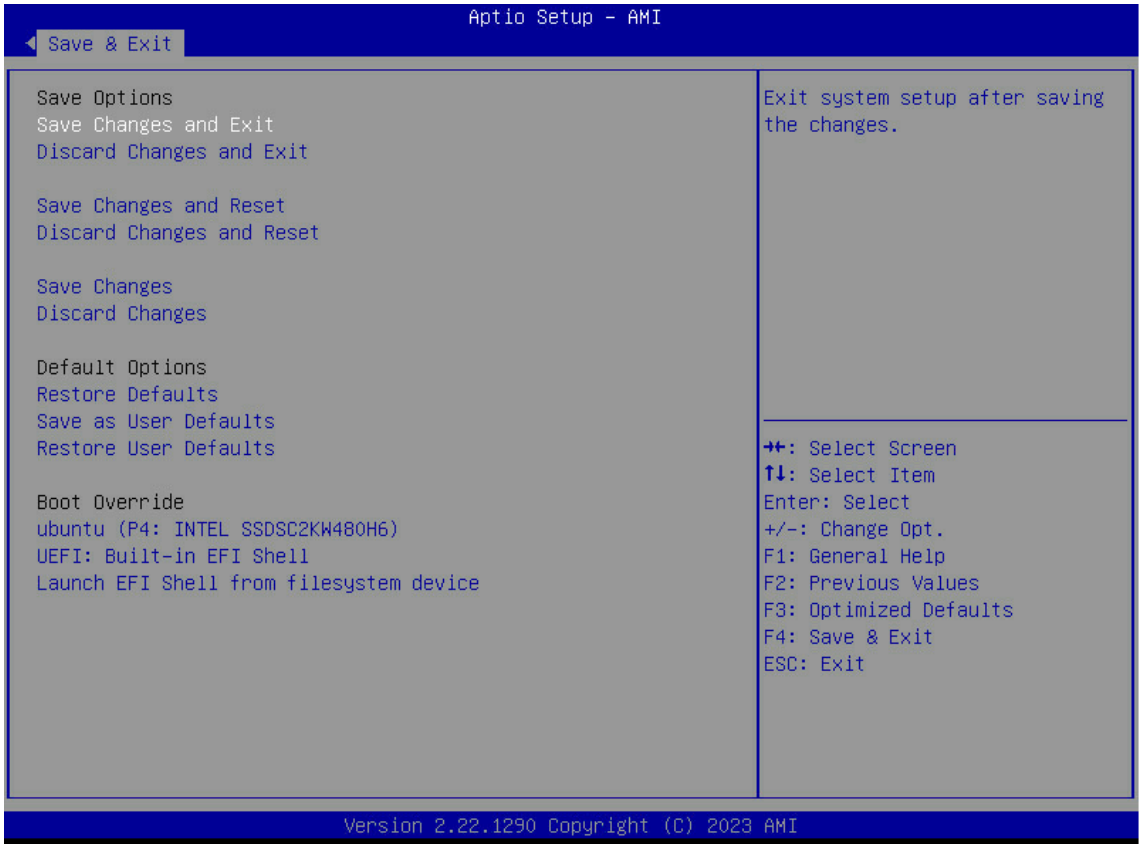


Boot		
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.	
	1	
Bootup NumLock State	Select the keyboard NumLock state.	
	▶On	Off
Quiet Boot	Enables/disables Quiet Boot option.	
	Enable	▶Disable
Boot Option #1	Sets the system boot order.	
	▶Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #2	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	▶NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled

Boot Option #3	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	►CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #4	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	►SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #5	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	►USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #6	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	►USB CD/DVD
	USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #7	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	►USB Key	USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #8	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	►USB Floppy
	USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #9	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	►USB Lan	Network
	UEFI AP:UEFI: Built-in EFI Shell	Disabled

Boot Option #10	Sets the system boot order.		
	Hard Disk// Move "*" to the desired Option	NVME	
	CD/DVD	SD	
	USB Hard Disk	USB CD/DVD	
	USB Key	USB Floppy	
	USB Lan	►Network	
	UEFI AP:UEFI: Built-in EFI Shell	Disabled	
Boot Option #11	Sets the system boot order.		
	Hard Disk// Move "*" to the desired Option	NVME	
	CD/DVD	SD	
	USB Hard Disk	USB CD/DVD	
	USB Key	USB Floppy	
	USB Lan	Network	
	►UEFI AP:UEFI: Built-in EFI Shell	Disabled	
Optimized Boot	Enables/disables Optimized Boot. Enabling Optimized Boot will disable Csm support and disable connecting Network devices to decrease boot time. While disabling Optimized Boot, make sure to restore Csm Support option to previous value before enabling Optimized Boot.		
	Enable	►Disable	
UEFI Hard Disk Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI Hard Disk Drives.		
	Boot Option #1	Sets the system boot order.	
		►ubuntu (P4: INTELSSDSC2KW480H6)	Disable
UEFI Application Boot Priorities	Specifies the Boot Device Priority sequence from available UEFI Application.		
	Boot Option #1	Sets the system boot order.	
		►UEFI: Built-in EFI Shell	Disable

4.10 Save & Exit



Exit	
Save Changes and Exit	Exit system setup after saving the changes.
Discard Changes and Exit	Exit system setup without saving any changes.
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Reset system setup without saving any changes.
Save Changes	Save changes done so far to any of the setup options.
Discard Changes	Discard changes done so far to any of the setup options
Restore Defaults	Restore/Load Default values for all the setup options.
Save as User Defaults	Save the changes done so far as User Defaults.
Restore User Defaults	Restore the User Defaults to all the setup options.
ubuntu (P4: INTEL SSDSC2KW480H6)	
UEFI: Built-in EFI Shell	
Launch EFI Shell from filesystem device	Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

4.11 BIOS Update Process

This is the manual for updating BIOS on **SB102-HK** system. Please check current system BIOS version is ASKA0020 or later. Here are the update procedures.

EFI:
1. Copy ASKA0030.bin to EFI folder
2. Copy EFI folder to USB stick or HDD
3. Boot into internal shell enters the usb EFI folder and executes the below command Bios.nsh
4. If the firmware update is complete, perform an AC power cycle.

Linux:
1. Copy ASKA0030.bin to AfuLnx64 folder
2. Copy AfuLnx64 folder to USB stick or HDD
3. Enter to AfuLnx64 folder and execute the below command./flash.sh
4. Reboot if complete the updated

NOTE
AFU FLASH Update may report change in ROM Layout. You can "F" to force the FLASH.

NOTE
Please refer to "**Bios Update Process.doc**" in bios release zip file for details.

4.12 BIOS Post Code

There are two ways to get post code,

1. check the LED debug card
2. execute the IPMI command as below

```
$ ipmitool -I lanplus -H "$BMC_IP" -U "$BMC_USER" -P "$BMC_PASSWD" raw 0x32 0x73 0x00
```

e.g. $ipmitool -I lanplus -H 192.168.0.3 -U admin -P admin raw 0x32 0x73 0x00

> **NOTE**
> **BMC IP:** -H $BMC_IP
> **User Account:** -U $BMC_USER
> **Password:** -P $BMC_PASSWD

Intel RC POST Code

Post Code	Description
KTI POST code - Major	
0xA0	Initialize KTI input structure default values
0xA1	Collect info such as SBSP, Boot Mode, Reset type etc
0xA3	Setup up minimum path between SBSP & other sockets
0xA6	Sync up with PBSPs
0xA7	Topology discovery and route calculation
0xA8	Program final route
0xA9	Program final IO SAD setting
0xAA	Protocol layer and other Uncore settings
0xAB	Transition links to full speed operation
0xAE	Coherency Settings
0xAF	KTI is done
KTI Error code	
0xD8	Boot Mode Error
0xD9	Minimum Path Setup Error
0xDA	Topology Discovery Error
0xDB	SAD Setup Error
0xDC	Unsupported Topology Error
0xDD	Full Speed Transition Error
0xDE	S3 Resume Error
0xDF	SW Check Error
MRC Test Points	
0x70	HBM State
0x71	HBM Debug State
0x72	HBM Internal State
0x7E	Pipe Sync State
0xB0	Dimm Detect
0xB1	Clock Init
0xB2	Access SPD Data
0xB3	Global Early State

0xB4	Rank Detect
0xB5	Parallel Dispatch
0xB6	DDRIO Init
0xB7	Channel Training
0xB8	Init Throttling
0xB9	Memory BIST
0xBA	Memory Init
0xBB	Print DDR Memory Map
0xBC	Config RAS
0xBD	Get Margins
0xBE	SSA API Init
0xBF	MRC Done
0xC1	Check POR
0xC2	Unlock Memory REGS
0xC3	Check Status
0xC4	Config XMP
0xC5	Memory Early Init
0xC6	Print DIMM Info
0xC7	NVDIMM Init
0xC9	SVL Scramble
0xCA	CMI Credit
0xCB	Check RAS
0xCC	Init ADR
0xCD	Init Structure Late State
0xCE	Memory Init Late State
0xCF	Select Boot Mode
0xD0	MKTME Early Flow
0xD1	SGX Pre-Memory Init
0xD2	Memory Health Teset
0xD3	Enable 2N mode
0xD5	CPL2 state
0xD6	Offset Training Result
0xD7	DIMM Manifest
0xD8	Turn Around
0xD9	CPGC OOO Mode
0xDA	Actm Mem Alias
0xDB	Enable Host Refresh
0xDC	SGX TDX Configure
0xDD	Disable Unused Memory Channel
MRC error code	
0xE0	SPD Decode Error
0xE6	RC DCA DFE Error
0xE7	RC Sweep LIB Internal Error
0xE8	No Memory Error
0xE9	LT Lock Error
0xEA	DDR Init Error
0xEB	Memory Test Error

0xEC	Vendor Specific Error
0xED	DIMM Incompatible Error
0XEE	MRC Compatibility Error
0xEF	MRC Structure Error
0xF0	Set Vdd Error
0xF1	IOT Memory Buffer Error
0xF2	RC Internal Error
0xF3	Invalid Register Access Error
0xF4	Set MC Freq Error
0xF5	Read MC Freq Error
0x70	DIMM Channel Error
0x74	BIST Check Error
0xF6	SMBUS Error
0xF7	PCU Error
0xF8	NGN Error
0xF9	Interleave Failure
0xFA	SKU Limit Error
0xFB	CAR Limit Error
0xFC	CMI Failure
0xFD	Value Out of Range
0xFE	DDRIO HWFSM Error
0xFF	MRC Pointer Error

AMI POST Code

Post Code	Description
0x10	PEI core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization is started (CPU module specific)
0x13	Pre-memory CPU initialization is started (CPU module specific)
0x14	Pre-memory CPU initialization is started (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x17	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x18	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1D~ 0x2A	Oem pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect(SPD) data reading
0x2C	Memory initialization. Memory Presence detection

0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization. (Other)
0x30	Reserved for ASL (See ASL status codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. BootStrap Processor(BSP) initialization
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-memory North Bridge initialization is started
0x38	Post-memory North Bridge initialization is started (North Bridge module specific)
0x39	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3A	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3B	Post-memory South Bridge initialization is started
0x3C	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3D	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3E	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3F~0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
S3 resume progress codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by th DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4~0xE7	Reserved for future AMI progress codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loadded
0xF5~0xF7	Reserved for future AMI progress codes

DXE Phase	
0x60	DXE code is started
0x61	NVRAM initialization
0x62	Initialization of the South Bridge runtimes services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Brodge module specific)
0x6C	North Bridge DXE initialization (North Brodge module specific)
0x6D	North Bridge DXE initialization (North Brodge module specific)
0x6E	North Bridge DXE initialization (North Brodge module specific)
0x6F	North Bridge DXE initialization (North Brodge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	North Bridge DXE initialization (South Brodge module specific)
0x74	North Bridge DXE initialization (South Brodge module specific)
0x75	North Bridge DXE initialization (South Brodge module specific)
0x76	North Bridge DXE initialization (South Brodge module specific)
0x77	North Bridge DXE initialization (South Brodge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A~0x7F	Reserved for future AMI DXE codes
0x80~0x8F	OEM DXE initialization codes
0x90	Boot Device Selection(BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E~0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE detect
0xA3	IDE Enable

0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Satrt of Setup
0xAA	Reserved for ASL(See ASL Status Codes selection below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL(See ASL Status Codes selection below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM initialization
0xB3	System Reset
0xB4	USB Hot Plug
0xB5	PCI bus Hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8~0xBF	Reserved for future AMI codes
0xC0~0xCF	OEM BDS initialization codes
ACPIASL Checkpoints	
0x01	System is entering S1 sleeping state
0x02	System is entering S2 sleeping state
0x03	System is entering S3 sleeping state
0x04	System is entering S4 sleeping state
0x05	System is entering S5 sleeping state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

Chapter 5. Technical Support

www.aicipc.com

Taiwan, Global Headquarters
Address: No. 152, Section 4, Linghang N. Rd, Dayuan District, Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China
Address: Room 215, Building 4, No.471 Guiping Road, Xuhui District, Shanghai City, 200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia
Address: No. 500, 5th Floor, 5th Entrance, 32A, Khoroshevskoye Shosse, Moscow, 123007
Tel: +7-4997019998A
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States
Address: 48531 Warm Springs Boulvard Suite 404 Fremont, CA 94539, United States
Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States
Address: 21808 Garcia Lane City of Industry, CA 91789, United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: + 1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States
Address: 322 Route 46 West Suite 100 Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands
Address: Peppelkade 58, 3992AK, Houten, The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com

For additional technical support or questions about trouble shooting, please contact the AIC® representative nearest to you or visit our AIC® website for more information.
AIC® website: https://www.aicipc.com/en/faq.