SB201-SU

Storage Barebone
User's Manual

UM_SB201-SU_v1.2_110325

Document Release History

Release Date	Version	Update Content
April, 2025	1	Released to public.
July, 2025	1.1	Update PSU spec.
November, 2025	1.2	Update internal drive bay (M.2).

Table of Contents

Preface i
Safety Instructions ii
About This Manual iv
Chapter 1. Product Features 1
1.1 Box Contents 1
1.1.1 Accessory Bag Contents 2
1.2 Specifications 3
1.3 System Block Diagram 4
1.4 Features 5
Chapter 2. Hardware Setup 8
2.1 Central Processing Unit 8
2.1.1 Installation 8
2.2 System Memory 14
2.2.1 Placement 14
2.2.2 DIMM Population 15
2.2.3 Mapping Table 17
2.2.4 Installation 18
2.3 Top Cover 19
2.4 Power Supply Unit 20
2.4.1 Installation 20
2.4.2 LED Indicator 20
2.5 Fan 21
2.6 Air Duct 22
2.7 Disk Drive 23
2.7.1 Disk Drive: 2.5-inch 23
2.7.2 LED Indicator 25
2.8 Riser Card 26
2.9 OCP Card 27
2.10 M.2 Card 28
2.11 Slide Rail 29
Chapter 3. Hardware Settings 32
3.1 Block Diagram 32
3.2 Placement 33
3.3 Content List 34
3.4 External Port 36
3.5 Connector Definition 37
3.6 Jumper Definition 41
3.7 LED 44
3.3.2 Connector 44
3.7.1 Rear Chassis LEDs 44
3.7.2 Internal LEDs 44
3.8 Drive Backplane: 8 Bay 46
3.8.1 Placement 46
3.8.2 Connector 47
3.8.3 Switch Setting 50

3.8.4 LED Definition 53
3.8.5 LED Definition 54
Chapter 4. BIOS Configuration Settings 55
4.1 Navigation Keys 55
4.2 BIOS Menu 56
4.2.1 Menu 56
4.2.2 Startup 56
4.3 Main 57
4.3.1 Main 57
4.4 Advanced 58
4.4.1 Trusted Computing 58
4.4.2 Redfish Host Interface Settings 59
4.4.3 AST2600 Super IO Configuration 59
4.4.4 Serial Port Console Redirection 59
4.4.5 Option ROM Dispatch Policy 60
4.4.6 PCI Subsystem Settings 60
4.4.7 USB Configuration 61
4.4.8 Network Stack Configuration 61
4.4.9 NVMe Configuration 62
4.4.10 T1s Auth Configuration 62
4.4.11 All Cpu Informaiton 62
4.4.12 RAM Disk Configuration 62
4.4.13 Asmedia 106x RAID Mode Setting #0 62
4.4.14 VLAN Configuration (MAC:D29C29CAB89) 63
4.4.15 MAC:D29C29CAB89-IPv4 Network Configuration 63
4.4.16 Intel(R) I210 Gigabit Network Connection - (Mac address) 63
4.4.17 VLAN Configuration (MAC:0015B2B34E44) 64
4.4.18 MAC:0015B2B34E44-IPv6 Network Configuration 64
4.4.19 MAC:0015B2B34E44-IPv4 Network Configuration 64
4.4.20 Intel(R) I210 Gigabit Network Connection - (Mac address) 64
4.4.21 VLAN Configuration (MAC:0015B2B34E45) 65
4.4.22 MAC:0015B2B34E45-IPv6 Network Configuration 65
4.4.23 MAC:0015B2B34E45-IPv4 Network Configuration 65
4.4.24 Driver Health 65
4.5 Platform Configuration 66
4.5.1 IBL-IO Configuration 66
4.5.2 Miscellaneous Configuration 67
4.5.3 Runtime Error Logging 67
4.5.4 IIO Error Enabling 69
4.5.5 CXL Error Enabling 70
4.5.6 PCIe Error Enabling 70
4.5.7 Error Control Setting 71
4.5.8 Crash Log Enabling 72
4.5.9 AWR Configuration 72
4.6 Socket Configuration 73
4.6.1 Processor Configuration 73
4.6.2 Common RefCode Configuration 74
4.6.3 Uncore Configuration 75
4.6.4 Memory Configuration 79

4.6.5 IIO Configuration 81
4.6.6 Advanced Power Management Configuration 106
4.7 Server Mangement 111
4.7.1 System Event Log 112
4.7.2 BMC Network Configuration 112
4.7.3 View System Event Log 112
4.8 Security 113
4.9 Boot 114
4.10 Save & Exit 117
4.11 BIOS Update Process 118
4.12 BIOS Post Code 119
Chapter 5. BMC Configuration Settings 126
5.1 Login 126
5.2 Web UI Common Features 127
5.2.1 Dashboard 127
5.2.2 Sensor 128
5.2.3 System Inventory 128
5.2.4 FRU Information 129
5.2.5 PSU Information 129
5.2.6 Logs & Report 130
5.2.7 Settings 131
5.2.8 Remote Control 131
5.2.9 Images Redirection 132
5.2.10 Chassis Identify 133
5.2.11 Power Control 134
5.2.12 Maitenance 135
5.2.13 Sign Out 136
Chapter 6. Technical Support 137



Copyright © 2025 AIC®, Inc. All Rights Reserved.

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

Preface

Copyright

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

Trademarks

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

Changes

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

Warning

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

Disclaimer

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

Instruction Symbols

Special attention should be given to the instruction symbols below.

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

Safety Instructions

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

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

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

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

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

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

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

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

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

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

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

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

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



About This Manual

Thank you for selecting and purchasing the SB201-SU.
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 SB201-SU. For the latest version of this user's manual, please refer to the AIC® website: https://www.aicipc.com/en/productdetail/51570.

Chapter 1 Product Features

SB201-SU is a flexible storage server barebone that is specifically designed to accommodate diverse corporations and enterprises for managing heavy workloads and multiple applications.

Chapter 2 Hardware Setup

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

Chapter 3 Hardware Settings

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

Chapter 4 BIOS Configuration Settings

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

Chapter 5 BMC Configuration Settings

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

Chapter 6 Technical Support

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

Chapter 1. Product Features

SB201-SU is a high density storage server that includes motherboard, chassis, power supply and disk drive. For more information about our product, please visit our website at https://www.aicipc.com/en/index.

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

1.1 Box Contents

This product contains the components listed below.

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

Pre-installed into the system		Number
✓	2000W/2400W 1+1 CRPS 80+ Titanium by CPU/NVMe supporting wattage SKU options	1+1
✓	2.5-inch hot swap disk drive tray Front: 15mm	24
	2.5-inch hot swap disk drive tray Rear: 15mm (SATA)	2
✓	Heat sink	2
✓	Easy swap fan 4 x 80mm	4
✓	AIC® Sirius motherboard	1
Accessory Item		**Number**
✓	EPE foam for front board: 575*420*105H	1
✓	EPE foam for rear board: 575*420*105H	1
✓	EPE foam for front tray: 575*300*155H	1
✓	EPE foam for rear tray: 575*300*155H	1
✓	EPE pad for Rail Box: 140*100*25T	1
✓	EPE foam (for liquid cooing): 470*305*60H	1
✓	EPE pad for heatsink: 150*100*25	3
✓	Power cord	vary per region
✓	28-inch tool-less slide rail assembly	1

Product features are subject to change without notice.

1.1.1 Accessory Bag Contents

Item	Part No.	Description	Number
CABLE TIE	H67-00002-06	YJ-120,NYLON/94V-2	4 pcs

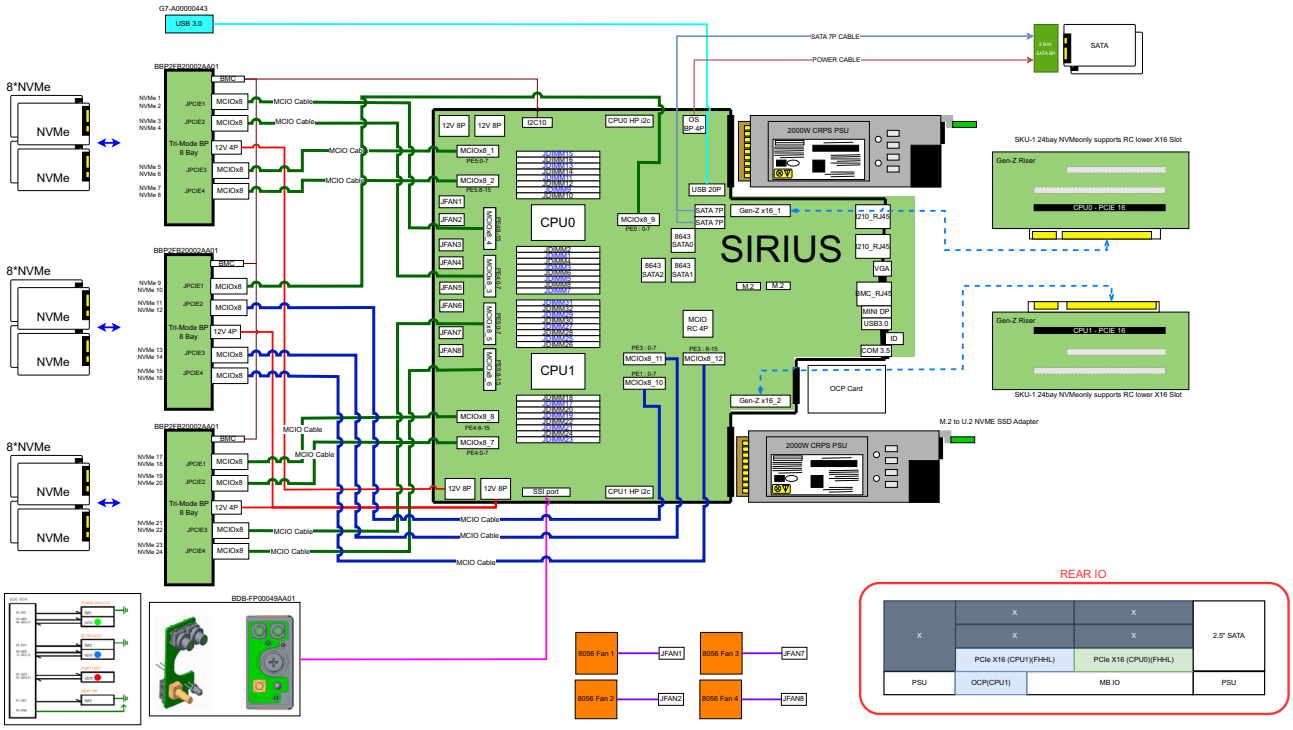
Product features are subject to change without notice.

1.2 Specifications

Dimensions (W x D x H)	mm : 438 x 820 x 87.5	
	inches : 17.2 x 32.2 x 3.4	
Motherboard	AIC Server Board Sirius	
Processor	Processor Support	• Dual Intel® Xeon® 6 6700E/6500P/6700P series • Supports CPU TDP 350W **Please contact AIC Technical Support for more info/details about optimized CPUs and specialized system*
	UPI Speeds	24GTs
	Socket Type	Socket E2 (LGA 4710 Socket)
System Memory	• Total 32 memory slots; 8 channel per CPU (2DPC) • DDR5 6400MHz(1DPC) 5200MHz(2DPC) 8000MHz(1DPC MCR) by 6700P/6500P series; • DDR5 6400MHz(1DPC) 5200MHz(2DPC 2Rx4 RDIMM only) by 6700E series; • DDR5 6400MHz(1DPC) 5200MHz(2DPC) 8000MHz(1DPC MCR) by Clearwater Forest	
Front Panel	Power button, ID button, Reset button, VGA, 2 x USB 3.0	
Drive Bays	External	2.5" hot swap 24
	Internal	2 × M.2/M-key/22110/2280 (PCIe Gen4)
Backplane	Front Options	• 3 x 8-port 2.5” Gen5 Tri-mode • 3 x 8-port E3.S Gen5 NVMe
	Rear Options	• 1 x 2-port 2.5” SAS/SATA • 1 x 2-port 2.5” Tri-mode + 1 x 2-port 2.5” SAS/SATA
Expansion Slots	PCIe 5.0	2 X16 FHHL/HHHL + 1 x OCP 3.0
Rear I/O	LAN	• 2 x RJ45 connectors for dual port GbE • 1 x RJ45 connector (for BMC management port)
	USB	2 x USB 3.0 Type-A
	Video Output	• 1 x DB-15 VGA connector • 1 x Mini display port
	Serial Port	1 x COM connector (Audio Jack)
Power Supply	2000W/2400W 1+1 CRPS 80+ Titanium by CPU/NVMe supporting wattage SKU options	
System Cooling	4 x 80x56mm hot swap fans	
System Management	• IPMI 2.0 • KVM over IP • Media redirection • Temperature, fan, voltage, PSU sensor monitor • System temperature	• System ID / System fail indicator • Remote power on/off/reset • SEL message alarm through mail • SNMP support

Riser Card (included)	• 1 x RC-PE2U26-TY • 1 x RC-PE2U27-TY	
System BIOS	BIOS Type	AMI UEFI BIOS
	BIOS Features	• ACPI • PXE • WOL • AC loss recovery • IPMI 2.0 KCS mode interface • SRIOV • SMBIOS • TPM • Serial console redirection • PCIe hotplug
On-board Devices	SATA	• 2 x SATA3 7-pin by ASM1062R (support RAID 0/1) • 12 x SATA3 by 3 x Mini-SAS connectors (power by ASM1164)
	BMC	Aspeed AST2600 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN • HTML5 • Redfish
	Network Controllers	• Realtek RTL8211FS 1GbE for BMC dedicated management port • 2 x Intel® I210 GbE Ethernet Controller
	Graphics	• Integrated VGA support by ASPEED AST2600 • Resolution up to 1920x1200 @60Hz 32bpp
Environmental Specifications	• Storage temperature: -10°C(14°F) ~ 60°C(140°F) • Operating temperature: 0°C(32°F) ~ 35°C(95°F) • Storage operating humidity: 5%~95% non-condensing	
Gross Weight	(w/ PSU & Rail)	kgs : 25
		lbs : 55
Packaging Dimensions	(W x D x H)	mm : 1155 x 615 x 328
		inches : 45.5 x 24.2 x 12.9
Mounting	Standard	36" tool-less slide rail

1.3 System Block Diagram



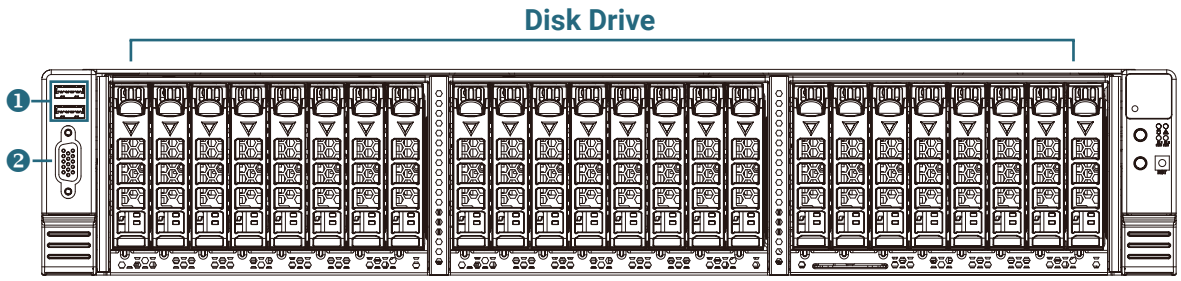
1.4 Features

SB201-SU is a reliable 2U storage server barebone with 24 hot swap drives bays. This product is designed to accommodate the AIC-patented serverboard, Sirius, which supports Dual Intel® Xeon® 6 6700E/6500P/6700P series and 32 DDR5 DIMM to offer greater performance, efficiency and utility for our customers.

In addition to the noteworthy features of the barebone, SB201-SU provides immediate and efficient management with Onboard Baseboard Management Controller and greater I/O extension. Featuring IPMI 2.0 and Aspeed AST2600 Advanced PCIe Graphics, the server board offers support for iKVM, Media Redirection, IPMI over LAN and Serial over LAN.

- 2U all-flash server solution
- 24 x 2.5” front hot-swappable PCIe Gen5 NVMe bays
- Supports Intel® Xeon® 6 Scalable Processors for highest every performance and improved power efficiency
- Supports DDR5 RDIMM and PCIe Gen5 extensions
- Onboard Baseboard Management Controller for system management and IPMI control
- Dedicated BMC management port
- Front-to-back airflow and hot swap redundant fans to provide optimal thermal conditions

Front Panel

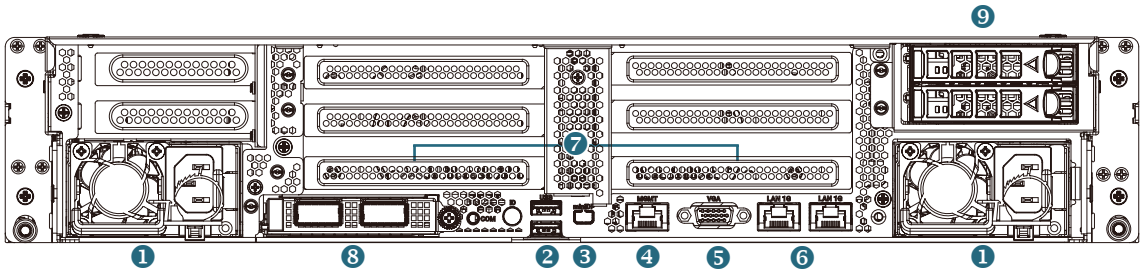


System Button and LED Indicator

Item	Description	Item	Description
	Power Button/LED		LAN1 LED / LAN2 LED
	Drive Activity LED	RST	System Reset Button
ID	System ID Button/LED		System Alert LED

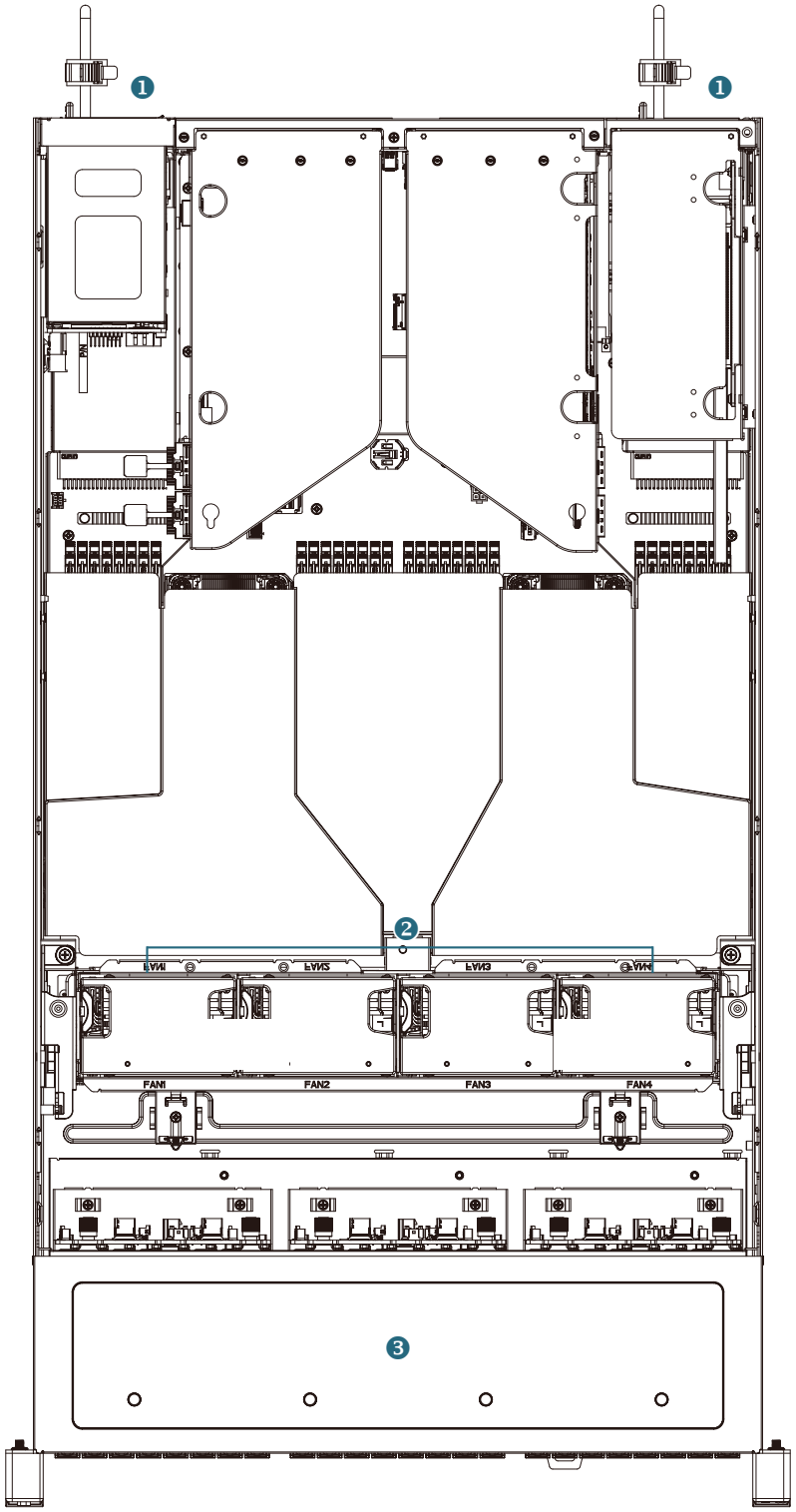
Item	Description
1	2 x USB 3.0
2	1 x VGA port

Rear Panel



Item	Description
1	2000W/2400W 1+1 CRPS 80+ Titanium by CPU/NVMe supporting wattage SKU options
2	2 x USB 3.0 Type A
3	1 x mini-display port connector
4	1x Gbe RJ45 dedicated BMC management
5	1 x external VGA port
6	2 x RJ45 connectors for dual port GbE
7	2 x PCIe 5.0 X16 FHHL/HHHL
8	1 x OCP 3.0
9	2 x 2.5-inch hot swap disk drive bays (SATA, 15mm)

Top View



Item	Description
1	2000W/2400W 1+1 CRPS 80+ Titanium by CPU/NVMe supporting wattage SKU options
2	4 x 80mm hot swap fans
3	24 x 2.5-inch hot swap disk drive

Chapter 2. Hardware Setup

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

2.1 Central Processing Unit

The serverboard supports dual Xeon scalable processors and Socket E2 (LGA 4710).

2.1.1 Installation

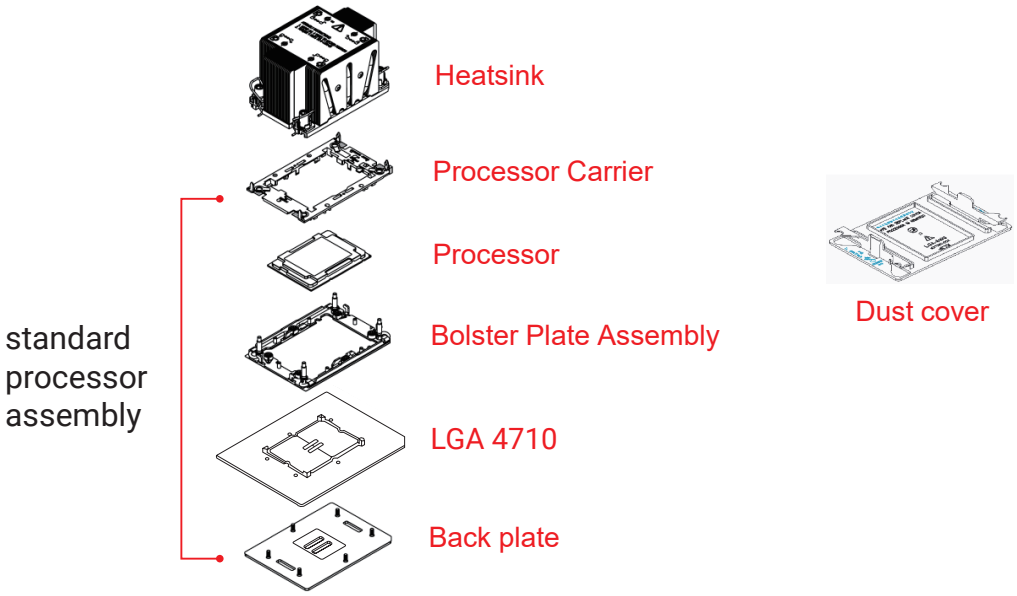
To ensure a safe and easy setup, you need to prepare before installation:

- ☑ 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.

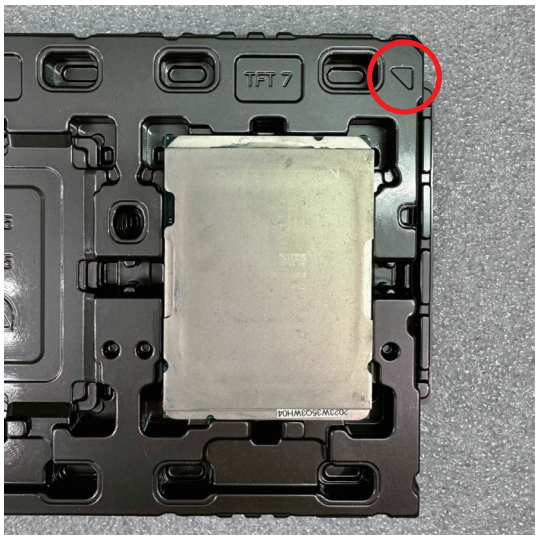


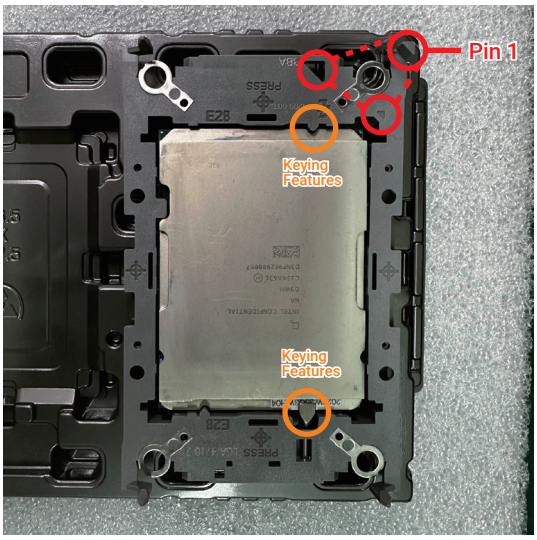
This information is provided for professional technicians only.

Processor Carrier Assembly

Procesures:

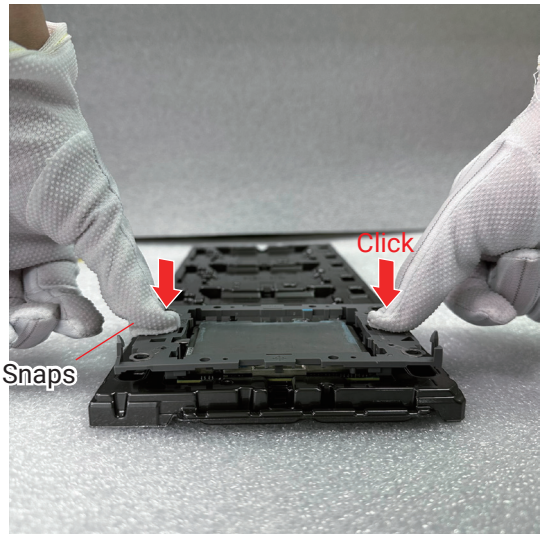
① Place the processor carrier on top of the processor that is in the package tray aligning pin 1 marks on the processor carrier to pin 1 of the processor.

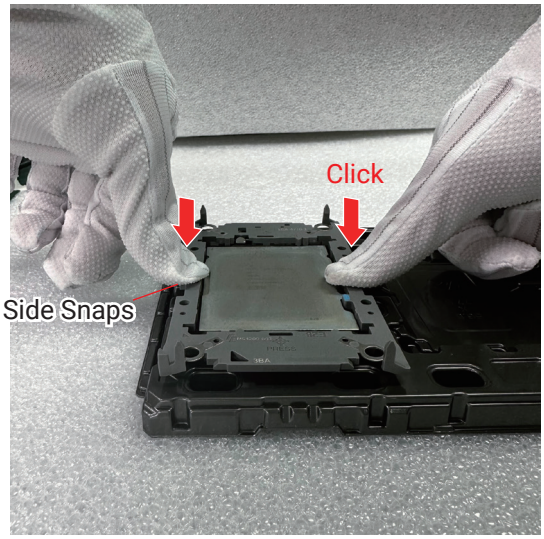




Make sure that the keying feature tabs of the processor carrier are aligned to the slots in the processor properly. If not check that the correct processor carrier is being used.

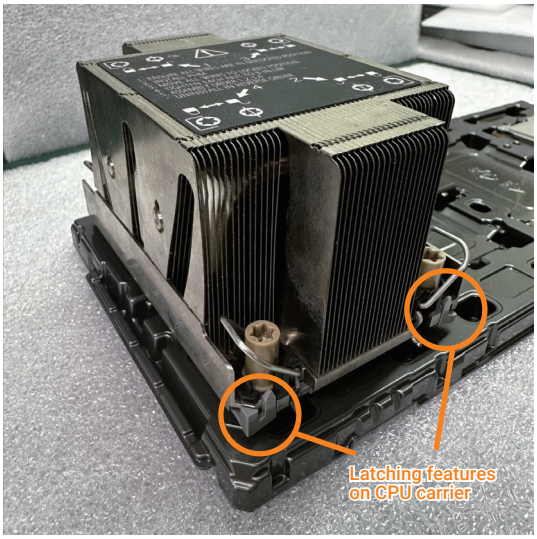
② Using both hands place the thumbs on the side of the carrier at the opposite end of the TIM break lever. Push down on one side at a time slightly pressing in the outward motion until a snap sound is heard.

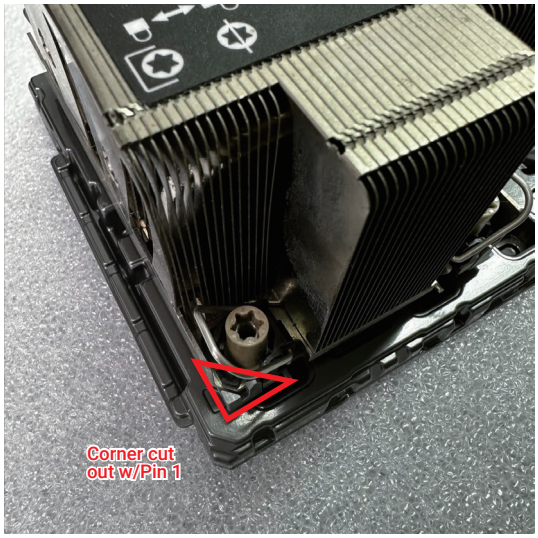




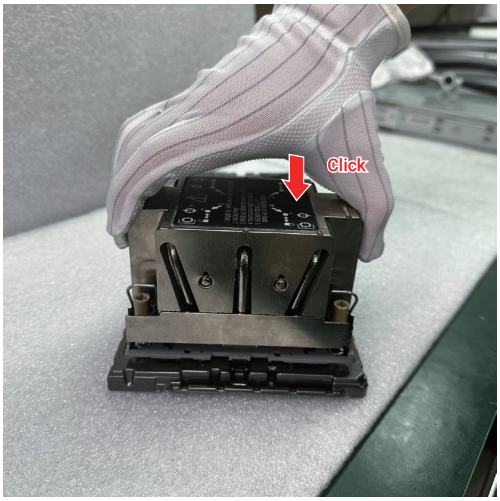
③ Align Pin 1 indicator of Processor carrier and the corner cut out of Heatsink. If there are two corners cut out, either orientation is fine.

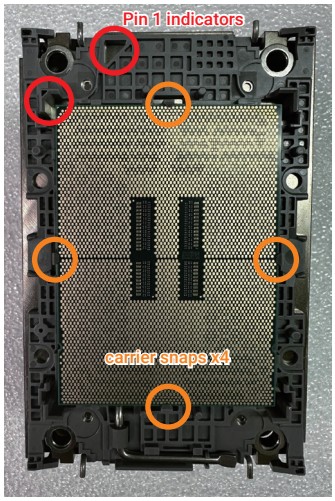
④ Place the heatsink ensure latching features on Processor carrier and heatsink are aligned during assembly.





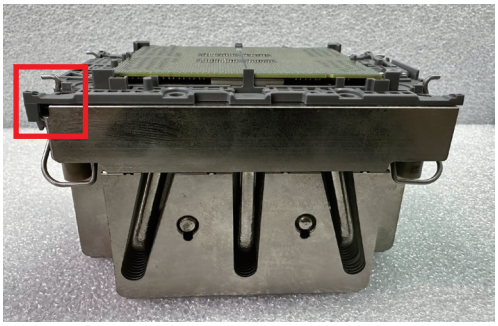
⑤ Press heatsink down firmly to engage carrier latching features to the heatsink at four corners.
⑥ Ensure correct alignment by locating Pin 1 indicators on both processor and processor carrier.





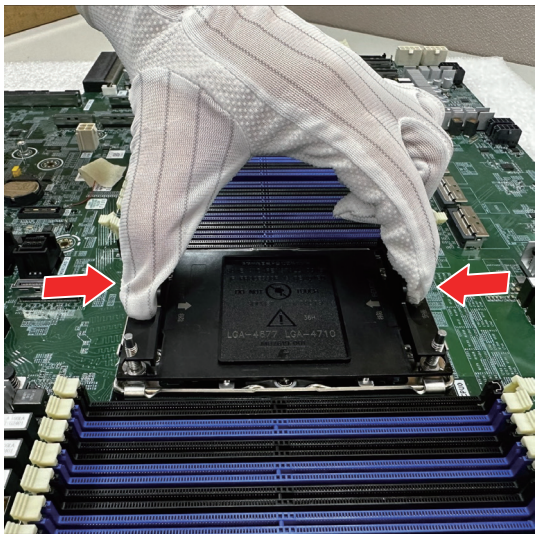
Look at all 4 carrier snaps to verify they are clipped onto package substrate.

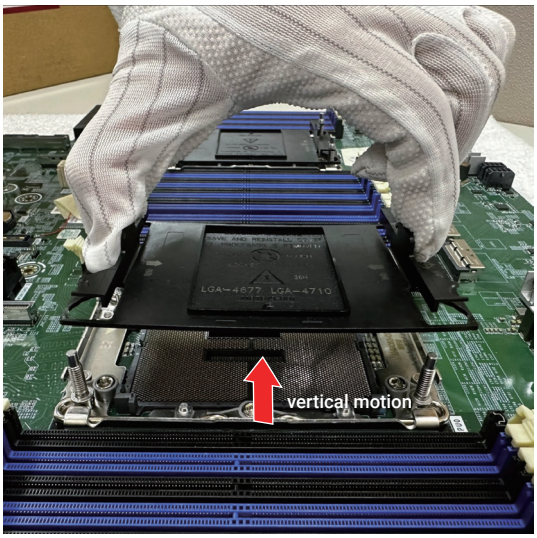
⑦ Verify that the carrier is properly latched to the heatsink at all four corners.

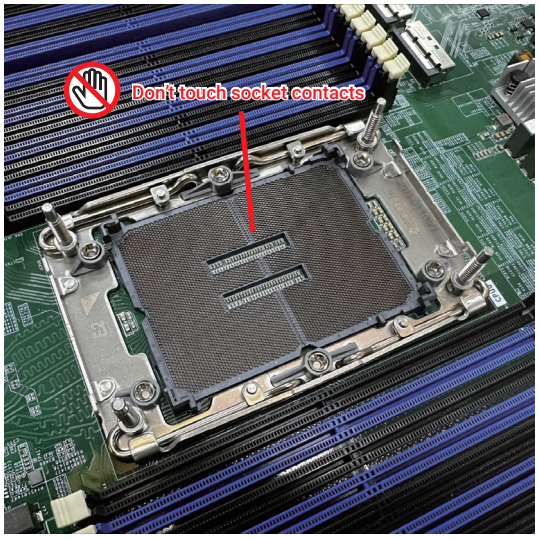


PHM Assembly to Socket

① Remove the socket cover for motherboard. Hold finger grips on socket cover and press inward on the grip tabs. Then pull the cover up and off vertically to remove.

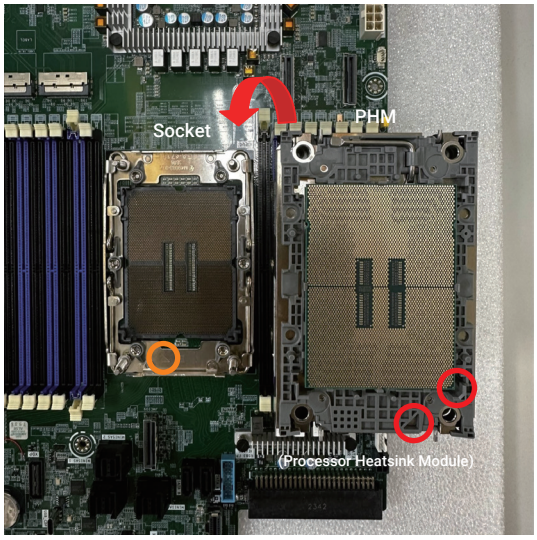




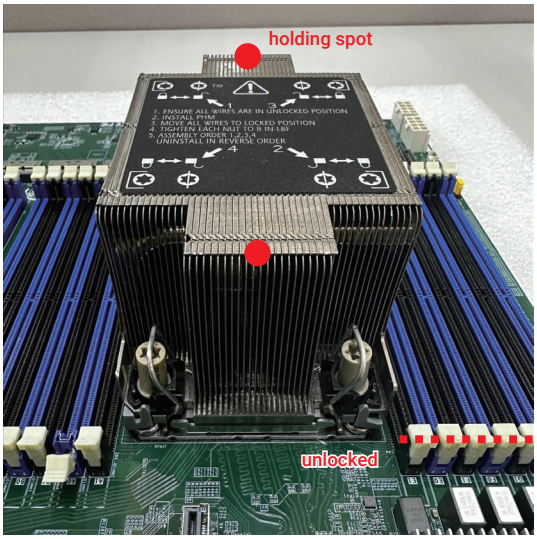


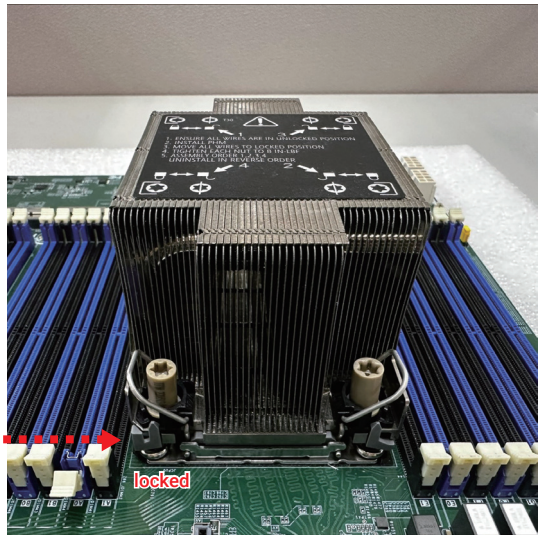
CAUTION
Do not touch socket contacts.

② Align Pin 1 indicators on processor/carrier to PCB Silkscreen Mark.



③ Holding PHM horizontal (with 2 hands), carefully lower vertically to engage PHM to bolster plate's alignment pins. Verify PHM is sitting horizontally over bolster plate assembly.

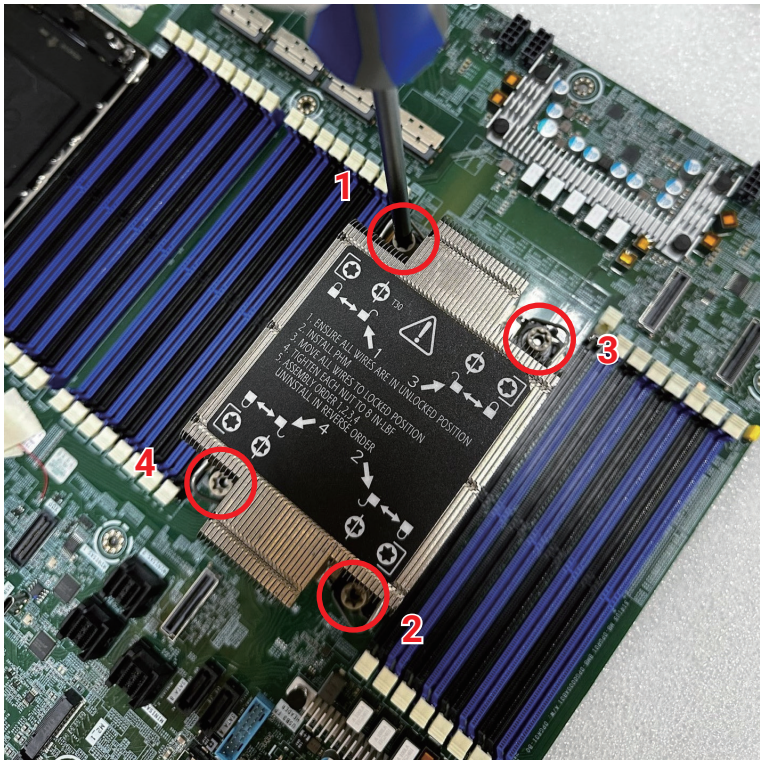




Set all four Anti-Tilt wires into the locked position (outward position).

If anti-tilt wires are not in locked positioned the anti tilt feature will not function properly and damage may occur.

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



This information is provided for professional technicians only.

2.2 System Memory

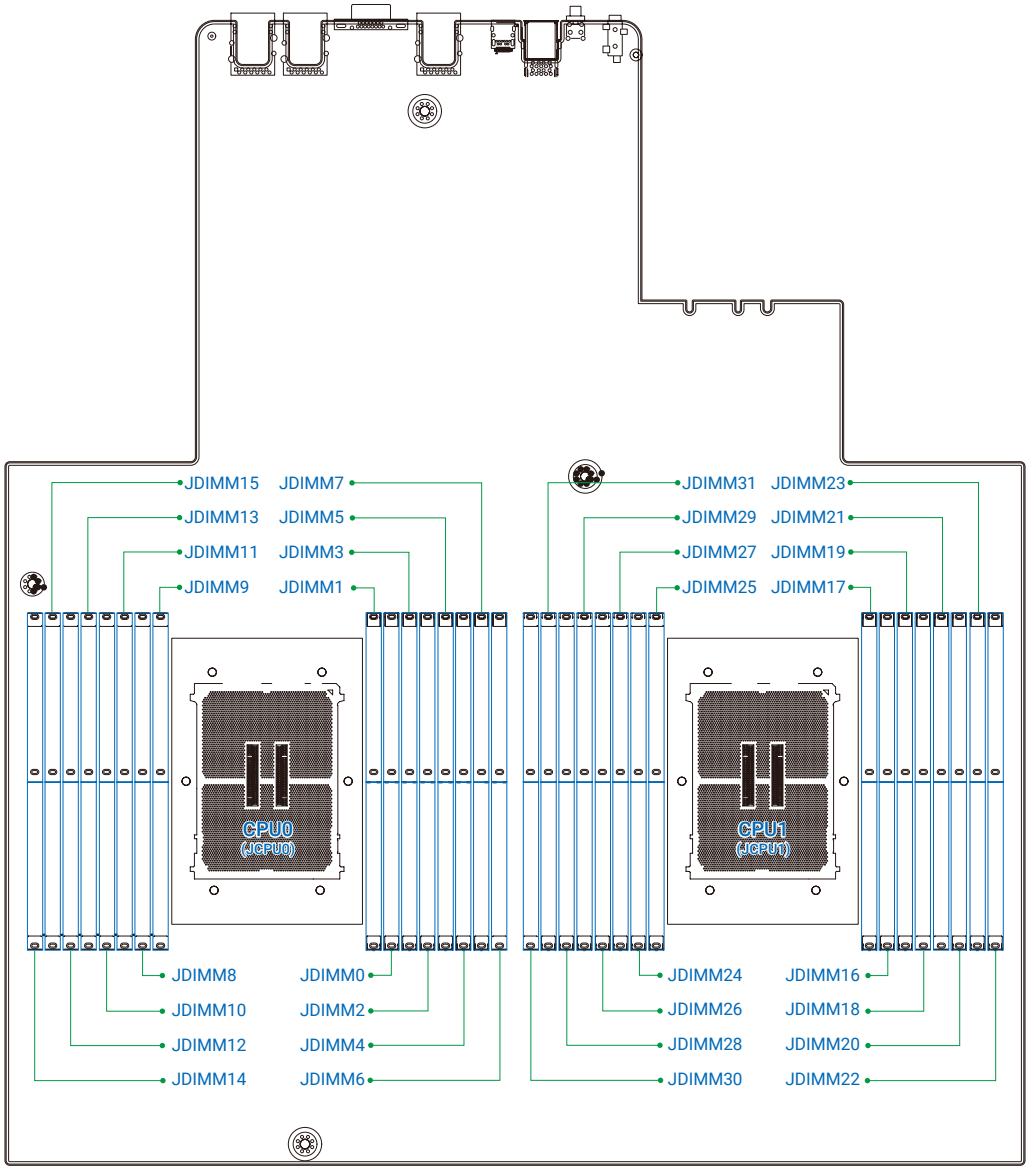
2.2.1 Placement

The DIMMs are displayed on the Sirius board as JDIMM0/JDIMM1/JDIMM2/JDIMM3/JDIMM4/ JDIMM5/JDIMM6/JDIMM7/JDIMM8/JDIMM9/ JDIMM10/JDIMM11/JDIMM12/JDIMM13/ JDIMM14/JDIMM15/JDIMM16/JDIMM17/ JDIMM18/JDIMM19/JDIMM20/JDIMM21/ JDIMM22/JDIMM23/JDIMM24/JDIMM25/ JDIMM26/JDIMM27/JDIMM28/JDIMM29/ JDIMM30/JDIMM31

To ensure satisfactory performance, you need to:

☑ Verify the DIMM type:
This product supports DDR5 RDIMM

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



2.2.2 DIMM Population

NOTE
Rules to abide by before installation:
- Must install at least one DDR5 DIMM per socket.
- 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	4		8			12	16
CPU0	JDIMM0	#	#		#	#		#	#
	JDIMM1					#		#	#
	JDIMM2			#	#		#	#	#
	JDIMM3						#		#
	JDIMM4		#		#	#		#	#
	JDIMM5					#		#	#
	JDIMM6			#	#		#	#	#
	JDIMM7						#		#
	JDIMM8		#		#	#		#	#
	JDIMM9					#		#	#
	JDIMM10			#	#		#	#	#
	JDIMM11						#		#
	JDIMM12		#		#	#		#	#
	JDIMM13					#		#	#
	JDIMM14			#	#		#	#	#
	JDIMM15						#		#

2 CPU Configurations

Placement		DIMM Number							
		1	4		8			12	16
CPU0	JDIMM0	#	#		#	#		#	#
	JDIMM1					#		#	#
	JDIMM2			#	#		#	#	#
	JDIMM3						#		#
	JDIMM4		#		#	#		#	#
	JDIMM5					#		#	#
	JDIMM6			#	#		#	#	#
	JDIMM7						#		#
	JDIMM8		#		#	#		#	#
	JDIMM9					#		#	#
	JDIMM10			#	#		#	#	#
	JDIMM11						#		#
	JDIMM12		#		#	#		#	#
	JDIMM13					#		#	#
	JDIMM14			#	#		#	#	#
	JDIMM15						#		#
Placement		1	4		8			12	16
CPU1	JDIMM16	#	#		#	#		#	#
	JDIMM17					#		#	#
	JDIMM18			#	#		#	#	#
	JDIMM19						#		#
	JDIMM20		#		#	#		#	#
	JDIMM21					#		#	#
	JDIMM22			#	#		#	#	#
	JDIMM23						#		#
	JDIMM24		#		#	#		#	#
	JDIMM25					#		#	#
	JDIMM26			#	#		#	#	#
	JDIMM27						#		#
	JDIMM28		#		#	#		#	#
	JDIMM29					#		#	#
	JDIMM30			#	#		#	#	#
	JDIMM31						#		#

2.2.3 Mapping Table

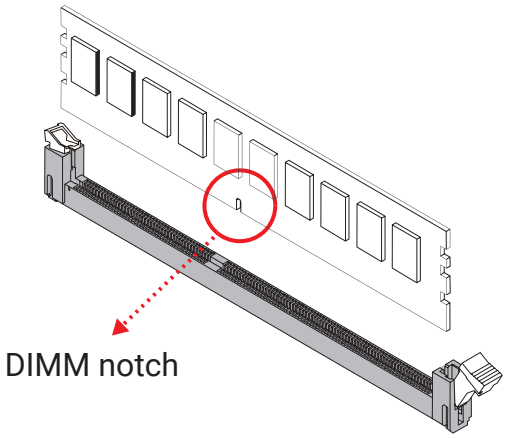
MB Location	Description	PCB silkscreen
CPU0 / CPU1	Lagecy CPU / Non-Lagecy CPU	CPU0 / CPU1
JDIMM0 / JDIMM1	CPU0 Channel A DIMM0 / DIMM1	A0 / A1
JDIMM2 / JDIMM3	CPU0 Channel B DIMM0 / DIMM1	B0 / B1
JDIMM4 / JDIMM5	CPU0 Channel C DIMM0 / DIMM1	C0 / C1
JDIMM6 / JDIMM7	CPU0 Channel D DIMM0 / DIMM1	D0 / D1
JDIMM8 / JDIMM9	CPU0 Channel E DIMM0 / DIMM1	E0 / E1
JDIMM10 / JDIMM11	CPU0 Channel F DIMM0 / DIMM1	F0 / F1
JDIMM12 / JDIMM13	CPU0 Channel G DIMM0 / DIMM1	G0 / G1
JDIMM14 / JDIMM15	CPU0 Channel H DIMM0 / DIMM1	H0 / H1
JDIMM16 / JDIMM17	CPU1 Channel A DIMM0 / DIMM1	A0 / A1
JDIMM18 / JDIMM19	CPU1 Channel B DIMM0 / DIMM1	B0 / B1
JDIMM20 / JDIMM21	CPU1 Channel C DIMM0 / DIMM1	C0 / C1
JDIMM22 / JDIMM23	CPU1 Channel D DIMM0 / DIMM1	D0 / D1
JDIMM24 / JDIMM25	CPU1 Channel E DIMM0 / DIMM1	E0 / E1
JDIMM26 / JDIMM27	CPU1 Channel F DIMM0 / DIMM1	F0 / F1
JDIMM28 / JDIMM29	CPU1 Channel G DIMM0 / DIMM1	G0 / G1
JDIMM30 / JDIMM31	CPU1 Channel H DIMM0 / DIMM1	H0 / H1
JMCIO1 / JMCIO2	CPU0 PE5 Lane 0-7 / 8-15	
JMCIO3 / JMCIO4	CPU0 PE4 Lane 7-0 / 15-8 (Lane Reversal)	
JMCIO5 / JMCIO6	CPU1 PE5 Lane 0-7 / 8-15	
JMCIO7 / JMCIO8	CPU1 PE4 Lane 0-7 / 8-15	
JMCIO9	CPU0 PE0 Lane 0-7	
JMCIO10	CPU1 PE1 Lane 0-7	
JMCIO11 / JMCIO12	CPU1 PE3 Lane 0-7 / 8-15	
JGENZ1	CPU0 PE3 Lane 0-1	GENZ1 CPU0
JGENZ2	CPU1 PE2 Lane 0-15	GENZ2 CPU1
JOCP1	CPU1 PE0 Lane 15-0 (Lane Reversal)	OCP CPU1
JNGFF1 / JNGFF2	CPU0 PE0 Lane 11-8 / 15-12 (Lane Reversal)	M2_1 / M2_2

2.2.4 Installation

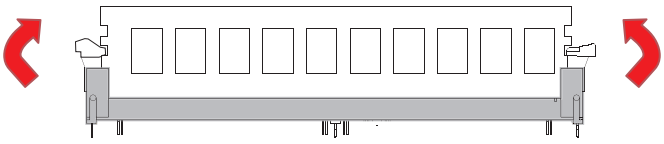
Step 1 Unlock the DIMM socket by pressing the retaining clip outward.



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

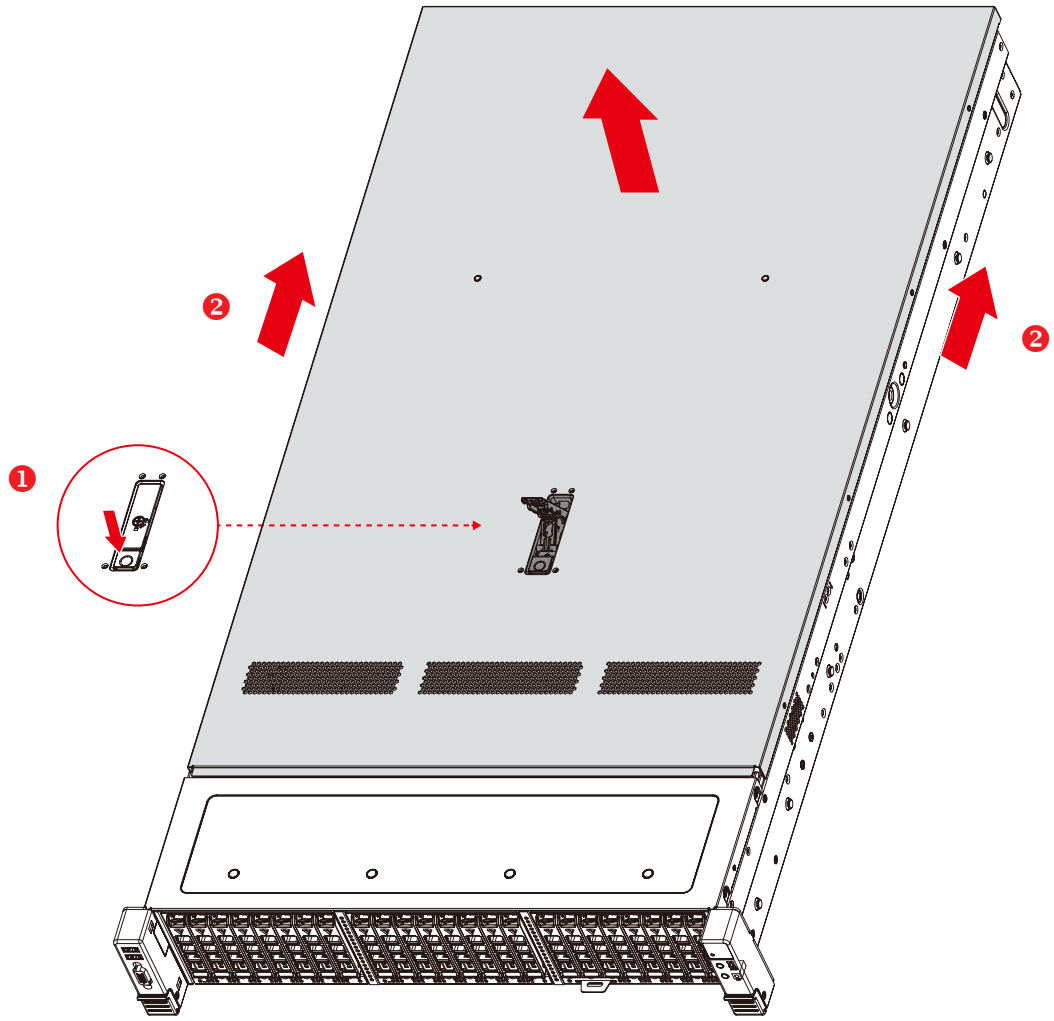


Step 3 Close the retaining clip to complete installation.



2.3 Top Cover

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

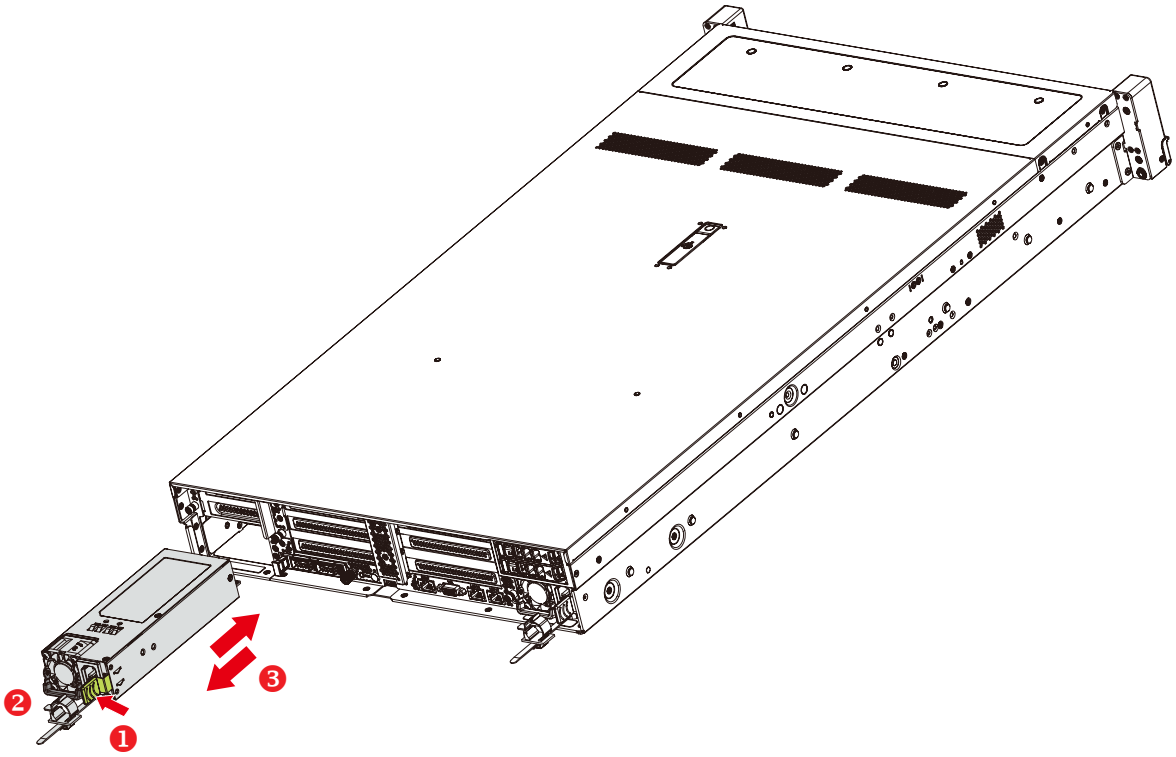


This information is provided for professional technicians only.

2.4 Power Supply Unit

2.4.1 Installation

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



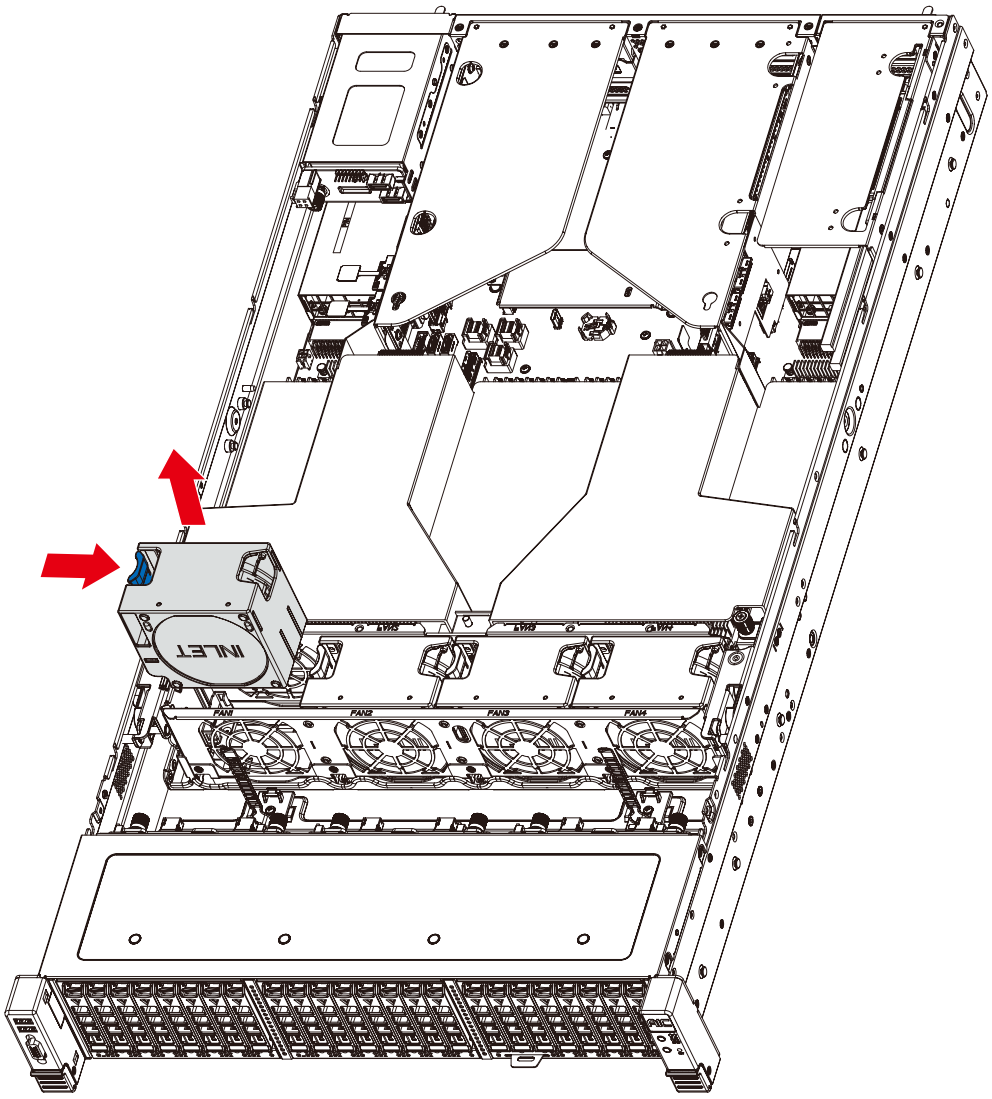
2.4.2 LED Indicator

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

This information is provided for professional technicians only.

2.5 Fan

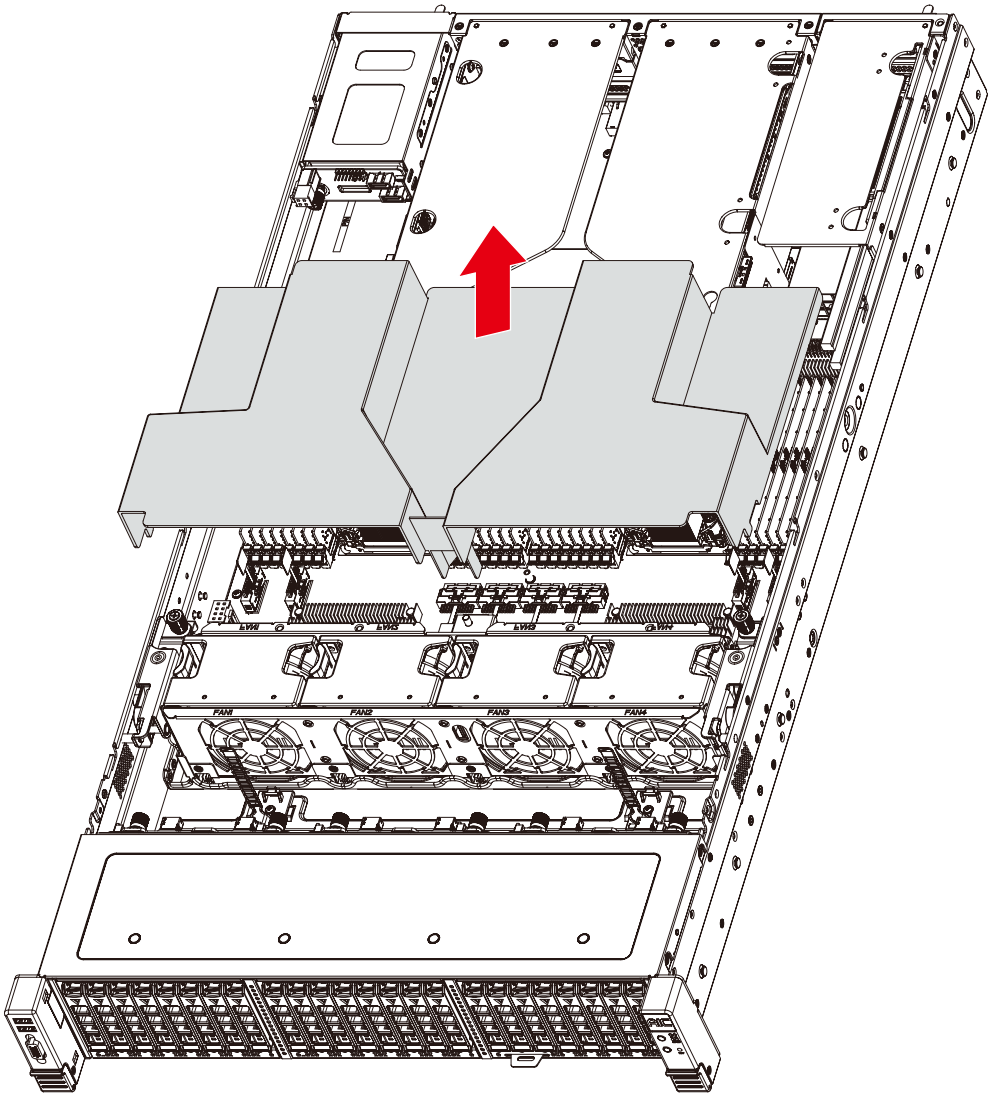
① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Unplug the fan cables and connectors from the server board.
③ Press the latch and pull the top fan out of the chassis.



This information is provided for professional technicians only.

2.6 Air Duct

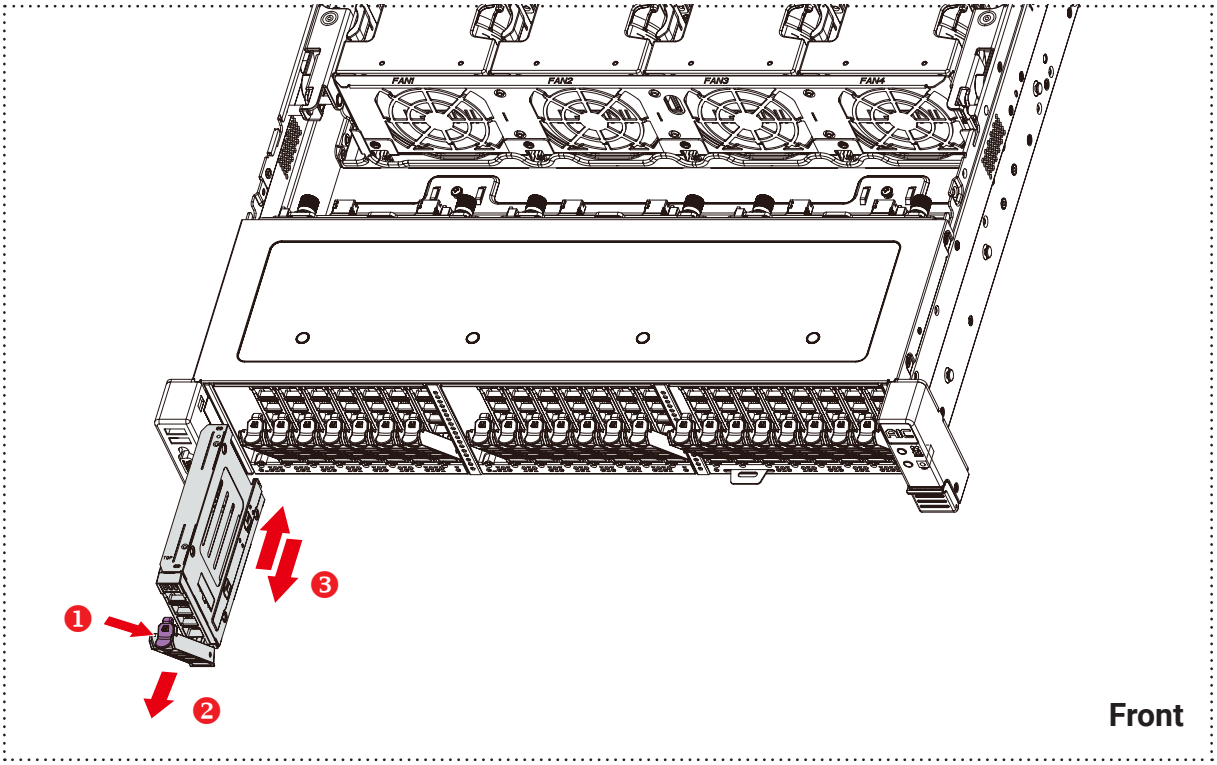
① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Lift the air duct upward to remove it.



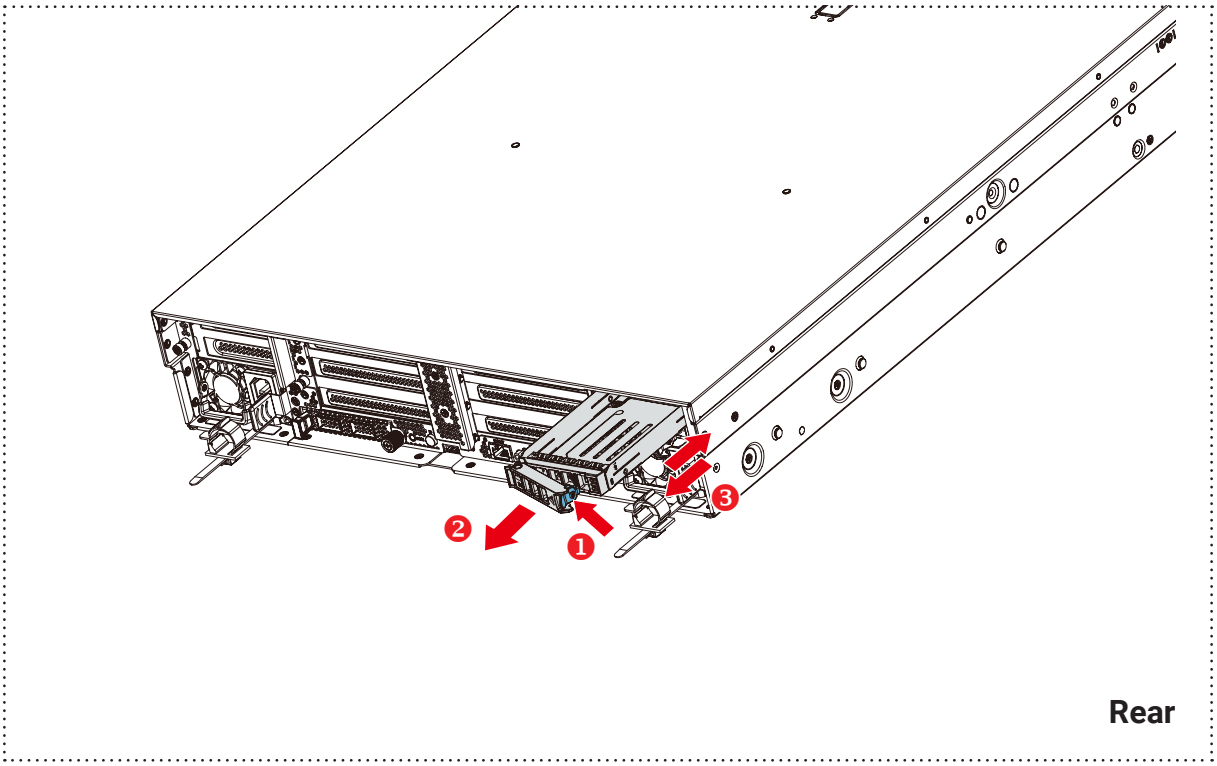
2.7 Disk Drive

2.7.1 Disk Drive: 2.5-inch

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

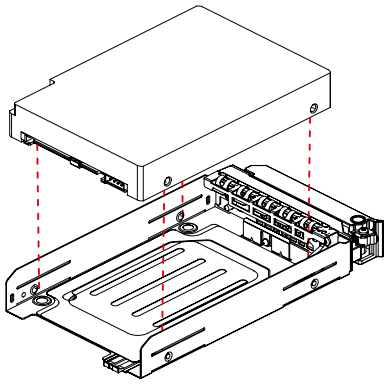


Front

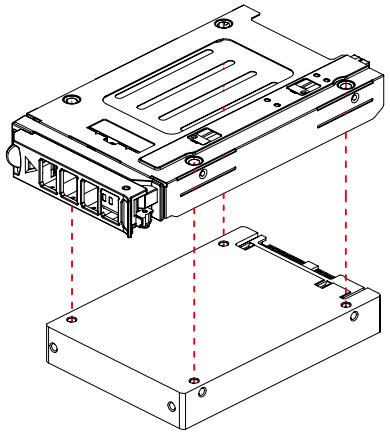


Rear

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



dimple placement



screw placement

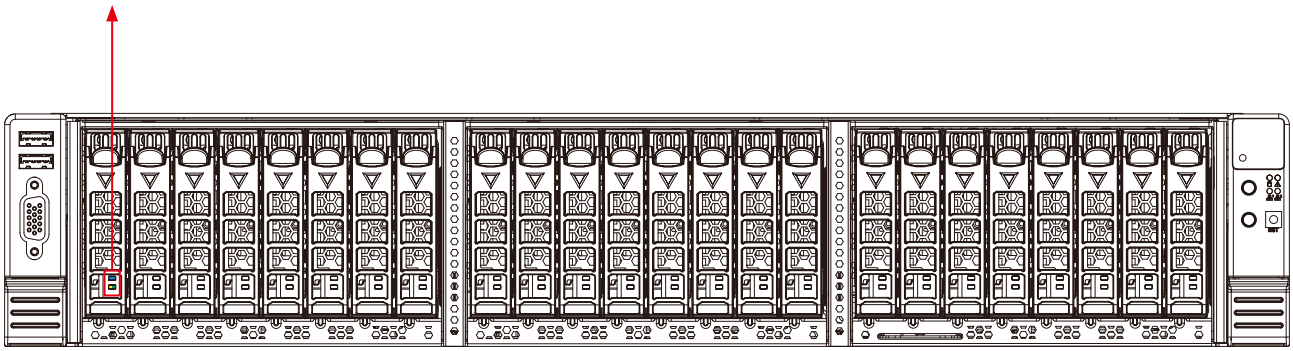
⑤ Push the tray with the installed disk drive into the end of the drive slot in the chassis.
⑥ Close the tray handle.

This information is provided for professional technicians only.

2.7.2 LED Indicator

NVMe

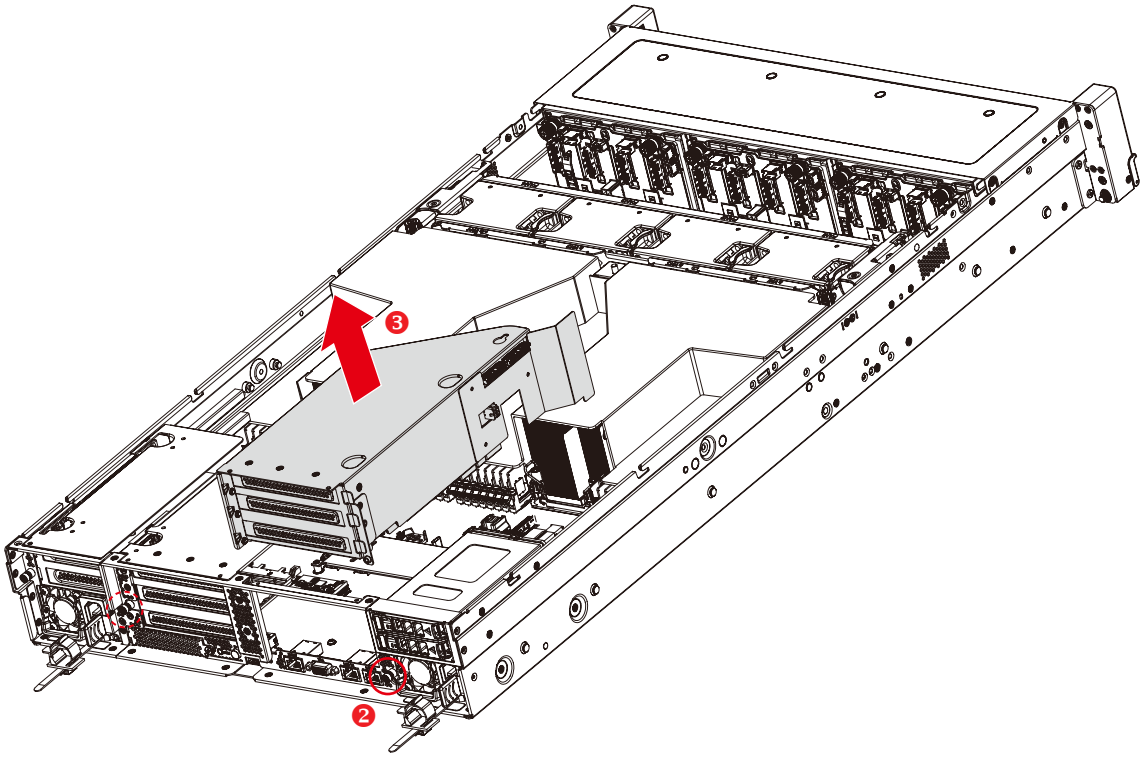
Indicator	Color	Behavior	Description
HDD Activity LEDs	Blue	On	HDD is present.
		Blinking	HDD Activity is detected or External control.
	---	Off	HDD is not connected.
HDD Fail LEDs	Yellow	On	HDD Fault
	Yellow	Blinking	HDD Rebuild
	---	Off	Normal
HDD Locate LED	Green	On	HDD Locate
	---	Off	Normal



Front panel

2.8 Riser Card

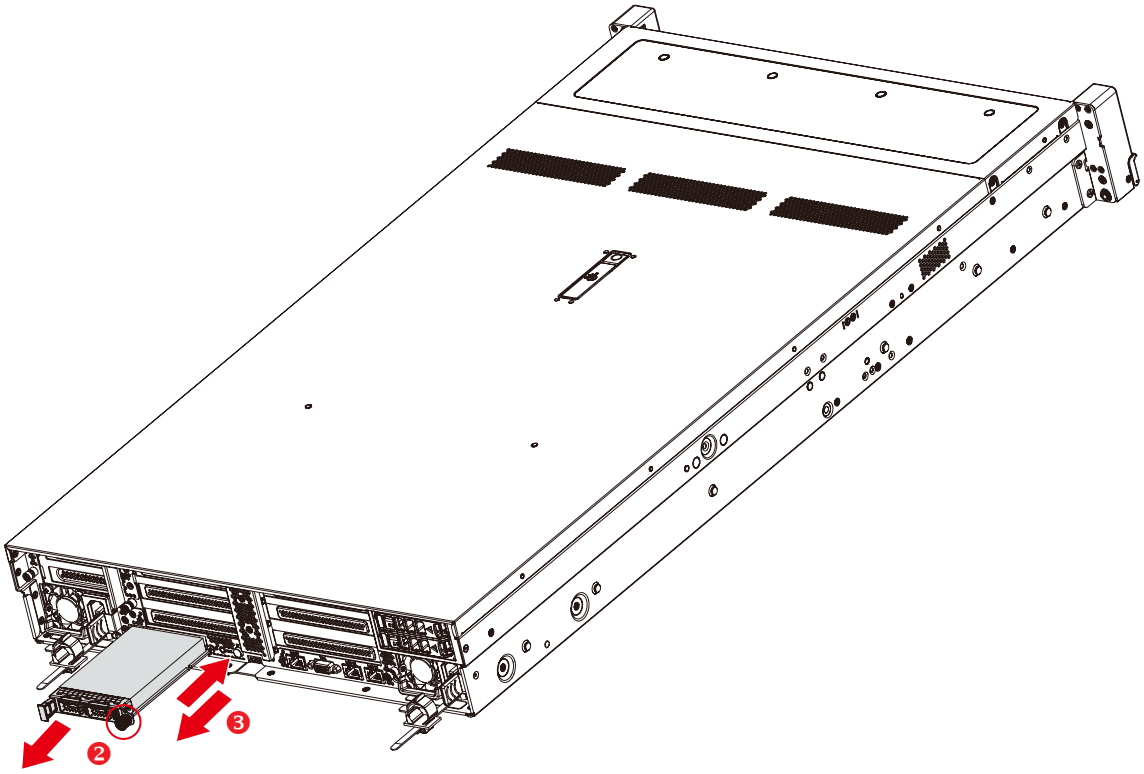
① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Loosen the captive screw (as marked in red circle).
③ Pull up the riser card and insert the PCIe card into the card slot.
④ Insert the replaced riser card into the appropriate card slot. Ensure that the card is properly aligned.



This information is provided for professional technicians only.

2.9 OCP Card

① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Loosen the captive screw.
③ Hold the handle on the left side and pull the OCP card out of the chassis.

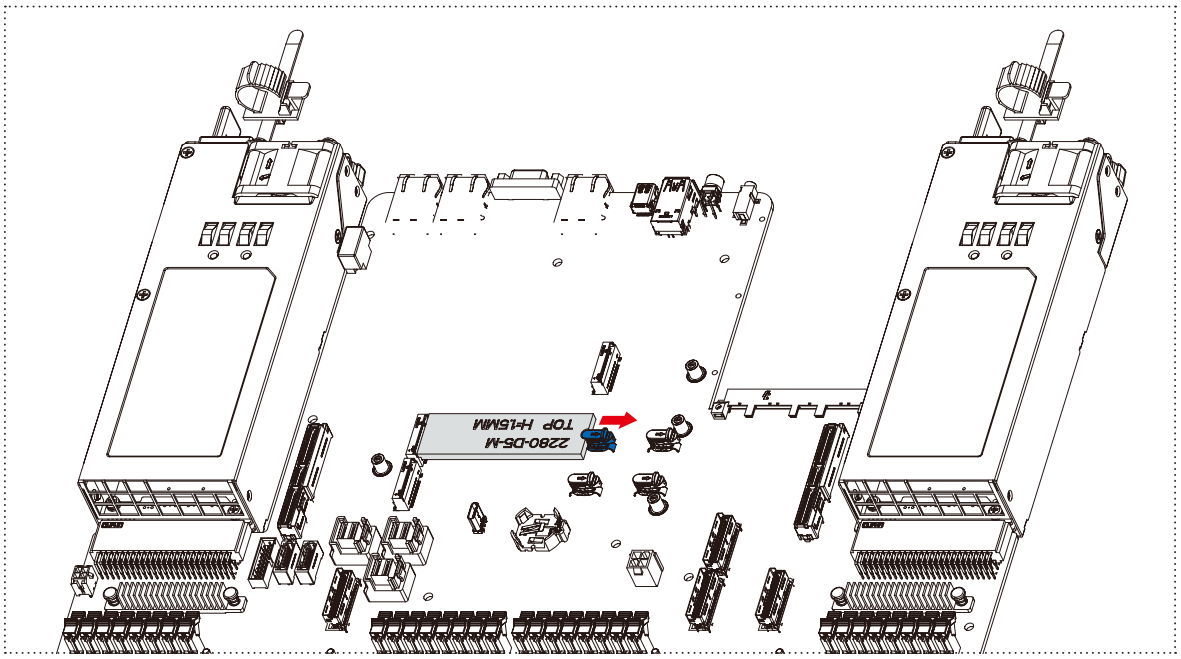


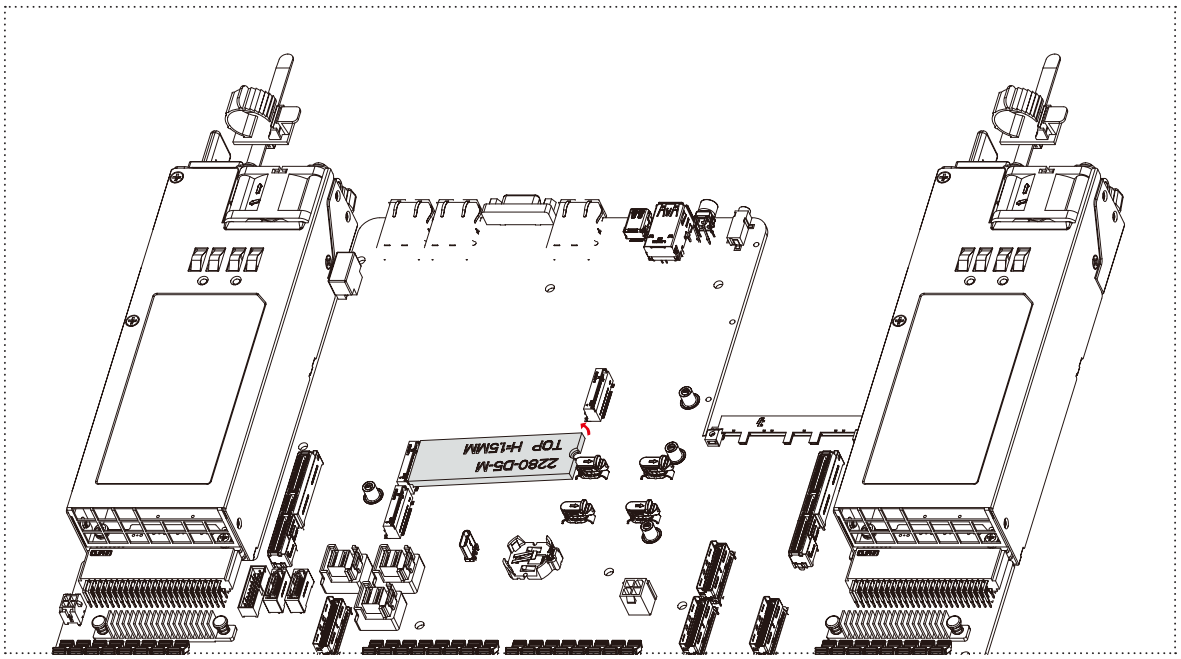
This information is provided for professional technicians only.

2.10 M.2 Card

Removal

① Remove the top cover from the chassis. Please refer to Section 2.3 Top Cover.
② Pull the latch to release the M.2 card. (The M.2 card will automatically pop up.)
③ Remove the M.2 card.





Installation

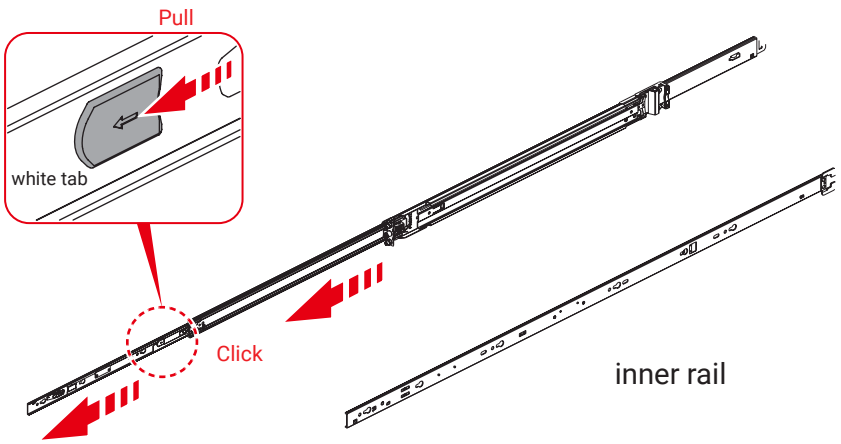
① Follow the steps in a reverse order to install the M.2 card. Align and insert the M.2 card into the socket.

2.11 Slide Rail

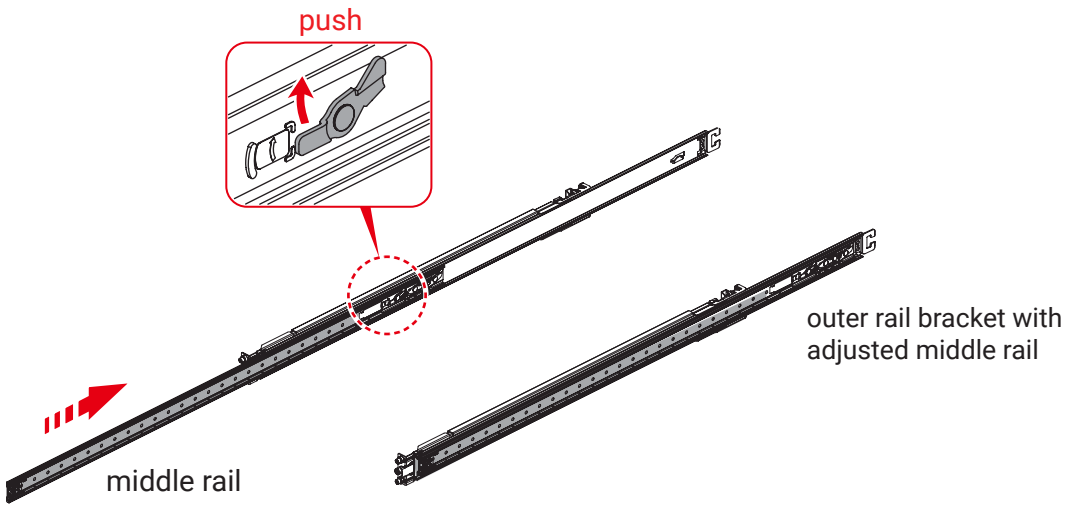
NOTE
This section provides a basic instruction for mounting the slide rail onto the system. Tool-less rails vary per order. The rail in this manual may not exactly match the rail for your system. Please refer to the specifications or quick installation guide that came with your purchased product.

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

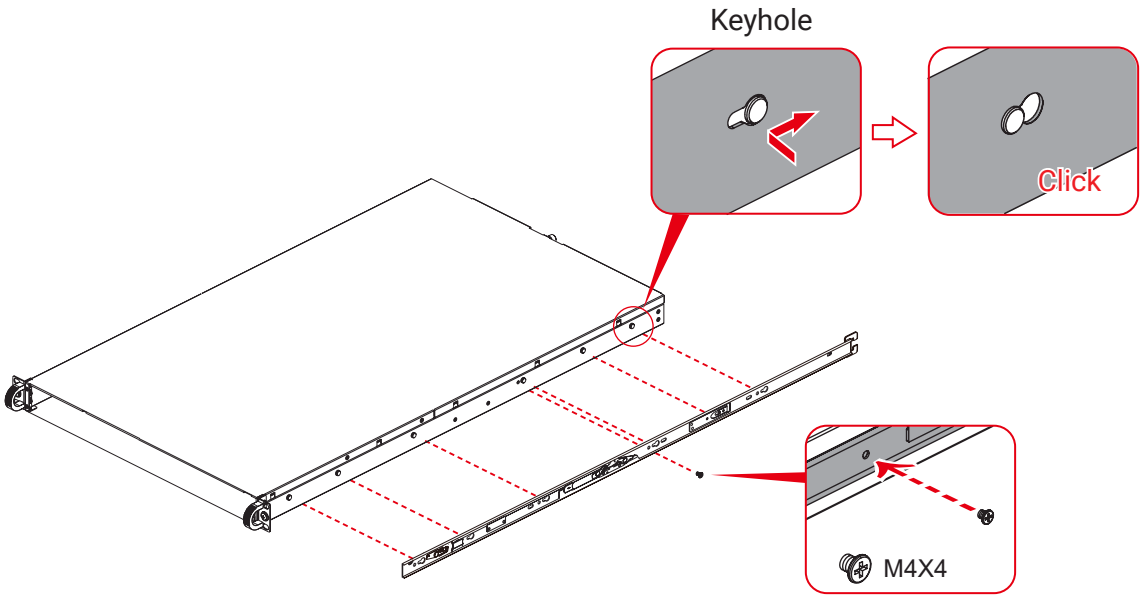
1. Pull the inner rail out of the slide rail until it clicks.
2. Detach the inner rail completely from the slide rail by pulling the white tab forward.



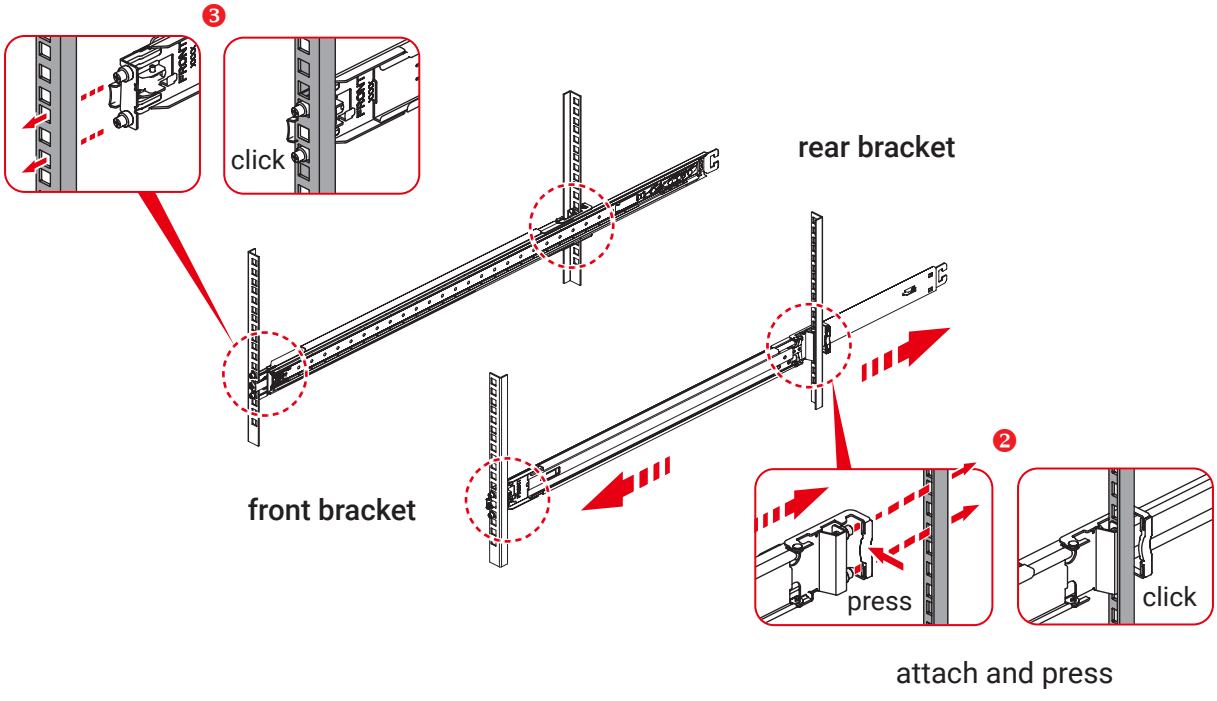
3. After the inner rail is dislodged, adjust the middle rail back to its original position by pushing the tab on the middle rail.



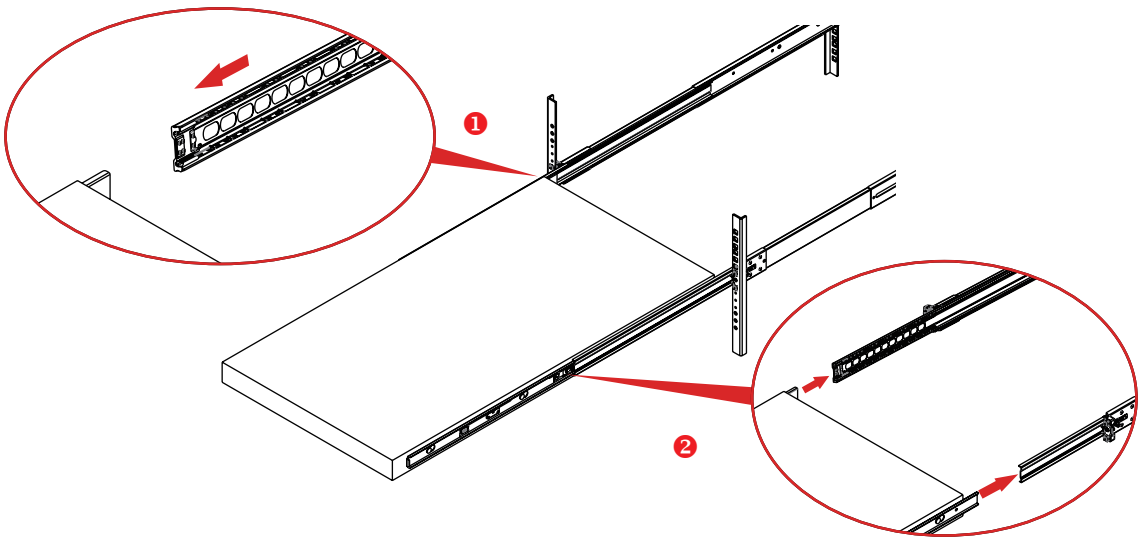
4. Install the inner rail onto the system barebone. Lock the keyholes and secure the screws on sides of the system.



5. Continue installing the outer rail bracket to the mounting frame.
   ① Pull the rear bracket to the fully extended position.
   ② Press the latch to attach the outer rail assembling to the rear bracket.
   ③ Aling the outer rail with the holes on the front bracket and push it onto the frame until it clicks.
   ④ Repeat to fully mount the bracket assembly on the other side.

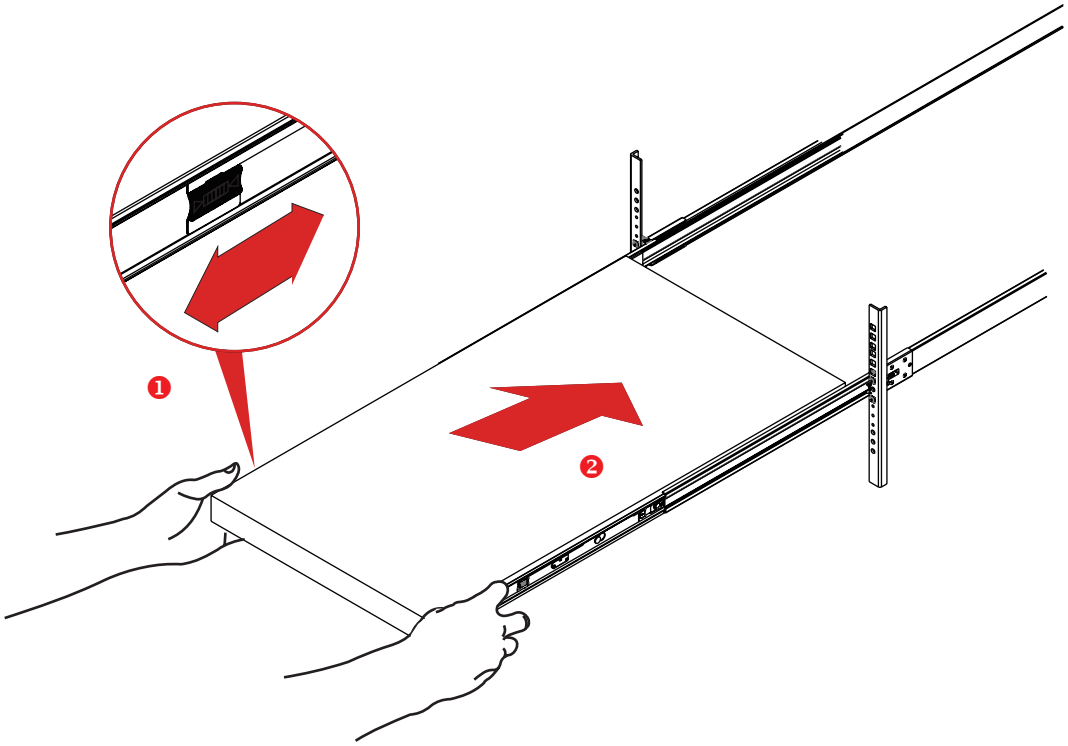


6. Pull out the middle channel until the ball bearing retainer is locked forward.



NOTE
Verify ball bearing retainer is locked forward.

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

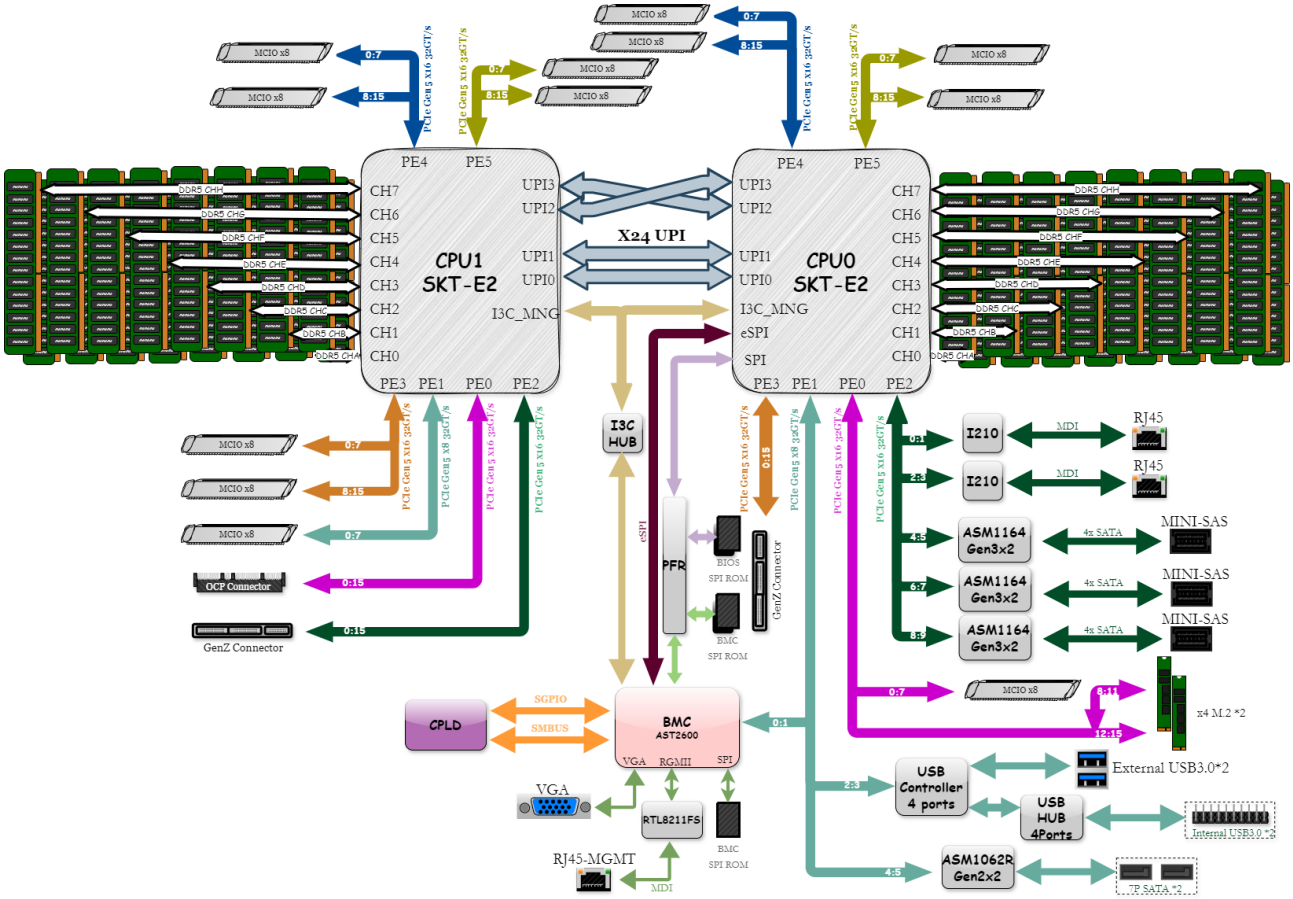


This information is provided for professional technicians only.

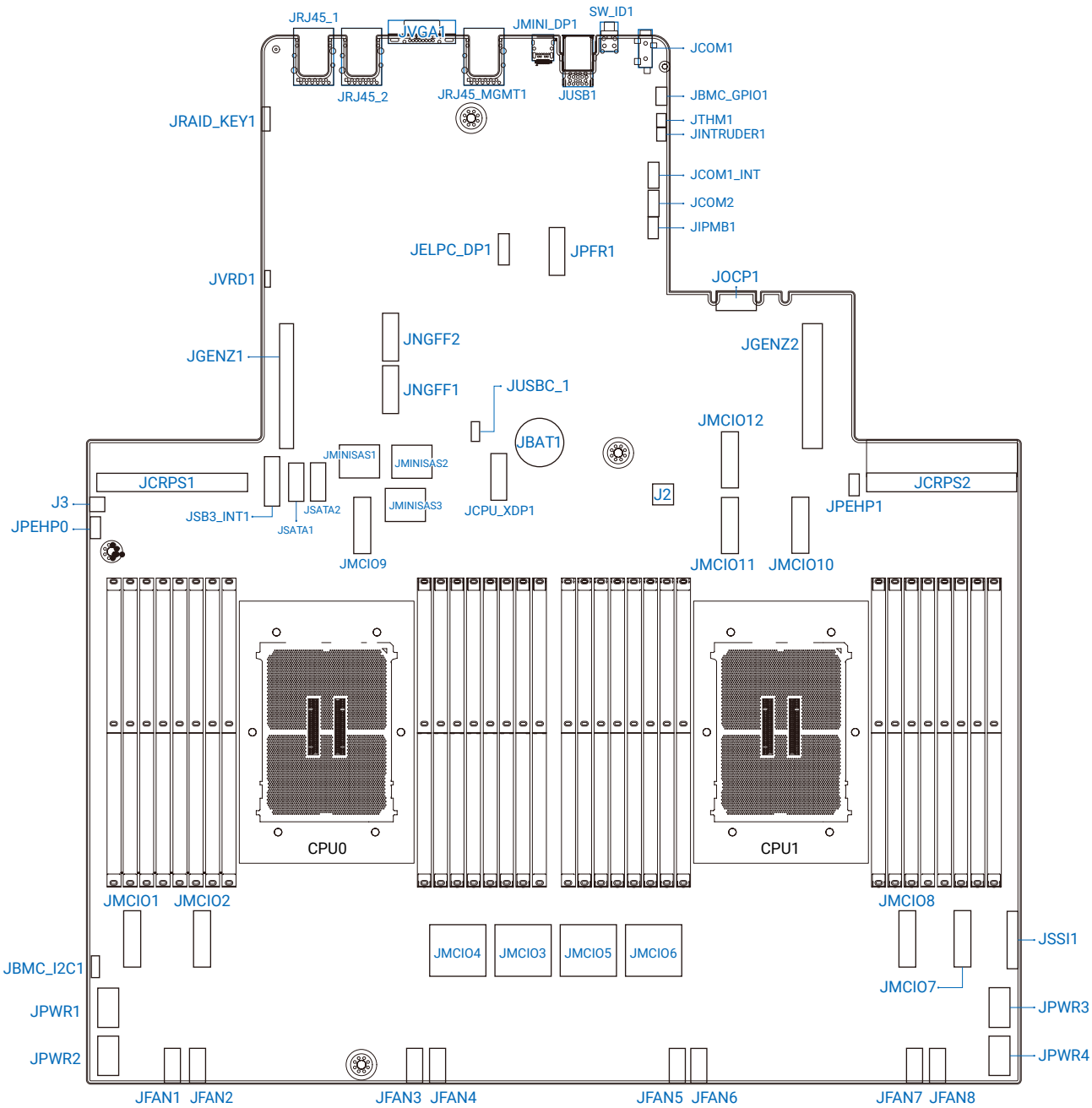
Chapter 3. Hardware Settings

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

3.1 Block Diagram



3.2 Placement



3.3 Content List

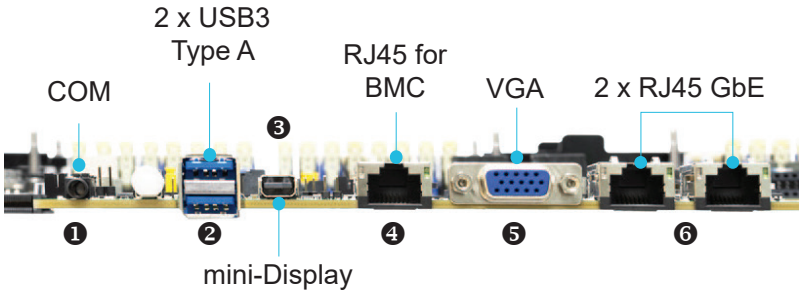
Internal Connectors

Connector	Description	Location
Power CONN(12VOUT)	4 x 2 Pin ATX CONN	JPWR1, JPWR2, JPWR3, JPWR4: 12V
Power CONN(CEM OUT)	2 x 2 Pin ATX CONN	J2: 12V, 3.3V, 3.3VSB
Power CONN(SATA OUT)	2 x 2 Pin Macro-Fit CONN	J3: 12V, 5V
CRPS PWR CONN	50P 2.54mm Power Connector	JCRPS1, JCRPS2
CPU	GNR-SP LGA4710-2	JCPU0, JCPU1
Front Panel	2 x 12 Pin 2.54mm Box Header	JSSI1
Serial ATA	7 Pin 1.27 mm Headers	JSATA1, JSATA2
VGA	2 x 8 Pin 2.0mm Box Header	JVGA1_INT1
COM1	2 x 5 Pin 2.0mm Box Header	JCOM1_INT1
COM2	2 x 5 Pin 2.0mm Box Header	JCOM2
Intruder	2 Pin 2.0mm Box Header	JINTRUDER1
External temperate sensor	2 Pin 2.0mm Box Header	JTHM1
BMC GPIO	2 x 3 Pin 2.0mm Box Header	JBMC_GPIO1
BMC IPMB	4 Pin 2.0mm Box Header	JIPMB1
PFR Module	GEN5_M2_KEY_M_H=8.5MM	JPFR1
eSPI Debug Port	2 x 6 Pin 2.0mm Box Header	JELPC_DP1
M.2 2080/20110	GEN5_M2_KEY_M_H=8.5MM	JNGFF1, JNGFF2
Front USB	2 x 5 Pin 2.0mm Box Header	JUSB3_INT
XDP CONN	Samtec QSH 60-Pin CONN	JCPU_XDP1
CDP CONN	USB type-C CONN	JUSBC_1
Battery Socket	2 Pin Socket	JBAT1
Clear CMOS	3 Pin 2.54mm Header	JCMOS1
DIMM Sockets	288 Pin DDR5 DIMM	JEDEC Specified DDR5 Connector: JDIMM1~32
BMC Debug Port	3 x 1 Pin 2.0mm Header	JBMC_DP1
BIOS SPI ROM Socket	SOIC-16 Socket	JSPI_BIOS1
BMC SPI ROM Socket	SOIC-16 Socket	JSPI_BMC1
BMC Reset	2 x 1 Pin 2.00mm Header	JBMC_RST1
BMC Buzzer	2 x 1 Pin 2.00mm Header	JBUZZER1
NCSI Select 1	3 x 1 Pin 2.00mm Header	JNCSI_SEL1
NCSI Select 2	3 x 1 Pin 2.00mm Header	JNCSI_SEL2
BMC Socflash Enable	2 x 1 Pin 2.00mm Header	JSOC_FLASH1
PCIE Hot-Plug SMB	4 x 2 pin 2.0mm Box Header	JPEHP0, JPEHP1
FAN CONN	4 x 2 Pin 3.0mm Box Header	JFAN1~JFAN8
BMC Disable	2 x 1 Pin 2.00mm Header	JBIOS_MUX1
BIOS Select 1	3 x 1 Pin 2.00mm Header	JBIOS_MUX2
BMC Select 1	3 x 1 Pin 2.00mm Header	JBMC_MUX1
BMC Clear Password	2 x 1 Pin 2.00mm	JCLR_PSWD1

External Connectors (rear panel)

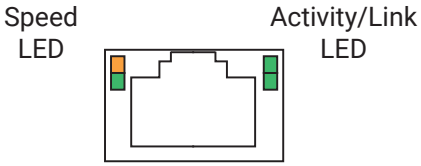
Connector	Description	Comments
Ethernet x2	RJ45	JRJ45_1, JRJ45_2: 10/100/1000M NIC (Intel I210)
VGA	DSUB 15 Pin Blue Female	JVGA1
USB3.0 x2	USB3.0 Type A	JUSB1
MINI-DP	MINI Display	JMINI_DP1
Ethernet x1	RJ45	JRJ45_MGMT1: 10/100/1000M PHYCEIVER (RTL8211FS)
SERIAL PORT	Phone Jack	JCOM1 (Baud Rate : 115200)

3.4 External Port



	Item
1	COM by Audio Jack (Baud Rate : 115200)
2	2 x USB 3.0 Type-A
3	mini-Display
4	RJ45 for BMC management
5	VGA Port
6	LAN RJ45 Port 1GbE

LAN LED Indicator

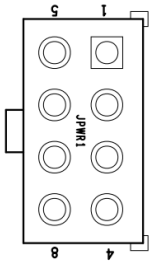


Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.

3.5 Connector Definition

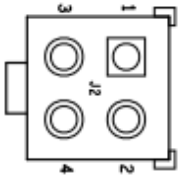
The main connector shall be 4pin x2, 2Pinx2, 2Pinx2 connector to support HDD BP, SATA BP, CEM, Riser and GPU card.

Power Connector (JPWR1, JPWR2, JPWR3, JPWR4)



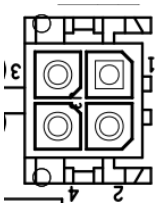
P12V_PSU	5	1	GND
P12V_PSU	6	2	GND
P12V_PSU	7	3	GND
P12V_PSU	8	4	GND

Power Connector (J2)



P3V3_AUX	3	1	P12V_PSU
GND	4	2	P3V3

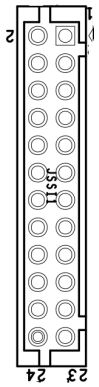
Power Connector (J3)



P12V_PSU	3	1	GND
P5V	4	2	GND

LED/Bezel Button Header (JSSI1)

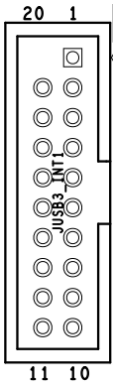
This is a 2x12-pin front panel header.



FP_HDR_PWR_LED	2	1	P3V3_AUX
NC	4	3	P5V_AUX
FP_PWR_LED_L	6	5	ID_LED_OUT_N
HDD_LED_P	8	7	SYS_HEALTH2#
HDD_LED_N	10	9	SYS_HEALTH#
FP_PWR_BTN_N	12	11	LAN1_ACTLED_PWR
GND	14	13	LAN1_ACTLED_N
FP_RST_BTN_N	16	15	SMBUS_SDA
GND	18	17	SMBUS_SCL
BMC_ID_IN_N	20	19	CHASSIS_OPEN
P3V3_AUX	22	21	LAN 2_ACTLED_PWR
FP_NMI_BTN_N	24	23	LAN2 _ACTLED_N

Front I/O USB Header (JUSB3_INT1)

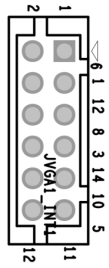
This is a 19-pin header that used to provide front I/O USB functionality.



		1	P5V_USB23
P5V_USB23	19	2	USB3_HUB_RX_R_DN2
USB3_HUB_RX_R_DN1	18	3	USB3_HUB_RX_R_DP2
USB3_HUB_RX_R_DP1	17	4	GND
GND	16	5	USB3_HUB_TX_R_DN2
USB3_HUB_TX_R_DN1	15	6	USB3_HUB_TX_R_DP2
USB3_HUB_TX_R_DP1	14	7	GND
GND	13	8	USB2_HUB_R_DN2
USB2_HUB_R_DN1	12	9	USB2_HUB_R_DP2
USB2_HUB_R_DP1	11	10	USB_HUB_OCI2_N(NC)

Front VGA Header (JVGA1_INT1)

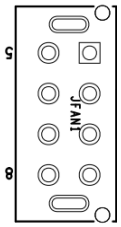
This is a 2x8-pin header that used to provide front VGA functionality.



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

FAN Header (JFAN1~JFAN8)

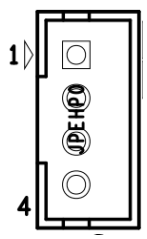
This is a 2x4-pin FAN header.



P12V_FANx	5	1	P12V_FANx
GND	6	2	GND
FANxA_R_TACH	7	3	FANxB_R_TACH
FANx_R_PWM	8	4	FANx_PRSNT_R_N

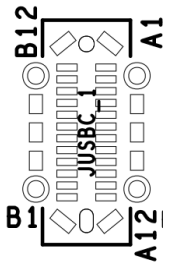
PCIe Hot-Plug Header (JPEHP0, JPEHP1)

This is a 1x4-pin header that used to provide PCIe Hot-Plug functionality.



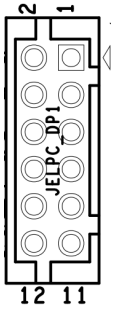
1	HP_HDR_CPUx_SCL
2	HP_HDR_CPUx_SDA
3	GND
4	HP_ALERT_CPUx_R_N

PMBus Header (JUSBC_1)
This USB type-C Connector is used to provide CPU Debug CDP functionality.



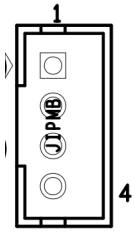
GND	A1	B12	GND
NC	A2	B11	NC
NC	A3	B10	NC
P5V_AUX	A4	B9	P5V_AUX
NC	A5	B8	I3C_DBG_TYPEC_LVC18_SDA
NC	A6	B7	NC
NC	A7	B6	NC
I3C_DBG_TYPEC_LVC18_SCL	A8	B5	NC
P5V_AUX	A9	B4	P5V_AUX
NC	A10	B3	NC
NC	A11	B2	NC
GND	A12	B1	GND

IPMB Header (JELPC_DP1)
This is a 2x6-pin header that used to provide eSPI Debug Port functionality.



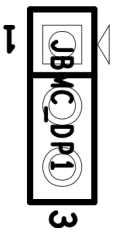
ESPI_DBP_CLK	2	1	GND
ESPI_DBP_CS_N	4	3	NC
ESPI_DBP_RST_N	6	5	ESPI_DBP_ALERT_N
ESPI_DBP_D3	8	7	ESPI_DBP_D2
P3V3_AUX	10	9	ESPI_DBP_D1
ESPI_DBP_D0	12	11	GND

BMC IPMB Header (JIPMB1)
This is a 1x4-pin header that used to provide BMC I2C14 IPMB functionality.



1	BMC_I2C_14_SDA
2	GND
3	BMC_I2C_14_SCL
4	NC

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



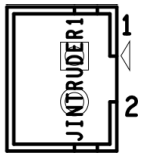
1	SPE_TXD
2	GND
3	SPE_RXD

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



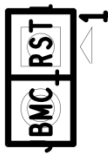
1	P5V
2	BMC_BUZZER-

Chassis Intrusion Header (JINTRUDER1)
This is a 1x2-pin header hat used to provide chassis intrusion functionality.



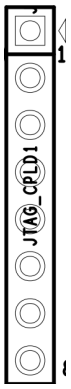
1	CHASSIS_OPEN
2	GND

BMC RESET Header (JBMC_RST1)
This is a 1x2-pin header that used to provide BMC RESET functionality.



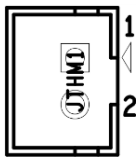
1	BMC_RESET
2	GND

CPLD JTAG Header (JTAG_CPLD1)
This is a 1x8-pin header that used to provide CPLD JTAG functionality.



1	P3V3_STBY
2	JTAG_CPLD_TDO
3	JTAG_CPLD_TDI
4	PU_JTAG_CPLD_P4
5	NC
6	JTAG_CPLD_TMS
7	GND
8	JTAG_CPLD_TCK

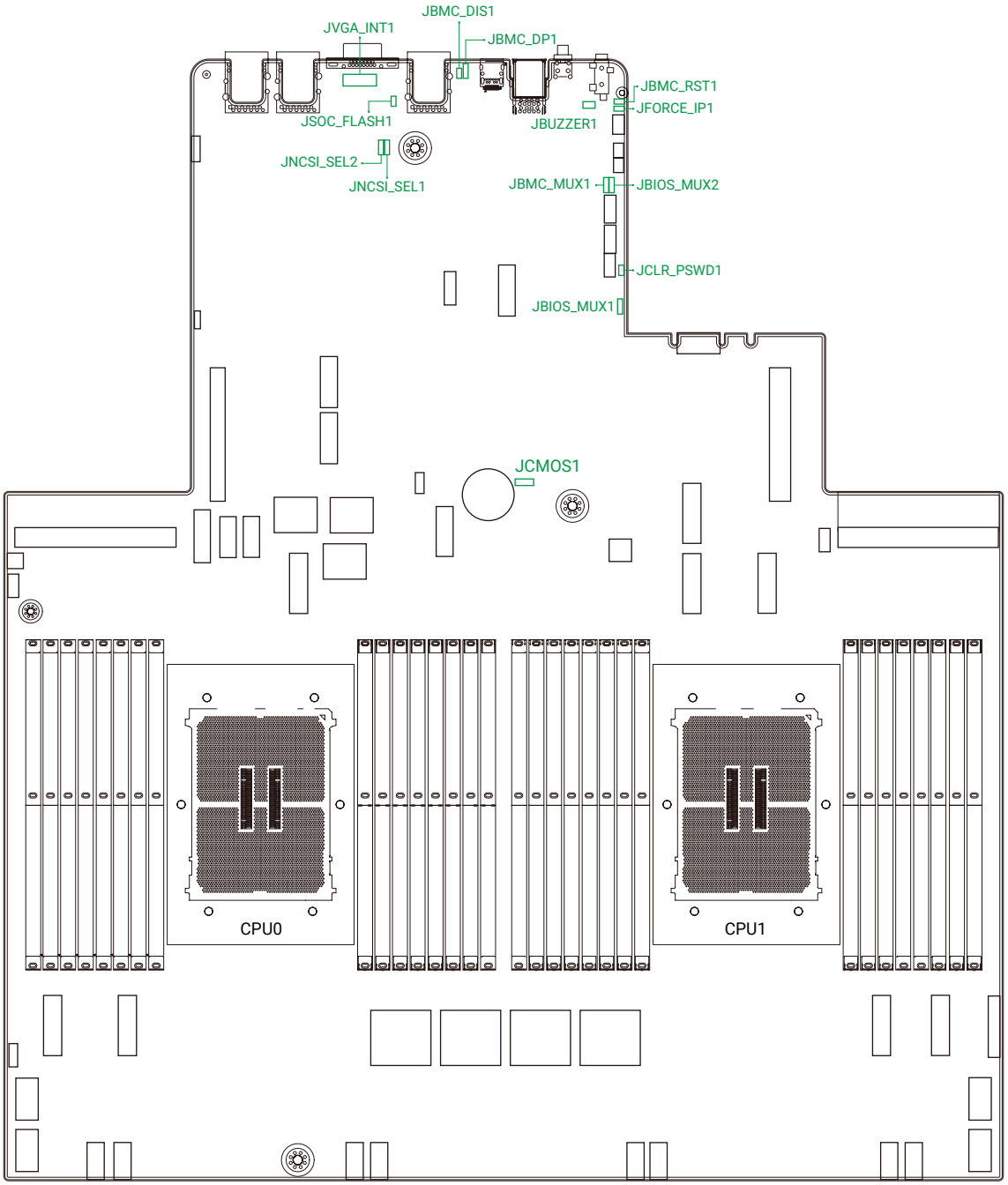
THM Pin Header (JTHM1)
This is a 1x2-pin header that used to external temperate senor functionality.



1	HM0_TD2_DP
2	HM0_TD2_DN

3.6 Jumper Definition

Location



CMOS Jumper (JCMOS1)

JCMOS1	Setting	
Pin1-2	Clear CMOS	
Pin2-3	Normal	Default

BMC Reset Jumper (JBMC_RST1)

JBMC_RST1	Setting	
Short	Reset BMC	
Open	Normal	Default

BMC Disable Jumper (JBMC_DIS1)

JBMC_DIS1	Setting	
Short	Disable BMC ARM boot	
Open	Normal	Default

CPU SPI Flash Jumper (JBIOS_MUX1, JBIOS_MUX2)

JBIOS_MUX1	JBIOS_MUX2	Setting	
Pin1-2	Pin1-2	CPU to Flash Bypass	Default
Pin1-2	Pin2-3	CPU to PFR Module	
Pin2-3	Pin1-2	BMC to Flash Bypass	
Pin2-3	Pin2-3	BMC to PFR Module	

NCSI Jumper (JNCSI_SEL1, JNCSI_SEL2)

JNCSI_SEL1	JNCSI_SEL2	Setting	
Pin1-2	Pin1-2	OCP	Default
Pin2-3	Pin1-2	I210_0	
Pin2-3	Pin2-3	I210_1	

I3C_CDP Jumper (JI3C_CDP1)

JI3C_CDP1	Setting	
Short	MBP MODE	Default
Open	I3C CDP MODE	

BMC Socflash Configurations Jumper (JSOC_FLASH1)

JSOC_FLASH1	Setting	
Short	Enable	
Open	Disable	Default

BMC SPI MUX Jumper (JBMC_MUX1)

JBMC_MUX1	Setting	
Pin1-2	BMC to PFR Module	
Pin2-3	BMC to Flash Bypass	Default

I3C SPD Switch Jumper (JNCSI_SEL1)

JNCSI_SEL1	Setting	
Pin1-2	Normal	Default
Pin2-3	Force on CPU to DIMM	

PMBUS Power select Jumper (JPMBUS_SEL1)

JPMBUS_SEL1	Setting	
Pin1-2	P3V3_AUX	Default
Pin2-3	P5V_AUX	

BMC Password Clear (JCLR_PSWD1)

JCLR_PSWD1	Setting	
Pin1-2	Enable	
Pin2-3	Disable	Default

3.7 LED

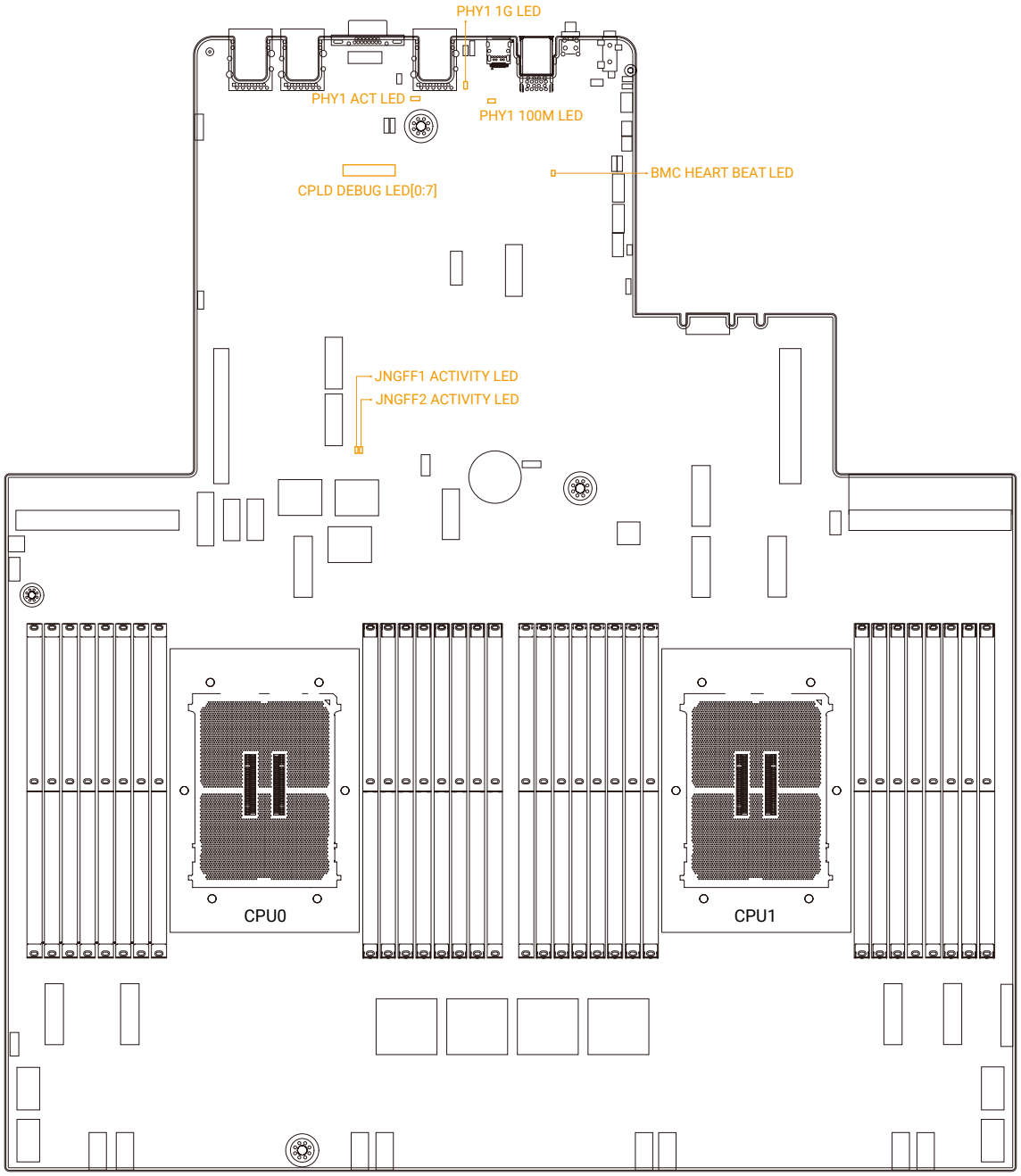
3.7.1 Rear Chassis LEDs

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

Item		Color	Behavior
NIC 1 – JRJ45_1	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off
NIC 2 – JRJ45_2	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off
PHY 1 – JRJ45_ MGMT1	Right	Green (Blinking)	PHY1 activity detected
		Off	PHY1 is not active, LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off

3.7.2 Internal LEDs

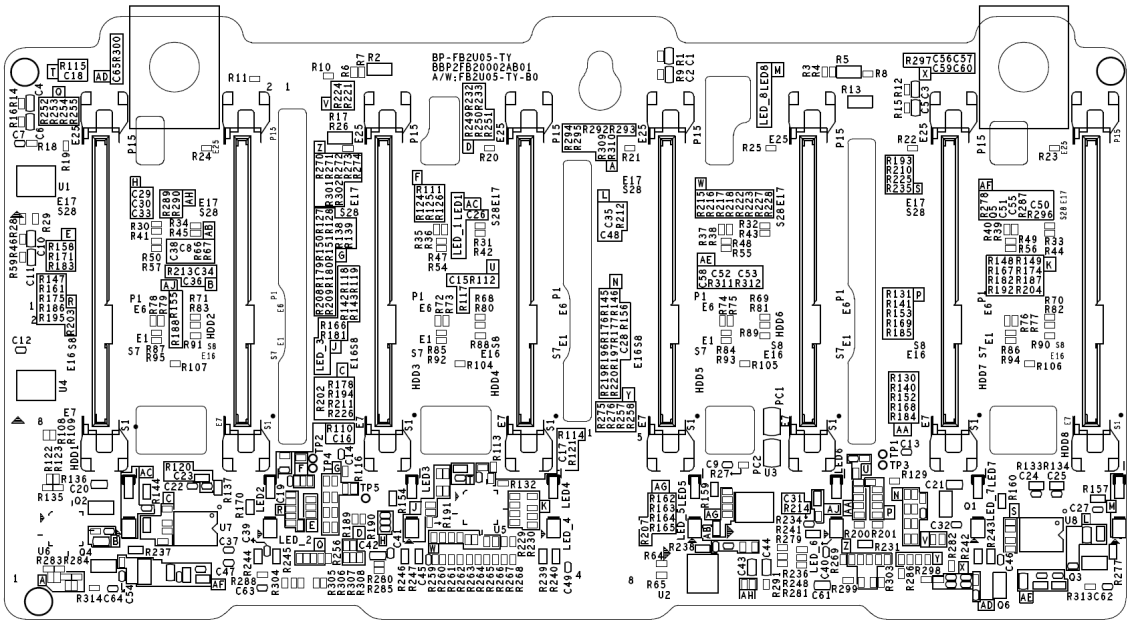
Item	Color	Behavior
BMC HEART BEAT LED	Green (Blinking)	BMC activity detected 1. 80Hz : Secure boot failed.(LED 50% on) 2. 20Hz : Boot passed with ABR(Show aout 3s and then exit) 3. 4Hz : ARM CA7 is reading flash or SRAM 4. 1Hz : ARM CA7 is reading peripherals 5. 0.5Hz : ARM CA7 is reading DRAM 6. 0.2Hz : No ARM CA7 read access cycles 7. 0.1Hz : No ARM CA7 read access cycles over 6~8s. Stay in mode 8 if there is no ARM CA7 reading access. Exit to mode 4-6 if there is any ARM CA7 reading access
	Green	BMC is not active
JNGFF1 ACTIVITY LED	Blue (Blinking)	JNGFF1 activity detected
	Off	JNGFF1 is not active
JNGFF2 ACTIVITY LED	Blue (Blinking)	JNGFF2 activity detected
	Off	JNGFF2 is not active
PHY1 1G LED	Yellow	1G link detected
PHY1 100M LED	Green	100M link detected1
PHY1 ACT LED	Green (Blinking)	Activity detected


PHY1 1G LED
PHY1 ACT LED
PHY1 100M LED
CPLD DEBUG LED[0:7]
BMC HEART BEAT LED
JNGFF1 ACTIVITY LED
JNGFF2 ACTIVITY LED
CPU0
CPU1

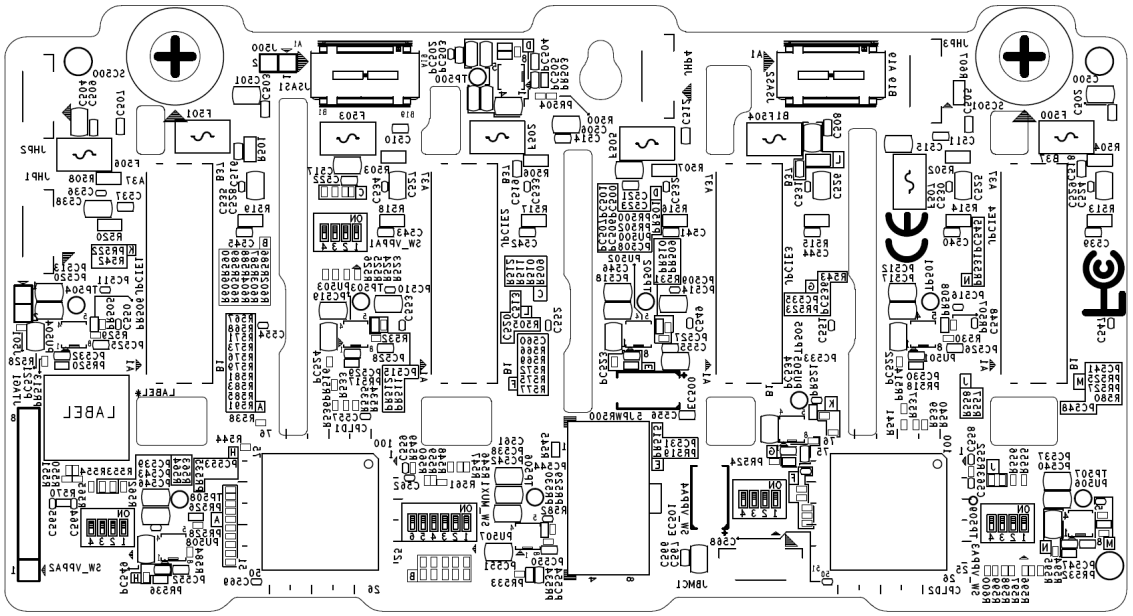
3.8 Drive Backplane: 8 Bay

3.8.1 Placement

Top view

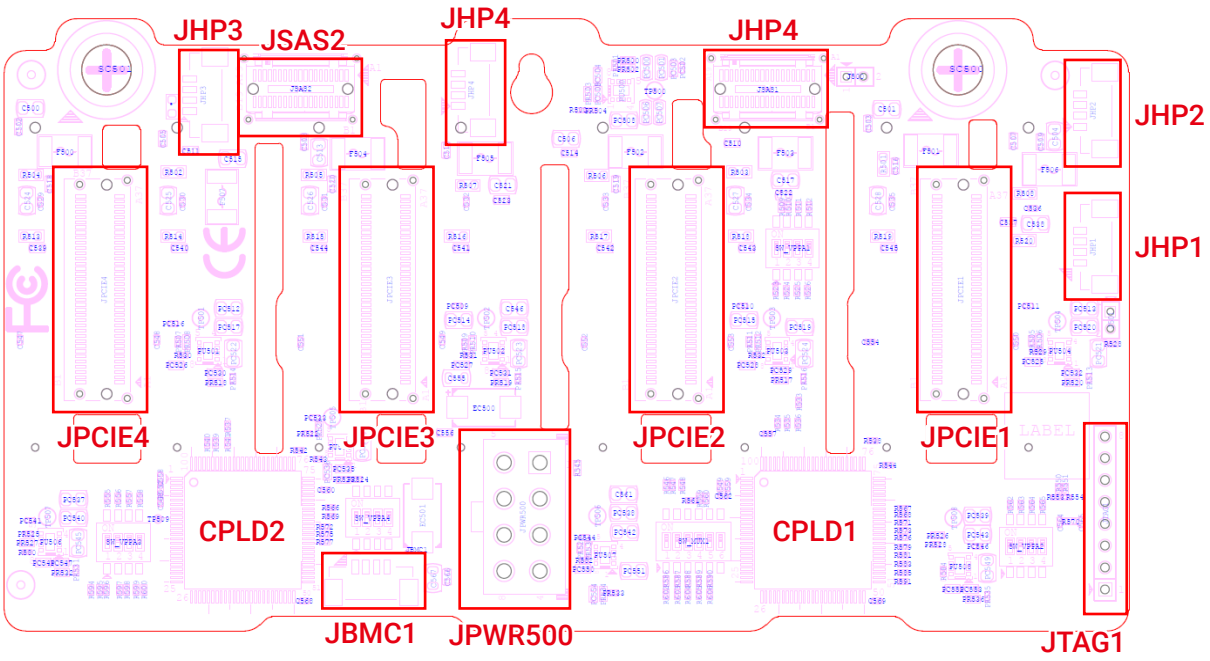


Bottom view



3.8.2 Connector

Bottom view



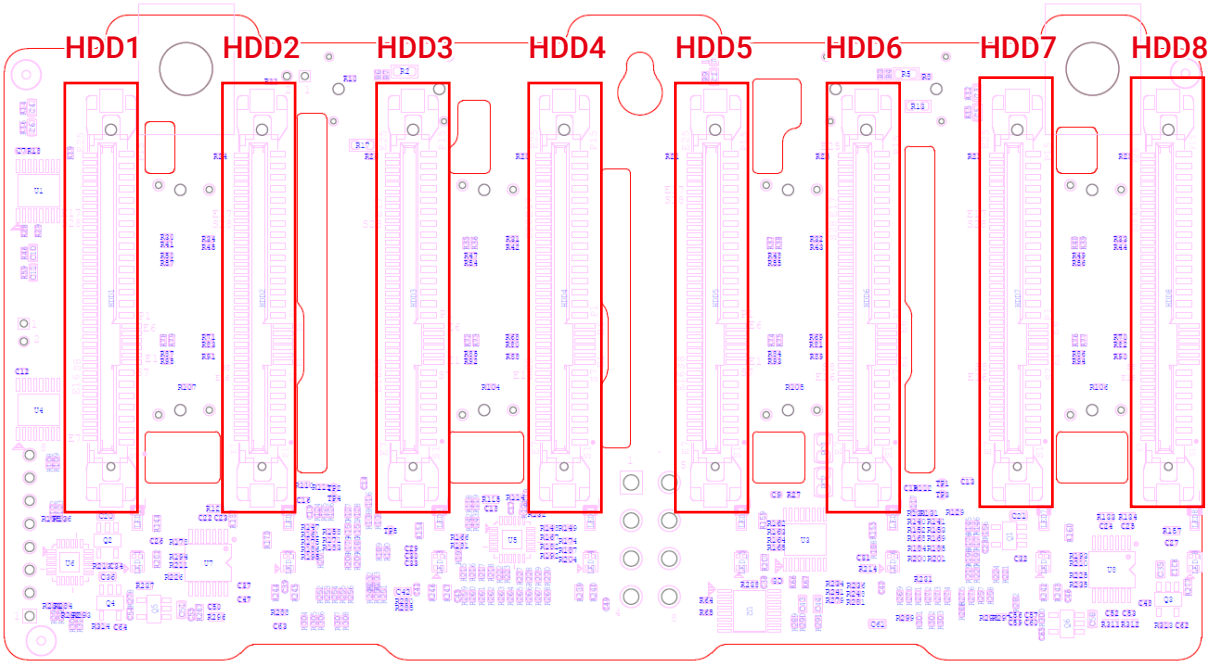
External Connectors

Connector	Description	Function
HDD1~HDD8	68P VERTICAL	HDD Connection(Gen5)

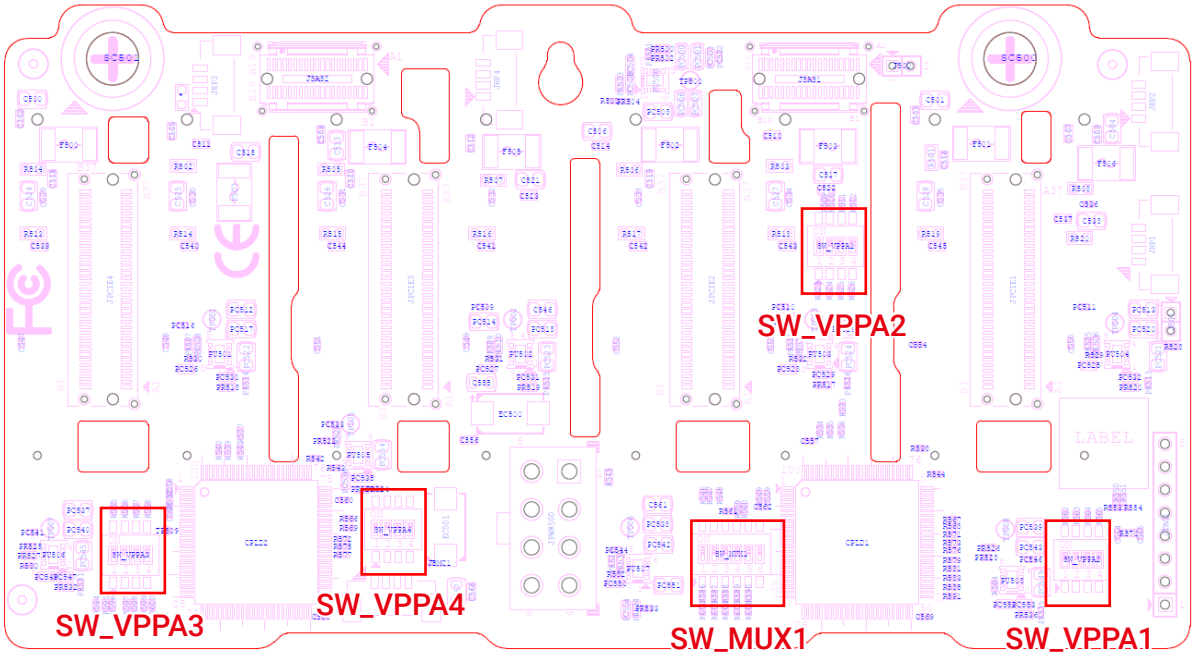
Internal Connectors

Connector	Description	Function
MCIO(JPCIE1~4)	74Pin VERTICAL	PCIE GEN5 Connection
Slimline 4i (JSAS1~2)	36Pin VERTICAL	SAS4 Connection
Power Connector(JPWR500)	2X4Pin	3V3/5V/12V
SMBus(JBMC1)	1X4Pin	BMC bus
SMBus(JHP1~4)	1X4Pin	VPP bus

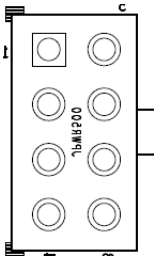
Top view



Switch Location

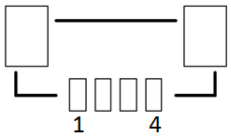


Power Connector (JPWR 500)



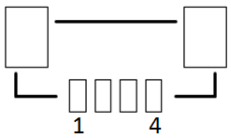
1	GND
2	GND
3	GND
4	GND
5	+12V
6	+12V
7	+12V
8	+12V

SMBUS Connector (JBMC1)



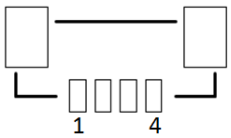
SMB_BP_BMC_SDA	1	2	GND
SMB_BP_BMC_SCL	3	4	SMB_BP_BMC_ALERT_N

SMBUS Connector (JHP1)



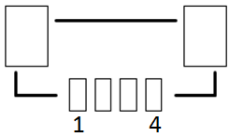
SMB_BP_SHP1_SDA	1	2	GND
SMB_BP_SHP1_SCL	3	4	BP_SHPINT_OUT1_N

SMBUS Connector (JHP2)



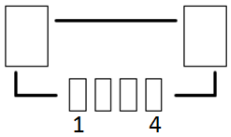
SMB_BP_SHP2_SDA	1	2	GND
SMB_BP_SHP2_SCL	3	4	BP_SHPINT_OUT2_N

SMBUS Connector (JHP3)



SMB_BP_SHP3_SDA	1	2	GND
SMB_BP_SHP3_SCL	3	4	BP_SHPINT_OUT3_N

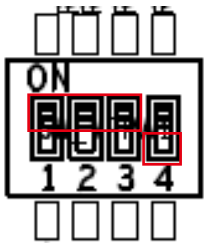
SMBUS Connector (JHP4)



SMB_BP_SHP4_SDA	1	2	GND
SMB_BP_SHP4_SCL	3	4	BP_SHPINT_OUT4_N

3.8.3 Switch Setting

SW_VPPA1: 0100 A2 A1 A0 X

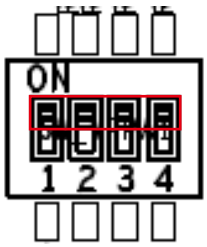


1	Addr_A0
2	Addr_A1
3	Addr_A2
4	SMB_SHP_BMC_SEL1

SW_VPPA1 pin1	Addr_A0	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_VPPA1 pin2	Addr_A1	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_VPPA1 pin3	Addr_A2	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0x40	0x42	0x44	0x46	0x48	0x4A	0x4C	0x4E
		Default							

		SHP(Default)	BMC	External
SW_VPPA1 pin4	SMB_SHP_BMC_SEL1	OFF=H	ON=L	
SW_VPPA2 pin4	SMB_SHP_BMC_EN1	ON =L	ON=L	OFF=H

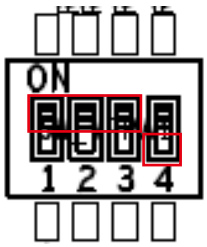
SW_VPPA2: 0100 A5 A4 A3 X



1	Addr_A3
2	Addr_A4
3	Addr_A5
4	SMB_SHP_BMC_EN1

SW_VPPA2 pin1	Addr_A3	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_VPPA2 pin2	Addr_A4	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_VPPA2 pin3	Addr_A5	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0x40	0x42	0x44	0x46	0x48	0x4A	0x4C	0x4E
		Default							

SW_VPPA3: 0100 B2 B1 B0 X

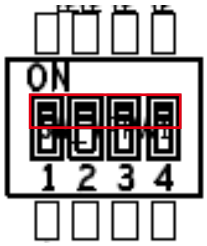


1	Addr_B0
2	Addr_B1
3	Addr_B2
4	SMB_SHP_BMC_SEL2

SW_VPPA3 pin1	Addr_A0	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_VPPA3 pin2	Addr_A1	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_VPPA3 pin3	Addr_A2	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0x40	0x42	0x44	0x46	0x48	0x4A	0x4C	0x4E
		Default							

		SHP(Default)	BMC	External
SW_VPPA3 pin4	SMB_SHP_BMC_SEL2	OFF=H	ON=L	
SW_VPPA4 pin4	SMB_SHP_BMC_EN2	ON =L	ON=L	OFF=H

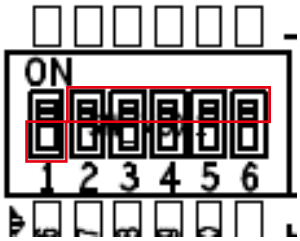
SW_VPPA4: 0100 B5 B4 B3 X



1	Addr_B3
2	Addr_B4
3	Addr_B5
4	SMB_SHP_BMC_EN2

SW_VPPA4 pin1	Addr_B3	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_VPPA4 pin2	Addr_B4	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_VPPA4 pin3	Addr_B5	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0x40	0x42	0x44	0x46	0x48	0x4A	0x4C	0x4E
		Default							

SW_MUX1: U5 1110 A2 A1 A0 X
U6 1110 B2 B1 B0 X



1	I2CMUX_A0
2	I2CMUX_A1
3	I2CMUX_A2
4	I2CMUX_B0
5	I2CMUX_B1
6	I2CMUX_B2

SSD1~8 I2C setting

SW_MUX1 pin1	I2CMUX_A0	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_MUX1 pin2	I2CMUX_A1	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_MUX1 pin3	I2CMUX_A2	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0xE0	0xE2	0xE4	0xE6	0xE8	0xEA	0xEC	0xEE
		Default							

CPLD1&CPLD2 Program/Registor setting

SW_MUX1 pin4	I2CMUX_B0	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H	ON=L	OFF=H
SW_MUX1 pin5	I2CMUX_B1	ON=L	ON=L	OFF=H	OFF=H	ON=L	ON=L	OFF=H	OFF=H
SW_MUX1 pin6	I2CMUX_B2	ON=L	ON=L	ON=L	ON=L	OFF=H	OFF=H	OFF=H	OFF=H
	Address	0xE0	0xE2	0xE4	0xE6	0xE8	0xEA	0xEC	0xEE
		Default							

3.8.4 LED Definition

HDD Activity LED Control Register					
Offset	**R/W**	**Bits**	**Default**	**Register Function**	**Description**
0x80	RW	[7]	1'b1	Reserved	Reserved
		[6]	1'b1	Reserved	Reserved
		[5]	1'b1	Reserved	Reserved
		[4]	1'b1	Reserved	Reserved
		[3]	1'b1	ACTIVITY_LED4_N	HDD4 Activity LED#
		[2]	1'b1	ACTIVITY_LED3_N	HDD3 Activity LED#
		[1]	1'b1	ACTIVITY_LED2_N	HDD2 Activity LED#
		[0]	1'b1	ACTIVITY_LED1_N	HDD1 Activity LED#

HDD Fault LED Control Register					
Offset	**R/W**	**Bits**	**Default**	**Register Function**	**Description**
0x81	RW	[7]	1'b1	Reserved	Reserved
		[6]	1'b1	Reserved	Reserved
		[5]	1'b1	Reserved	Reserved
		[4]	1'b1	Reserved	Reserved
		[3]	1'b1	FAULT_LED4_N	HDD4 Fault LED#
		[2]	1'b1	FAULT_LED3_N	HDD3 Fault LED#
		[1]	1'b1	FAULT_LED2_N	HDD2 Fault LED#
		[0]	1'b1	FAULT_LED1_N	HDD1 Fault LED#

HDD Locate LED Control Register					
Offset	**R/W**	**Bits**	**Default**	**Register Function**	**Description**
0x82	RW	[7]	1'b1	Reserved	Reserved
		[6]	1'b1	Reserved	Reserved
		[5]	1'b1	Reserved	Reserved
		[4]	1'b1	Reserved	Reserved
		[3]	1'b1	LOCATE_LED4_N	HDD4 Locate LED#
		[2]	1'b1	LOCATE_LED3_N	HDD3 Locate LED#
		[1]	1'b1	LOCATE_LED2_N	HDD2 Locate LED#
		[0]	1'b1	LOCATE_LED1_N	HDD1 Locate LED#

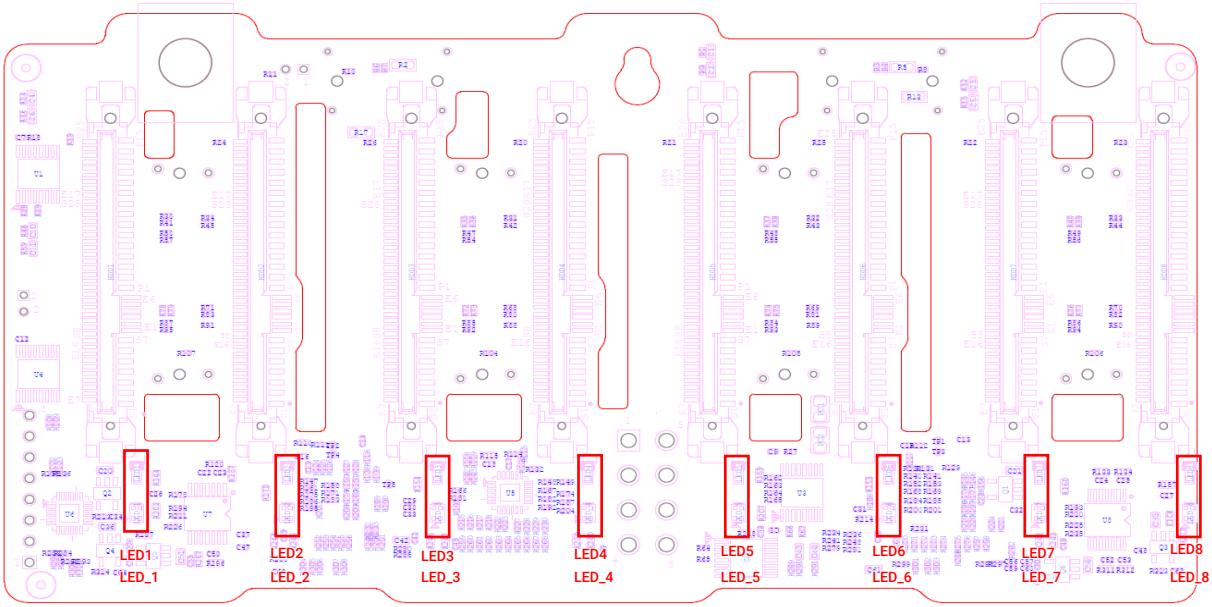
HDD Detection	
HDDINx_N=1'b0 & SDD_IFDET_N=1'b0	SAS, SATA
HDDINx_N=1'b1 & SDD_IFDET_N=1'b0	PCIe

3.8.5 LED Definition

Activity LED	
SAS, SATA (**0x4A[0] = 1'b0**, From HDD P11)	
SAS, SATA (**0x4A[0] = 1'b1**, From SGPIO)	
No Activity	LED ON
Activity	LED 4Hz blinking
PCIe (From HDD P11)	
No Activity	LED ON
Activity	LED 4Hz blinking

Locate LED & Fail LED	
PCIe (From VPP)	
Locate = 1'b0 & Fail = =1'b1 (Fail)	LED ON (Fail LED)
Locate = 1'b1 & Fail = =1'b0 (Locate)	LED 4Hz blinking (Loc LED)
Locate = 1'b1 & Fail = =1'b1 (Rebuild)	LED 1Hz blinking (Fail LED)
PCIe (From HDD P11)	
Locate = 1'b0 & Fail = =1'b1 (Fail)	LED ON (Fail LED)
Locate = 1'b1 & Fail = =1'b0 (Locate)	LED 4Hz blinking (Fail LED)
Locate = 1'b1 & Fail = =1'b1 (Rebuild)	LED 1Hz blinking (Fail LED)

LED Location



Chapter 4. BIOS Configuration Settings

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

To enter BIOS configuration settings,

- Press **Esc** key during the Power-On-Self-Test (POST)

To enter BIOS after POST, you have to restart the system by using one of the three methods:

- Press **Ctrl** + **Alt** + **Delete.**
- Press the reset button on the system chassis.
- Turn the system off and on.

NOTE

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

4.1 Navigation Keys

The navigation keys are listed below.

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

4.2 BIOS Menu

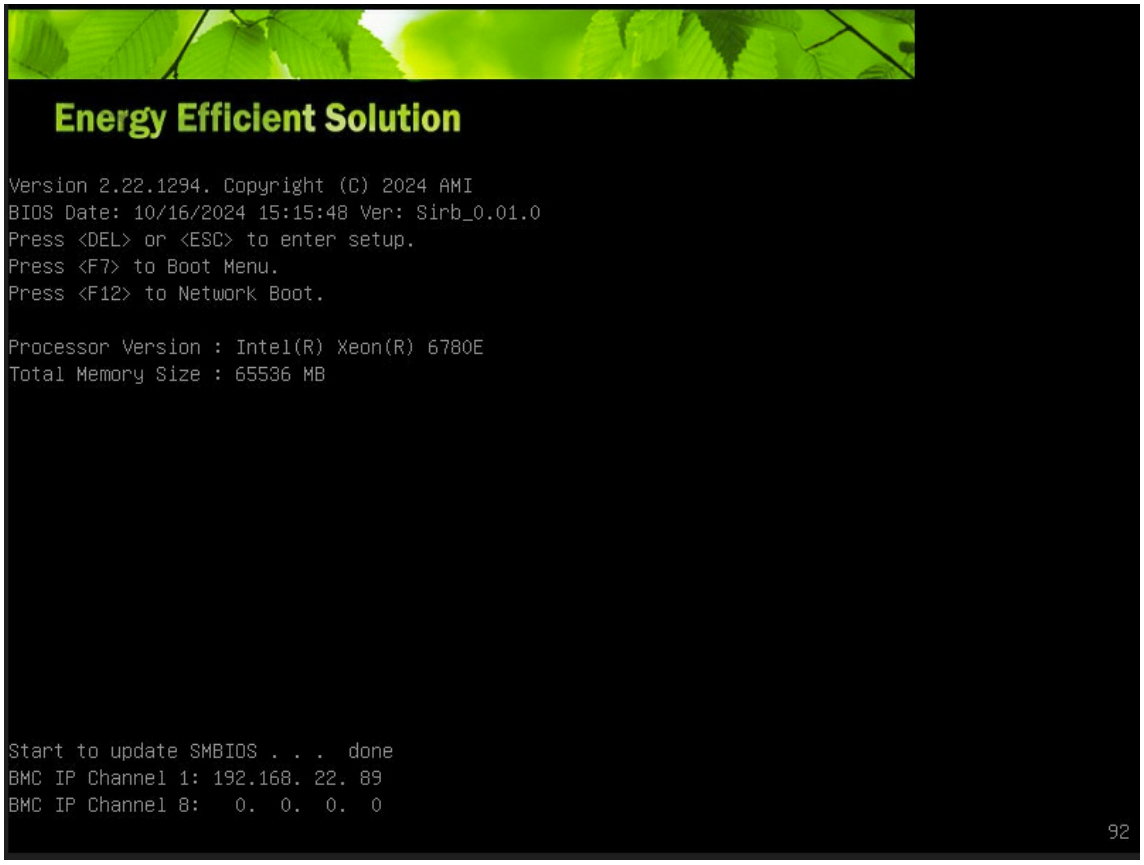
4.2.1 Menu

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

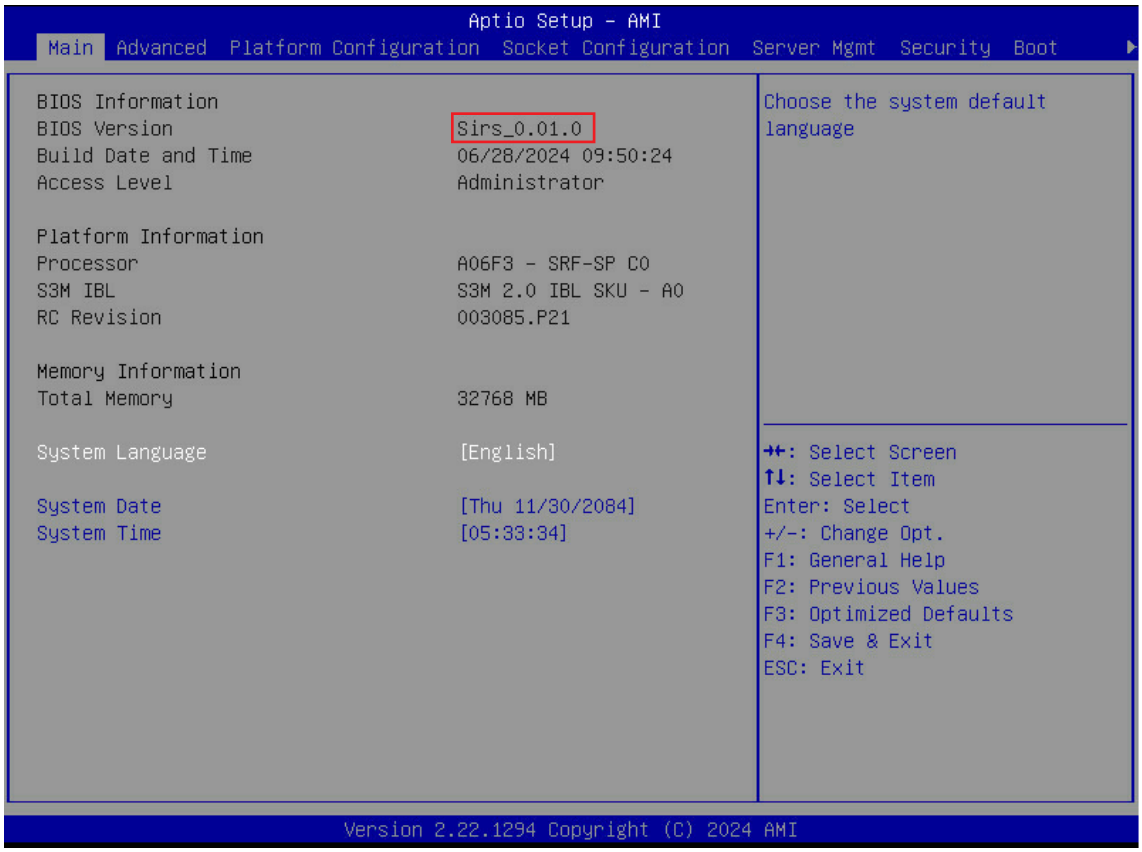
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Platform Configuration	Allows configuration of platform settings such as PCH, miscellaneous, and server ME configuration.
Socket Configuration	Allows configuration of socket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

4.2.2 Startup

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



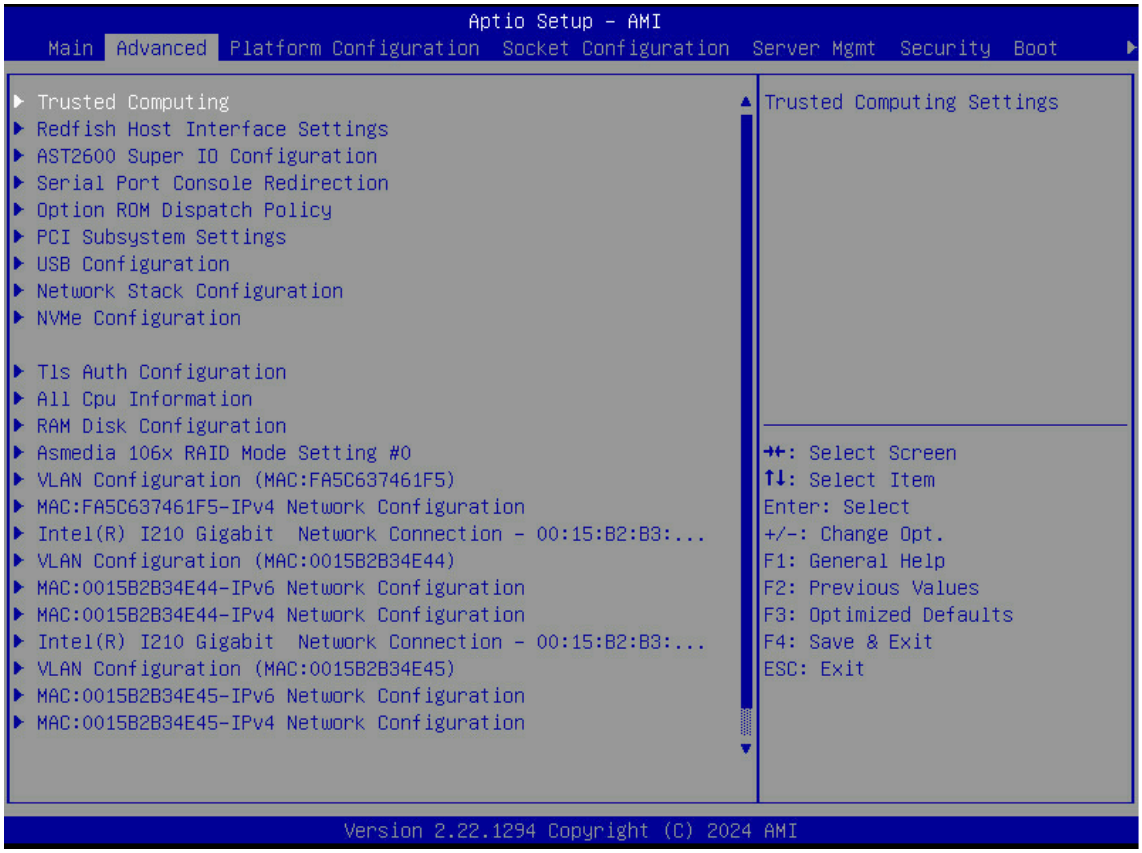
4.3 Main



4.3.1 Main

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

4.4 Advanced



4.4.1 Trusted Computing

Trusted Computing Settings.

Trusted Computing			
Security Device Support	Enables or disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.		
	▶Enable	Disable	
SHA256 PCR Bank	Enable or Disable SHA256 PCR Bank		
	▶Enable	Disable	
SHA384 PCR Bank	Enable or Disable SHA384 PCR Bank		
	Enable	▶Disable	
Pending operation	Schedule an Operation for the Security Device. **NOTE** Your Computer will reboot during restart in order to change State of Security Device.		
	▶None	TPM Clear	
Platform Hierarchy	Enable or Disable Platform Hierarchy		
	▶Enable	Disable	
Storage Hierarchy	Enable or Disable Storage Hierarchy		
	▶Enable	Disable	
Endorsement Hierarchy	Enable or Disable Endorsement Hierarchy		
	▶Enable	Disable	
Physical Presence Spec Version	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.		
	1.2	▶1.3	
Device Select	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated		
	TPM 1.2	TPM 2.0	▶Auto

4.4.2 Redfish Host Interface Settings

Redfish Host Interface Parameters.

Redfish Host Interface Settings			
Redfish	Enable/Disable AMI Redfish.		
	▶Enable	Disable	
Authentication mode	Select authentication mode.		
	Authentication None	▶Basic Authentication	Session Authentication

4.4.3 AST2600 Super IO Configuration

System Super IO Chip Parameters.

AST2600 Super IO Configuration				
Serial Port 1 Configuration	Set Parameters of Serial Port 1 (COMA)			
	Serial Port	Enables/disables Serial Port (COM)		
		▶Enable	Disable	
	Change Settings	Select an optimal settings for Super IO Device.		
		▶Auto	IO=3F8h; IRQ=4;	IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
		IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=2E8h IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
Serial Port 2 Configuration	Set Parameters of Serial Port 2 (COMB)			
	Serial Port	Enables/disables Serial Port (COM)		
		▶Enable	Disable	
	Change Settings	Select an optimal settings for Super IO Device.		
		▶Auto	IO=2F8h; IRQ=3;	IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
		IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;	IO=2E8h IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;
Serial Port 3 Configuration	Set Parameters of Serial Port 3 (COMC)			
	Serial Port	Enables/disables Serial Port (COM)		
		Enable	▶Disable	
Serial Port 4 Configuration	Set Parameters of Serial Port4 (COMD)			
	Serial Port	Enables/disables Serial Port (COM)		
		Enable	▶Disable	

4.4.4 Serial Port Console Redirection

Serial Port Console Redirection.

Serial Port Console Redirection					
Console Redirection (COM0/1)	Enables/disables console redirection.				
	Enable	▶Disable			
Console Redirection EMS	Console Redirection Enable or Disable.				
	Enable	▶Disable			
Console Redirection Settings	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.				
	Out-of-Band Mgmt Port	Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.			
		▶COM0	COM1		
	Terminal Type EMS	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation.			
		VT100	VT100Plus	▶VT-UTFB	ANSI
	Bits per second EMS	Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may repuire lower speeds.			
		9600	19200	57600	▶115200
		230400	460800	921600	

Console Redirection Settings	Flow Control EMS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.		
		▶None	Hardware RTS/CTS	Software Xon/Xoff

4.4.5 Option ROM Dispatch Policy

Option ROM Dispatch Policy.

Option ROM Dispatch Policy		
Restore if Failure	If system fails to boot and this option is set to 'Enabled', software will reset settings of this page as well as CSM page to its default values automatically.	
	▶Enable	Disable
Primary Video Ignore	If software will detect that due to the Policy settings, Option ROM of Primary Video Device will not dispatch, it will ignore this device policy settings, and restore it to 'Enable' automatically.	
	▶Enable	Disable
On Board Network Controller	Onboard Device has: UEFI [X] Legacy [ ] Embedded ROM(s). VIDx8086:DIDx1533 @ s0|Bx60|Dx0|Fx0	
	▶Enable	Disable
On Board Network Controller	Onboard Device has: UEFI [X] Legacy [ ] Embedded ROM(s). VIDx8086:DIDx1533 @ s0|Bx60|Dx0|Fx0	
	▶Enable	Disable
On Board Display Controller	Onboard Device has: UEFI [X] Legacy [ ] Embedded ROM(s). VIDx1A03:DIDx2000 @ s0|Bx3A|Dx0|Fx0	
	▶Enable	Disable
Slot #1-8 Empty	Enable or Disable Option ROM execution for selected Slot.	
	▶Enable	Disable

4.4.6 PCI Subsystem Settings

PCI, PCI-X and PCI Express Settings.

PCI Subsystem Settings		
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

4.4.7 USB Configuration

USB Configuration Parameters

USB Configuration					
Legacy USB Support	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE optional will keep USB devices available only for EFI applications.				
	▶Enable	Disable	Auto		
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.				
	▶Enable	Disable			
USB Mass Storage Driver Support	Enable/Disable USB Mass Storage Driver Support.				
	▶Enable	Disable			
USB 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' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.				
	▶Auto	Manual			
AMI Virtual CDROMO 1.00	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drivers are emulated as 'CDROM', drives with no media will be emulated according to a 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. Opticall drivers are emulated as 'CDROM', drives with no media will be emulated according to a drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM

4.4.8 Network Stack Configuration

Network Stack Settings.

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

4.4.9 NVMe Configuration
NVMe Device Options Settings.

4.4.10 T1s Auth Configuration
Press <Enter> to select T1s Auth Configuration.

T1s Auth Configuration				
Server CA Configuration	Press <Enter> to configures server CA.			
	Enroll Cert	Press <Enter> to enroll cert.		
		Enroll Cert Using File	Enroll Cert Using File	
		Cert GUID	Input digit character in 11111111-2222-3333-4444-1234567890ab format.	
		Commit Changes and Exit	Commit Changes and Exit.	
		Discard Changes and Extit	Discard Changes and Exit.	
	Delete Cert	Press <Enter> to delete cert.		
		FE9C6606-8B49-44A3-8B6B-DEA3A0E032	GUID for CERT	
			Enable	▶Disable

4.4.11 All Cpu Informaiton
Display all cpu information.

4.4.12 RAM Disk Configuration
Press <Enter> to Adds/Removes RAM disks.

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

4.4.13 Asmedia 106x RAID Mode Setting #0
Asmedia 106x RAID Mode Setting HII

4.4.14 VLAN Configuration (MAC:D29C29CAB89)

VLAN Configuration (MAC:D29C29CAB89)

VLAN Configuration (MAC:D29C29CAB89)		
Enter Configuration Menu	Press ENTER to enter configuration menu for VLAN configuration.	
	VLAN ID	VLAN ID of new VLAN or existing VLAN, valid value is 0~4094.
		0
	Priority	802.1Q Priority, valid value is 0~7.
		0
	Add VLAN	Create a new VLAN or update existing VLAN.
	Remove VLAN	Remove selected VLANs.

4.4.15 MAC:D29C29CAB89-IPv4 Network Configuration

Configure network parameters (MAC:D29C29CAB89)

MAC:D29C29CAB89-IPv4 Network Configuration		
Configured	Indicate whether network address configured successfully or not.	
	Enabled	▶Disabled
Save Changes and Exit	Save Changes and exit.	

4.4.16 Intel(R) I210 Gigabit Network Connection - (Mac address)

Configure Gigabit Ethernet device parameters

Intel(R) I210 Gigabit Network Connection - 00:15:B2:B3:...				
NIC Configuration	Click to configure the network device port.			
	Link Speed	Specifies the port speed used for the selected boot protocol.		
		▶Auto Negotiated	10 Mbps Half	10 Mbps Full
		100 Mbps Half	100 Mbps Full	
	Wake On Lan	Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior ofo Wake on LAN in OS controlled power states.		
		▶Enabled	Disabled	
Blink LEDs	Blink LEDs for a duration up to 15 seconds.			
	0			

4.4.17 VLAN Configuration (MAC:0015B2B34E44)

VLAN Configuration (MAC:0015B2B34E44)

VLAN Configuration (MAC:0015B2B34E44)		
Enter Configuration Menu	Press ENTER to enter configuration menu for VLAN configuration.	
	VLAN ID	VLAN ID of new VLAN or existing VLAN, valid value is 0~4094.
		0
	Priority	802.1Q Priority, valid value is 0~7.
		0
	Add VLAN	Create a new VLAN or update existing VLAN.
	Remove VLAN	Remove selected VLANs.

4.4.18 MAC:0015B2B34E44-IPv6 Network Configuration

Configure IPv6 network parameters (MAC:0015B2B34E44)

MAC:0015B2B34E44-IPv6 Network Configuration			
Enter Configuration Menu	Press ENTER to enter configuration menu for IPv6 configuration.		
	Interface ID	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3	
		2:15:B2:FF:FE:B3:4E:44	
	DAD Transmit Count	The number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.	
		1	
	Policy	automatic or manual	
		►automatic	manual
	Save Changes and Exit	Save changes for interface ID, DAD transmit count, policy, and data in advanced configuration.	

4.4.19 MAC:0015B2B34E44-IPv4 Network Configuration

Configure network parameters (MAC:0015B2B34E44)

MAC:0015B2B34E44-IPv4 Network Configuration		
Configured	Indicate whether network address configured successfully or not.	
	Enabled	►Disabled
Save Changes and Exit	Save Changes and exit.	

4.4.20 Intel(R) I210 Gigabit Network Connection - (Mac address)

Configure Gigabit Ethernet device parameters

Intel(R) I210 Gigabit Network Connection - 00:15:B2:B3:...				
NIC Configuration	Click to configure the network device port.			
	Link Speed	Specifies the port speed used for the selected boot protocol.		
		►Auto Negotiated	10 Mbps Half	10 Mbps Full
		100 Mbps Half	100 Mbps Full	
	Wake On Lan	Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior ofo Wake on LAN in OS controlled power states.		
		►Enabled	Disabled	
Blink LEDs	Blink LEDs for a duration up to 15 seconds.			
	0			

4.4.21 VLAN Configuration (MAC:0015B2B34E45)

VLAN Configuration (MAC:0015B2B34E45)

VLAN Configuration (MAC:0015B2B34E45)		
Enter Configuration Menu	Press ENTER to enter configuration menu for VLAN configuration.	
	VLAN ID	VLAN ID of new VLAN or existing VLAN, valid value is 0~4094.
		0
	Priority	802.1Q Priority, valid value is 0~7.
		0
	Add VLAN	Create a new VLAN or update existing VLAN.
	Remove VLAN	Remove selected VLANs.

4.4.22 MAC:0015B2B34E45-IPv6 Network Configuration

Configure IPv6 network parameters (MAC:0015B2B34E45)

MAC:0015B2B34E45-IPv6 Network Configuration			
Enter Configuration Menu	Press ENTER to enter configuration menu for IPv6 configuration.		
	Interface ID	The 64 bit alternative interface ID for the device. The string is colon separated. e.g. ff:dd:88:66:cc:1:2:3	
		2:15:B2:FF:FE:B3:4E:45	
	DAD Transmit Count	The number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection on a tentative address. A value of zero indicates that Duplicate Address Detection is not performed.	
		1	
	Policy	automatic or manual	
		▶automatic	manual
	Save Changes and Exit	Save changes for interface ID, DAD transmit count, policy, and data in advanced configuration.	

4.4.23 MAC:0015B2B34E45-IPv4 Network Configuration

Configure network parameters (MAC:0015B2B34E45)

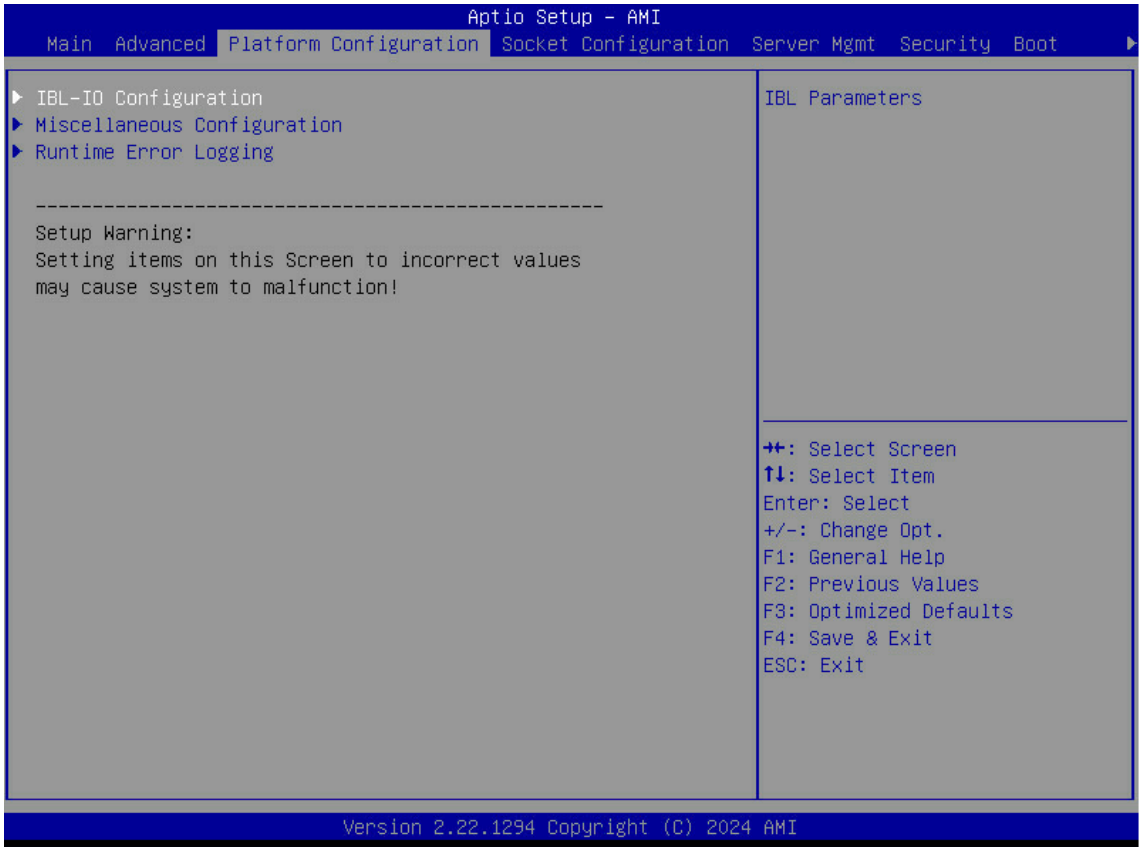
MAC:0015B2B34E45-IPv4 Network Configuration		
Configured	Indicate whether network address configured successfully or not.	
	Enabled	▶Disabled
Save Changes and Exit	Save Changes and exit.	

4.4.24 Driver Health

Provides Health Status for the Drivers/Controllers

Driver Health		
Intel(R) RRO/1000 9.8.40 PCI-E	Provides Health Status for the Drivers/Controllers	
	Healthy	
Intel(R) RRO/1000 8.7.10 PCI-E	Controller 5E1BBC98 Child 0	Provides Health Status for the Drivers/Controllers.
		Healthy
	Intel(R) I210 Gigabit Network Connection	Provides Health Status for the Drivers/Controllers.
		Healthy
Intel(R) RRO/1000 8.7.10 PCI-E	Controller 5E1BBC98 Child 0	Provides Health Status for the Drivers/Controllers.
		Healthy
	Intel(R) I210 Gigabit Network Connection	Provides Health Status for the Drivers/Controllers.
		Healthy

4.5 Platform Configuration



4.5.1 IBL-IO Configuration

IBL Parameters.

IBL-IO Configuration								
Enable/Disable ADR	Enable or disable Automatic DIMM Refresh (ADR)							
	▶Platform-POR	Enabled	Disabled					
Enable/Disable ADR Timer	Enable or disable ADR Timer.							
	▶Platform-POR	Enabled	Disabled					
Host Partition Reset ADR Enable	Enables/Disables ADR on Host Partition Reset							
	▶Platform-POR	Enabled	Disabled					
ADR timer 1 expire time	Type desired ADR timer expire time, valid value - <1, 255>. Entered time is scaled by ADR timer time unit.							
	1							
ADR timer 1 unit	Select ADR timer time unit.							
	1us	10us	100us	1ms	10ms	100ms	▶1s	10s
ADR timer 2 expire time	Type desired ADR timer expire time, valid value - <1, 255>. Entered time is scaled by ADR timer time unit.							
	1							
ADR timer 2 unit	1us	10us	100us	1ms	10ms	100ms	▶1s	10s

4.5.2 Miscellaneous Configuration

Miscellaneous Configuration				
ISCLK Configuration	ISCLK Setup Knob			
	SSC1 Enable	Enables SSC for SSC PLL1		
		▶Disable	Enable	
	SSC2 Enable	Enables SSC for SSC PLL2		
		▶Diable	Enable	
Wake On Lan Support	Enable or Disable Wake On Lan Support.			
	▶Enabled	Disabled		
Active Video	Select active Video type			
	▶Auto	Onboard Device	PICE Device	
Wake On Lan from S5	Enables or Disables Wake on Lan from S5			
	Enabled	▶Disabled		
Boot to Network	Enables or Disables Boot to Network.			
	Enabled	▶Disabled		
ARI Support	Enable or disable the ARI support.			
	▶Enabled	Disabled		
RTC Wake system from S4/S5	Enable: Enable Wake on RTC feature. Disable: Disable Wake on RTC feature. Enabled and set wake time: Enable System wake on alarm event and set wake on the day::hr::min::sec specified.			
	▶Disable	Enable	Enable and set wake on time	
Firmware Configuration	Firmware Configuration options.			
	Ignore Policy Update	Production	Test	
	Internal	▶Restricted	Restricted SV	
Clock SSC Support	Enable or disable the Clock Spread Spectrum support.			
	▶SSC Off	SSC= -0.3%	SSC= -0.5%	Hardware

4.5.3 Runtime Error Logging

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

Runtime Error Logging				
System Errors	System Error Enable/Disable setup options.			
	▶Enable	Disable		
S/W Error Injection Support	When Enabled S/W Error Injection is supported by unlocking MSR 0x790			
	▶Disable	Enable		
RAS Log Level	RAS Log setup options.			
	None	▶MIN (BASIC_FLOW)	MID (BASIC_FLOW, FUNC_FLOW)	MAX (BASIC_FLOW, FUNC_FLOW, REG)
Cloak Devhide registers from being accessible from OS	Enable/Disable OS to access Devhide registers.			
	Enable	▶Disable		
Corrected Error Cloaking	When enabled, Corrected errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled.			
	Enable	▶Disable		
UCNA Cloaking	When enabled, UCNA errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled.			
	Enable	▶Disable		
FatalErrDebugHalt	DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjuction with ITP as thread will halt in Fatal error flow			
	Enable	▶Disable		
Mca Bank Warm Boot Clear Errors	Enable/Disable Mca Bank Warm Boot Clear Errors.			
	▶Enable	Disable		
Clear Shadow Registers	Enable/Disable clearing shadow registers.			
	▶Enable	Disable		
OOB RAS Support	Enable/Disable OOB RAS feature.			
	Enable	▶Disable		

RSA Performance Support	Enable/Disable RAS Performance Support.		
	▶Enable	Disable	
eMCA Settings	Press <Enter> to view or change the eMCA configuration.		
	EMCA Error Support	Enable/Disable EMCA Error support.	
		▶Enable	Disable
	LMCE Support	Enable/Disable Local MCE firmware support.	
		▶Enable	Disable
	EMCA Logging Support	Enable/Disable EMCA Logging.	
		▶Enable	Disable
	Ignore OS ELOG Opt-in	Enable/Disable Ignore OS ELOG Opt-in and log.	
		Enable	▶Disable
	Multi Error Section Support	Enable/Disable multi error section support.	
		Enable	▶Disable
	EMCA CMCI-SMI Morphing	Enable/Disable EMCA CSMI.	
		Disable	▶EMCA gen 2 CSMI
	EMCA CMCI-SMI Threshold	Set the threshold of correctable error for signaling CMCI-CSMI	
		0	
	CSMI Dynamic Disable	[Enable] - BIOS disables CSMI when error threshold reached. [Disabled] - CSMI always on.	
		Enable	▶Disable
	EMCA MCE-SMI Enable	Enable/Disable EMCA Uncorrected SMI for gen2.	
		Disable	▶EMCA gen 2 - MSMI
	Corrected Error eLog	Enable/Disable Corrected Error eLog.	
		▶Enable	Disable
	Memory Error eLog	Enable/Disable Memory Error eLog.	
		▶Enable	Disable
	Processor Error eLog	Enable/Disable Processor Errror eLog.	
		▶Enable	Disable
	Ubox Error Mask	Mask SMI generation for Ubox Error.	
		Enable	▶Disable
Whea Settings	Press <Enter> to view or change the WHEA configuration.		
	WHEA Support	Enable/Disable WHEA support.	
		▶Enable	Disable
	Whea Log Memory Error	Enable/Disable Whea Log Memory Error.	
		▶Enable	Disable
	Whea Log Processor Error	Enable/Disable Whea Log Processor Error.	
		▶Enable	Disable
	Whea Log PCI Error	Enable/Disable Whea Log PCI Error.	
		▶Enable	Disable
Memory Error Enabling	Press <Enter> to view or change the Memory errors enabling options.		
	Memory Corrected Error	Enable/Disable Memory Corrected Error.	
		▶Enable	Disable
	Spare Interrupt	Spare Interrupt Selection. For Error Pin setting, please enable IIO Error Pin0 Enable.	
		Disable	▶SMI	CMCI
	Pfd	Pfd is to identify hard error out from errors. Auto indicates PFD is enabled dynamically based on system configuration.	
		Disable	Enable	▶Auto

4.5.4 IIO Error Enabling

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

IIO Error Enabling				
IIO/IBL Global Error Support	Enable/Disable IIO/IBL Error Support.			
	▶Enable	Disable		
Os Native AER Support	Select FFM or OS native for AER error handling. If select OS native, BIOS also initialize FFM first until handshake, which depends on OS capability.			
	Enable	▶Disable		
IIO MCA Support	Enable/Disable IIO MCA Support.			
	▶Enable	Disable		
IIO Non-Fatal Error to IOMCA	Enable/Disable IIO severity 1 error to MCA.			
	▶Non-Fatal to FATAL	Non-Fatal to SRAR	Non-Fatal to UCNA	Disable
IIO Error Pin0 Enable	Enable/Disable IIO Error Pin0.			
	Enable	▶Disable		
IIO OOB Mode	Enable/Disable System Event Generation when Error Pin is enabled.			
	▶Enable	Disable		
IIO Error Registers Clear	Enable/Disable Clear IIO Error Registers.			
	▶Enable	Disable		
IIO eDPC Support	Enable/Disable IIO eDPC Support.			
	▶Disable	On Fatal Error	On Fatal and Non-Fatal Errors	
IIO Coherent Interface Error	Enable/Disable IIO Coherent Interface Error.			
	▶Enable	Disable		
IIO Misc. Error	Enable or disable IIO Misc. Error.			
	▶Enable	Disable		
IIO Vtd Error	Enable or disable IIO Vtd Error.			
	▶Enable	Disable		
IIO Dma Error	Enable or disable IIO Dma Error.			
	▶Enable	Disable		
IIO Dmi Error	Enable or disable IIO Dmi Error.			
	▶Enable	Disable		
PCIE Error	Enable or disable PCIE Error.			
	▶Enable	Disable		
ITC/OTC CA/MA Errors	Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.			
	Enable	▶Disable		

4.5.5 CXL Error Enabling

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

PCIe Error Enabling			
CXL Memory Event FW Notification(MEFN) Support	Enable/Disable CXL Memory Event FW Notification(MEFN) Support.		
	Disable MEFN Support	▶Enable FFM MEFN Support	Enable OSFM MEFN Support
CXL MEFN with Primary Mailbox	Enable/Disable CXL MEFN with Primary Mailbox Only.		
	Enable	▶Disable	

4.5.6 PCIe Error Enabling

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

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

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

4.5.7 Error Control Setting

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

Error Control Setting		
Latch First Corrected Error in KTI	Enable or disable latch first corrected error in KTI.	
	Enable	▶Disable

4.5.8 Crash Log Enabling

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

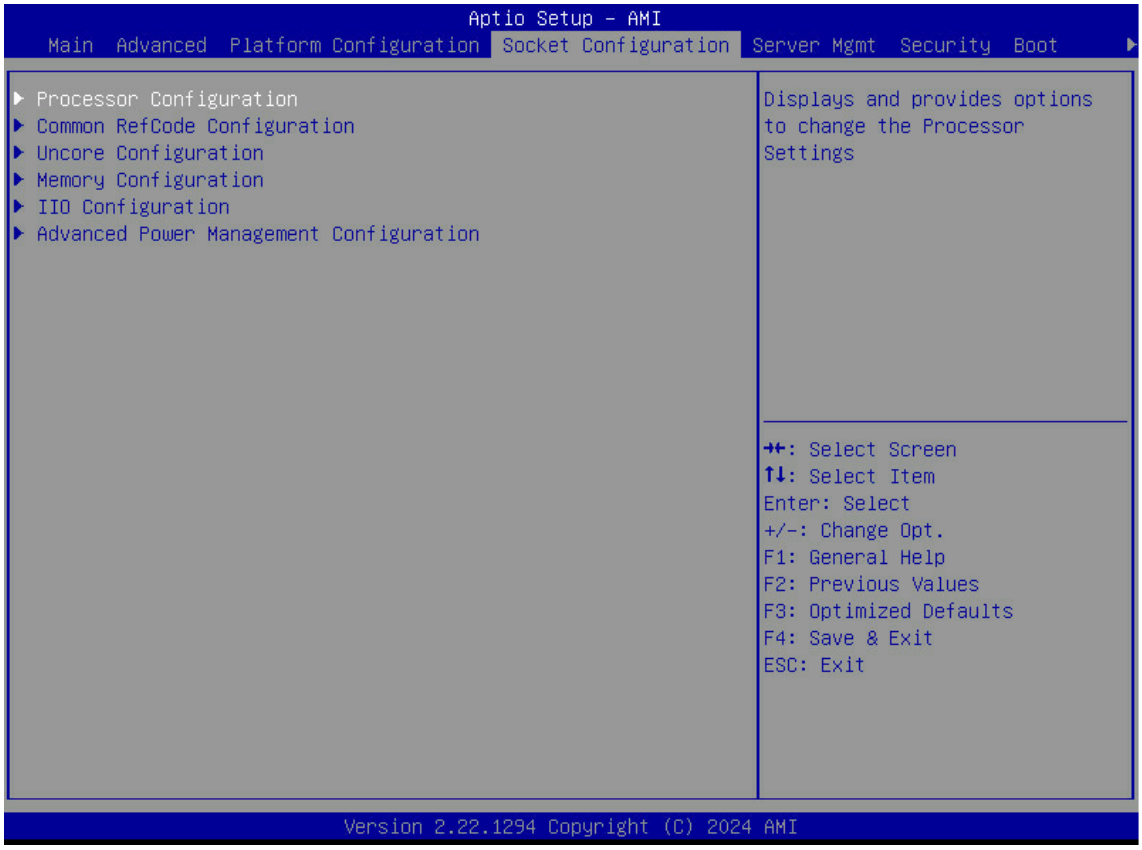
Error Control Setting			
CPU CrashLog Feature	The feature helps collecting crash data from OOBMSM SSRAM.		
	▶Auto	Enable	Disable
Core CrashLog Disable	The feature helps to disable CPU Core crash log.		
	▶no	yes	
TOR CrashLog Disable	The feature helps to disable CPU TOR crash log.		
	▶no	yes	
Uncore CrashLog Disable	The feature helps to disable CPU Uncore crash log.		
	▶no	yes	
MCERR Trigger CrashLog Disable	The feature helps to disable MCERR to trigger crash log.		
	no	▶yes	
CPU Clear CrashLog	Option to clear CPU CrashLog after collection.		
	▶Enable	Disable	
CPU Crashlog ReArm	Option to ReArm CPU CrashLog after collection.		
	▶Enable	Disable	

4.5.9 AWR Configuration

Asynchronous Warm Reset Configuration.

AWR Configuration		
Ierr Global Reset	Enables = when Ierr present in last boot, do Global reset.	
	▶Enable	Disable
Stall For BMC	When enabled, system will enter spin loop during asynchronous warm reset allowing manual error collection.	
	Enable	▶Disable
BMC RootPort	RootPort that BMC is connected to.	
	▶6	12

4.6 Socket Configuration



4.6.1 Processor Configuration

Displays and provides option to change the Processor Settings.

Processor Configuration			
Per-Socket Configuration	Change Per-Socket Settings.		
	CPU Socket 0 Configuration	Module Disable Bitmap(Hex) For every bit: set to Disable or clear to Enable	
		NOTE Any user module disable will force Static SST-PP. And any input to disable all 0-127 cores(Bitmap 0xFFFFFFFF) on the first Die of SBSP will be ignored.	
		Disable Bitmap: 0	
Hardware Prefetcher	MLC Streamer Prefetcher (MSR 1A4h Bit[0]).		
	►Enable	Disable	
Adjacent Cache Prefetch	MLC Spatial Prefetcher (MSR 1A4h Bit[1]).		
	►Enable	Disable	
DCU Streamer Prefetcher	DCU Streamer Prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[2]). Auto will skip the register programming and keep the hardware default setting.		
	Enable	Disable	►Auto
DCU IP Prefetcher	DCU IP Prefetcher is an L1 data cache prefetcher (MSR 1A4h Bit[3]).		
	►Enable	Disable	

Enable Intel(R) TXT	Enable Intel(R) TXT.			
	Enable	▶Disable		
VMX	Enables the Vanderpool Technology, takes effect after reboot.			
	▶Enable	Disable		
Enable SMX	Enables Safer Mode Extensions.			
	Enable	▶Disable		
Lock Chipset	Lock or Unlock chipset.			
	▶Enable	Disable		
MSR Lock Control	Enable - MSR 3Ah will be locked. Power Good reset is needed to remove lock bits.			
	▶Enable	Disable		
PPIN Control	Unlock and Enable/Disable PPIN Control.			
	Lock/Disable	▶Unlock/Enable		
AES-NI	Enable/Disable AES-NI support.			
	▶Enable	Disable		
Core Crash Data GPRs	Enabling this may expose personal or confidential information that may be held in the GPRs at the time of the Crash trigger.			
	▶Disabled	Gprs Enabled, Smm Gprs Enabled	Gprs Enabled, Smm Gprs Disabled	
HWLS Control	Hardware Lockstep control. Enable specific core-pairs for HWLS.			
	Disabled	C0/C1 HWLS	C2/C3 HWLS	C0/C1 HWLS & C2/C3 (all) HWLS
Processor trace	Enable/Disable processor trace feature from CPU MSR. Enabling this feature will immediately start trace collection.			
	Enable	▶Disable		

4.6.2 Common RefCode Configuration

Displays and provide option to change the Common RefCode Settings.

Common RefCode Configuration		
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 Uncore Configuration

Displays and provides option to change the Uncore Settings.

Uncore Configuration						
Uncore General Configuration	Display and provides option to change the Uncore General Settings.					
	Uncore Status	Uncore Status Help				
	Degrade Precedence	Choose Topology Precedence to degrade features if system options are in conflict or choose Feature Precedence to degrade topology if system options are in conflict.				
		▶Topology Precedence	Feature Precedence			
	Link Frequency Select	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility.				
		16.0GT/s	20.0GT/s			
		24.0GT/s	▶Auto	Use Per Link Setting		
	Link L0p Enable	Enable - Set the c_l0_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.				
		▶Auto	Enable	Disable		
	Link L1 Enable	Enable - Set the c_l1_en, Disable - Reset it, Auto - Auto decides based on Si Compatibility.				
		▶Auto	Enable	Disable		
	Directory Mode Enable	Directory Mode Enable, Auto - Auto decides based on Si Compatibility.				
		▶Auto	Enable	Disable		
	XPT Remote Prefetch	XPT Remote Prefetch				
		▶Auto	Enable	Disable		
	KTI Prefetch	KTI Prefetch, Auto - Auto decides based on Si Compatibility.				
		▶Auto	Enable	Disable		
	RdCur for XPT Prefetch	Enable - Set the suppress_mem_rd_prefetch_rdcur, Disable - Reset it, Auto - Auto decides based on Si Compatibility.				
		▶Auto	Enable	Disable		
	CPU SKU Type Mismatch check	Yes or No to do CPU SKU Type Mismatch check.				
		▶Yes	No			
	Loctorem Thresholds Normal	TOR Thresholds - Loctorem Thresholds Empty Settings, Auto - Auto decides based on Si Compatibility.				
		Disable	▶Auto			
		Low	Medium	High		
	Loctorem Thresholds Normal	TOR Thresholds - Loctorem Thresholds Normal Settings, Auto - Auto decides based on Si Compatibility.				
		Disable	▶Auto			
		Low	Medium	High		
	IO Directory Cache (IODC)	IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores), Auto - Auto sets to WCiLF				
		Disable	▶Auto	Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow	Enable for Remote InvItoM Hybrid AllocNon-Alloc	Enable for Remote InvItoM and Remote WViLF
	Legacy VGA Socket	Socket that claims the legacy VGA range; valid values are 0-3; 0 is default.				
		0				
	Demand Prioritization	Auto: Defaults to Disable. Disable: Default values are loaded. Enable: Will enable Demand Prioritization for performance improvement.				
		▶Auto	Enable	Disable		
	Distress QoS	Distress QoS tuning recipes.				
		▶Mode 0 - Disable the Distress QoS Feature	Mode 2 - M2M Qos Enable;CHA Qos Enable			
	On Demand In-band Provisioning Lock	Enable/ Disable On Demand In-band Provisioning Lock.				
		▶Yes	No			

Uncore General Configuration	S3m Telemetry update period	S3m Telemetry update period in minutes. <65535> represent Disable.					
		1440					
	Splitlock	Enable - Enable the split lock. Disable - Disable the split lock. Auto - Auto decides based on Si Compatibility.					
		Auto	Enable	▶Disable			
	XPT Prefetch	XPT Prefetch, Auto - Auto decides based on Si Compatibility.					
		▶Auto	Enable	Disable			
	Legacy VGA Stack	Iio Device Instance that claims the legacy VGA range; valid values are 0-11.					
		1					
	PCIe Remote P2P Relaxed Ordering	Relax P2P write ordering in hardware if software enforces ordering, or doesn't care. Default is DISABLE, so hardware will enforce P2P write ordering.					
		Enable	▶Disable				
	Uncore Debug Print Level	Uncore Debug message Print level setting. Fatal - Fatal message. Warning - Warning message. Summary - Simple message. Detail - Verbose. All - All message aboves.					
		Fatal	Warning	Summary	Detail	▶All	
	Stale AtoS	Stale A to S Dir optimization, Auto - Auto decides based on Si Compatibility.					
		▶Auto	Enable	Disable			
	LLC dead line alloc	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC, Auto - Auto decides based on Si Compatibility.					
		Auto	▶Enable	Disable			
	Opportunistic-LLC-to-SF Migration	Control opportunistic-LLC-to-SF migration feature enable or disable, Auto - Auto decides based on Si Compatibility.					
		Auto	Enable	▶Disable			
	MBA BW Calibration Profiles	Choice of MBA BW throttling curve, Auto - Auto decides based on Si Compatibility.					
		Liner BW shaping	Biased BW shaping	Legacy BW shaping	▶Auto		
	PMM MBA BW downscale	PMM BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling PMM BW throttling in a 2:1 ratio vs. DDR throttling.					
		▶1x	1/2x	1/4x	1/8x		
	CXL (Type3) MBA BW downscale	CXL (Type3) BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling CXL (Type3) BW throttling in a 2:1 ratio vs. DDR throttling.					
		▶1x	1/2x	1/4x	1/8x		
	Remote Target MBA BW downscale	Remote Target BW downscaling vs the baseline Total memory BW profile. Eg: picking 1/2x results in scaling Remote Target BW throttling in a 2:1 ratio vs. DDR throttling.					
		▶1x	1/2x	1/4x	1/8x		
	MMCFG Base	Select MMCFG Base, Auto - Auto decides based on Si Compatibility.					
		▶Auto	1G	1.5G	1.75G	2G	2.25G	3G

Uncore General Configuration	MMCFG Size	Select MMCFG Size, Auto - Auto decides based on Si Compatibility.						
		64M	128M	256M	512M	1G	2G	▶Auto
	MMIO High Base	Select MMIO High Base.						
		248T	120T	88T	60T	30T		
		56T	40T	32T	24T	16T		
		4T	2T	1T	512G	▶Auto		
	MMIO High Granularity Size	Selects the allocation size used to assign mmioh resources. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.						
		1G	4G	16G	32G	64G	256G	1024G	▶Auto
	MCTP Bus Owner Selection	Select the MCTP Bus Owner.						
		▶CPU as Bus Owner	CPU as Bus Owner Proxy					
	Clock Modulation Enabled	Clock Modulation Enabled, Auto - Auto decides based on Si Compatibility.						
		▶Auto	Enable	Disable				
	Enable MMIO Downstream	PECI MMIO Downstream Access Configuration.						
		▶Disable all PECI Agents	Enable all PECI Agents	Use per-PECI Agent enable bit	Auto			
	PECI Trust Mode	PECI Trust Mode Configuration.						
		All PECI Agents untrusted	All PECI Agents trusted	▶Use per-PECI agent trust mode	Auto			
	Legacy Agent	Legacy PECI agent in trust bit enable.						
		Disable	▶Enable	Auto				
	SMBus Agent	SMBus PECI agent in trust bit enable.						
		▶Disable	Enable	Auto				
	Generic Agent	Generic PECI agent in trust bit enable.						
		▶Disable	Enable	Auto				
	eSPI Agent	EPSI PECI agent in trust bit enable.						
		▶Disable	Enable	Auto				
	MCTP EID Start	Controls the start value used for the MCTP EID.						
		8						
	MCTP EID Range	Controls the range value used for the MCTP EID.						
		0						
	Reduce LLC Age-Bit Default	LLC shared line protection by reducing default Age bit setting. May be helpful for some workloads.						
		Disable	Enable	▶Auto				

Uncore Per Socket Configuration	CPU0	CPU 0 Configuration Silk Screen Equivalent -> CPU1					
		CPU 0 UPI Port 0-3	CPU 0 UPI Port 0-3 Configuration.				
			Link Disable	Disable a single UPI port. No: Not disable; Yes: Disable			
				►No	Yes		
			Current UPI Link Speed	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility			
				16.0GT/s	20.0GT/s	24.0GT/s	►Auto
		Bus Resources Allocation Ratio	Bus resources allocation ratio, range 0 to 8.				
			1				
		HIOP STACK DISABLE	Enables/Disables given HIOP STACK. Default is AUTO no stack is disabled. 1 - The stacks indicated by the bit locations are disabled. 0 - The stacks indicated by the bit locations are not modified. The stack order is abstracted so each bit 0 = stack 0 ... bit n = stack n. For PE numbering convention bits are incrementally mapped from bit0 to instances HC(0->n), {TIP(0->n), ETH(0->n)}*, then PE(0->n) and PE(a->x). The bit setting for each stack expect ETH, can be overridden by BIOS based on CPU-knob compatibility. TIP and ETH only if available in system .				
			0				
	CPU1	CPU 1 Configuration Silk Screen Equivalent -> CPU2					
		CPU 0 UPI Port 0-3	CPU 1 UPI Port 0-3 Configuration.				
			Link Diable	Disable a single UPI port. No: Not disable; Yes: Disable			
				►No	Yes		
			Current UPI Link Speed	Allows for selecting the UPI Link Frequency, Auto - Auto decides based on Si Compatibility			
				16.0GT/s	20.0GT/s	24.0GT/s	►Auto
		Bus Resources Allocation Ratio	Bus resources allocation ratio, range 0 to 8.				
			1				
		HIOP STACK DISABLE	Enables/Disables given HIOP STACK. Default is AUTO no stack is disabled. 1 - The stacks indicated by the bit locations are disabled. 0 - The stacks indicated by the bit locations are not modified. The stack order is abstracted so each bit 0 = stack 0 ... bit n = stack n. For PE numbering convention bits are incrementally mapped from bit0 to instances HC(0->n), {TIP(0->n), ETH(0->n)}*, then PE(0->n) and PE(a->x). The bit setting for each stack expect ETH, can be overridden by BIOS based on CPU-knob compatibility. TIP and ETH only if available in system .				
			0				

4.6.4 Memory Configuration

Displays and provides option to change Memory Settings.

Memory Configuration						
DDR PPR Type	Selects DDR Post Package Repair Type- Hard/ Soft/ Disabled.					
	▶PPR Disabled	Hard PPR	Soft PPR			
DDR MBIST	Enable/Disable DDR mPPR (Memory Built-In Self-Test)					
	Enabled	▶Disabled				
DDR mPPR	Enable/Disable DDR MBIST (Memory Built-In Self-Test Post Package Repair)					
	Enabled	▶Disabled				
DDR MBIST On Ranks In Parallel	It provides flexibility in case that the vendor Idd values could dictate DDR MBIST execution concurrency. 1 - 1 rank at a time. 2 - 2 ranks at a time. 3 - 3 ranks at a time.					
	1	2	▶3			
PTRR Victim Refresh Mode	Select between +1/-1 or +1/-1/+2 and -2 victim refresh mode.					
	▶+1/-1	+1/-1/+2/-2				
Host Memory Frequency	Maximum Host DDR Memory Frequency Selections in MT/s. If the "AUTO" option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support).					
	Note For MCR, DDR DRAM frequency is half of Host frequency.					
	▶Auto	4800	5200	5600	6000	6400
DDR Over Clock Enable	Determines if enable DDR Over Clock.					
	Enabled	▶Disabled				
Allow Memory Test Correctable Error	Enable - Logs error and allows correctable errors during memory test(DIMM Rank not removed). Disable - Logs error and removes DIMM Rank.					
	▶Enabled	Disabled				
Global Scrambling	Enable - Enables global data scrambling. Disable - Disables global data scrambling					
	▶Enabled	Disabled				
Scrambling Seed Low	Low 32 bits of the scrambling seed.					
	41003					
Scrambling Seed High	High 32 bits of the scrambling seed.					
	54165					
UEFI Memory Map Special Purpose Me	Allow or disallow the SP Memory Flag to be set in the UEFI Memory Map and in the ACPI SRAT table.					
	▶Enabled	Disabled				
ACPI SRAT Special Purpose Memory Flag	Allow or disallow the ACPI SRAT SP Memory Flag to be set when UEFI Memory Map Special Purpose Flag is enabled.					
	▶Enabled	Disabled				
Memory Topology	Displays memory topology with Dimm population information.					
Memory RAS Configuration	Displays and provides option to change the Memory RAS Settings.					
	Dynamic ECC Mode Selection	Enable/Disable Dynamic ECC Mode Selection				
		Enabled	▶Disabled			
	Mirror Mode	Full Mirror Mode will set entire 1LM memory in system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable XPT Prefetch.					
		▶Disabled	Full Mirror Mode			
	Memory Correctable Error Flood Policy	[Disabled] Don't deal with Memory CE flood. [Once] Only First Memory CE will trigger SMI, and BIOS will disable silicon SMI. [Frequency] Disable SMI when Memory CE reach threshold within time limits.				
		Disable	Once	▶Frequency		

Memory RAS Configuration	Correctable Error Threshold	Correctable Error Threshold (0x01 - 0x7fff) used for sparing, and leaky bucket		
		7FFF		
	Trigger SW Error Threshold	Enable or Disable Sparing trigger SW Error Match Threshold.		
		►Enable	Disabled	
	SW Per Bank Threshold	SW Per Bank Correctable Error Threshold (1-0x7FFF) used for bank level error.		
		3		
	SW Per Row Threshold	SW Per Row Correctable Error Threshold (1-0x7FFF) used for row level error.		
		2		
	SW Correctable Error Time Window	Sw Correctable Error time window based interface in Hour (0-24).		
		24		
	Leaky bucket time window based interface	Enable/Disable leaky bucket time window based interface.		
		Enable	►Disabled	
	Leaky bucket low bit	Leaky bucket low bit" (0x1-0x29)		
		28		
	Leaky bucket high bit	Leaky bucket high bit" (0x1-0x29)		
		29		
	ADDDC Sparing	Enable/Disable ADDDC Sparing (ADDDC will be diabled if Mirroring is enabled.		
		Enable	►Disabled	
	Patrol Scrub Interval	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto!		
		24		
	DDR5 ECS	Disable: Disable ECS/Result collection. Enable: Enable ECS without Result Collection. Enable ECS with Result Collection: Enable ECS/Result Collection.		
		Disabled	►Enabled	Enable ECS with Result Collection

4.6.5 IIO Configuration

Displays and provides option to change IIO Settings.

IIO Configuration									
Socket0 Configuration	PCI Express 0	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.						
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.					
				Enable	▶Disable				
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.						
			▶Auto	x4x4x4x4	x4x4_x8				
			x_x8x4x4	x_x8x_x8	x_x_x_x16				
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4				
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4				
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4				
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2				
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2				
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2				
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2				
		Port A	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.					
				Enable	▶Disable				
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.					
				Enable	▶Disable				
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.					
				Yes	▶No				
			Override Max Link Width	Override the max link width that was set by bifurcation.					
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.					
				Enable	▶Disable				
			Requested Link Speed	Choose Link Speed for this PCIe port.					
				▶Auto	Gen 1 (2.5 GT/s)				
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)				
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)				
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.					
				▶-6.0 dB	-3.5 dB				
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.					
				Distinct	Common	▶Auto			
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.					
				▶Enable	Disable				
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.					
				128B	256B	512B	▶Auto		
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.					
				▶Auto	Disable				

Socket0 Configuration	PCI Express 0	Port A	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
				▶KTI Option	Auto		
				Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow		
				Enable for Remote InvItoM Hybrid AllocFlow	Enable for Remote InvItoM and Remote WViLF		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 0	Port E/G	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.						
				Enable	▶Disable					
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.						
				Enable	▶Disable					
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.						
				Yes	▶No					
			Override Max Link Width	Override the max link width that was set by bifurcation.						
				▶Auto	x1	x2	x4	x8	x16	
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.						
				Enable	▶Disable					
			Requested Link Speed	Choose Link Speed for this PCIe port.						
				▶Auto	Gen 1 (2.5 GT/s)					
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)					
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)					
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.						
				▶-6.0 dB	-3.5 dB					
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.						
				Distinct	Common	▶Auto				
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.						
				▶Enable	Disable					
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.						
				128B	256B	512B	▶Auto			
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.						
				▶Auto	Disable					
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.						
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS			
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS			
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.						
				▶Enable	Disable					

Socket0 Configuration	PCI Express 0	Port E/G	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.
				Disable / ▶Auto / Force Enable
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
				Enable / ▶Disable
			MCTP	Enable/Disable MCTP
				▶Enable / Disable
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.
				▶Enable / Disable
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.
				Enable / ▶Disable

Socket0 Configuration	PCI Express 1	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.					
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.				
				Enable	▶Disable			
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.					
			▶Auto	x4x4x4x4	x4x4_x8			
			x_x8x4x4	x_x8x_x8	x_x_x_x16			
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4			
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4			
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4			
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2			
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2			
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2			
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2			
		Port E/F/H	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			

Socket0 Configuration	PCI Express 1	Port E/F/H	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 1	Port G	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			

Socket0 Configuration	PCI Express 1	Port G	Requested Link Speed	Choose Link Speed for this PCIe port.			
				▶Auto	Gen 1 (2.5 GT/s)		
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)		
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)		
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.			
				▶-6.0 dB	-3.5 dB		
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.			
				Distinct	Common	▶Auto	
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.			
				▶Enable	Disable		
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.			
				128B	256B	512B	▶Auto
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.			
				Auto	▶Disable		
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				▶Enable	Disable		

Socket0 Configuration	PCI Express 1	Port G	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 2	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.					
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.				
				Enable	▶Disable			
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.					
			▶Auto	x4x4x4x4	x4x4_x8			
			x_x8x4x4	x_x8x_x8	x_x_x_x16			
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4			
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4			
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4			
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2			
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2			
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2			
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2			
		Port A	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			

Socket0 Configuration	PCI Express 2	Port A	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
				▶KTI Option	Auto		
				Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow		
				Enable for Remote InvItoM Hybrid AllocFlow	Enable for Remote InvItoM and Remote WViLF		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				▶Enable	Disable		

Socket0 Configuration	PCI Express 2	Port B/C/D/E/F/G	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.					
				Enable	▶Disable				
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.					
				Enable	▶Disable				
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.					
				Yes	▶No				
			Override Max Link Width	Override the max link width that was set by bifurcation.					
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.					
				Enable	▶Disable				
			Requested Link Speed	Choose Link Speed for this PCIe port.					
				▶Auto	Gen 1 (2.5 GT/s)				
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)				
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)				
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.					
				▶-6.0 dB	-3.5 dB				
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.					
				Distinct	Common	▶Auto			
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.					
				▶Enable	Disable				
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.					
				128B	256B	512B	▶Auto		
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.					
				▶Auto	Disable				
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.					
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS		
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS		
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.					
				Enable	▶Disable				

Socket0 Configuration	PCI Express 0	Port B/C/D/E/F/G	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.
				Disable / ▶Auto / Force Enable
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
				Enable / ▶Disable
			MCTP	Enable/Disable MCTP
				▶Enable / Disable
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.
				▶Enable / Disable
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.
				Enable / ▶Disable

Socket0 Configuration	PCI Express 3	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.					
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.				
				Enable	▶Disable			
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.					
			▶Auto	x4x4x4x4	x4x4_x8			
			x_x8x4x4	x_x8x_x8	x_x_x_x16			
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4			
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4			
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4			
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2			
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2			
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2			
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2			
		Port A	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			

Socket0 Configuration	PCI Express 3	Port A	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
				▶KTI Option	Auto		
				Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow		
				Enable for Remote InvItoM Hybrid AllocFlow	Enable for Remote InvItoM and Remote WViLF		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 4	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.					
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.				
				Enable	▶Disable			
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.					
			▶Auto	x4x4x4x4	x4x4_x8			
			x_x8x4x4	x_x8x_x8	x_x_x_x16			
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4			
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4			
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4			
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2			
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2			
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2			
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2			
		Port A	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				▶Enable	Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			

Socket0 Configuration	PCI Express 4	Port A	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
				▶KTI Option	Auto		
				Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow		
				Enable for Remote InvItoM Hybrid AllocFlow	Enable for Remote InvItoM and Remote WViLF		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 4	Port C	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				▶Enable	Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.				
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS	
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS	
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.				
				Enable	▶Disable			

Socket0 Configuration	PCI Express 4	Port C	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.
				Disable / ▶Auto / Force Enable
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
				▶Enable / Disable
			MCTP	Enable/Disable MCTP
				▶Enable / Disable
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.
				▶Enable / Disable
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.
				Enable / ▶Disable

Socket0 Configuration	PCI Express 4	Port E/G	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				▶Enable	Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.				
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS	
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS	
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.				
				Enable	▶Disable			

Socket0 Configuration	PCI Express 4	Port E/G	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.
				Disable / ▶Auto / Force Enable
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port
				Enable / ▶Disable
			MCTP	Enable/Disable MCTP
				▶Enable / Disable
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.
				▶Enable / Disable
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.
				Enable / ▶Disable

Socket0 Configuration	PCI Express 5	Intel VMD technology	Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.					
			Intel VMD technology	Enable/ Disable VMD in this IIO Domain.				
				Enable	▶Disable			
		Bifurcation	Selects PCIe port Bifurcation for selected slot(s) Port Format: xGxExCxA The port can further be x2x2 Disable - disable all PCIe lanes and the controller.					
			▶Auto	x4x4x4x4	x4x4_x8			
			x_x8x4x4	x_x8x_x8	x_x_x_x16			
			x2x2x4x_x8	x4x2x2x_x8	x_x8x2x2x4			
			x2x2x4x4x4	x4x2x2x4x4	x4x4x2x2x4			
			x2x2x2x2x_x8	x2x2x2x2x4x4	x2x2x4x2x2x4			
			x4x2x2x2x2x4	x2x2x2x2x2x2x4	x_x8x4x2x2			
			x4x4x4x2x2	x_x8x2x2x2x2	x2x2x4x4x2x2			
			x4x2x2x4x2x2	x4x4x2x2x2x2	x2x2x2x2x4x2x2			
			x2x2x4x2x2x2x2	x4x2x2x2x2x2x2	x2x2x2x2x2x2x2x2			
		Port A	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			

Socket0 Configuration	PCI Express 5	Port A	L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.			
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.			
				Enable	▶Disable		
			PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			IODC Configuration	Enable/Disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores)			
				▶KTI Option	Auto		
				Enable for Remote InvItoM Hybrid Push	InvItoM AllocFlow		
				Enable for Remote InvItoM Hybrid AllocFlow	Enable for Remote InvItoM and Remote WViLF		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		

Socket0 Configuration	PCI Express 5	Port E	Suprise Hot Plug Capable	This option specifies if the link is considered Suprise Hot Plug capable.				
				Enable	▶Disable			
			PCIe Loopback Mode	Enable/Disable loopback support for this PCIe port.				
				Enable	▶Disable			
			Link Disable	This option disables the link so that the no training occurs but the CFG space is still active.				
				Yes	▶No			
			Override Max Link Width	Override the max link width that was set by bifurcation.				
				▶Auto	x1	x2	x4	x8	x16
			Support VC1	Enable/Disable PCIe Port VC1 support. X2 ports share the same VC1 channel.				
				Enable	▶Disable			
			Requested Link Speed	Choose Link Speed for this PCIe port.				
				▶Auto	Gen 1 (2.5 GT/s)			
				Gen 2 (5 GT/s)	Gen 3 (8 GT/s)			
				Gen 4 (16 GT/s)	Gen 5 (32 GT/s)			
			DeEmphasis	DeEmphasis control (LNKCON2[6] for this PCIe port.				
				▶-6.0 dB	-3.5 dB			
			Clocking	Configure port clocking via LNKCON[6]. This refers to this components and the down stream component. 'Auto' keeps board default.				
				Distinct	Common	▶Auto		
			Data Link Feature Exchange	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities(DLFCAP) register.				
				▶Enable	Disable			
			MPSS	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.				
				128B	256B	512B	▶Auto	
			ASPM Support	This option can disable ASPM support in PCIe root port. 'Auto' keeps hardware default.				
				▶Auto	Disable			
			L1 Exit Latency	The length of time this port requires to complete transition from L1 to L0.				
				<1uS	1uS-2uS	2uS-4uS	4uS-8uS	
				▶8uS-16uS	16uS-32uS	32uS-64uS	>64uS	
			Extended Sync	Enable/disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.				
				Enable	▶Disable			

Socket0 Configuration	PCI Express 5	Port E	PCIe 10-bit Tag Support	'Disable' option can disable PCIe 10-bit Tag Requester (not Completer) support in a PCIe Root Port. 'Auto' keeps hardware default. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Port, however OS could reconfigure and enable it. Advanced user may use 'Force Enable' option to enforce enabling 10-bit Tag in a hierarchy where Root Port is 10-bit Tag Completer capable, but not all nodes support 10-bit Tag Completer. The user assures, there will be no peer-to-peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such hierarchy 10-bit Tag Requester is not enabled in Root Port regardless of Root Port capability.			
				Disable	▶Auto	Force Enable	
			Unsupported Request	Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port			
				Enable	▶Disable		
			MCTP	Enable/Disable MCTP			
				▶Enable	Disable		
			Equalization Bypass To Highest Rate on port	Equalization Bypass To Highest Rate Support Enable/Disable.			
				▶Enable	Disable		
			Intel VMD technology	Enable/ Disable Intel Volume Management Device Technology on specific root port.			
				Enable	▶Disable		
	IOAT 0	CPM	Select CPM Enable/Disable				
			▶Enable	Disable			
		HQM	Select HQM Enable/Disable				
			▶Enable	Disable			
		North Trace Hub	Enable/Disable CPU Trace Hub.				
			NOTE DMA protection (Vtd) should be disabled.				
			Enable	▶Disable			
	IOAT 2	North Trace Hub	Enable/Disable CPU Trace Hub.				
			NOTE DMA protection (Vtd) should be disabled.				
			Enable	▶Disable			
	IOAT 3	CPM	Select CPM Enable/Disable				
			▶Enable	Disable			
		HQM	Select HQM Enable/Disable				
			▶Enable	Disable			
	RP Correctable Err		Applies to root ports only. Enable interrupt on correctable errors.				
			Enable	▶Disable			
	RP NonFatal Uncorrectable Err		Applies to root ports only. Enable interrupt on a non-fatal error.				
			Enable	▶Disable			
	RP Fatal Uncorrectable Err		Applies to root ports only. Enable interrupt on fatal errors.				
			Enable	▶Disable			
	Sierra Peak Memory Region Buffer S		Select size of memory buffer for each single Sierra Peak instance.				
			▶None	1MB	8MB	64MB	
			128MB	256MB	512MB	1GB	
			2GB	4GB	8GB		

Intel VT for Directed I/O (VT-d)	Press <Enter> to bring up the Intel Virtualization for Directed I/O (VT-d) Configuration menu.				
	DMA Control Opt-In Flag	Enable DMA_CTRL_PLATFORM_OPT_IN_FLAG in DMAR in ACPI to request OS to enable DMA protection. Not compatible with Direct Device Assignment (DDA).			
		►Enable	Disable		
	Pre-boot DMA Protection	Enable DMA Protection in Pre-boot environment.			
		►Enable	Disable		
	SATC Support	Enable/Disable SATC support.			
		►Enable	Disable		
	RHSA Support	Enable/Disable RHSA support.			
		►Enable	Disable		
	SIDP Support	Enable/Disable SIDP support.			
		►Enable	Disable		
	PCIe ACSCTL	Enable/Disable overwrite of PCI Access Control Services Control Services Control register in PCI root ports.			
		Enable	►Disable		
	Cache Allocation	Enable cache allocation. This knob is independent of VT-d support.			
		Enable	►Disable		
	PRS Capability for PCIe	Enable/Disable support for page request services capability on discrete PCIe devices. Enabling should only be to test vehicle for PCIe cards supporting PRS, and it might lead to platform hang.			
		►Auto	Enable	Disable	
Global Configuration	Stores Global Configuration Options.				
	Delay before link training	Custom delay before PCIe link training on IIO ports(in milisecond).			
		0			
	Delay after link training	Custom delay after PCIe link training on IIO ports(in milisecond).			
		0			
	Hot Plug	Enable/Disable PCIe Hot Plug globally.			
		►Enable	Disable		
	Hot Plug Polling Rate	The rate that PCIe root ports should poll for a hot plugged device. 'Auto' keeps silicon registers default.			
		Auto	►500ms	1s	
	NPEM	Enable/Disable NPEM globally.			
		Enable	►Disable		
	NoSnoop Write Config	NoSnoop Write Configuration			
		►Enable	Disable		
	Force NoSnoop Write Config	Force NoSnoop Write Configuration			
		Enable	►Disable		
	Problematic port	Selects whether problematic port lock flows need to be enabled in the system. Selection allows for P-P or NP-NP lock flows or neither.			
		►Disable	NP-NP problematic	P-P problematic	
	Allocating Write Flows	Selects Vc0/VCp writes selection for all CPU PCIe ports as either allocating or non-allocating. Auto enables POR setting			
		►Allocating	Non-Allocating		
	EN1K	Enables 1K granularity for I/O space decode in each of the virtual P2P bridges corresponding to root ports, and DMI ports			
		Enable	►Disable		
	Completion Timeout(Global)	Enable / disable the PCIe Completion Timeout in Device Control2 register.			
		Pre-Port	►Glabal		
	Global Timeout Value	Completion Timeout to program in Device Control2 register.			
		50us to 50ms	50us to 100us	1ms to 10ms	16ms to 55ms
		65ms to 210ms	►260ms to 900ms	1s to 3.5s	Disable

Global Configuration	ASPM Support (Global)	This option can disable ASPM support for all PCIe root ports.			
		►Disable	Per-Port		
	Snoop Response Hold Off for PCIe S	Sets Snoop Response Hold Off value, 256 cycles as Default			
		9			
	Snoop Response Hold Off for IOAT S	Sets Snoop Response Hold Off value, 256 cycles as Default			
		A			
	LTR Support	This option can disable Latency Tolerance Reporting support in all PCIe root ports. 'Auto' keeps hardware default.			
		►Auto	Disable		
	Extended Tag Support	This option can disable 8-bit Tag support in all PCIe root ports. 'Auto' keeps hardware default.			
		►Auto	Disable		
	10-bit Tag Support	This option can disable 10-bit Tag Requester (not Completer) support in all PCIe Root Ports. 'Auto' keeps hardware default. 10-bit Tag Completer support is required in all gen4 and newer devices per PCIe specification. When disabled system FW does not configure 10-bit Tag in hierarchy under Root Ports, however OS can reconfigure and enable it.			
		►Auto	Disable		
	Atomic Operations Support	This option can disable Atomic Operation Routing support in all PCIe root ports and block Atomic Operation Requester in PCI hierarchy. 'Auto' keeps hardware default.			
		►Auto	Disable		
	Max Read Request Size	This option can set Max Read Request Size in PCI hierarchy. 'Default' keeps hardware default.			
		AUTO	128B	256B	512B
		1024B	2048B	►4096B	
	PTM Support	This option can disable Precision Time Management support in PCI hierarchy. 'Auto' keeps hardware default.			
		►Auto	Disable		
	Relaxed Ordering	Relaxed Ordering Enable/Disable.			
		►Enable	Disable		
	ENQCMD/ENQCMDS	Enqueue requests support Enable/Disable			
		►Enable	Disable		
	Equalization Bypass To Highest Rate	Equalization Bypass To Highest Rate Support Enable/Disable			
		►Enable	Disable		
	Restore PCIe EQ coefficient	Enable/Disable PCIe EQ coefficient restoring			
		Enable	►Disable		
	AET CPU Trace Hub	Enable/Disable CPU Trace Hub for AET event tracing			
		Enable	►Disable		
	Miscellaneous Global Options				
	MultiCast	Enable MultiCast (for validation use)			
		Enable	►Disable		
	Retimer Low Latency Mode	Enable 16GT/s and 32GT/s HW autonomous re-timer low latency mode.			
		Disable	►Enable	16GT/s Only	32GT/s Only

4.6.6 Advanced Power Management Configuration

Displays and provides to change the Power Management settings.

Advanced Power Management Configuration						
CPU P State Control	P State Control Configuration Sub Menu, include Turbo, XE and etc.					
	Intel SST-PP		Intel SST-PP Select allows user to choose level. AUTO: Keep current SST-PP level; in multi sockets system, choose lowest common level when level mask mismatch between sockets.			
			▶Auto	Level 0	Level 1	
	SpeedStep (Pstates)		Enable/Disable EIST (P-States).			
			▶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 Efficiency		
	Turbo Mode		Enable/Disable processor Turbo Mode.			
			▶Enable	Disable		
	Energy Efficient Turbo		Enable/Disable Energy Efficient Turbo. Enable: MSR 0x1FC Bit[19] = 0 Disable: MSR 0x1FC Bit[19] = 1.			
			▶Enable	Disable		
	CPU Flex Ratio Override		Enable/Disable CPU Flex Ratio Programming NOTE: Dynamic SST-PP and SST-BF will be disabled when CPU Flex Ratio Override is enabled.			
			Enable	▶Disable		
	Per P-Limit	Program PERF_P_LIMIT CSR Sub Menu.				
		Perf P-Limit Differential	Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.			
			1			
		Perf P-Limit Clip	Maximum value the floor is allowed to be set to for perf P-limit.			
			1F			
		Perf P-Limit Threshold	Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.			
			F			
		Perf P Limit	Enable/Disable Performance P-Limit			
			Enable	▶Disable		
Hardware PM State Control	Hardware P-States		• Disable: Hardware chooses a P-state based on OS Request (Legacy P-States). • Native Mode: Hardware chooses a P-state based on OS guidance. • Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance). **NOTE** When HWP mode is Disable or Out of Band Mode, Dynamic SST-PP,SST-BF and SST-CP will be disabled.			
			▶Native Mode	Out of Band Mode	Native Mode with No Legacy Support	Disable
	HardwarePM Interrupt		Enable/Disable Hardware PM Interrupt			
			Enable	▶Disable		
	APS rocketing		Enable/Disable 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		

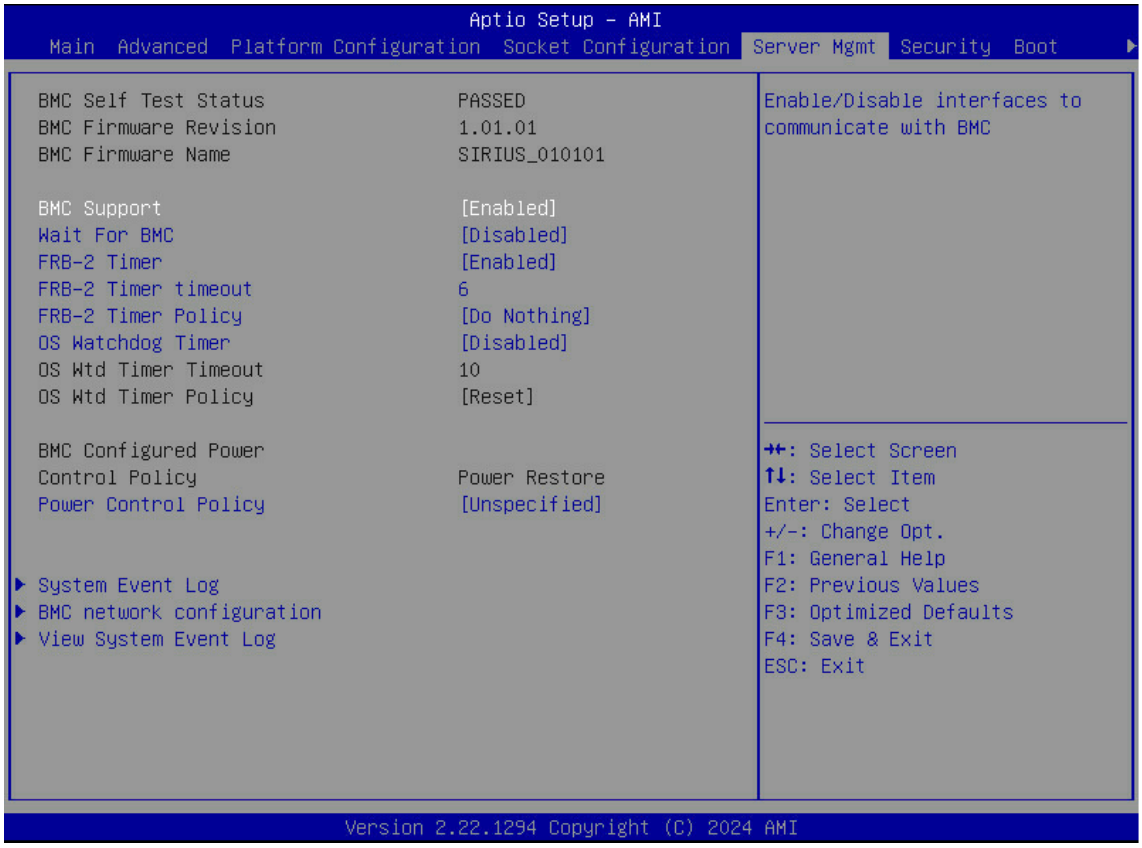
Hardware PM State Control	Native ASPM	Enabled - OS Controlled ASPM, Disabled - ASPM Off, AUTO - BIOS Controlled ASPM		
		►Auto	Enabled	Disabled
CPU C State Control	CPU C State setting.			
	Monitor MWAIT	Allows Monitor and MWAIT instructions.		
		►Enable	Disable	
	ACPI C1 Enumeration	Enumerate C1/C1e as ACPI C1.		
		C1	►C1e	
	ACPI C6x Enumeration	• AUTO: Maps to C6S-P as ACPI C2 • Disable: Don't enumerate any C6S state in ACPI • C6S as ACPI C2/C3: Enumerate C6S as ACPI C2/C3 state. PkgC6 is not allowed • C6S-P as ACPI C2/C3: Enumerate • C6S-P as ACPI C2/C3 state. PkgC6 is allowed.		
		►Auto	Disable	C6S as ACPI C2
		C6S as ACPI C3	C6S-P as ACPI C2	C6S-P as ACPI C3
Package C State Control	Package C State setting.			
	Package C State	Package C State limit, the state Auto maps is program specific.		
		C0/C1 state	C2 state	
		C6(non Retention) state	No Limit	
		►Auto		
	PKG CST CONFIG CONTROL MSR Lock	Enable - MSR E2h will be locked. Power Good reset is needed to remove lock bits.		
		Enable	►Disable	
	C2C3TT	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = C2C3TT CSR Bit[11:0].		
		0		
	LTR IIO Input	Take IIO LTR input: MSR 1FCh Bit[35] = 0 Ignore IIO LTR input: MSR 1FCh Bit[35] = 1.		
		Take IIO LTR input.	►Ignore IIO LTR input.	
	Latency Tolerance Requirement (LTR)	Program PCIE_ILTR_OVRD CSR Sub Menu.		
		PCIe ILTR Override Control	Allows manual overrides for PCIE_ILTR_OVRD	
			Enable	►Disable

CPU Thermal Management	CPU Thermal Related setting.			
	Prochot Response Power	System will be below this power limit when xxPROCHOT is asserted. Unit = 0.125 W. The PROCHOT response power physical bounds are set inside the CPU. User is expected to run appropriate workload to determine the valid range of power consumption. Default value = TDP.		
		0		
	Prochot Response Lock	Lock the Prochot settings until next reset.		
		Enable	►Disable	
	Therm-Monitor-Status Filter	Enables Filter based therm_monitor_status(IA32_THERM_STATUS[0]) reporting.		
		Enable	►Disable	
	TCC Activation Offset	Offset from factory set TCC activation temperature at which the Thermal Control Circuit must be activated.		
		0		
CPU- Advanced PM Tuning	Setting UFS, Energy Per Bias, Pwr_Ctl etc.			
	Uncore Freq Control	Mode 0: Power Limited Ordered Throttling Mode 1: Power Limited Proportional Throttling		
		Mode 0	►Mode 1	
	Uncore Freq Ratio:	0: Set dynamic Uncore frequency range from max and min fused values. Otherwise Uncore will run at a constant frequency ratio, the UFS algorithm will be disabled, but physical limits may still reduce frequency.		
		0		
	Energy Perf BIAS	Energy Perf BIAS Sub Menu.		
		Power Performance Tuning	Options decides who Controls EPB. • In OS mode: IA32_ENERGY_PERF_BIAS is used • In BIOS mode: ENERGY_PERF_BIAS_CONFIG is used • In PECI mode: PCS53 is used	
			►OS Controls EPB	BIOS Controls EPB	PECI Controls EPB
		Dynamic Loadline Switch	Dynamic Loadline Switch control. MSR 0x1FC[Bit33].	
			►Enable	Disable
		Workload Configuration	This allows optimization for the workload characterization. The three options for selection.	
			►Balanced	I/O sensitive
		Averaging Time Window	This is used to control the effective window of the average for C0 and P0 time.	
			1A	
		P0 TotalTimeThres-hold Low	The HW switching mechanism DIABLES the performance setting (0) when the totoal P0 time is less than this threshold.	
			28	
		P0 TotalTimeThres-hold High	The HW switching mechanism ENABLES the performance setting (0) when the totoal P0 time is greater than this threshold.	
			3F	

SOCKET RAPL Config	SOCKET RAPL Configuration Sub Menu - TURBO_POWER_LIMIT CSR & MSR.							
	Package RAPL Limit MSR&TPMI Lock	Enable/Disable locking of Package RAPL Limit MSR&TPMI and a reset will be required to unlock the register.						
		Enable			►Disable			
	Package RAPL Limit CSR Lock	Enable/Disable locking of Package RAPL Limit CSR and a reset will be required to unlock the register.						
		►Enable			Disable			
	PL1 Power Limit	PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the Fused TDP value will be programmed. A value greater than Fused TDP value will not be programmed.						
		0						
	PL1 Time Window	PL1 value in seconds. The value may vary from 1 to 5. Indicates the time window over which TDP value should be maintained.						
		►1	1.25	1.5	1.75	2	2.5	3	3.5
		4	5						
	PL2 Power Limit	PL2 Power Limit in Watts. The value may vary from 0 to 120% Fused TDP Value. If the value is 0, BIOS programs 120% * Fused TDP value.						
		0						
	PL2 Time Window	PL2 value in seconds. The value may vary from 0.012 to 0.039. Indicates the time window over which TDP value should be maintained.						
		►0.012	0.014	0.016	0.02	0.023	0.027	0.031	0.039
System Power Control (Psys)	System Power Control (Psys) Sub Menu.							
	Platform RAPL Limit CSR Lock	Enable/Disable locking of Platform Power Limit CSR and a reset will be required to unlock the register.						
		►Enable			Disable			
	Platform RAPL Info Lock	Enable/Disable locking of Platform Power Info registers and a reset will be required to unlock the register.						
		►Enable			Disable			
	Platform RAPL Limit&Info	Configure Platform RAPL Limit and Info by Platform Power Limit and Info CSR. SKIP: Use hardware default Manual: External customer to input manually Other options: Predefined board configures (PSU Config 1: 1600W PSU, PSU Config 2: 2130W PSU)						
		►SKIP		Beechnut City 1x PSU Config1		Beechnut City 1x PSU Config2		Beechnut City 2x PSU Config1	
		Beechnut City 2x PSU Config2		Beechnut City 3x PSU Config1		Manual			
	Platform RAPL Domain	Configure Psys socket primary and secondary by B2P mailbox PSYS_CONFIG. SKIP: Use hardware default Manual: External customer to input manually BEECHNUTCITY Domain Config 1: Even socket is primary and odd socket is secondary BEECHNUTCITY Domain Config 2: Even socket is secondary and odd socket is primary						
		►SKIP				BEECHNUTCITY Domain Config 1			
		BEECHNUTCITY Domain Config 2				Manual			

PMax Detector Configuration	PMax Detector Control Sub Menu.				
	PMax Config Sign	Negative: Detector will trip on higher power consumption. Positive: Detector will trip on lower power consumption.			
		►Positive	Negative		
	PMax Config Positive Offset	Input decimal correction factor to program. Valid input values are 0 to 63. Will be positive based on PMAX Config Sign value.			
		0			
	Trigger Setup	Possible selection options [0], [1], [2] [0] = Interaction disabled (default) [1] = Enable external trigger mode [2] = Enable internal trigger observability			
		0			
Memory Power & Thermal Configuration	Displays and provides options to change the Memory Settings.				
	DRAM RAPL Configuraion	DRAM RAPL Control Sub Menu.			
		DRAM RAPL Power Limit Lock CSR	This Option allows unlock/lock DRAM_PLANE_POWER_LIMIT.pp_pwr_lim_lock. Enable - Lock Disable - Unlock		
			►Enable	Disable	
		Override BW_LIMIT_TF	Allows custom tuning of BW_LIMIT_TF		
			0		
	Memory Thermal	Set memory thermal settings.			
		Throttling Mode	Configure Thermal Throttling Mode.		
			►CLTT	CLTT with PECI	Disable
		MEMTRIP REPORTING	Disable - Processor will ignore all Mem Trip tree. Enable - Processor will include all Mem Trip tree.		
			Enable	►Disable	
	MR4 based 2x Refresh	Enable MR4 based 2x Refresh			
		Enable	►Disable		
	DDR 2x Refresh Enable	Enable/Disable 2x Refresh. Auto= dynamically			
		►Auto	Enable	Disable	
	Select Temperature Refresh Value	Option to manually enter Temperature refresh value. Select Manual to enter value, Auto for default.			
		►Auto	Manual		
	Dimm Temperature Offset Cooling Type	DIMM cooling type to define temperature Offset value.			
		►Air cooling	Liquid cooling (tube)	Immersion cooling	
	MEMHOT INPUT	Configue Memhot input.			
		►Enable	Disable		
	MEMHOT OUTPUT	Configure MEMHOT Output Mode options: Enable/Disable the Throt Output high, mid and low bit fields.			
		Disabled	►Enable only temphi	Enable only temphi & mid	Enable only temphi, mid and low
	Memory Power Savings Advanced Options	Advanced Settings for CKE and related Memory Power Savings Features.			
		CKE Throttling	Configures CKE Throttling.		
			►Auto	Manual	

4.7 Server Mangement



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

4.7.1 System Event Log

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

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

4.7.2 BMC Network Configuration

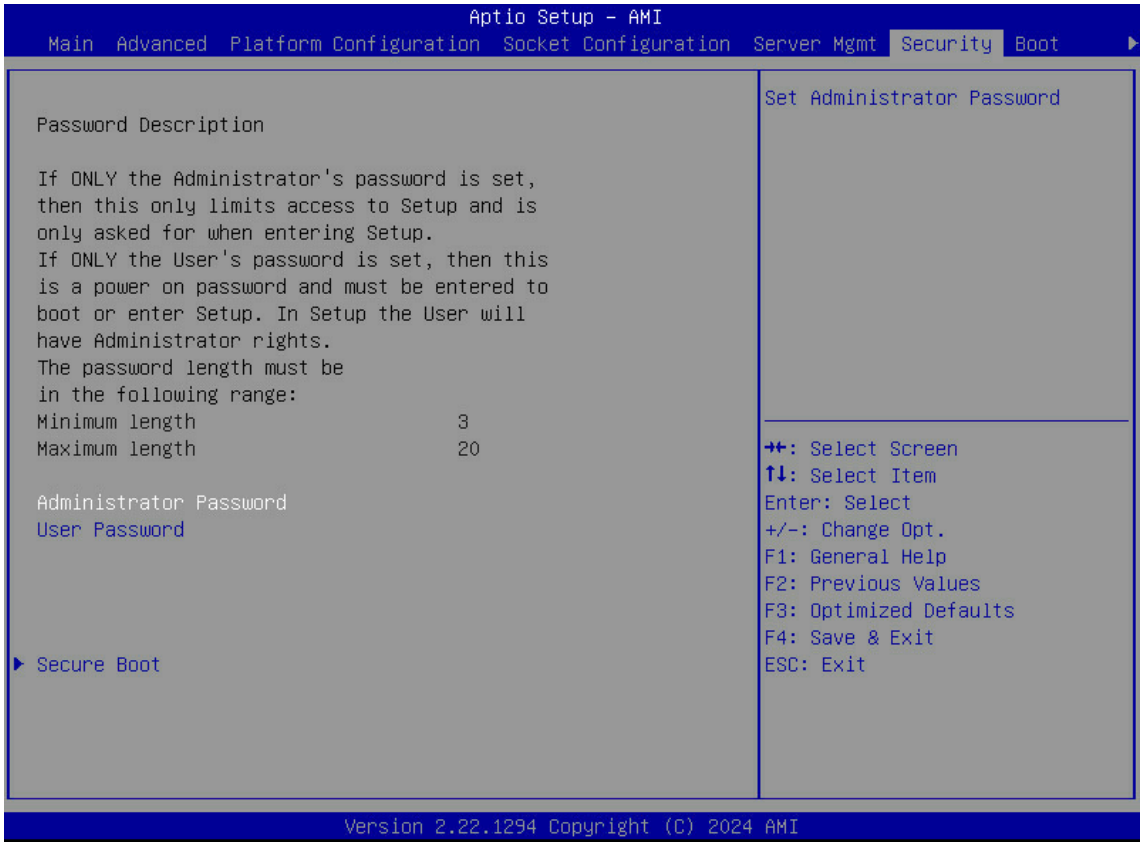
Configures BMC network parameters.

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

4.7.3 View System Event Log

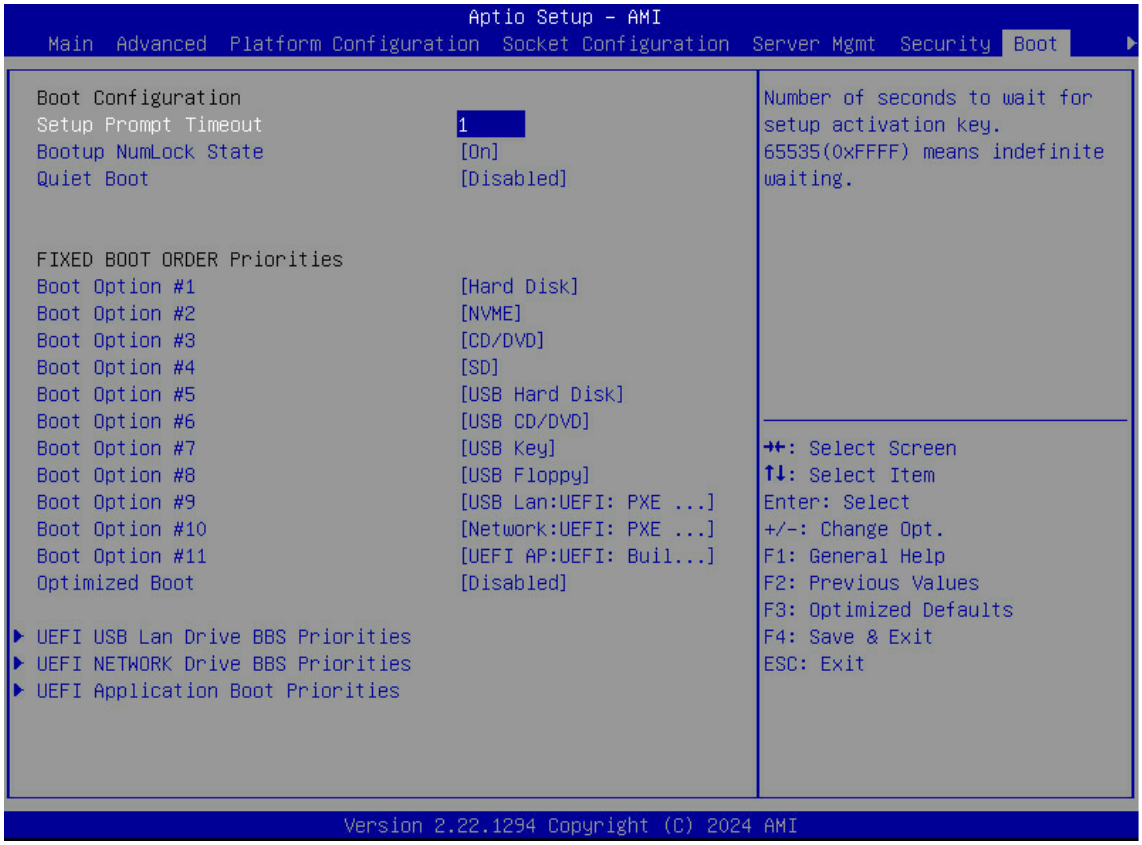
Press <Enter> to view the System Event Log Records.

4.8 Security



Security			
Administrator Password	Set administer password.		
User Password	Set User Password.		
Secure Boot	Secure boot configuration.		
	Secure Boot	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset.	
		▶Enabled	Disabled
	Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.	
		▶Standard	Custom

4.9 Boot

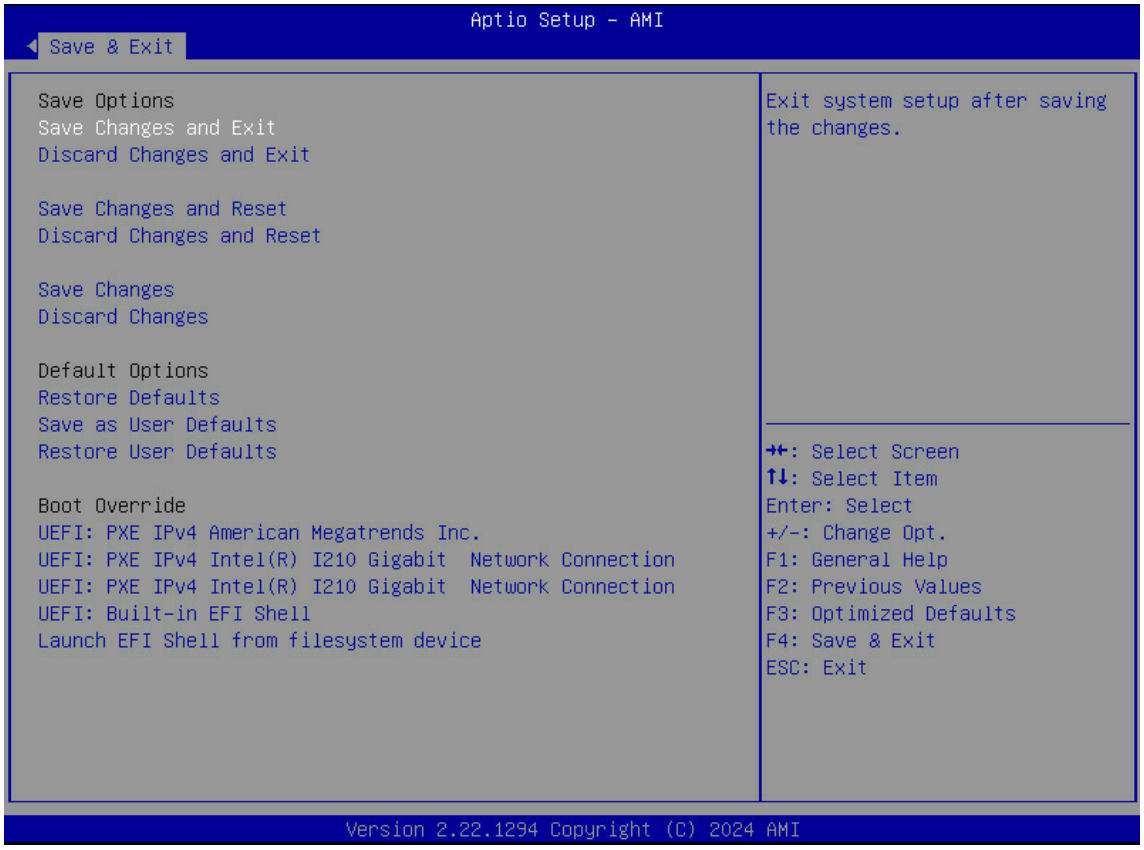


Boot		
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.	
	1	
Bootup NumLock State	Select the keyboard NumLock state.	
	▶On	Off
Quiet Boot	Enables or disables Quiet Boot option.	
	Enable	▶Disable
Boot Option #1	Sets the system boot order.	
	▶Hard Disk	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #2	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	▶NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled

Boot Option #3	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	▶CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #4	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	▶SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #5	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	▶USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #6	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	▶USB CD/DVD
	USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #7	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	▶USB Key	USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #8	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	▶USB Floppy
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled
Boot Option #9	Sets the system boot order.	
	Hard Disk// Move "*" to the desired Option	NVME
	CD/DVD	SD
	USB Hard Disk	USB CD/DVD
	USB Key	USB Floppy
	▶USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection
	UEFI AP:UEFI: Built-in EFI Shell	Disabled

Boot Option #10	Sets the system boot order.		
	Hard Disk// Move "*" to the desired Option	NVME	
	CD/DVD	SD	
	USB Hard Disk	USB CD/DVD	
	USB Key	USB Floppy	
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	►Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection	
	UEFI AP:UEFI: Built-in EFI Shell	Disabled	
Boot Option #11	Sets the system boot order.		
	Hard Disk// Move "*" to the desired Option	NVME	
	CD/DVD	SD	
	USB Hard Disk	USB CD/DVD	
	USB Key	USB Floppy	
	USB Lan:UEFI: PXE IPv4 American Megatrends Inc.	Network:UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection	
	►UEFI AP:UEFI: Built-in EFI Shell	Disabled	
Optimized Boot	Enables or disables Optimized Boot. Enabling Optimized Boot will disable Csm support and disable connecting Network devices to decrease boot time. While disabling Optimized Boot, make sure to restore Csm Support option to previous value before enabling Optimized Boot.		
	Enable	►Disable	
UEFI USB Lan Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI USB Lan Drives.		
	Boot Option #1	Sets the system boot order.	
		►UEFI: PXE IPv4 American Megatrends Inc.	Disable
UEFI NETWORK Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI NETWORK Drives.		
	Boot Option #1	Sets the system boot order.	
		►UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection	UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection / Disable
	Boot Option #2	Sets the system boot order.	
		UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection)	►UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection / Disable
UEFI Application Boot Priorities	Specifies the Boot Device Priority sequence from available UEFI Application.		
	Boot Option #1	Sets the system boot order.	
		►UEFI: Built-in EFI Shell	Disable

4.10 Save & Exit



Exit	
Save Changes and Exit	Exit system setup after saving the changes.
Discard Changes and Exit	Exit system setup without saving any changes.
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Reset system setup without saving any changes.
Save Changes	Save changes done so far to any of the setup options.
Discard Changes	Discard changes done so far to any of the setup options
Restore Defaults	Restore/Load Default values for all the setup options.
Save as User Defaults	Save the changes done so far as User Defaults.
Restore User Defaults	Restore the User Defaults to all the setup options.
UEFI: PXE IPv4 American Megatrends Inc.	
UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection)	
UEFI: PXE IPv4 Intel(R) I210 Gigabit Network Connection)	
UEFI: Built-in EFI Shell	
Launch EFI Shell from filesystem device	Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

4.11 BIOS Update Process

This is the manual for updating BIOS on **Sirius** system. Please check current system BIOS version is Sirs0010 or later. Here are the update procedures.

EFI:
1. Copy Sirs0010.bin to EFI folder
2. Copy EFI folder to USB stick or HDD
3. Boot into internal shell enters the usb EFI folder and executes the below command flash.nsh
4. If the firmware update is complete, perform an AC power cycle.

Linux:
1. Copy Sirs0010.bin to AfuLnx64 folder
2. Copy AfuLnx64 folder to USB stick or HDD
3. Enter to AfuLnx64 folder and execute the below command./flash.sh
4. Reboot if complete the updated



NOTE

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

4.12 BIOS Post Code

There are two ways to get post code,

1. Check the LED debug card
2. Execute the IPMI command as below

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

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

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

Intel RC POST Code

Post Code	Description
KTI POST code - Major	
0xA0	Initialize KTI input structure default values
0xA1	Collect info such as SBSP, Boot Mode, Reset type etc
0xA3	Setup up minimum path between SBSP & other sockets
0xA6	Sync up with PBSPs
0xA7	Topology discovery and route calculation
0xA8	Program final route
0xA9	Program final IO SAD setting
0xAA	Protocol layer and other Uncore settings
0xAB	Transition links to full speed operation
0xAE	Coherency Settings
0xAF	KTI is done
KTI Error code	
0xD8	Boot Mode Error
0xD9	Minimum Path Setup Error
0xDA	Topology Discovery Error
0xDB	SAD Setup Error
0xDC	Unsupported Topology Error
0xDD	Full Speed Transition Error
0xDE	S3 Resume Error
0xDF	SW Check Error
0xE0	2LM SUPPORT Error
MRC Test Points	
0x70	HBM State
0x71	HBM Debug State
0x72	HBM Internal State
0x73	NVRAM Socket
0x74	DDR MBIST
0x7D	Automation Test
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
0xD6	Offset Training Result
0xD7	DIMM Manifest
0xD8	Turn Around
0xD9	CPGC OOO Mode
0xDA	Actm Mem Alias
0xDB	Enable Host Refresh
0xDC	SGX TDX Configure
0xDD	Disable Unused Memory Channel
0xDE	Security Pre MEM Decode
0xDF	Memory Security Pre MEM
0xE0	Rx Data Calibration
0xE1	MMC
0xE2	Population POR
0xE3	Domain Security Pre MEM

MRC error code	
0xE1	ERR_STAGGERED_SYNC
0xE2	RC Internal2 Error
0xE3	Microcontroller Error
0xE6	RC DCA DFE Error
0xE7	RC Sweep LIB Internal Error
0xE8	No Memory Error
0xE9	LT Lock Error
0xEA	DDR Init Error
0xEB	Memory Test Error
0xEC	Vendor Specific Error
0xED	DIMM Incompatible Error
0XEE	MRC Compatibility Error
0xEF	MRC Structure Error
0xF0	Set Vdd Error
0xF1	IOT Memory Buffer Error
0xF2	RC Internal Error
0xF3	Invalid Register Access Error
0xF4	Set MC Freq Error
0xF5	Read MC Freq Error
0x70	DIMM Channel Error
0x74	BIST Check Error
0x75	DDR Freq Not Found Error
0x76	PIPE Error
0xF6	SMBUS Error
0xF7	PCU Error
0xF8	NGN Error
0xF9	Interleave Failure
0xFA	SKU Limit Error
0xFB	CAR Limit Error
0xFC	CMI Failure
0xFD	Value Out of Range
0xFE	DDRIO HWFSM Error
0xFF	MRC Pointer Error

AMI POST Code

Post Code	Description
0x10	PEI core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization is started (CPU module specific)
0x13	Pre-memory CPU initialization is started (CPU module specific)
0x14	Pre-memory CPU initialization is started (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x17	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x18	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1D~ 0x2A	Oem pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect(SPD) data reading
0x2C	Memory initialization. Memory Presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization. (Other)
0x30	Reserved for ASL (See ASL status codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. BootStrap Processor(BSP) initialization
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-memory North Bridge initialization is started
0x38	Post-memory North Bridge initialization is started (North Bridge module specific)
0x39	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3A	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3B	Post-memory South Bridge initialization is started
0x3C	Post-memory South Bridge initialization is started (South Bridge module specific)

0x3D	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3E	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3F~0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
S3 resume progress codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by th DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4~0xE7	Reserved for future AMI progress codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loadded
0xF5~0xF7	Reserved for future AMI progress codes

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

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

Chapter 5. BMC Configuration Settings

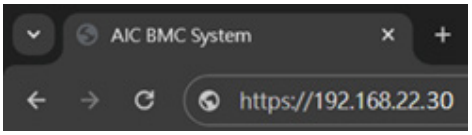
5.1 Login

NOTE
For further details about the BMC, please refer to Sirius BMC Manual for reference.
AIC® website link: https://www.aicipc.com/en/productdetail/51518.

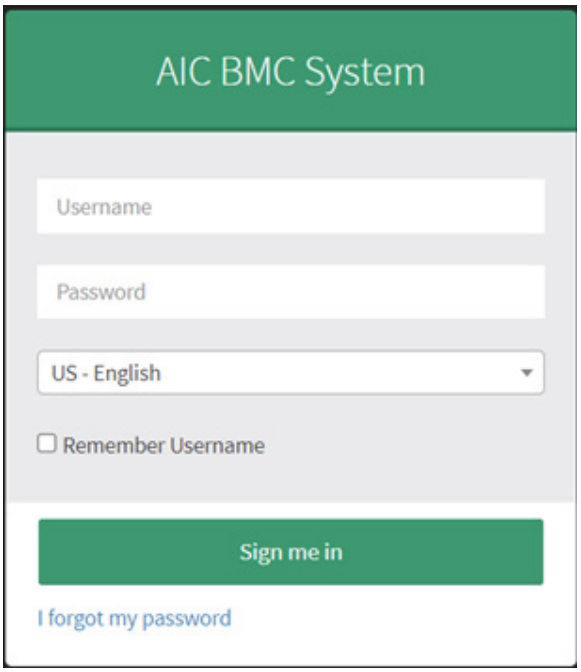
The computer and BMC need to be on the same subnet. After setting the static IP, they should be able to communicate. To establish a connection, follow the steps below.

Step 1 Use the computer's terminal to ping the BMC IP address and ensure that it can be pinged.

Step 2 If the BMC IP address is pingable, open a web browser on your computer, enter the BMC IP address in the URL bar.



Step 3 Initial access prompts you to enter the User Name and Password. A sample screenshot of the login screen is given below.



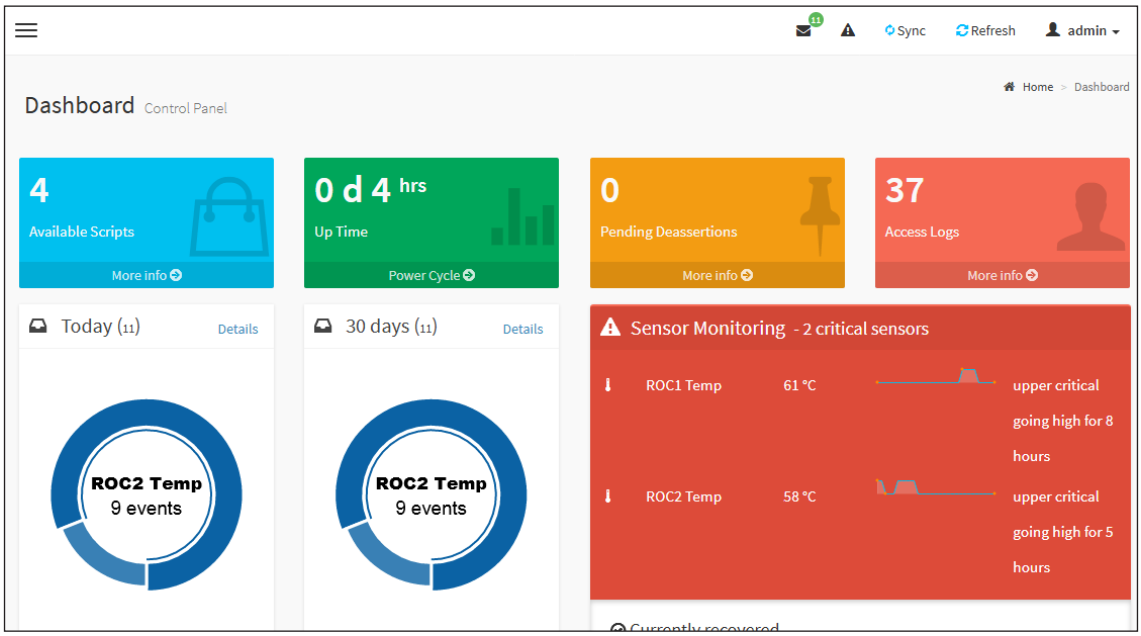
Default Username: **admin**
Default Password: **admin**

5.2 Web UI Common Features

The following content is a brief description of the menu bar. For further details about the BMC, please refer to Sirius BMC Manual for reference.
AIC® website link: https://www.aicipc.com/en/productdetail/51518.

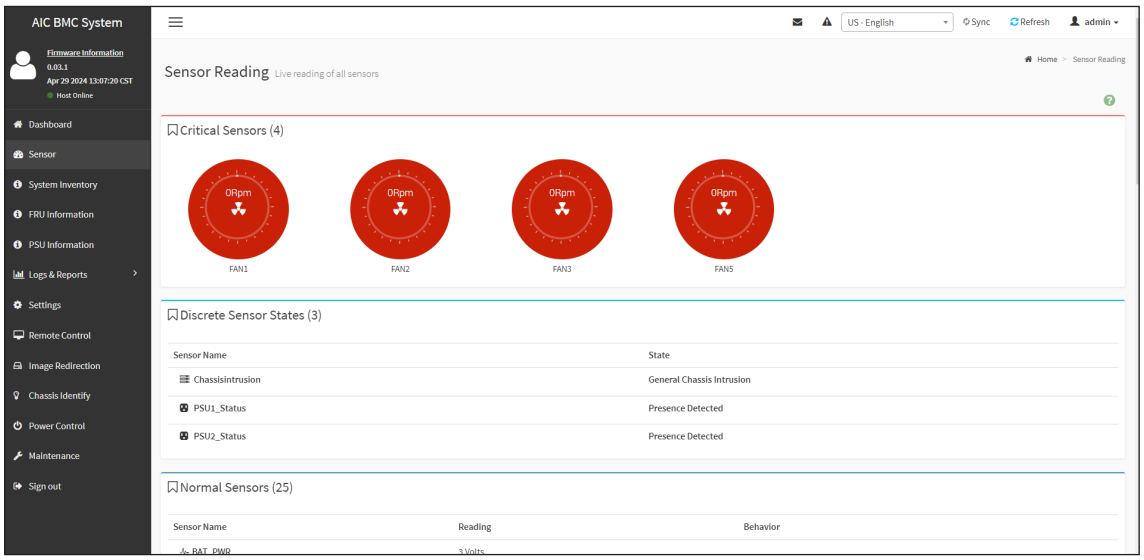
5.2.1 Dashboard

The Dashboard page gives the overall information about the status of a device.
To open the Dashboard page, click Dashboard from the menu bar. A sample screenshot of the Dashboard page is shown below.



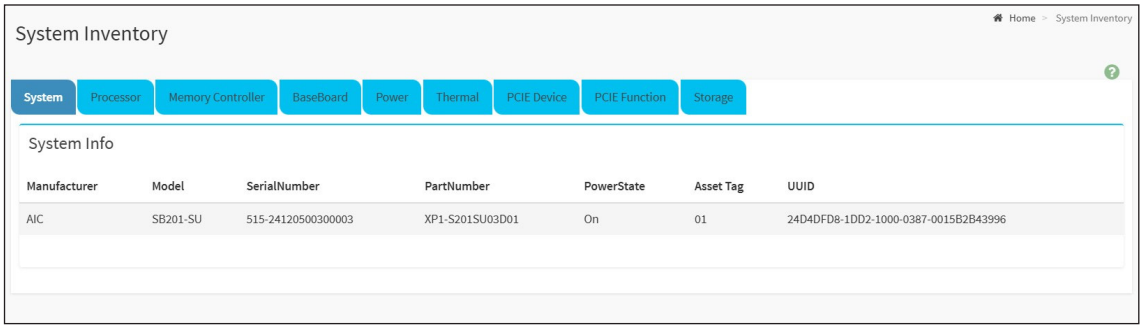
5.2.2 Sensor

The Sensor Reading page displays all the sensor related information.
To open the Sensor Reading page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.
A screenshot of Sensor Reading page is given below.



5.2.3 System Inventory

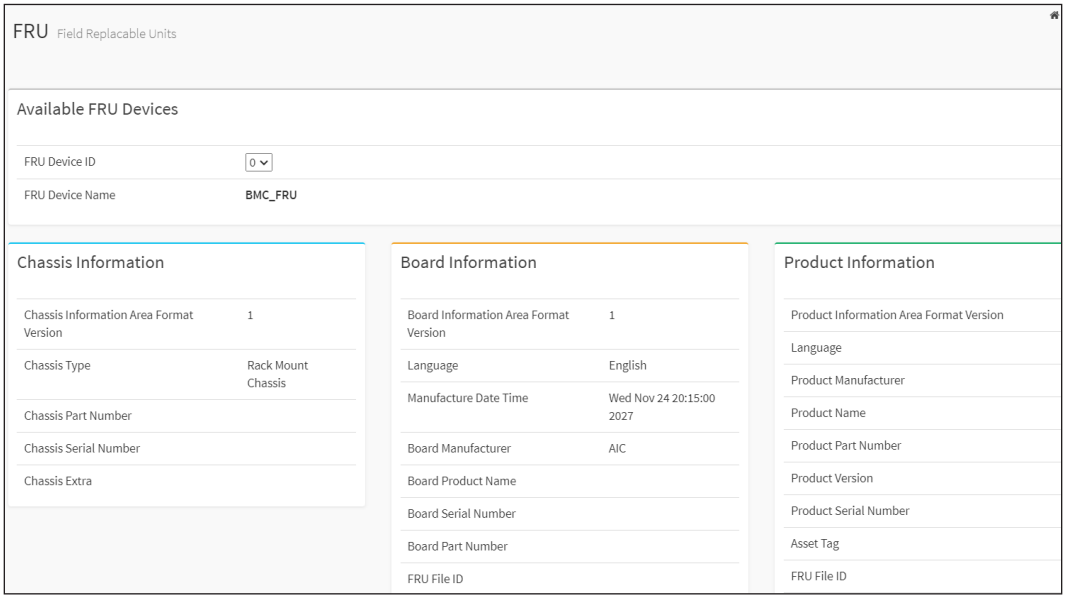
To open System Inventory main page, click System Inventory from the menu bar.
A screenshot displaying the menu items under System Inventory is shown below:



5.2.4 FRU Information

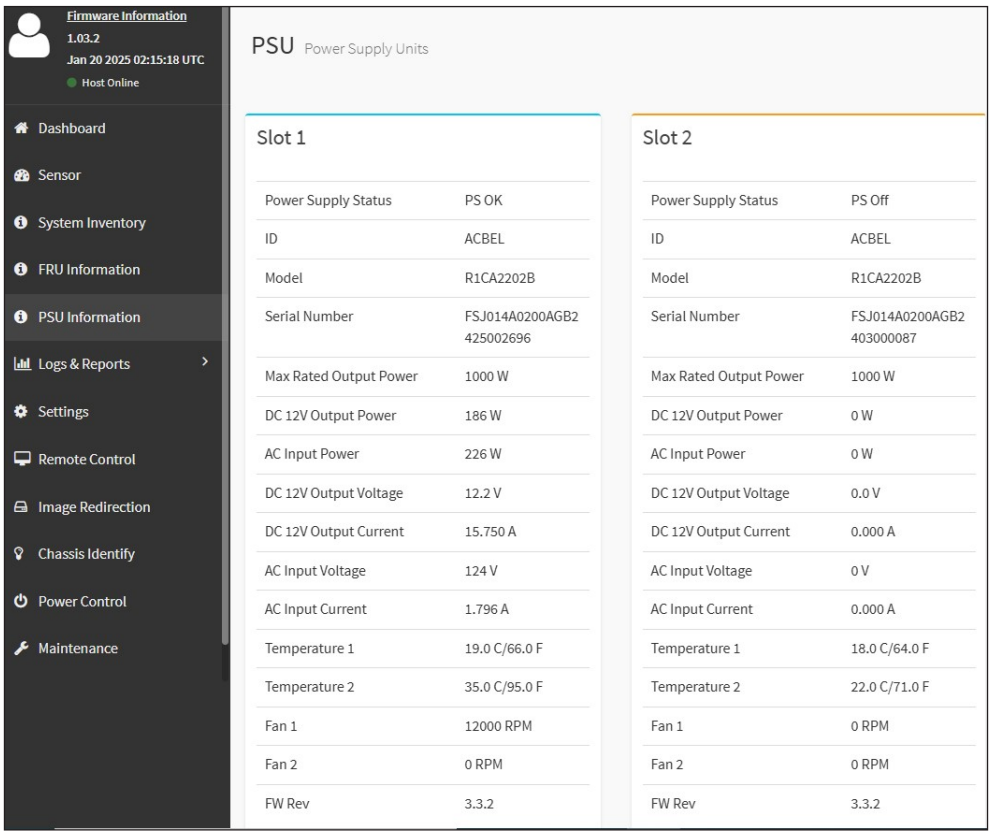
FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information page, click FRU Information from the menu bar. Select a FRU Device ID from the FRU Information section to view the details of the selected device. A screenshot of FRU Information page is given below.



5.2.5 PSU Information

To open the PSU Information page, click PSU Information from the menu bar. A screenshot of PSU Information page is given below.

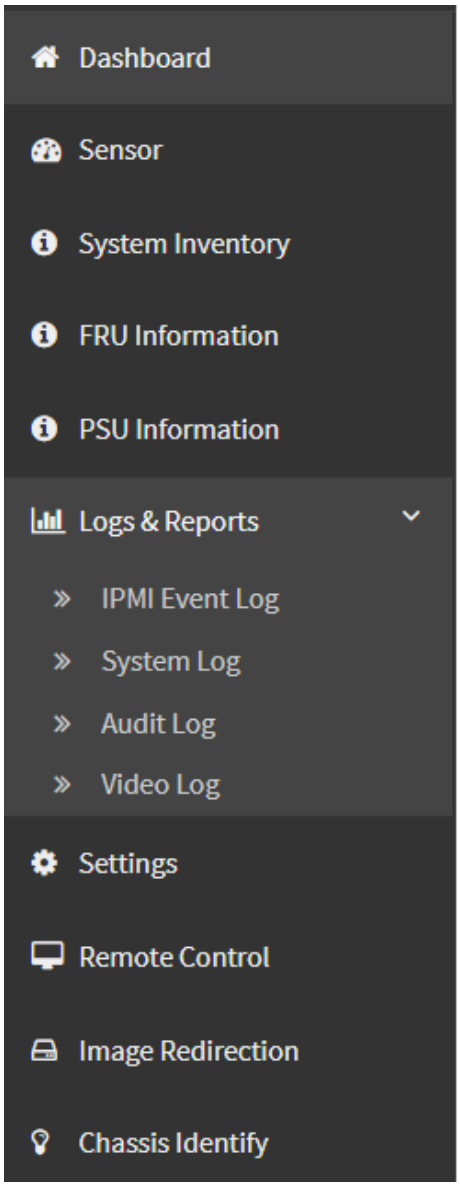


5.2.6 Logs & Report

To open the Logs & Reports page, click Logs & Reports from the menu bar. The Logs & Reports page displays the following information.

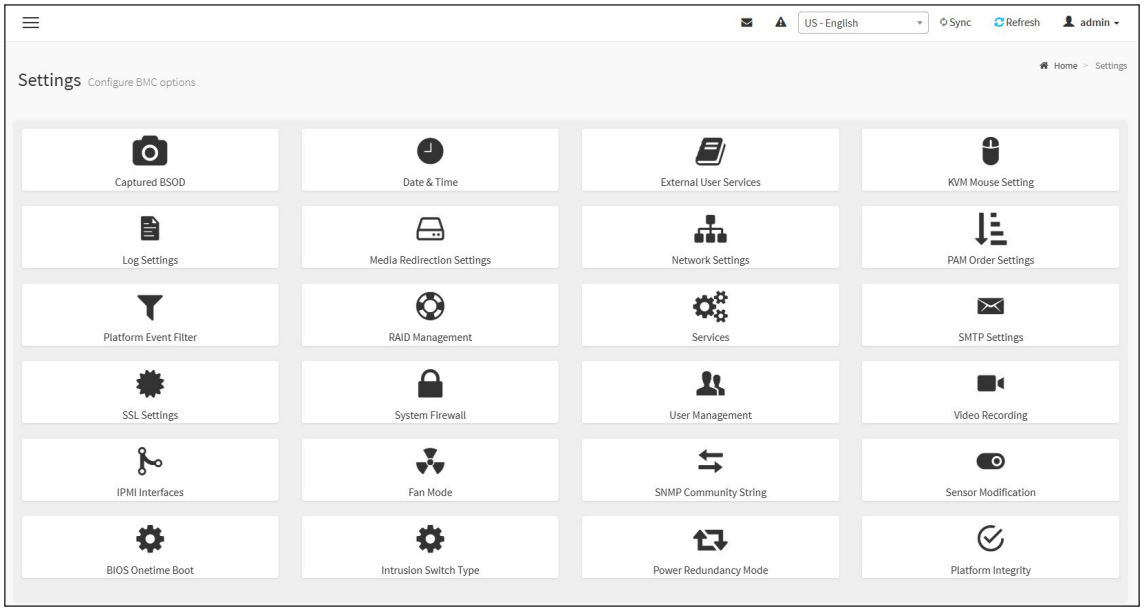
- IPMI Event Log
- System Log
- Audit Log
- Video Log

A screenshot displaying the menu items under Logs & Reports is shown below



5.2.7 Settings

To open the Settings page, click Settings from the menu bar. This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.

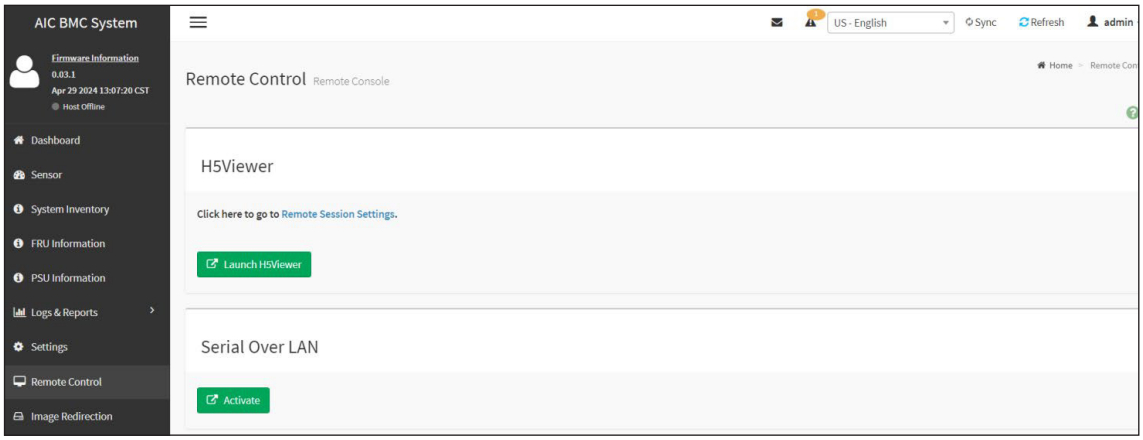


A detailed description of the Configuration menu is given below.

5.2.8 Remote Control

Click Remote Control from the menu bar. A sample screenshot is displayed below.

- Launch H5Viewer
- Serial Over LAN



5.2.9 Images Redirection

This page is used to configure the images into BMC for redirection. This can be done either by uploading an image into BMC say, **Local Media** or by mounting the image from the remote system, **Remote Media**.
To open Images Redirection page, click Images Redirection from the menu bar.
A sample screenshot of Images Redirection page is shown below.



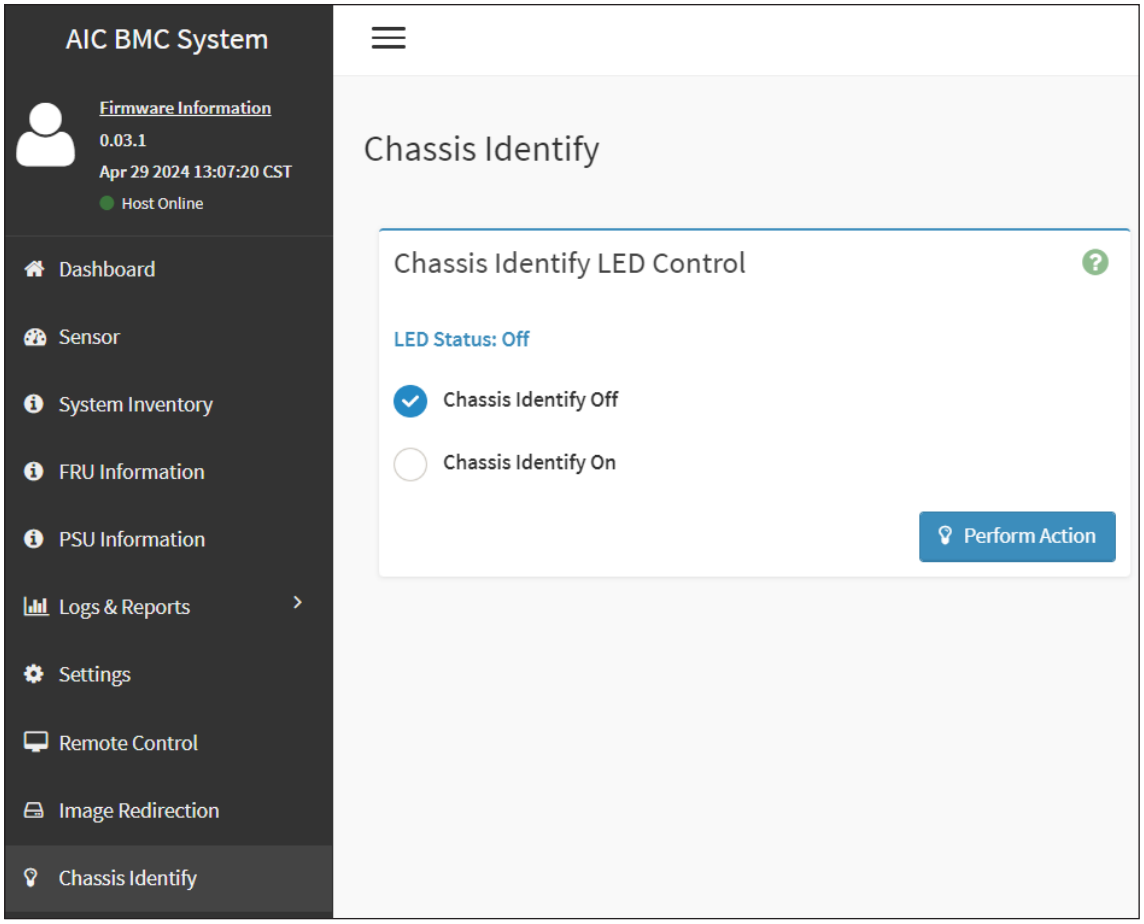
The fields of Images Redirection page are explained below.

- Remote Images

NOTE
Media will always be redirected using the lowest available instance number, regardless of the instance slot opted in Web UI. This is applicable for both local and remote media images.

5.2.10 Chassis Identify

To open Chassis Identify, click Chassis Identify from the menu bar. A sample screenshot of Chassis Identify is shown below.

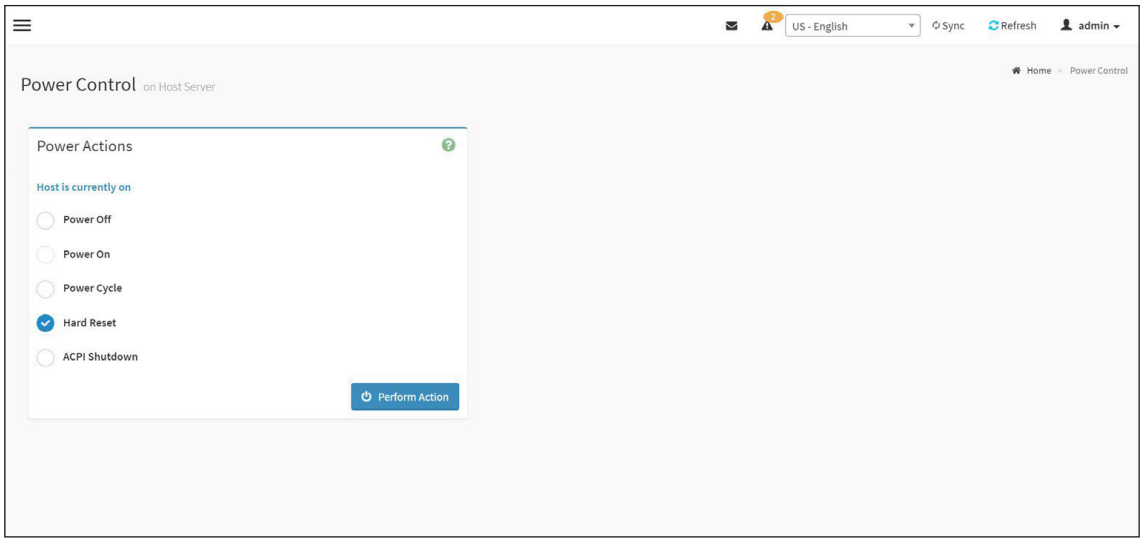


The various options of Chassis Identify are given below.

- Chassis Identify Off: This option will turn off the Chassis Identify LED.
- Chassis Identify On: This option will turn on the Chassis Identify LED.

5.2.11 Power Control

This page allows you to view and control the power of your server.
To open Power Control, click Power Control from the menu bar. A sample screenshot of Power Control is shown below.



The various options of Power Control are given below.
Power Off: To immediately power off the server.
Power On: To power on the server.
Power Cycle: This option will first power off, and then reboot the system (cold boot).
Hard Reset: This option will reboot the system without powering off (warm boot).
ACPI Shutdown: This option to initiate operating system shutdown prior to the shutdown.
Perform Action: Click this option to perform the selected operation.

Procedure
Select an action and click **Perform Action** to proceed with the selected action.

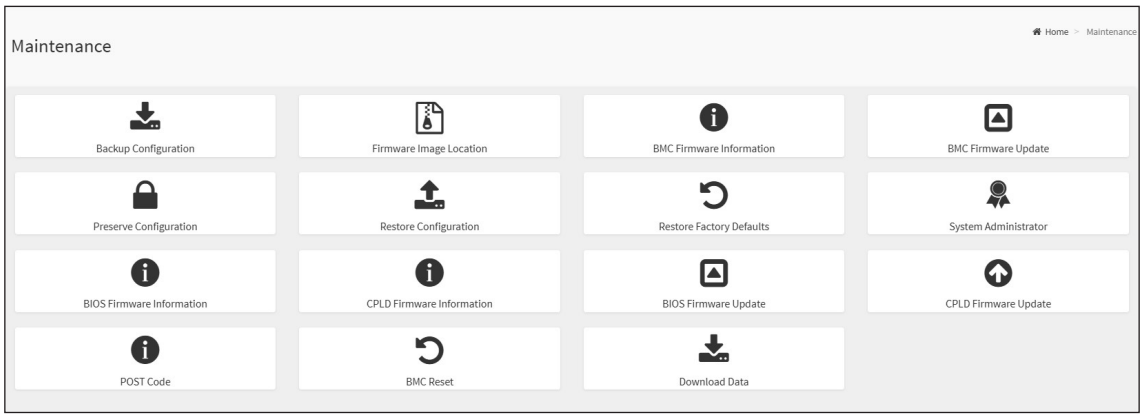
NOTE
During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

5.2.12 Maitenance

To open the Maintenance page, click Maintenance from the menu bar. This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

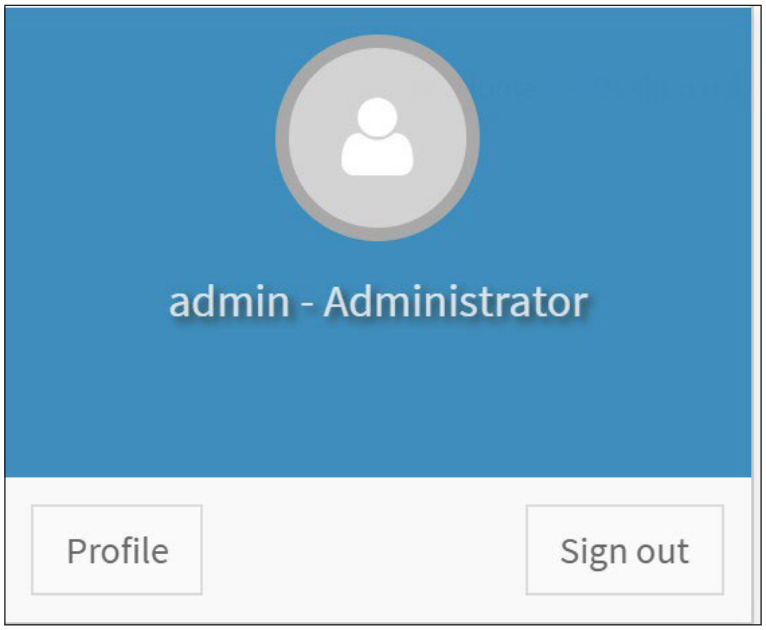
- Backup Confifiguration
- Firmware Image Location
- BMC Firmware Information
- BMC Firmware Update
- Preserve Confifiguration
- Restore Confifiguration
- Restore Factory Defaults
- System Administrator
- BIOS Firmware Information
- CPLD Firmware Information
- BIOS Firmware Update
- CPLD Firmware Update
- POST Code
- BMC Reset
- Download Data

A sample screenshot of Maintenance page is displayed below.



5.2.13 Sign Out

To log out from, click the admin on the top right corner of the screen. A sample screenshot of admin option is shown below.



Click **Sign Out** to perform log out. A Warning message will be prompted you to proceed further, click **OK** to log out or **Cancel** to retain the interface.

Chapter 6. Technical Support

www.aicipc.com

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

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

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

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

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

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

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

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