Vega

Server Motherboard
User's Manual

UM_Vega_v1.6_012226

Table of Contents

Preface i
Safety Instructions ii
About This Manual iii
Chapter 1. Product Features 1
1.1 Component 1
1.2 Specifications 2
1.3 Feature 3
Chapter 2. Hardware Setup 4
2.1 Central Processing Unit 4
2.1.1 Installation 4
2.2 System Memory 10
2.2.1 Placement 10
2.2.2 DDR5 DIMM Support 11
2.2.3 DIMM Population guide 11
2.2.4 DIMM Mixing Rules 12
2.2.5 Mapping Table 13
2.2.6 Installation 14
2.3 RTC (Real Time Clock) Battery 15
2.3.2 Installation Guide 16
2.3.3 Removal Guide 17
Chapter 3. Motherboard Settings 18
3.1 Block Diagram 18
3.2 Placement 19
3.3 Content List 20
3.4 External Port 22
3.5 Connector Definition 23
3.6 Jumper Definition 32
3.7 LED 35
3.7.1 Rear Chassis LEDs 35
3.7.2 Internal LEDs 35
Chapter 4. BIOS Configuration Settings 36
4.1 Navigation Keys 36
4.2 BIOS Menu 37
4.2.1 Menu 37
4.2.2 Startup 37
4.3 Main 38
4.3.1 Main 38
4.4 Advanced 39
4.4.1 Trusted Computing 39
4.4.2 ACPI Settings 40
4.4.3 Redfish Host Interface Settings 40
4.4.4 AST2600 Super IO Configuration 40
4.4.5 Serial Port Console Redirection 40
4.4.6 Option ROM Dispatch Policy 40

4.4.7 PCI Subsystem Settings 41
4.4.8 Network Stack Configuration 41
4.4.9 All Cpu Informaiton 41
4.4.10 RAM Disk Configuration 41
4.5 Platform Configuration 42
4.5.1 PCH-IO Configuration 42
4.5.2 Miscellaneous Configuration 44
4.5.3 Server ME Configuration 46
4.5.4 Runtime Error Logging 46
4.5.4 IIO Error Enabling 48
4.5.5 PCIe Error Enabling 49
4.5.6 Error Control Setting 50
4.5.7 Crash Log Enabling 51
4.5.8 DWR Configuration 51
4.6 Socket Configuration 52
4.6.1 Processor Configuration 52
4.6.2 Uncore Configuration 54
4.6.3 Memory Configuration 56
4.6.4 IIO Configuration 58
4.6.5 Advanced Power Management Configuration 68
4.7 Server Mangement 72
4.7.1 System Event Log 73
4.7.2 BMC Network Configuration 73
4.8 Security 74
4.9 Boot 75
4.10 Save & Exit 78
4.11 BIOS Post Code 79
Chapter 5. Technical Support 85

Document Release History

Release Date	Version	Update Content
September, 2024	1	User's Manual release to public.
December, 2024	1.1	Update Specifications content/MB image.
February, 2025	1.2	Update connector pin define.
April, 2025	1.3	Update content of component, spec and feature. (1.1~1.3)
June, 2025	1.4	Update DIMM population guide and rules. Add RTC Battery installation guide.
June, 2025	1.5	Update BIOS content.
January, 2026	1.6	Remove connector info. (PFR)

Copyright © 2024 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

When installing, operating, or performing maintenance on this equipment, the following safety precautions should always be taken into account in order to reduce the risk of fire, electric shock, and personal injury.

Carefully read the safety instructions below before using this product.

- Observe all of the warning and instruction signs distinctively marked on the product.
- Before performing system installations, please consult the User's Manual provided with this product.
- Do not place this product on an uneven or weak surface (unstable cart, stand, table, ect.) that might induce the product to fall and sustain serious damage.
- Install only the equipment or device identified in the User's Manual. Deploying other equipment or device with this motherboard could invoke improper connection of circuitry that leads to fire or personal injury.
- This product should only be operated with the type of power source indicated on the marked label. If you are questionable about which type of power supply is used in your area, consult your dealer or local Power Company.
- Disconnect the power supply module before removing power from the system.
- Unplug this product from the wall outlet before cleaning. Use a damp cloth for cleaning. Do not use liquid cleaners or aerosol cleaners.
- Do not use this product near a water source, including faucet and lavatory.
- Never spill liquids of any kind on this product.
- Never shove objects of any kind into this product's open slots, as they may touch dangerous voltage points or short out parts and could result in fire or electric shock.
- Do not block or cover slots and openings in this unit, as they were made for ventilation and prevent this unit from overheating. Do not place this product in a built-in installation unless proper ventilation is available.
- Do not disassemble this product. This product should only be taken apart by trained personnel. Opening or removing covers and circuit boards may expose you to electric shock or other risks. Incorrect reassembly can also cause electric shock when the unit is subsequently used.
- Risk of explosion is possible if battery is replaced with an incompatible type. Dispose of used batteries accordingly.
- This product is equipped with a three-wire grounding type plug, a plug with a third (grounding) pin. As a safety feature, this plug is intended to fit only into a grounding type power outlet. If you are unable to insert the plug into the outlet, contact your electrician to replace the outlet. Do not remove the grounding type plug or use a 3-Prong To 2-Prong Adapter to circumvent the safety feature; doing so may result in electric shock and/or damage to this product.

About This Manual

Thank you for selecting and purchasing the Vega server board.
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 the Vega motherboard.

Chapter 1 Product Features
This chapter delivers the overall layout of the product, including the fundamental components on the motherboard, design specifications, and noteworthy features. Vega is an ideal server grade motherboard that is specifically designed to accommodate diverse enterprises for managing heavy workloads, databases, nearline applications, and cloud deployments. This product supports the dual processor with Socket E1 (LGA-4677-X) socket type with a memory support of 8 channel DDR5 RDIMM/LRDIMM with EEC up to 5600/4800 MHz.

Chapter 2 Hardware Setup
This chapter displays an easy installation guide for assembling the CPU (Central Processing Unit) and memory module. Utmost caution for proceeding to set up the hardware is highly advised. The components on the motherboard are highly fragile and vulnerable to exterior influence. Do not attempt to endanger the device by placing the device in a potentially unstable or hazardous surroundings, including positioning the device on an uneven grounds or humid environments.

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 location 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 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.

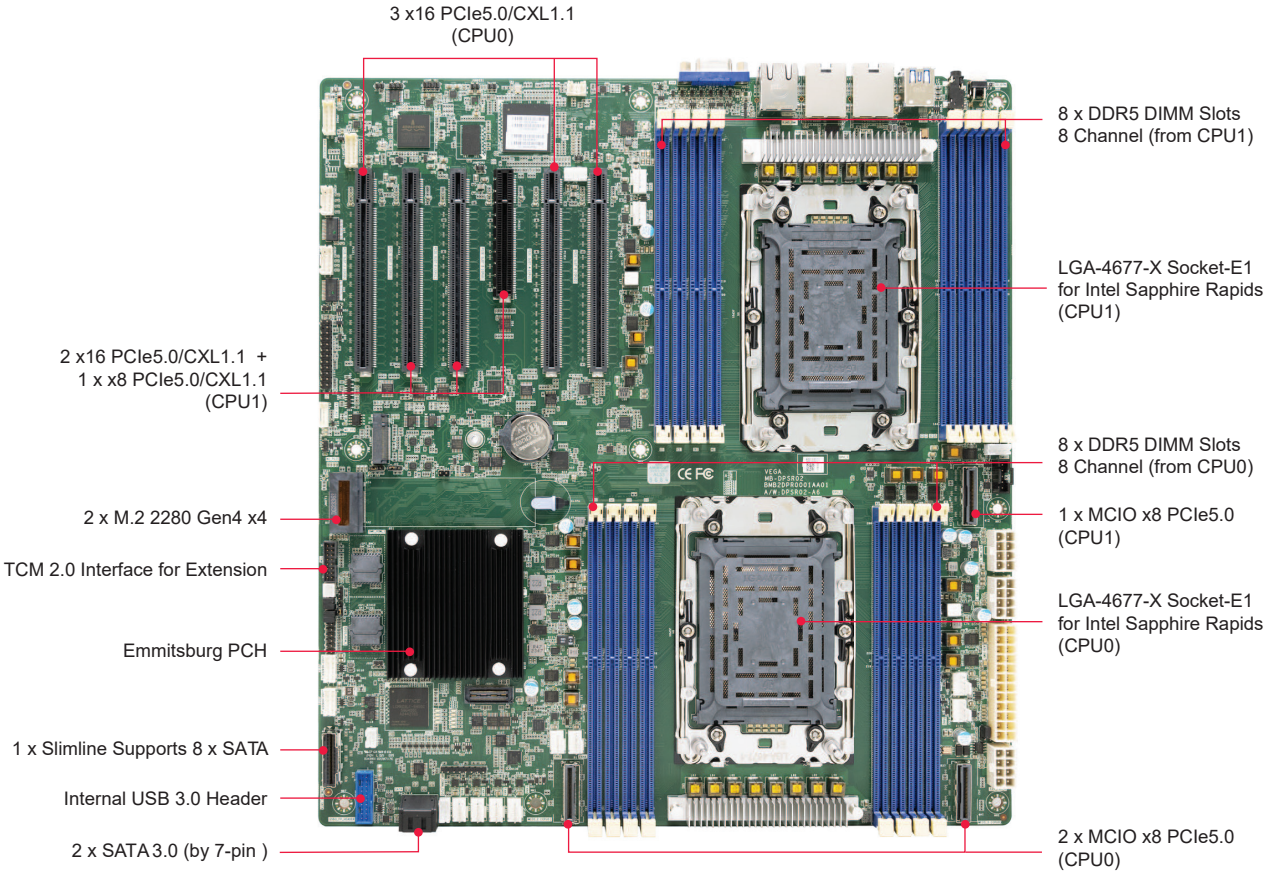
BMC Configuration Settings
BMC Configuration Settings illustrates the diverse functions of IPMI BMC, including the details on logging into the web page and assorted definitions. These descriptions are helpful in configuring various functions through Web GUI without entering the BIOS setup. For more information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

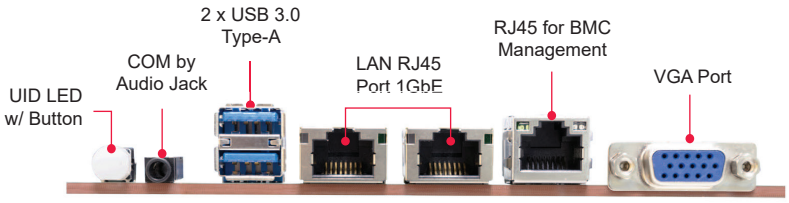
Chapter 1. Product Features

This section describes the hardware specifications and features of the Vega motherboard. The fundamental components of the Vega severboard are provided below.

1.1 Component

Vega Serverboard





Dimensions
mm : 304.8 x 332.7
inches : 12 x 13

Product specifications and features are subject to change without prior notice.

1.2 Specifications

System	Processor Support	Dual Intel® Sapphire Rapids / Emerald Rapids CPU
	CPU TDP	350W
	UPI Speeds	16/20GTs
	Socket Type	Socket E1 (LGA-4677-X)
	System Memory	• DDR5 5600/4800MHz RDIMM (1DPC) • Total 16 memory slots; 8 slots per CPU (1DPC) • Support up to 4TB (3DS RDIMM)
	Expansion Slots	Total support 112 lanes of PCIe5.0 • PCIe slots (up to 5 x16 CXL1.1 devices) - 3 x16 PCIe5.0/CXL1.1 (CPU0) - 2 x16 PCIe5.0/CXL1.1 (CPU1) - 1 x8 PCIe5.0 (CPU1) • MCIO - 3 MCIO x8 PCIe5.0 • M.2 - 2 M.2 2280-D5-M PCIe Gen4 x4
System BIOS	BIOS Type	AMI UEFI BIOS
	BIOS Features	• ACPI • PXE • WOL • AC loss recovery • IPMI 2.0 KCS mode interface • SRIOV • SMBIOS • TPM • Serial console redirection • PCIe hotplug
On-board Devices	SATA	Emmitsburg PCH on-chip solution • 2 x SATA3.0 (6 Gb/s) 7-pin connectors • 1 x Slimline connector (up to 8 SATA ports)
	BMC	ASPEED AST2600

On-board Devices	Network Controller	• Realtek RTL8211FS 1GbE for BMC dedicated management port • Broadcom BCM5720 dual port 1GbE (NCSI for share NIC)
	Graphics	• Integrated VGA support by ASPEED AST2600 • Resolution up to 1920x1200 @60Hz 32bpp
	Additional Information	TPM 2.0 - NUVOTON NPCT760AABYX
Input/Output	SATA	• 2 x SATA3.0 12Gb/s (by 7-pin) • 1 x Slimline connector supports 8 x SATA
	LAN	• 1 x RJ45 GbE connector for BMC dedicate management port • 2 x RJ45 1GbE connectors
	USB	• USB3 - 2 x USB3.1 Gen1 double stack Type-A connectors at rear I/O - 1 x USB3 pin header supports two USB3.1 Gen1 • USB2 - 2 x USB2.0 pin headers support two USB2.0
	VGA	1 x DB-15 VGA connector
	Serial Port	1 x COM connector (Audio Jack)
	Others	1 x external UID/switch button
	Additional Information	Security: • TCM 2.0 interface for extension • TPM 2.0 onboard (Default: N/A; optional by SKU)

1.3 Feature

The Vega server board offers the latest Xeon® Scalable Processors technology solutions with compelling performance and provides premium power efficiency, which is optimized for efficient performance platforms (storage, security and communications infrastructure)

Vega supports dual 4th/5th Generation Intel® Xeon® Scalable Processors with 3 UPIs (up to 20GTs), per CPU cores up to 60, and TDP up to 350W. With builtin Intel® C741, it supports up to 4TB DDR5 3DS RDIMM with 16 memory slots and memory speeds up to 5600MHz.

The high speed expansion I/O includes 5 x16 PCIe5.0/CXL1.1 slots, 1 x8 PCIe5.0 slot, 3 MCIO x8 PCIe5.0, 2 M.2 2280 PCIe4.0 x4, 2 SATA3.0 7pin connectors (6 Gb/s), and 1 slimline connector (up to 8 SATA). Security featuresinclude TPM 2.0 and TCM 2.0interface for extension.

- Supports 4th/5th Gen Intel® Xeon® Scalable Processors for highest every performance and improved power efficiency
- Supports 16DDR5 DIMM slots for maximum memory performance
- Supports Compute Express Link (CXL1.1)
- Six PCIe slots can support three FHFL PCIe5.0 x16 add-in cards
- Supports three MCIO x8, total 24 PCIe5.0 lanes

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 Socket E1 (LGA-4677-X).

2.1.1 Installation

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

☑ a T30 torque screwdriver

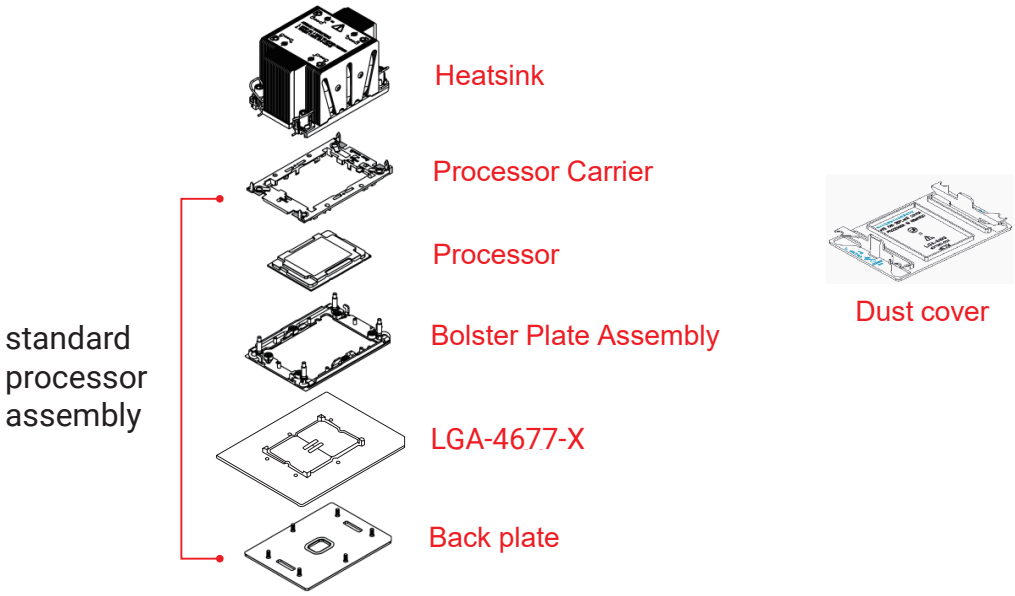
☑ ESD wrist strap/mat and conductive foam pad

☑ 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.

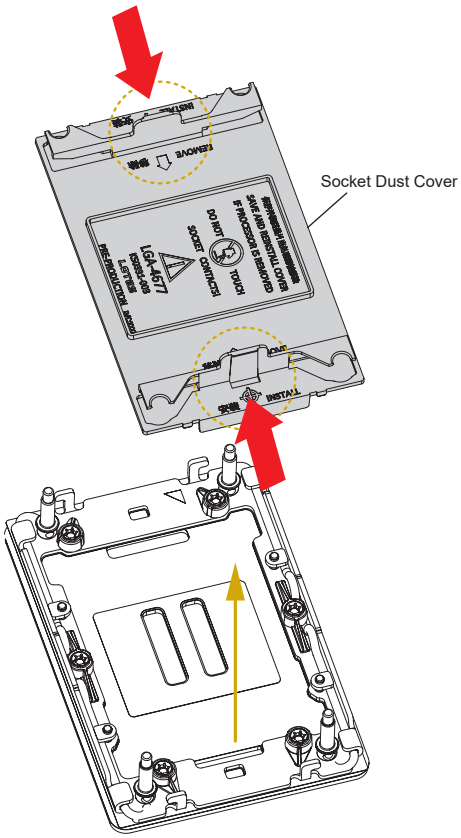
Standard Processor Assembly:
A standard processor assembly is comprised of 5 components: processor carrier, processor, bolster plate assembly, socket and back plate.



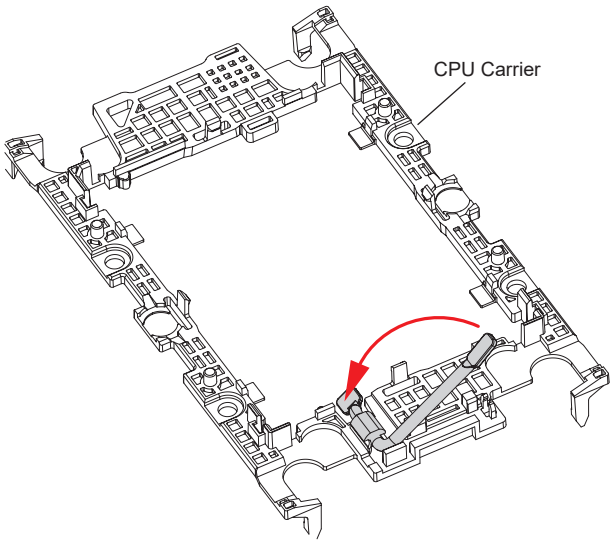
This information is provided for professional technicians only.

Procedure:

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

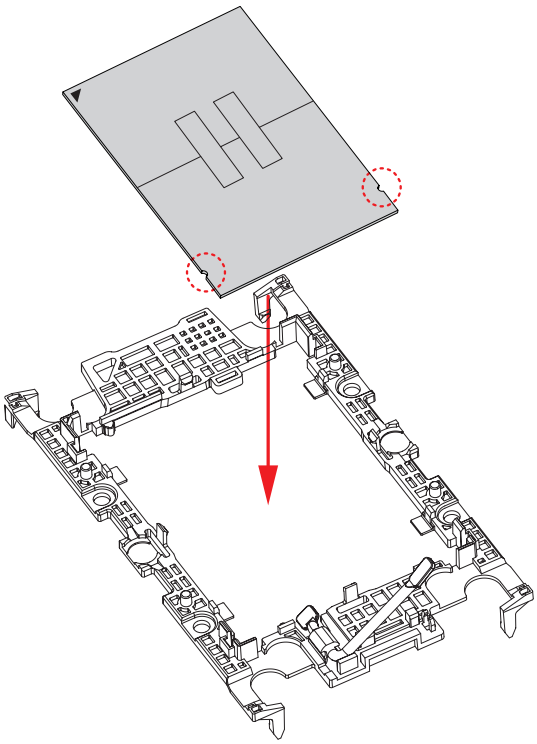


② Release the handle on the CPU carrier.

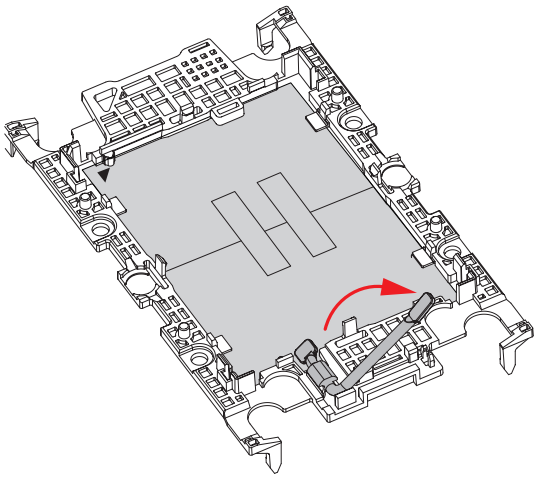


③ Insert the CPU into the CPU carrier. Carefully align and insert on side of the CPU and then the other.

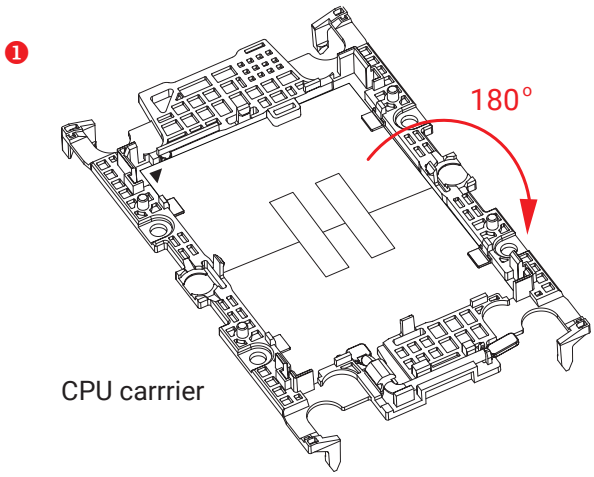
> **NOTE**
> Must ensure to match the direction and the notch of the CPU with the carrier.

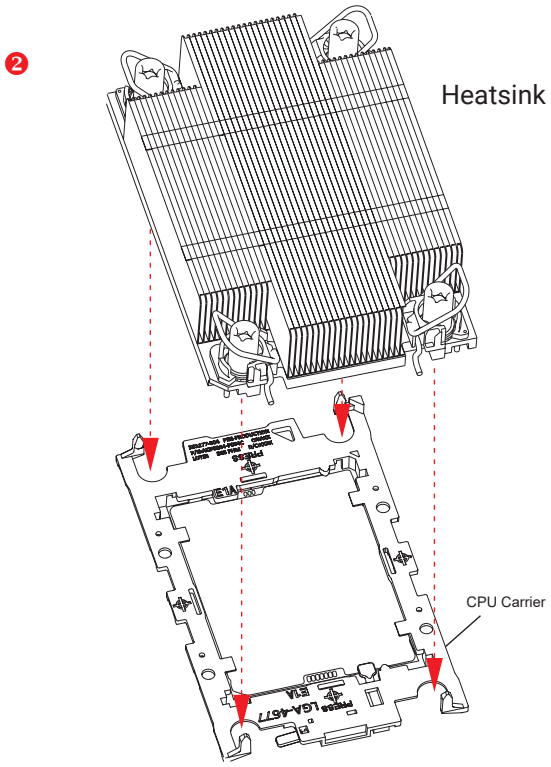


④ Close the handle after inserting the CPU.



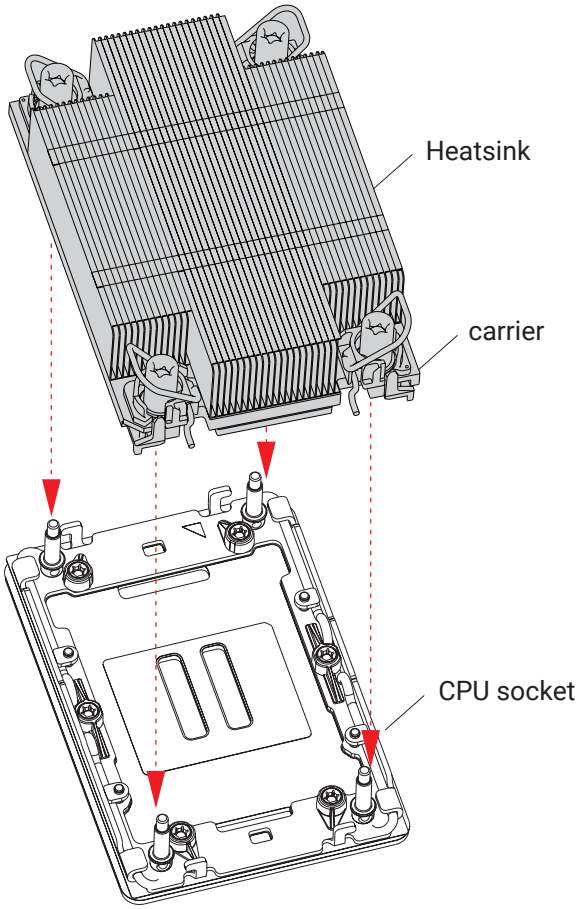
⑤ Reverse the CPU carrier to 180 degrees and attach the heat sink onto the CPU carrier with the Syringe thermal paste.



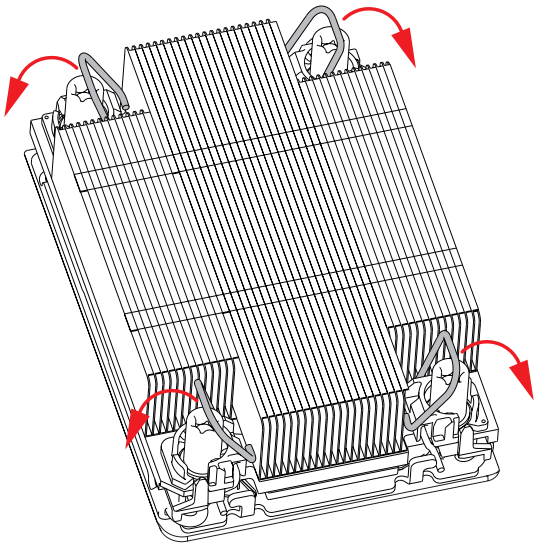


⑥ Install the assembled heatsink and CPU carrier onto the CPU socket.

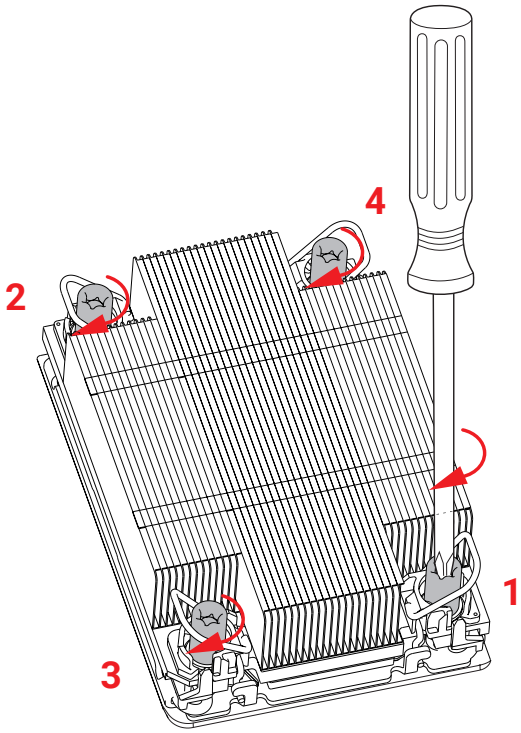
CAUTION
Failure to tighten the heat sink screws in the specified order may cause damage to the processor socket assembly. Heat sink screws is recommended to be tightened to 8 in-lbs torque, but can be tightened to 12 in-lbs torque according to the indicated order on the top of the heatsink label.



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

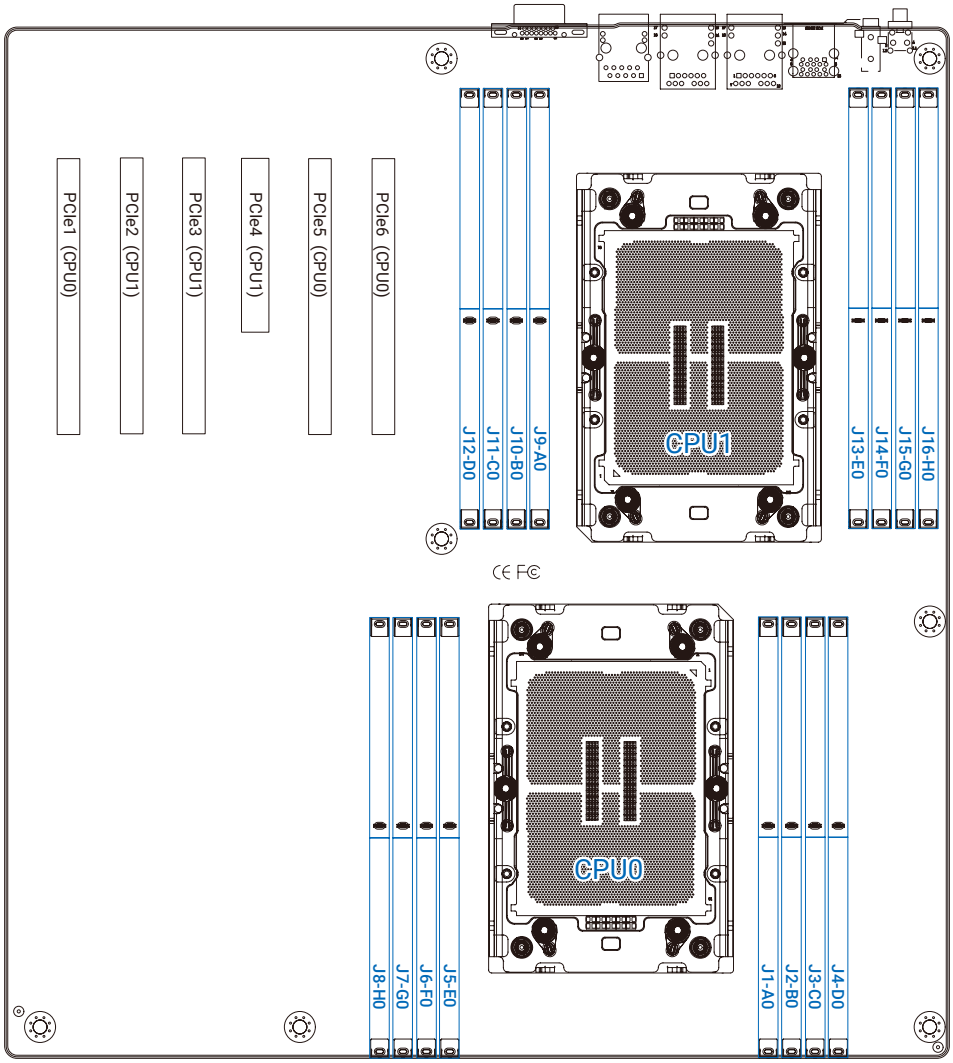
2.2.1 Placement

The DIMMs are displayed on the Vega board as J1/J2/J3/J4/J5/J6/J7/J8/J9/J10/J11/J12/J13/J14/J15/J16

To ensure satisfactory performance, you need to:

☑ Verify the DIMM type:
This product supports DDR5 RDIMM/LRDIMM

☑ 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 DDR5 DIMM Support

- 8 channel DDR5 with ECC up to 4800MT/s (Sapphire Rapids 1DPC)
- 8 channel DDR5 with ECC up to 5600MT/s (Emerald Rapids 1DPC)

Type	Ranks Per DIMM and Data Width	DRAM Density & DIMM Capacity			Max Operating Speed (MT/s) ; Voltage (V); DIMM Per Channel (DPC)
		16Gb	24Gb	32Gb	1.1V
RDIMM	SRx8 (RC D)	16Gb	24Gb	NA	4800 (SPR, 1DPC) 5600 (EMR, 1DPC)
	SRx4 (RC C)	32GB	48GB	NA	
	SRx4 (RC F) 9x4	32GB	NA	NA	
	DRx8 (RC E)	32GB	48GB	NA	
	DRx4 (RC A)	64GB	96GB	128GB	
	DRx4(RC B) 9x4	64GB	NA	NA	
Supported DIMM generations		DDR5-4800, DDR5-5600	DDR5-4800, DDR5-5600	DDR5-5600	

2.2.3 DIMM Population guide

For SPR and EMR, there should be at least one DDR5 DIMM per socket.DDR config does not have to be these same on all sockets in a system,but it requires at least one DIMM.

DIMM	Population	SPR 16Gb/32Gb DDR5	EMR 16Gb/32Gb DDR5	EMR 24Gb DDR5	SPR 24Gb DDR5
1	A0	POR	POR	POR	NOT POR
	B0	POR	POR	POR	NOT POR
	E0	POR	POR	POR	NOT POR
	F0	POR	POR	POR	NOT POR
2	A0, G0	POR	POR	NOT POR	NOT POR
	C0, E0	POR	POR	NOT POR	NOT POR
4	A0, C0, E0, G0	POR	POR	NOT POR	NOT POR
6	A0, C0, D0, E0, F0, G0	POR	POR	POR	NOT POR
	A0, B0, C0, E0, G0, H0	POR	POR	POR	NOT POR
	B0, C0, D0, E0, F0, H0	POR	POR	POR	NOT POR
	A0, B0, D0, F0, G0, H0	POR	POR	POR	NOT POR
8	A0, B0, C0, D0, E0, F0, G0, H0	POR	POR	POR	POR

POR (Plan of Record): An IC (integrated circuit) manufacturer's chip will have technical specifications that define its functionalities. The POR refers to whether these functionalities are planned to be supported.

2.2.4 DIMM Mixing Rules

1. All DIMMs must be DDR5 DIMMs.
2. All DIMMs in a Processor socket must have the same number of ranks.
3. x8 DIMMs and x4 DIMMs can not be mixed in the same channel orsame Processor socket.
4. Mixing of non-3DS and 3DS RDIMMs is not allowed in the samechannel, across different channels, and across different sockets.
5. Density mixing is not allowed.
6. 16 Gb configurations on each socket with the following considerations:
   - -Mixing 3DS and non-3DS on a platform is not allowed
   - -Density mixing is not allowed.
   - -Starting configurations with 24 Gb require the same memoryconfiguration on all sockets (validation limitation). Failovers can failto non-socket symmetric configurations.
7. 9x4 RDIMMs can not be mixed with non 9x4 RDIMMs.
8. All DDR5 DIMMs will be set to the speed of the lowest DIMM.
9. Mixing of DDR5 operating frequencies is not validated within a socketor across sockets by Intel. When DIMMs with different maximumfrequencies are mixed in the same channel or across different channelsacross Processor sockets, BIOS will determine and set the DIMM speedto the highest common frequency across all channels on the platform.For example, if a 4000 MT/s max frequency DIMM is installed in onechannel and a 4400 MT/s max frequency DIMM in another, BIOS setsthe platform speed to 4000 MT/s.

DIMM Mixing support clarifications

Mixing support	Across channels (1DPC)
Vendor Mixing (Same DIMM speed rating)	Supported
DDR5-4800 w/ DDR5-5600*	Supported **
RDIMM x4 w/ x8	Not Supported
3DS RDIMM / RDIMM	Not Supported
Rank Mixing: 16 DIMM only	Not Supported
DRAM Density 16Gb/24Gb/32Gb	Not Supported

* DDR5 4800 and DDR5600 mixing doesn't allow in the same channel whether these DIMMs are from the same memory vendors or different memory vendors.

** Mixing support is across channels.

2.2.5 Mapping Table

MB Location	Description	PCB silkscreen
JCPU0	Legacy CPU	CPU0
JCPU1	Non-Legacy CPU	CPU1
J1	CPU0 Channel A DIMM0	A0
J2	CPU0 Channel B DIMM0	B0
J3	CPU0 Channel C DIMM0	C0
J4	CPU0 Channel D DIMM0	D0
J5	CPU0 Channel E DIMM0	E0
J6	CPU0 Channel F DIMM0	F0
J7	CPU0 Channel G DIMM0	G0
J8	CPU0 Channel H DIMM0	H0
J9	CPU1 Channel A DIMM0	A0
J10	CPU1 Channel B DIMM0	B0
J11	CPU1 Channel C DIMM0	C0
J12	CPU1 Channel D DIMM0	D0
J13	CPU1 Channel E DIMM0	E0
J14	CPU1 Channel F DIMM0	F0
J15	CPU1 Channel G DIMM0	G0
J16	CPU1 Channel H DIMM0	H0
PCIE1	CPU0 PE2 Lane 0-15	PCIE SLOT 1 (CPU0)
PCIE2	CPU1 PE0 Lane 0-15	PCIE SLOT 3 (CPU1)
PCIE3	CPU1 PE1 Lane 0-15	PCIE SLOT 2 (CPU1)
PCIE4	CPU0 PE1 Lane 0-15	PCIE SLOT 5 (CPU0)
PCIE5	CPU1 PE4 Lane 0-7 (Lane reversal)	PCIE SLOT 4 (CPU1)
PCIE6	CPU0 PE0 Lane 0-15	PCIE SLOT 6 (CPU0)

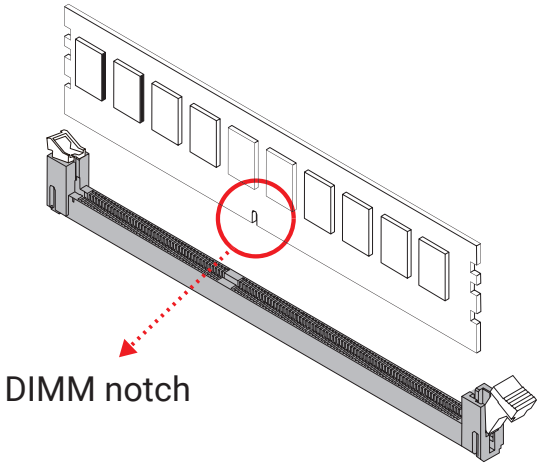
Mapping table of Port Number in Sapphire Rapids XCC and MCC

BIOS Menu	Core Count (XCC&MCC) Socket Ports	BIOS Menu - IIO
PCIE SLOT 1	CPU0-PE2	(CPU0)- IIO PCIe Port3
PCIE SLOT 2	CPU1-PE1	(CPU1)- IIO PCIe Port2
PCIE SLOT 3	CPU1-PE0	(CPU1)- IIO PCIe Port1
PCIE SLOT 4	CPU1-PE4	(CPU1)- IIO PCIe Port5
PCIE SLOT 5	CPU0-PE1	(CPU0)- IIO PCIe Port2
PCIE SLOT 6	CPU0-PE0	(CPU0)- IIO PCIe Port1

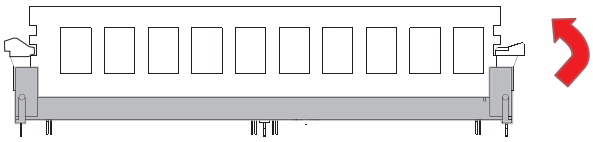
2.2.6 Installation

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

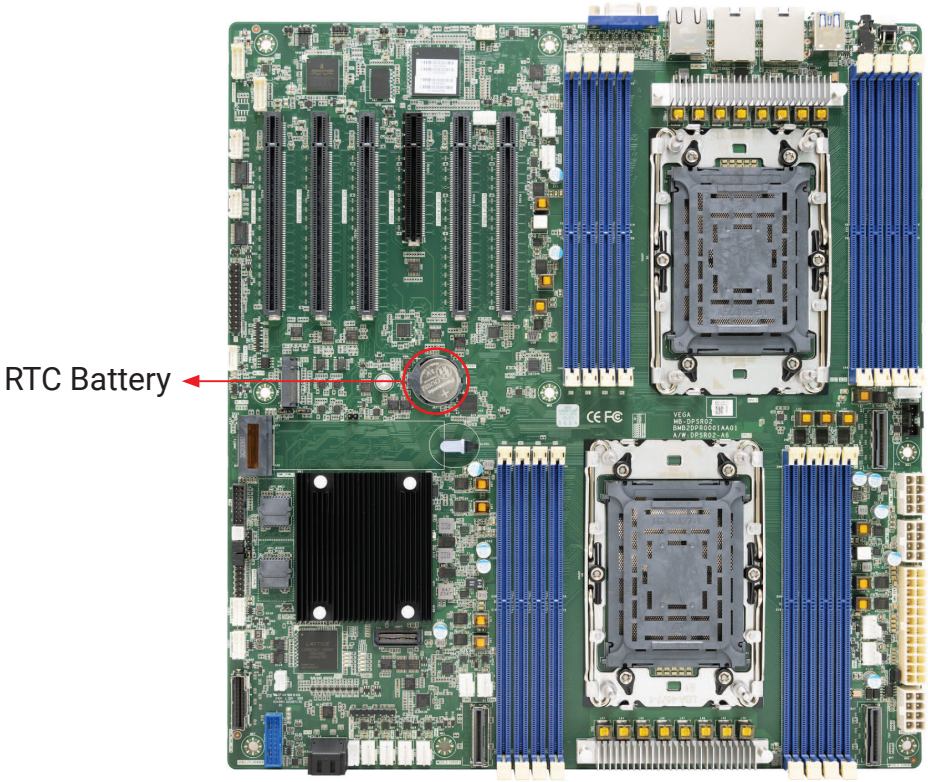
Step 2 Insert the memory module into the slot. Make sure that the DIMM notch is accurately positioned.



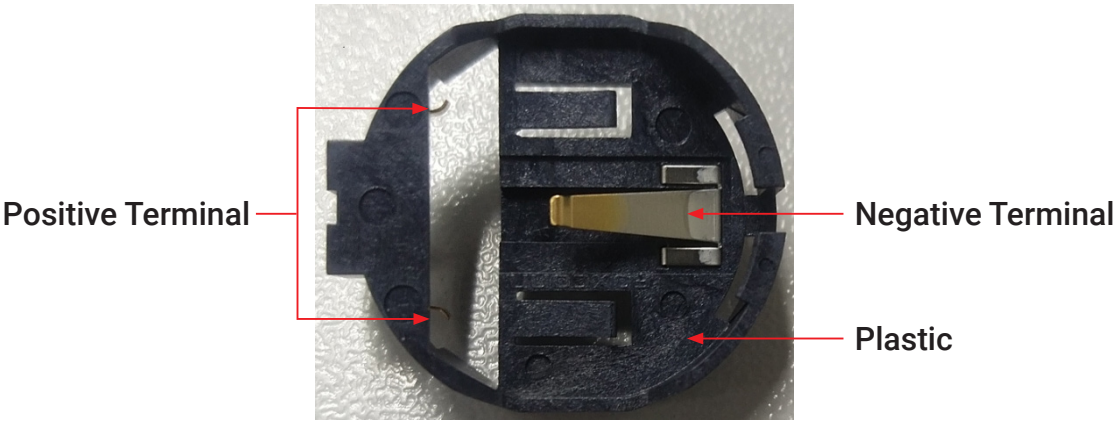
Step 3 Close the retaining clip to complete installation.



2.3 RTC (Real Time Clock) Battery



2.3.1 Component Composition



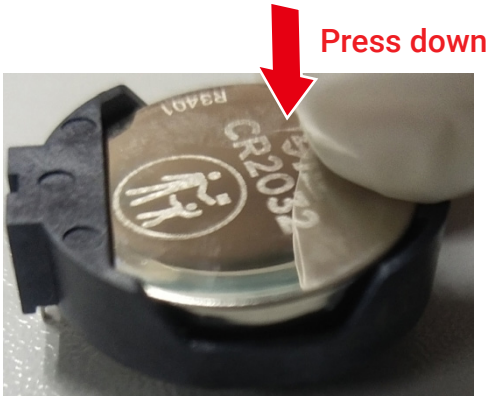
Battery Positive Electrode

Battery Negative Electrode

2.3.2 Installation Guide

① The battery should be positive side up and inserted from the negative terminal end of the battery holder.

② Press the edge of the battery at the negative terminal end of the battery holder to push the battery into the holder.

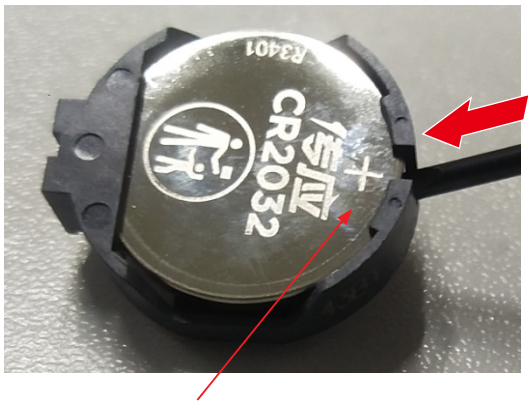


③ Complete the installation.

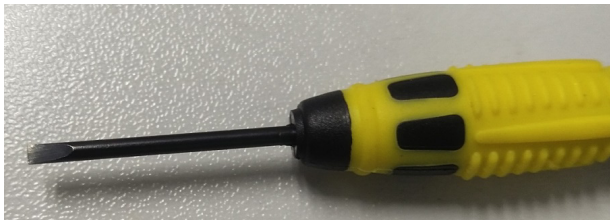
NOTE
Operators must wear anti-static gloves and an anti-static wrist strap during operation.

2.3.3 Removal Guide

① Use a 2.0mm flathead screwdriver and insert it snugly against the battery from the slot at the negative terminal end.



Negative Terminal



2.0mm Flathead Screwdriver

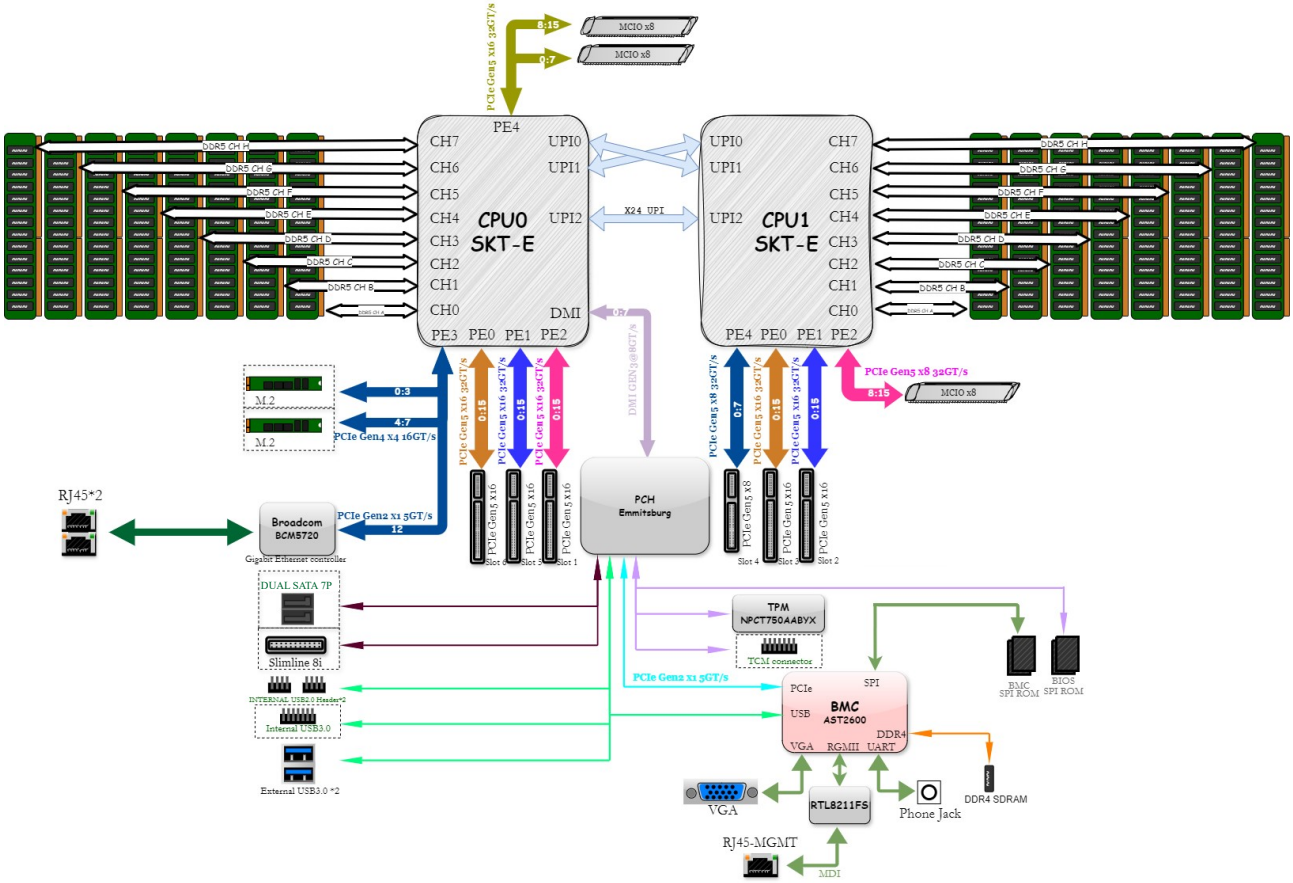
② Then, pry the battery backward and the battery will automatically pop out.

NOTE
Operators must wear anti-static gloves and an anti-static wrist strap during operation.

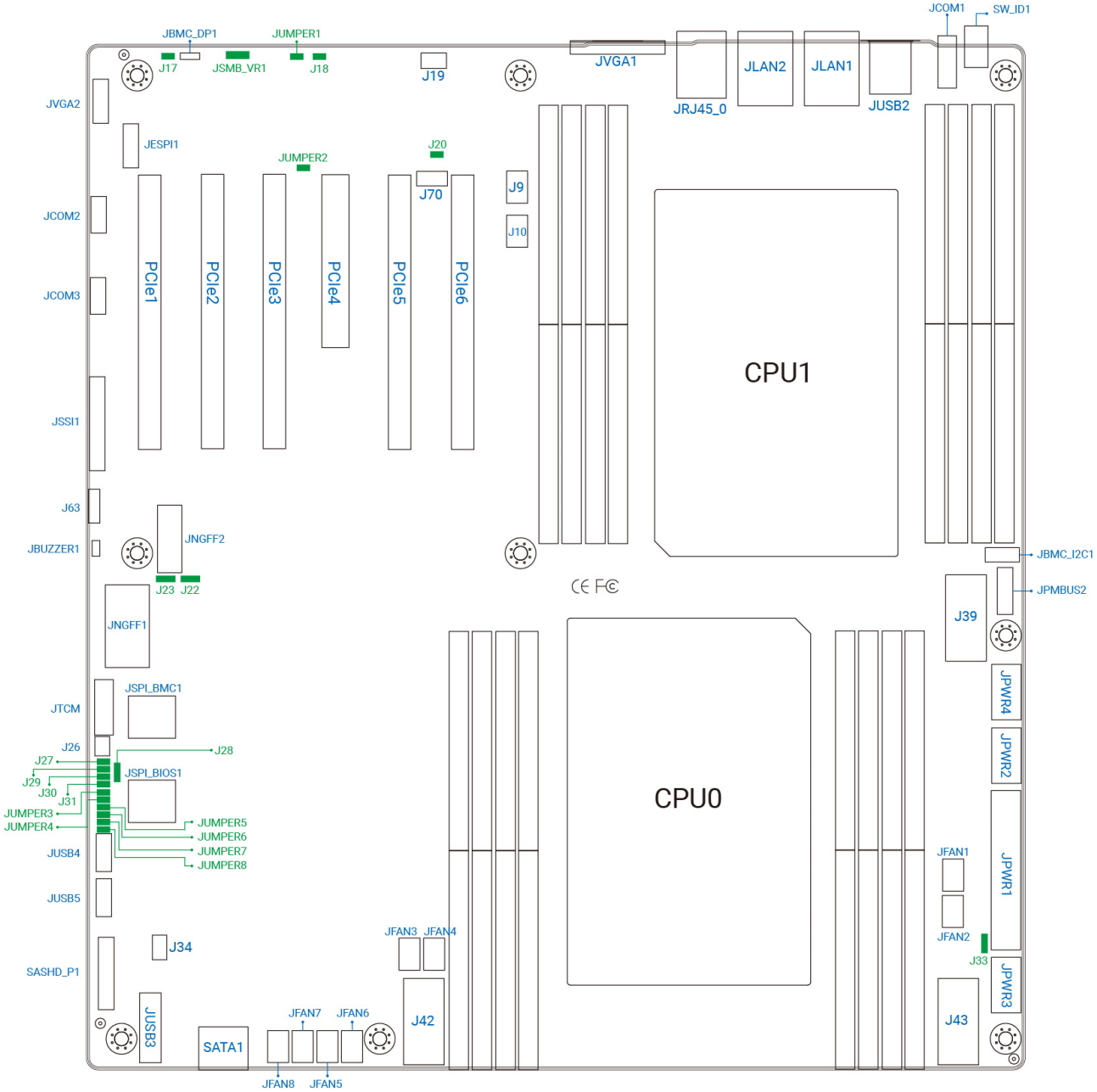
Chapter 3. Motherboard Settings

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

3.1 Block Diagram



3.2 Placement



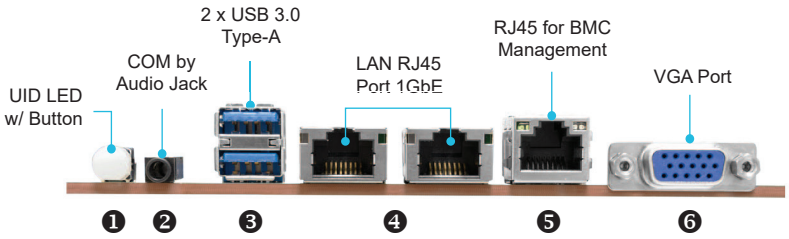
3.3 Content List

Connector	Description	Location
Power CONN	4 x 2 Pin ATX CONN	JPWR2, JPWR3, JPWR4: 12V
Power CONN	12 x 2 Pin ATX CONN	PWR1: 12V, 5V, 3.3V, 5VSB
CPU	SPR-LGA4677	U4, U5
Front Panel	2 x 12 Pin 2.54mm Box Header	JSSI1
Front USB3.0	10 x 2 Pin 2.0mm Box Header	JUSB3
Front USB2.0	5 x 2 Pin 2.0mm Box Header	JUSB4, JUSB5
PCIe Gen5	MCIO X8 CONN	J42, J43, J39
Serial ATA	Slimline X8 CONN	SASHD_P1
Dual Serial ATA	2 x 7 Pin 1.27 mm CONN	SATA1
VGA	2 x 8 Pin 2.0mm Box Header	JVGA2
COM1	2 x 5 Pin 2.0mm Box Header	JCOM3
COM2	2 x 5 Pin 2.0mm Box Header	JCOM2
Intruder	2 Pin 2.0mm Box Header	J26
BMC GPIO	2 x 3 Pin 2.0mm Box Header	J19
BMC IPMB	4 Pin 2.0mm Box Header	J70
M.2 2280	GEN4_M2_KEY_M_H=10.85MM (stack type)	JNGFF1
eSPI Debug Port	2 x 6 Pin 2.0mm Box Header	
XDP CONN	Samtec QSH 60-Pin CONN	JXDP1
TCM CONN	2 x 8 Pin 2.0mm Box Header	JTCM
Battery Socket	2 Pin Socket	BAT1
Clear CMOS	2 Pin 2.54mm Header	JUMPER6
DIMM Sockets	288 Pin DDR5 DIMM	JEDEC Specified DDR5 Connector: J1~16
BMC Debug Port	3 x 1 Pin 2.0mm Header	JBMC_DP1
BIOS SPI ROM Socket	SOIC-16 Socket	JSPI_BIOS1
BMC SPI ROM Socket	SOIC-16 Socket	JSPI_BMC1
BMC Reset	2 x 1 Pin 2.00mm Header	J20
BMC Buzzer	2 x 1 Pin 2.00mm Header	JBUZZER1
BMC Socflash Enable	2 x 1 Pin 2.00mm Header	JUMPER2
VROC Key	4 x 1 Pin 2.0mm Box Header	J63
FAN CONN	4 x 1 Pin 2.54mm Box Header	JFAN1~JFAN10
PMBUS Power Select	3 x 1 Pin 2.0mm Header	J33
BMC Bypass	3 x 1 Pin 2.0mm Header	J28
PCH Bypass	3 x 1 Pin 2.0mm Header	J22, J23
BMC RST Password	2 x 1 Pin 2.0mm Header	J17
BMC Disable	2 x 1 Pin 2.0mm Header	J18
VRM SMB	3 x 1 Pin 2.54mm Header	JSMB_VR1
Program CPLD FW	8 x 1 Pin 2.54mm Header	J35
BMC Reset	2 x 1 Pin 2.0mm Header	J20
BMC Debug Port	3 x 1 Pin 2.0mm Header	JBMC_DP1
BMC I2C	4 x 1 Pin 1.25mm Header	JBMC_I2C1
SGPIO	3 x 1 Pin 2.0 mm Header	J34

External Connectors (rear panel)

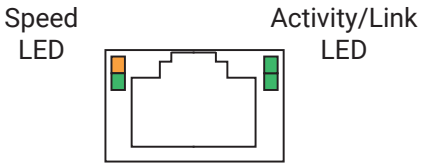
Connector	Description	Comments
Ethernet x2	RJ45	JLAN1, JLAN_2, 10/100/1000M NIC (BCM5720)
VGA	DSUB 15 Pin Blue Female	JVGA1
USB3.0 x2	USB3.0 Type A	JUSB2
Ethernet x1	RJ45	JRJ45_0, 10/100/1000M PHYRECEIVER (RTL8211FS)
SERIAL PORT	Phone Jack	JCOM1
ID LED	Button	SW_ID1

3.4 External Port



	Item
1	UID LED with Button
2	COM by Audio Jack (Baud rate 115200 bit/s)
3	2 x USB 3.0 Type-A
4	LAN RJ45 Port 1GbE
5	RJ45 for BMC management
6	VGA Port

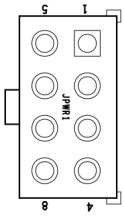
LAN LED Indicator



Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.

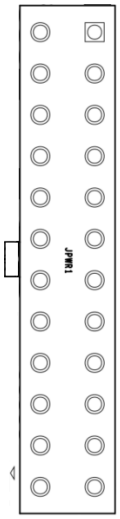
3.5 Connector Definition

Power Connector (JPWR2, JPWR3, JPWR4)
The main connector shall be 4pinx2, 12Pinx2 connector to support HDD BP, SATA BP, CEM.



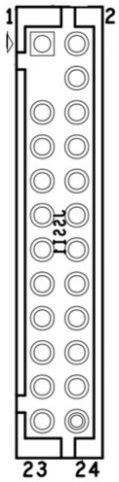
P12V_PSU	5	1	GND
P12V_PSU	6	2	GND
P12V_PSU	7	3	GND
P12V_PSU	8	4	GND

Power Connector (JPWR1)



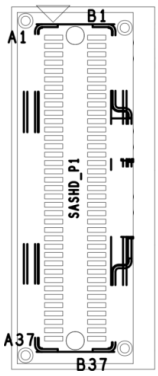
P3V3_PSU	13	1	P3V3_PSU
NC	14	2	P3V3_PSU
GND	15	3	GND
PSU_PSON_ BUF_N	16	4	P5V_PSU
GND	17	5	GND
GND	18	6	P5V_PSU
GND	19	7	GND
NC	20	8	PSU_PWROK
P5V_PSU	21	9	P5V_STBY_PSU
P5V_PSU	22	10	P12V_PSU
P5V_PSU	23	11	P12V_PSU
GND	24	12	P3V3_PSU

LED/Bezel Button Header (JSSI1)
This connector is a 2 x 12 Pin header.



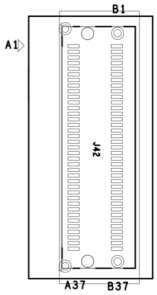
FP_HDR_PWR_LED	1	2	P3V3_DUAL
NC	3	4	P5V_STBY_PSU
FP_PWR_LED_L	5	6	ID_LED_OUT_N
HDD_LED_P	7	8	SYS_HEALTH2#
HDD_LED_N	9	10	SYS_HEALTH#
FP_PWR_BTN_N	11	12	LAN1_ACTLED_PWR
GND	13	14	LAN1_ACTLED_N
FP_RST_BTN_N	15	16	I2C_FRONT_SDA_R
GND	17	18	I2C_FRONT_SCL_R
BMC_ID_IN_N	19	20	CHASSIS_OPEN
P3V3_DUAL	21	22	LAN2_ACTLED_PWR
FP_NMI_BTN_N	23	24	LAN2_ACTLED_N

Power Connector (JPWR2, JPWR3, JPWR4)
The main connector shall be 4pinx2, 12Pinx2 connector to support HDD BP, SATA BP, CEM.



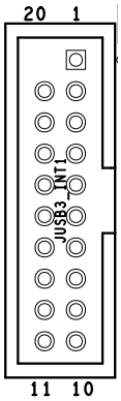
GND	A1	B1	GND
SATA_RXP_0_C	A2	B2	SATA_TXP_0_C
SATA_RXN_0_C	A3	B3	SATA_TXN_0_C
GND	A4	B4	GND
SATA_RXP_1_C	A5	B5	SATA_TXP_1_C
SATA_RXN_1_C	A6	B6	SATA_TXN_1_C
GND	A7	B7	GND
NC	A8	B8	SGPIO_SATA1_CLOCK_CONN
NC	A9	B9	SGPIO_SATA1_LOAD_CONN
NC	A10	B10	NC
NC	A11	B11	SGPIO_SATA1_DATA_CONN
NC	A12	B12	NC
GND	A13	B13	GND
SATA_RXP_2_C	A14	B14	SATA_TXP_2_C
SATA_RXN_2_C	A15	B15	SATA_TXN_2_C
GND	A16	B16	GND
SATA_RXP_3_C	A17	B17	SATA_TXP_3_C
SATA_RXN_3_C	A18	B18	SATA_TXN_3_C
GND	A19	B19	GND
SATA_RXP_4_C	A20	B20	SATA_TXP_4_C
SATA_RXN_4_C	A21	B21	SATA_TXN_4_C
GND	A22	B22	GND
SATA_RXP_5_C	A23	B23	SATA_TXP_5_C
SATA_RXN_5_C	A24	B24	SATA_TXN_5_C
GND	A25	B25	GND
NC	A26	B26	NC
NC	A27	B27	NC
NC	A28	B28	NC
NC	A29	B29	NC
NC	A30	B30	NC
GND	A31	B31	GND
SATA_RXP_6_C	A32	B32	SATA_TXP_6_C
SATA_RXN_6_C	A33	B33	SATA_TXN_6_C
GND	A34	B34	GND
SATA_RXP_7_C	A35	B35	SATA_TXP_7_C
SATA_RXN_7_C	A36	B36	SATA_TXN_7_C
GND	A37	B37	GND

MCIO CONN Pin Description (J39, J42, J43)
This connector is a 74 Pin connector.



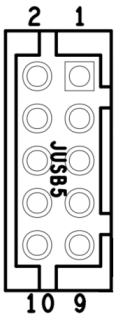
GND	B1	A1	GND
CPU0_PCIEx_TX_DP_x	B2	A2	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B3	A3	CPU0_PCIEx_RX_DN_x
GND	B4	A4	GND
CPU0_PCIEx_TX_DP_x	B5	A5	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B6	A6	CPU0_PCIEx_RX_DN_x
GND	B7	A7	GND
I2C_CPUx_MCIOx_SCL	B8	A8	CPU0_MCIOx_BP_TYPE_R
I2C_CPUx_MCIOx_SDA	B9	A9	CPU0_MCIOx_SMB_ALERT_N
GND	B10	A10	GND
RST_CPUx_MCIOx_PERST_R_N	B11	A11	CLK_100M_CPUx_MCIOx_x_DP
CPUx_MCIOx_PRSNT_R_N	B12	A12	CLK_100M_CPUx_MCIOx_x_DN
GND	B13	A13	GND
CPU0_PCIEx_TX_DP_x	B14	A14	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B15	A15	CPU0_PCIEx_RX_DN_x
GND	B16	A16	GND
CPU0_PCIEx_TX_DP_x	B17	A17	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B18	A18	CPU0_PCIEx_RX_DN_x
GND	B19	A19	GND
CPU0_PCIEx_TX_DP_x	B20	A20	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B21	A21	CPU0_PCIEx_RX_DN_x
GND	B22	A22	GND
CPU0_PCIEx_TX_DP_x	B23	A23	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B24	A24	CPU0_PCIEx_RX_DN_x
GND	B25	A25	GND
I2C_CPUx_MCIOx_SCL	B26	A26	CPU0_MCIOx_BP_TYPE_R
I2C_CPUx_MCIOx_SDA	B27	A27	CPU0_MCIOx_SMB_ALERT_N
GND	B28	A28	GND
RST_CPUx_MCIOx_PERST_R_N	B29	A29	CLK_100M_CPUx_MCIOx_x_DP
CPUx_MCIOx_PRSNT_R_N	B30	A30	CLK_100M_CPUx_MCIOx_x_DN
GND	B31	A31	GND
CPU0_PCIEx_TX_DP_x	B32	A32	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B33	A33	CPU0_PCIEx_RX_DN_x
GND	B34	A34	GND
CPU0_PCIEx_TX_DP_x	B35	A35	CPU0_PCIEx_RX_DP_x
CPU0_PCIEx_TX_DN_x	B36	A36	CPU0_PCIEx_RX_DN_x
GND	B37	A37	GND

Front I/O USB Header (JUSB3)
This is a 19-pin header that used to provide front I/O USB functionality.



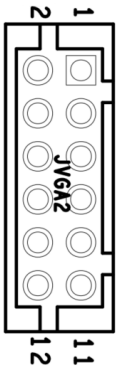
		1	P5V_USB23
P5V_USB23	19	2	USB3_CONTROLLER_RX_R_DP3
USB3_CONTROLLER_RX_R_DP2	18	3	USB3_CONTROLLER_RX_R_DN3
USB3_CONTROLLER_RX_R_DN2	17	4	GND
GND	16	5	USB3_CONTROLLER_TX_R_DP3
USB3_CONTROLLER_TX_R_DP2	15	6	USB3_CONTROLLER_TX_R_DN3
USB3_CONTROLLER_TX_R_DN2	14	7	GND
GND	13	8	USB2_CONTROLLER_R_DN3
USB2_CONTROLLER_R_DN2	12	9	USB2_CONTROLLER_R_DP3
USB2_CONTROLLER_R_DP2	11	10	USB_CONTROLLER_OCI23_N

USB2.0 Header (JUSB4, JUSB5)
This is a 2x5-pin header that used to provide front USB2.0 functionality.



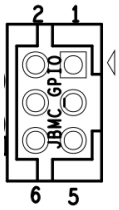
P5V_USBx	2	1	P5V_USBx
PCH_FP_USB2_N_x	4	3	PCH_FP_USB2_N_x
PCH_FP_USB2_P_x	6	5	PCH_FP_USB2_P_x
GND	8	7	GND
GND	10	9	USB_CONTROLLER_OCIx_N

Front VGA Header (JVGA2)
This is a 2x6-pin header that used to provide front VGA functionality.



GND	2	1	DVO_5V
DACROA	4	3	GND
GND	6	5	DDC_DATAO
DACGOA	8	7	AVSYNCO
GND	10	9	AHSYNCO
DACBOA	12	11	DDC_CLKO

BMC GPIO Header (J19)
This connector is a 2x3-pin header.

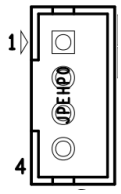


RACK_EXTRST_R_N	2	1	GND
BMC_GPY1	4	3	I2C_G16_SDA_R
BMC_GPY0	6	5	I2C_G16_SCL_R

FAN Header (JFAN1~JFAN10)
This is a 4-pin fan header.

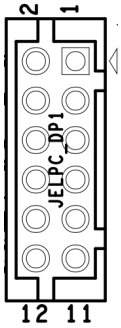
1	GND
2	P12V_FANx
3	FANx_TACH
4	FANx_PWM_R

PCIe Hot-Plug Header (JPEHP0, JPEHP1)
This is a 1x4-pin header that used to provide PCIe Hot-Plug functionality.



1	I2C_CPUx_PE_HP_SCL
2	I2C_CPUx_PE_HP_SDA
3	GND
4	I2C_CPUx_PE_HP_ALERT_R_N

IPMB Header (JESPI1)
This is a 2x6-pin header that used to provide eSPI Debug Port functionality.

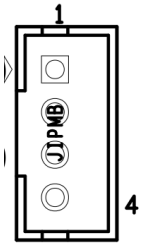


ESPI_DBP_CLK	2	1	GND
ESPI_DBP_CS_N	4	3	NC
ESPI_DBP_RST_N	6	5	ESPI_DBP_ALERT_N
ESPI_DBP_D3	8	7	ESPI_DBP_D2
P3V3_DUAL	10	9	ESPI_DBP_D1
ESPI_DBP_D0	12	11	GND

VROC KEY Box Header (J63)
This is a 1x4-pin header that used to provide VROC KEY functionality.

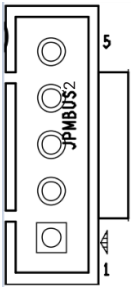
1	GND
2	PU_KEY_CONN_KEY2
3	GND
4	PCH_SATA_RAID_KEY_R

BMC IPMB BOX Header (J70)
This is a 1x4-pin header that used to provide BMC I2C14 IPMB functionality.



1	I2C_G14_SDA_R
2	GND
3	I2C_G14_SCL_R
4	NC

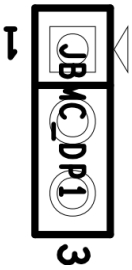
PMBUS Box Header (JPMBUS2)
This is a 1x5-pin header that used to provide PMBus functionality.



1	SMB_PMBUS_SCL
2	SMB_PMBUS_SDA
3	PMBUS_ALERT_N_C
4	GND
5	P5V_P3V3_STBY

NOTE
For pin5: It's a choosable power source according to J33.

BMC Debug port Header (JBMC_DP1)
This is a 1x3-pin header that used to provide BMC Debug port functionality.

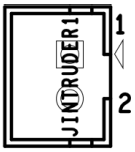


1	SPE_TXD
2	GND
3	SPE_RXD

BUZZER Header (JBUZZER1)
This is a 1x2-pin header that used to provide Buzzer functionality.

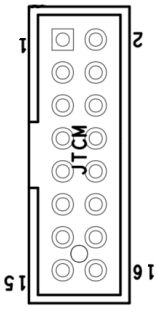
1	P5V_PSU
2	BMC_BUZZER

Chassis Intrusion Header (J26)
This is a 1x2-pin header that used to provide chassis intrusion functionality.



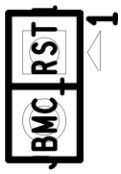
1	CHASSIS_OPEN
2	GND

Trusted Cryptographic Module Header (JTCM)
This is a 2x8-pin header.



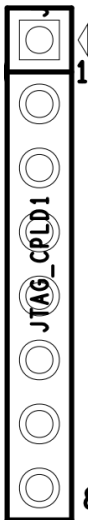
P3V3_DUAL	1	2	GND
P3V3_DUAL	3	4	PCH_SPI_IRQ_R_N
TPM_CONN_RST_N	5	6	SPI_TCM_CS_R_N
TPM_CONN_SPI_CLK	7	8	GND
GND	9	10	TPM_CONN_SPI_MISO
TPM_CONN_SPI_MOSI	11	12	HOST_TCM_PRSNT_R_N
MODULE_PRSNT_R_N	13	14	NC
HOST_TCM_PP_BUF	15	16	NC

BMC RESET Header (J20)
This is a 1x2-pin header that used to provide BMC RESET functionality.



1	BMC_RESET
2	GND

CPLD JTAG Header (J35)
This is a 1x8-pin header that used to provide CPLD JTAG functionality.

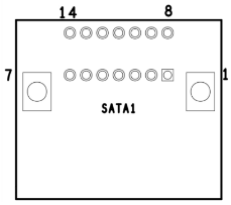


1	P3V3_DUAL
2	JTAG_CPLD_TDO
3	JTAG_CPLD_TDI
4	JTAG_HDR_PRSNT_N
5	NC
6	JTAG_CPLD_TMS
7	GND
8	JTAG_CPLD_TCK

VRM SMB Header (JSMB_VR1)
This is a 1x3-pin header that used to provide VRM SMB functionality.

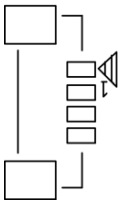
1	I2C_BMC_6_VR_CPU_SCL
2	GND
3	I2C_BMC_6_VR_CPU_SDA

Dual port SATA Connector (SATA1)
This connector is a 2x7-pin header.



GND	S1	S8	GND
SATA_TXP_DOM_0_C	S2	S9	SATA_TXP_DOM_1_C
SATA_TXN_DOM_0_C	S3	S10	SATA_TXN_DOM_1_C
GND	S4	S11	GND
SATA_RXN_DOM_0_C	S5	S12	SATA_RXN_DOM_1_C
SATA_RXP_DOM_0_C	S6	S13	SATA_RXP_DOM_1_C
GND	S7	S14	GND

BMC I2C Header (JBMC_I2C1)
This connector is a 1x4-pin header.



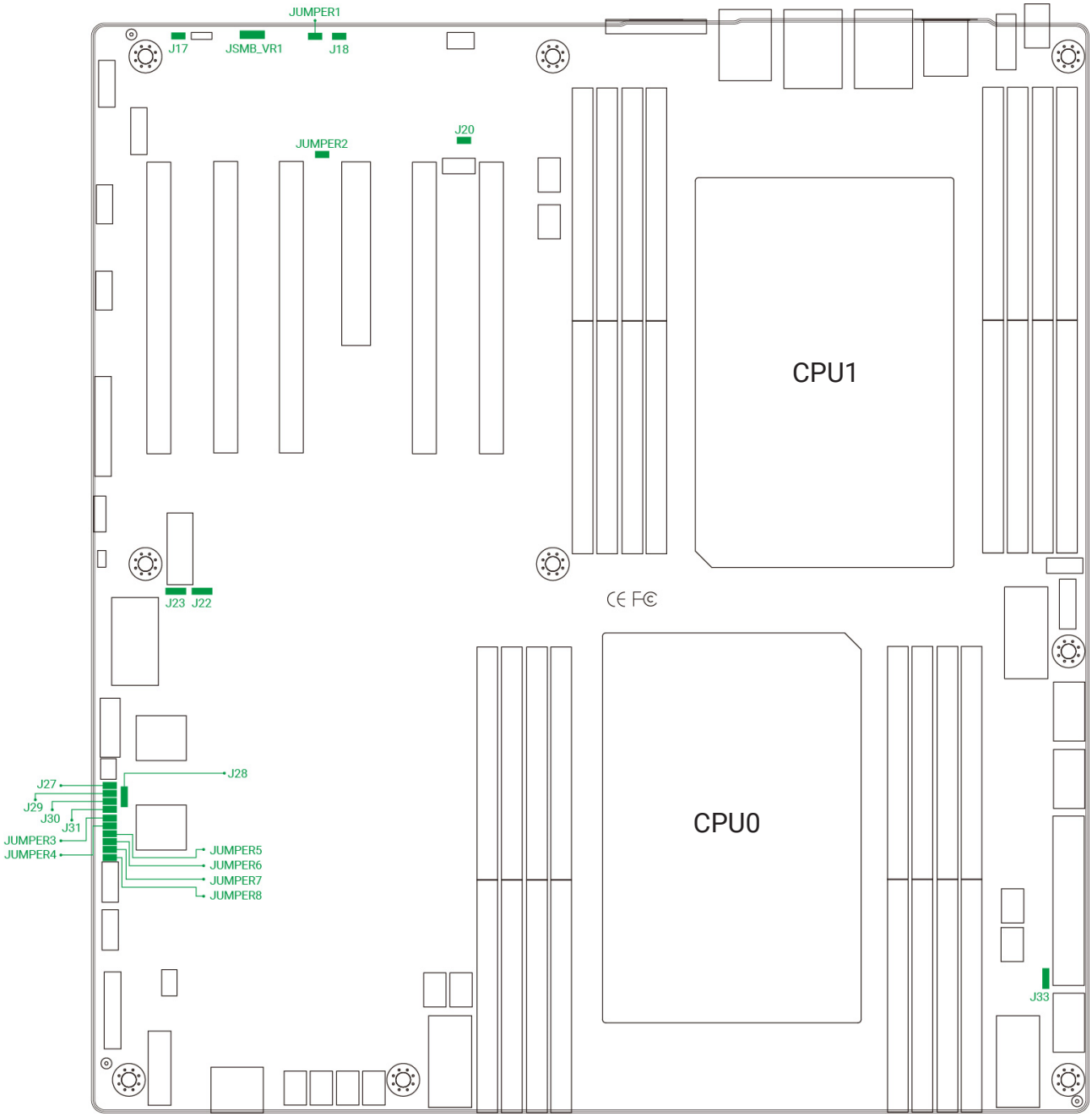
1	BMC_I2C_G8_SCL
2	BMC_I2C_G8_SDA
3	BP_BMC_I2C8_ALERT_N
4	GND

SGPIO Header (J34)
This connector is a 1x4-pin header.

1	SGPIO_SATA1_CLOCK_HDR
2	SGPIO_SATA1_LOAD_HDR
3	SGPIO_SATA1_DATA_HDR
4	GND

3.6 Jumper Definition

Location



CMOS Jumper (JUMPER6)

JUMPER6	Setting	
Short	Clear CMOS	
Open	Normal	Default

BMC Reset Jumper (J20)

J20	Setting	
Short	Reset BMC	
Open	Normal	Default

BMC Disable Jumper (J18)

J18	Setting	
Short	Reset BMC	
Open	Normal	Default

CPU SPI Flash Jumper (J22, J23)

J23	J22	Setting	
Pin1-2	Pin1-2	CPU to Flash Bypass	Default

BMC Reset Password Jumper (J17)

J17	Setting	
Short	Reset Password	
Open	Normal	Default

BMC Socflash Configurations Jumper (JUMPER2)

JUMPER2	Setting	
Short	Enable	
Open	Disable	Default

BMC SPI MUX Jumper (J28)

J28	Setting	
Pin2-3	BMC to Flash Bypass	Default

PMBUS Power select Jumper (J33)

J33	Setting	
Pin1-2	P3V3_DUAL	Default
Pin2-3	P5V_STBY_PSU	

3.7 LED

3.7.1 Rear Chassis LEDs

The NIC port/LED should be connected to Vaux (standby) voltage in order to provide the same functionality as stand-up NIC cards for WOL support.

Item		Color	Behavior
NIC 1 – JLAN1	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off
NIC 2 – JLAN2	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off
BMC Management – RJ45_0	Right	Green (Blinking)	BMC Management activity detected
		Off	BMC Management is not active, LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off

3.7.2 Internal LEDs

Item	Color	Behavior
HEART BEAT LED	Green (Blinking)	BMC activity detected
	Green (Off)	BMC is not active
CPLD_LED_MODE	Yellow / Off	Yellow: Port80 MODE, OFF: Sequence MODE
JNGFF1 ACTIVITY LED	Blue (Blinking)	JNGFF1 Upper activity detected
	Off	JNGFF1 Upper is not active
	Blue (Blinking)	JNGFF1 Lower activity detected
	Off	JNGFF1 Lower is not active

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

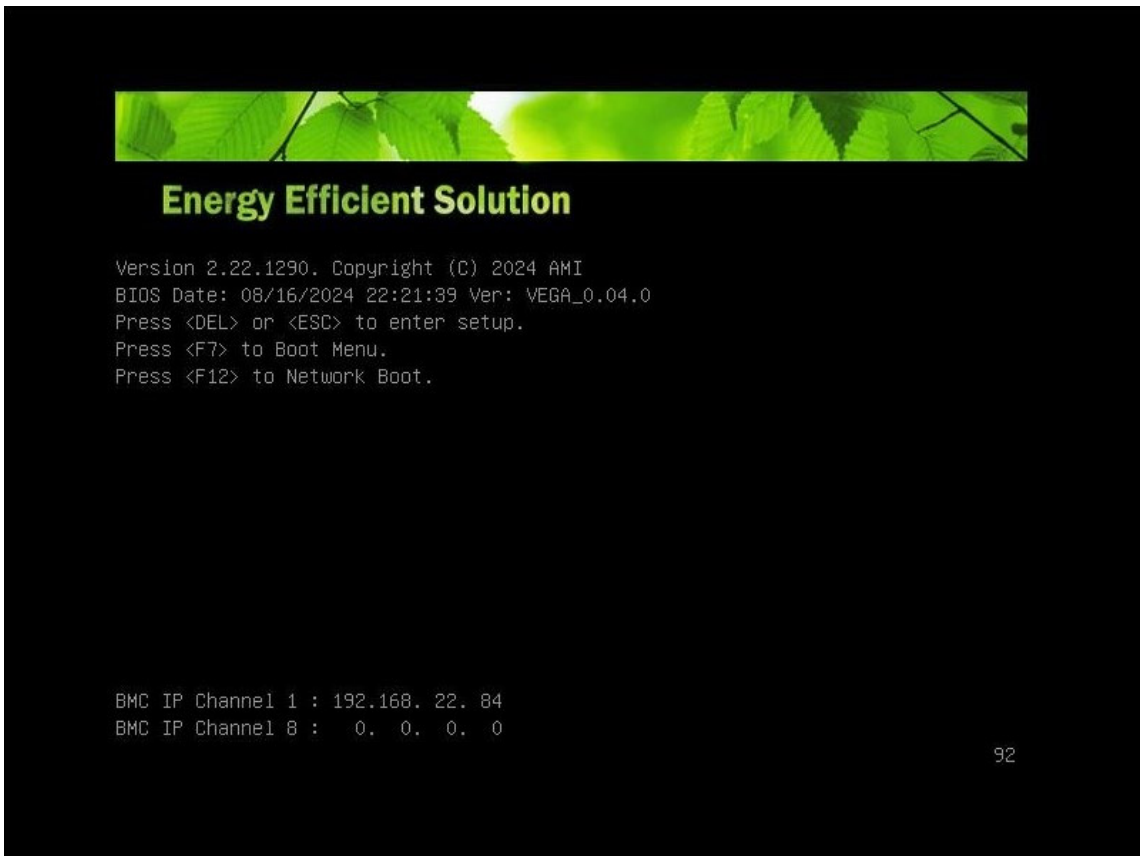
4.2.1 Menu

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

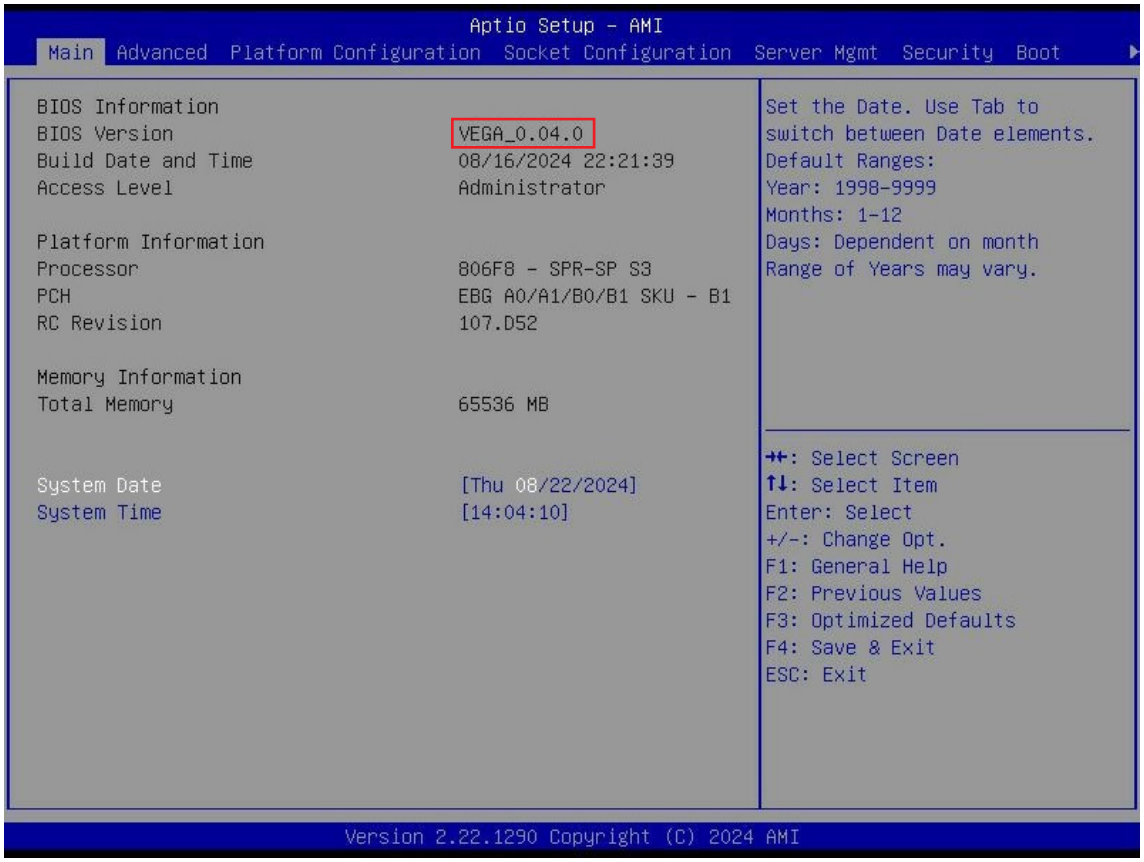
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Platform Configuration	Allows configuration of platform settings such as PCH, miscellaneous, and server ME configuration.
Socket Configuration	Allows configuration of socket 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.



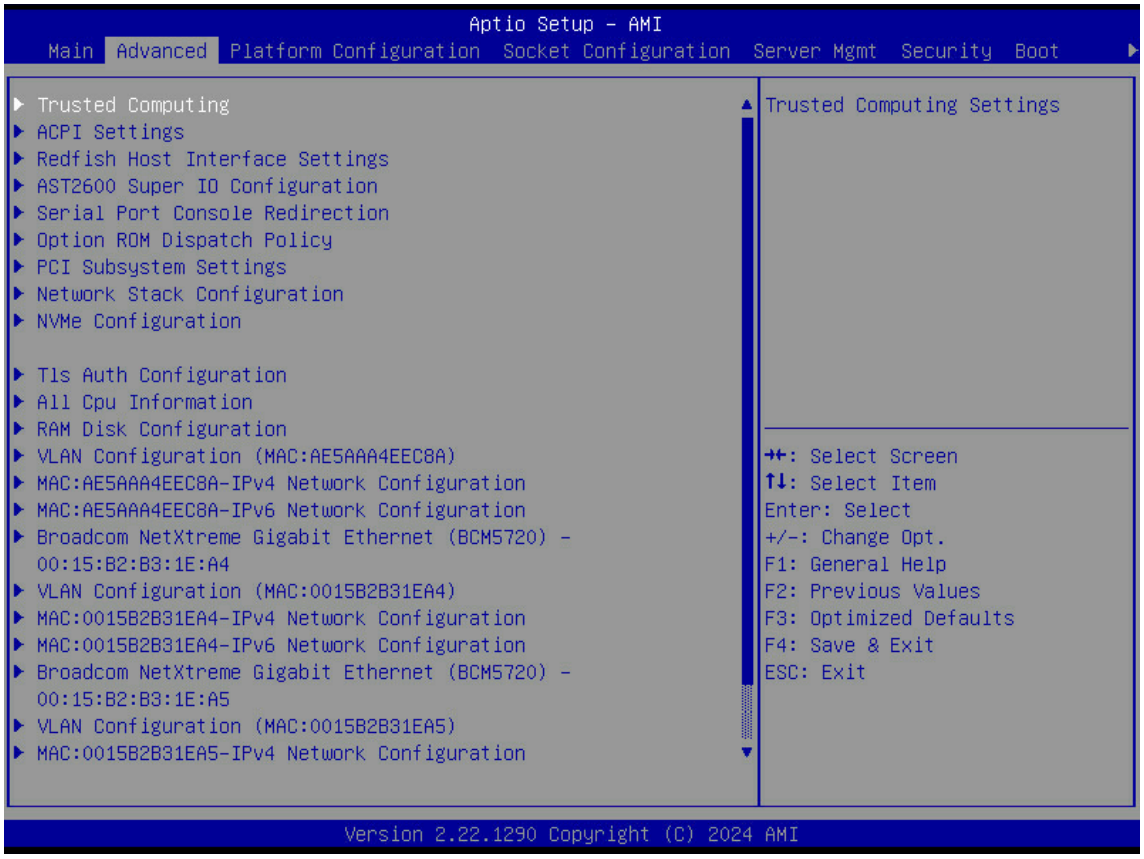
4.3 Main



4.3.1 Main

Main	
System Date	Configures the current date. Set the date. Use tab to switch between date elements.
System Time	Configures the current time. 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	
SHA256 PCR Bank	Enable or Disable SHA256 PCR Bank		
	▶Enable	Disable	
SHA384 PCR Bank	Enable or Disable SHA384 PCR Bank		
	Enable	▶Disable	
Pending operation	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.		
	▶None	TPM Clear	
Platform Hierarchy	Enable or Disable Platform Hierarchy		
	▶Enable	Disable	
Storage Hierarchy	Enable or Disable Storage Hierarchy		
	▶Enable	Disable	
Endorsement Hierarchy	Enable or Disable Endorsement Hierarchy		
	▶Enable	Disable	
Physical Presence Spec Version	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.		
	1.2	▶1.3	
Device Select	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated		
	TPM 1.2	TPM 2.0	▶Auto

4.4.2 ACPI Settings

System ACPI Parameters.

ACPI Settings		
Enable ACPI Auto Configuration	Enables or disables BIOS ACPI Auto Configuration.	
	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 (COM0/1)	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.

Option ROM Dispatch Policy		
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 All Cpu Informaiton

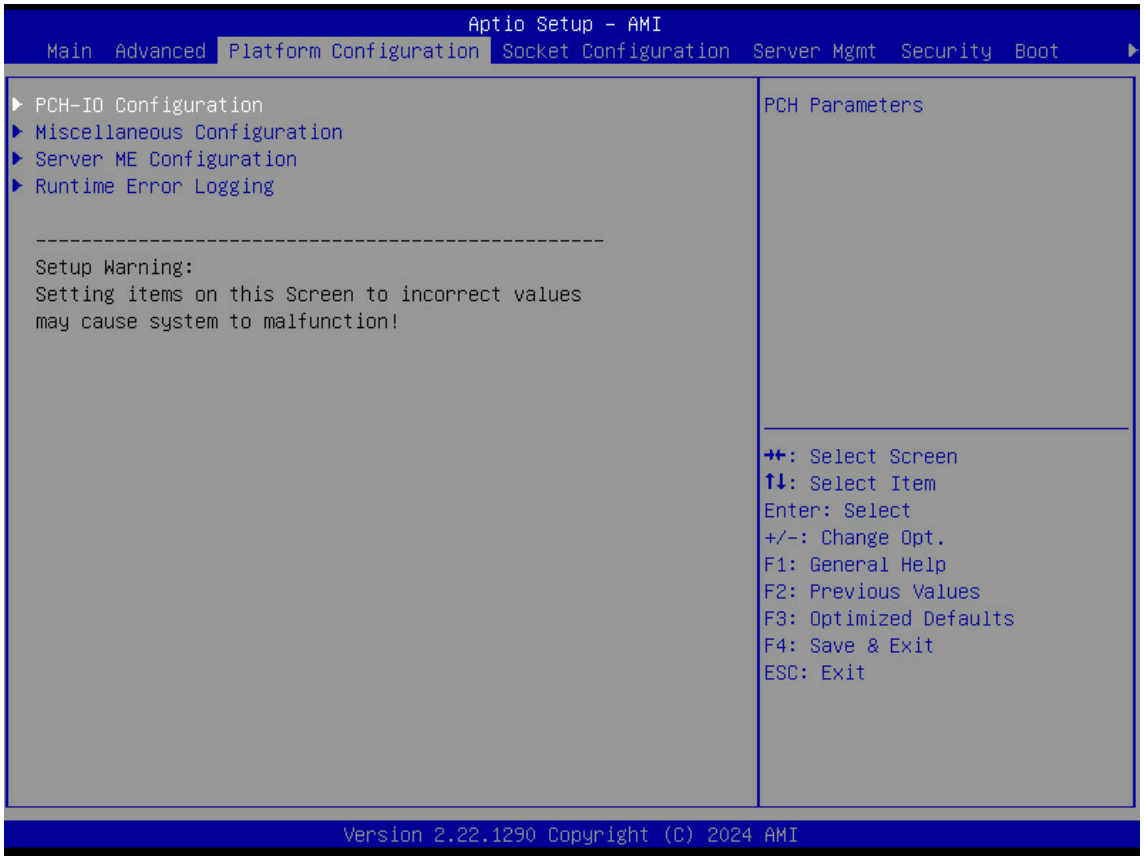
Display all cpu information.

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.	
RAM Disk 0: [0x5F0BD018, 0x5F0BE017]	Select for remove.	
	Enabled	▶Disabled
Remove selected RAM disk(s)	Removes selected RAM disk(s).	

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 1/2/3 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 1-3 SATA and RST Configuration	SATA Port 0-7	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 "Disabled" 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
	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	
	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 Miscellaneous Configuration

Miscellaneous Configuration				
Application Profile Configuration	Application Profile Configuration provides a quick method of BIOS knob tuning accordingly to application. It's based on benchmark tests and may be not suitable to all workloads. You can still override the options.			
	▶Auto	General Computing	Memory Bandwidth	Matrix Calculation
	Energy Efficiency	Server Side Java	OLTP	Virtualization
KCS Access Control Policy	Decides when IPMI commands shall be sent through KCS interface.Allow All - Always, Restricted - until BIOS DONE is signaled, Deny All - Never			
	▶Allow All	Restricted	Deny All	
Reset Platform on Memory Map Change	Causes a platform reset if the memory map has changed. Required for S4 resume to function at first boot.			
	Enabled	▶Disabled		
Fan PWM Offset	Valid Offset 0-100. This number is added to the calculated PWM value to increase Fan Speed.			
	30			
Wake On Lan Support	Enable or Disable Wake On Lan Support.			
	▶Enabled	Disabled		
Breakpoint Type	Halt at specified points in BIOS.			
	▶None	After MRC	After KTI RC	After Resource Allocation
	After POST	After Fulll Speed Setup	Ready for IBIST	
Enforced Password Support	Enables or Disables the Enforced Password support. Enabling it will allow the BIOS to send the Seed, Algorithm and password information to BMC.			
	Enabled	▶Disabled		
Advanced Debug Function	Advanced Debug Function (Dfx Knob).			
	▶Auto	Enabled	Disabled	
Serial Debug Message Level	Disable = no messages, Minimum = critical messages, Normal = critical & informational messages, Maximum = all messages, Auto = Minimum (default) or Normal (Advanced Debug mode)			
	Disable	Minimum	Normal	
	Maximum	▶Auto	Fixed PCD	
Trace Messages	Enables display of every IO access.			
	▶Disabled	Enabled	Enabled for registry writes only.	
Training Messages	Enabled = set to display the training results. Training results also get displayed if debug messages is set to Maximum.			
	Enabled	▶Disabled		
Active Video	Select active Video type			
	Auto	▶Onboard Device	PICE Device	
PS2 Port Swap	Enables or Disables the PS2 port swap			
	Enabled	▶Disabled		
Wake On Lan from S5	Enables or Disables Wake on Lan from S5			
	Enabled	▶Disabled		
Boot to Network	Enables or Disables Boot to Network.			
	Enabled	▶Disabled		
ARI Support	Enable or disable the ARI support			
	▶Enabled	Disabled		
RTC Wake system from S4/S5	Enable: Enable Wake on RTC feature. Disable: Disable Wake on RTC feature. Enabled and set wake time: Enable System wake on alarm event and set wake on the day::hr::min::sec specified.			
	▶Disable	Enable	Enable and set wake on time	
Firmware Configuration	Firmware Configuration options.			
	Ignore Policy Update	Production	Test	
	Internal	▶Restricted	Restricted SV	

Warm-Reset Elimination	When enabled, BIOS will skip warm-reset on the cold-reset path			
	▶Disable	Enable	Auto	
External SSC - CK440	External SSC - CK440			
	▶SSC Off	SSC=-0.3%	SSC=-0.5%	Hardware
Emulation BIOS Skip S3M Access	Emulation BIOS use it to skip S3M access.Enable: S3M is skipped;Disable: S3M is not skipped. Auto: Automatically enables/disables S3M			
	Disable	Enable	▶Auto	
BMC remote setup	BMC modify setup variables.Enable: BMC can modify setup variables;Disable: BMC can not modify setup variables.			
	▶Disable	Enable		
Force Boot With FULL Socket Number	Force Boot With FULL Socket Number			
	▶Disable	1 Socket	2 Socket	
	4 Socket	8 Socket		

4.5.3 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

4.5.4 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
IIO Dmi Error	Enable/Disable IIO Dmi 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.

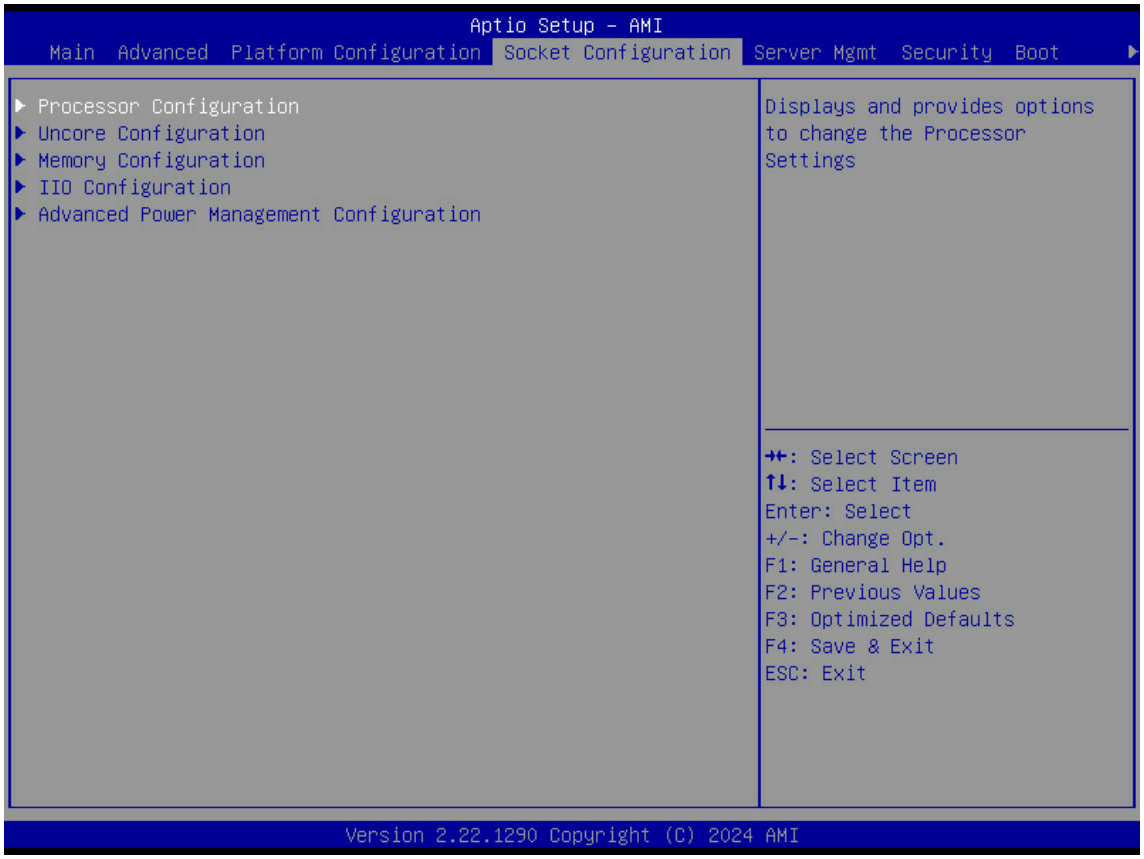
Error Control Setting			
CPU CrashLog Feature	The feature helps collecting crash data from OOBMSM SSRAM.		
	▶Auto	Enable	Disable
Core CrashLog Disable	The feature helps to disable CPU Core crash log.		
	▶no	yes	
TOR CrashLog Disable	The feature helps to disable CPU TOR crash log.		
	▶no	yes	
Uncore CrashLog 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	
Enable LP [Global]	Enables Logical processor(Software Method to Enable/Disable Logical Processor threads)		
	▶ALL LPs	Single LP	
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)	

PSMI Configuration	PSMI Configuration			
	Global PSMI Enable	Global PSMI Enable.		
		▶Enable	Disable	Force setup
	Socket 0/1 Configuration	PSMI Enable	PSMI Enable	
			Enable	▶Disable

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
	Limit CPU PA to 46 bits	Limit CPU physical address to 46 bits to support older Hyper-v. If enabled, automatically disables TME-MT.					
		▶Disable	Enable				
	MCTP Bus Owner Selection	Select the MCTP Bus Owner					
		▶PCH SPS as Bus Owner (Proxy)	CPU as Bus owner				

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						
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 0-5/7 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 PCIe port.				
			▶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/2A/3A/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		
		SRIS	Enable or Disable SRIS			
			▶NO	YES		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			▶Enable	Disable		
		CXL Drift Buffer	Enable/Disable CXL Drift Buffer if there is a common referrence clock.			
			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			

Socket0 Configuration	Port 1A/2A/3A/4E/4G/5A/5C/5E/5G	(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

Socket0 Configuration	Port 4A/4C	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
		SRIS	Enable or Disable SRIS ►NO / YES
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable. ►Enable / Disable
		CXL Drift Buffer	Enable/Disable CXL Drift Buffer if there is a common referrence clock. 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

Socket0 Configuration	Port 4A/4C	(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	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 0-5/7 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		

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/2A/3A/3C/3E/3G 4A/4C/4E/4G/5A/5E 0A/0C	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		
		SRIS	Enable or Disable SRIS			
			▶No	Yes		
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable.			
			▶Enable	Disable		
		CXL Drift Buffer	Enable/Disable CXL Drift Buffer if there is a common reference clock.			
			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			

Socket1 Configuration	Port 1A/2A/3A/3C/3E/3G 4A/4C/4E/4G/5A/5E 0A/0C	(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 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
		SRIS	Enable or Disable SRIS ▶No Yes
		Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable. ▶Enable Disable
		CXL Drift Buffer	Enable/Disable CXL Drift Buffer if there is a common reference clock. 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

Socket1 Configuration	Port 0E/0G	(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			
		CPM	Select CPM Enable/Disable				
			▶Enable	Disable			
		HQM	Select HQM 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.

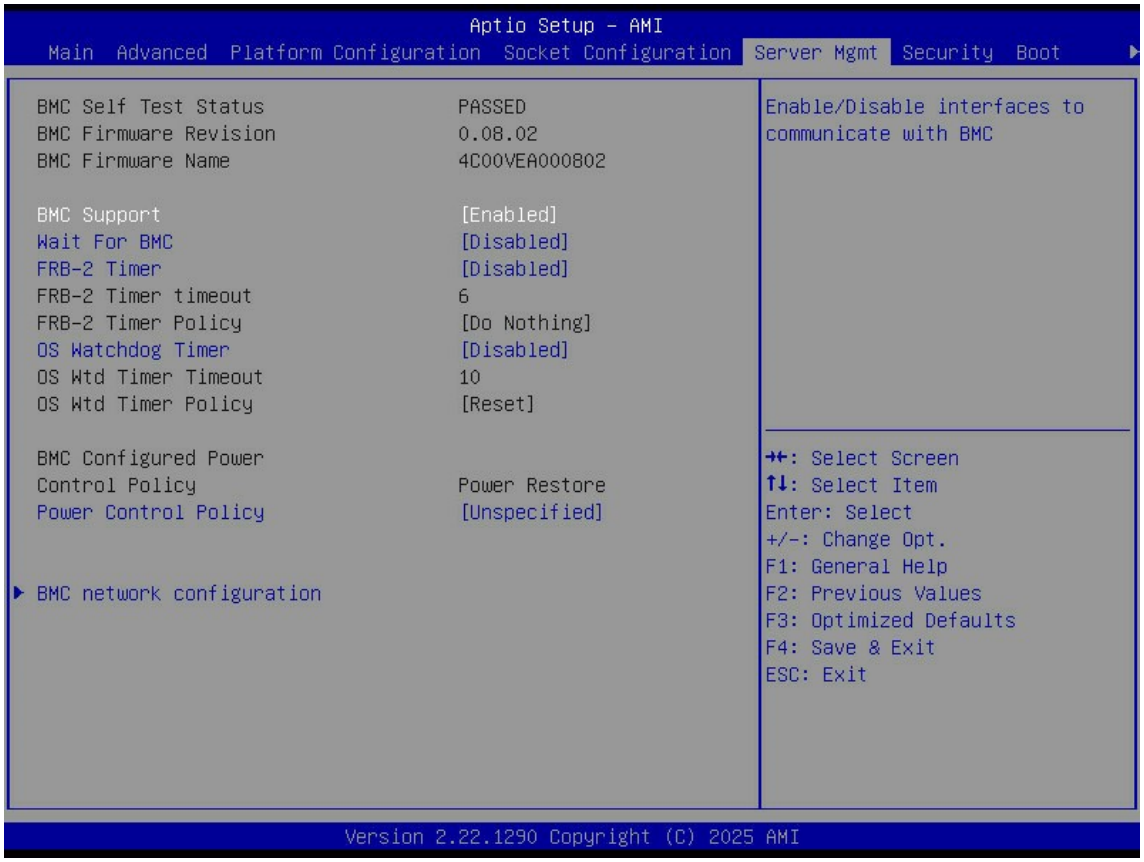
Advanced Power Management Configuration					
CPU P State Control	P State Control Configuration Sub Menu, include Turbo, XE and etc.				
	SpeedStep (Pstates)	Enable/Disable EIST (P-States).			
		▶Enable	Disable		
	EIST PSD Function	Choose HW_ALL/SW_ALL in _PSD return.			
		▶HW_ALL	SW_ALL		
	Turbo Mode	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	
		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 BMC Network Configuration

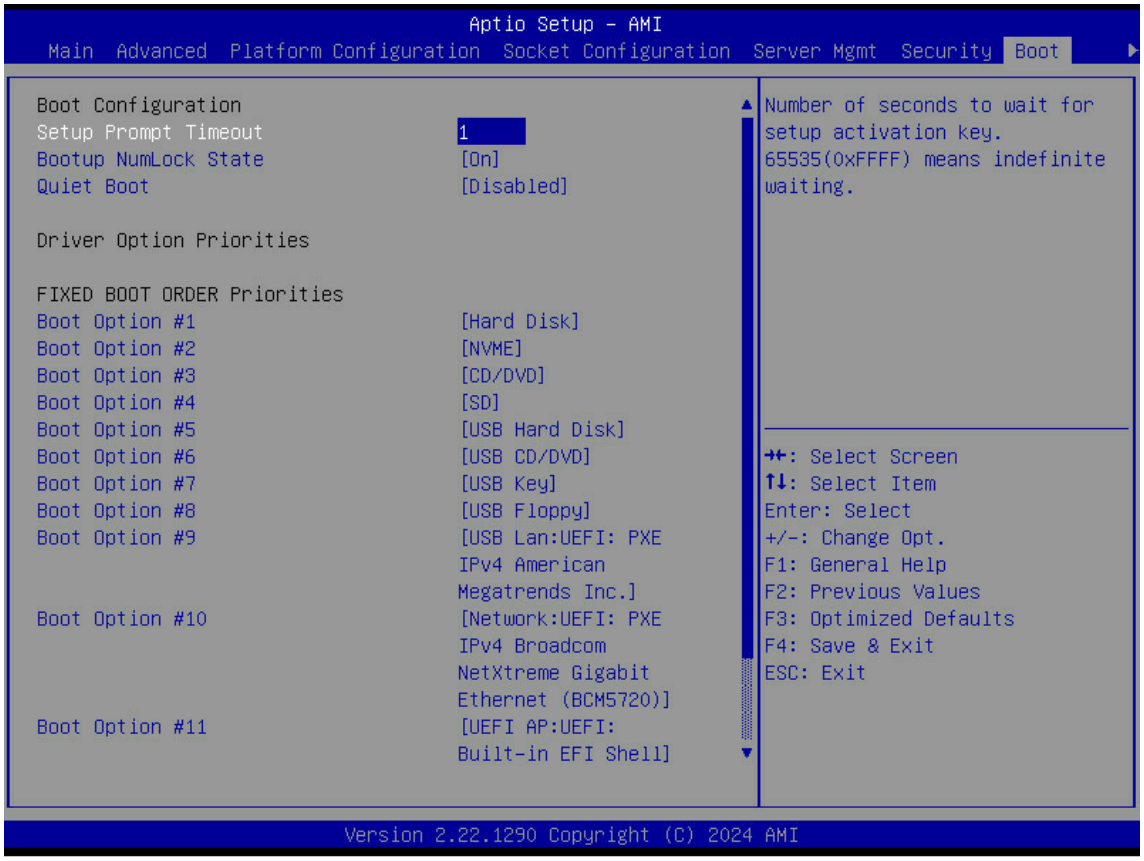
Configures BMC network parameters.

BMC Network Configuration				
Configure IPv4 support				
Configuration Address source Lan1/2	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
	Current Configuration Address source	DynamicAddressBmcDhcp		
	Station IP address	0.0.0.0		
	Subnet mask	0.0.0.0		
	Station MAC address	0-0-0-0-0-0		
	Gateway IP address	0.0.0.0		
	Gateway MAC address	0-0-0-0-0-0		
Configure IPv6 support				
IPv6 Support Lan1/2	Enables/disables LAN1 IPv6 Support			
	▶Enabled	Disabled		
Configuration Address source Lan1/2	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 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	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.		
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
	Restore Factory Keys	Force System to User Mode. Install factory default Secure Boot key databases.	
	Expert Key Management	Enables expert users to modify Secure Boot Policy variables without variable authentication.	

4.9 Boot

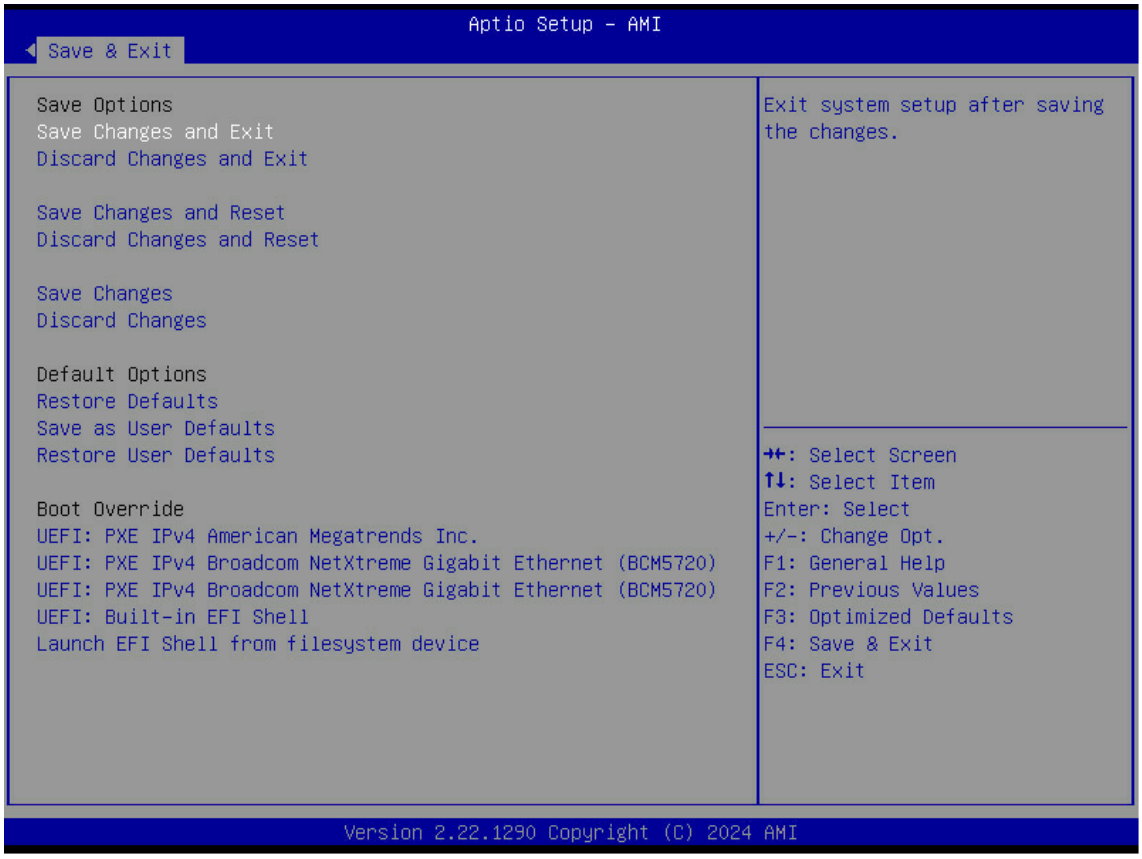


Boot		
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.	
	1	
Bootup NumLock State	Select the keyboard NumLock state.	
	▶On	Off
Quiet Boot	Enables/disables Quiet Boot option.	
	Enable	▶Disable
Boot Option #1	Sets the system boot order.	
	▶Hard Disk	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)
	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:UEFI: PXE IPv4 American Megatrends Inc.	▶Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)		
	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:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)		
	▶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 USB Lan Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI USB Lan Drives.			
	Boot Option #1	Sets the system boot order.		
		▶UEFI: PXE IPv4 American Megatrends Inc.	Disable	
UEFI NETWORK Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI NETWORK Drives.			
	Boot Option #1	Sets the system boot order.		
		▶UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	Disable
	Boot Option #2	Sets the system boot order.		
		UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	▶UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	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.
UEFI: PXE IPv4 American Megatrends Inc.	
UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	
UEFI: PXE IPv4 Broadcom NetXtreme Gigabit Ethernet (BCM5720)	
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 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
ACPI ASL 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: +7-4997019998
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.