Scutum

Server Motherboard
User's Manual

UM_Scutum_v1.1_071025

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 9
2.2.1 Placement 9
2.2.2 DIMM Population 10
2.2.3 Installation 11
Chapter 3. Motherboard Settings 12
3.1 Block Diagram 12
3.2 Placement 13
3.3 Content List 14
3.4 External Port 16
3.5 Connector Definition 18
3.6 Jumper Setting 33
3.7 Internal LED 39
Chapter 4. BIOS Configuration Settings 40
4.1 Navigation Keys 40
4.2 BIOS Setup 41
4.2.1 Menu 41
4.2.2 Startup 41
4.3 Main 42
4.3.1 Main 42
4.4 Advanced 43
4.4.1 Trusted Computing 43
4.4.2 Serial Port Console Redirection 44
4.4.3 SIO Configuration 44
4.4.4 PCI Subsystem Settings 44
4.4.5 USB Configuration 44
4.4.6 Network Stack Configuration 45
4.4.7 T1s Auth Configuration 45
4.4.8 RAM Disk Configuration 45
4.4.9 Driver Health 45
4.5 Platform Configuration 46
4.5.1 PCH Configuration 46
4.5.2 Server ME Configuration 48
4.5.3 Server ME Debug Configuration 48

4.5.4 Runtime Error Logging 49
4.6 Socket Configuration 50
4.6.1 Processor Configuration 50
4.6.2 Common RefCode Configuration 51
4.6.3 Memory Configuration 51
4.6.4 IIO Configuration 52
4.6.5 Advanced Power Management Configuration 53
4.7 Server Mangement 57
4.7.1 Processor Configuration 57
4.7.2 System Event Log 58
4.7.3 BMC Network Configuration 58
4.8 Security 59
4.9 Boot 60
4.10 Exit 61
4.11 BIOS Post Code 62
Chapter 5. Technical Support 68

Document Release History

Release Date	Version	Update Content
January, 2024	1	User's Manual release to public.
July, 2025	1.1	Remove connector J6.

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

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

Preface

Copyright

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

Trademarks

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

Changes

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

Warning

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

Disclaimer

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

Instruction Symbols

Special attention should be given to the instruction symbols below.

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

Safety Instructions

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 Scutum 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 Scutum 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. Scutum 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 P+(LGA-4189) socket type with a memory support of 8 channel DDR4 RDIMM/LRDIMM/Barlow Pass with EEC up to 3200/2933 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 BMC Configuration Settings
This chapter illustrates the diverse functions of IPMI BMC, including the details on logging into the web page and assorted definitions. These descriptions are helpful in configuring various functions through Web GUI without entering the BIOS setup. For more information of BMC configurations, please refer to IPMI BMC (Aspeed AST2500) User's Manual for a more detailed description.

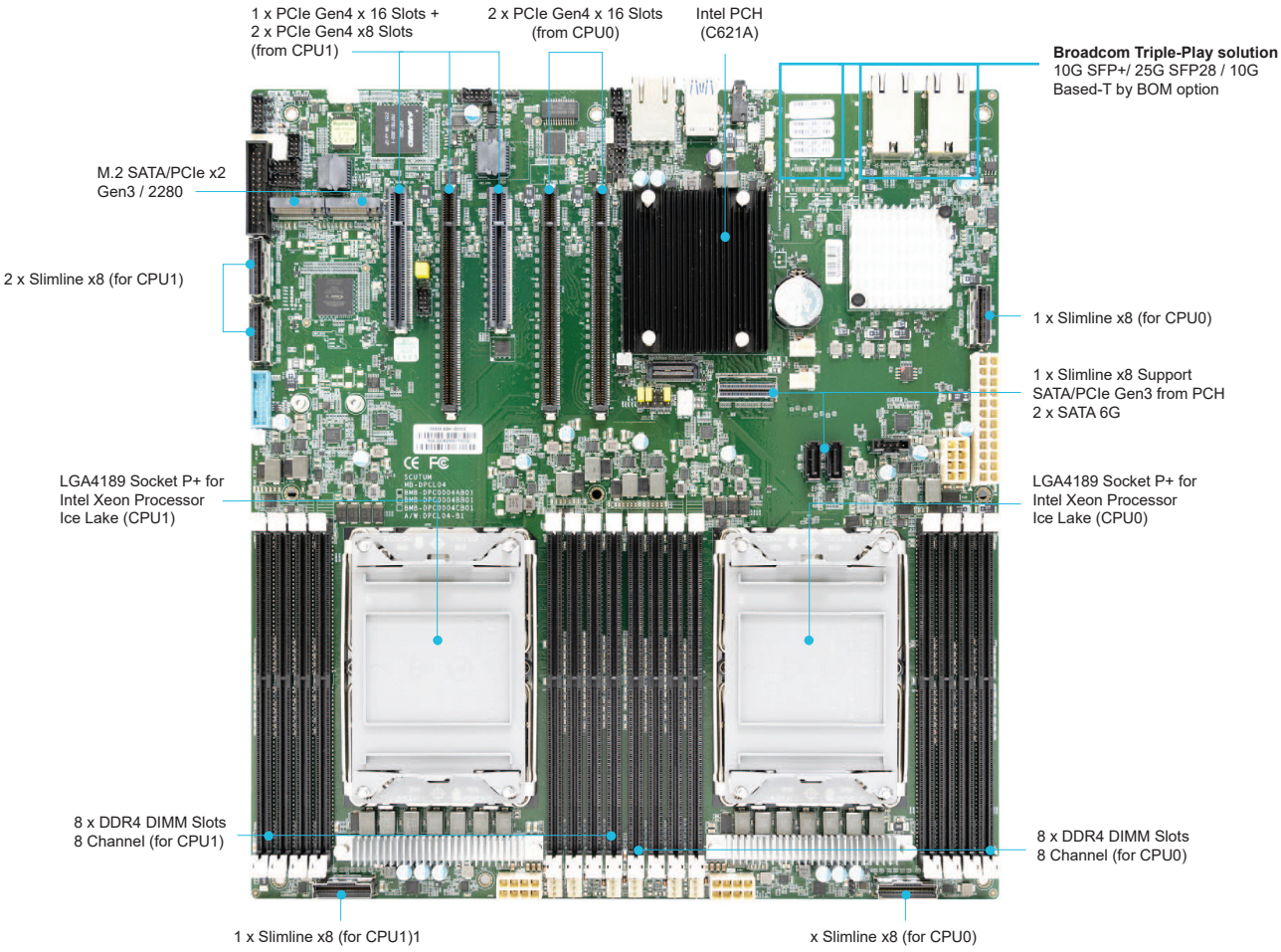
Chapter 6 Technical Support
For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: https://www.aicipc.com/en/index.
It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

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

1.1 Component

Scutum Serverboard



Dimensions
mm : 304.8 x 330.2
inches : 12 x 13

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

1.2 Specifications

System	Processor Support	3rd Gen Intel® Xeon® Scalable Processors (Ice lake CPU)
	CPU TDP	270W
	UPI Speeds	10.4 / 11.2 GT/s
	Socket Type	Socket P+ (LGA-4189)
	System Memory	• 8 x memory channels per CPU(1DPC) • 16 x DIMM slots support: DDR4 3200/2933MHz RDIMM/LRDIMM - up to 512GB RDIMM SRx4 (16Gb) - up to 1024GB RDIMM DRx4 (16Gb) - up to 4096GB RDIMM 3DS 8Rx4 (16Gb) - up to 2048GB LRDIMM QRx4 (16Gb) - up to 4096GB LRDIMM 3DS 8Rx4 (16Gb) • Intel® Optane™ DC Persistent Memory (Barlow Pass) support
	Expansion Slots	• CPU0: 2 x PCIe Gen4 x16 slots + 2 x slimline x8 • CPU1: 1 x PCIe Gen4 x16 slot 2 x PCIe Gen4 x8 3 x slimline x8
System BIOS	BIOS Type	AMI UEFI BIOS
	BIOS Features	• ACPI • PXE • AC loss recovery • IPMI KCS interface • SMBIOS • Serial console redirection • SRIOV • TPM • PCIe Hotplug
On-board Devices	SATA	Lewisburg PCH on-chip solution supports 10 x SATA 6.0 Gb/s • 2 x SATA 7pin support #7 with 5V by jumper setting + 8 x SATA by slimline (supports both SATA/PCIe by PCH HSIO)
	BMC	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN • SMASH Support • HTML5 • Redfish

On-board Devices	Network Controller	• Realtek RTL8211E GbE for BMC dedicate management port • Intel I210 GbE • Broadcom BCM57416/57417 co-design to support 10GBase-T/10G SFP+ / 25G SFP28 (by BOM option) (NCSI shared NIC - reserved for BCM57416 & I210 by jumper setting)
	Graphics	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • PCIe VGA/2D Controller • 1920x1200@60Hz 32bpp
Input/Output	SATA	Lewisburg PCH on-chip solution support 10 x SATA 6.0 Gb/s • 2 x SATA 7pin support #7 with 5V by jumper setting + 8 x SATA by slimline (supports both SATA/PCIe by PCH HSIO)
	LAN	• 1 x GbE RJ45 dedicated to BMC management • Dual port of RJ45 10G / SFP+ 10G / SFP28 25G (by BOM option)
	USB	• 2 x USB 3.0 double-stake type A connectors • 2 x USB pin headers support USB3.0/2.0
	Video Output	1 x internal VGA pin-header
	Serial Port	• 1 x external COM port by audio jack • 1 x COM2 box header • 1 x COM1 box header share with rear IO audio jack
	Others	1 x TPM 2.0 onboard option (designed reserved, BTO only)

1.3 Feature

The Scutum 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)

By implementing Intel® Xeon® Scalable Processors, fully integrated microarchitecture supports up to 3 x 16 lanes, 2 x8 lanes PCIe slots, 5 slimlinex8 of PCIe Gen4 and Broadcom LOM Triple-Play NIC solution (10G SFP+/ 25G SFP28 / 10G Based-T by BOM option), providing eight channels per CPU with total sixteen DIMM slots deployment which can support up to DDR4 3200/2933MHz, Scutum server board can meet both cost efficiency and performance requirement for lots of applications.

Featured with ground breaking technologies including Intel® Next Generation Microarchitecture and Instruction Set (AVX-512, VMD), Speed Shift Technology, UPI link speeds up to 11.2GT/s, the Scutum server board enable next generation server solutions with an incredible leap in performance.

- Supports 3rd Gen Intel® Xeon® Scalable Processors for highest server performance and improved power efficiency
- Supports 16 DDR4 DIMM slots for maximum memory performance
- Supports up to 3 x 16 lanes, 2 x8 lanes PCIe Gen4 slots, 5 x slimlinex8 PCIe Gen4
- Onboard Baseboard Management Controller for system management and IPMI control
- Embedded components for 5+ year long life
- Rackmount Technology Extension (RTX) form factor utilizes full internal chassis volume for optimum I/O configurations

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 P4 (LGA-4189).

2.1.1 Installation

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

☑ a T30 torque screwdriver

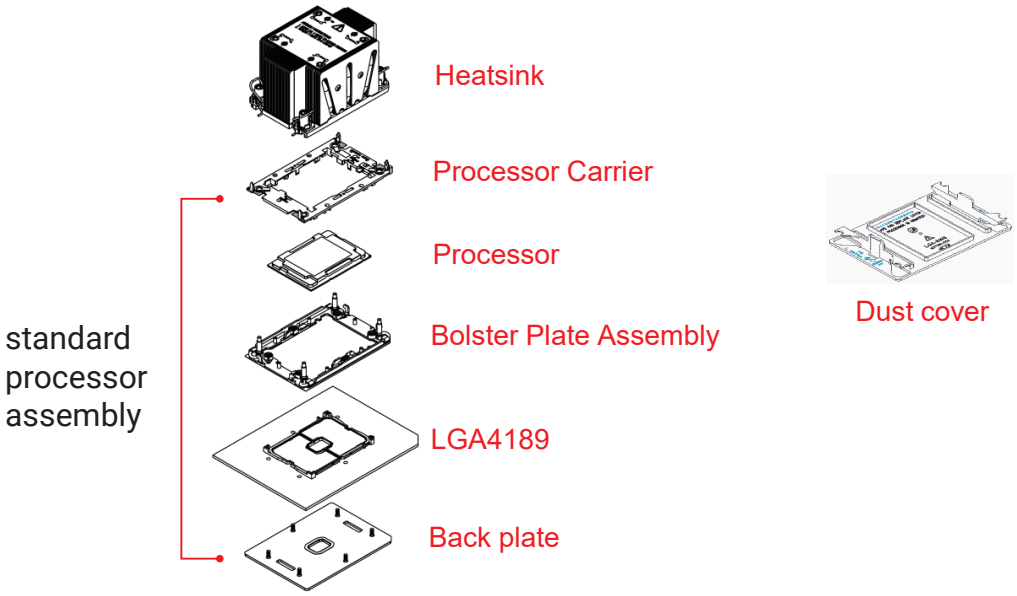
☑ ESD wrist strap/mat and conductive foam pad

☑ 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.

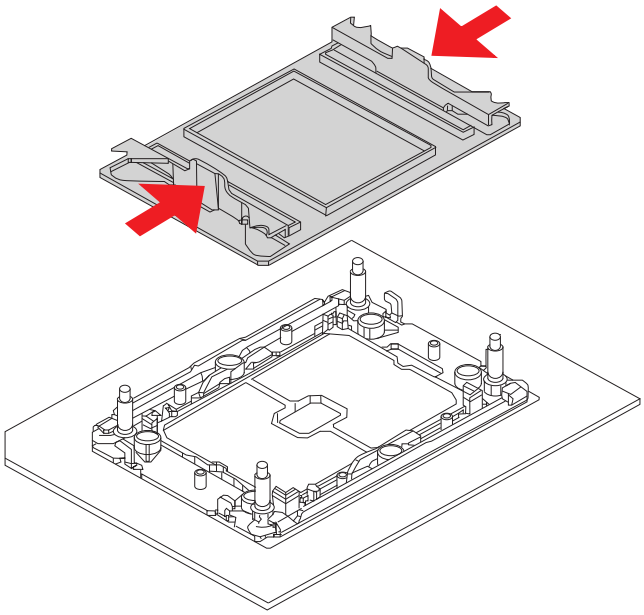
Standard Processor Assembly:
A standard processor assembly is comprised of 5 components: processor carrier, processor, bolster plate assembly, socket and back plate.



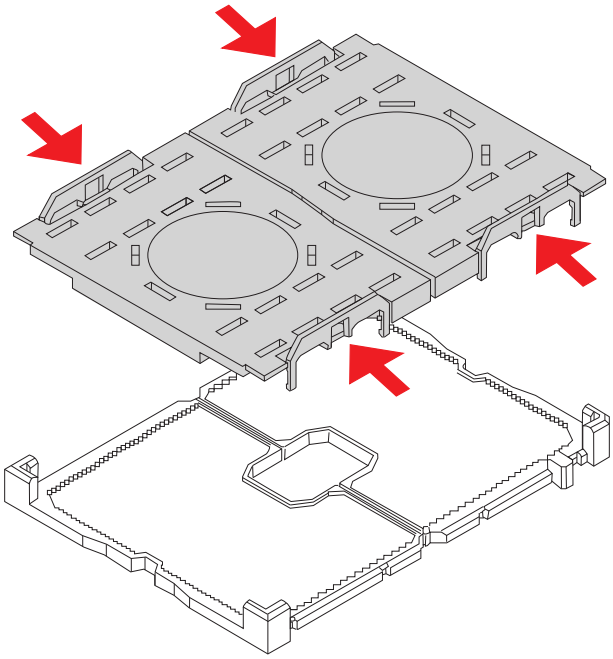
This information is provided for professional technicians only.

Procedure:

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

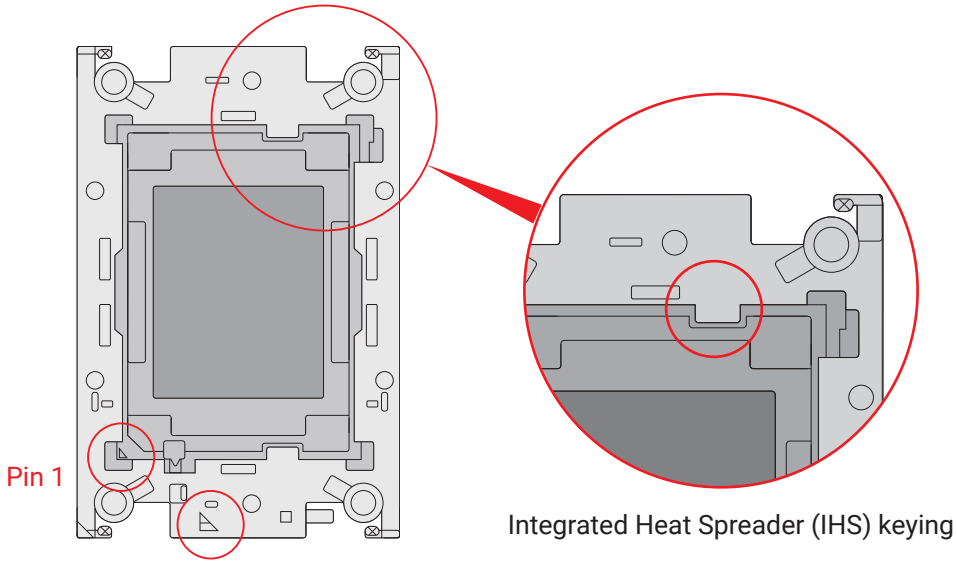


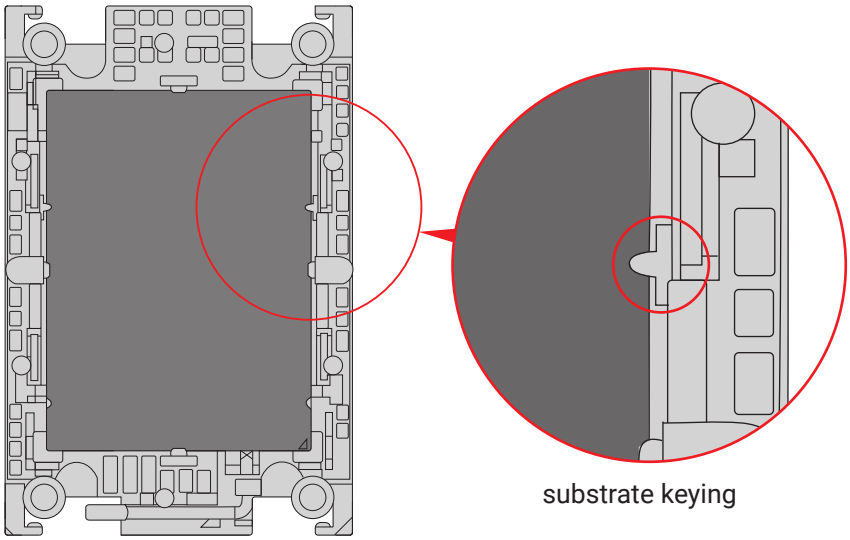
② Remove the Pnp cap from the socket. Press the tabs on both sides to remove.



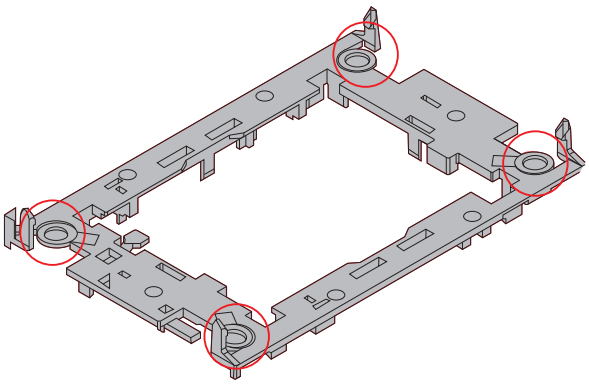
③ Insert the CPU into the CPU carrier. Carefully align and insert on side of the CPU and then the other.

> **NOTE**
> Must ensure to match the direction and pin of the CPU with the carrier. Refer to the placement of pin 1.

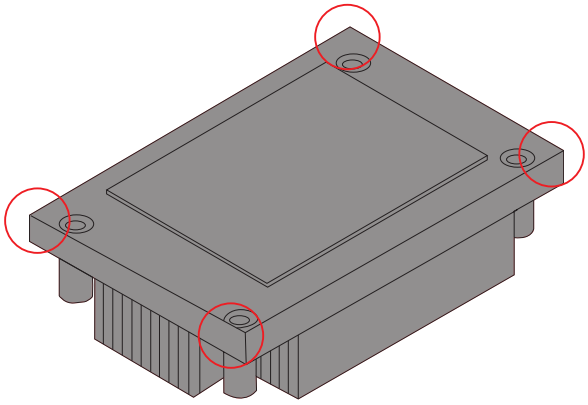




④ Attach the heat sink onto the CPU carrier. Hook the corners of the CPU carrier to the back side of the heat sink.



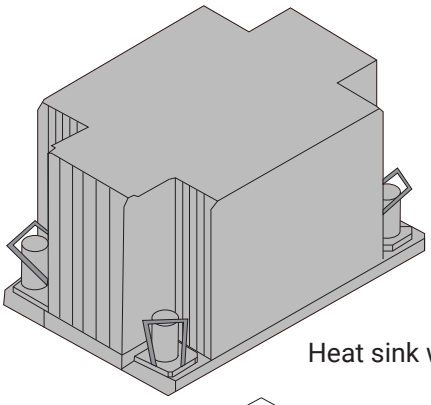
CPU carrrier



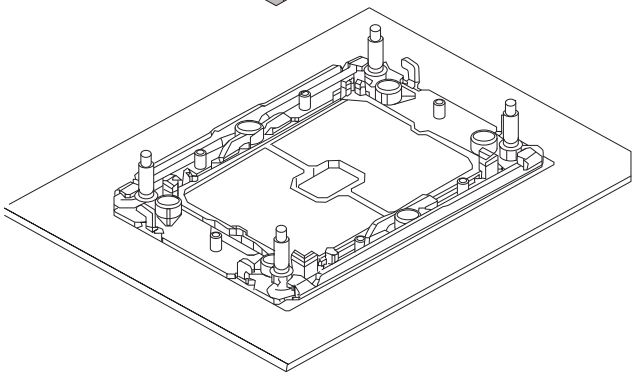
Heat sink back side

⑤ Install the assembled heat sink and CPU carrier onto the CPU socket. 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.

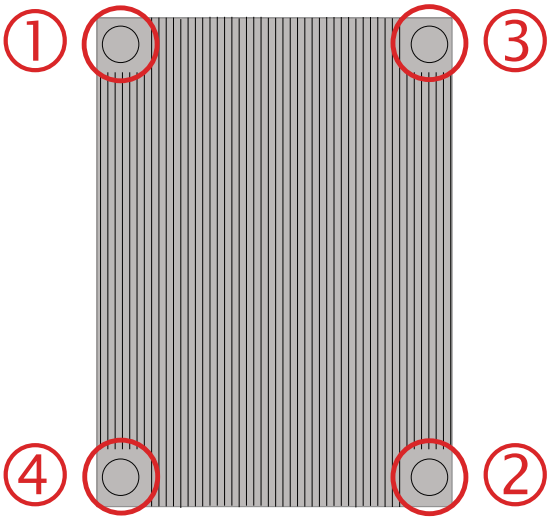
> **CAUTION**
> Failure to tighten the heat sink screws in the specified order may cause damage to the processor socket assembly. Heat sink screws is recommended to be tightened to 8 in-lbs torque, but can be tightened to 12 in-lbs torque according to the indicated order on the top of the heatsink label.



Heat sink with carrier

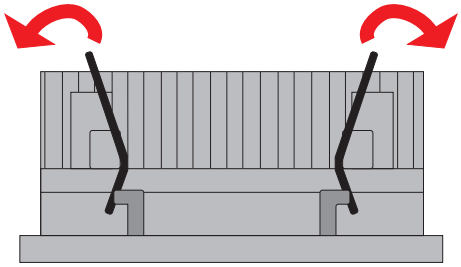


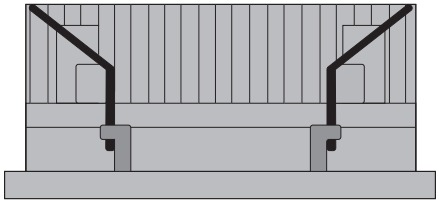
CPU socket



Screw tightening order

⑥ Press the rotating wire located on the four corners of the heat sink to latch position to secure the heat sink.





Latched postion

This information is provided for professional technicians only.

2.2 System Memory

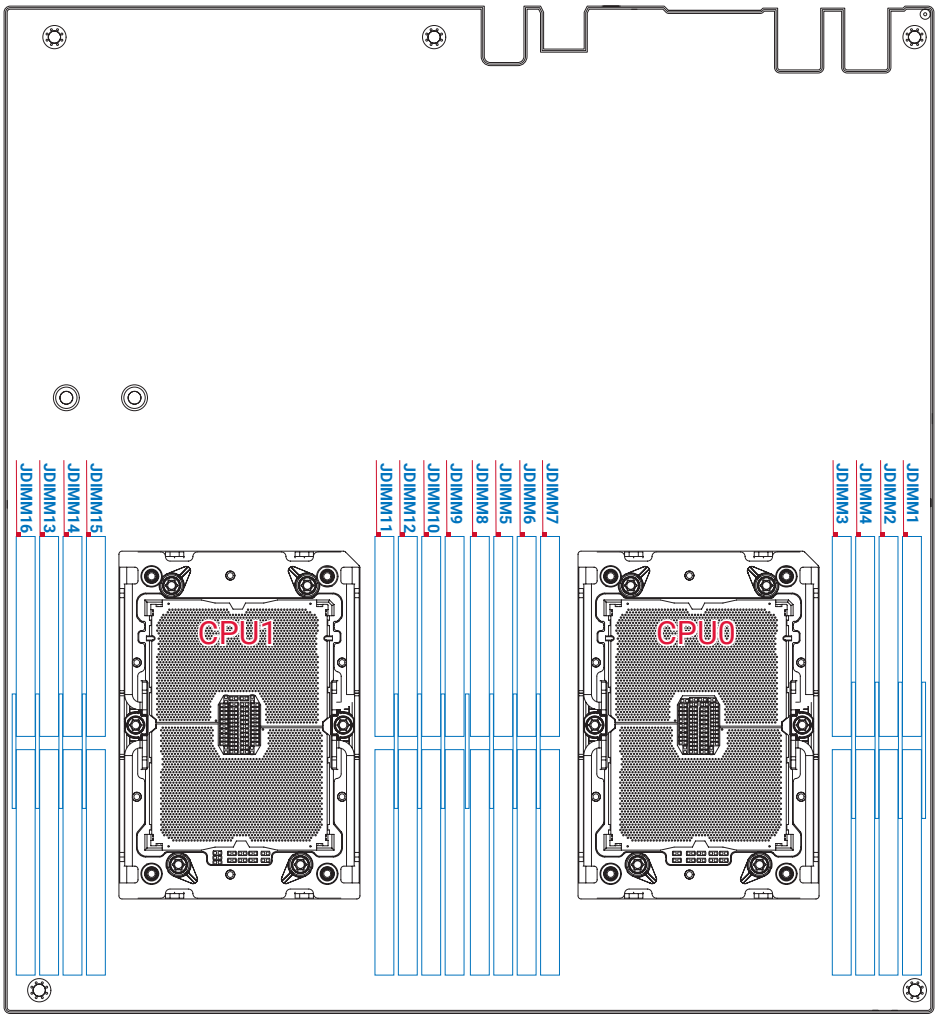
2.2.1 Placement

The DIMMs are displayed on the Scutum board as JDIMM1/JDIMM2/JDIMM3/JDIMM4/JDIMM5/JDIMM6/JDIMM7/JDIMM8/JDIMM9/JDIMM10/JDIMM11/JDIMM12/JDIMM13/JDIMM14/JDIMM15/JDIMM16

To ensure satisfactory performance, you need to:

☑ Verify the DIMM type:
This product supports DDR4 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 DIMM Population

NOTE

Rules to abide by before installation:

- Must install at least one DDR4 DIMM per socket.
- If only one DIMM is populated in a channel, you must install it in the slot furthest away from the CPU.
- Must populate DIMM0 before DIMM1.

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

1 CPU Configuration

Placement		DIMM Number				
		1	2	4	6	8
CPU0	JDIMM1		#	#	#	#
	JDIMM2	#			#	#
	JDIMM4				#	#
	JDIMM3			#		#
	JDIMM7			#		#
	JDIMM6				#	#
	JDIMM5		#	#	#	#
	JDIMM8				#	#

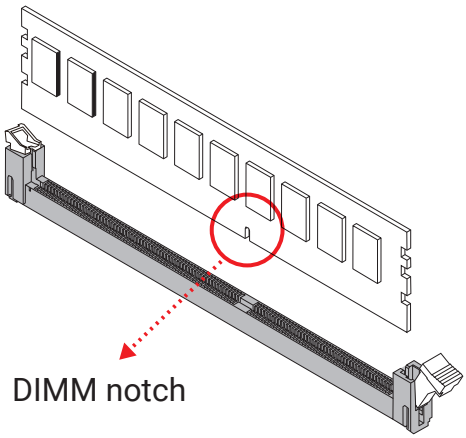
2 CPU Configurations

Placement		DIMM Number				
		1	2	4	6	8
CPU0	JDIMM1		#	#	#	#
	JDIMM2	#			#	#
	JDIMM4				#	#
	JDIMM3			#		#
	JDIMM7			#		#
	JDIMM6				#	#
	JDIMM5		#	#	#	#
	JDIMM8				#	#
Placement		1	2	4	6	8
CPU1	JDIMM9		#	#	#	#
	JDIMM10	#			#	#
	JDIMM12				#	#
	JDIMM11			#		#
	JDIMM15			#		#
	JDIMM14				#	#
	JDIMM13		#	#	#	#
	JDIMM16				#	#

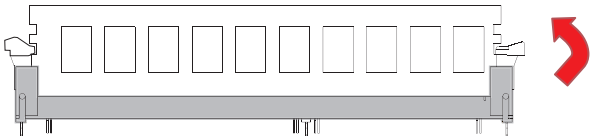
2.2.3 Installation

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.



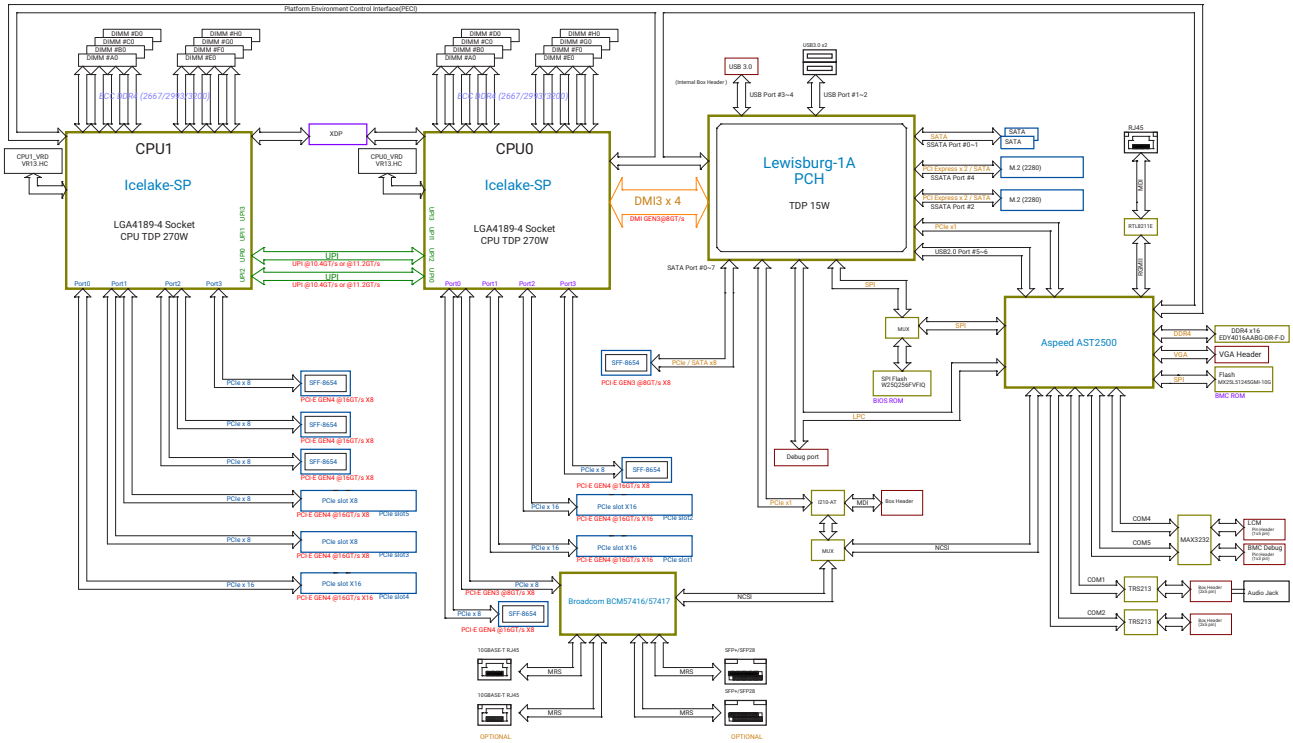
Step 3 Close the retaining clip to complete installation.



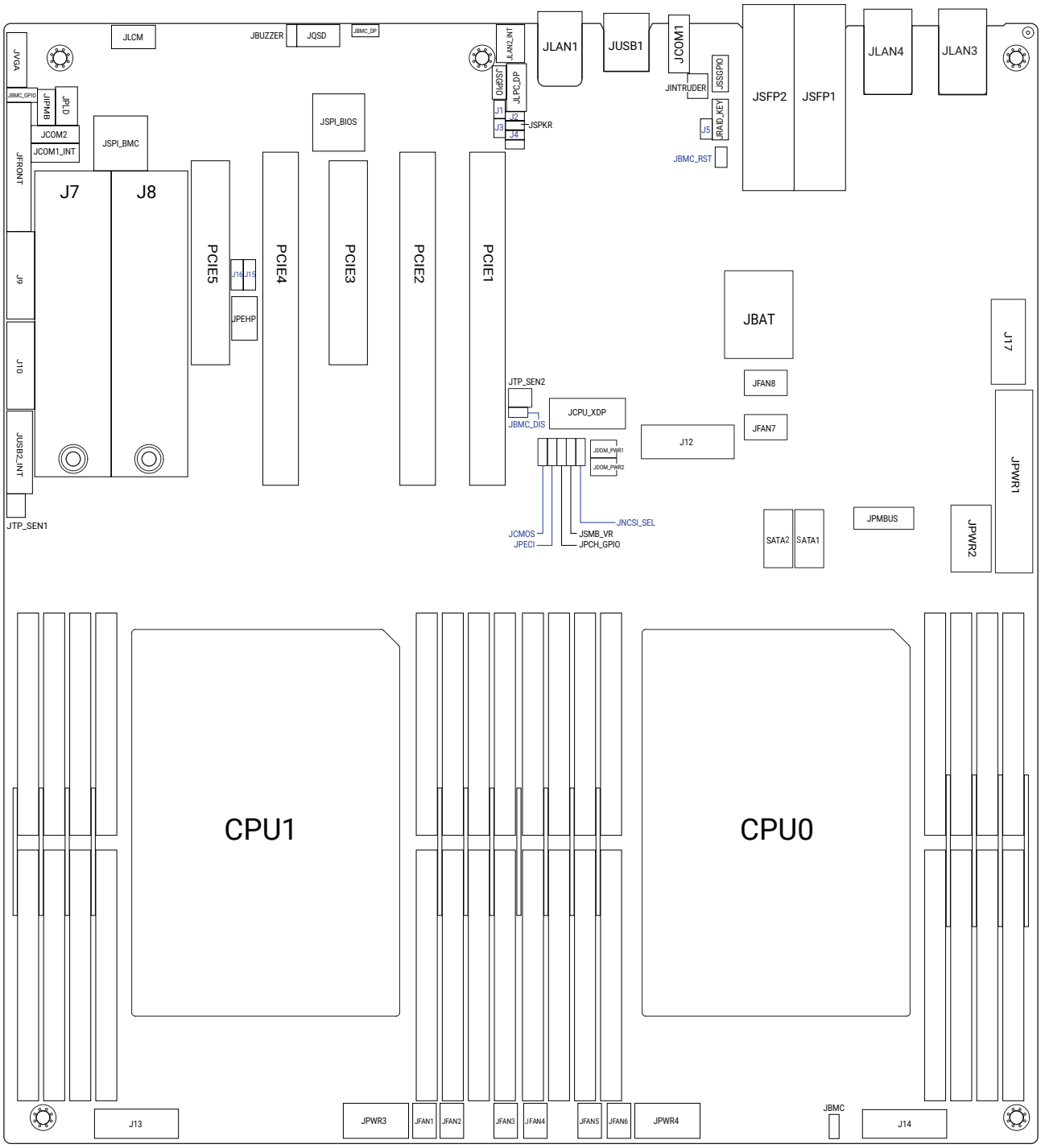
Chapter 3. Motherboard Settings

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

3.1 Block Diagram



3.2 Placement



3.3 Content List

External Connectors - Rear I/O

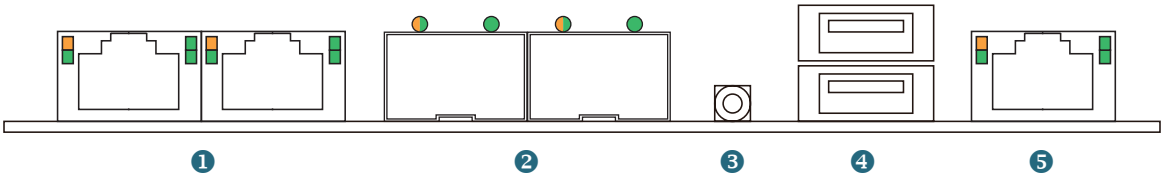
Port/Slot/Socket	
Phone Jack COM Port	JCOM1
USB 3.0 Type A Port	JUSB1
RJ45 Port	JLAN1 for dedicated management port JLAN3 (optional) JLAN4 (optional)
SFP+/28 Port	JSFP1 (optional) JSFP2 (optional)

Internal Connectors Summary

Connector	Placement
Power Supply	JPWR1: 12V, 5V, 3.3V, 5VSB
Power Supply	JPWR2, JPWR3, JPWR4: 12V
SATA-DOM Power	JDOM_PWR1, JDOM_PWR2: 5V
DIMM Socket	JDIMM1~16
Front Panel Header	JFRONT
Serial SATA Connector	SATA1, SATA2
Serial Port Header	JCOM1_INT, JCOM2
LCM Header	JLCM
USB3.0 Header	JUSB2_INT
XDP Connector	JCPU_XDP (optional)
LPC Debug Port Header	JLPC_DP
BMC Debug Port Header	JBMC_DP
BMC Debug Port Select Header	J2
BMC GPIO Header	JBMC_GPIO
PLD Download Header	JPLD
PLD QSD Header	JQSD
SGPIO Header	JSGPIO
SSGPIO Header	JSSGPIO
Clear CMOS Header	JCMOS
BMC I2C10	JBMC
RTC Battery Holder	JBAT
Intruder Header	JINTRUDER
PMBUS Header	JPMBUS
BIOS SPI ROM Socket	JSPI_BIOS
BMC SPI ROM Socket	JSPI_BMC

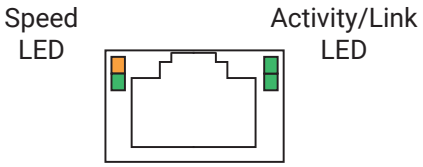
Connector	Placement
BMC Reset Header	JBMC_RST
BMC Disable Header	JBMC_DIS
PCH Speaker Header	JSPKR
NCSI Select Header	JNCSI_SEL
PECI Select Header	JPECI
BIOS Recovery Mode Header	J6
ME Force Recovery Mode Header	J3
Flash Descriptor Security override	J5
No Reboot (Watch Dog) Header	J1
IPMB Header	JIPMB
PCH GPIO Header	JPCH_GPIO
BMC Socflash Enable Header	J4
External Thermal Sensor Header	JTP_SEN1, JTP_SEN2
VROC Key Header	JRAID_KEY
BMC Buzzer Header	JBUZZER
VRM SMB Header	JSMB_VR
I210 MDI Header	JLAN2_INT
CPU0 PCIE4.0 x16 Slot	PCIE1, PCIE2
CPU0 PCIE4.0 x8 Connector	J14, J17
CPU1 PCIE4.0 x16 Slot	PCIE4
CPU1 PCIE4.0 x8 Slot	PCIE3, PCIE5
CPU1 PCIE4.0 x8 Connector	J9, J10, J13
PCH PCIE3.0 x4*2/SATA *8 Connector	J12
PCH PCIE3.0 x2/SATA *1 Connector	J7, J8
Fan Connector	JFAN1~8
VGA Connector	JVGA
J12 Slimline PCIE/SATA Select Header	J15, J16
CPU PCIe Hot Plug Header	JPEHP

3.4 External Port



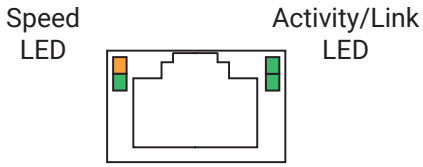
	Item		Item
1	2 * RJ45 for 10Gb Ethernet	4	2 * USB 3.2 Gen1
2	2 * SFP+/SFP28 for 10Gb/25Gb Ethernet	5	RJ45 for BMC management
3	COM by Phone Jack		

BMC Management RJ45 LED Indicator



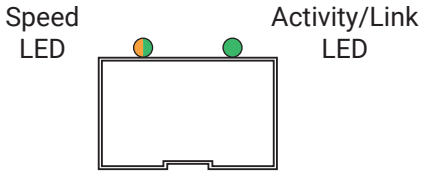
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.

10GBASE-T RJ45 LED Indicator



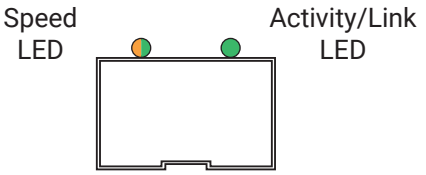
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	No link.
	Green	10G bps connection.
	Orange	1G bps connection.

SFP+ LED Indicator



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

SFP28 LED Indicator

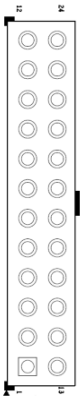


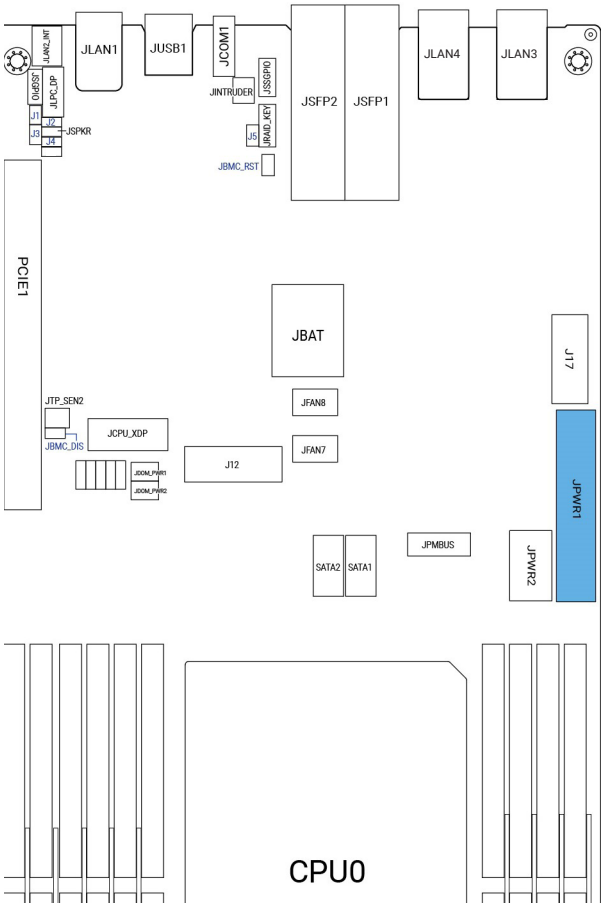
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	No link.
	Green	25G bps connection.
	Orange	10G bps connection.

3.5 Connector Definition

Power Supply Connector (JPWR1)
This is a 2x12-pin connector that provides the motherboard with power.

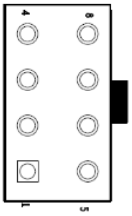
+3.3V	13	1	+3.3V
N.C.	14	2	+3.3V
GND	15	3	GND
PSON	16	4	+5V
GND	17	5	GND
GND	18	6	+5V
GND	19	7	GND
N.C.	20	8	PWROK
+5V	21	9	+5VSB
+5V	22	10	+12V
+5V	23	11	+12V
GND	24	12	+3.3V

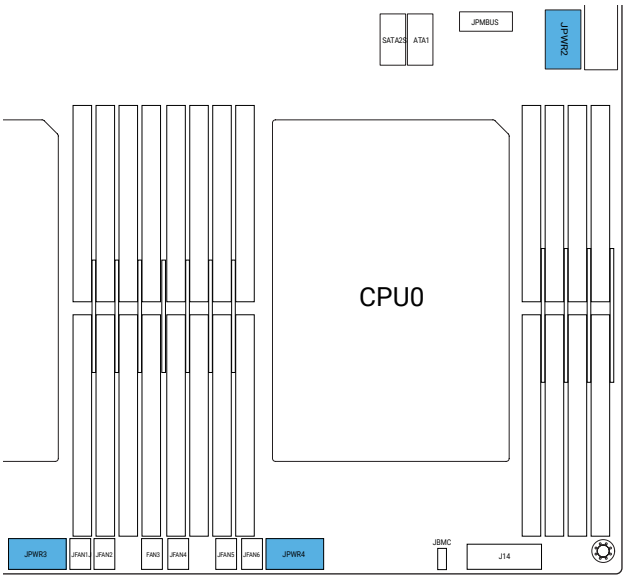




Power Supply Connector (JPWR2, JPWR3, JPWR4)
This is a 2x4-pin connector that provides the motherboard with power.

+12V	5	1	GND
+12V	6	2	GND
+12V	7	3	GND
+12V	8	4	GND

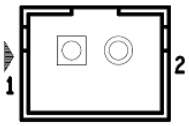


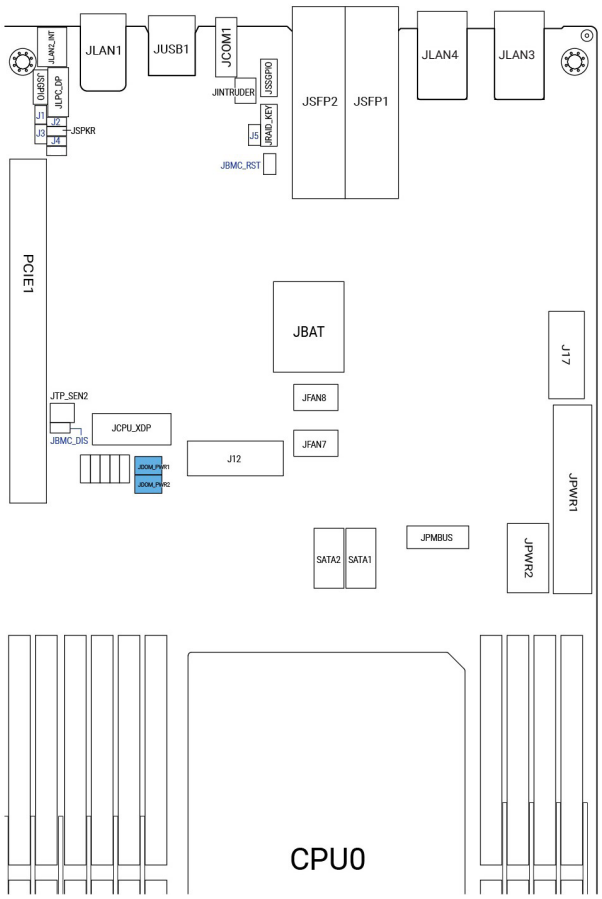


SATA DOM Power Header (JDOM_PWR1, JDOM_PWR2)

This is a 2-pin header that supplies power to SATA DOM.

1	GND
2	+5V

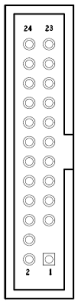


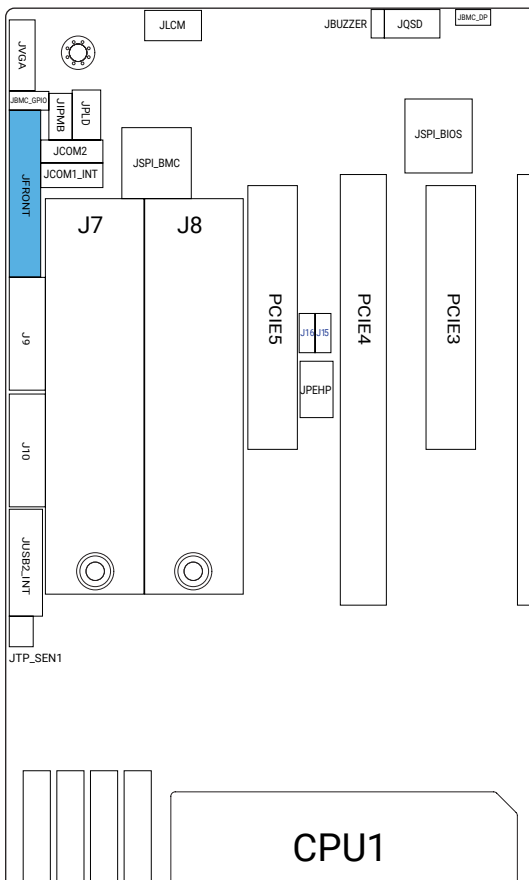


Front Panel Header (JFRONT)

This is a 2x12-pin header that supports the management of switches and controls from the front panel.

+3.3V_DUAL	2	1	PWR_LED+
+5VSB	4	3	KEY (no pin)
UID_LED#	6	5	PWR_LED-
SYS_HEALTH#2	8	7	+3.3V
SYS_HEALTH#1	10	9	HDD_LED#
LAN1_LINK_UP	12	11	SW_PWR_BTN#
LAN1_TRAFFIC	14	13	GND
I2C8SDA	16	15	SW_RST_BTN#
I2C8SCL	18	17	GND
INTRUDER#	20	19	UID_SW_IN#
LAN2_LINK_UP	22	21	+3.3V_DUAL
LAN2_TRAFFIC	24	23	FP_NMI_BTN

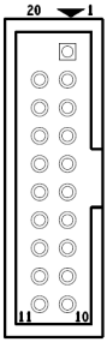


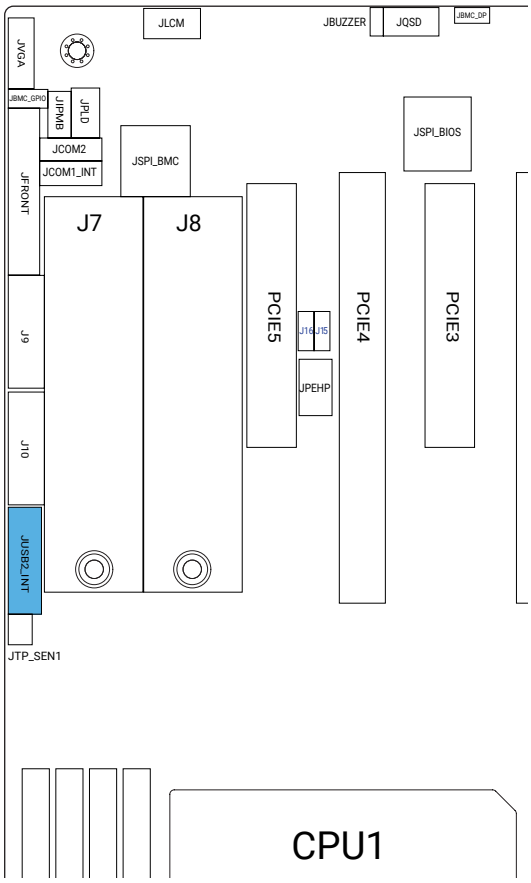


Front I/O USB Header (JUSB2_INT)

This is a 2x10-pin header that supports USB in the front panel.

KEY (no pin)	20	1	+5V
+5V	19	2	USB3_P03_ESD_RXN
USB3_P04_ESD_RXN	18	3	USB3_P03_ESD_RXP
USB3_P04_ESD_RXP	17	4	GND
GND	16	5	USB3_P03_ESD_TXN
USB3_P04_ESD_TXN	15	6	USB3_P03_ESD_TXP
USB3_P04_ESD_TXP	14	7	GND
GND	13	8	USB2_P03_ESD_DN
USB2_P04_ESD_DN	12	9	USB2_P03_ESD_DP
USB2_P04_ESD_DP	11	10	USB2_OC2_N

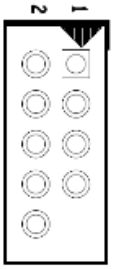


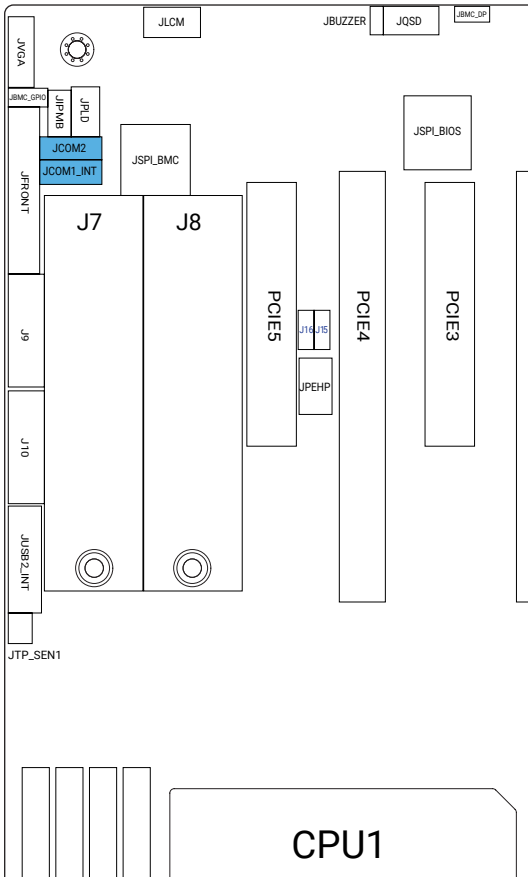


COM Port Header (JCOM1_INT, JCOM2)

This is a 2x5-pin header that used to provide COM port functionality.

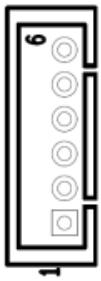
DCD	2	1	DSR
RXD	4	3	RTS
TXD	6	5	CTS
DTR	8	7	RI
GND	10	9	KEY (on pin)

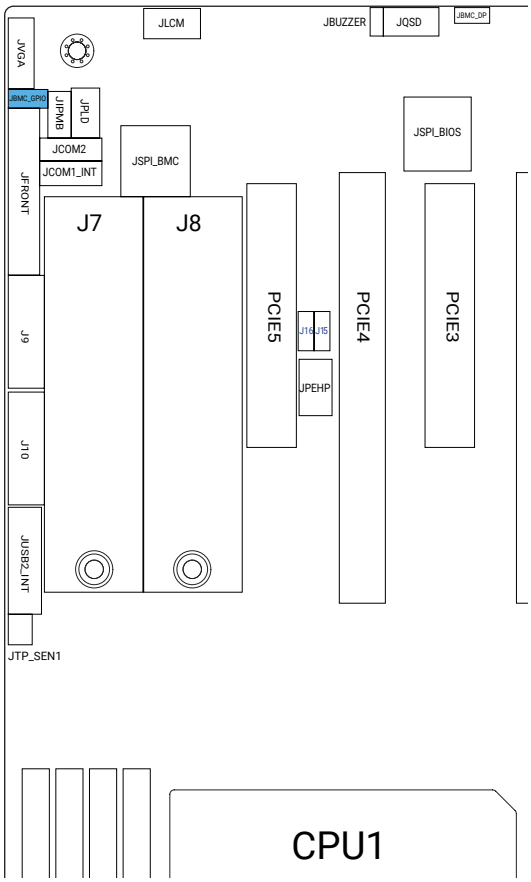




BMC GPIO Header (JBMC_GPIO)
This is a 1x6-pin header is used to provide BMC GPIO(General Purpuse Input and Output).

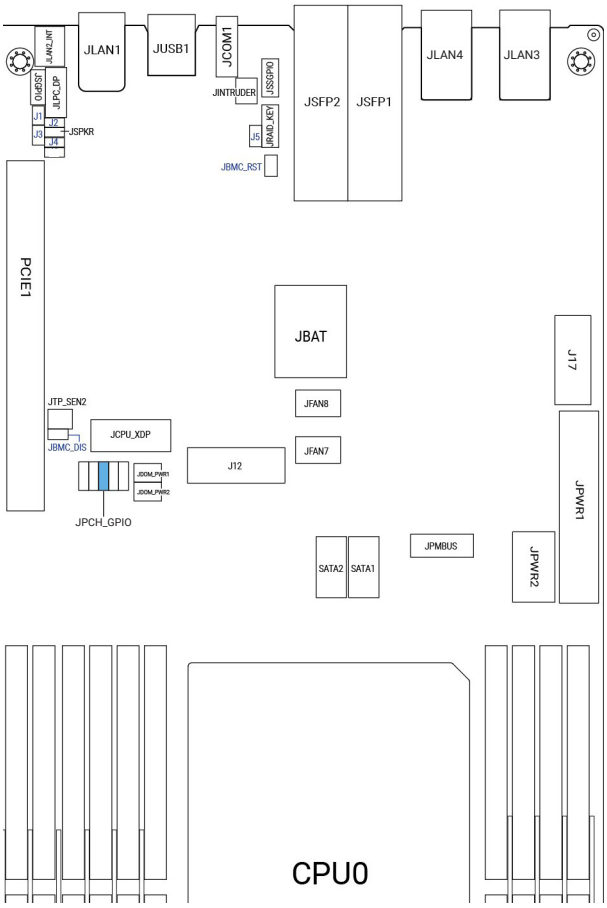
1	EXTRST#
2	BMC_GPY1
3	BMC_GPY0
4	I2C9SDA
5	I2C9SCL
6	GND





PCH GPIO Header (JPCH_GPIO)
This is a 3-pin header defines an input and output signal to the platform controller hub.

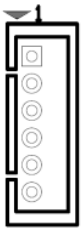
1	PCH_GPP_C16
2	PCH_GPP_C17
3	GND

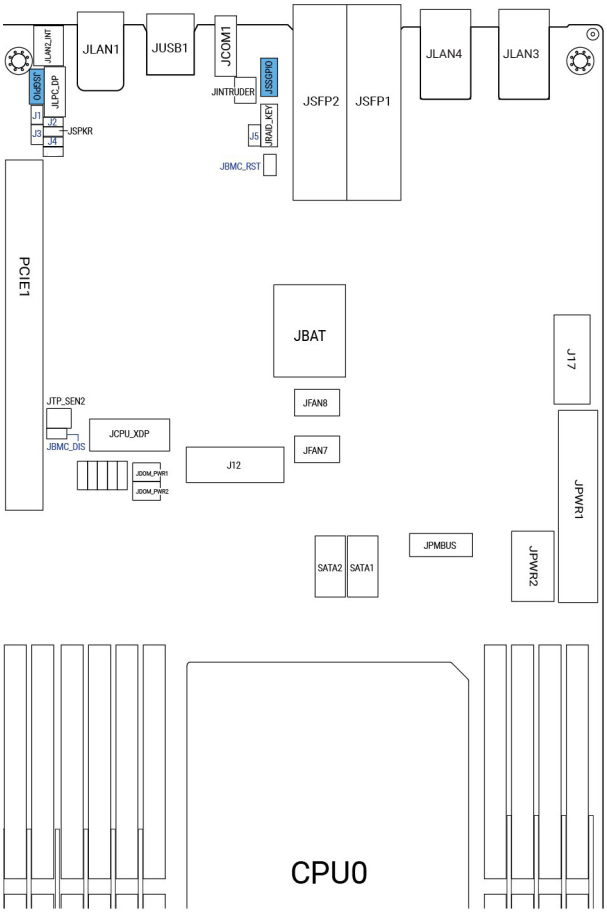


PCH SGPIO Header (JSGPIO, JSSGPIO)

This is a 6-pin connector that is used to control general device data.

1	GND
2	DATA1
3	DATA0
4	LOAD
5	CLOCK
6	+3.3V

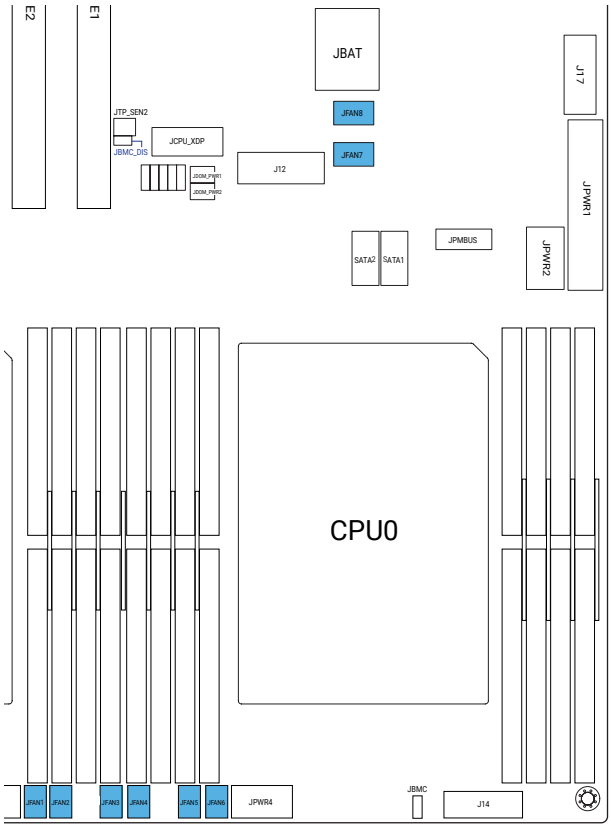




FAN Header (JFAN1~8)

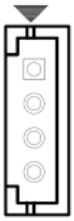
This is a 4-pin wafer that connects fan to motherboard.

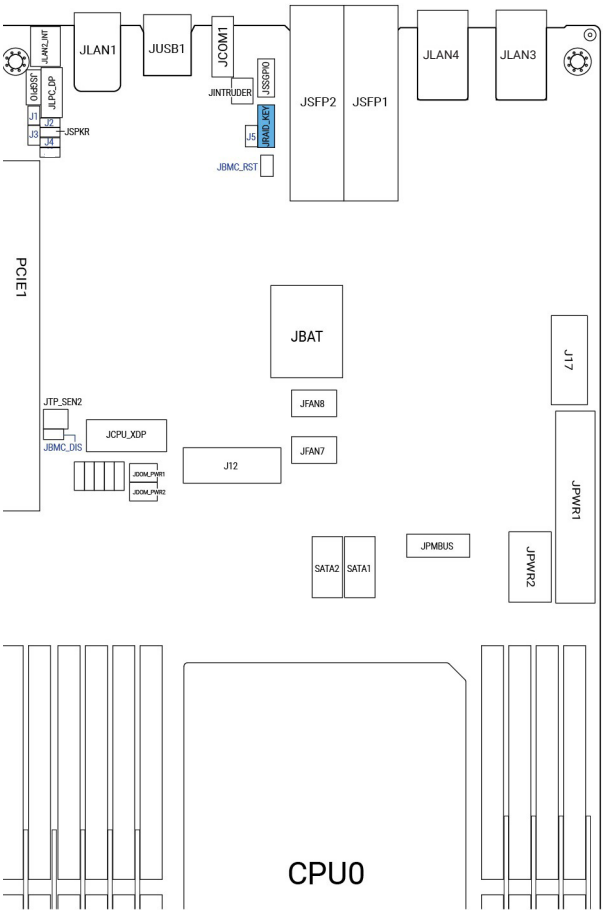
1	GND
2	+12V
3	TACH
4	PWM



VROC KEY Box Header (JRAID_KEY)
This is a 4-pin key that supports VROC (Intel® Virtual RAID on CPU), specifically used for NVMe SSDs.

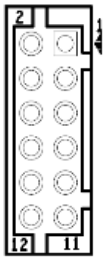
1	GND
2	KEY1
3	GND
4	KEY2

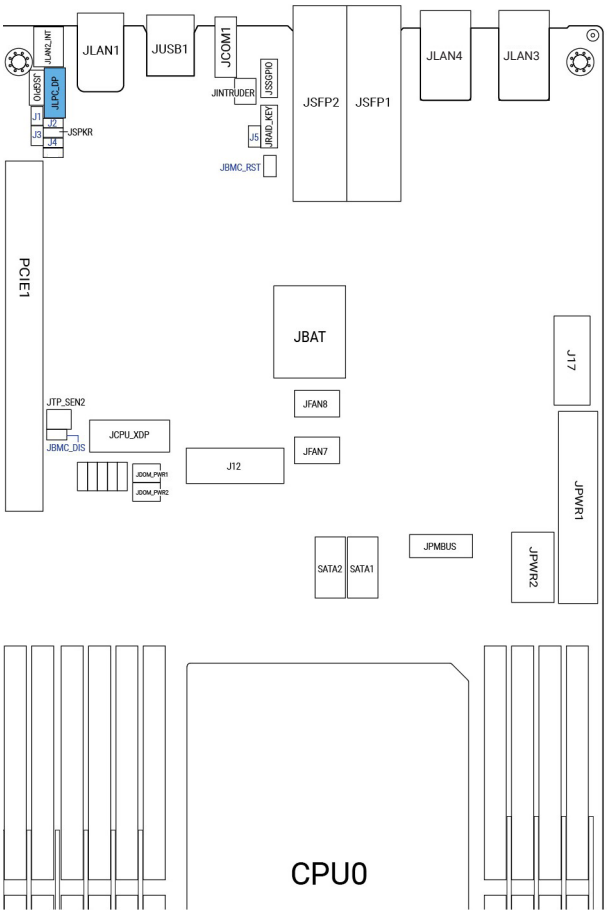




LPC Debug Port Header (JLPC_DP)
This is a 2x6-pin header for low pin count debug.

CLK_24M	2	1	GND
LFRAME_N	4	3	PIRQA
PLTRST_N	6	5	SERIRQ
LAD3	8	7	LAD2
+3.3V	10	9	LAD1
LAD0	12	11	GND

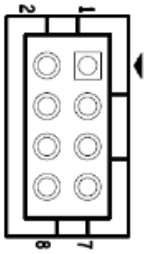


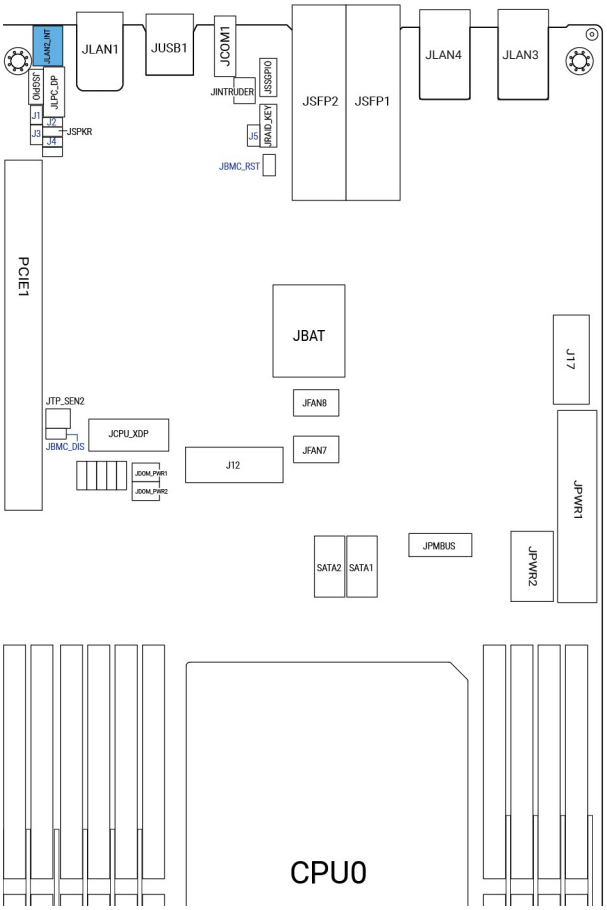


I210 MDI Box Header (JLAN2_INT)

This 2x4-pin header is used to provide I210 MDI(Media Dependent Interface) functionality.

MDI_DN2	2	1	MDI_DP3
MDI_DP2	4	3	MDI_DN3
MDI_DN1	6	5	MDI_DP0
MDI_DP1	8	7	MDI_DN0

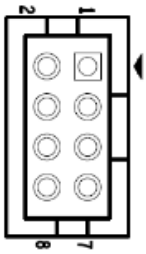


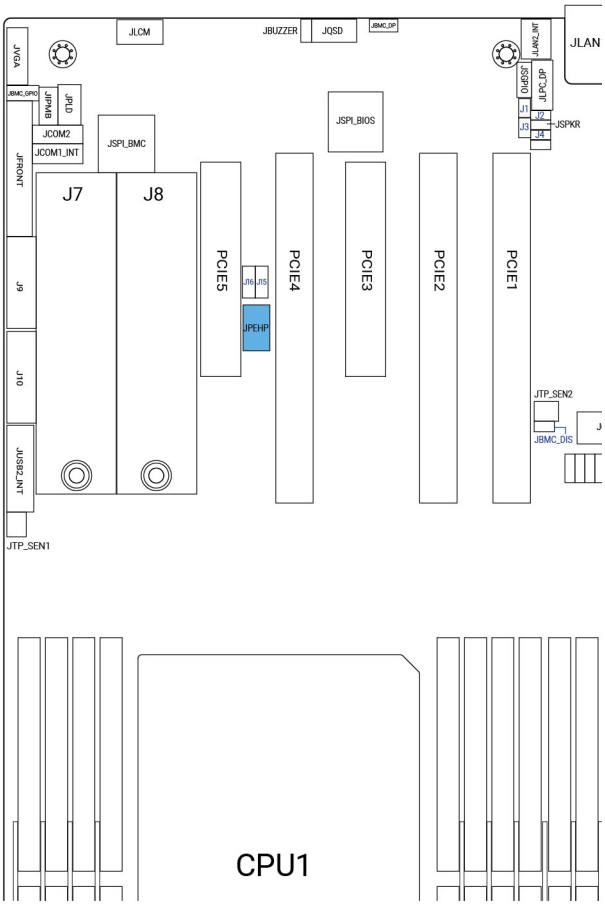


CPU PCIe Hot Plug Box Header (JPEHP)

This is a 2x4-pin header that provides CPU PCIe hot plug.

SMB_CPU1_SDA	2	1	SMB_CPU0_SDA
GND	4	3	GND
SMB_CPU1_SCL	6	5	SMB_CPU0_SCL
SMB_CPU1_ALERT#	8	7	SMB_CPU0_ALERT#

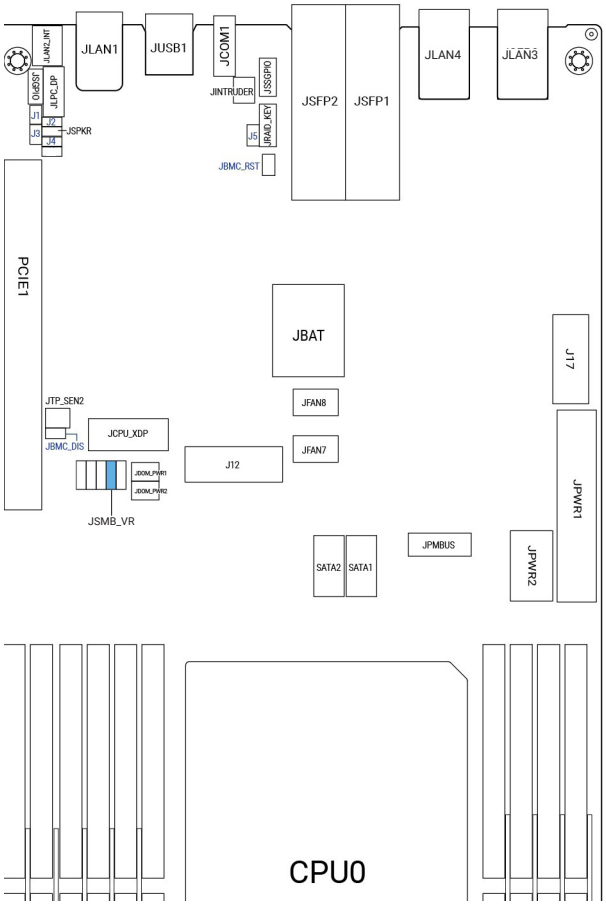




VRM SMB Header (JSMB_VR)

This is a 3-pin SMBus header that supports VRM (Voltage Regulator Module).

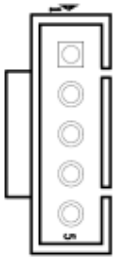
1	SMB_VR_DAT
2	GND
3	SMB_VR_CLK

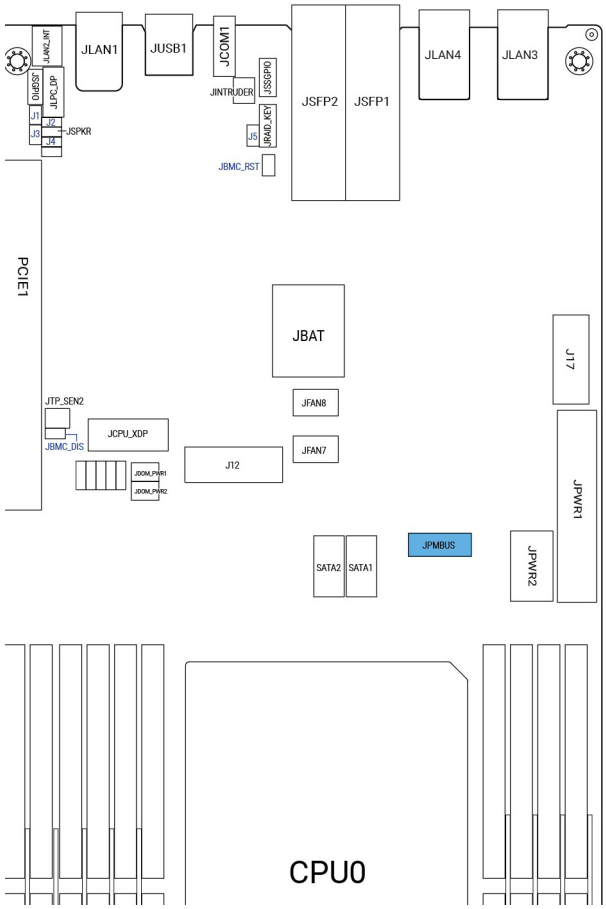


PMBUS Box Header (JPMBUS)

This is a 5-pin header that is used to provide PMBus functionality.

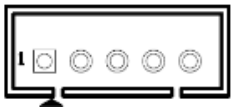
1	SMB_PMBUS_CLK
2	SMB_PMBUS_DATA
3	PMBUS_ALERT_N
4	GND
5	5VSB

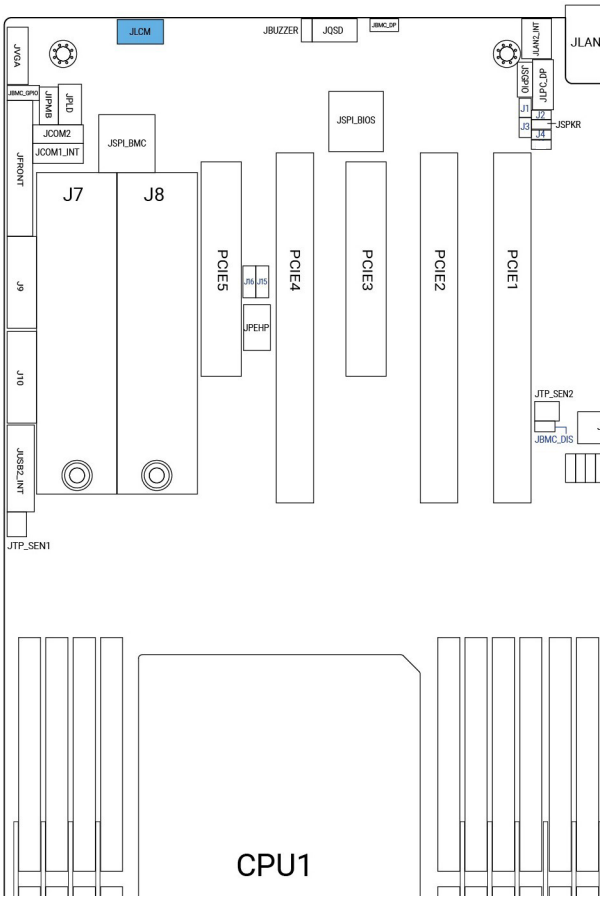




LCM Box Header (JLCM)
This is a 5-pin header that supports the LCM(LCD Module).

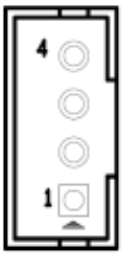
1	SW_PWR_BTN#
2	SW_RST_BTN#
3	TXD
4	RXD
5	GND

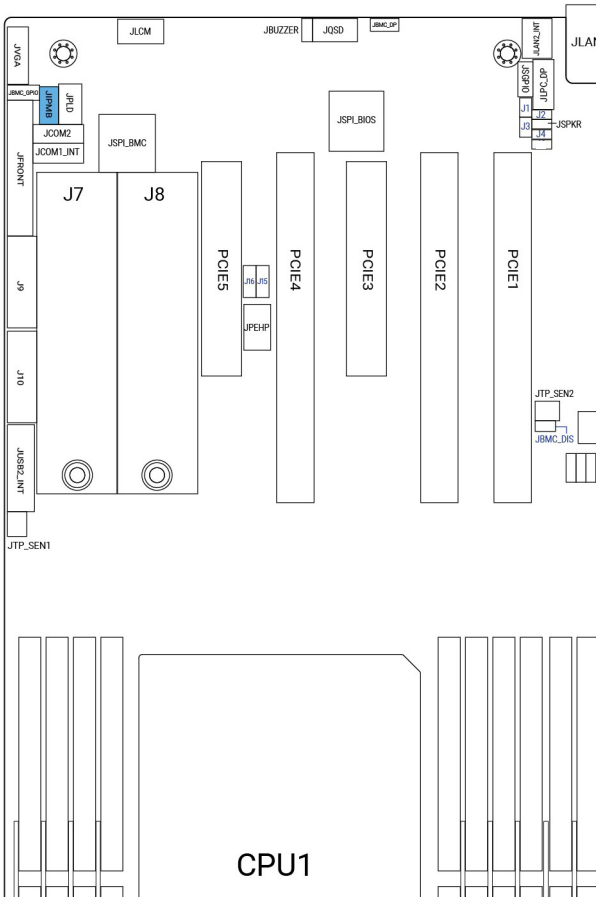




IPMB Box Header (JIPMB)
This is a 1x4-pin header is used to provide IPMB functionality.

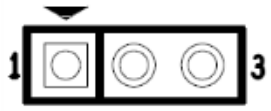
1	IPMB_SDA
2	GND
3	IPMB_SCL
4	N.C.

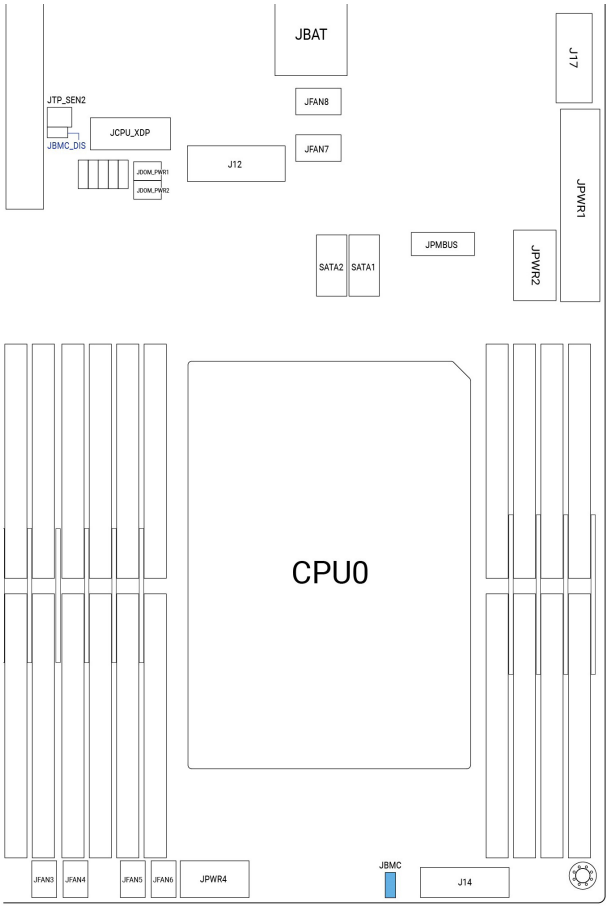




BMC I2C10 Box Header (JBMC)
This is a 1x6-pin header is used to provide BMC I2C10 management bus.

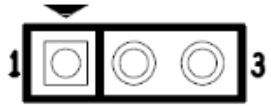
1	I2C10_SCL
2	I2C10_SDA
3	GND

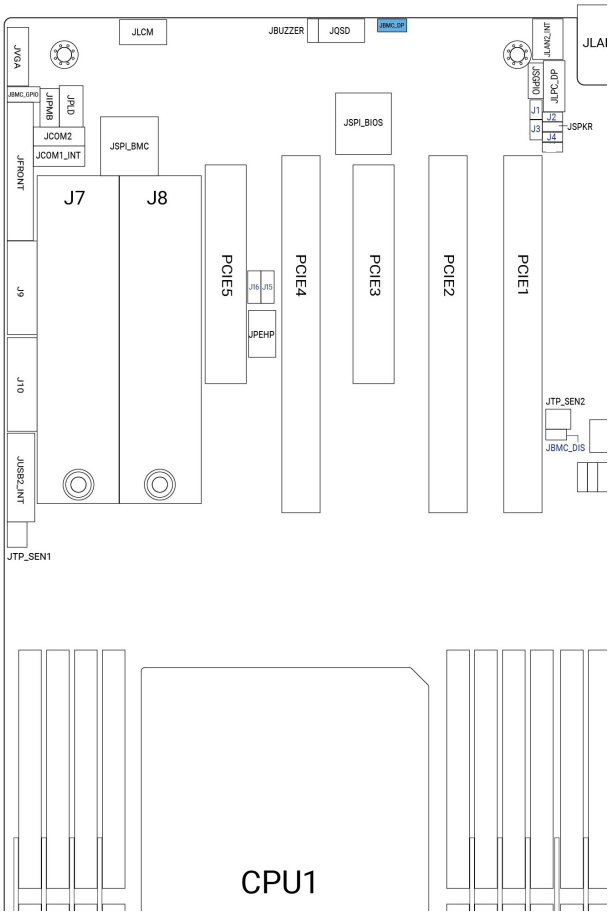




BMC Debug port Header (JBMC_DP)
This is a 3-pin connector that supports BMC debug.

1	SPE_TXD
2	SPE_RXD
3	GND

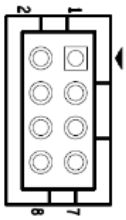


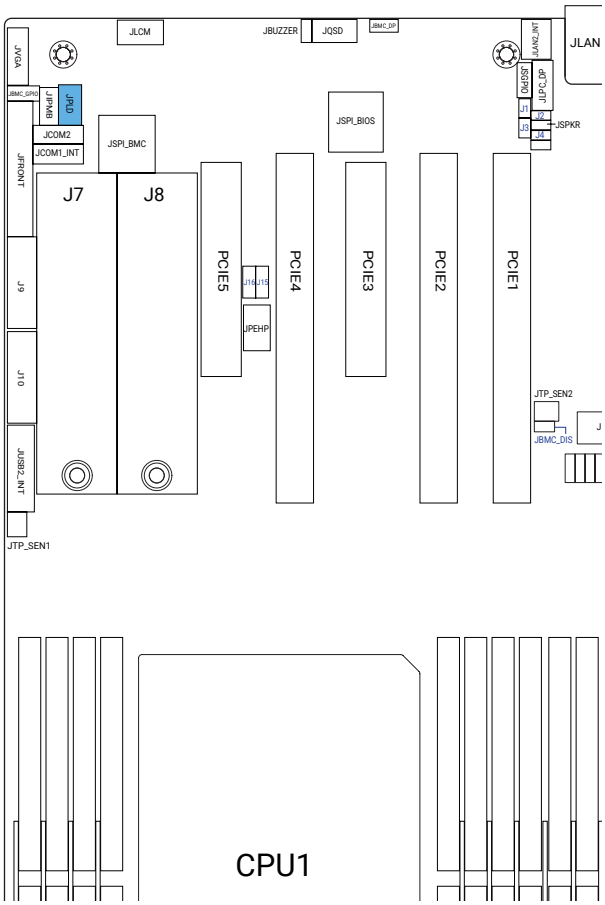


PLD Download Header (JPLD)

This 2x4-pin header is that supports PLD(Programmable Logical Device) download cable.

GND	2	1	JTAG_TCK
+3.3V_DUAL	4	3	JTAG_TDO
JTAG_EN	6	5	JTAG_TMS
FORCE_EN	8	7	JTAG_TDI

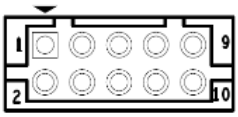


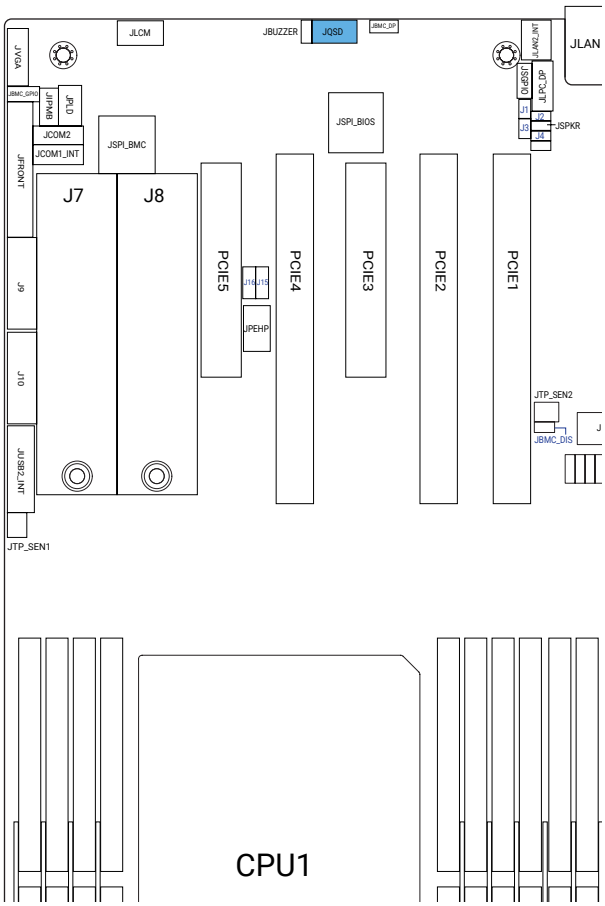


PLD QSD Header (JQSD)

This is a 2x5-pin header that supports PLD(Programmable Logical Device) debug.

+3.3V_DUAL	2	1	QSD_CLK
GND	4	3	QSD_LD#
SMB_SCL	6	5	QSD_DI
SMB_SDA	8	7	QSD_DO
MCU_PRSNT#	10	9	GND

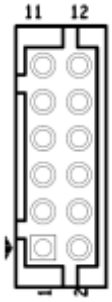


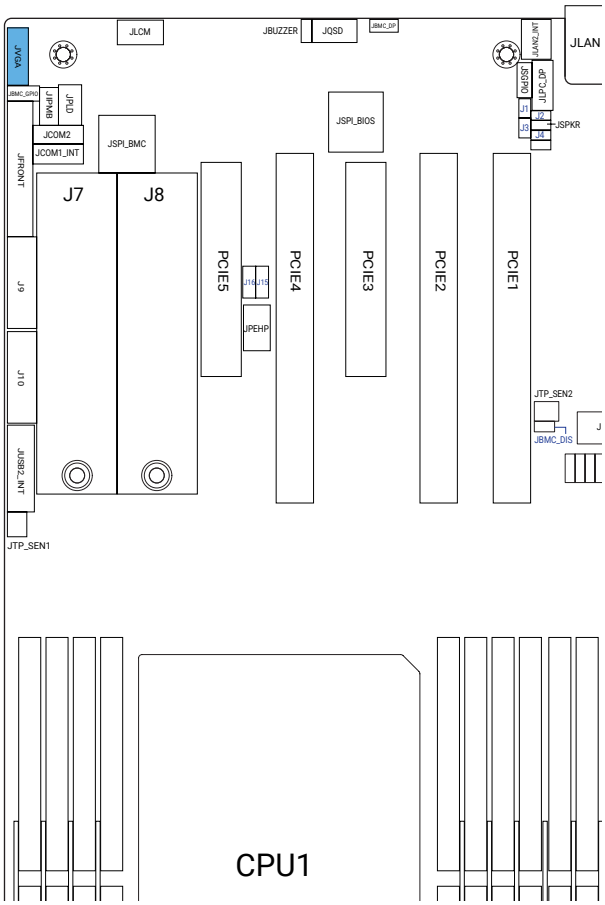


VGA Box Header (JVGA)

This is a 1x6-pin header is used to provide VGA functionality.

GND	2	1	+5V
RED	4	3	GND
GND	6	5	DDC_SDA
GREEN	8	7	VSYNC
GND	10	9	HSYNC
BLUE	12	11	DDC_SCL

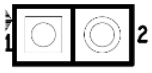




PCH Speaker Header (JSPKR)

This connector is a 2 x 1 Pin header.

1	+5V
2	SPKR



BMC Buzzer Header (JBUZZER)

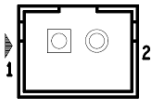
This connector is a 2 x 1 Pin header.

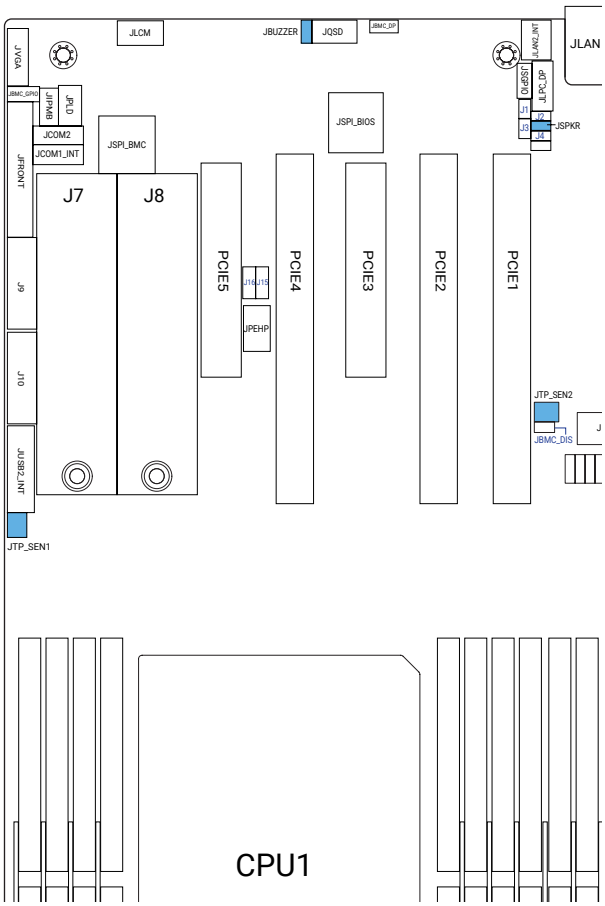
1	+5V
2	BUZZER

External Thermal Sensor Header (JTP_SEN1, JTP_SEN2)

This connector is a 2 x 1 Pin header.

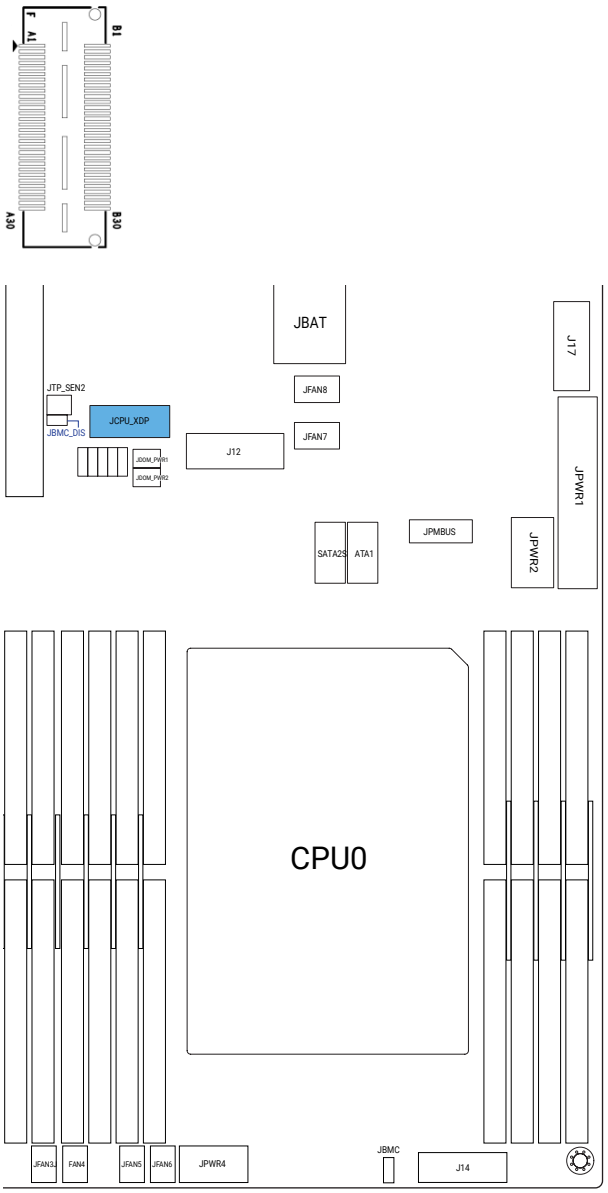
1	TD+
2	TD-





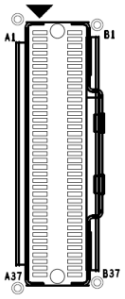
CPU XDP Header (JCPU_XDP)
This is a 2 x 30 Pin header that is used to provide CPU XDP functionality.

P1V05_PCH	A1	B1	XDP_TMS
XDP_TCK	A2	B2	XDP_TDO
XDP_TDI	A3	B3	XDP_PCH_SYSRST#
XDP_ITP_PMODE	A4	B4	XDP_TRST
XDP_CPU_TRST_N	A5	B5	XDP_PREQ_N
XDP_PRDY_N	A6	B6	PVCCIO_CPU0
XDP_CPU0_PTI0_CLK	A7	B7	XDP_CPU1_PTI0_CLK
XDP_SPI_PCH_IO2	A8	B8	GND
XDP_PRESENT_N	A9	B9	XDP_CPU1_PTI0
XDP_CPU0_PTI0	A10	B10	XDP_CPU1_PTI1
XDP_CPU0_PTI1	A11	B11	XDP_CPU1_PTI2
XDP_CPU0_PTI2	A12	B12	XDP_CPU1_PTI3
XDP_CPU0_PTI3	A13	B13	XDP_CPU1_PTI4
XDP_CPU0_PTI4	A14	B14	XDP_CPU1_PTI5
XDP_CPU0_PTI5	A15	B15	XDP_CPU1_PTI6
XDP_CPU0_PTI6	A16	B16	XDP_CPU1_PTI7
XDP_CPU0_PTI7	A17	B17	N.C.
XDP_CPU0_PTI8	A18	B18	XDP_SYSPWROK
XDP_CPU0_PTI9	A19	B19	CPU_PWR_DEBUG_N
XDP_CPU0_PTI10	A20	B20	XDP_PWRBTN_N
XDP_CPU0_PTI11	A21	B21	RST_RSMRST_N
XDP_CPU0_PTI12	A22	B22	N.C.
XDP_CPU0_PTI13	A23	B23	N.C.
XDP_CPU0_PTI14	A24	B24	SMB_HOST_3V3_CLK
XDP_CPU0_PTI15	A25	B25	SMB_HOST_3V3_DAT
JTAG_SSB_TCK	A26	B26	N.C.
XDP_CPU_MBP_N3	A27	B27	N.C.
XDP_CPU_MBP_N2	A28	B28	N.C.
GND	A29	B29	GND
XDP_CPU0_PTI1_CLK	A30	B30	N.C.



SFF-8654 Connector (PCIe 4.0)
(J9, J10, J13, J14, J17)
This 2 x 37 Pin header is used to provide PCIe 4.0 SSD functionality.

GND	A1	B1	GND
RX0+	A2	B2	TX0+
RX0-	A3	B3	TX0-
GND	A4	B4	GND
RX1+	A5	B5	TX1+
RX1-	A6	B6	TX1-
GND	A7	B7	GND
N.C.	A8	B8	PEHP_SCL
N.C.	A9	B9	PEHP_SDA
GND	A10	B10	GND
CLK0+	A11	B11	PERST0#
CLK0-	A12	B12	N.C.
GND	A13	B13	GND
RX2+	A14	B14	TX2+
RX2-	A15	B15	TX2-
GND	A16	B16	GND
RX3+	A17	B17	TX3+
RX3-	A18	B18	TX3-
GND	A19	B19	GND
RX4+	A20	B20	TX4+
RX4-	A21	B21	TX4-
GND	A22	B22	GND
RX5+	A23	B23	TX5+
RX5-	A24	B24	TX5-
GND	A25	B25	GND
N.C.	A26	B26	PEHP_ALERT#
N.C.	A27	B27	N.C.
GND	A28	B28	GND
CLK1+	A29	B29	PERST1#
CLK1-	A30	B30	N.C.
GND	A31	B31	GND
RX6+	A32	B32	TX6+
RX6-	A33	B33	TX6-
GND	A34	B34	GND
RX7+	A35	B35	TX7+
RX7-	A36	B36	TX7-
GND	A37	B37	GND



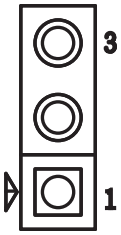
SFF-8654 Connector (PCIe 3.0/SATA3) (J12)
This 2 x 37 Pin header is used to provide PCIe 3.0/SATA3 SSD functionality.

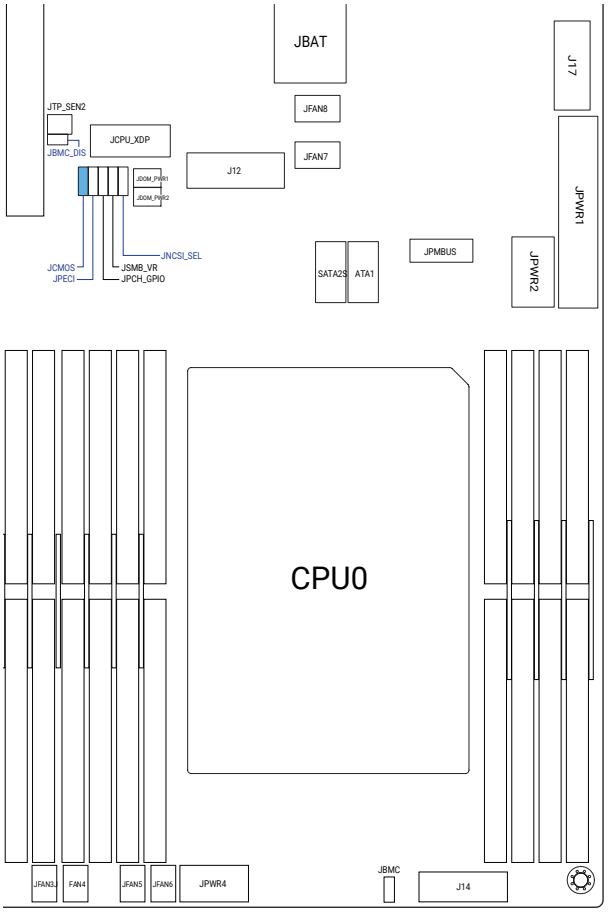
GND	A1	B1	GND
RX0+/RX+	A2	B2	TX0+/TX+
RX0-/RX-	A3	B3	TX0-/TX-
GND	A4	B4	GND
RX1+/RX+	A5	B5	TX1+/TX+
RX1-/RX-	A6	B6	TX1-/TX-
GND	A7	B7	GND
N.C.	A8	B8	SMB_SCL
N.C.	A9	B9	SMB_SDA
GND	A10	B10	GND
CLK0+	A11	B11	PERST0#
CLK0-	A12	B12	N.C.
GND	A13	B13	GND
RX2+/RX+	A14	B14	TX2+/TX+
RX2-/RX-	A15	B15	TX2-/TX-
GND	A16	B16	GND
RX3+/RX+	A17	B17	TX3+/TX+
RX3-/RX-	A18	B18	TX3-/TX-
GND	A19	B19	GND
RX4+/RX+	A20	B20	TX4+/TX+
RX4-/RX-	A21	B21	TX4-/TX-
GND	A22	B22	GND
RX5+/RX+	A23	B23	TX5+/TX+
RX5-/RX-	A24	B24	TX5-/TX-
GND	A25	B25	GND
N.C.	A26	B26	SMB_SCL
N.C.	A27	B27	SMB_SDA
GND	A28	B28	GND
CLK1+	A29	B29	PERST1#
CLK1-	A30	B30	N.C.
GND	A31	B31	GND
RX6+/RX+	A32	B32	TX6+/TX+
RX6-/RX-	A33	B33	TX6-/TX-
GND	A34	B34	GND
RX7+/RX+	A35	B35	TX7+/TX+
RX7-/RX-	A36	B36	TX7-/TX-
GND	A37	B37	GND

3.6 Jumper Setting

CMOS Jumper (JCMOS)
This is a 3-pin jumper that resets BIOS changes to default value.

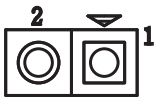
JCMOS	Setting	
Pin1-2	Normal	Default
Pin2-3	Clear CMOS	

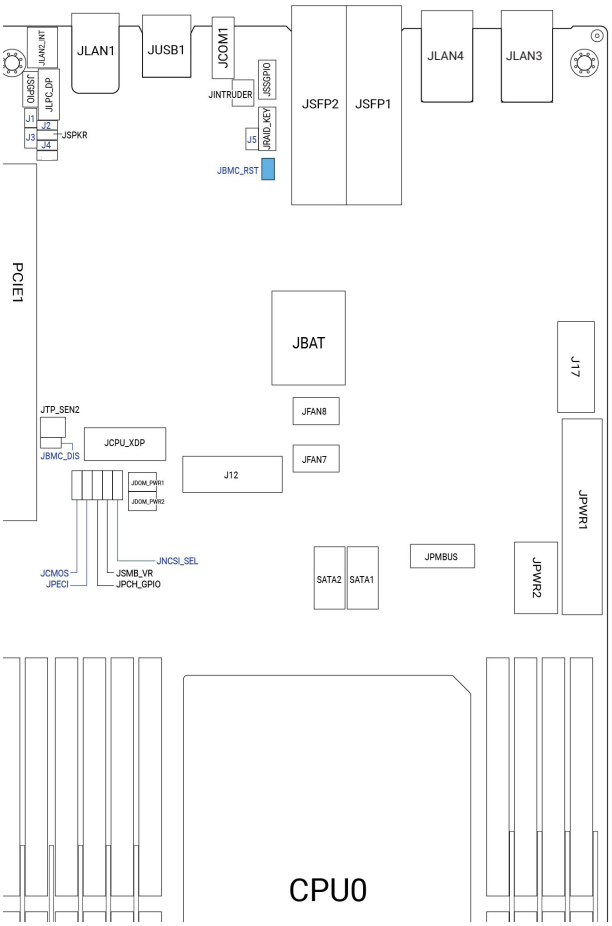




BMC Reset Jumper (JBMC_RST)
This is a 2-pin jumper that reboots the BMC.

JBMC_RST	Setting	
Short	Reset BMC	
Open	Normal	Default

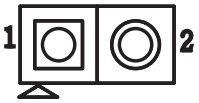


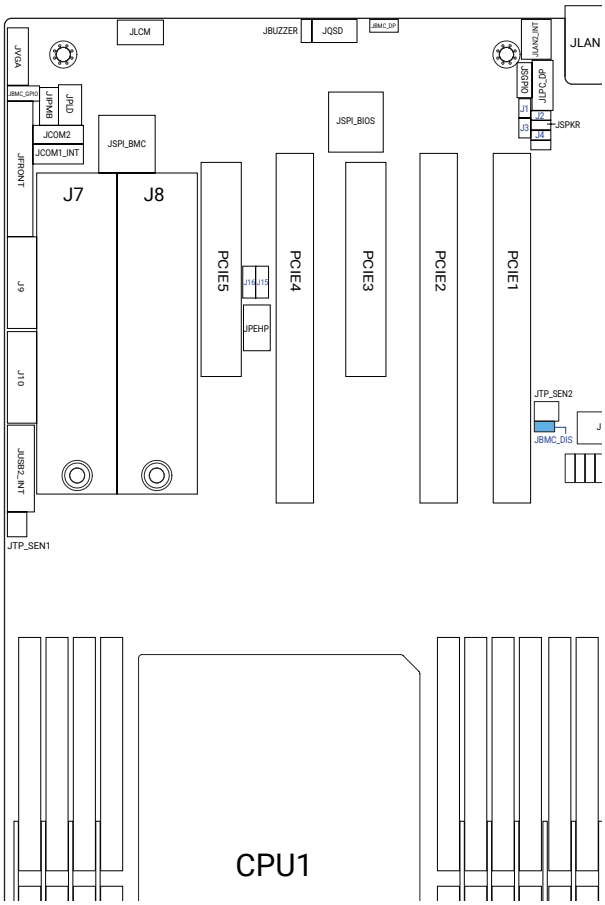


BMC ARM Disable Jumper (JBMC_DIS)

This is a 2-pin jumper that disables BMC ARM support.

JBMC_DIS	Setting	
Short	Disable	
Open	Normal	Default

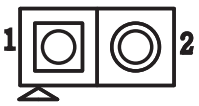


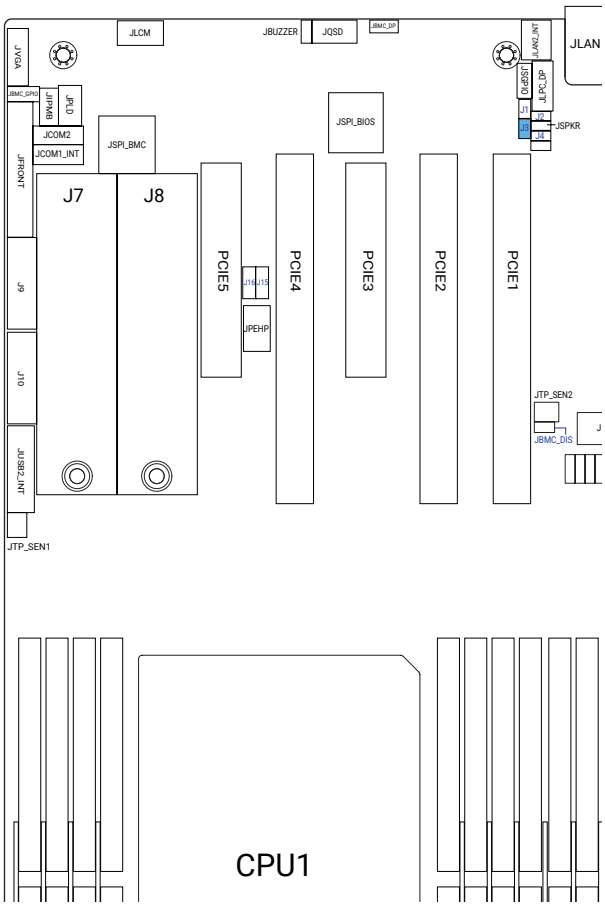


ME Force Recovery Mode Jumper (J3)

This is a 2-pin jumper that enables ME firmware to recovery mode.

J3	Setting	
Short	ME Recovery Mode	
Open	Normal	Default

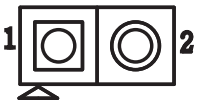


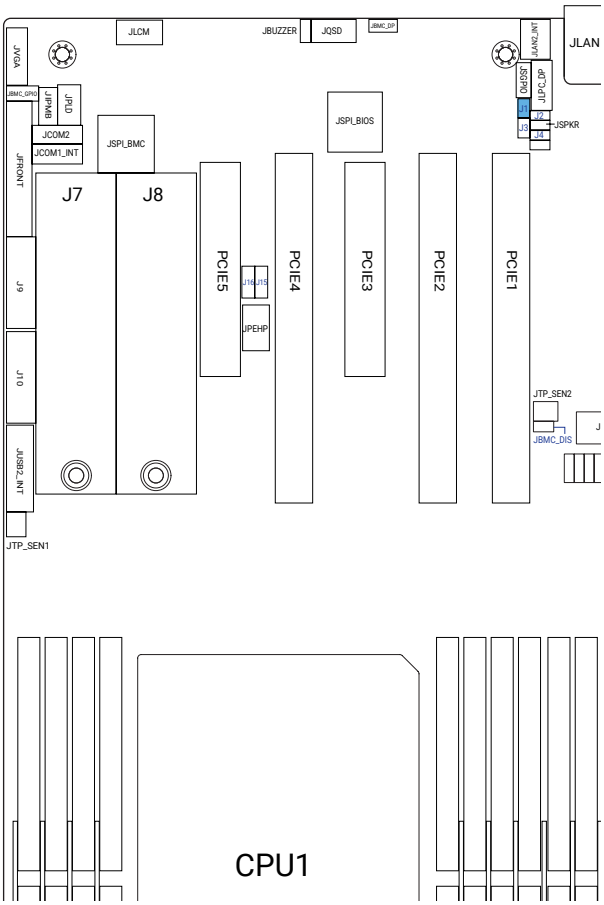


No Reboot (Watch Dog) Jumper (J1)

This is a 2-pin jumper that enables the watchdog timer without reboot.

J1	Setting	
Short	Enable	
Open	Disable	Default

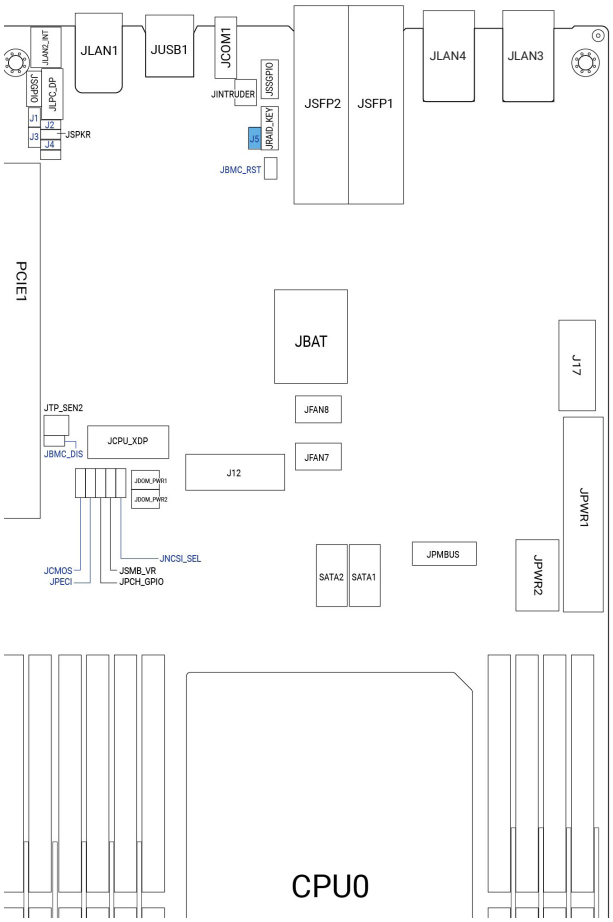




Flash Descriptor Security override Jumper (J5)

This is a 2-pin jumper that enables the override of flash descriptor.

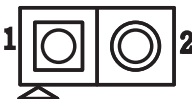
J5	Setting	
Short	Flash Security override	
Open	Normal	Default

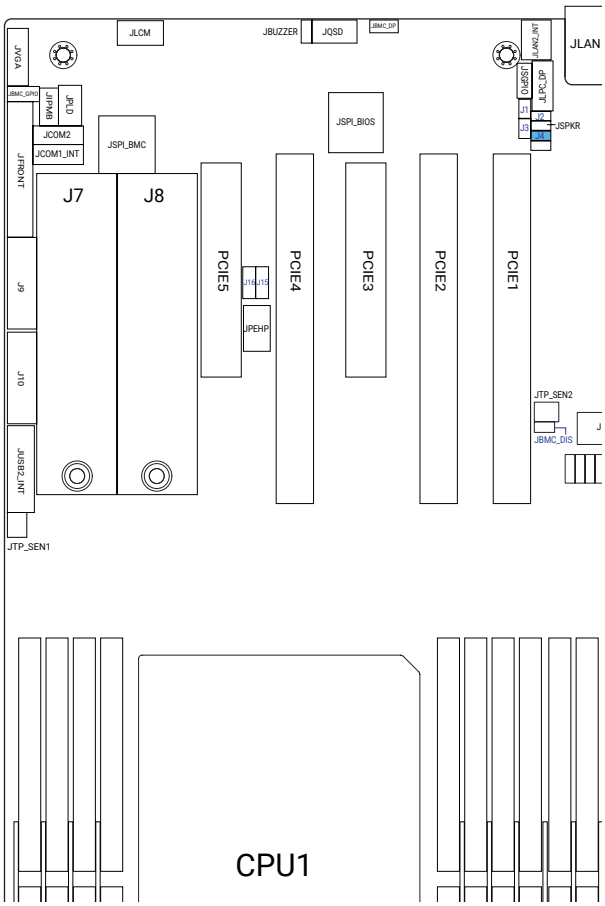


BMC SoC Flash Configuration Jumper (J4)

This is a 2-pin jumper that enables BMC SOC Flash.

J4	Setting	
Short	Enable	
Open	Disable	Default

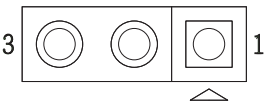


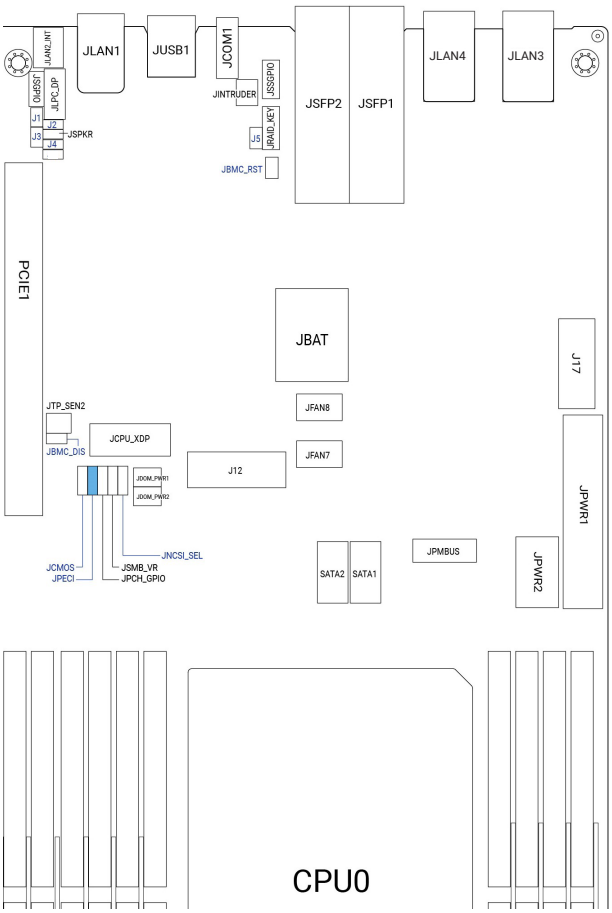


PECI Master Select Jumper (JPECI)

This is a 3-pin jumper that enables PECI access to BMC for DTS (Digital Thermal Sensor).

JPECI	Setting	
Pin1-2	PCH	Default
Pin2-3	BMC	

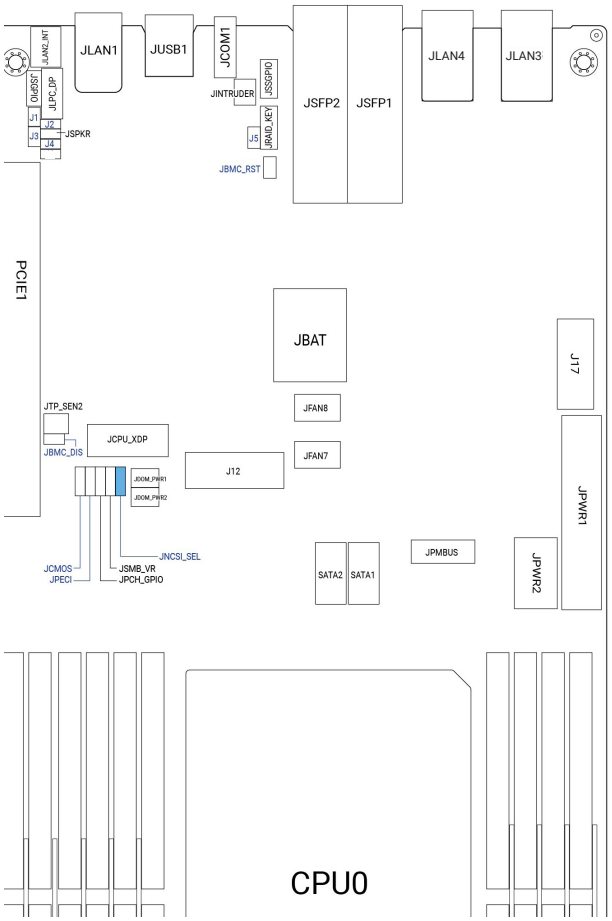




BMC NCSI Select Jumper (JNCSI_SEL)

This is a 3-pin jumper that enables connection between BMC and other NICs.

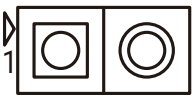
JNCSI_SEL	Setting	
Pin 1-2	I210	Default
Pin 2-3	BCM57416	

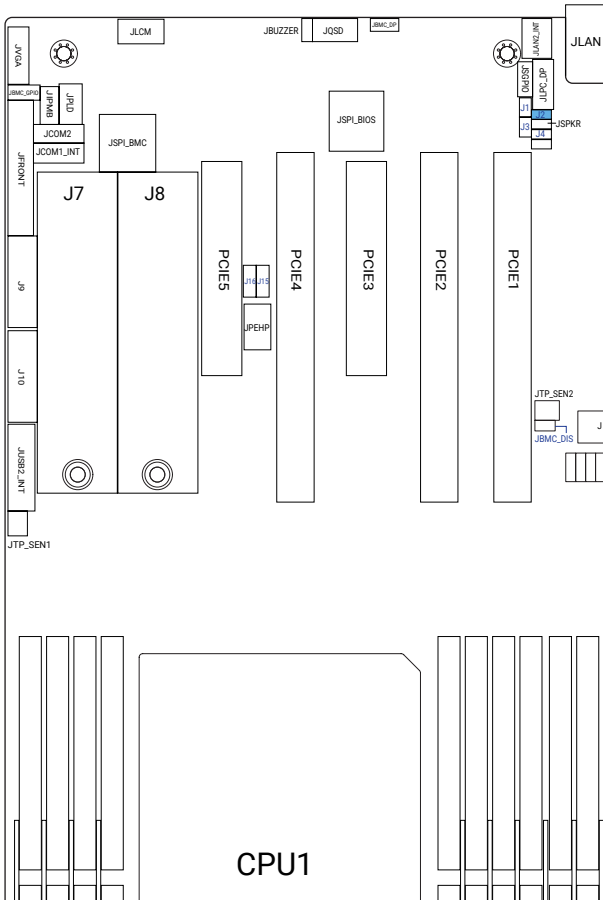


BMC Debug Port Select Jumper (J2)

This is a 2-pin jumper that configures BMC debug port.

J2	Setting	
Short	JCOM1	
Open	JBMC_DP	Default

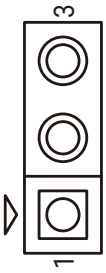


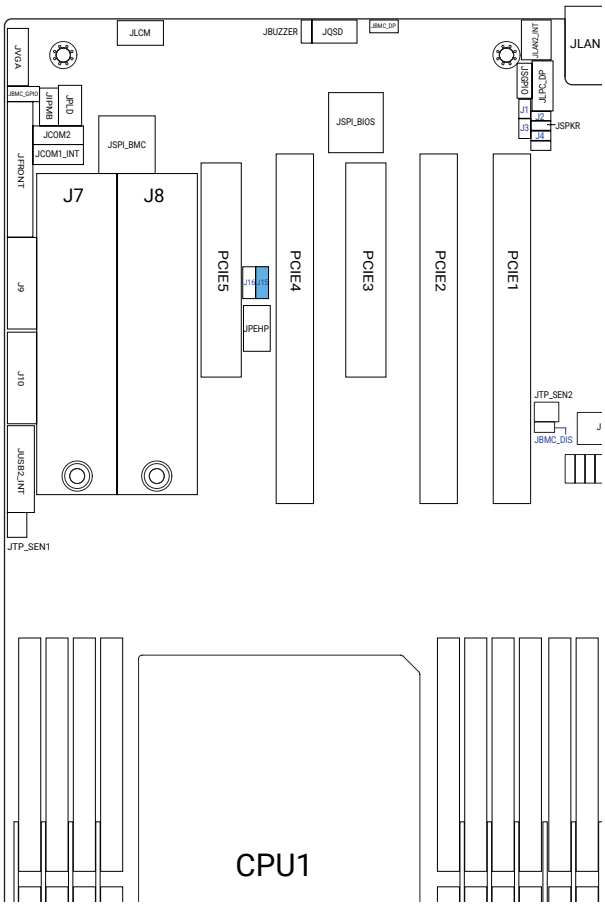


J12 SSD1 PCIE/SATA Select Jumper (J15)

This is a 3-pin jumper that configures PCIE/SATA SSD1.

J15	Setting	
Pin1-2	SATA	Default
Pin2-3	PCIe X4	

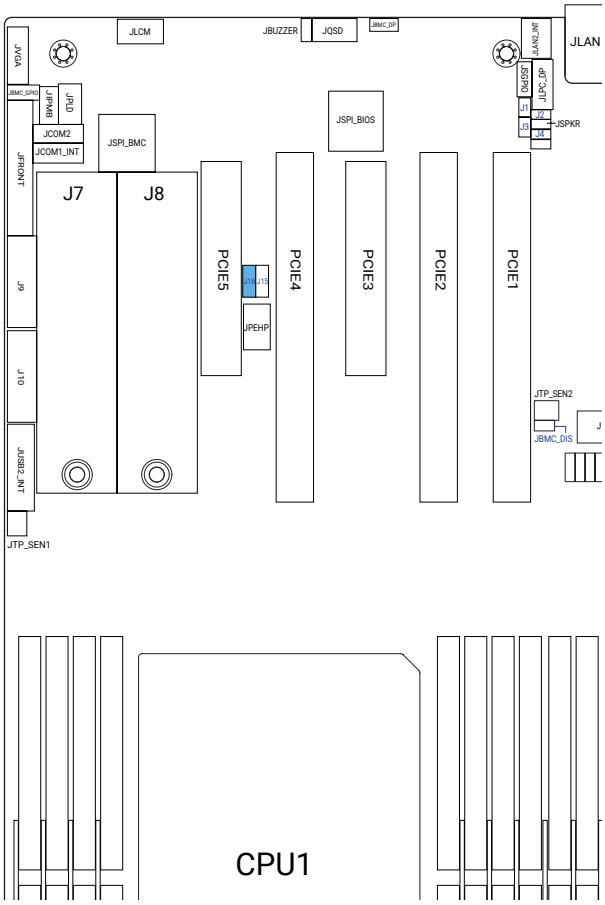




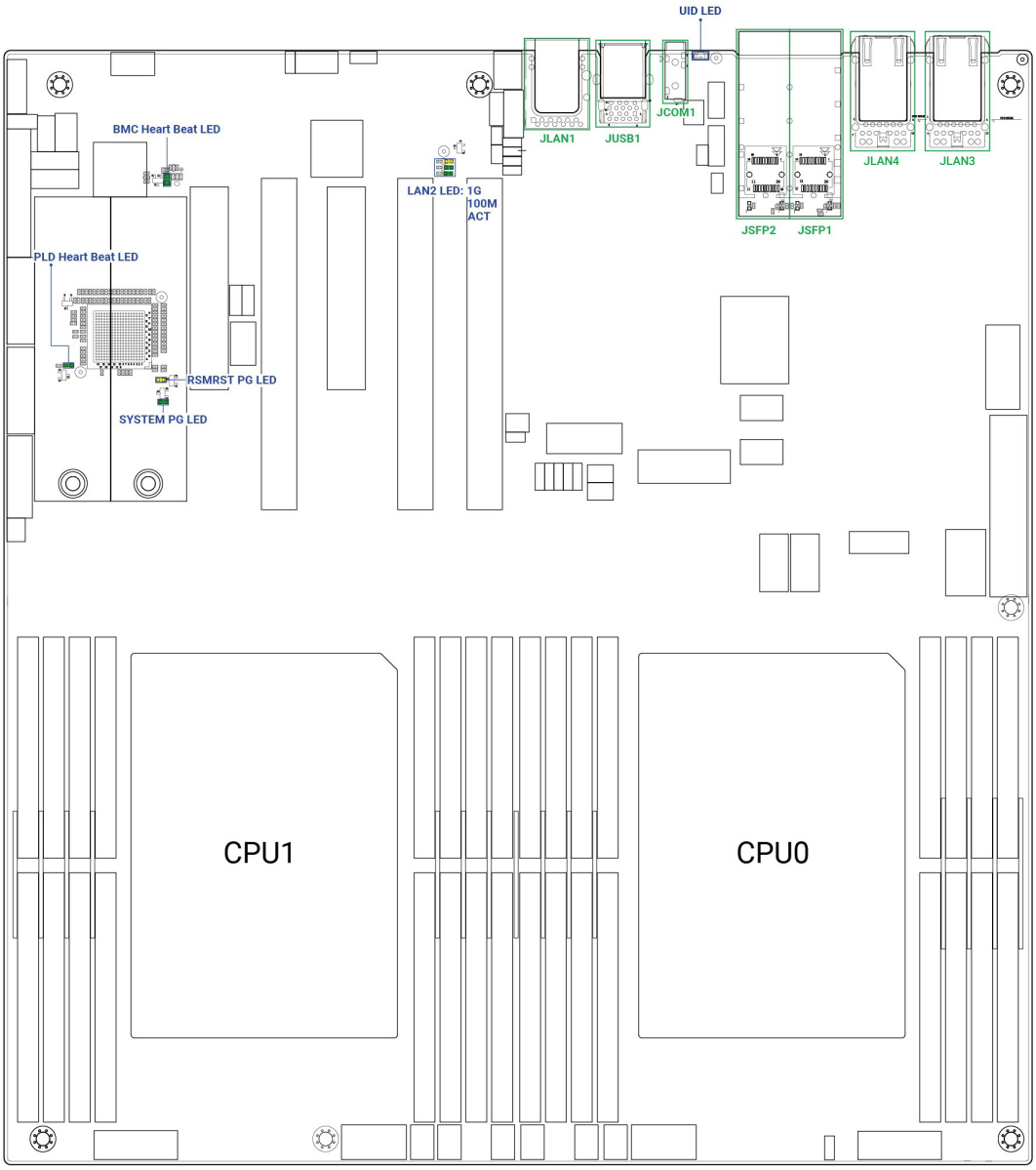
J12 SSD2 PCIE/SATA Select Jumper (J16)

This is a 3-pin jumper that configures PCIE/SATA SSD2.

J16	Setting	
Pin1-2	SATA	Default
Pin2-3	PCIe X4	



3.7 Internal LED



Item	Color	Behavior
BMC HEART BEAT LED	Green (Blinking)	BMC activity is detected.
	Green	BMC is not active.
PLD HEART BEAT LED	Green (Blinking)	PLD activity is detected.
SYSTEM PG LED	Green	System power good is ready.
	Off	System power good is not ready.
RSMRST PG LED	Yellow	Resume Well Reset is ready.
	Off	Resume Well Reset is not ready.
LAN2 LED	Yellow (LED7)	Link speed: 1G.
	Green (LED8)	Link speed: 100M.
	Green (LED6)	LAN is active. (Blinking)

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.
< F5> < F6 >	Change values.
< F7 >	Discard Change and Exit.
< F9 >	Load Optimal Default for all values.
< F10 >	Save changes and exit.
< F12 >	Print Screen.
< Esc >	Exit the current menu screen.

4.2 BIOS Setup

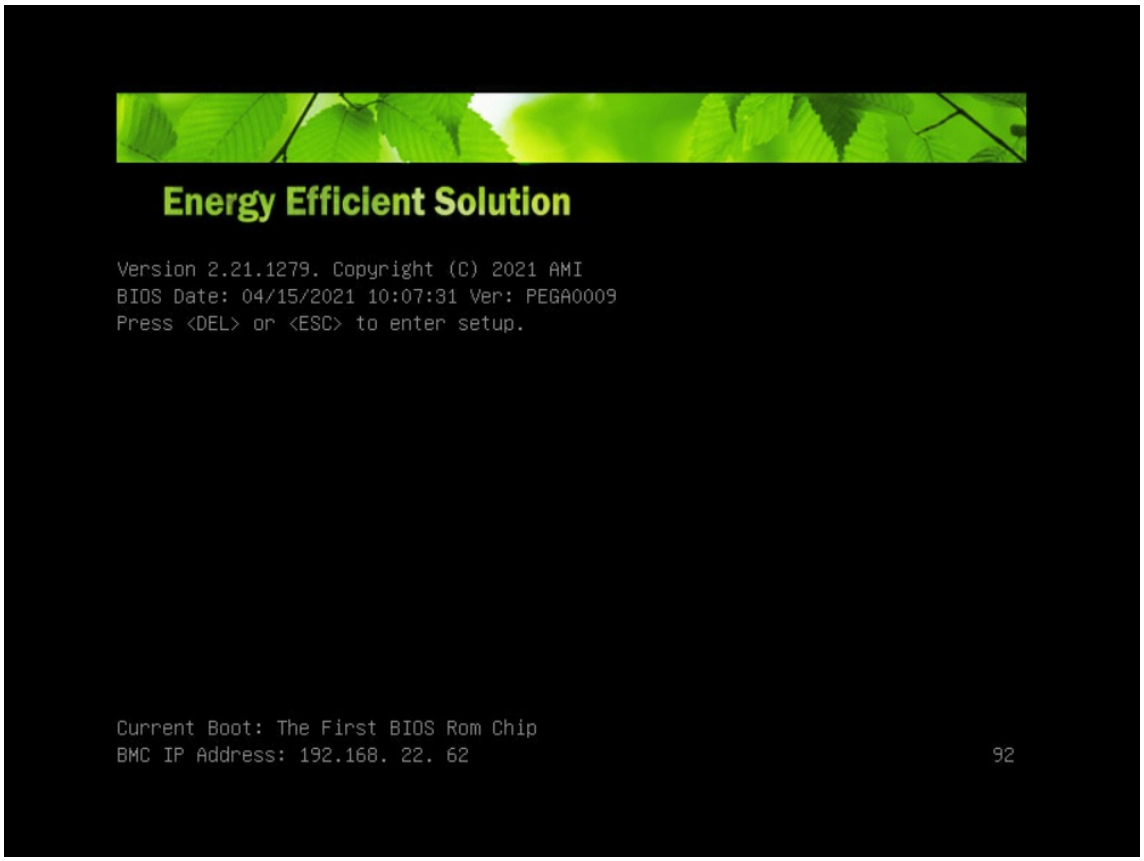
4.2.1 Menu

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

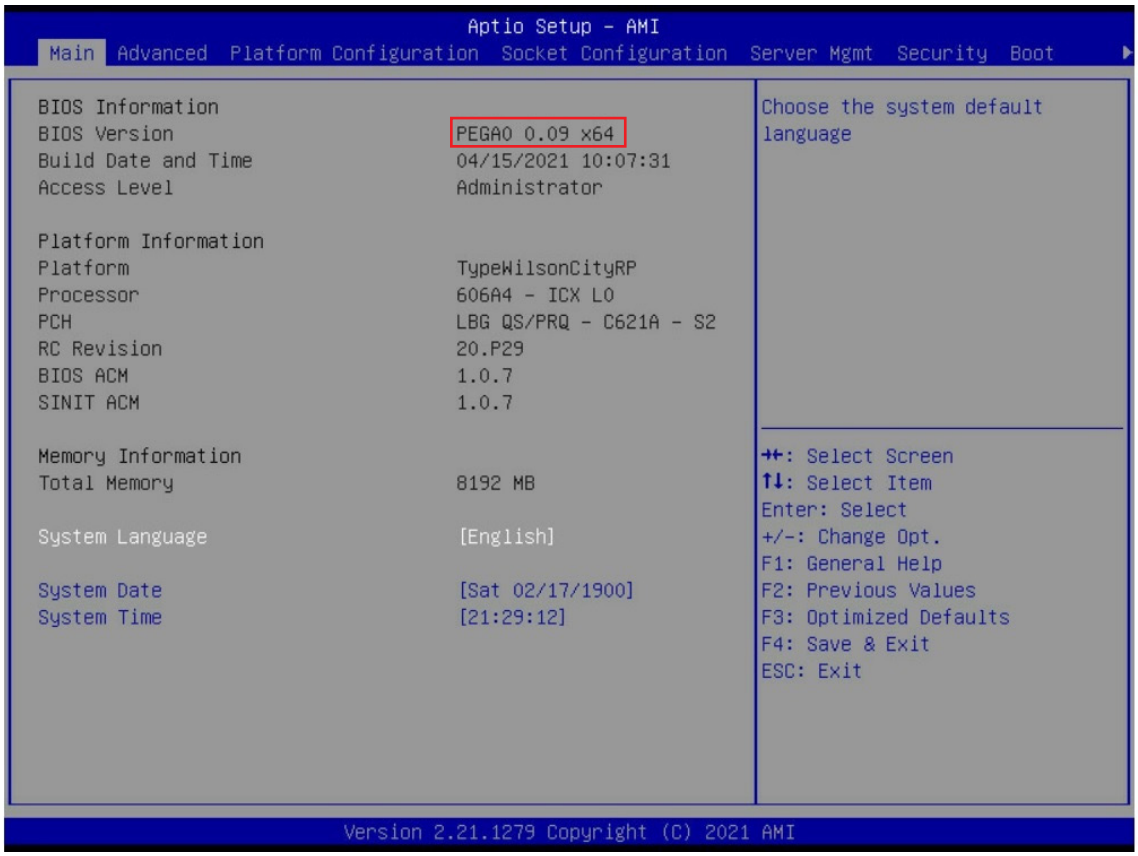
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Platform Configuration	Allows configuration of platform settings such as PCH, miscellaneous, and server ME configuration.
Socket Configuration	Allows configuration of socket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



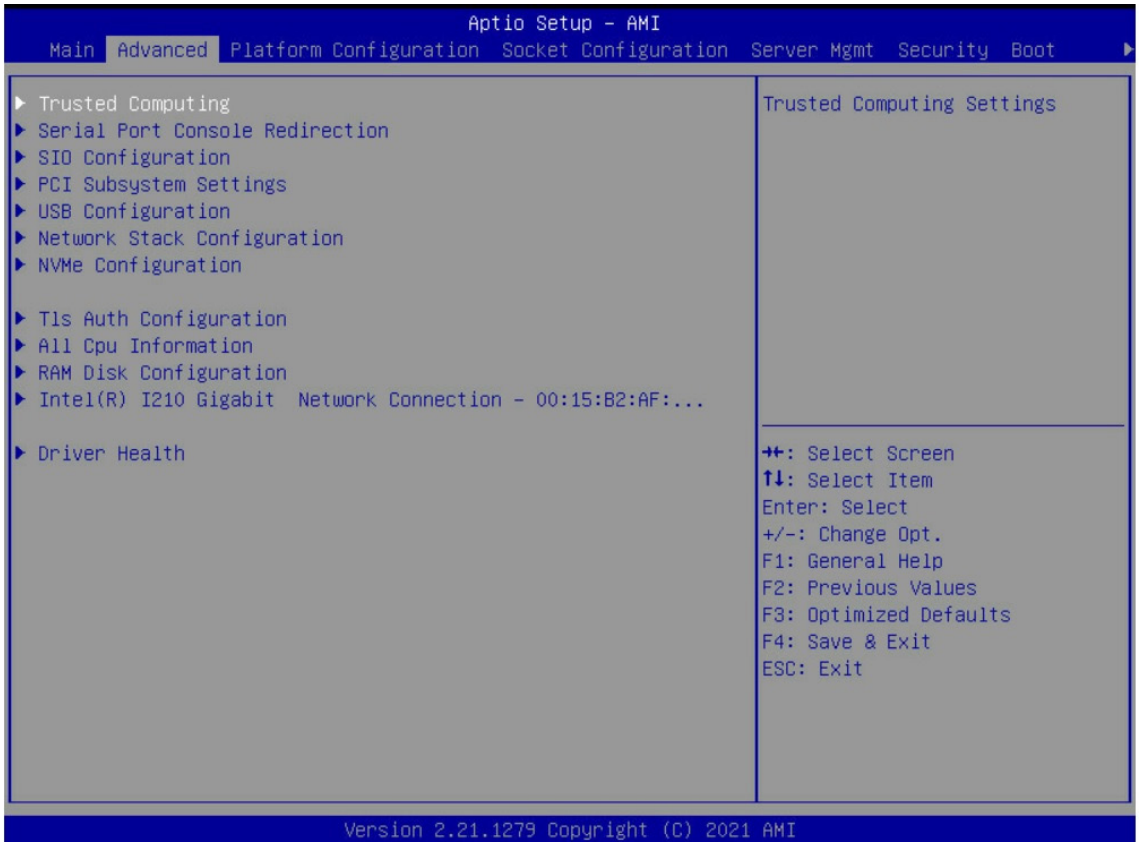
4.3 Main



4.3.1 Main

Main	
System Language	Configures the language used in the system.
System time	Configures the current time.
System date	Configures the current date.

4.4 Advanced



4.4.1 Trusted Computing

Trusted Computing Settings.

Trusted Computing			
Security Device Support	Enables/disables BIOS support for security device.		
	▶Enable	Disable	
SHA-1/256/384 PCR Bank	Enables/disables SHA-1/SHA-256/SHA-384 PCR Bank.		
	▶Enable	Disable	
Pending opertation	Schedules an operation for the security deivce. NOTE: Your computer will reboot during restart in order to change the state of the security device.		
	▶None	TPM Clear	
Platform Hierarchy	Enables/disables platform hierarchy.		
	▶Enable	Disable	
Storage Hierarchy	Enables/disables storage hierarchy.		
	▶Enable	Disable	
Endorsement Hierarchy	Enables/disables endorsement hierarchy.		
	▶Enable	Disable	
TPM 2.0 UEFI Spec Version	Select the TCG2 spec version support. • TCG_1_2: The compatible mode for Win8/10. • TCG_2: Support new TCG2 protocol and event format for win10 or later.		
	TCG_1_2	▶TCG_2	
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: TPM 1.2 will restrict support to TPM 1.2 devices. • TPM 2.0: TPM 2.0 will restrict support to TPM 2.0 devices. • Auto: Auto will support both with the defualt set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.		
	▶None	TPM 1.2	TPM 2.0

4.4.2 Serial Port Console Redirection

Serial Port Console Redirection.

Serial Port Console Redirection			
Console Redirection	Enables/disables console redirection.		
	Enable	Disable	
Legacy Console Redirection Settings	Redirection COM Port	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.	
		▶COM0	COM1
	Resolution	On Legacy OS, the number of rows and columns supported redirection.	
		▶80x24	80x25
	Redirect After POST	• When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy O.S. • When Always Enable is selected, then Legacy Console Redirection is enabled for legacy O.S.	
		▶Always Enable	Bootloader

4.4.3 SIO Configuration

SIO Configuration.

SIO Configuration				
[*Active*] Serial Port 1/2/3/4	Use this device	Enables/disables this logical device.		
		▶Enable	Disable	
	Possible	Allows the user to change the device user settings. New settings will be reflected on this setup page after system restarts.		
		Use Automatic Settings	IO=3F8h; IRQ=4: DMA;	IO=3F8h; IRQ=3, 4, 7, 10, 11, 12; DMA;
		IO=2F8h; IRQ=3, 4, 7, 10, 11, 12; DMA;	IO=3E8h; IRQ=3, 4, 7, 10, 11, 12; DMA;	IO=2E8h IRQ=3, 4, 7, 10, 11, 12; DMA;

4.4.4 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 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	

4.4.5 USB Configuration

USB Configuration Parameters.

USB Configuration				
XHCI Hand-off	This is a workaround for 0Ses without XHCI ownership change should be claimed by XHCI driver			
	▶Enable	Disable		
SB Mass Storage Driver Storage	Enables/disables USB Mass Storage Driver Support			
	▶Enable	Disable		
POST 60/64 Emulation	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware 0Ses.			
	▶Enable	Disable		
SB transfer time-out	The time-out value for control, bulk, and interrupt transfers.			
	1 sec	5 sec	10 sec	▶20 sec
Device reset time-out	USB mass storage device Start Unit command time-out.			
	10 sec	▶20 sec	30 sec	40 sec

Device power-up delay	Maximum time the device will take before it properly reports itself to the host controller. • Auto: For a root port, it is 100 ms; for a hub port, the delay is taken from hub descriptor.				
	▶Auto	Manual			
AMI Virtual CDROM0 1.00	Mass storage device emulation type. • Auto: Enumerates devices according to their media format. Optical drives are emulated as "CDROM," drives with not media will be emulated according to drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM
AMI Virtual HDisk0 1.00	Mass storage device emulation type. • Auto: Enumerates devices according to their media format. Optical drives are emulated as "CDROM," drives with not media will be emulated according to drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM

4.4.6 Network Stack Configuration

Network Stack Settings.

Network Stack Configuration		
Network Stack	Enables/disables UEFI Network Stack.	
	Enable	▶Disable

4.4.7 T1s Auth Configuration

Select T1s Auth Configuration.

T1s Auth Configuration			
Server CA Configuration	Configures server CA.		
	Enroll Cert	Enroll Cert Using File	Enroll Cert using file.
		Commit Changes and Exit	Commit changes and exit.
		Discard Changes and Exit	Discard changes and exit.
	Delete Cert		

4.4.8 RAM Disk Configuration

Adds/Removes RAM disks.

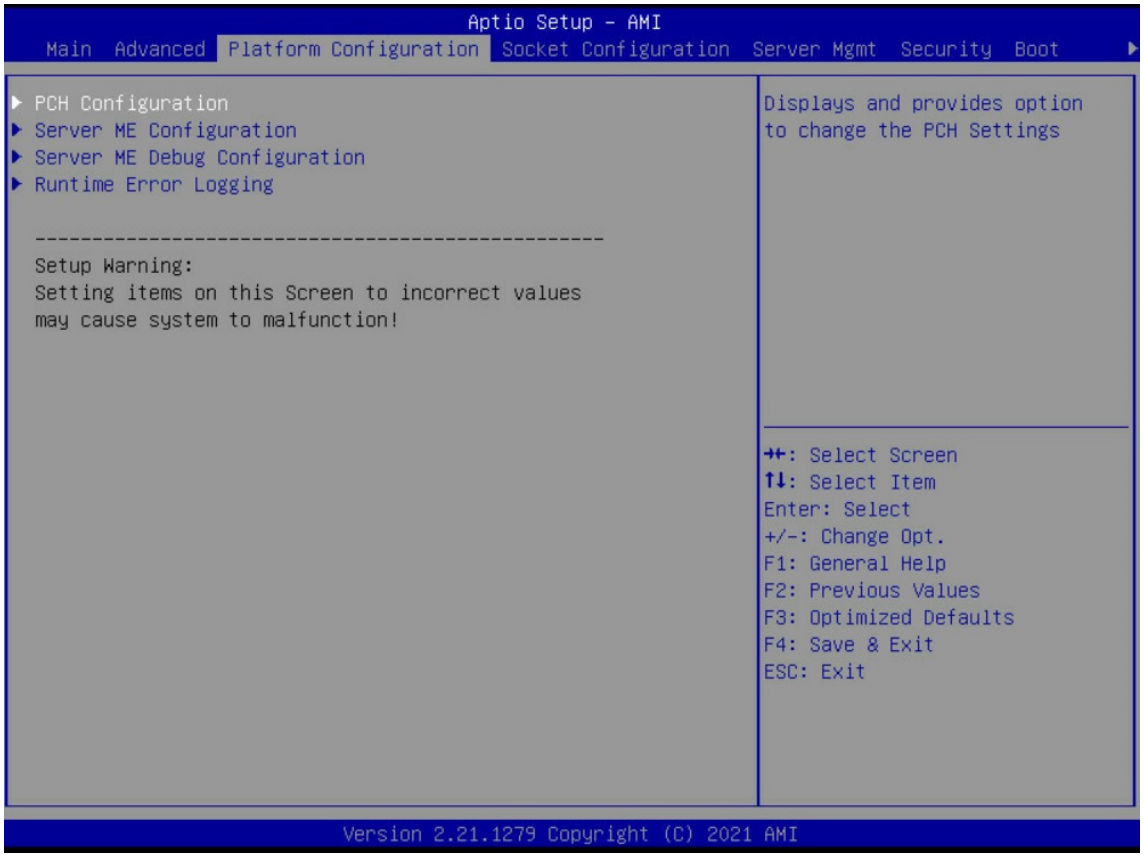
RAM Disk Configuration			
Disk Memory Type	Specifies type of memory to use from available memory pool in system to create a disk.		
	▶Boot Service Data	Reserved	
Create Raw	Creates a raw RAM disk.		
	Size (Hex)	The valid RAM disk size should be multiples of RAM disk block size.	
		▶1	
		Create & Exit	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	Select to remove.		
	Enable	▶Disable	
Remove selected RAM disk(s)	Removes selected RAM disk(s).		

4.4.9 Driver Health

Provides Health Status for the Drivers/Controllers.

Driver Health		
Network Stack	Enables/disables UEFI Network Stack.	
	Enable	▶Disable

4.5 Platform Configuration



4.5.1 PCH Configuration

Displays and provides option to change the PCH Settings.

PCH Configuration				
PCH Configuration	Enables/disables Intel(R) IO controller hub devices.			
	External SSC Enable - CK420	Enable Spread Spectrum - only affects external clock generator.		
		Enable	▶Disable	
	PCIe P11 SSC	PCIe P11 SSC percentage. • Auto: Keep hw default, no BIOS override. Range is 0.0%-2.0%		
		Auto	▶Disable	0.5%
	Shutdown Policy	Allows to configure Shutdown Policy Select in General Interrupt Register. Available modes are INIT and PLTRST.		
		INIT	▶PLTRST	
PCH SATA Configuration	SATA Controller	Enables/disables SATA controller.		
		▶Enable	Disable	
	Configure SATA as	Identify the SATA port is connected to solid state drive or hard disk drive.		
		▶AHCI	RAID	
	SATA test mode	Enables/disables SATA test mode.		
		Enable	▶Disable	
	SATA Mode options	SATA mode related options.		
		SATA HDD Unlock	Enable: HDD password unlock is enabled in the OS.	
			▶Enable	Disable
		SATA LED locate	If enabled LED/SGPIO hardware is attached.	
			▶Enable	Disable
	Support Aggressive Link Power	Enables/disables SALP.		
		▶Enable	Disable	

PCH SATA Configuration	Hot Plug	Designates this port as hot pluggable.				
		▶AHCI	RAID			
	Configure as eSATA	Configures port as external SATA (eSATA).				
		Enable	▶Disable			
	Mechanical Presence Switch	Controls reporting if this port has an mechanical presence switch. NOTE: Requires hardware support.				
		▶Enable	Disable			
	Spin Up Device	If enabled for any 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.				
		Enable	▶Disable			
	SATA Device Type	Identify the SATA port is connected to solid state drive or hard disk drive.				
		▶Hard Disk Drive	Solid State Drive			
	SATA Topology	Identify the SATA topology if it is the default or ISATA or Flex or DirectConnect or M2.				
		▶Unknown	ISATA	Direct Connect	Flex	M2
PCH sSATA Configuration	sSATA Controller	Enables/disables SATA controller.				
		▶Enable	Disable			
	Configure sSATA as	Identify the SATA port is connected to solid state drive or hard disk drive.				
		▶AHCI	RAID			
	SATA test mode	Enables/disables SATA test mode.				
		Enable	▶Disable			
PCH sSATA Configuration	SATA Mode options	SATA mode related options.				
		SATA HDD Unlock	Enable: HDD password unlock is enabled in the OS.			
			▶Enable	Disable		
		SATA LED locate	If enabled LED/SGPIO hardware is attached.			
			▶Enable	Disable		
	Support Aggressive Link Power	Enables/disables SALP.				
		▶Enable	Disable			
	sSATA Port 0-5	Enables/disables SATA port.				
		▶Enable	Disable			
	Hot Plug	Designates this port as hot pluggable.				
		AHCI	RAID			
	Configure as eSATA	Configures port as external SATA (eSATA).				
		Enable	▶Disable			
	Mechanical Presence Switch	Controls reporting if this port has an mechanical presence switch. NOTE: Requires hardware support.				
		▶Enable	Disable			
	Spin Up Device	If enabled for any 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.				
		Enable	▶Disable			
	SATA Device Type	Identifies the SATA port is connected to solid state drive or hard disk drive.				
		▶Hard Disk Drive	Solid State Drive			
	SATA Topology	Identifies the SATA Topology if it is the default or ISATA or Flex or DirectConnect or M2.				
		▶Unknown	ISATA	Direct Connect	Flex	M2

USB Configuration	USB Per-Connector Disable	Selectively enables/disables each of the USB physical connector (physical port). Once a connector is disabled, any USB devices plug into the connector will not be detected by BIOS or OS.									
		Enable	▶Disable								
	Wake On Usb Enable	Enables/disables support for XHCI Wake on USB on connect/disconnect.									
		Enable	▶Disable								
	XHCI BAR below 4GB	Enables to work around WSK12 KDUSB 64-bit BAR issue.									
		Enable	▶Disable								
ADR Configuration	Enable/Disable ADR	Enables/disables Automatic DIMM Refresh (ADR). This is not available if eADR is enabled since eADR requires ADR to be enabled.									
		▶Platform-POR	Enable	Disable							
	ADR GPIO	Select between GPIO_B or GPIO_C.									
		▶GPIO B	GPIO C								
	Host Partition Reset ADR Enable	Enables/disables ADR on host partition reset.									
		▶Platform-POR	Enable	Disable							
	Enable/Disable ADR Timer	Held-off for debug purposed only.									
		▶Platform-POR	Enable	Disable							
	ADR timer expire time	Select proper ADR timer value.									
		▶Platform-POR	25 uS	50 uS	100 uS	0 uS					
	ADR timer multiplier	Select proper ADR timer multiplier.									
		▶Platform-PDR	x1	x8	x24	x40	x56	x64	x72	x80	x88	x96

4.5.2 Server ME Configuration

Configures 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. Provided the 8000h value if the altitude is unknown.
	▶8000
MCTP Bus Owner	MCTP bus owner location of PCIe: [15:8], [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.
	▶0

4.5.3 Server ME Debug Configuration

Server ME firmware debug parameters configuration.

Server ME Debug Configuration					
Server ME General Configuration	Server ME basic features configuration.				
	ME Initialization Complete Timeout	This option defines how ling BIOS waits for ME to initialize.			
		▶2			
	Enable HSIO Messaging	Enables/disables HSIO messaging.			
		Enable	▶Disable		
	DRAM Init Done Enable	Enables/disables notifying ME about DRAM initialization. (It enables/disables UMA functionality.)			
		▶Enable	Disable		
	DRAM Initialization Status	Overrides the DRAM initialization status value.			
		Auto - true status	▶0 - Success	1 - No Memory in Channels	2 - Memory Init Error
	Host Reset Warning	Enables/disables sending Host Reset Warning to ME.			
		▶Enable	Disable		
	Pre-DramInit Done ME Reset	When ME is in recovery because of internal error try to reset it.			
		Enable	▶Disable		
	HMRFP0_LOCK Message	Enables/disables sending HMRFP0_LOCK message to ME.			
		▶Enable	Disable		

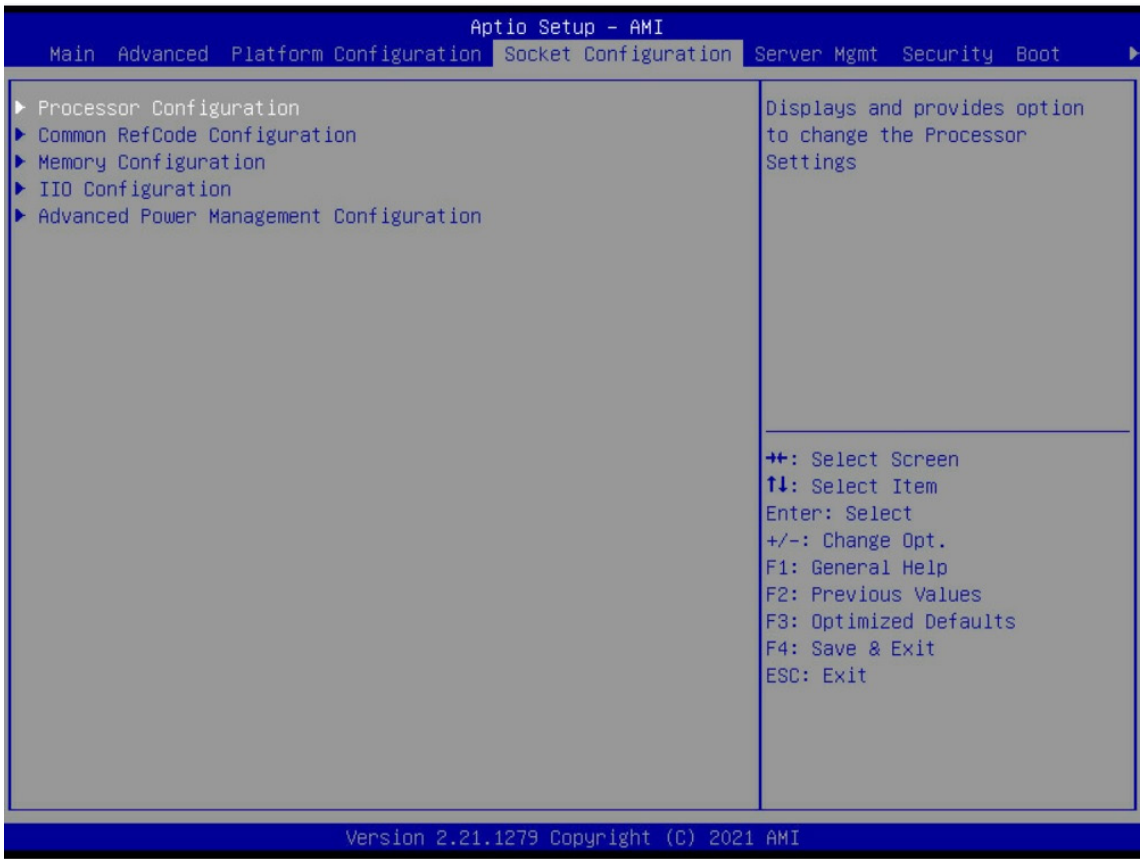
Server ME General Configuration	HMRFP0_ENABLE Message	Enables/disables sending HMRFP0_ENABLE message to ME.		
		Enable	▶Disable	
	END_OF_POST Message	Enables/disables sending END_OF_POST message to ME.		
		▶Enable	Disable	
	REGION_SELECT Message	Enables/disables sending REGION_SELECT message to ME.		
		Enable	▶Disable	
	CF9 global reset promotion	Enables/disables promoting CF9 reset to global.		
		Enable	▶Disable	
	Global Reset Lock	Enables/disables locking the joint ME and host reset capability.		
		▶Enable	Disable	
	HECI-1/2/3 Enable	Overrides HECU-1/2/3 status on PCI or let firmware decide based on ME type (auto).		
		▶Auto	Enable	Disable
	IDEr Enable	Overrides IDEr status on PCI, or let firmware decide based on ME type (auto).		
		▶Auto	Enable	Disable
	KT Enable	Overrides KT status on PCI, or let firmware decide based on ME type (auto).		
		▶Auto	Enable	Disable
	HECI-1/2/3 Hide in ME	Enables sending request to ME to hide or disable HECI-1/2/3 on host PCI		
		▶Off	Hide	Disable
	DOI3 Setting for HECI Disable	Setting this option disables setting DOI3 bit for all HECI devices.		
		Enable	▶Disable	
	Break RTC Configuration	This is a test option which breaks RTC configuration.		
		▶Enable	Disable	
	Core BIOS Done Message	Enables/disables Core BIOS Done message sent to ME.		
		Enable	▶Disable	
	Delayed Authentication Mode (DAM)	Enables overriding the state of the Delayed Authentication Mode (DAM).		
		Enable	▶Disable	
	Enable HECI Dump	Enables full HECI dumps in debug output.		
		Enable	▶Disable	
NM Configuration	Boot Mode Override	Enables overriding the boot mode requested in NMFS.		
		Enable	▶Disable	
	Cores Disable Override	Enables overriding the value of the number of cores to disable requested in NMFS register.		
		Enable	▶Disable	
	Power Measurement Override	Overrides power measurement support status reported to ME.		
		Enable	▶Disable	
	Hardware Change Override	Overrides hardware change detection status reported to ME.		
		Enable	▶Disable	
	PTU Load Override	In MROM-less system force loading PTU regardless of ME request.		
		Enable	▶Disable	

4.5.4 Runtime Error Logging

To view or change the runtime error log configuration.

Runtime Error Logging		
System Errors	System Error enable/disable setup options.	
	▶Enable	Disable

4.6 Socket Configuration



4.6.1 Processor Configuration

Displays and provides option to change the Processor Settings.

Processor Configuration		
Hyper- Threading [ALL]	Enables Hyper Threading (Software Method to enable/disable logical processor threads).	
	▶Enable	Disable
Legacy Agent	Legacy PECI agent in trust bit enable.	
	▶Enable	Disable
SMBus Agent	SMBus PECI agent in trust bit enable.	
	Enable	▶Disable
IE Agent	IE PECI agent in trust bit enable.	
	▶Enable	Disable
Generic Agent	Generic PECI agent in trust bit enable.	
	Enable	▶Disable
eSPI Agent	ESPI PECI agent in trust bit enable.-	
	Enable	▶Disable
DBP-F	The DBP-F can be turned off by writing into the (MSR 792h [5:6] for CLX, and MSR 6Dh [2:3] for ICX).	
	Enable	▶Disable
Lock Chipset	Locks or unlocks chipset.	
	Enable	▶Disable
MSR Lock Control	Enable: MSR 3Ah and CSR 80h will be locked. Power good reset is needed to remove lock bits.	
	▶Enable	Disable
PKG CST CONFIG CONTROL MSR Lock	Enable: MSR E2h will be locked. Power good reset is needed to remove lock bits.	
	▶Enable	Disable
Total Memory Encryption (TME)	Enables/disables Total memory Encryption (TME).	
	▶Enable	Disable

4.6.2 Common RefCode Configuration

Displays and provides option to change the Common RefCode Settings.

Common RefCode Configuration										
MMCFG Base	Select MMCFG base.									
	▶Auto	1G	1.5G	1.75G	2G	2.5G	3G			
MMCFG Size	Select MMCFG size.									
	▶Auto	64M	128M	256M	512M	1G	2G			
MMIO High Base	Select MMIO high base.									
	3584T	512G	1T	2T	4T	16T	24T	▶32T	40T	56T
MMIO High Granularity Size	Select the allocation size used to assign mmioh resources. Total mmioh space can be up to 32 x granularity. Per stack mmioh resource assignments are multiples of granularity where 1 unit per stack is the default allocation.									
	1G	4G	16G	▶64G	256G	1024G				
Isoc Mode	Enables/disables Isoc.									
	▶Auto	Enable	Disable							
Numa	Enables/disables Non uniform Memory Access (Numa).									
	▶Enable	Disable								
Virtual Numa	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors.									
	Enable	▶Disable								

4.6.3 Memory Configuration

Displays and provides option to change Memory Settings.

Memory Configuration				
Enforce POR	• Enable: Enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. • Disable: Disables this feature and user if able to run at higher frequencies, specified in DDR frequency limit field (limited by processor support). • Auto: Sets it to the MRC default setting.			
	▶POR	Disable		
Enforce Population POR	Enables Memory Population POR Enforcement. Selecting Enforce Validated Populations will only allow populations that have been validated.			
	▶Enforce Supported Population	Enforce Validated Populations	Disable Enforcement	
PPR Type	Select Post Package Repair Type. • Auto: Sets it to the MRC default setting; current default is Soft PPR.			
	▶Soft PPR	Hard PPR	PPR Disable	
PPR Error Injection test	Enables/disables support for c-script err inj test.			
	Enable	▶Disable		
Memory Frequency	Maximum Memory Frequency Selections in Mhz. If Enforce POR is disabled, user will be able to run at higher frequency than the memory support (limited by processor support). Do not select reserved.			
	▶Auto	1200~4800-OvrClk		
MRC Promote Warnings	Determines if warnings are promoted to system level.			
	▶Enable	Disable		
Halt on mem Training Error	Halts on mem Training Error disable/enable.			
	▶Enable	Disable		
Rank Switch Configuration	TA Floor enforces t_rrdr, t_rrdd minimum of 3; Rcven Ave attempts to match Rcven logic delay across ranks.			
	TA Floor	▶Rcven Ave	Reserved	Disable
Enable ADR	Enables the detecting and enabling of ADR. This is not available if eADR is enabled since eADR requires ADR to be enabled.			
	▶Enable	Disable		
Legacy ADR Mode	Enables/disables Legacy ADR mode. This is not available if eADR is enabled since eADR requires this mode to be enabled.			
	▶Enable	Disable		

Minimum System Memory Size	Minimum memory size assigned as system memory when only JEDEC NVDIMMs are present.			
	▶2GB	4GB	6GB	8GB
NVDIMM Energy Policy	Sets the energy policy for NVDIMMs			
	▶Device-Managed	Host-Managed		
ADR Data Save Mode	DATA Save mode for ADR. Batterybacked or Type 01 NVDIMM.			
	▶NVDIMMs	Batterybacked DIMMs	Disable	
Erase-Arm NVDIMMs	Enables/disables Erasing and Arming NVDIMMs.			
	▶Enable	Disable		
Restore NVDIMMs	Enables/disables Automatic restoring of NVDIMMs.			
	▶Enable	Disable		
Interleave NVDIMMs	Controls if NVDIMMs are interleaved together or not.			
	▶Enable	Disable		
Memory Topology	Displays memory topology with DIMM population information.			

4.6.4 IIO Configuration

Displays and provides option to change IIO Settings.

IIO Configuration							
Socket0/1 Configuration	IOU0/1/2/3/4 (IIO PCIe Port 1/2/3/4/5)	Select PCIe port Bifurcation for selected slot (s).					
		Auto	x4x4x4x4	x4x4x8			
		x8x4x4	x8x8	▶x16			
	Sck0 RP Correctable Err	Applies to root ports only. Enable interrupt on a non-fatal error.					
		Yes	▶No				
	Sck0 RP Fatal Uncorrectable Err	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.					
		Yes	▶No				
	Port 0/DMI	Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D)					
	Port 1A/2A/4A/5A	PCI-E Port	In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/disable is used to enable/disable and expose/hide its CFG space.				
			▶Auto	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 (16GT/s)
IOAT Configuration	Sck0/1 IOAT Config	DNA	Select Dma enable/disable for each CB device.				
			▶Yes	No			
		No snoop	Enables/disables for each CB device.				
			Yes	▶No			
	Disable TPH	TLP Processing Hint disable.					
		Yes	▶No				
	Prioritize TPH	Prioritize TPH.					
		Enable	▶Disable				
	Relaxed Ordering	Enables/disables Relaxed Ordering.					
		Yes	▶No				
Intel VT for Directed I/O (VT-d)	Intel VT for Directed I/O	Enables/disables VT-d Interrupt Remapping support.					
		▶Enable	Disable				
	DMA Control Opt-In Flag	Enables/disables DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).					
		Enable	▶Disable				

Intel VT for Directed I/O (VT-d)	Interrupt Remapping	Enables/disables Interrupt Remapping support.		
		▶Auto	Enable	Disable
	X2APIC Opt Out	Enables/disables X2APIC_OPT_OUT bit.		
		Enable	▶Disable	
	Pre-boot DM Protection	Enables DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and VTD_INFO is installed in PEI.)		
		Enable	▶Disable	
Intel VMD technology	Intel VMD for Volume Management Device on Socket 0/1	Enable/disable VMD	Enables/disables VMD in this stack.	
			Enable	▶Disable
Intel AIC Retimer/ AIC SSD Technology (non-VMD)	Intel AIC Retimer/AIC SSD on So cket 0/1	A nonce Intel AIC Retimer/AIC SSD HW at Stack1(Port 1A-1D). Override IOU0 bifurcation if required.		
		Enable	▶Disable	
Detected PCIe retimers	Socket 0/1 retimers configuration.			
PCIe Low Latency Retimers	Enables/disables PCIe low latency retimers.			
	Yes	▶No		
Skip PCIe retimers detection	Skip PCIe retimers detection to speed up the boot. Retimers are present only in specific HW configurations.			
	Yes	▶No		

4.6.5 Advanced Power Management Configuration

Displays and provides to change the Power Management settings.

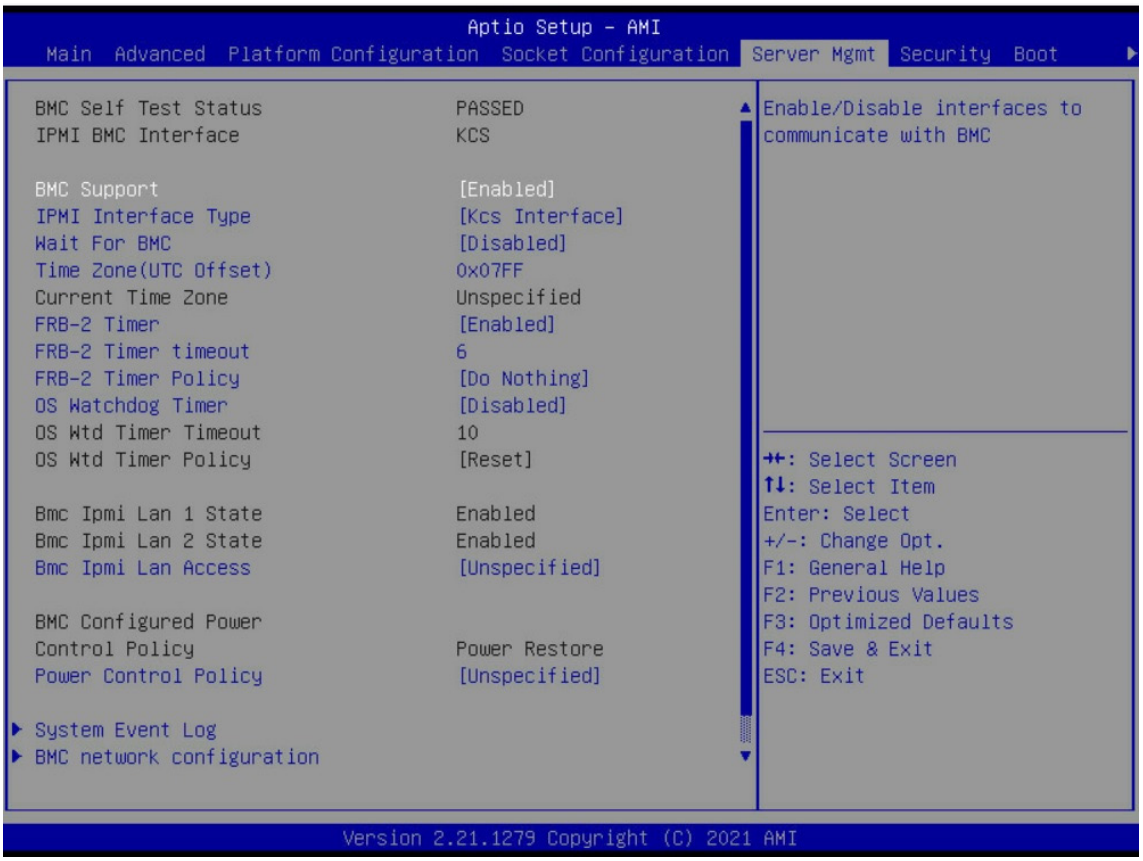
Advanced Power Management Configuration				
CPU P State Control	P State Control Configuration Sun Menu, include Turbo, XE and etc.			
	Uncore Freq Scaling	If disabled, user can input Uncore Frequency.		
		▶Enable	Disable	
	AVX License Pre-Grant Override	If disabled, user can input Uncore Frequency.		
		Enable	▶Disable	
	SpeedStep (Pstates)	Enables/disables EIST (P-States).		
		▶Enable	Disable	
	AVX P1	AVX P1 level selection.		
		▶Normal	Level 1	Level 2
	Dynamic SST-PP	Supports Dynamic SST-PP Select. NOTE: Disable: Static SST-PP can be displayed.		
		Enable	▶Disable	
	Intel SST-PP	Intel SST-PP Select allows user to choose from up to two additional base frequency conditions.		
		▶Base	Config 3	Config 4
	Activate SST-BF	This option allows SST-BF to be enabled.		
		Enable	▶Disable	
	EIST PSD Function	Choose HW_ALL/SW_ALL in _PSD return.		
		▶HW_ALL	SW_ALL	
	Boot performance mode	Select the performance state that the BIOS will set before OS hand off.		
		▶Max Performance	Max Efficient	Set by Intel Node Manager
	Energy Efficient Turbo	Energy Efficient Turbo Disable, MSR 0x1FC [19]		
		▶Enable	Disable	
	Turbo Mode	Enables/disables processor Turbo Mode (requires EMTTM enabled too.)		
		▶Enable	Disable	
	CPU Flex Ratio Override	Enables/disabled CPU Flex Ratio Programming.		
		Enable	▶Disable	
	GPSS timer	P-state change hysteresis time window.		
		0 us	50 us	▶500 us

Hardware PM State Control	Hardware P-State setting.				
	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).			
		▶Native Mode	Out of Band Mode	Native Mode with No Legacy Support	Disable
	HardwarePM Interrupt	Enables/disables Hardware PM Interrupt.			
		Enable	▶Disable		
	EPP Enable	When disabled, HW masks EPP in CPUID [6],10 and uses EPB for EPP.			
		▶Enable	Disable		
	APS rocketing	Enables/disables the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.			
		Enable	▶Disable		
	Scalability	Enables/disables Core Performance to Frequency Scalability Based Optimizations in the CPU.			
		Enable	▶Disable		
	Native ASPN	• Enable: OS Controlled ASPM. • Disable: ASPM off. • Auto: BIOS Controlled ASPM.			
		▶Auto	Enable	Disable	
CPU C State Control	CPU C State setting.				
	Enable Monitor MWAIT	Allows Monitor and MWAIT instructions.			
		▶Enable	Disable		
	CPU C1 auto demotion	Allows CPU to automatically demote to C1. Takes effect after reboot.			
		▶Enable	Disable		
	CPU C1 auto undemotion	Allows CPU to automatically undemote to C1. Takes effect after reboot.			
		▶Enable	Disable		
	CPU C6 report	Enables/disables CPU C6(ACPI C3) report to OS.			
		▶Auto	Enable	Disable	
	Enhanced Halt State (C1E)	Core C1E auto promotion control. Takes effect after reboot.			
		▶Enable	Disable		
	OS ACPI Cx	Report CC3/CC6 to OS ACPI C2 or ACPI C3.			
		▶ACPI C2	ACPI C3		
Package C State Control	Package C State setting.				
	Package C State	Package C State limit.			
		Auto	C0/C1 state	C2 state	▶C6 (non Retention) state
	Register Access Low Latency Mode	Enables lower latency mode for register accesses. NOTE: Enabling this mode will prevent PkgC6 as register access fabric is prevented from going into idle.			
		Enable	▶Disable		
	C2C3TT	Default = 0, means [Auto]. C2 to C3 Translation Timer, PPDN_INIT = 1:10:1:74 Bit [11:0].			
		▶0			
	Dynamic L1	PCU_MISC_CONFIG Bit [21] = dynamic L1 enable.			
		▶Enable	Disable		
	PKG C-state Lat. Neg.	MSR 1FCh Bit [30] = PCH_NEG_DISABLE.			
		▶Enable	Disable		

Package C State Control	LTR IIO Input	MSR 1FCh Bit [29] = LTR_IIO_DISABLE. Disable = Ignore IIO LTR input.			
		Take IIO LTR input	▶Ignore IIO LTR input		
	Latency Tolerance Requirement (LTR)	Program PCIE_IL TR_OVRD 1:30:1:0xFC Sub Menu.			
		PCIe LTR Override Control	Allows manual overrides for PCIE_IL TR_IVRD.		
			Enable	▶Disable	
	Enable PKGC_SA_PS_CRITERIA	Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.			
		Auto	▶Enable	Disable	
	PkgC SA PS Criteria Power Management Control	Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.			
		MDLL Off	Enable to shut down MDLL during SR.		
			▶Auto	Enable	Disable
	PkGc Interrupt Response Time	Programmable Package C-state interrupt response time setup control.			
		VALID	Enable	▶Disable	
CPU Thermal Management	CPU T State Control	CPU Thermal Related setting.			
		Software Controlled T-States	Enables/disables Software Controlled T-States.		
			Enable	▶Disable	
	PROCHOT Modes	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.			
		▶Input-only	Both Input and Output	Output-only	Disable
	Thermal Monitor	Enables/disables Thermal Monitor			
		▶Enable	Disable		
	Therm-Monitor-Status Filter	Enables Filter based therm_monitor_status(IA32_THERMAL_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	Min=0, Max=57		
	TCC Activation Offset	Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated.			
		▶0	Min=0, Max=58		
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	▶OS Controls EPB	BIOS Controls EPB	PECI Controls EPB
		PECI PCS EPB	Controls whether PECI has control over EPB		
			▶OS controls EPB	PECI controls EPB using PCS.	
		Dynamic Loadline Switch	Dynamic Loadline Switch control. MSR 0x1FC[Bit24].		
			▶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		

CPU- Advanced PM Tuning	Energy Perf Bias	P0 Total Time Threshold Low	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than this threshold. ►28
		P0 Total Time Threshold High	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is greater than this threshold. ►3F
	SAPM Control	Energy Perf BIAS Sub Menu. ►Enable	Disable
	EET Mode	Coarse Grained Mode decides whether to grant user request turbo or P1. Fine Grained Mode decides how much turbo to be granted. More helpful with Scalability Enabled. ►Coarse Grained Mode	Fine Grained Mode

4.7 Server Mangement



4.7.1 Processor Configuration

Displays and provides option to change the Processor Settings.

Processor Configuration				
BMC Support	Enables/disables interfaces to communicate with BMC.			
	▶Enable	Disable		
IPMI Interface Type	Type of Interface to communicate BMC from Host.			
	▶Kcs Interface	Bt Interface		
Wait for BMC	Wait for BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during AS power ON. It takes around 30 seconds to initialize Host to BMC interfaces.			
	Enable	▶Disable		
Time Zone(UTC Offset)	Enter UTC Offset in hours. i.e. from -24:00 to +24:00. These values will be converted into minutes and programmed to BMC. Enter 0x07FF to consider BIOS time as local time.			
	▶0x07FF			
FRB-2 Timer	Enables/disables FRB-2 timer (POST timer).			
	▶Enable	Disable		
FRB-2 Timer timeout	Enter value between 1 to 30 minutes for FRB-2 Timer Expiration.			
	▶6	1-30		
FRB-2 Timer Policy	Configures how the system should respond if the FRB-2 Timer expires. Not available is 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		
BMC IPMI LAN Access	Enables/disables BMC IPMI LAN.			
	Enable	Disable	▶Unspecified	
Power Control Policy	Configures 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 Power Up	Last Power State	Power Restore	▶Unspecified

4.7.2 System Event Log

Configures SEL event log.

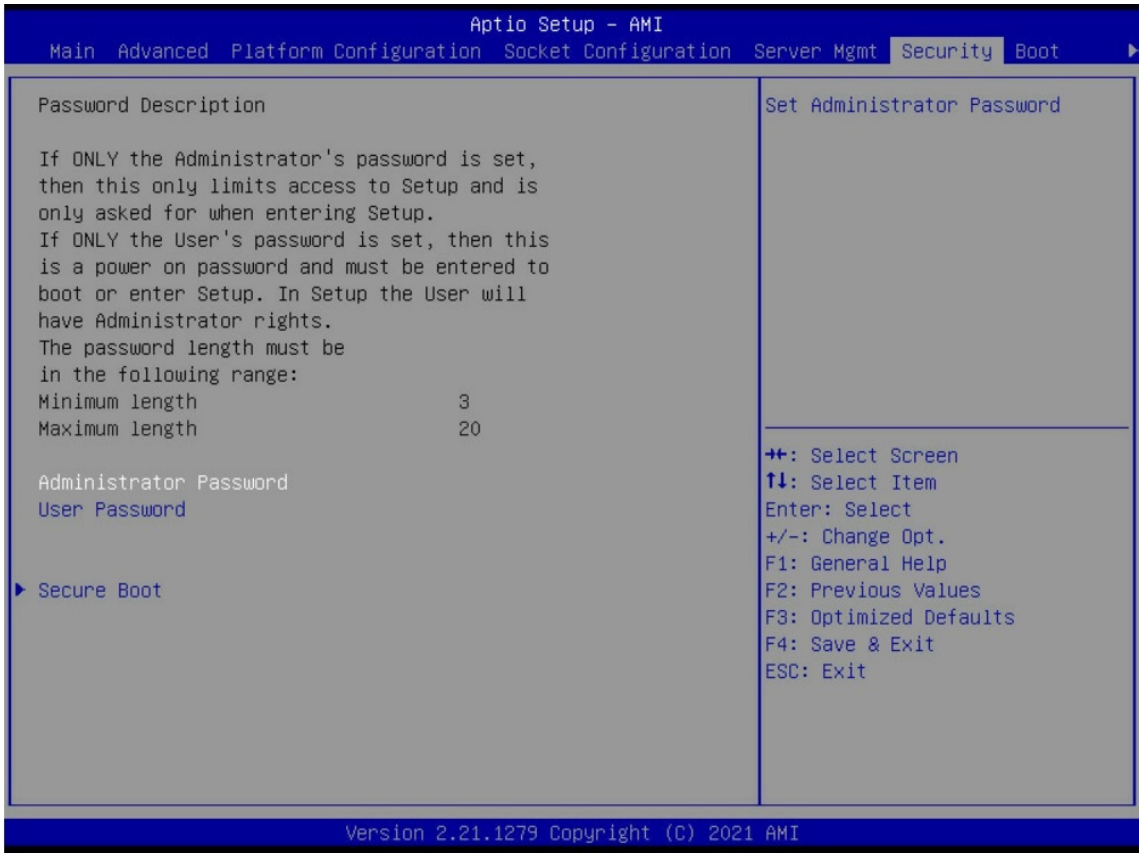
System Event Log				
SEL Components	Change this to enable or disable event logging error/progress codes during boot.			
	▶Enable		Disable	
Erase SEL	Choose options for erasing SEL.			
	Yes, on next reset		Yes, on every reset	▶No
When SEL is Full	Choose options for reactions to full SEL.			
	▶Do Nothing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

4.7.3 BMC Network Configuration

Configures BMC network parameters.

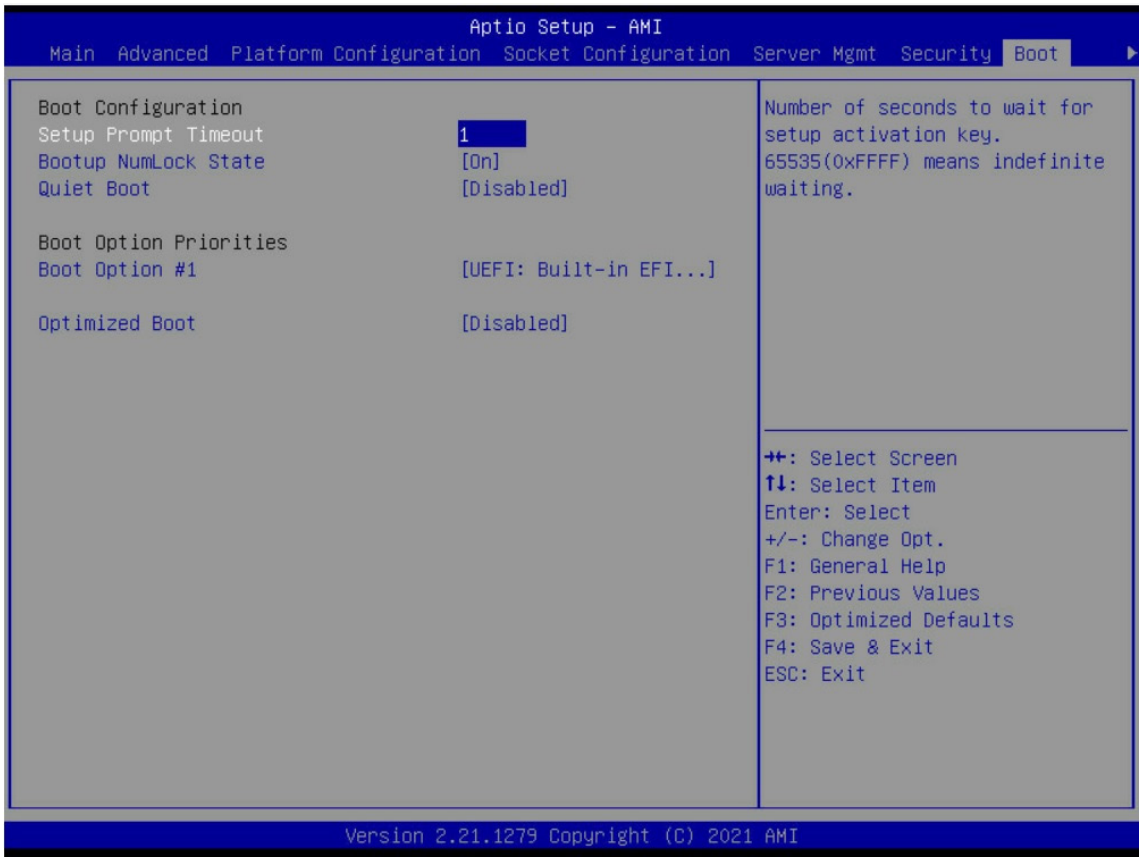
BMC Network Configuration			
Configuration Address source	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.		
	▶Enable	Disable	
IPv6 Support	Enables/disables LAN1 IPv6 Support		
	▶Unspecified	Static	Dynamic BMC DHCP
Configuration Router LAN1/2 Address	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	Dynamic BMC DHCP

4.8 Security



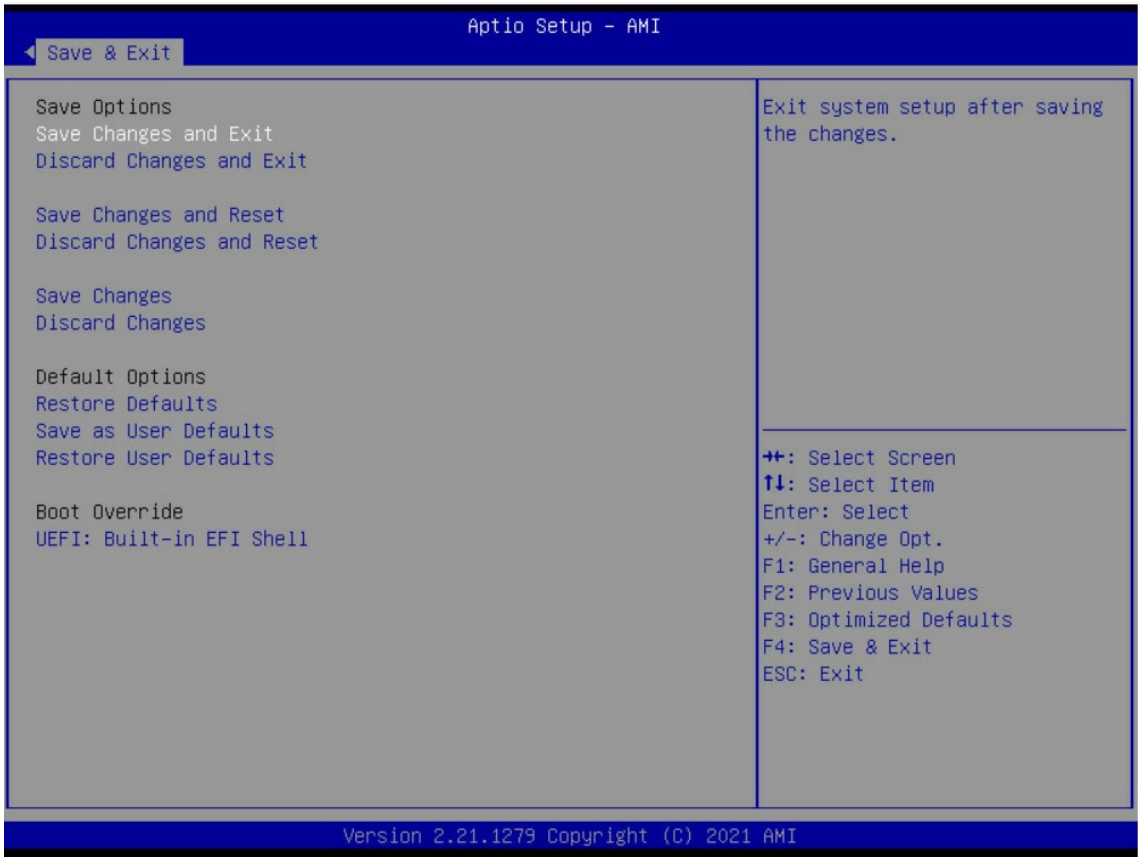
Security			
Administrator Password	Set administer password.		
Set User Password	Create new password.		
Secure Boot	Secure boot configuration.		
	Secure Boot	▶Enable	Disable
	Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.	
		▶Standard	Custom

4.9 Boot



Boot		
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65565 (0xFFFF) means indefinite waiting.	
	On	
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.	
	▶UEFI: Built-in EFI Shell	Disable
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

4.10 Exit



Exit	
Save Change 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.

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 test points	
0xA0	Initialize KTI inuput 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 opeartion
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
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 Errror
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. Meory 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 Reste (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.